aws

Guía GuardDuty del usuario de Amazon

Amazon GuardDuty

Amazon GuardDuty: Guía GuardDuty del usuario de Amazon

Table of Contents

¿Qué es Amazon GuardDuty?

Amazon GuardDuty es un servicio de supervisión de seguridad que analiza y procesa eventos de AWS CloudTrail administraciónOrígenes de datos fundamentales, registros de AWS CloudTrail eventos, registros de flujo de VPC (de instancias de Amazon EC2) y registros de DNS. También procesa características como los registros de auditoría de Kubernetes, la actividad de inicio de sesión de RDS, los registros de S3, los volúmenes de EBS, la supervisión en tiempo de ejecución y los registros de la actividad de red de Lambda. Utiliza fuentes de información de amenazas, como listas de direcciones IP y dominios malintencionados, y machine learning para identificar la actividad inesperada y potencialmente no permitida, así como la actividad malintencionada en su entorno de AWS. Esto puede incluir problemas como el escalado de privilegios; el uso de credenciales expuestas; la comunicación con direcciones IP o dominios malintencionados; la presencia de malware en las cargas de trabajo de los contenedores y las instancias de Amazon EC2; o la detección de patrones atípicos de eventos de inicio de sesión en la base de datos. Por ejemplo, GuardDuty puede detectar instancias EC2 comprometidas y cargas de trabajo de contenedores que sirven para generar malware o minar bitcoins. También supervisa el comportamiento de acceso a las cuentas de AWS en busca de señales de peligro, como implementaciones de infraestructura no autorizadas (por ejemplo, la implementación de instancias en una región que no se ha usado nunca) o llamadas a la API atípicas (por ejemplo, el cambio de la política de contraseñas para reducir la complejidad de las contraseñas).

GuardDuty le informa del estado de su AWS entorno mediante resultados de seguridad que puede ver en la GuardDuty consola o a través de Amazon EventBridge. GuardDuty también le ayuda a exportar sus hallazgos a un bucket de Amazon Simple Storage Service (S3) y a integrarlos con otros servicios, como DetectiveAWS Security Hub.

Precios para GuardDuty

Para obtener información sobre GuardDuty los precios, consulta Amazon GuardDuty Pricing.

Acceder GuardDuty

Puede trabajar con él GuardDuty de cualquiera de las siguientes maneras:

GuardDuty consola

https://console.aws.amazon.com/guardduty

La consola es una interfaz basada en navegador para obtener acceso y usar GuardDuty. La GuardDuty consola proporciona acceso a su GuardDuty cuenta, datos y recursos.

Herramientas de línea de comando de AWS

Con las herramientas de línea de AWS comandos, puede emitir comandos en la línea de comandos del sistema para realizar GuardDuty tareas y AWS tareas. Las herramientas de la línea de comandos son útiles si desea crear scripts que lleven a cabo tareas.

Para obtener información sobre la instalación y el uso de la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface. Para ver los AWS CLI comandos disponibles GuardDuty, consulte la referencia de comandos de CLI.

GuardDuty API HTTPS

Puedes acceder GuardDuty y AWS programar mediante la API GuardDuty HTTPS, que te permite enviar solicitudes HTTPS directamente al servicio. Para obtener más información, consulte la Referencia de la API de GuardDuty .

SDK de AWS

AWS ofrece kits de desarrollo de software (SDK) que se componen de bibliotecas y código de muestra para diversos lenguajes de programación y plataformas (Java, Python, Ruby, .NET, iOS, Android, etc.). Los SDK permiten crear cómodamente acceso mediante programación a GuardDuty. Para obtener información sobre los SDK de AWS (por ejemplo, cómo descargarlos e instalarlos), consulte Herramientas para Amazon Web Services.

Empezar con GuardDuty

Este tutorial proporciona una introducción práctica a GuardDuty. Los requisitos mínimos para GuardDuty habilitarla como cuenta independiente o como GuardDuty administrador se describen en el paso 1. AWS Organizations Los pasos 2 a 5 incluyen el uso de las funciones adicionales recomendadas por usted GuardDuty para aprovechar al máximo sus hallazgos.

Temas

Antes de empezar

GuardDuty es un servicio de detección de amenazas que supervisa Orígenes de datos fundamentales registros de AWS CloudTrail eventos, eventos AWS CloudTrail de administración, registros de flujo de Amazon VPC y registros de DNS. GuardDuty también analiza las funciones asociadas a sus tipos de protección solo si las habilita por separado. Las características incluyen los registros de auditoría de Kubernetes, la actividad de inicio de sesión de RDS, los registros de S3, los volúmenes de EBS, la supervisión en tiempo de ejecución y los registros de actividad de la red de Lambda. El uso de estas fuentes de datos y funciones (si están habilitadas) GuardDuty genera resultados de seguridad para su cuenta.

Después de habilitarlo GuardDuty, comienza a monitorear su entorno. Puedes inhabilitarla GuardDuty para cualquier cuenta de cualquier región y en cualquier momento. Esto impedirá el procesamiento GuardDuty de las fuentes de datos fundamentales y de cualquier función que estuviera habilitada por separado.

No necesita habilitar ninguno de los Orígenes de datos fundamentales de forma explícita. Amazon GuardDuty extrae flujos de datos independientes directamente de esos servicios. En el caso de una GuardDuty cuenta nueva, todos los tipos de protección disponibles compatibles con una Región de AWS están activados e incluidos en el período de prueba gratuito de 30 días de forma

predeterminada. Puede excluirse voluntariamente de uno o de todos ellos. Si ya es GuardDuty cliente, puede optar por activar alguno o todos los planes de protección disponibles en su Región de AWS cuenta. Para obtener más información, consulte Características asociadas a cada tipo de protección en GuardDuty.

Al habilitarla GuardDuty, tenga en cuenta los siguientes elementos:

- GuardDuty es un servicio regional, lo que significa que cualquiera de los procedimientos de configuración que siga en esta página debe repetirse en cada región con la que desee supervisar GuardDuty.

  Le recomendamos encarecidamente que lo habilite GuardDuty en todas AWS las regiones compatibles. Esto permite GuardDuty generar información sobre actividades no autorizadas o inusuales, incluso en las regiones que no está utilizando activamente. Esto también permite GuardDuty monitorear AWS CloudTrail los eventos para AWS servicios globales como IAM. Si no GuardDuty está habilitada en todas las regiones compatibles, se reduce su capacidad para detectar actividades que involucren servicios globales. Para obtener una lista completa de las regiones en las GuardDuty que está disponible, consulteRegiones y puntos de conexión.
- Cualquier usuario con privilegios de administrador en una AWS cuenta puede GuardDuty habilitarlos; sin embargo, siguiendo las prácticas recomendadas de seguridad en materia de privilegios mínimos, se recomienda crear un rol, usuario o grupo de IAM para administrarlo GuardDuty específicamente. Para obtener información sobre los permisos necesarios para habilitarlos, GuardDuty consultePermisos requeridos para habilitar GuardDuty.
- Cuando se habilita GuardDuty por primera vez en una región Región de AWS, de forma predeterminada, también se habilitan todos los tipos de protección disponibles y compatibles en esa región, incluida la protección contra malware. GuardDuty crea un rol vinculado a un servicio para tu cuenta llamado. `AWSServiceRoleForAmazonGuardDuty` Esta función incluye los permisos y las políticas de confianza que permiten GuardDuty consumir y analizar los eventos directamente desde ellos Orígenes de datos fundamentales para generar conclusiones de seguridad. La protección contra malware crea otro rol vinculado a un servicio para su cuenta llamado `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Esta función incluye los permisos y las políticas de confianza que permiten a Malware Protection realizar análisis sin agentes para detectar malware en su GuardDuty cuenta. Permite GuardDuty crear una instantánea del volumen de EBS en su cuenta y compartirla con la GuardDuty cuenta de servicio. Para obtener más información, consulte Permisos de rol vinculados al servicio para GuardDuty. Para obtener más información acerca de los roles vinculados a servicios, consulte Uso de roles vinculados a servicios.

- Cuando lo habilita GuardDuty por primera vez en una región, su AWS cuenta se inscribe automáticamente en una prueba GuardDuty gratuita de 30 días para esa región.

Paso 1: Habilita Amazon GuardDuty

El primer paso para usarlo GuardDuty es habilitarlo en su cuenta. Una vez activado, GuardDuty comenzará inmediatamente a monitorear las amenazas a la seguridad en la región actual.

Si, como GuardDuty administrador, desea gestionar GuardDuty los resultados de otras cuentas de su organización, debe añadir las cuentas de GuardDuty los miembros y activarlas también. Elija una opción para aprender a habilitarla GuardDuty en su entorno.

Standalone account environment

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/
2. Elija Comenzar.
3. Selecciona Activar GuardDuty.

Multi-account environment

> **Important**
>
> Como requisitos previos para este proceso, debe estar en la misma organización que todas las cuentas que desee administrar y tener acceso a la cuenta de AWS Organizations administración para delegar un administrador GuardDuty en su organización. Es posible que se necesiten permisos adicionales para delegar un administrador. Para más información, consulte Permisos necesarios para designar una cuenta de GuardDuty administrador delegado.

Para designar una cuenta de administrador delegado GuardDuty

1. Abra la AWS Organizations consola en https://console.aws.amazon.com/organizations/ con la cuenta de administración.
2. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   ¿ GuardDuty Ya está habilitada en tu cuenta?

- Si aún no GuardDuty está activado, puede seleccionar Comenzar y, a continuación, designar un administrador GuardDuty delegado en la GuardDuty página de bienvenida.
- Si GuardDuty está habilitada, puede designar un administrador GuardDuty delegado en la página de configuración.

3. Introduzca el ID de AWS cuenta de doce dígitos de la cuenta que desee designar como administrador GuardDuty delegado de la organización y seleccione Delegado.

> **Note**
>
> Si aún no GuardDuty está activado, la designación de un administrador delegado habilitará esa cuenta en GuardDuty su región actual.

Agregación de cuentas de miembro

Este procedimiento abarca la adición de cuentas de miembros a una cuenta de administrador GuardDuty delegado mediante. AWS Organizations También existe la opción de agregar miembros mediante invitación. Para obtener más información sobre ambos métodos para asociar miembros GuardDuty, consulte. Administrar varias cuentas en Amazon GuardDuty

1. Inicie sesión en la cuenta de administrado delegado
2. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
3. En el panel de navegación, elija Settings (Configuración) y Accounts (Cuentas).

   En la tabla de cuentas aparecen todas las cuentas de la organización.
4. Para elegir las cuentas que desea agregar como miembros, seleccione la casilla situada junto al ID de la cuenta. A continuación, en el menú Acción, seleccione Agregar miembro.

> **Tip**
>
> Puede automatizar la adición de nuevas cuentas como miembros activando la característica Habilitación automática; sin embargo, esto solo se aplica a las cuentas que se unen a su organización una vez habilitada la característica.

Paso 2: generación de resultados de muestra y exploración de las operaciones básicas

Cuando GuardDuty descubre un problema de seguridad, genera un hallazgo. Un GuardDuty hallazgo es un conjunto de datos que contiene detalles relacionados con ese problema de seguridad único. Los detalles del resultado se pueden utilizar para ayudarle a investigar el problema.

GuardDuty permite generar ejemplos de hallazgos con valores indicativos, que se pueden utilizar para probar la GuardDuty funcionalidad y familiarizarse con los hallazgos antes de tener que responder a un problema de seguridad real descubierto por GuardDuty la persona. Siga la guía que aparece a continuación para generar ejemplos de resultados para cada tipo de hallazgo disponible. Si desea conocer otras formas de generar ejemplos de resultados, incluida la generación de un evento de seguridad simulado en su cuenta, consulte. GuardDuty Hallazgos de ejemplo

Creación y exploración de los resultados de muestra

1. En el panel de navegación, seleccione Configuración.
2. En la página Settings, en Sample findings, elija Generate sample findings.
3. En el panel de navegación, elija Resumen para ver la información sobre los hallazgos generados en su AWS entorno. Para obtener más información acerca de los componentes del panel de resumen, consulte Panel Resumen.
4. En el panel de navegación, seleccione Findings (resultados). Los resultados de muestra se muestran en la página Resultados actuales con el prefijo [SAMPLE].
5. Seleccione un resultado de la lista para ver sus detalles.

    - Puede revisar los distintos campos de información disponibles en el panel de detalles del resultado. Los distintos tipos de resultados pueden tener campos diferentes. Para obtener más información acerca de los campos disponibles en todos los tipos de resultados, consulte Detalles de los resultados. Puede llevar a cabo las siguientes acciones en el panel de detalles:

        - Seleccione el ID de resultado en la parte superior del panel para abrir los detalles JSON completos del resultado. El archivo JSON completo también se puede descargar desde este panel. El JSON contiene información adicional que no se incluye en la vista de consola y es el formato que pueden incorporar otras herramientas y servicios.

- Consulte la sección Recurso afectado. Si se trata de una conclusión real, la información que aparece aquí le ayudará a identificar un recurso en su cuenta que deba investigarse e incluirá enlaces a los recursos adecuados AWS Management Console para utilizar.
- Seleccione los iconos de la lupa con el signo + o - para crear un filtro inclusivo o exclusivo para ese detalle. Para obtener más información acerca de los filtros de resultados, consulte Filtrado de hallazgos.

6. Archivado de todos los resultados de muestra

   a. Para seleccionar todos los resultados, marque la casilla de verificación situada en la parte superior de la lista.

   b. Anule la selección de los resultados que desee conservar.

   c. Seleccione el menú Acciones y, a continuación, seleccione Archivar para ocultar los resultados de muestra.

> **Note**
>
> Para ver los resultados archivados, seleccione Actual y, a continuación, Archivado para cambiar la vista de los resultados.

Paso 3: Configurar la exportación de GuardDuty los resultados a un bucket de Amazon S3

GuardDuty recomienda configurar los ajustes para exportar los hallazgos, ya que le permite exportar los hallazgos a un bucket de S3 para su almacenamiento indefinido más allá del período de retención de GuardDuty 90 días. Esto le permite mantener un registro de los hallazgos o realizar un seguimiento de los problemas en su AWS entorno a lo largo del tiempo. El proceso que se describe aquí explica cómo configurar un nuevo bucket de S3 y crear una nueva clave de KMS para cifrar los resultados desde la consola. Para obtener más información al respecto, incluido cómo utilizar su propio bucket existente o uno de otra cuenta, consulte Exportación de resultados.

Configuración de la opción de exportación de resultados de S3

1. Para cifrar los hallazgos, necesitará una clave KMS con una política que permita GuardDuty usar esa clave para el cifrado. Los siguientes pasos le ayudarán a crear una nueva clave de KMS. Si utilizas una clave KMS de otra cuenta, debes aplicar la política de claves iniciando sesión en

el Cuenta de AWS propietario de la clave. La región de su clave de KMS y de su bucket de S3 debe ser la misma. Sin embargo, puede utilizar este mismo bucket y el mismo par de claves para cada región desde la que desee exportar los resultados.

a. Abra la AWS KMS consola en https://console.aws.amazon.com/kms.

b. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.

c. En el panel de navegación, elija Claves administradas por el cliente.

d. Elija Create key.

e. Elija Simétrico en Tipo de clave y, a continuación, elija Siguiente.

> **Note**
>
> Para más información acerca de la creación de claves de KMS, consulte Creating keys en la Guía para desarrolladores de AWS Key Management Service .

f. Proporcione un Alias para la clave y, a continuación, seleccione Siguiente.

g. Seleccione Siguiente y, a continuación, vuelva a seleccionar Siguiente para aceptar los permisos de administración y uso predeterminados.

h. Después de Revisar la configuración, seleccione Finalizar para crear la clave.

i. En la página Claves administradas por el cliente, elija el alias de su clave.

j. En la pestaña Política de claves, elija Cambiar a la vista de política.

k. Elija Editar y añada la siguiente política clave a su clave de KMS, lo que le permitirá GuardDuty acceder a su clave. Esta declaración permite GuardDuty usar solo la clave a la que se agrega esta política. Al editar la política de claves, asegúrese de que la sintaxis de JSON sea válida. Si agrega la instrucción antes de la instrucción final, debe agregar una coma después del corchete de cierre.

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "arn:aws:kms:Region1:444455556666:key/KMSKeyId",
    "Condition": {
```

```
        "StringEquals": {
            "aws:SourceAccount": "111122223333",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:111122223333:detector/SourceDetectorID"
        }
    }
}
```

Sustituya *Region1* por la región de su clave de KMS. Sustituya *444455556666* por el propietario de Cuenta de AWS la clave KMS. Sustituya el *KMS KeyId* por el identificador de clave de la clave de KMS que haya elegido para el cifrado. Para identificar todos estos valores (región e ID de clave), consulta el ARN de tu clave de KMS. Cuenta de AWS Para localizar el ARN de clave, consulte Finding the key ID and ARN.

Del mismo modo, sustituya *111122223333* por el Cuenta de AWS de la cuenta. GuardDuty Sustituya la *Región 2* por la Región de la cuenta. GuardDuty Sustituya el *SourceDetectorID* por el ID del detector de la GuardDuty cuenta de la *Región* 2.

Para encontrar el de `detectorId` tu cuenta y la región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

l. Seleccione Guardar.

2. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
3. En el panel de navegación, seleccione Configuración.
4. En Opciones de exportación de resultados, elija Configurar ahora.
5. Seleccione Nuevo bucket. Facilite un nombre único para su bucket de S3.
6. (Opcional) Puede probar su nueva configuración de exportación generando resultados de muestra. En el panel de navegación, seleccione Configuración.
7. En la sección Resultados de muestra, seleccione Generar resultados de muestra. Los nuevos ejemplos de resultados aparecerán como entradas en el depósito de S3 que se creará GuardDuty en un plazo máximo de cinco minutos.

Paso 4: Configure las alertas de GuardDuty búsqueda a través de las redes sociales

GuardDuty se integra con Amazon EventBridge, que se puede utilizar para enviar los datos de los resultados a otras aplicaciones y servicios para su procesamiento. Con EventBridge él, puede utilizar

GuardDuty los hallazgos para iniciar respuestas automáticas a sus hallazgos conectando los eventos de búsqueda con objetivos, como AWS Lambda las funciones, la automatización de Amazon EC2 Systems Manager, Amazon Simple Notification Service (SNS) y más.

En este ejemplo, creará un tema de SNS para que sea el objetivo de una regla y, a continuación, lo utilizará EventBridge para crear una EventBridge regla a partir de la cual se recopilen los datos de los hallazgos. GuardDuty La regla resultante reenvía los detalles de los resultados a una dirección de correo electrónico. Para obtener información sobre cómo enviar resultados a Slack o Amazon Chime y cómo modificar los tipos de resultados por los que se envían las alertas, consulte Configuración de un tema y un punto de conexión de Amazon SNS.

Creación de un tema de SNS para sus alertas de resultados

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En el panel de navegación, elija Temas.
3. Elija Create Topic (Crear tema).
4. En Tipo, seleccione Estándar.
5. En Nombre, ingrese **`GuardDuty`**.
6. Elija Create Topic (Crear tema). Se abrirán los detalles del nuevo tema.
7. En la sección Subscriptions (Suscripciones), elija Create subscription (Crear suscripción).
8. En Protocolo, seleccione Correo electrónico.
9. En Punto de conexión, introduzca la dirección de correo electrónico a la que desea enviar notificaciones.
10. Seleccione Crear suscripción.

    Después de crear su suscripción, debe confirmarla a través de su dirección de correo electrónico.
11. Para comprobar si hay un mensaje de suscripción, vaya a la bandeja de entrada de su correo electrónico y, en el mensaje de suscripción, seleccione Confirmar suscripción.

> **Note**
>
> Para comprobar el estado de la confirmación de correo electrónico, vaya a la consola de SNS y seleccione Suscripciones.

Para crear una EventBridge regla que recoja los GuardDuty hallazgos y les dé formato

1. Abra la EventBridge consola en https://console.aws.amazon.com/events/.
2. En el panel de navegación, seleccione Reglas.
3. Seleccione Crear regla.
4. Escriba un nombre y una descripción para la regla.

   Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.
5. En Bus de eventos, elija Predeterminado.
6. En Tipo de regla, elija Regla con un patrón de evento.
7. Seleccione Siguiente.
8. En Origen de eventos, seleccione (Eventos de AWS).
9. En la sección Patrón de eventos, seleccione Formulario de patrón de eventos.
10. En Origen de evento, seleccione Servicios de AWS .
11. En Servicio de AWS , seleccione GuardDuty.
12. En Tipo de evento, elija GuardDutyBuscar.
13. Seleccione Siguiente.
14. En Tipos de destino, seleccione Servicio de AWS .
15. En Seleccionar un destino, elija Tema de SNS y, en Tema, elija el nombre del tema de SNS que creó anteriormente.
16. En la sección Additional settings, en Configurar la entrada de destino, elija Transformador de entrada.

    Al añadir un transformador de entrada, los datos de búsqueda de JSON enviados se GuardDuty convierten en un mensaje legible para las personas.
17. Elija Configurar transformador de entrada.
18. En la sección Transformador de entrada de destino, en Ruta de entrada, pegue el siguiente código:

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
```

```
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

19. Para formatear el correo electrónico, en el caso de la plantilla, pega el siguiente código y asegúrate de reemplazar el texto en rojo por los valores correspondientes a tu región:

```
"You have a severity severity GuardDuty finding type Finding_Type in
 the Region_Name Region."
"Finding Description:"
"Finding_Description."
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=region#/findings?search=id%3DFinding_ID"
```

20. Seleccione Confirmar.
21. Seleccione Siguiente.
22. (Opcional) Introduzca una o varias etiquetas para la regla. Para obtener más información, consulta las EventBridge etiquetas de Amazon en la Guía del EventBridge usuario de Amazon.
23. Seleccione Siguiente.
24. Revise los detalles de la regla y seleccione Crear regla.
25. (Opcional) Pruebe la nueva regla generando resultados de muestra con el proceso descrito en el paso 2. Recibirá un correo electrónico por cada resultado de muestra que se genere.

Siguientes pasos

A medida que las utilice GuardDuty, comprenderá los tipos de hallazgos que son relevantes para su entorno. Cada vez que reciba un nuevo resultado, podrá encontrar información, como recomendaciones para corregir dicho resultado, al seleccionar Más información en la descripción del resultado en el panel de detalles del resultado o al buscar el nombre del resultado en Tipos de resultados.

Las siguientes funciones le ayudarán a GuardDuty ajustarlo para que pueda proporcionar los hallazgos más relevantes para su AWS entorno:

- Para ordenar fácilmente los resultados en función de criterios específicos, como el ID de instancia, el ID de cuenta, el nombre del bucket de S3, etc., puede crear filtros y guardarlos en ellos GuardDuty. Para obtener más información, consulte Filtrado de hallazgos.
- Si recibe resultados sobre el comportamiento esperado de su entorno, puede archivarlos automáticamente en función de los criterios que defina con las reglas de supresión.
- Para evitar que las conclusiones se generen a partir de un subconjunto de direcciones IP fiables o para que las IP de los GuardDuty monitores queden fuera del ámbito de supervisión habitual, puedes configurar listas de IP fiables y de amenazas.

Conceptos y terminología

A medida que comiences con Amazon GuardDuty, podrás beneficiarte de conocer sus conceptos clave.

Cuenta

Una cuenta estándar de Amazon Web Services (AWS) que contiene tus AWS recursos. Puede iniciar sesión AWS con su cuenta y activarla GuardDuty.

También puedes invitar a otras cuentas a que activen tu AWS cuenta GuardDuty y se asocien a ella GuardDuty. Si se aceptan tus invitaciones, tu cuenta se designará como cuenta GuardDuty de administrador y las cuentas añadidas pasarán a ser tus cuentas de miembro. A continuación, podrá ver y gestionar los GuardDuty resultados de esas cuentas en su nombre.

Los usuarios de la cuenta de administrador pueden configurar GuardDuty , ver y gestionar GuardDuty los resultados de su propia cuenta y de todas las cuentas de sus miembros. Puede tener hasta 10 000 cuentas de miembros en ella GuardDuty.

Los usuarios de las cuentas de los miembros pueden configurar GuardDuty , ver y gestionar GuardDuty los resultados de su cuenta (a través de la consola GuardDuty de administración o de la GuardDuty API). Los usuarios de cuentas de miembros no pueden ver ni administrar los resultados de las cuentas de otros miembros.

Una AWS cuenta no puede ser una cuenta de GuardDuty administrador y una cuenta de miembro al mismo tiempo. Las cuentas de AWS solo pueden aceptar una invitación de suscripción. La aceptación de una invitación de suscripción es opcional.

Para obtener más información, consulte Administrar varias cuentas en Amazon GuardDuty.

Detector

Todos los GuardDuty hallazgos están asociados a un detector, que es un objeto que representa el GuardDuty servicio. El detector es una entidad regional, y se requiere un detector único Región de AWS en cada una de las que GuardDuty opere. Cuando se activa GuardDuty en una región, se genera un nuevo detector con un DetectoriD alfanumérico único de 32 en esa región. El formato de un detectorId es `12abc34d567e8fa901bc2d34e56789f0`.

Para encontrar el correspondiente `detectorId` a su cuenta y a la región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

> **Note**
>
> En entornos multicuenta, todos los resultados para las cuentas de miembro se agregan al detector de la cuenta de administrador.

Algunas GuardDuty funciones se configuran a través del detector, como la configuración de la frecuencia de notificación de los CloudWatch eventos y la activación o desactivación de las fuentes de datos opcionales GuardDuty para su procesamiento.

Origen de datos

El origen o la ubicación de un conjunto de datos. Para detectar una actividad no autorizada o inesperada en su AWS entorno. GuardDuty analiza y procesa datos de registros de AWS CloudTrail eventos, eventos de AWS CloudTrail administración, eventos de AWS CloudTrail datos para S3, registros de flujo de VPC, registros de DNS, registros de auditoría de EKS, monitoreo de la actividad de inicio de sesión de RDS y volúmenes de EBS. Para obtener más información, consulte Orígenes de datos fundamentales.

Característica

Un objeto de función configurado para su plan de GuardDuty protección ayuda a detectar una actividad no autorizada o inesperada en su entorno. AWS Cada plan de GuardDuty protección configura el objeto de función correspondiente para analizar y procesar los datos. Algunos de los objetos de característica incluyen los registros de auditoría de EKS, la supervisión de la actividad de inicio de sesión en RDS y los volúmenes de EBS. Para obtener más información, consulte Activación de funciones en GuardDuty.

Resultado

Un problema potencial de seguridad descubierto por GuardDuty. Para obtener más información, consulte Entender los GuardDuty hallazgos de Amazon.

Los resultados se muestran en la GuardDuty consola y contienen una descripción detallada del problema de seguridad. También puedes recuperar las conclusiones generadas llamando a las operaciones GetFindingsy a la ListFindingsAPI.

También puedes ver tus GuardDuty hallazgos a través de los CloudWatch eventos de Amazon. GuardDuty envía los resultados a Amazon CloudWatch a través del protocolo HTTPS. Para obtener más información, consulte Creación de respuestas personalizadas a GuardDuty los hallazgos con Amazon CloudWatch Events.

Opciones de análisis

Cuando la protección contra GuardDuty malware está habilitada, le permite especificar qué instancias de Amazon EC2 y volúmenes de Amazon Elastic Block Store (EBS) debe escanear u omitir. Esta característica le permite agregar las etiquetas existentes que están asociadas a las instancias de EC2 y al volumen de EBS a una lista de etiquetas de inclusión o a una lista de etiquetas de exclusión. Los recursos asociados a las etiquetas que agregue a una lista de etiquetas de inclusión se analizan en busca de malware y los que se agregan a una lista de etiquetas de exclusión no se analizan. Para obtener más información, consulte Opciones de análisis con etiquetas definidas por el usuario.

Retención de instantáneas

Cuando la protección contra GuardDuty malware está habilitada, ofrece la opción de conservar las instantáneas de los volúmenes de EBS en su cuenta. AWS GuardDuty genera las réplicas de los volúmenes de EBS en función de las instantáneas de sus volúmenes de EBS. Puede retener las instantáneas de sus volúmenes de EBS solo si el análisis de la Protección contra malware detecta malware en las réplicas de los volúmenes de EBS. Si no se detecta ningún malware en las réplicas de los volúmenes de EBS, elimina GuardDuty automáticamente las instantáneas de sus volúmenes de EBS, independientemente de la configuración de retención de las instantáneas. Para obtener más información, consulte Retención de instantáneas.

Regla de supresión

Las reglas de supresión permiten crear combinaciones de atributos muy específicas para suprimir los resultados. Por ejemplo, puede definir una regla a través del GuardDuty filtro para archivar automáticamente solo las instancias `Recon:EC2/Portscan` de una VPC específica, que ejecuten una AMI específica o que tengan una etiqueta EC2 específica. Esta regla daría lugar a que los resultados del escaneo de puertos se archivaran automáticamente desde las instancias que cumplan los criterios. Sin embargo, sigue permitiendo emitir alertas si GuardDuty detecta instancias que estén llevando a cabo otras actividades maliciosas, como la minería de criptomonedas.

Las reglas de supresión definidas en la cuenta de GuardDuty administrador se aplican a las cuentas de los GuardDuty miembros. GuardDuty las cuentas de los miembros no pueden modificar las reglas de supresión.

Con las reglas de supresión, GuardDuty sigue generando todos los hallazgos. Las reglas de supresión facilitan la eliminación de resultados, mientras mantienen un historial completo e inmutable de todas las actividades.

Normalmente, las reglas de supresión se utilizan para ocultar los hallazgos del entorno que se consideran falsos positivos y reducir así el ruido de los resultados con poco valor para que pueda centrarse en amenazas más importantes. Para obtener más información, consulte Reglas de supresión.

Lista de IP de confianza

Una lista de direcciones IP confiables para una comunicación altamente segura con su AWS entorno. GuardDuty no genera resultados basados en listas de IP confiables. Para obtener más información, consulte Uso de listas de IP de confianza y listas de amenazas.

Lista de IP de amenazas

Una lista de direcciones IP maliciosas conocidas. Además de generar hallazgos debido a una actividad potencialmente sospechosa, GuardDuty también genera hallazgos basados en estas listas de amenazas. Para obtener más información, consulte Uso de listas de IP de confianza y listas de amenazas.

Activación de funciones en GuardDuty

Cuando habilita Amazon GuardDuty por primera vez o habilita un tipo de protección en él GuardDuty, GuardDuty comienza a procesar lo correspondiente Orígenes de datos fundamentales en su AWS entorno. GuardDuty usa estas fuentes de datos para procesar un flujo de eventos, como registros de flujo de VPC, registros de DNS y registros de AWS CloudTrail eventos y administración. A continuación, analiza estos eventos para identificar posibles amenazas de seguridad y genera resultados en su cuenta.

Además de las fuentes de datos de registro, GuardDuty puede utilizar datos adicionales de otros AWS servicios de su AWS entorno para supervisar y analizar posibles amenazas a la seguridad.

Activación de características

Al añadir GuardDuty protecciones adicionales, por ejemplo, S3 Protection, Runtime Monitoring o EKS Protection, puede configurar la GuardDuty función correspondiente al tipo de protección. Históricamente, en las API se utilizaban `dataSources` las denominadas GuardDuty protecciones. Sin embargo, después de marzo de 2023, los nuevos tipos de GuardDuty protección ahora se configuran como `features` y no`dataSources`. GuardDuty sigue siendo compatible con la configuración de los tipos de protección lanzados antes de marzo de 2023, por ejemplo, `dataSources` a través de la API, pero los nuevos tipos de protección solo están disponibles a partir de`features`.

Si administra los tipos de GuardDuty configuración y protección a través de la consola, este cambio no lo afectará directamente y no tendrá que tomar ninguna medida. La activación de funciones afecta al comportamiento de las API que se invocan para habilitar GuardDuty o proteger los tipos de API que contienen GuardDuty. Para obtener más información, consulte GuardDuty Cambios en la API.

GuardDuty Cambios en la API en marzo de 2023

Las GuardDuty API configuran funciones de protección que no pertenecen a la lista deOrígenes de datos fundamentales. Un objeto de característica contiene detalles de la característica, como el nombre y el estado de la característica, y puede contener configuración adicional para algunas de las características. Esta migración afecta a las siguientes API de la Amazon GuardDuty API Reference:

- CreateDetector
- GetDetector

- UpdateDetector
- GetMemberDetectors
- UpdateMemberDetectors
- DescribeOrganizationConfiguration
- UpdateOrganizationConfiguration
- GetRemainingFreeTrialDays
- GetUsageStatistics

Activación de características en comparación con orígenes de datos

Históricamente, todas las GuardDuty funciones se transferían a través de un `dataSources` objeto de la API. A partir de marzo de 2023, GuardDuty prefiere el `features` objeto en lugar del `dataSources` objeto de la API. Todos los orígenes de datos anteriores tienen las características correspondientes, pero es posible que las características más recientes no tengan los orígenes de datos correspondientes.

En la siguiente lista se muestra la comparación entre los objetos `dataSources` y `features` cuando se pasan a través de una API:

- El objeto `dataSources` contiene objetos para cada tipo de protección y su estado. El `features` objeto es una lista de funciones disponibles que corresponden a cada tipo de protección incluido GuardDuty.

  A partir de marzo de 2023, la activación de las funciones será la única forma de configurar GuardDuty las nuevas funciones en su AWS entorno.
- El `dataSources` esquema de la solicitud o respuesta de la API es el mismo en todos los Región de AWS lugares GuardDuty disponibles. Sin embargo, es posible que no todas las características estén disponibles en todas las regiones. Por lo tanto, los nombres de las características disponibles pueden variar según la región.

Descripción del funcionamiento de la activación de características

Las GuardDuty API seguirán devolviendo un `dataSources` objeto, según proceda, y también devolverán un `features` objeto que contenga la misma información en un formato diferente. GuardDuty las funciones lanzadas antes de marzo de 2023 estarán disponibles a través de `dataSources` object y `features` object. GuardDuty las funciones lanzadas desde marzo de 2023

solo estarán disponibles a través del `features` objeto. No puede crear ni actualizar un detector, ni describir su organización de AWS Organizations con la notación de los objetos `dataSources` y `features` en la misma solicitud de la API. Para habilitar los tipos de GuardDuty protección, tendrá que migrar las fuentes de datos existentes al `features` objeto mediante las mismas API que ahora también incluyen el `features` objeto.

> **Note**
>
> GuardDuty no añadirá una nueva fuente de datos después de esta modificación.

GuardDuty ha dejado en desuso el uso de fuentes de datos. Sin embargo, sigue admitiendo los Orígenes de datos fundamentales. GuardDuty Las prácticas recomendadas recomiendan utilizar la activación de funciones para cualquier tipo de protección que ya esté activado en su cuenta. En las prácticas recomendadas también se requiere el uso de la activación de características cuando se habilita un nuevo tipo de protección para la cuenta.

Incorporación de cambios de activación de características

- Si administras GuardDuty las configuraciones mediante API, SDK o AWS CloudFormation plantillas y deseas habilitar posibles GuardDuty funciones nuevas, tendrás que modificar el código y la plantilla, respectivamente. Para obtener más información, consulta las API actualizadas en la Amazon GuardDuty API Reference.
- En el GuardDuty caso de las funciones configuradas antes de esta actualización, puede seguir utilizando las API, los SDK o la AWS CloudFormation plantilla. Sin embargo, le recomendamos que cambie para usar el objeto `feature`.

  Todos los orígenes de datos tienen un objeto de característica equivalente. Para obtener más información, consulte Asignación de `dataSources` a `features`.
- Actualmente, `additionalConfiguration` en el objeto `features` solo está disponible para ciertos tipos de protecciones.
  - Para estos tipos de protección, si la función `AdditionalConfiguration` `status` está configurada en `ENABLED` pero la configuración de la función no `status` está establecida en`ENABLED`, no GuardDuty realizará ninguna acción en este caso.
  - Esto afecta a las siguientes API:
    - UpdateDetector
    - UpdateMemberDetectors

- UpdateOrganizationConfiguration

Asignación de `dataSources` a `features`

En la siguiente tabla se muestra la asignación de los tipos de protecciones, `dataSources` y `features`.

GuardDuty tipo de protección	Nombre de la fuente de datos *	Nombre de la función
Logs de flujo de VPC	`flowLogs` (solo lectura; no se puede modificar)	`FLOW_LOGS` (solo lectura; no se puede modificar)
Registros de DNS	`dnsLogs` (solo lectura; no se puede modificar)	`DNS_LOGS` (solo lectura; no se puede modificar)
CloudTrail eventos	`cloudLogs` (solo lectura; no se puede modificar)	`CLOUD_LOGS` (solo lectura; no se puede modificar)
S3	`s3Logs`	`S3_DATA_EVENTS`
Supervisión de registros de auditoría de EKS	`kubernetes.auditlogs`	`EKS_AUDIT_LOGS`
Protección contra malware	`malwareProtection.scanEc2InstanceWithFindings.ebsVolumes`	`EBS_MALWARE_PROTECTION`
Eventos de inicio de sesión de RDS	GuardDuty solo proporciona compatibilidad con la activación de funciones para estos tipos de protección.	`RDS_LOGIN_EVENTS`

GuardDuty tipo de protección	Nombre de la fuente de datos *	Nombre de la función
Supervisión en tiempo de ejecución de EKS		`EKS_RUNTIME_MONITORING`
Supervisión del tiempo de ejecución		`RUNTIME_MONITORING`

GuardDuty agente de seguridad para clústeres de Amazon EKS		`EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`
		
		`RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`

GuardDuty agente de seguridad para clústeres de Amazon ECS		`RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT`

GuardDuty tipo de protección	Nombre de la fuente de datos *	Nombre de la función
Protección de Lambda		`LAMBDA_NETWORK_LOGS`

* GetUsageStatistics usa sus propios nombres de `dataSource`. Para obtener más información, consulte Estimación de costos GuardDuty o GetUsageStatistics.

Orígenes de datos fundamentales

GuardDuty utiliza las fuentes de datos fundamentales para detectar la comunicación con dominios y direcciones IP maliciosos conocidos e identificar comportamientos anómalos. Todos los datos de registro se cifran mientras GuardDuty se transfieren de estas fuentes a otras. GuardDutyextrae varios campos de estas fuentes de registros para crear perfiles y detectar anomalías y, a continuación, descarta estos registros.

En las siguientes secciones se describe cómo se GuardDuty utiliza cada fuente de datos compatible. Cuando habilita GuardDuty su Cuenta de AWS, comienza a monitorear GuardDuty automáticamente estas fuentes de registro.

Temas

AWS CloudTrail registros de eventos

AWS CloudTrail te proporciona un historial de las llamadas a la AWS API de tu cuenta, incluidas las llamadas a la AWS Management Console API realizadas con los AWS SDK, las herramientas de línea de comandos y determinados AWS servicios. CloudTrail también te ayuda a identificar qué usuarios y cuentas invocaron AWS las API de los servicios compatibles CloudTrail, la dirección IP de origen desde la que se invocaron las llamadas y el momento en que se invocaron las llamadas. Para obtener más información, consulte What is AWS CloudTrail en la Guía del usuario de AWS CloudTrail .

GuardDuty también supervisa los eventos CloudTrail de administración. Cuando lo habilita GuardDuty, comienza a consumir los eventos de CloudTrail administración directamente CloudTrail a través de un flujo de eventos independiente y duplicado y analiza sus registros de CloudTrail eventos. No hay ningún cargo adicional cuando se GuardDuty accede a los eventos registrados en él. CloudTrail

GuardDuty no gestiona sus CloudTrail eventos ni afecta a sus CloudTrail configuraciones existentes. Del mismo modo, sus CloudTrail configuraciones no afectan a la forma en GuardDuty que consume

y procesa los registros de eventos. Para gestionar el acceso y la retención de tus CloudTrail eventos, usa la consola CloudTrail de servicio o la API. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos en la Guía AWS CloudTrail del usuario.

¿Cómo GuardDuty gestiona los eventos AWS CloudTrail globales

En la mayoría de AWS los servicios, los CloudTrail eventos se registran en el Región de AWS lugar donde se crearon. En el caso de servicios globales como AWS Identity and Access Management (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3), Amazon y CloudFront Amazon Route 53 (Route 53), los eventos solo se generan en la región en la que se producen, pero tienen una importancia mundial.

Cuando GuardDuty consume eventos de servicio CloudTrail global con valor de seguridad, como configuraciones de red o permisos de usuario, replica esos eventos y los procesa en cada región en la que los haya activado. GuardDuty Este comportamiento ayuda a GuardDuty mantener los perfiles de usuario y rol en cada región, lo cual es vital para detectar eventos anómalos.

Le recomendamos encarecidamente que active todos GuardDuty los Regiones de AWS que estén habilitados para usted Cuenta de AWS. Esto ayuda GuardDuty a detectar actividades no autorizadas o inusuales, incluso en las regiones que quizás no utilices activamente.

AWS CloudTrail eventos de gestión

Los eventos de administración también se conocen como eventos del plano de control. Estos eventos proporcionan información sobre las operaciones de administración que se llevan a cabo con los recursos de su AWS cuenta.

A continuación se muestran ejemplos de eventos de CloudTrail administración que se GuardDuty supervisan:

- Configuración de la seguridad (operaciones de la API `AttachRolePolicy` de IAM)
- Configuración de reglas para el direccionamiento de datos (operaciones de la API `CreateSubnet` de Amazon EC2)
- Configuración del registro (operaciones AWS CloudTrail `CreateTrail` de API)

Logs de flujo de VPC

La función VPC Flow Logs de Amazon VPC captura información sobre el tráfico IP que entra y sale de las interfaces de red conectadas a las instancias de Amazon Elastic Compute Cloud (Amazon EC2) de su entorno. AWS

Cuando lo habilita GuardDuty, comienza a analizar inmediatamente los registros de flujo de VPC de las instancias de Amazon EC2 de su cuenta. Consume los eventos de registro de flujo de VPC directamente desde la característica de Registros de flujo de VPC a través de una secuencia independiente y duplicada de registros de flujo. Este proceso no afecta a ninguna configuración de los registros de flujo existentes.

GuardDuty Protección Lambda

Lambda Protection es una mejora opcional de Amazon. GuardDuty En la actualidad, la supervisión de la actividad de la red de Lambda en GuardDuty incluye los registros de flujo de Amazon VPC de todas las funciones de Lambda de su cuenta, incluso los registros que no utilizan redes de VPC. Para proteger su función Lambda de posibles amenazas de seguridad, tendrá que configurar Lambda Protection en su cuenta. GuardDuty Para obtener más información, consulte GuardDuty Protección Lambda.

GuardDuty Supervisión del tiempo de ejecución

Si administra el agente de seguridad (de forma manual o a través de él GuardDuty) en EKS Runtime Monitoring o Runtime Monitoring for EC2, y si actualmente GuardDuty está desplegado en una instancia de Amazon EC2 y recibe Tipos de eventos de tiempo de ejecución recopilados el de esta instancia GuardDuty , no se le Cuenta de AWS cobrará por el análisis de los registros de flujo de VPC de esta instancia de Amazon EC2. Esto ayuda a GuardDuty evitar el doble de los gastos de uso de la cuenta.

GuardDuty no administra tus registros de flujo ni los hace accesibles en tu cuenta. Para administrar el acceso y la retención de los registros de flujo, debe configurar la característica Registros de flujo de VPC.

Registros de DNS

Si utiliza resolutores de AWS DNS para sus instancias de Amazon EC2 (la configuración predeterminada), GuardDuty podrá acceder a sus registros de DNS de solicitudes y respuestas

y procesarlos a través de los resolutores de DNS AWS internos. Si utilizas otro solucionador de DNS, como OpenDNS o GoogleDNS, o si configuras tus propios solucionadores de DNS, no podrás acceder a los datos de esta fuente de datos ni GuardDuty procesarlos.

Cuando la habilitas GuardDuty, comienza inmediatamente a analizar tus registros de DNS a partir de un flujo de datos independiente. Este flujo de datos es independiente de los datos proporcionados a través de la característica Registro de consultas del solucionador de Route 53. La configuración de esta función no afecta al GuardDuty análisis.

> **Note**
>
> GuardDuty no admite la supervisión de los registros de DNS para las instancias de Amazon EC2 que se lanzan AWS Outposts porque la función de registro de Amazon Route 53 Resolver consultas no está disponible en ese entorno.

Protección EKS en Amazon GuardDuty

La supervisión de registros de auditoría de EKS lo ayuda a detectar actividades potencialmente sospechosas en los clústeres de EKS en Amazon Elastic Kubernetes Service (Amazon EKS). La supervisión de registros de auditoría de EKS utiliza los registros de auditoría de Kubernetes para capturar las actividades cronológicas de los usuarios, las aplicaciones que utilizan la API de Kubernetes y el plano de control. Para obtener más información, consulte Registros de auditoría de Kubernetes.

> **Note**
>
> El monitoreo del tiempo de ejecución de EKS se administra como parte del monitoreo del tiempo de ejecución. Para obtener más información, consulte GuardDuty Supervisión del tiempo de ejecución.

Características en la protección de EKS

Registros de auditoría de Kubernetes

Los registros de auditoría de Kubernetes capturan las acciones secuenciales del clúster de Amazon EKS, incluidas las actividades de los usuarios, las aplicaciones que utilizan la API de Kubernetes y el plano de control. El registro de auditoría es un componente de todos los clústeres de Kubernetes.

Para obtener más información, consulte la sección de auditorías en la documentación de Kubernetes.

Amazon EKS permite que los registros de auditoría de Kubernetes se ingieran como CloudWatch Amazon Logs a través de la función de registro del plano de control de EKS. GuardDuty no gestiona el registro del plano de control de Amazon EKS ni permite que los registros de auditoría de Kubernetes estén accesibles en su cuenta si no los ha habilitado para Amazon EKS. Para administrar el acceso a los registros de auditoría de Kubernetes y su retención, debe configurar la característica de registro del plano de control de Amazon EKS. Para obtener más información, consulte Habilitar y deshabilitar registros de plano de control en la Guía del usuario de Amazon EKS.

Para obtener información sobre la configuración de la supervisión de registros de auditoría de EKS, consulte Supervisión de registros de auditoría de EKS.

Supervisión de registros de auditoría de EKS

La supervisión de registros de auditoría de EKS le ayuda a detectar actividades potencialmente sospechosas en sus clústeres de EKS dentro de Amazon Elastic Kubernetes Service. Cuando habilita la monitorización de registros de auditoría de EKS, comienza GuardDuty inmediatamente a monitorizar Registros de auditoría de Kubernetes desde sus clústeres de Amazon EKS y a analizarlos para detectar posibles actividades maliciosas o sospechosas. Consume los eventos del registro de auditoría de Kubernetes directamente desde la función de registro del plano de control de Amazon EKS a través de un flujo independiente y duplicado de registros de auditoría. Este proceso no requiere ninguna configuración adicional ni afecta a ninguna configuración de registro del plano de control de Amazon EKS existente que pueda tener.

Al deshabilitar la supervisión de registros de auditoría de EKS, deja de monitorear y analizar GuardDuty inmediatamente los registros de auditoría de Kubernetes para sus recursos de Amazon EKS.

Es posible que el monitoreo de registros de auditoría de EKS no esté disponible en todos los Regiones de AWS lugares donde GuardDuty esté disponible. Para obtener más información, consulte Disponibilidad de características específicas por región.

Cómo afecta GuardDuty el período de prueba gratuito de 30 días a las cuentas

- Al activarlo GuardDuty por primera vez, el periodo de prueba gratuito de 30 días ya incluye la monitorización del registro de auditoría de EKS en EKS Protection.
- GuardDuty Las cuentas existentes pueden habilitar la monitorización de registros de auditoría de EKS por primera vez con un período de prueba gratuito de 30 días.

Configuración de la supervisión de registros de auditoría de EKS para una cuenta independiente

Elija el método de acceso que prefiera para activar o desactivar la supervisión de registros de auditoría de EKS para una cuenta independiente.

Console

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, elija Protección de EKS.

3. En la pestaña Configuración, puede ver el estado de la configuración actual de la supervisión de registros de auditoría de EKS. En la sección Supervisión de registros de auditoría de EKS, seleccione Habilitar para habilitar o Deshabilitar para deshabilitar la característica de supervisión de registros de auditoría de EKS.
4. Seleccione Guardar.

API/CLI

- Ejecute la operación de la updateDetectorAPI utilizando el ID de detector regional de la cuenta de GuardDuty administrador delegado y pasando el nombre del `features` objeto como `EKS_AUDIT_LOGS` y su estado como `ENABLED` o`DISABLED`.

  Como alternativa, también puede activar o desactivar la supervisión del registro de auditoría de EKS ejecutando un AWS CLI comando. El siguiente código de ejemplo habilita la monitorización del registro de auditoría de GuardDuty EKS. Para desactivarlo, sustituya `ENABLED` por `DISABLED`.

  Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración en la consola https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  features [{"Name" : "EKS_AUDIT_LOGS", "Status" : "ENABLED"}]'
  ```

Configuración de la supervisión de registros de auditoría de EKS en entornos con varias cuentas

En un entorno con varias cuentas, solo la cuenta de GuardDuty administrador delegado tiene la opción de activar o desactivar la función de supervisión del registro de auditoría de EKS, para las cuentas de los miembros de su organización. Las cuentas de GuardDuty los miembros no pueden modificar esta configuración desde sus cuentas. La cuenta de GuardDuty administrador delegado administra sus cuentas de miembros mediante AWS Organizations. Esta cuenta de GuardDuty administrador delegado puede optar por habilitar automáticamente la supervisión del registro de auditoría de EKS para todas las cuentas nuevas a medida que se unan a la organización. Para obtener más información sobre los entornos de varias cuentas, consulta Administrar varias cuentas en Amazon. GuardDuty

Configuración de EKS Audit Log Monitoring para una cuenta de administrador delegado GuardDuty

Elija el método de acceso que prefiera para configurar la supervisión del registro de auditoría de EKS para la cuenta de GuardDuty administrador delegado.

Console

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de administración.
2. En el panel de navegación, elija Protección de EKS.
3. En la pestaña Configuración, puede ver el estado de la configuración actual de la supervisión de registros de auditoría de EKS en la respectiva sección. Para actualizar la configuración de la cuenta de GuardDuty administrador delegado, seleccione Editar en el panel de supervisión del registro de auditoría de EKS.
4. Realice una de las acciones siguientes:

   Uso de Habilitar para todas las cuentas

   - Elija Habilitar para todas las cuentas. Esto habilitará el plan de protección para todas las GuardDuty cuentas activas de su AWS organización, incluidas las nuevas cuentas que se unan a la organización.
   - Seleccione Guardar.

   Uso de Configurar cuentas manualmente

   - Para habilitar el plan de protección solo para la cuenta de GuardDuty administrador delegado, elija Configurar las cuentas manualmente.
   - Seleccione Activar en la sección de la cuenta de GuardDuty administrador delegado (esta cuenta).
   - Seleccione Guardar.

API/CLI

Ejecute la operación de la API updateDetector con su propio ID de detector regional y pase el `name` del objeto `features` como `EKS_AUDIT_LOGS` y `status` como `ENABLED` o `DISABLED`.

Para encontrar la correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

Puede activar o desactivar la supervisión del registro de auditoría de EKS ejecutando el siguiente AWS CLI comando. Asegúrese de utilizar el *`ID de detector`* válido de la cuenta de GuardDuty administrador delegado.

> **Note**
>
> El siguiente código de ejemplo habilita la supervisión de registros de auditoría de EKS. *`Asegúrese de sustituir 12abc34d567e8fa901bc2d34e56789f0 por la de la cuenta de administrador delegado y 555555555555 por la de la cuenta de administrador delegado. detector-id GuardDuty`* Cuenta de AWS GuardDuty

Para `detectorId` encontrar la correspondiente a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 555555555555 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

Para deshabilitar la supervisión de registros de auditoría de EKS, sustituya `ENABLED` por `DISABLED`.

Habilitación automática de la supervisión de registros de auditoría de EKS para todas las cuentas de miembros

Elija su método de acceso preferido para habilitar la supervisión de registros de auditoría de EKS en todas las cuentas de miembros existentes en la organización.

Console

1. Inicia sesión en la GuardDuty consola AWS Management Console y ábrela en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.
2. Realice una de las acciones siguientes:

Mediante la página Protección de EKS

1. En el panel de navegación, elija Protección de EKS.
2. En la pestaña Configuración, puede ver el estado actual de la supervisión de registros de auditoría de EKS para las cuentas de miembros activos de su organización.

   Para actualizar la configuración de la Supervisión de registros de auditoría de EKS, elija Editar.
3. Elija Habilitar para todas las cuentas. Esta acción habilita automáticamente la supervisión de registros de auditoría de EKS para las cuentas nuevas y existentes de la organización.
4. Seleccione Guardar.

> **Note**
>
> La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Uso de la página Cuentas

1. En el panel de navegación, elija Accounts (Cuentas).
2. En la página Cuentas, seleccione las preferencias para Habilitar automáticamente antes de Agregar cuentas mediante invitación.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para todas las cuentas en Supervisión de registros de auditoría de EKS.
4. Seleccione Guardar.

Si no puede utilizar la opción Habilitar para todas las cuentas y desea personalizar la configuración de la Supervisión de registros de auditoría de EKS para cuentas específicas de su organización, consulte Activación o desactivación de forma selectiva de la supervisión de registros de auditoría de EKS para las cuentas de miembros.

API/CLI

- Para activar o desactivar la Supervisión de registros de auditoría de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio *ID de detector*.
- El siguiente ejemplo muestra cómo se puede habilitar la supervisión de registros de auditoría de EKS para una sola cuenta de miembro. Para desactivarlo, sustituya `ENABLED` por `DISABLED`.

  Para encontrar las de `detectorId` su cuenta y su región actual, consulte la página de configuración en la consola https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación de la Supervisión de registros de auditoría de EKS para todas las cuentas de miembros activos existentes

Elija su método de acceso preferido para habilitar la supervisión de registros de auditoría de EKS en todas las cuentas de miembros activos existentes en la organización.

Console

1. Inicia sesión en la GuardDuty consola AWS Management Console y ábrela en https://console.aws.amazon.com/guardduty/.

   Inicie sesión con las credenciales de la cuenta GuardDuty de administrador delegado.
2. En el panel de navegación, elija Protección de EKS.

3. En la página de protección de EKS, puede ver el estado actual de la configuración de análisis GuardDutyde malware iniciada. En la sección Cuentas de miembros activas, seleccione Acciones.
4. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
5. Seleccione Guardar.

API/CLI

- Para activar o desactivar la Supervisión de registros de auditoría de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio *`ID de detector`*.
- El siguiente ejemplo muestra cómo se puede habilitar la supervisión de registros de auditoría de EKS para una sola cuenta de miembro. Para desactivarlo, sustituya `ENABLED` por `DISABLED`.

  Para encontrar el de `detectorId` su cuenta y su región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación automática de la Supervisión de registros de auditoría de EKS para las cuentas de miembros nuevos

Las cuentas de los miembros recién agregadas deben habilitarse GuardDuty antes de seleccionar la configuración del análisis GuardDuty de malware iniciado. Las cuentas de los miembros gestionadas

mediante invitación pueden configurar manualmente la detección GuardDuty de malware iniciada para sus cuentas. Para obtener más información, consulte Step 3 - Accept an invitation.

Elija su método de acceso preferido para habilitar la supervisión de registros de auditoría de EKS en las cuentas de miembros nuevos que se unen a la organización.

Console

La cuenta de GuardDuty administrador delegado puede habilitar la supervisión del registro de auditoría de EKS para las cuentas de los nuevos miembros de una organización, mediante la página de supervisión del registro de auditoría de EKS o la página de cuentas.

Habilitación automática de la Supervisión de registros de auditoría de EKS para las cuentas de miembros nuevos

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.
2. Realice una de las acciones siguientes:
   - Mediante la página Protección de EKS:
     1. En el panel de navegación, elija Protección de EKS.
     2. En la página Protección de EKS, seleccione Editar en Supervisión de registros de auditoría de EKS.
     3. Elija Configurar cuentas manualmente.
     4. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que, cada vez que una nueva cuenta se una a su organización, la supervisión de registros de auditoría de EKS se habilite automáticamente para la cuenta. Solo la cuenta de GuardDuty administrador delegado de la organización puede modificar esta configuración.
     5. Seleccione Guardar.
   - Mediante la página Cuentas:
     1. En el panel de navegación, elija Accounts (Cuentas).
     2. En la página Cuentas, seleccione Habilitar automáticamente las preferencias.
     3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para las cuentas nuevas en Supervisión de registros de auditoría de EKS.

4. Seleccione Guardar.

API/CLI

- Para activar o desactivar la Supervisión de registros de auditoría de EKS de forma selectiva para las cuentas nuevas, ejecute la operación de la API UpdateOrganizationConfiguration con su propio *ID de detector*.
- El siguiente ejemplo muestra cómo puede habilitar la supervisión de registros de auditoría de EKS para los nuevos miembros que se unan a su organización. También puede pasar una lista de ID de cuentas separadas por un espacio.

  Para encontrar la correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración en la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "EKS_AUDIT_LOGS", "AutoEnable": "NEW"}]'
```

Activación o desactivación de forma selectiva de la supervisión de registros de auditoría de EKS para las cuentas de miembros

Elija su método de acceso preferido para activar o desactiva la supervisión de registros de auditoría de EKS en cuentas de miembros selectivas en la organización.

Console

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.
2. En el panel de navegación, elija Accounts (Cuentas).

   En la página Cuentas, revise la columna Supervisión de registros de auditoría de EKS para ver el estado de su cuenta de miembro.
3. Activación o desactivación de la Supervisión de registros de auditoría de EKS

   Seleccione una cuenta que desee configurar para la Supervisión de registros de auditoría de EKS. Puede seleccionar varias cuentas de manera simultánea. En el menú desplegable

Editar planes de protección, seleccione Supervisión de registros de auditoría de EKS y, a continuación, elija la opción adecuada.

API/CLI

Para activar o desactivar la Supervisión de registros de auditoría de EKS de forma selectiva para sus cuentas de miembros, invoque la operación de la API updateMemberDetectors con su propio *ID de detector*.

El siguiente ejemplo muestra cómo se puede habilitar la supervisión de registros de auditoría de EKS para una sola cuenta de miembro. Para desactivarlo, sustituya `ENABLED` por `DISABLED`. También puede pasar una lista de ID de cuentas separadas por un espacio.

Para encontrar las de `detectorId` su cuenta y su región actual, consulte la página de configuración en la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 111122223333 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

Protección Lambda en Amazon GuardDuty

La protección de Lambda lo ayuda a identificar posibles amenazas de seguridad cuando se invoca una función de AWS Lambda en su entorno de AWS . Al habilitar Lambda Protection, GuardDuty comienza a monitorear los registros de actividad de la red Lambda, empezando por Logs de flujo de VPC todas las funciones de Lambda por cuenta, incluidos los registros que no utilizan redes de VPC, y se generan cuando se invoca la función Lambda. Si GuardDuty identifica tráfico de red sospechoso que sea indicativo de la presencia de un fragmento de código potencialmente malicioso en su función Lambda, GuardDuty generará un hallazgo.

> **Note**
>
> La supervisión de la actividad de red de Lambda no incluye los registros de las funciones de Lambda@Edge.

Puede configurar Lambda Protection para cualquier cuenta o disponible Regiones de AWS en cualquier momento. De forma predeterminada, una GuardDuty cuenta existente puede habilitar Lambda Protection con un período de prueba de 30 días. Para una GuardDuty cuenta nueva, Lambda Protection ya está habilitada e incluida en el período de prueba de 30 días. Para obtener más información sobre las estadísticas de uso, consulte Estimación del costo.

GuardDuty supervisa los registros de actividad de la red generados al invocar las funciones Lambda. En la actualidad, la supervisión de la actividad de red de Lambda incluye los registros de flujos de Amazon VPC de todas las funciones de Lambda de su cuenta, tales como los registros que no utilizan redes de VPC y están sujetos a cambios, incluida la expansión a otras actividades de la red, como los datos de consultas de DNS generados al invocar las funciones de Lambda. La expansión a otras formas de supervisión de la actividad de la red aumentará el volumen de datos que GuardDuty se procesarán para Lambda Protection. Esto afectará directamente al costo de uso de la protección de Lambda. Cada vez que GuardDuty comience a monitorear un registro de actividad de red adicional, enviará un aviso a las cuentas que hayan activado Lambda Protection, al menos 30 días antes del lanzamiento.

Característica en la protección de Lambda

Supervisión de la actividad de red de Lambda

Al activar Lambda Protection, supervisa los registros de actividad de red de GuardDuty Lambda que se generan cuando se invoca una función de Lambda asociada a su cuenta. Esto le ayuda a detectar posibles amenazas a la seguridad de la función Lambda. GuardDuty supervisa los registros de flujo de VPC de todas las funciones de Lambda, incluidas las que no utilizan redes de VPC. En el caso de las funciones de Lambda que están configuradas para usar redes de VPC, no es necesario habilitar los registros de flujo de VPC para las interfaces de red elásticas (ENI) creadas por Lambda. GuardDuty GuardDuty solo cobra por la cantidad de datos de registro de actividad de red Lambda procesados (en GB) para generar un hallazgo. GuardDuty optimiza los costes mediante la aplicación de filtros inteligentes y el análisis de un subconjunto de registros de actividad de la red Lambda que son relevantes para la detección de amenazas. Para obtener información sobre los precios, consulta los GuardDuty precios de Amazon.

GuardDuty no administra los registros de actividad de la red Lambda (incluidos los registros de flujo de VPC y no VPC) ni los hace accesibles en su cuenta.

Configuración de la protección de Lambda

Configuración de la protección de Lambda para una cuenta independiente

En el caso de las cuentas asociadas AWS Organizations, puede automatizar este proceso mediante las instrucciones de la GuardDuty consola o la API, tal y como se describe en la siguiente sección.

Elija el método de acceso que prefiera para habilitar o deshabilitar la protección de Lambda para una cuenta independiente.

Console

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, en Configuración, elija Protección de Lambda.
3. En la página Protección de Lambda se muestra el estado actual de su cuenta. Puede habilitar o deshabilitar la característica en cualquier momento mediante la selección de Habilitar o Deshabilitar.
4. Seleccione Guardar.

API/CLI

Ejecute la operación de la API updateDetector con su propio ID de detector regional y pase el `name` del objeto `features` como `LAMBDA_NETWORK_LOGS` y `status` como `ENABLED` o `DISABLED`.

También puede activar o desactivar la supervisión de actividad de red Lambda ejecutando el siguiente AWS CLI comando. No olvide utilizar su propio *`ID de detector`* válido.

> **Note**
>
> En el siguiente código de ejemplo se habilita la supervisión de la actividad de red de Lambda. Para desactivarlo, sustituya `ENABLED` por `DISABLED`.

Para encontrar la correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "LAMBDA_NETWORK_LOGS", "Status" : "ENABLED"}]'
```

Configuración de la protección de Lambda en entornos con varias cuentas

En un entorno de varias cuentas, solo la cuenta de GuardDuty administrador delegado tiene la opción de activar o desactivar Lambda Protection para las cuentas de los miembros de su organización. Las cuentas de GuardDuty los miembros no pueden modificar esta configuración desde sus cuentas. La cuenta de GuardDuty administrador delegado administra las cuentas de los miembros mediante AWS Organizations. La cuenta de GuardDuty administrador delegado puede optar por habilitar automáticamente Lambda Network Activity Monitoring para todas las cuentas nuevas a medida que se unan a la organización. Para obtener más información sobre los entornos de varias cuentas, consulta Administrar varias cuentas en Amazon GuardDuty.

Configuración de Lambda Protection para una cuenta de administrador delegado GuardDuty

Elija el método de acceso que prefiera para activar o desactivar la supervisión de actividad de red Lambda para la cuenta de administrador delegado. GuardDuty

Console

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de administración.
2. En el panel de navegación, en Configuración, elija Protección de Lambda.
3. En la página Protección de Lambda, seleccione Editar.
4. Realice una de las acciones siguientes:

   Uso de Habilitar para todas las cuentas

   - Elija Habilitar para todas las cuentas. Esto habilitará el plan de protección para todas las GuardDuty cuentas activas de su AWS organización, incluidas las cuentas nuevas que se unan a la organización.
   - Seleccione Guardar.

   Uso de Configurar cuentas manualmente

   - Para habilitar el plan de protección solo para la cuenta de GuardDuty administrador delegado, elija Configurar cuentas manualmente.
   - Seleccione Activar en la sección de la cuenta de GuardDuty administrador delegado (esta cuenta).
   - Seleccione Guardar.

API/CLI

Ejecute la operación de la API updateDetector con su propio ID de detector regional y pase el `name` del objeto `features` como `LAMBDA_NETWORK_LOGS` y `status` como `ENABLED` o `DISABLED`.

Puede activar o desactivar la supervisión de actividad de red Lambda ejecutando el siguiente AWS CLI comando. Asegúrese de utilizar el ID de *`detector`* válido de la cuenta de GuardDuty administrador delegado.

> **Note**
>
> En el siguiente código de ejemplo se habilita la supervisión de la actividad de red de Lambda. Para desactivarlo, sustituya `ENABLED` por `DISABLED`.

Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 555555555555 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":
 "ENABLED"}]'
```

Habilitación automática de la Supervisión de la actividad de red de Lambda para todas las cuentas de miembros

Elija su método de acceso preferido para habilitar la característica de supervisión de la actividad de red de Lambda en todas las cuentas de miembros. Esto incluye las cuentas de miembros existentes y las cuentas nuevas que se unen a la organización.

Console

1. Inicia sesión en la GuardDuty consola AWS Management Console y ábrela en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.
2. Realice una de las acciones siguientes:

   Uso de la página Protección de Lambda

   1. En el panel de navegación, elija Protección de Lambda.
   2. Elija Habilitar para todas las cuentas. Esta acción habilita automáticamente la supervisión de la actividad de red de Lambda para las cuentas nuevas y existentes de la organización.
   3. Seleccione Guardar.

> **Note**
>
> La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Uso de la página Cuentas

1. En el panel de navegación, elija Accounts (Cuentas).
2. En la página Cuentas, seleccione las preferencias para Habilitar automáticamente antes de Agregar cuentas mediante invitación.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para todas las cuentas en Supervisión de la actividad de red de Lambda.

> **Note**
>
> De forma predeterminada, esta acción activa automáticamente la opción de activación automática GuardDuty para las cuentas de nuevos miembros.

4. Seleccione Guardar.

Si no puede utilizar la opción Habilitar para todas las cuentas, consulte Habilitación o deshabilitación selectiva de la supervisión de la actividad de red de Lambda para las cuentas de miembros.

API/CLI

- Para habilitar o deshabilitar la supervisión de la actividad de red de Lambda de forma selectiva para las cuentas de miembros, invoque la operación de la API updateMemberDetectors con su propio *`ID de detector`*.
- En el siguiente ejemplo se muestra cómo se puede habilitar la supervisión de la actividad de red de Lambda para una sola cuenta de miembro. Para deshabilitar una cuenta de miembro, sustituya `ENABLED` por `DISABLED`.

  Para encontrar la correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación de la supervisión de la actividad de red de Lambda para todas las cuentas de miembros activas existentes

Elija su método de acceso preferido para habilitar la supervisión de la actividad de red de Lambda para todas las cuentas de miembros activas existentes de la organización.

Console

Configuración de la supervisión de la actividad de red de Lambda para todas las cuentas de miembros activas existentes

1. Inicia sesión en la GuardDuty consola AWS Management Console y ábrela en https://console.aws.amazon.com/guardduty/.

   Inicie sesión con las credenciales de la cuenta GuardDuty de administrador delegado.
2. En el panel de navegación, elija Protección de Lambda.
3. En la página Protección de Lambda, puede ver el estado actual de la configuración. En la sección Cuentas de miembros activas, seleccione Acciones.
4. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
5. Seleccione Confirmar.

API/CLI

- Para habilitar o deshabilitar la supervisión de la actividad de red de Lambda de forma selectiva para las cuentas de miembros, invoque la operación de la API updateMemberDetectors con su propio *`ID de detector`*.

- En el siguiente ejemplo se muestra cómo se puede habilitar la supervisión de la actividad de red de Lambda para una sola cuenta de miembro. Para deshabilitar una cuenta de miembro, sustituya `ENABLED` por `DISABLED`.

  Para encontrar las correspondientes `detectorId` a tu cuenta y a la región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
  ```

  También puede pasar una lista de ID de cuentas separadas por un espacio.
- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación automática de la Supervisión de la actividad de red de Lambda para las nuevas cuentas de miembros

Elija su método de acceso preferido para habilitar la supervisión de la actividad de red de Lambda en las nuevas cuentas de miembros que se unen a la organización.

Console

La cuenta de GuardDuty administrador delegado puede activar Lambda Network Activity Monitoring para las cuentas de los nuevos miembros de una organización mediante la página Lambda Protection o la página Cuentas.

Habilitación automática de la Supervisión de la actividad de red de Lambda para las nuevas cuentas de miembros

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.
2. Realice una de las acciones siguientes:
   - Uso de la página Protección de Lambda:

     1. En el panel de navegación, elija Protección de Lambda.
     2. En la página Protección de Lambda, seleccione Editar.

3. Elija Configurar cuentas manualmente.
4. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que cada vez que una nueva cuenta se una a su organización, la protección de Lambda se habilitará automáticamente para la cuenta. Solo la cuenta de GuardDuty administrador delegado de la organización puede modificar esta configuración.
5. Seleccione Guardar.

- Mediante la página Cuentas:

1. En el panel de navegación, elija Accounts (Cuentas).
2. En la página Cuentas, seleccione Habilitar automáticamente las preferencias.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para las nuevas cuentas en Supervisión de la actividad de red de Lambda.
4. Seleccione Guardar.

API/CLI

- A fin de habilitar o deshabilitar la supervisión de la actividad de red de Lambda para las nuevas cuentas de miembros, invoque la operación de la API UpdateOrganizationConfiguration con su propio *`ID de detector`*.
- En el siguiente ejemplo se muestra cómo se puede habilitar la supervisión de la actividad de red de Lambda para una sola cuenta de miembro. Para deshabilitar esta característica, consulte Habilitación o deshabilitación selectiva de la supervisión de la actividad de red de Lambda para las cuentas de miembros. Si no quiere habilitarla para todas las cuentas nuevas que se unan a la organización, establezca `AutoEnable` en `NONE`.

  Para encontrar la correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración en la consola https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
   "LAMBDA_NETWORK_LOGS", "AutoEnable": "NEW"}]'
  ```

  También puede pasar una lista de ID de cuentas separadas por un espacio.
- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación o deshabilitación selectiva de la supervisión de la actividad de red de Lambda para las cuentas de miembros

Elija el método de acceso que prefiera para habilitar o deshabilitar de forma selectiva la supervisión de la actividad de red de Lambda en las cuentas de miembros.

Console

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.
2. En el panel de navegación, en Configuración, seleccione Cuentas.

   En la página Cuentas, revise la columna Supervisión de la actividad de red de Lambda. Indica si la supervisión de la actividad de red de Lambda está habilitada o no.
3. Elija la cuenta para la que desee configurar la protección de Lambda. Puede elegir varias cuentas a la vez.
4. En el menú desplegable Editar planes de protección, elija Supervisión de la actividad de red de Lambda y, a continuación, elija una acción adecuada.

API/CLI

Invoque la API updateMemberDetectors con su propio *ID de detector*.

En el siguiente ejemplo se muestra cómo se puede habilitar la supervisión de la actividad de red de Lambda para una sola cuenta de miembro. Para desactivarlo, sustituya `ENABLED` por `DISABLED`.

Para encontrar las de `detectorId` su cuenta y su región actual, consulte la página de configuración en la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":
 "ENABLED"}]'
```

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Protección contra malware en Amazon GuardDuty

La Protección contra malware ayuda a detectar la presencia potencial de malware mediante el análisis de los volúmenes de Amazon Elastic Block Store (Amazon EBS) adjuntados a las instancias y cargas de trabajo de contenedores de Amazon Elastic Compute Cloud (Amazon EC2). La protección contra malware ofrece opciones de análisis en las que puede decidir si desea incluir o excluir instancias y cargas de trabajo de contenedores específicas de Amazon EC2 en el momento del análisis. También ofrece la opción de conservar en sus cuentas las instantáneas de los volúmenes de Amazon EBS adjuntos a las instancias de Amazon EC2 o a las cargas de trabajo de contenedores. GuardDuty Las instantáneas se conservan solo cuando se encuentra malware y se generan los resultados de la protección contra malware.

La protección contra malware ofrece dos tipos de análisis para detectar actividades potencialmente maliciosas en las instancias de Amazon EC2 y las cargas de trabajo de contenedores: el análisis de malware GuardDuty iniciado y el análisis de malware bajo demanda. En la siguiente tabla, se muestra la comparación entre ambos tipos de análisis.

Factor	GuardDuty-análisis de malware iniciado	Análisis de malware bajo demanda
Cómo se invoca el análisis	Tras activar el análisis GuardDuty de malware iniciado, siempre que se GuardDuty genere un hallazgo que indique la posible presencia de malware en una instancia de Amazon EC2 o en una carga de trabajo de un contenedo r GuardDuty , se iniciará automáticamente un análisis de malware sin agentes en los volúmenes de Amazon EBS adjuntos al recurso potencialmente afectado. Para obtener más información,	Para iniciar un análisis de malware bajo demanda, puede proporcionar el nombre de recurso de Amazon (ARN) asociado a la instancia o carga de trabajo de contenedo r de Amazon EC2. Puede iniciar un análisis de malware bajo demanda incluso cuando no se haya GuardDuty encontrado nada relacionado con su recurso. Para obtener más información, consulte Análisis de malware bajo demanda.

Factor	GuardDuty-análisis de malware iniciado	Análisis de malware bajo demanda
	consulte GuardDuty-análisis de malware iniciado.	
Se necesita configuración	Para utilizar el análisis GuardDuty de malware iniciado por correo electrónico, debe habilitarlo en su cuenta. Para obtener más informaci ón, consulte Configuración del GuardDuty análisis de malware iniciado.	Tu cuenta debe estar GuardDuty habilitada. Para utilizar el análisis de malware bajo demanda, no es necesaria ninguna configura ción a nivel de función.
Tiempo de espera para iniciar un nuevo análisis	Cada vez que se GuardDuty genera uno de ellosHallazgos que invocan un análisis GuardDuty de malware iniciado, el análisis de malware se inicia automátic amente solo una vez cada 24 horas.	Puede iniciar un análisis de malware bajo demanda en el mismo recurso en cualquier momento después de 1 hora desde la hora de inicio del análisis anterior.
Disponibilidad del periodo de prueba gratuito de 30 días	Cuando actives la GuardDuty detección de malware iniciada por primera vez en tu cuenta, podrás utilizar un período de prueba gratuito de 30 días*.	No hay un período de prueba gratuito* con el análisis de malware bajo demanda para cuentas nuevas o existentes GuardDuty .

Factor	GuardDuty-análisis de malware iniciado	Análisis de malware bajo demanda
Opciones de análisis	Una vez que hayas configurado el análisis GuardDuty de malware iniciado, Malware Protection también te ayuda a seleccionar qué recursos analizar u omitir. La Protección contra malware no iniciará un análisis automático de los recursos que decida excluir de este.	El análisis de malware bajo demanda admite una etiqueta global:`GuardDuty Excluded` . Opciones de análisis con etiquetas definidas por el usuariono se aplica al análisis de software malicioso bajo demanda porque el ARN del recurso se proporciona manualmente.

*Se incurrirá en costos de uso al crear y retener las instantáneas de los volúmenes de EBS. Para obtener más información sobre cómo configurar su cuenta para conservar las instantáneas, consulte. Retención de instantáneas

La protección contra malware es una mejora opcional y está diseñada de forma que no afecte al rendimiento de sus recursos. GuardDuty Para obtener información sobre cómo funciona la protección contra malware en GuardDuty Internet, consulteCaracterística de protección contra malware. Para obtener información sobre la disponibilidad de la protección contra malware en diferentes Regiones de AWS versiones, consulteRegiones y puntos de conexión.

> **Note**
>
> GuardDuty La protección contra malware no es compatible con Fargate ni con Amazon EKS ni con Amazon ECS.

Característica de protección contra malware

Volumen de Elastic Block Storage (EBS)

En esta sección se explica cómo Malware Protection, que incluye tanto el análisis de malware GuardDuty iniciado como el análisis de malware a pedido, analiza los volúmenes de Amazon

EBS asociados a sus instancias de Amazon EC2 y cargas de trabajo de contenedores. Antes de continuar, tenga en cuenta las siguientes personalizaciones:

- Opciones de análisis: la Protección contra malware ofrece la posibilidad de especificar etiquetas para incluir o excluir las instancias de Amazon EC2 y los volúmenes de Amazon EBS del proceso de análisis. Solo el análisis GuardDuty de malware iniciado con ayuda de las opciones de análisis con etiquetas definidas por el usuario. Tanto el análisis GuardDuty de malware iniciado como el análisis de malware bajo demanda admiten la etiqueta global. `GuardDutyExcluded` Para obtener más información, consulte Opciones de análisis con etiquetas definidas por el usuario.
- Retención de instantáneas: Malware Protection ofrece una opción para conservar las instantáneas de sus volúmenes de Amazon EBS en su cuenta. AWS Esta opción está desactivada de forma predeterminada. Puede optar por conservar las instantáneas para los escaneos de malware GuardDuty iniciados o bajo demanda. Para obtener más información, consulte Retención de instantáneas.

Si GuardDuty genera un hallazgo que indica la posible presencia de malware en una instancia de Amazon EC2 o en la carga de trabajo de un contenedor y se ha activado el tipo de análisis GuardDuty iniciado en Malware Protection, es posible que se invoque un análisis de malware GuardDuty iniciado en función de las opciones de análisis disponibles.

Para iniciar un análisis de malware bajo demanda en los volúmenes de Amazon EBS asociados a una instancia de Amazon EC2, proporcione el nombre de recurso de Amazon (ARN) de la instancia de Amazon EC2.

Como respuesta a un análisis de malware bajo demanda o a un análisis GuardDuty de malware iniciado automáticamente, GuardDuty crea instantáneas de los volúmenes de EBS pertinentes adjuntos al recurso potencialmente afectado y las comparte con el. GuardDuty cuenta de servicio A partir de estas instantáneas, GuardDuty crea una réplica cifrada del volumen de EBS en la cuenta de servicio.

Una vez finalizado el escaneo, GuardDuty elimina las réplicas cifradas de los volúmenes de EBS y las instantáneas de los volúmenes de EBS. Si encuentra malware y ha activado la configuración de retención de instantáneas, las instantáneas de sus volúmenes de EBS no se eliminarán y se conservarán automáticamente en su cuenta. AWS Si no se encuentra ningún malware, las instantáneas de sus volúmenes de EBS no se retendrán, independientemente de la configuración de retención de instantáneas. La configuración de retención de instantáneas está desactivada de manera predeterminada. Para obtener información sobre los costos de las instantáneas y su retención, consulte Precios de Amazon EBS.

GuardDuty conservará cada volumen de réplica de EBS en la cuenta de servicio durante un máximo de 55 horas. Si se produce una interrupción del servicio o un fallo en una réplica de un volumen de EBS y en su análisis de software malicioso, GuardDuty se conservará dicho volumen de EBS durante un máximo de siete días. El período prolongado de retención del volumen sirve para clasificar y solucionar la interrupción o el fallo. GuardDuty Malware Protection eliminará las réplicas de los volúmenes de EBS de la cuenta de servicio una vez que se haya solucionado la interrupción o el fallo, o una vez transcurrido el período de retención prolongado.

Volúmenes de Amazon EBS compatibles para el análisis de malware

En todos los Regiones de AWS lugares GuardDuty compatibles con la función Malware Protection, puede escanear los volúmenes de Amazon EBS cifrados o sin cifrar. Puede tener volúmenes de Amazon EBS cifrados con una clave gestionada por el cliente Clave administrada de AWSo con una clave. En la actualidad, algunos de ellos Regiones de AWS admiten ambas formas de cifrar los volúmenes de Amazon EBS, mientras que otros solo admiten claves administradas por el cliente.

Para obtener más información sobre los casos en los que aún no se admite esta capacidad, consulte China Regions

La siguiente lista describe la clave que se GuardDuty utiliza independientemente de que los volúmenes de Amazon EBS estén cifrados o no:

- Los volúmenes de Amazon EBS que no están cifrados o cifrados con Clave administrada de AWS: GuardDuty utilizan su propia clave para cifrar las réplicas de los volúmenes de Amazon EBS.

  Si su cuenta pertenece a una Región de AWS que no admite el escaneo de volúmenes de Amazon EBS que están cifrados con el valor predeterminado Clave administrada de AWS de EBS, consulte. Modificación del identificador de AWS KMS clave predeterminado de un volumen de Amazon EBS
- Volúmenes de Amazon EBS cifrados con una clave administrada por el cliente: GuardDuty utilizan la misma clave para cifrar el volumen de EBS de réplica.

Malware Protection no admite el escaneo de instancias de Amazon EC2 con `productCode` as. `marketplace` Si se inicia un análisis de malware para una instancia de Amazon EC2 de este tipo, se omitirá el análisis. Para obtener más información, consulte `UNSUPPORTED_PRODUCT_CODE_TYPE` en Motivos para omitir un recurso durante el análisis de malware.

Modificación del identificador de AWS KMS clave predeterminado de un volumen de Amazon EBS

De forma predeterminada, al invocar la CreateVolumeAPI con el cifrado establecido en `true` y sin especificar el ID de clave de KMS, se crea un volumen de Amazon EBS que se cifra con la AWS KMS clave predeterminada para el cifrado de EBS. Sin embargo, cuando no se proporciona una clave de cifrado de forma explícita, puede modificar la clave predeterminada invocando la ModifyEbsDefaultKmsKeyIdAPI o utilizando el comando correspondiente. AWS CLI

Para modificar la ID de clave predeterminada de EBS, agregue el siguiente permiso necesario a su política de IAM: `ec2:modifyEbsDefaultKmsKeyId`. Cualquier volumen de Amazon EBS recién creado que elija cifrar, pero que no especifique un ID de clave de KMS asociado, utilizará el ID de clave predeterminado. Utilice uno de los siguientes métodos para actualizar la ID de clave predeterminada de EBS:

Modificación de la ID de clave de KMS predeterminada de un volumen de Amazon EBS

Realice una de las acciones siguientes:

- Uso de una API: puede utilizar la ModifyEbsDefaultKmsKeyIdAPI. Para obtener información sobre cómo ver el estado de cifrado de su volumen, consulte Crear un volumen de Amazon EBS.
- Uso del AWS CLI comando: el siguiente ejemplo modifica el ID de clave de KMS predeterminado que cifrará los volúmenes de Amazon EBS si no proporciona un ID de clave de KMS. Asegúrese de sustituir la región por la Región de AWS de su ID de clave KM.

  ```
  aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-
  id AKIAIOSFODNN7EXAMPLE
  ```

  El comando anterior generará un resultado similar al siguiente:

  ```
  {
    "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
  }
  ```

  Para obtener más información, consulta modify-ebs-default-kms-key-id.

Personalizaciones en la Protección contra malware

En esta sección, se describe cómo puede personalizar las opciones de análisis para sus instancias de Amazon EC2 o cargas de trabajo de contenedores cuando se invoca un análisis de malware, ya sea que se inicie bajo demanda o de forma automática. GuardDuty

Configuración general

Retención de instantáneas

GuardDuty le ofrece la opción de conservar las instantáneas de sus volúmenes de EBS en su cuenta. AWS La configuración de retención de instantáneas está desactivada de manera predeterminada. Las instantáneas solo se retendrán si ha activado esta configuración antes de que se inicie el análisis.

Cuando se inicia el escaneo, GuardDuty genera las réplicas de los volúmenes de EBS en función de las instantáneas de los volúmenes de EBS. Cuando se complete el análisis y se haya activado la configuración de conservación de instantáneas en su cuenta, las instantáneas de sus volúmenes de EBS solo se retendrán cuando se detecte malware y se genere Tipos de búsqueda de protección contra malware. Ya sea que haya activado o no la configuración de retención de instantáneas, cuando no se detecte ningún malware, las instantáneas de los volúmenes de GuardDuty EBS se eliminarán automáticamente.

Costo de uso de instantáneas

Durante el análisis de malware, a medida que se GuardDuty crean las instantáneas de los volúmenes de Amazon EBS, hay un coste de uso asociado a este paso. Si activa la configuración de retención de instantáneas en su cuenta, cuando se detecte malware y se conserven las instantáneas, incurrirá en costos de uso por el mismo. Para obtener información sobre el costo de las instantáneas y su retención, consulte Precios de Amazon EBS.

Elija su método de acceso preferido para activar la configuración de retención de instantáneas.

Console

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, en Planes de protección, elija Protección contra malware.
3. Elija Configuración general en la sección inferior de la consola. Para retener las instantáneas, active Retención de instantáneas.

API/CLI

1. Ejecute UpdateMalwareScanSettingspara actualizar la configuración actual de retención de instantáneas.
2. Como alternativa, puede ejecutar el siguiente AWS CLI comando para conservar automáticamente las instantáneas cuando GuardDuty Malware Protection detecte información.

   Asegúrese de sustituir el *detector-id* por su propio `detectorId` válido.
3. Para encontrar las correspondientes `detectorId` a su cuenta y región actuales, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625554d637e0e4bb3b2 --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

4. Si desea desactivar la retención de instantáneas, sustituya `RETENTION_WITH_FINDING` por `NO_RETENTION`.

Opciones de análisis con etiquetas definidas por el usuario

Al utilizar el análisis GuardDuty de malware iniciado, también puede especificar etiquetas para incluir o excluir las instancias de Amazon EC2 y los volúmenes de Amazon EBS del proceso de análisis y detección de amenazas. Puede personalizar cada análisis GuardDuty de malware iniciado editando las etiquetas de la lista de etiquetas de inclusión o exclusión. Cada lista puede incluir hasta 50 etiquetas.

Si aún no tiene etiquetas definidas por el usuario asociadas a sus recursos de EC2, consulte Etiquetar los recursos de Amazon EC2 en la Guía del usuario de Amazon EC2 para instancias de Linux o Etiquetar los recursos de Amazon EC2 en la Guía del usuario de Amazon EC2 para instancias de Windows.

> **Note**
>
> El análisis de malware bajo demanda no admite opciones de análisis con etiquetas definidas por el usuario. Es compatible con Etiqueta `GuardDutyExcluded` global.

Exclusión de las instancias de EC2 del análisis de malware

Si desea excluir cualquier instancia de Amazon EC2 o volumen de Amazon EBS durante el proceso de digitalización, puede configurar la `GuardDutyExcluded` etiqueta `true` para cualquier instancia de Amazon EC2 o volumen de Amazon EBS y no la escaneará. GuardDuty Para obtener más información acerca de las etiquetas de `GuardDutyExcluded`, consulte Permisos de roles vinculados a servicios para Protección contra malware. También puede agregar una etiqueta de instancia de Amazon EC2 a una lista de exclusión. Si agrega varias etiquetas a la lista de exclusión de etiquetas, cualquier instancia de Amazon EC2 que contenga al menos una de estas etiquetas se excluirá del proceso de análisis de malware.

Elija el método de acceso que prefiera para agregar una etiqueta asociada a una instancia de Amazon EC2 a una lista de exclusión.

Console

1. Abra la consola en https://console.aws.amazon.com/guardduty/ GuardDuty .
2. En el panel de navegación, en Planes de protección, elija Protección contra malware.
3. Amplíe la sección Etiquetas de inclusión/exclusión. Elija Add tags (Añadir etiquetas).
4. Elija Etiquetas de exclusión y, a continuación, elija Confirmar.
5. Especifique el par **`Key`**-**`Value`** de la etiqueta que desee excluir. Es opcional proporcionar el **`Value`**. Después de agregar todas las etiquetas, elija Guardar.

   > **Important**
   >
   > Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte Restricciones de las etiquetas en la Guía del usuario de Amazon EC2 para instancias de Linux o Restricciones de las etiquetas en la Guía del usuario de Amazon EC2 para instancias de Windows.

   Si no se proporciona un valor para una clave y la instancia de EC2 está etiquetada con la clave especificada, esta instancia de EC2 se excluirá del proceso de análisis GuardDuty de software malicioso iniciado, independientemente del valor asignado a la etiqueta.

API/CLI

- Para actualizar la configuración del análisis de malware, excluya del proceso de análisis una instancia de EC2 o una carga de trabajo de contenedores.

  El siguiente comando de AWS CLI ejemplo añade una nueva etiqueta a la lista de etiquetas de exclusión. Asegúrese de sustituir el *detector-id* de ejemplo por su propio `detectorId` válido.

  `MapEquals` es una lista de pares `Key-Value`.

  Para encontrar la correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Exclude":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

  > **Important**
  >
  > Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte Restricciones de las etiquetas en la Guía del usuario de Amazon EC2 para instancias de Linux o Restricciones de las etiquetas en la Guía del usuario de Amazon EC2 para instancias de Windows.

Inclusión de las instancias de EC2 en el análisis de malware

Si desea analizar una instancia de EC2, agregue su etiqueta a la lista de inclusión. Al agregar una etiqueta a una lista de inclusión de etiquetas, las instancias de EC2 que no contengan ninguna de las etiquetas agregadas se omiten del análisis de malware. Si agrega varias etiquetas a la lista de inclusión de etiquetas, se incluirá en el análisis de malware una instancia de EC2 que contenga al menos una de esas etiquetas. A veces, es posible que se omita una instancia de EC2 durante el proceso de análisis. Para obtener más información, consulte Motivos para omitir un recurso durante el análisis de malware.

Elija el método de acceso que prefiera para agregar una etiqueta asociada a una instancia de EC2 a una lista de inclusión.

Console

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, en Planes de protección, elija Protección contra malware.
3. Amplíe la sección Etiquetas de inclusión/exclusión. Elija Add tags (Añadir etiquetas).
4. Elija Etiquetas de inclusión y, a continuación, elija Confirmar.
5. Elija Agregar nueva etiqueta de inclusión y especifique el par de **`Key`** y **`Value`** de la etiqueta que desee incluir. Es opcional proporcionar el **`Value`**.

   Una vez que haya agregado todas las etiquetas de inclusión, elija Guardar.

   Si no se proporciona un valor para una clave y se etiqueta una instancia de EC2 con la clave especificada, esta instancia de EC2 se incluirá en el proceso de análisis de protección contra malware, independientemente del valor asignado a la etiqueta.

API/CLI

- Actualice la configuración del análisis de malware para que incluya una instancia de EC2 o una carga de trabajo de contenedores.

  El siguiente comando de AWS CLI ejemplo agrega una etiqueta nueva a la lista de etiquetas de inclusión. Asegúrese de sustituir el *`detector-id`* de ejemplo por su propio `detectorId` válido. Sustituya el ejemplo *`TestKey`*y *`TestValue`*por el `Value` par `Key` y de la etiqueta asociada a su recurso de EC2.

  `MapEquals` es una lista de pares `Key-Value`.

  Para encontrar la correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Include":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

> **Important**
>
> Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte Restricciones de las etiquetas en la Guía del usuario de Amazon EC2 para instancias de Linux o Restricciones de las etiquetas en la Guía del usuario de Amazon EC2 para instancias de Windows.

> **Note**
>
> La detección de una nueva etiqueta puede tardar hasta 5 minutos. GuardDuty

En cualquier momento, puede elegir entre etiquetas de inclusión o etiquetas de exclusión, pero no ambas. Si quiere cambiar de una etiqueta a otra, selecciónela en el menú desplegable cuando agregue nuevas etiquetas y confirme su selección. Esta acción borra todas las etiquetas actuales.

Etiqueta **`GuardDutyExcluded`** global

Las instantáneas de los volúmenes de EBS se crean con una etiqueta `GuardDutyScanId` de manera predeterminada. No quite esta etiqueta, ya que si lo hace, no podrá acceder GuardDuty a las instantáneas. Ambos tipos de análisis de protección contra malware no analizan las instancias de Amazon EC2 ni los volúmenes de Amazon EBS que tienen la etiqueta `GuardDutyExcluded` establecida como `true`. Si se realiza un análisis de protección contra malware en este tipo de recurso, se generará una ID de análisis, pero este se omitirá con un motivo `EXCLUDED_BY_SCAN_SETTINGS`. Para obtener más información, consulte Motivos para omitir un recurso durante el análisis de malware.

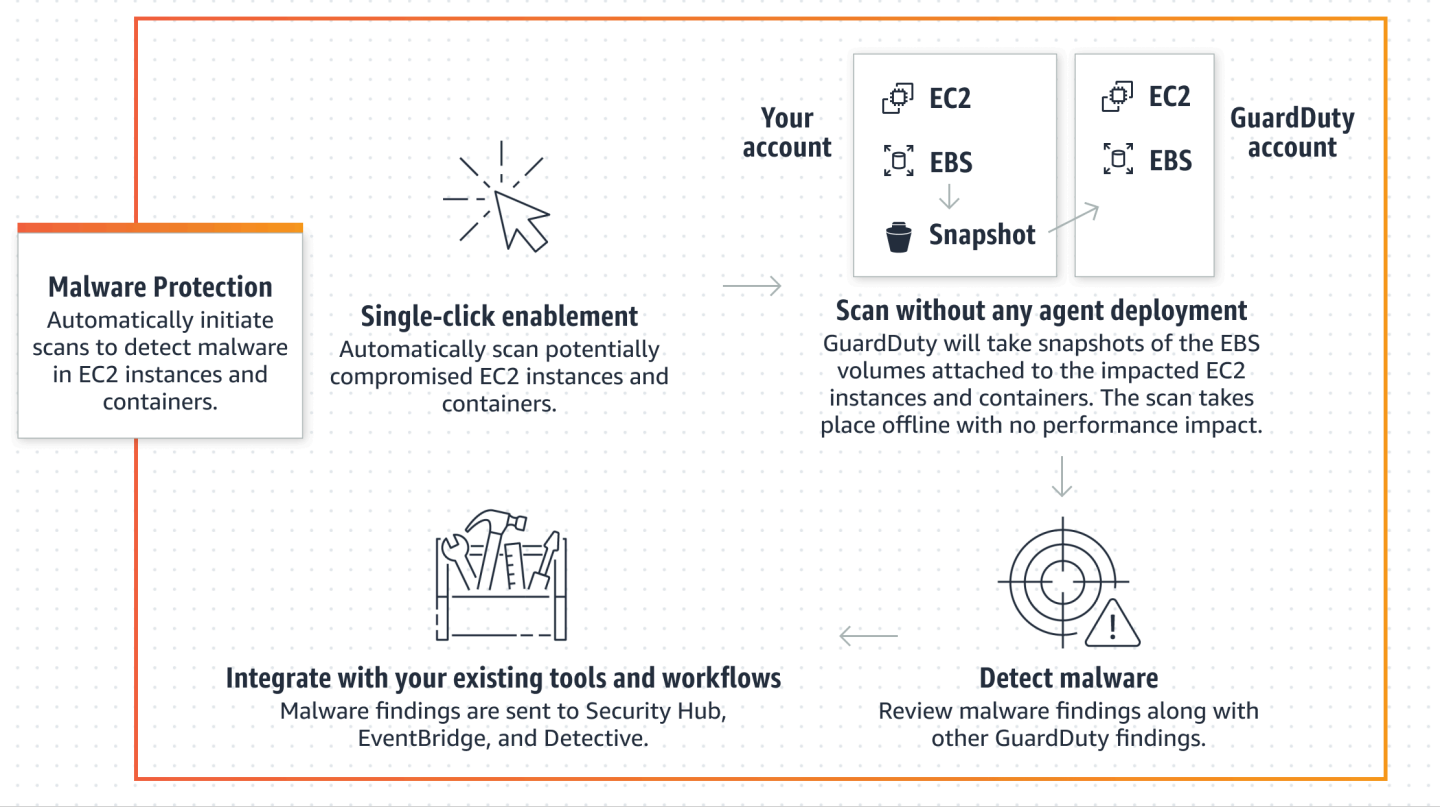
GuardDuty-análisis de malware iniciado

Con el análisis GuardDuty de malware iniciado activado, cada vez que GuardDuty detecta una actividad maliciosa que indique la posible presencia de malware en la carga de trabajo de la instancia o contenedor de Amazon EC2 GuardDuty y se Hallazgos que invocan un análisis GuardDuty de malware iniciado genera GuardDuty , inicia automáticamente un escaneo sin agente en los volúmenes de Amazon Elastic Block Store (Amazon EBS) adjuntos a la carga de trabajo de la instancia o contenedor de Amazon EC2 potencialmente afectada para detectar la presencia de malware. Con las opciones de análisis, puede agregar etiquetas de inclusión asociadas

a los recursos que desee analizar o agregar etiquetas de exclusión asociadas a los recursos que desee omitir en el proceso de análisis. Al iniciar el análisis automáticamente, siempre se tendrán en cuenta sus opciones de análisis. También puede optar por activar la configuración de retención de instantáneas para retener las instantáneas de sus volúmenes de EBS solo si la Protección contra malware detecta la presencia de malware. Para obtener más información, consulte Personalizaciones en la Protección contra malware.

Para cada carga de trabajo de instancia y contenedor de Amazon EC2 que GuardDuty genere hallazgos, se invoca un análisis GuardDuty de malware iniciado automáticamente una vez cada 24 horas. Para obtener información sobre cómo se analizan los volúmenes de Amazon EBS adjuntos a la instancia o carga de trabajo de contenedor de Amazon EC2, consulte Característica de protección contra malware.

En la siguiente imagen se describe cómo funciona el GuardDuty análisis de malware iniciado.



Cuando se encuentra malware, GuardDuty se genera. Tipos de búsqueda de protección contra malware Si GuardDuty no se detecta la presencia de malware en el mismo recurso, no se realizará ningún análisis de malware GuardDuty iniciado. También puede iniciar un análisis de malware bajo demanda en el mismo recurso. Para obtener más información, consulte Análisis de malware bajo demanda.

Cómo afecta el período de prueba gratuita de 30 días a las cuentas GuardDuty

Puedes activar o desactivar la función de análisis de malware GuardDuty iniciada en cualquier cuenta o disponible Regiones de AWS en cualquier momento.

- Al activarla GuardDuty por primera vez (GuardDuty cuenta nueva), el análisis GuardDuty de malware iniciado ya está activado e incluido en el período de prueba gratuito de 30 días.
- GuardDuty Las cuentas existentes pueden activar el análisis GuardDuty de malware iniciado por primera vez con un período de prueba gratuito de 30 días.
- Si ya tienes una GuardDuty cuenta que utilizaba la protección contra malware antes de que el análisis de malware bajo demanda estuviera disponible de forma generalizada y esta GuardDuty cuenta ya utiliza el modelo de precios correspondiente Región de AWS, no es necesario realizar ninguna acción para seguir utilizando el análisis GuardDuty de malware iniciado.

> **Note**
>
> Si dispone de un periodo de prueba gratuito de 30 días, se seguirán aplicando los costos de uso por la creación de instantáneas de los volúmenes de Amazon EBS y su retención. Para obtener más información, consulte Precios de Amazon EBS.

Para obtener información sobre cómo habilitar el análisis GuardDuty de malware iniciado por terceros, consulte. Configuración del GuardDuty análisis de malware iniciado

Configuración del GuardDuty análisis de malware iniciado

Cómo configurar el análisis GuardDuty de malware iniciado desde cero para una cuenta independiente

En el caso de las cuentas asociadas AWS Organizations, puedes automatizar este proceso mediante la configuración de la consola, tal y como se describe en la siguiente sección.

Para activar o desactivar el GuardDuty análisis de malware iniciado

Elija el método de acceso que prefiera para configurar el análisis GuardDuty de malware iniciado para una cuenta independiente.

Console

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, en Planes de protección, elija Protección contra malware.
3. El panel Protección contra malware muestra el estado actual del análisis GuardDuty de malware iniciado en su cuenta. Puede activarlo o desactivarlo en cualquier momento mediante la selección de Activar o Desactivar respectivamente.
4. Seleccione Guardar.

API/CLI

- Ejecute la operación de la API updateDetector con su propio ID de detector regional y pase el objeto `dataSources` con los `EbsVolumes` establecidos en `true` o `false`.

  También puede activar o desactivar el análisis GuardDuty de malware iniciado mediante herramientas de línea de AWS comandos ejecutando el siguiente AWS CLI comando. No olvide utilizar su propio *`ID de detector`* válido.

  > **Note**
  >
  > El siguiente código de ejemplo habilita el análisis GuardDuty de malware iniciado por correo electrónico. Para desactivarlo, sustituya `true` por `false`.

  Para encontrar el correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
 aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "EBS_MALWARE_PROTECTION", "Status" : "ENABLED"}]'
```

Configuración del análisis GuardDuty de malware iniciado en entornos con varias cuentas

En un entorno con varias cuentas, solo las cuentas de GuardDuty administrador pueden configurar GuardDuty la detección de malware iniciada. GuardDuty las cuentas de administrador pueden habilitar o deshabilitar el uso de escaneos de malware GuardDuty iniciados por ellos para sus

cuentas de miembros. Una vez que la cuenta de administrador haya configurado la detección de malware GuardDuty iniciada por un usuario, ésta seguirá los ajustes de la cuenta de administrador y no podrá modificarlos a través de la consola. GuardDuty Las cuentas de administrador que gestionen sus cuentas de miembros con el servicio de AWS Organizations asistencia pueden optar por activar automáticamente la detección de malware GuardDuty iniciada en todas las cuentas nuevas y existentes de la organización. Para obtener más información, consulte Administrar GuardDuty cuentas con AWS Organizations.

Establecer un acceso confiable para permitir la detección GuardDuty de malware iniciada

Si la cuenta de administrador GuardDuty delegado no es la misma que la cuenta de administración de su organización, la cuenta de administración debe habilitar el análisis GuardDuty de malware iniciado por la organización. De esta forma, la cuenta de administrador delegado puede crear las cuentas de los miembros Permisos de roles vinculados a servicios para Protección contra malware mediante las que se administran. AWS Organizations

> **Note**
>
> Antes de designar una cuenta de GuardDuty administrador delegado, consulte. Recomendaciones y consideraciones

Elija el método de acceso que prefiera para permitir que la cuenta de GuardDuty administrador delegado GuardDuty habilite el análisis de malware iniciado para detectar las cuentas de los miembros de la organización.

Console

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Para iniciar sesión, utilice la cuenta de administración de su AWS Organizations organización.

2. a. Si no ha designado una cuenta de GuardDuty administrador delegado, entonces:

      En la página de configuración, en la sección Cuenta de GuardDuty administrador delegado, introduzca los 12 dígitos **`account ID`** que desee designar para administrar la GuardDuty política en su organización. Elija Delegar.

   b. i. Si ya ha designado una cuenta de GuardDuty administrador delegado diferente de la cuenta de administración, haga lo siguiente:

En la página Configuración, en Administrador delegado, active la configuración Permisos. Esta acción permitirá a la cuenta de GuardDuty administrador delegado adjuntar los permisos pertinentes a las cuentas de los miembros y habilitar la detección de malware GuardDuty iniciada en estas cuentas de los miembros.

ii. Si ya has designado una cuenta de GuardDuty administrador delegado que sea igual a la cuenta de administración, puedes activar directamente la detección de malware GuardDuty iniciada por terceros en las cuentas de los miembros. Para obtener más información, consulte Habilite automáticamente el análisis GuardDuty de malware iniciado por usted en todas las cuentas de los miembros.

> **Tip**
>
> Si la cuenta de GuardDuty administrador delegado es diferente de tu cuenta de administración, debes proporcionar permisos a la cuenta de GuardDuty administrador delegado para permitir la detección de malware GuardDuty iniciada por software malicioso en las cuentas de los miembros.

3. Si quieres permitir que la cuenta de GuardDuty administrador delegado active la detección de cuentas de miembros GuardDuty de otras regiones iniciada por software malicioso, cámbiala y repite los pasos Región de AWS anteriores.

API/CLI

1. Con sus credenciales de la cuenta de administración, ejecute el siguiente comando:

```
aws organizations enable-aws-service-access --service-principal malware-
protection.guardduty.amazonaws.com
```

2. (Opcional) Para habilitar la detección de malware GuardDuty iniciada para la cuenta de administración que no sea una cuenta de administrador delegado, la cuenta de administración primero creará la detección de malware de Permisos de roles vinculados a servicios para Protección contra malware forma explícita en su cuenta y, a continuación, habilitará la detección de malware GuardDuty iniciada desde la cuenta de administrador delegado, de forma similar a la de cualquier otra cuenta de miembro.

```
aws iam create-service-linked-role --aws-service-name malware-
protection.guardduty.amazonaws.com
```

3. Ha designado la cuenta de GuardDuty administrador delegado en la cuenta actualmente seleccionada. Región de AWS Si ha designado una cuenta como cuenta de GuardDuty administrador delegado en una región, esa cuenta debe ser su cuenta de GuardDuty administrador delegado en todas las demás regiones. Repita el paso anterior para el resto de las regiones.

Configuración del análisis GuardDuty de malware iniciado para una cuenta de administrador delegado GuardDuty

Elija el método de acceso que prefiera para activar o desactivar el análisis GuardDuty de malware iniciado por una cuenta de administrador delegado GuardDuty .

Console

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de administración.
2. En el panel de navegación, elija Protección contra malware.
3. En la página Protección contra malware, selecciona Editar junto a la exploración GuardDuty de malware iniciada.
4. Realice una de las acciones siguientes:

   Uso de Habilitar para todas las cuentas

   - Elija Habilitar para todas las cuentas. Esto habilitará el plan de protección para todas las GuardDuty cuentas activas de su AWS organización, incluidas las cuentas nuevas que se unan a la organización.
   - Seleccione Guardar.

   Uso de Configurar cuentas manualmente

   - Para habilitar el plan de protección solo para la cuenta de GuardDuty administrador delegado, elija Configurar cuentas manualmente.

- Seleccione Activar en la sección de la cuenta de GuardDuty administrador delegado (esta cuenta).
- Seleccione Guardar.

API/CLI

Ejecute la operación de la API updateDetector con su propio ID de detector regional y pase el `name` del objeto `features` como `EBS_MALWARE_PROTECTION` y `status` como `ENABLED` o `DISABLED`.

Puede activar o desactivar el análisis GuardDuty de malware iniciado mediante la ejecución del siguiente AWS CLI comando. Asegúrese de utilizar el ID de *`detector`* válido de la cuenta de GuardDuty administrador delegado.

> **Note**
>
> El siguiente código de ejemplo habilita el análisis GuardDuty de malware iniciado por el usuario. Para desactivarlo, sustituya `ENABLED` por `DISABLED`.

Para encontrar el correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /
              --account-ids 555555555555 /
              --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Habilite automáticamente el análisis GuardDuty de malware iniciado por usted en todas las cuentas de los miembros

Elige tu método de acceso preferido para activar la función de detección de malware GuardDuty iniciada en todas las cuentas de los miembros. Esto incluye las cuentas de miembros existentes y las cuentas nuevas que se unen a la organización.

Console

1. Inicie sesión en la GuardDuty consola AWS Management Console y ábrala en https://console.aws.amazon.com/guardduty/.

Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. Realice una de las acciones siguientes:

   Uso de la página Protección contra malware

   1. En el panel de navegación, elija Protección contra malware.
   2. En la página de protección contra malware, selecciona Editar en la sección de análisis GuardDutyde malware iniciada.
   3. Elija Habilitar para todas las cuentas. Esta acción habilita automáticamente el análisis GuardDuty de malware iniciado para detectar tanto las cuentas existentes como las nuevas de la organización.
   4. Seleccione Guardar.

   > **Note**
   >
   > La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

   Uso de la página Cuentas

   1. En el panel de navegación, elija Accounts (Cuentas).
   2. En la página Cuentas, seleccione las preferencias para Habilitar automáticamente antes de Agregar cuentas mediante invitación.
   3. En la ventana Administrar preferencias de activación automática, selecciona Activar para todas las cuentas sometidas a un análisis GuardDutyde malware iniciado.
   4. En la página Protección contra malware, selecciona Editar en la sección de análisis GuardDutyde malware iniciado.
   5. Elija Habilitar para todas las cuentas. Esta acción habilita automáticamente el análisis GuardDuty de malware iniciado para detectar tanto las cuentas existentes como las nuevas de la organización.
   6. Seleccione Guardar.

> **Note**
>
> La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Uso de la página Cuentas

1. En el panel de navegación, elija Accounts (Cuentas).
2. En la página Cuentas, seleccione las preferencias para Habilitar automáticamente antes de Agregar cuentas mediante invitación.
3. En la ventana Administrar preferencias de activación automática, selecciona Activar para todas las cuentas sometidas a un análisis GuardDutyde malware iniciado.
4. Seleccione Guardar.

Si no puede utilizar la opción Habilitar para todas las cuentas, consulte Activa o desactiva de forma selectiva el análisis GuardDuty de malware iniciado en las cuentas de los miembros.

API/CLI

- *Para activar o desactivar de forma selectiva el análisis GuardDuty de malware iniciado en las cuentas de sus miembros, ejecute la operación de la updateMemberDetectorsAPI con su propio identificador de detección.*
- En el siguiente ejemplo, se muestra cómo activar el análisis GuardDuty de malware iniciado por una cuenta de un solo miembro. Para deshabilitar una cuenta de miembro, sustituya `ENABLED` por `DISABLED`.

  Para encontrar la correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
  ```

  También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilite el análisis GuardDuty de malware iniciado por correo electrónico para todas las cuentas de miembros activas existentes

Elige el método de acceso que prefieras para activar el análisis GuardDuty de malware iniciado en todas las cuentas de miembros activos existentes en la organización.

Para configurar el análisis GuardDuty de malware iniciado para todas las cuentas de miembros activas existentes

1. Inicie sesión en la GuardDuty consola AWS Management Console y ábrala en https://console.aws.amazon.com/guardduty/.

   Inicie sesión con las credenciales de la cuenta GuardDuty de administrador delegado.
2. En el panel de navegación, elija Protección contra malware.
3. En la sección Protección contra malware, puede ver el estado actual de la configuración de análisis GuardDutyde malware iniciada. En la sección Cuentas de miembros activas, seleccione Acciones.
4. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
5. Seleccione Guardar.

Habilite automáticamente el análisis GuardDuty de malware iniciado para las cuentas de los nuevos miembros

Las cuentas de los miembros recién agregadas deben habilitarse GuardDuty antes de seleccionar la configuración del análisis GuardDuty de malware iniciado. Las cuentas de los miembros gestionadas mediante invitación pueden configurar manualmente la detección GuardDuty de malware iniciada para sus cuentas. Para obtener más información, consulte Step 3 - Accept an invitation.

Elija el método de acceso que prefiera para activar la detección de malware GuardDuty iniciada en busca de nuevas cuentas que se unan a su organización.

Console

La cuenta de GuardDuty administrador delegado puede activar el análisis GuardDuty de software malicioso iniciado para detectar nuevas cuentas de miembros en una organización mediante la página de protección contra malware o la página de cuentas.

Para habilitar automáticamente el análisis GuardDuty de malware iniciado para las cuentas de nuevos miembros

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.
2. Realice una de las acciones siguientes:
   - Mediante la página Protección contra malware:
     1. En el panel de navegación, elija Protección contra malware.
     2. En la página de protección contra malware, seleccione Editar en el análisis GuardDutyde malware iniciado.
     3. Elija Configurar cuentas manualmente.
     4. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que cada vez que una nueva cuenta se incorpore a tu organización, el análisis de malware GuardDuty iniciado se active automáticamente en esa cuenta. Solo la cuenta de GuardDuty administrador delegado de la organización puede modificar esta configuración.
     5. Seleccione Guardar.
   - Mediante la página Cuentas:
     1. En el panel de navegación, elija Accounts (Cuentas).
     2. En la página Cuentas, seleccione Habilitar automáticamente las preferencias.
     3. En la ventana Administrar preferencias de activación automática, selecciona Habilitar cuentas nuevas en el marco de un análisis GuardDutyde malware iniciado.
     4. Seleccione Guardar.

API/CLI

- *Para activar o desactivar la detección de malware GuardDuty iniciada por una cuenta de nuevos miembros, invoca la operación de la*

UpdateOrganizationConfigurationAPI con tu propio identificador de detección.

- En el siguiente ejemplo, se muestra cómo se puede activar el análisis GuardDuty de malware iniciado por una cuenta de un solo miembro. Para deshabilitar esta característica, consulte Activa o desactiva de forma selectiva el análisis GuardDuty de malware iniciado en las cuentas de los miembros. Si no quiere habilitarla para todas las cuentas nuevas que se unan a la organización, establezca `AutoEnable` en `NONE`.

  Para encontrar la correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name":
   "EBS_MALWARE_PROTECTION", "AutoEnable": NEW}]'
  ```

  También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Activa o desactiva de forma selectiva el análisis GuardDuty de malware iniciado en las cuentas de los miembros

Elija el método de acceso que prefiera para configurar de forma selectiva el análisis GuardDuty de malware iniciado para las cuentas de los miembros.

Console

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, elija Accounts (Cuentas).
3. En la página de cuentas, consulta la columna GuardDutyde análisis de malware iniciada para ver el estado de tu cuenta de miembro.
4. Seleccione la cuenta para la que desee configurar el análisis GuardDuty de malware iniciado. Puede seleccionar varias cuentas de manera simultánea.
5. En el menú Editar planes de protección, elija la opción adecuada para GuardDutyiniciar el análisis de malware.

API/CLI

Para activar o desactivar de forma selectiva el análisis GuardDuty de malware iniciado en las cuentas de sus miembros, ejecute la operación de la updateMemberDetectorsAPI con su propio identificador de detección.

En el siguiente ejemplo, se muestra cómo activar el análisis GuardDuty de malware iniciado por una cuenta de un solo miembro. Para desactivarlo, sustituya `ENABLED` por `DISABLED`.

Para encontrar la correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION",
 "Status": "ENABLED"}]'
```

> **Note**
>
> También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Para activar o desactivar de forma selectiva el análisis GuardDuty de malware iniciado por sus cuentas de miembros, ejecute la operación de la updateMemberDetectorsAPI con su propio identificador de *detección*. En el siguiente ejemplo, se muestra cómo activar el análisis GuardDuty de malware iniciado por una cuenta de un solo miembro. Para desactivarlo, sustituya `true` por `false`.

Para encontrar la correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 123456789012 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

> **Note**
>
> También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilite el análisis GuardDuty de malware iniciado previamente para detectar las cuentas existentes en la organización administradas mediante invitación

El rol vinculado al servicio de protección contra GuardDuty malware (SLR) debe crearse en las cuentas de los miembros. La cuenta de administrador no puede habilitar la función de análisis de malware GuardDuty iniciada en las cuentas de los miembros que no estén administradas por. AWS Organizations

Actualmente, puedes realizar los siguientes pasos a través de la GuardDuty consola en https://console.aws.amazon.com/guardduty/ para activar el análisis GuardDuty de malware iniciado en las cuentas de los miembros existentes.

Console

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Inicie sesión con las credenciales de su cuenta de administrador.
2. En el panel de navegación, elija Accounts (Cuentas).
3. Seleccione la cuenta de miembro para la que desee activar el análisis GuardDuty de malware iniciado. Puede seleccionar varias cuentas de manera simultánea.
4. Elija Acciones.
5. Seleccione Desasociar miembro.
6. En su cuenta de miembro, seleccione Protección contra malware en Planes de protección, en el panel de navegación.
7. Selecciona Habilitar el análisis GuardDuty de malware iniciado por iniciación automática. GuardDuty creará una cámara réflex para la cuenta del miembro. Para obtener más información sobre los SLR, consulte Permisos de roles vinculados a servicios para Protección contra malware.

8. En la cuenta de administrador, seleccione Cuentas en el panel de navegación.
9. Elija la cuenta de miembro que debe volver a agregarse a la organización.
10. Seleccione Acciones y Agregar miembro.

API/CLI

1. Utilice la cuenta de administrador para ejecutar la DisassociateMembersAPI en las cuentas de los miembros que deseen activar la detección de malware GuardDuty iniciada por terceros.
2. Utilice su cuenta de miembro para invocar y UpdateDetectoractivar el análisis GuardDuty de malware iniciado.

   Para encontrar la correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

   ```
   aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
   {"EbsVolumes":true}}}'
   ```
3. Usa la cuenta de administrador para ejecutar la CreateMembersAPI y volver a añadir al miembro a la organización.

Hallazgos que invocan un análisis GuardDuty de malware iniciado

Se invoca un análisis de malware GuardDuty iniciado cuando GuardDuty detecta un comportamiento sospechoso indicativo de malware en las cargas de trabajo de instancias o contenedores de Amazon EC2.

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- CryptoCurrency:EC2/BitcoinTool.B

- CryptoCurrency:EC2/BitcoinTool.B!DNS
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce (solo salientes)
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/RDPBruteForce (solo salientes)
- UnauthorizedAccess:EC2/SSHBruteForce (solo salientes)
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay
- Backdoor:Runtime/C&CActivity.B
- Backdoor:Runtime/C&CActivity.B!DNS
- CryptoCurrency:Runtime/BitcoinTool.B
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Execution:Runtime/NewBinaryExecuted
- Execution:Runtime/NewLibraryLoaded
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation

- Impact:Runtime/CryptoMinerExecuted
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS
- UnauthorizedAccess:Runtime/MetadataDNSRebind

Análisis de malware bajo demanda

El análisis de malware bajo demanda le ayuda a detectar la presencia de malware en los volúmenes de Amazon Elastic Block Store (Amazon EBS) asociados a sus instancias de Amazon EC2. Sin necesidad de configuración, puede proporcionar el nombre de recurso de Amazon (ARN) de la instancia de Amazon EC2 que desee analizar para iniciar un análisis de malware bajo demanda. Puede iniciar un análisis de malware bajo demanda a través de la GuardDuty consola o la API. Antes de iniciar un análisis de malware bajo demanda, puede establecer la configuración de Retención de instantáneas que prefiera. Los siguientes escenarios pueden ayudarle a identificar cuándo utilizar el tipo de análisis de malware bajo demanda con GuardDuty:

- Desea detectar la presencia de malware en sus instancias de Amazon EC2 sin activar el análisis GuardDuty de malware iniciado.
- Ha activado el análisis GuardDuty de malware iniciado por ordenador y se ha iniciado un análisis automáticamente. Tras seguir la corrección recomendada para el tipo de resultado que ha generado la protección contra malware, si desea iniciar un análisis en el mismo recurso, puede

iniciar un análisis de malware bajo demanda una vez transcurrida 1 hora desde la hora de inicio del análisis anterior.

El análisis de malware bajo demanda no requiere que hayan transcurrido 24 horas desde el momento en que se inició el análisis de malware anterior. Debería haber transcurrido una hora antes de iniciar un análisis de malware bajo demanda en el mismo recurso. Para evitar la duplicación de un análisis de malware en la misma instancia de EC2, consulte Volver a analizar la misma instancia de Amazon EC2.

> **Note**
>
> El análisis de malware bajo demanda no está incluido en el período de prueba gratuito de 30 días con. GuardDuty El costo de uso se aplica al volumen total de Amazon EBS analizado por cada análisis de malware. Para obtener más información, consulta los GuardDuty precios de Amazon. Para obtener información sobre el costo de crear las instantáneas del volumen de Amazon EBS y su retención, consulte Precios de Amazon EBS.

Funcionamiento del análisis de malware bajo demanda

Con el análisis de malware bajo demanda, puede iniciar una solicitud de análisis de malware para su instancia de Amazon EC2 incluso cuando esté en uso. Tras iniciar un análisis de malware bajo demanda, GuardDuty crea instantáneas de los volúmenes de Amazon EBS adjuntos a la instancia de Amazon EC2 cuyo nombre de recurso de Amazon (ARN) se proporcionó para el análisis. A continuación, GuardDuty comparte estas instantáneas con. GuardDuty cuenta de servicio GuardDuty crea réplicas de volúmenes EBS cifrados a partir de esas instantáneas de la GuardDuty cuenta de servicio. Para obtener más información sobre cómo se analizan los volúmenes de Amazon EBS, consulte Volumen de Elastic Block Storage (EBS).

> **Note**
>
> GuardDuty crea las instantáneas de los datos que ya se han escrito en los volúmenes de Amazon EBS point-in-time al iniciar un análisis de malware bajo demanda.

Si se encuentra malware y ha activado la configuración de conservación de instantáneas, las instantáneas de su volumen de EBS se retendrán automáticamente en su Cuenta de AWS. El

análisis de malware bajo demanda genera el Tipos de búsqueda de protección contra malware. Si no se encuentra ningún malware, las instantáneas de sus volúmenes de EBS se eliminarán, independientemente de la configuración de retención de instantáneas.

Las instantáneas de los volúmenes de EBS se crean con una etiqueta `GuardDutyScanId` de manera predeterminada. No elimine esta etiqueta, ya que si lo hace, no podrá acceder GuardDuty a las instantáneas. Ambos tipos de análisis de protección contra malware no analizan las instancias de Amazon EC2 ni los volúmenes de Amazon EBS que tienen la etiqueta `GuardDutyExcluded` establecida como `true`. Si se realiza un análisis de protección contra malware en este tipo de recurso, se generará una ID de análisis, pero este se omitirá con un motivo `EXCLUDED_BY_SCAN_SETTINGS`. Para obtener más información, consulte Motivos para omitir un recurso durante el análisis de malware.

AWS Organizations política de control de servicios: acceso denegado

Al utilizar las políticas de control de servicios (SCP) de AWS Organizations, la cuenta de GuardDuty administrador delegado puede restringir los permisos y denegar acciones, como iniciar un análisis de malware bajo demanda para detectar una instancia de Amazon EC2 propiedad de sus cuentas.

Como cuenta de GuardDuty miembro, al iniciar un análisis de malware bajo demanda para sus instancias de Amazon EC2, es posible que reciba un error. Puede conectarse con la cuenta de administración para saber por qué se ha configurado una SCP para su cuenta de miembro. Para más información, consulte Efectos de las SCP en los permisos.

Introducción al análisis de malware bajo demanda

Como cuenta de GuardDuty administrador, puedes iniciar un análisis de malware bajo demanda en nombre de las cuentas de los miembros activos que tengan configurados los siguientes requisitos previos en sus cuentas. Las cuentas independientes y las cuentas de miembros activos también GuardDuty pueden iniciar un análisis de malware bajo demanda para sus propias instancias de Amazon EC2.

Requisitos previos

- GuardDuty debe estar habilitado en el Regiones de AWS lugar en el que desee iniciar el análisis de malware bajo demanda.
- Asegúrese de que el AWS política gestionada: AmazonGuardDutyFullAccess esté asociado al usuario de IAM o rol de IAM. Necesitará la clave de acceso y la clave secreta asociadas al usuario de IAM o rol de IAM.

- Como cuenta de GuardDuty administrador delegado, tiene la opción de iniciar un análisis de malware bajo demanda en nombre de una cuenta de miembro activa.
- Si tiene una cuenta de miembro que no tiene la Permisos de roles vinculados a servicios para Protección contra malware, al iniciar un análisis de malware bajo demanda para detectar una instancia de Amazon EC2 que pertenezca a su cuenta, se creará automáticamente el SLR para protección contra malware.

> **Important**
>
> Asegúrese de que nadie elimine los permisos de la SLR para la protección contra malware cuando el análisis de malware, ya sea GuardDuty iniciado o bajo demanda, aún esté en curso. Si lo hace, impedirá que el análisis se complete correctamente y proporcione un resultado definitivo.

Antes de iniciar un análisis de malware bajo demanda, asegúrese de que no se haya iniciado ningún análisis en el mismo recurso en la última hora; de lo contrario, se eliminará el duplicado. Para obtener más información, consulte Volver a analizar el mismo recurso.

Inicio de un análisis de malware bajo demanda

Elija el método de acceso que prefiera para iniciar un análisis de malware bajo demanda.

Console

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. Inicie el análisis mediante una de las siguientes opciones:
    a. Mediante la página Protección contra malware:
        i. En el panel de navegación, en Planes de protección, elija Protección contra malware.
        ii. En la página Protección contra malware, proporcione el ARN de la instancia de Amazon EC2[1] para la que desea iniciar el análisis.
    b. Mediante la página Análisis de malware:
        i. En el panel de navegación, elija Análisis de malware.

ii. Seleccione Iniciar análisis bajo demanda y proporcione el ARN de la instancia de Amazon EC2[1] para la que desea iniciar el análisis.

iii. Si se ha vuelto a hacer el análisis, seleccione una ID de instancia de Amazon EC2 en la página Análisis de malware.

Amplíe el menú desplegable Iniciar análisis bajo demanda y seleccione Volver a analizar la instancia seleccionada.

3. Después de iniciar correctamente un análisis con cualquiera de los métodos, se genera una ID de análisis. Puede utilizar este ID de análisis para hacer un seguimiento del progreso del análisis. Para obtener más información, consulte Supervisión de los estados y resultados de los análisis de malware.

API/CLI

StartMalwareScanInvoque que acepte la instancia 1 `resourceArn` de Amazon EC2 para la que desea iniciar un análisis de malware bajo demanda.

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-
east-1:555555555555:instance/i-b188560f"
```

Tras iniciar correctamente un análisis, `StartMalwareScan` devuelve una `scanId`. Invoque el DescribeMalwareScansmonitor para ver el progreso del análisis iniciado.

[1]Para obtener información sobre el formato del ARN de su instancia de Amazon EC2, consulte Nombre de recurso de Amazon (ARN). Para las instancias de Amazon EC2, puede utilizar el siguiente formato de ARN de ejemplo sustituyendo los valores de la partición, la región, la ID de Cuenta de AWS y la ID de la instancia de Amazon EC2. Para obtener información sobre la longitud del ID de instancia, consulte ID de recursos.

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

Volver a analizar la misma instancia de Amazon EC2

Tanto si el análisis se GuardDuty inicia como si es a petición, puede iniciar un nuevo análisis de malware bajo demanda en la misma instancia de EC2 transcurrido 1 hora desde la hora de inicio del análisis de malware anterior. Si el nuevo análisis de malware se inicia una hora desde el inicio del

anterior, su solicitud generará el siguiente error y no se generará ninguna ID de análisis para esta solicitud.

```
A scan was initiated on this resource recently. You can request a scan on
the same resource one hour after the previous scan start time.
```

Para obtener información sobre cómo iniciar un nuevo análisis en el mismo recurso, consulte Inicio de un análisis de malware bajo demanda.

Para hacer un seguimiento del estado de los análisis de malware, consulte Supervisar los estados de los escaneos y los resultados de la protección contra malware GuardDuty .

Supervisar los estados de los escaneos y los resultados de la protección contra malware GuardDuty

Puede supervisar el estado de cada análisis de GuardDuty Malware Protection. Los valores posibles de Estado de un análisis son `Completed`, `Running`, `Skipped` y `Failed`.

Una vez finalizado el análisis, el Resultado del análisis se rellena para los análisis que tienen el Estado `Completed`. Los valores posibles para el Resultado del análisis son `Clean` y `Infected`. Con Tipo de análisis, puede identificar si el análisis de malware fue `GuardDuty initiated` o `On demand`.

Los resultados de cada análisis de malware tienen un periodo de retención de 90 días. Elija el método de acceso que prefiera para realizar un seguimiento del estado de su análisis de malware.

Console

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, elija Análisis de malware.
3. Puede filtrar los análisis de malware según las siguientes Propiedades disponibles en los Criterios de filtro.
   - ID de análisis
   - ID de cuenta
   - ARN de instancia de EC2
   - Tipo de análisis
   - Estado del análisis

Para obtener información sobre las propiedades utilizadas como criterios de filtro, consulte Detalles de los resultados.

API/CLI

- Una vez que el análisis de malware tenga un resultado, puede filtrar los análisis de malware en función de su `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE`, `GUARDDUTY_FINDING_ID`, `SCAN_STATUS` y `SCAN_START_TIME`.

  Los criterios de `GUARDDUTY_FINDING_ID` filtrado están disponibles cuando `SCAN_TYPE` se GuardDuty inicia el. Para obtener información sobre cualquier criterio de filtro, consulte Detalles de los resultados.
- Puede cambiar los *`filter-criteria`* de ejemplo en el siguiente comando. Actualmente, puede filtrar de una `CriterionKey` a la vez. Las opciones de `CriterionKey` son `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE` `GUARDDUTY_FINDING_ID`, `SCAN_STATUS` y `SCAN_START_TIME`.

  Si utiliza la misma `CriterionKey` que se muestra a continuación, asegúrese de sustituir el `EqualsValue` de ejemplo por su propio *`scan-id`* de AWS válida.

  Sustituya el `detector-id` de ejemplo por su propio *`detector-id`* válido. Puede cambiar los *`max-results`* (hasta 50) y los *`sort-criteria`*. El `AttributeName` es obligatorio y debe ser `scanStartTime`.

  ```
  aws guardduty describe-malware-scans --detector-
  id 60b87779336485625 54d637e0e4bb3b2 --max-results 1 --sort-criteria
   '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
   '{"FilterCriterion":[{"CriterionKey":"SCAN_ID", "FilterCondition":
  {"EqualsValue":"123456789012"}}] }'
  ```
- La respuesta de este comando muestra un resultado como máximo con detalles sobre el recurso afectado y los resultados de malware (si está `Infected`).

GuardDuty cuentas de servicio por Región de AWS

Cuando se crea una instantánea y se comparte con una cuenta de GuardDuty servicio, se crea un nuevo evento en tus CloudTrail registros. Este evento especifica la `snapshotId` and `userId`

(cuenta GuardDuty de servicio correspondiente Región de AWS). Para obtener más información, consulte Característica de protección contra malware.

El siguiente ejemplo es un fragmento de un CloudTrail evento que muestra el cuerpo de la solicitud: `ModifySnapshotAttribute`

```
"requestParameters": {
        "snapshotId": "snap-1234567890abcdef0",
        "createVolumePermission": {
            "add": {
                "items": [
                    {
                        "userId": "111122223333"
                    }
                ]
            }
        },
        "attributeType": "CREATE_VOLUME_PERMISSION"
    }
```

En la siguiente tabla se muestran las cuentas GuardDuty de servicio de cada región. `userId`Es la cuenta GuardDuty de servicio y depende de la región seleccionada.

Región de AWS	Código de región	GuardDuty ID de cuenta de servicio (**`userId`**)
Este de EE. UU. (Norte de Virginia)	us-east-1	652050842985
Este de EE. UU. (Ohio)	us-east-2	178123968615
Oeste de EE. UU. (Norte de California)	us-west-1	669213148797
Oeste de EE. UU. (Oregón)	us-west-2	447226417196
Asia-Pacífico (Bombay)	ap-south-1	913179291432
Asia-Pacífico (Osaka)	ap-northeast-3	089661699081

Región de AWS	Código de región	GuardDuty ID de cuenta de servicio (**`userId`**)
Asia-Pacífico (Seúl)	ap-northeast-2	039163547507
Asia-Pacífico (Tokio)	ap-northeast-1	874749492622
Asia-Pacífico (Singapur)	ap-southeast-1	247460962669
Asia-Pacífico (Sídney)	ap-southeast-2	124839743349
Canadá (centro)	ca-central-1	175877067165
Oeste de Canadá (Calgary)	ca-west-1	894794104037
Europa (Fráncfort)	eu-central-1	002294850712
Europa (Irlanda)	eu-west-1	283769539786
Europa (Londres)	eu-west-2	310125036783
Europa (París)	eu-west-3	866607715269
Europa (Estocolmo)	eu-north-1	693780578038
China (Pekín)	cn-north-1	448721096076
China (Ningxia)	cn-northwest-1	480864352451
América del Sur (São Paulo)	sa-east-1	546914126324
Asia-Pacífico (Hyderabad) (Activar)	ap-south-2	682251015962
Asia-Pacífico (Melbourne) (Activar)	ap-southeast-4	353488359550
Europa (España) (Activar)	eu-south-2	936182149045

Región de AWS	Código de región	GuardDuty ID de cuenta de servicio (**`userId`**)
Europa (Zúrich) (Activar)	eu-central-2	867642063380
Israel (Tel Aviv) (Activar)	il-central-1	619233833001
Europa (Milán) (Activar)	eu-south-1	977238331021
Asia-Pacífico (Hong Kong) (Activar)	ap-east-1	249472122084
Medio Oriente (Baréin) (Activar)	me-south-1	404001805210
África (Ciudad del Cabo) (Activar)	af-south-1	957664736811
Asia-Pacífico (Yakarta) (Activar)	ap-southeast-3	452118225523
Medio Oriente (EAU) (Activar)	me-central-1	828603743433

Cuotas de protección contra malware

La protección contra malware tiene la siguiente disponibilidad predeterminada de los diversos recursos que utiliza la característica.

Ámbito	Predeterminado	Comentarios
Extracción y análisis de datos en un documento comprimido o archivado	5	El número máximo de niveles anidados permitidos en un documento archivado.
Número de documentos dentro de un documento archivado	1 000	El número máximo de archivos que se pueden analizar dentro de un archivo.

Ámbito	Predeterminado	Comentarios
		Este recuento es la suma del número de documento s extraídos del archivo y el número de documento s extraídos de todos los archivos anidados.
Número de amenazas	32	El número máximo de amenazas que puede ver en el panel de resultados. GuardDuty Es posible que Malware Protection haya detectado más nombres de amenazas. Si el número de nombres de amenazas detectadas es superior al valor predeterminado, puede ver los detalles del JSON seleccionando el identificador de búsqueda situado debajo del nombre de búsqueda en el panel de detalles de la GuardDuty consola.
Número de archivos por amenaza detectada	5	El número máximo de archivos identificados por amenaza detectada. Por ejemplo, si GuardDuty detecta 10 archivos asociados a una sola amenaza, la amenaza mostrará un máximo de 5 archivos.

Ámbito	Predeterminado	Comentarios
Volúmenes de EBS por análisis por instancia	11	El número máximo de volúmenes de EBS que GuardDuty se pueden escanear por instancia de EC2. Si hay más de 11 volúmenes de EBS que deben escanearse, GuardDuty Malware Protection los ordena `deviceName` alfabéticamente y selecciona los primeros 11 volúmenes de EBS.
Tamaño del volumen de EBS	1024 GB	El tamaño máximo del volumen de EBS en GB que GuardDuty Malware Protection puede escanear en cada región.

Ámbito	Predeterminado	Comentarios
Tipos de sistemas de archivos compatibles	GuardDuty Malware Protection puede analizar los siguientes tipos de sistemas de archivos: • Sistema de archivos de nueva tecnología (NTFS) • Sistema de archivos X (XFS) • Sistema de archivos de segunda extensión (ext2) • Sistema de archivos de cuarta extensión (ext4) • Sistema de archivos con tabla de asignación de archivos (FAT) • Sistema de archivos con tabla de asignación de archivos virtuales (VFAT)	N/A.
Etiquetas de opciones de análisis	50	El máximo número de etiquetas de recursos que puede agregar para personalizar la configuración de las opciones de análisis de malware. Para obtener más información, consulte Opciones de análisis con etiquetas definidas por el usuario.

Ámbito	Predeterminado	Comentarios
Periodo de conservación de hallazgos	90	El número máximo de días que GuardDuty retiene un hallazgo. Para obtener la información más reciente, consulte Cuotas para Amazon GuardDuty.
Periodo de retención de análisis de malware	90	El número máximo de días que GuardDuty Malware Protection conserva el historial de un análisis. Para obtener más información acerca de la visualización de análisis de malware recientes, consulte Supervisar los estados de los escaneos y los resultados de la protección contra malware GuardDuty .
Transacciones por segundo (TPS) para análisis de malware bajo demanda	1	El número de solicitudes de análisis de malware bajo demanda que se pueden iniciar por segundo en cada región.
Límite de ampliación para el análisis de malware bajo demanda	1	El número de solicitudes de análisis de malware bajo demanda simultáneas que se pueden iniciar por segundo en cada región.

GuardDuty Protección RDS

RDS Protection en Amazon GuardDuty analiza y perfila la actividad de inicio de sesión en RDS para detectar posibles amenazas de acceso a sus bases de datos de Amazon Aurora (Amazon Aurora compatible con MySQL Edition y Aurora PostgreSQL compatible con Aurora). Esta característica le permite identificar comportamientos de inicio de sesión potencialmente sospechosos. La protección de RDS no requiere infraestructura adicional; está diseñada para no afectar al rendimiento de las instancias de bases de datos.

Cuando RDS Protection detecta un intento de inicio de sesión potencialmente sospechoso o anómalo que indica una amenaza para su base de datos, GuardDuty genera un nuevo hallazgo con detalles sobre la base de datos potencialmente comprometida.

Puedes activar o desactivar la función de protección RDS para cualquier cuenta en cualquier Región de AWS lugar en el que esta función esté disponible en Amazon GuardDuty y en cualquier momento. Una GuardDuty cuenta existente puede activar la protección de RDS con un período de prueba de 30 días. En el caso de una GuardDuty cuenta nueva, la protección RDS ya está habilitada e incluida en el período de prueba gratuito de 30 días. Para obtener más información, consulte Estimación del costo.

> **Note**
>
> Cuando la función de protección RDS no está habilitada, GuardDuty no recopila su actividad de inicio de sesión en el RDS ni detecta un comportamiento de inicio de sesión anómalo o sospechoso.

Para obtener información sobre Regiones de AWS dónde aún GuardDuty no es compatible con la protección RDS, consulte. Disponibilidad de características específicas por región

Bases de datos compatibles de Amazon Aurora

En la siguiente tabla, se muestran las versiones compatibles de base de datos de Aurora.

Motor de base de datos de Amazon Aurora	Versiones del motor admitidas
Aurora MySQL	• 2.10.2 o posteriores

Motor de base de datos de Amazon Aurora	Versiones del motor admitidas
	• 3.02.1 o posteriores
Aurora PostgreSQL	• 10.17 o posteriores • 11.12 o posteriores • 12.7 o posteriores • 13.3 o posteriores • 14.3 o posteriores • 15.2 o posterior • 16.1 o posterior

Cómo la protección de RDS utiliza la supervisión de la actividad de inicio de sesión de RDS

La protección RDS de Amazon le GuardDuty ayuda a proteger las bases de datos de Amazon Aurora (Aurora) compatibles en su cuenta. Tras activar la función de protección de RDS, comienza GuardDuty inmediatamente a supervisar la actividad de inicio de sesión de RDS desde las bases de datos de Aurora de su cuenta. GuardDuty supervisa y perfila continuamente la actividad de inicio de sesión de RDS para detectar actividades sospechosas, por ejemplo, el acceso no autorizado a la base de datos Aurora de su cuenta por parte de un actor externo nunca antes visto. Al activar la Protección de RDS por primera vez o al tener una instancia de base de datos recién creada, es necesario un periodo de aprendizaje para establecer un comportamiento normal que sirva de referencia. Por este motivo, es posible que las instancias de bases de datos recién habilitadas o creadas no tengan asociado un resultado de inicio de sesión anómalo hasta dentro de dos semanas. Para obtener más información, consulte Supervisión de la actividad de inicio de sesión de RDS.

Cuando RDS Protection detecta una amenaza potencial, como un patrón inusual en una serie de intentos de inicio de sesión correctos, fallidos o incompletos, GuardDuty genera un nuevo hallazgo con detalles sobre la instancia de base de datos potencialmente comprometida. Para obtener más información, consulte Tipos de búsqueda de RDS Protection. Si deshabilita la protección de RDS, deja de supervisar GuardDuty inmediatamente la actividad de inicio de sesión en RDS y no puede detectar ninguna amenaza potencial para las instancias de base de datos compatibles.

> **Note**
>
> GuardDuty no gestiona su actividad de inicio de sesión Bases de datos compatibles ni la de RDS, ni pone a su disposición la actividad de inicio de sesión de RDS.

Configuración de la protección de RDS para una cuenta independiente

Console

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, elija Protección de RDS.
3. La página Protección de RDS muestra el estado actual de su cuenta. Puede habilitar o deshabilitar la característica en cualquier momento mediante la selección de Habilitar o Deshabilitar. Confirme la opción elegida.

API/CLI

Ejecute la operación de la API updateDetector con su propio ID de detector regional y pase el `name` del objeto `features` como `RDS_LOGIN_EVENTS` y `status` como `ENABLED` o `DISABLED`.

También puede activar o desactivar la protección RDS ejecutando el siguiente AWS CLI comando. No olvide utilizar su propio *`ID de detector`* válido.

> **Note**
>
> El siguiente código de ejemplo habilita la protección de RDS. Para desactivarlo, sustituya `ENABLED` por `DISABLED`.

Para encontrar la correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "RDS_LOGIN_EVENTS", "Status" : "ENABLED"}]'
```

Configuración de la protección de RDS en entornos multicuenta

En un entorno de cuentas múltiples, solo la cuenta de GuardDuty administrador delegado tiene la opción de activar o desactivar la función de protección RDS para las cuentas de los miembros de su organización. Las cuentas de GuardDuty los miembros no pueden modificar esta configuración desde sus cuentas. La cuenta de GuardDuty administrador delegado administra sus cuentas de miembros mediante AWS Organizations. Esta cuenta de GuardDuty administrador delegado puede optar por habilitar automáticamente la supervisión de la actividad de inicio de sesión de RDS para todas las cuentas nuevas a medida que se unan a la organización. Para obtener más información sobre los entornos de varias cuentas, consulta Administrar varias cuentas en Amazon. GuardDuty

Configuración de la protección de RDS para una cuenta de administrador delegado GuardDuty

Elija el método de acceso que prefiera para configurar la supervisión de la actividad de inicio de sesión de RDS para la cuenta de administrador delegado GuardDuty .

Console

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de administración.
2. En el panel de navegación, elija Protección de RDS.
3. En la página Protección de RDS, elija Editar.
4. Realice una de las acciones siguientes:

   Uso de Habilitar para todas las cuentas

   - Elija Habilitar para todas las cuentas. Esto habilitará el plan de protección para todas las GuardDuty cuentas activas de su AWS organización, incluidas las cuentas nuevas que se unan a la organización.
   - Seleccione Guardar.

   Uso de Configurar cuentas manualmente

   - Para habilitar el plan de protección solo para la cuenta de GuardDuty administrador delegado, elija Configurar cuentas manualmente.

- Seleccione Activar en la sección de la cuenta de GuardDuty administrador delegado (esta cuenta).
- Seleccione Guardar.

API/CLI

Ejecute la operación de la API updateDetector con su propio ID de detector regional y pase el `name` del objeto `features` como `RDS_LOGIN_EVENTS` y `status` como `ENABLED` o `DISABLED`.

Puede activar o desactivar la protección RDS ejecutando el siguiente AWS CLI comando. Asegúrese de utilizar el ID de *`detector`* válido de la cuenta de GuardDuty administrador delegado.

> **Note**
>
> El siguiente código de ejemplo habilita la protección de RDS. Para desactivarlo, sustituya `ENABLED` por `DISABLED`.

Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 555555555555 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

Habilitación automática de la protección de RDS para todas las cuentas de miembros

Elija su método de acceso preferido para habilitar la característica de protección de RDS en todas las cuentas de miembros. Esto incluye las cuentas de miembros existentes y las cuentas nuevas que se unen a la organización.

Console

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.
2. Realice una de las acciones siguientes:

Mediante la página Protección de RDS

1. En el panel de navegación, elija Protección de RDS.
2. Elija Habilitar para todas las cuentas. Esta acción habilita automáticamente la protección de RDS para las cuentas nuevas y existentes de la organización.
3. Seleccione Guardar.

> **Note**
>
> La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Uso de la página Cuentas

1. En el panel de navegación, elija Accounts (Cuentas).
2. En la página Cuentas, seleccione las preferencias para Habilitar automáticamente antes de Agregar cuentas mediante invitación.
3. En la ventana Administrar preferencias de habilitación automática, elija Habilitar para todas las cuentas en Supervisión de la actividad de inicio de sesión de RDS.
4. Seleccione Guardar.

Si no puede utilizar la opción Habilitar para todas las cuentas, consulte Activación o desactivación de la Protección de RDS para las cuentas de miembros de forma selectiva.

API/CLI

- Para activar o desactivar la Protección de RDS de forma selectiva para sus cuentas de miembro, invoque la operación de la API updateMemberDetectors con su propio *`ID de detector`*.
- El siguiente ejemplo muestra cómo se puede habilitar la protección de RDS para una sola cuenta de miembro. Para desactivarlo, sustituya `ENABLED` por `DISABLED`.

  Para encontrar las de `detectorId` su cuenta y su región actual, consulte la página de configuración en la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

> **Note**
>
> También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación de la protección de RDS para todas las cuentas de miembros activos existentes

Elija su método de acceso preferido para habilitar la protección de RDS en todas las cuentas de miembros activos existentes en la organización.

Console

Configuración de la protección de RDS para todas las cuentas de miembros activos existentes

1. Inicia sesión en la GuardDuty consola AWS Management Console y ábrela en https://console.aws.amazon.com/guardduty/.

   Inicie sesión con las credenciales de la cuenta GuardDuty de administrador delegado.
2. En el panel de navegación, elija Protección de RDS.
3. En la página Protección de RDS, puede ver el estado actual de la configuración. En la sección Cuentas de miembros activas, seleccione Acciones.
4. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
5. Seleccione Confirmar.

API/CLI

- Para activar o desactivar la Protección de RDS de forma selectiva para sus cuentas de miembro, invoque la operación de la API updateMemberDetectors con su propio *ID de detector*.
- El siguiente ejemplo muestra cómo se puede habilitar la protección de RDS para una sola cuenta de miembro. Para desactivarlo, sustituya `ENABLED` por `DISABLED`.

  Para encontrar las correspondientes `detectorId` a tu cuenta y a la región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación automática de la Protección de RDS para las cuentas de miembros nuevos

Elija su método de acceso preferido para habilitar la actividad de inicio de sesión de RDS para las cuentas nuevas que se unan a la organización.

Console

La cuenta de GuardDuty administrador delegado puede habilitar las cuentas de nuevos miembros de una organización a través de la consola, desde la página de protección de RDS o desde la página de cuentas.

Habilitación automática de la Protección de RDS para las cuentas de miembros nuevos

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. Realice una de las acciones siguientes:

   - Mediante la página Protección de RDS:

     1. En el panel de navegación, elija Protección de RDS.
     2. En la página Protección de RDS, elija Editar.
     3. Elija Configurar cuentas manualmente.
     4. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que, cada vez que una nueva cuenta se una a su organización, la protección de RDS se habilite automáticamente para la cuenta. Solo la cuenta de GuardDuty administrador delegado de la organización puede modificar esta configuración.
     5. Seleccione Guardar.

   - Mediante la página Cuentas:

     1. En el panel de navegación, elija Accounts (Cuentas).
     2. En la página Cuentas, seleccione Habilitar automáticamente las preferencias.
     3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para las cuentas nuevas en Supervisión de la actividad de inicio de sesión de RDS.
     4. Seleccione Guardar.

API/CLI

- Para activar o desactivar la Protección de RDS de forma selectiva para sus cuentas de miembro, invoque la operación de la API UpdateOrganizationConfiguration con su propio *`ID de detector`*.
- El siguiente ejemplo muestra cómo se puede habilitar la protección de RDS para una sola cuenta de miembro. Para deshabilitar esta característica, consulte Activación o desactivación de la Protección de RDS para las cuentas de miembros de forma selectiva. Si no quiere habilitarla para todas las cuentas nuevas que se unan a la organización, establezca `autoEnable` en `NONE`.

  Para encontrar la correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración en la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "RDS_LOGIN_EVENTS", "AutoEnable": "NEW"}]'
```

> **Note**
>
> También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Activación o desactivación de la Protección de RDS para las cuentas de miembros de forma selectiva

Elija el método de acceso que prefiera para activar o desactivar de forma selectiva la supervisión de la actividad de inicio de sesión en RDS en las cuentas de miembros.

Console

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.
2. En el panel de navegación, elija Accounts (Cuentas).

   En la página Cuentas, revise la columna Actividad de inicio de sesión de RDS para ver el estado de su cuenta de miembro.
3. Activación o desactivación de forma selectiva de la actividad de inicio de sesión en RDS

   Seleccione la cuenta para la que desee configurar la protección de RDS. Puede seleccionar varias cuentas de manera simultánea. En el menú desplegable Editar planes de protección, seleccione Actividad de inicio de sesión de RDS y, a continuación, elija la opción adecuada.

API/CLI

Para activar o desactivar la Protección de RDS de forma selectiva para sus cuentas de miembro, invoque la operación de la API updateMemberDetectors con su propio *ID de detector*.

El siguiente ejemplo muestra cómo se puede habilitar la protección de RDS para una sola cuenta de miembro. Para desactivarlo, sustituya `ENABLED` por `DISABLED`.

Para encontrar las de `detectorId` su cuenta y su región actual, consulte la página de configuración en la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

> **Note**
>
> También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Característica de protección de RDS

Supervisión de la actividad de inicio de sesión de RDS

La actividad de inicio de sesión de RDS captura los intentos de inicio de sesión correctos y fallidos hechos en la Bases de datos compatibles de Amazon Aurora en su entorno de AWS . Para ayudarle a proteger sus bases de datos, GuardDuty RDS Protection supervisa continuamente la actividad de inicio de sesión para detectar posibles intentos de inicio de sesión sospechosos. Por ejemplo, un adversario puede intentar acceder por fuerza bruta a una base de datos de Amazon Aurora si adivina la contraseña de la base de datos.

Al activar la función de protección de RDS, GuardDuty se inicia automáticamente la supervisión de la actividad de inicio de sesión en RDS de sus bases de datos directamente desde el servicio Aurora. Si hay indicios de un comportamiento de inicio de sesión anómalo, GuardDuty genera un resultado con detalles sobre la base de datos potencialmente comprometida. Al activar la Protección de RDS por primera vez o al tener una instancia de base de datos recién creada, es necesario un periodo de aprendizaje para establecer un comportamiento normal que sirva de referencia. Por este motivo, es posible que las instancias de bases de datos recién habilitadas o creadas no tengan asociado un resultado de inicio de sesión anómalo hasta dentro de dos semanas.

La función de protección RDS no requiere ninguna configuración adicional; no afecta a ninguna de las configuraciones de base de datos de Amazon Aurora existentes. GuardDuty no administra las bases de datos compatibles ni la actividad de inicio de sesión de RDS, ni pone a su disposición la actividad de inicio de sesión de RDS.

Si opta por habilitar automáticamente la función de protección RDS para las cuentas de los nuevos miembros al unirse a su organización, esta acción se habilita automáticamente GuardDuty para esas nuevas cuentas de miembros. Para obtener más información sobre cómo configurar la supervisión de la actividad de inicio de sesión en RDS como una característica, consulte GuardDuty Protección RDS.

GuardDuty Supervisión del tiempo de ejecución

Runtime Monitoring observa y analiza los eventos a nivel del sistema operativo, las redes y los archivos para ayudarlo a detectar posibles amenazas en AWS cargas de trabajo específicas de su entorno.

GuardDuty lanzó inicialmente Runtime Monitoring para admitir únicamente los recursos de Amazon Elastic Kubernetes Service (Amazon EKS). Sin embargo, ahora también puede utilizar la función Runtime Monitoring para detectar amenazas para sus recursos de AWS Fargate Amazon Elastic Container Service (Amazon ECS) y Amazon Elastic Compute Cloud (Amazon EC2).

En este documento y en otras secciones relacionadas con la supervisión del tiempo de ejecución, se GuardDuty utiliza la terminología de tipo de recurso para referirse a los recursos de Amazon EKS, Fargate, Amazon ECS y Amazon EC2.

Runtime Monitoring utiliza un agente GuardDuty de seguridad que añade visibilidad al comportamiento en tiempo de ejecución, como el acceso a los archivos, la ejecución de procesos, los argumentos de la línea de comandos y las conexiones de red. Para cada tipo de recurso que desee monitorear para detectar posibles amenazas, puede administrar el agente de seguridad para ese tipo de recurso específico de forma automática o manual (con la excepción de Fargate (solo Amazon ECS)). Administrar el agente de seguridad automáticamente significa que usted permite GuardDuty instalar y actualizar el agente de seguridad en su nombre. Por otro lado, si administra manualmente el agente de seguridad de sus recursos, es responsable de instalar y actualizar el agente de seguridad, según sea necesario.

Con esta capacidad ampliada, GuardDuty puede ayudarlo a identificar y responder a las posibles amenazas que puedan afectar a las aplicaciones y los datos que se ejecutan en sus cargas de trabajo e instancias individuales. Por ejemplo, una amenaza puede empezar por comprometer un único contenedor en el que se ejecuta una aplicación web vulnerable. Es posible que esta aplicación web tenga permisos de acceso a los contenedores y las cargas de trabajo subyacentes. En este escenario, las credenciales mal configuradas podrían dar lugar a un acceso más amplio a la cuenta y a los datos almacenados en ella.

Al analizar los eventos de tiempo de ejecución de los contenedores y las cargas de trabajo individuales, es GuardDuty posible identificar si un contenedor y AWS las credenciales asociadas están en peligro en una fase inicial, y detectar los intentos de escalar los privilegios, las solicitudes de API sospechosas y el acceso malintencionado a los datos de su entorno.

Contenido

Cómo funcionan

Para utilizar Runtime Monitoring, debe habilitar Runtime Monitoring y, a continuación, administrar el agente de GuardDuty seguridad. La siguiente lista explica este proceso de dos pasos:

1. Habilite Runtime Monitoring en su cuenta para que GuardDuty pueda aceptar los eventos de tiempo de ejecución que reciba de sus instancias de Amazon EC2, clústeres de Amazon ECS y cargas de trabajo de Amazon EKS.
2. Administre el GuardDuty agente para los recursos individuales cuyo comportamiento en tiempo de ejecución desee supervisar. Según el tipo de recurso, puede optar por implementar el agente de GuardDuty seguridad manualmente o GuardDuty permitir que lo administre en su nombre, lo que se denomina configuración automática del agente.

   GuardDuty utiliza funciones de identidad de instancia que autentican el agente de seguridad de cada tipo de recurso para enviar los eventos de tiempo de ejecución asociados al punto final de la VPC.

> **Note**
>
> GuardDuty no administra los eventos de tiempo de ejecución de sus instancias de Amazon EC2, clústeres de Amazon ECS o clústeres de Amazon EKS, ni los pone a su disposición.

Si administra el agente de seguridad (de forma manual o a través de él GuardDuty) en EKS Runtime Monitoring o Runtime Monitoring for EC2, y si actualmente GuardDuty está desplegado en una instancia de Amazon EC2 y recibe Tipos de eventos de tiempo de ejecución recopilados el de esta instancia GuardDuty , no se le Cuenta de AWS cobrará por el análisis de los registros de flujo de VPC de esta instancia de Amazon EC2. Esto ayuda a GuardDuty evitar el doble de los gastos de uso de la cuenta.

En los siguientes temas se explica cómo la activación de Runtime Monitoring y la administración del agente de GuardDuty seguridad funcionan de forma diferente para cada tipo de recurso.

Contenido

Cómo funciona Runtime Monitoring con las instancias de Amazon EC2

Sus instancias de Amazon EC2 pueden ejecutar varios tipos de aplicaciones y cargas de trabajo en su entorno. AWS Cuando habilita Runtime Monitoring y administra el agente de GuardDuty seguridad, le GuardDuty ayuda a detectar amenazas en sus instancias Amazon EC2 existentes y en posibles instancias nuevas. Esta función también es compatible con las instancias Amazon EC2 gestionadas por Amazon ECS.

La activación de Runtime GuardDuty Monitoring permite consumir eventos de tiempo de ejecución de procesos nuevos y en ejecución en instancias de Amazon EC2. GuardDuty requiere un agente de seguridad al que enviar los eventos de tiempo de ejecución desde su instancia EC2 a. GuardDuty

En el caso de las instancias Amazon EC2, el agente GuardDuty de seguridad funciona a nivel de instancia. Puede decidir si quiere monitorizar todas las instancias de Amazon EC2 de su cuenta o

solo algunas de ellas. Si desea administrar instancias selectivas, el agente de seguridad solo es necesario para estas instancias.

GuardDuty también puede consumir eventos de tiempo de ejecución de tareas nuevas y tareas existentes que se ejecutan en instancias de Amazon EC2 dentro de los clústeres de Amazon ECS.

Para instalar el agente GuardDuty de seguridad, Runtime Monitoring ofrece las dos opciones siguientes:

- Utilice una configuración de agentes automatizada (recomendado), o
- Administre el agente de seguridad manualmente

Utilice la configuración automática de los agentes mediante GuardDuty (recomendado)

Utilice una configuración de agente automatizada que permita GuardDuty instalar el agente de seguridad en sus instancias de Amazon EC2 en su nombre. GuardDuty también administra las actualizaciones del agente de seguridad.

De forma predeterminada, GuardDuty instala el agente de seguridad en todas las instancias de su cuenta. Si desea GuardDuty instalar y administrar el agente de seguridad solo para determinadas instancias de EC2, añada etiquetas de inclusión o exclusión a las instancias de EC2, según sea necesario.

A veces, es posible que no desee supervisar los eventos de tiempo de ejecución de todas las instancias de Amazon EC2 que pertenecen a su cuenta. En los casos en los que desee supervisar los eventos de tiempo de ejecución de un número limitado de instancias, añada una etiqueta de inclusión como`GuardDutyManaged`: `true` a las instancias seleccionadas. Empezando por la disponibilidad de la configuración de agentes automatizada para Amazon EC2, si su instancia de EC2 tiene una etiqueta de inclusión (`GuardDutyManaged`:`true`), GuardDuty respetará la etiqueta y gestionará el agente de seguridad para las instancias seleccionadas, incluso si no habilita explícitamente la configuración automática del agente.

Por otro lado, si hay un número limitado de instancias de EC2 para las que no desea supervisar los eventos de tiempo de ejecución, añada una etiqueta de exclusión (`GuardDutyManaged`:`false`) a las instancias seleccionadas. GuardDuty respetará la etiqueta de exclusión al no instalar ni administrar el agente de seguridad para estos recursos de EC2.

Impact

Cuando utiliza la configuración de agentes automatizada en una Cuenta de AWS u otra organización, permite GuardDuty realizar los siguientes pasos en su nombre:

- GuardDuty crea una asociación de SSM para todas las instancias de Amazon EC2 gestionadas por SSM y que aparecen en Fleet Manager en la consola https://console.aws.amazon.com/systems-manager/.
- Uso de etiquetas de inclusión con la configuración automática del agente deshabilitada: después de habilitar Runtime Monitoring, si no habilita la configuración automática del agente pero agrega una etiqueta de inclusión a su instancia de Amazon EC2, significa que está permitiendo GuardDuty administrar el agente de seguridad en su nombre. A continuación, la asociación SSM instalará el agente de seguridad en cada instancia que tenga la etiqueta de inclusión (:)`GuardDutyManaged`. `true`
- Si habilita la configuración automática del agente, la asociación SSM instalará el agente de seguridad en todas las instancias de EC2 que pertenezcan a su cuenta.
- Uso de etiquetas de exclusión con configuración de agente automatizada: antes de habilitar la configuración automática de agentes, al añadir una etiqueta de exclusión a la instancia de Amazon EC2, significa que está permitiendo GuardDuty impedir la instalación y la administración del agente de seguridad para la instancia seleccionada.

  Ahora, al habilitar la configuración automática del agente, la asociación SSM instalará y administrará el agente de seguridad en todas las instancias de EC2, excepto en las que estén etiquetadas con la etiqueta de exclusión.
- GuardDuty crea puntos de enlace de VPC en todas las VPC, incluidas las VPC compartidas, siempre que haya al menos una instancia EC2 de Linux en esa VPC que no se encuentre en los estados de instancia terminada o de cierre. Para obtener información sobre los diferentes estados de las instancias, consulte el ciclo de vida de las instancias en la Guía del usuario de Amazon EC2 para instancias de Linux.

  GuardDuty también es compatibleUso de una VPC compartida con agentes de seguridad automatizados. Cuando se tengan en cuenta todos los requisitos previos para su organización Cuenta de AWS, GuardDuty utilizará la VPC compartida para recibir los eventos de tiempo de ejecución.

> **Note**
>
> El uso de los puntos finales de VPC que se crean no conlleva ningún coste adicional. GuardDuty

Administre el agente de seguridad manualmente

Hay dos formas de administrar manualmente el agente de seguridad de Amazon EC2:

- Utilice los documentos GuardDuty gestionados AWS Systems Manager para instalar el agente de seguridad en las instancias de Amazon EC2 que ya están gestionadas por SSM.

  Siempre que lance una nueva instancia de Amazon EC2, asegúrese de que esté habilitada para SSM.
- Utilice los scripts del administrador de paquetes RPM (RPM) para instalar el agente de seguridad en las instancias de Amazon EC2, estén o no gestionadas por SSM.

Siguiente paso

Para empezar con la configuración de Runtime Monitoring para monitorizar las instancias de Amazon EC2, consulte. Requisitos previos para la compatibilidad con instancias Amazon EC2

Cómo funciona Runtime Monitoring con Fargate (solo en Amazon ECS)

Cuando habilita la monitorización del tiempo de ejecución GuardDuty , está preparado para consumir los eventos de tiempo de ejecución de una tarea. Estas tareas se ejecutan dentro de los clústeres de Amazon ECS, que a su vez se ejecutan en las AWS Fargate (Fargate) instancias. GuardDuty Para recibir estos eventos de tiempo de ejecución, debe usar el agente de seguridad dedicado y totalmente administrado.

Actualmente, Runtime Monitoring no admite las tareas lanzadas por AWS Batch y AWS CodePipeline.

Actualmente, Runtime Monitoring admite la administración del agente de seguridad para sus clústeres de Amazon ECS (AWS Fargate) únicamente a través de GuardDuty. No se admite la administración manual del agente de seguridad en los clústeres de Amazon ECS.

Puede GuardDuty permitir la administración del agente GuardDuty de seguridad en su nombre mediante la configuración automática del agente para una AWS cuenta o una organización. GuardDuty empezará a implementar el agente de seguridad en las nuevas tareas de Fargate que se lanzan en sus clústeres de Amazon ECS. La siguiente lista especifica qué esperar al habilitar el agente de GuardDuty seguridad.

Impacto de habilitar el agente GuardDuty de seguridad

GuardDuty crea un punto final de nube privada virtual (VPC)

Al implementar el agente de GuardDuty seguridad, GuardDuty creará un punto final de VPC a través del cual el agente de seguridad envía los eventos de tiempo de ejecución. GuardDuty

GuardDuty añade un contenedor sidecar

Para una nueva tarea o servicio de Fargate que comience a ejecutarse, se adjunta un GuardDuty contenedor (sidecar) a cada contenedor de la tarea Fargate de Amazon ECS. El agente de GuardDuty seguridad se encuentra dentro del contenedor adjunto. GuardDuty Esto ayuda GuardDuty a recopilar los eventos de tiempo de ejecución de cada contenedor que se ejecuta dentro de estas tareas.

Cuando inicias una tarea de Fargate, si el GuardDuty contenedor (sidecar) no puede iniciarse en buen estado, Runtime Monitoring está diseñado para no impedir que las tareas se ejecuten.

De forma predeterminada, las tareas de Fargate son inmutables. GuardDuty no desplegará el sidecar cuando una tarea ya esté en ejecución. Si desea supervisar un contenedor en una tarea que ya está en ejecución, puede detener la tarea e iniciarla de nuevo.

Cómo funciona Runtime Monitoring con los clústeres de Amazon EKS

Runtime Monitoring utiliza un complemento EKS `aws-guardduty-agent`, también denominado agente GuardDuty de seguridad. Una vez desplegado el agente de GuardDuty seguridad en los clústeres de EKS, GuardDuty puede recibir los eventos de tiempo de ejecución de dichos clústeres de EKS.

Puede supervisar los eventos de tiempo de ejecución de sus clústeres de Amazon EKS a nivel de cuenta o de clúster. Puede administrar el agente GuardDuty de seguridad solo para los clústeres de Amazon EKS que desee supervisar para detectar amenazas. Puede administrar el agente GuardDuty de seguridad manualmente o GuardDuty permitir que lo administre en su nombre mediante la configuración automática del agente.

Cuando utilice el enfoque de configuración de agentes automatizado GuardDuty para poder gestionar el despliegue del agente de seguridad en su nombre, este creará automáticamente un punto final de Amazon Virtual Private Cloud (Amazon VPC). El agente de seguridad envía los eventos de tiempo de ejecución GuardDuty mediante este punto de conexión de Amazon VPC.

Actualmente, GuardDuty es compatible con los clústeres de Amazon EKS que se ejecutan en instancias de Amazon EC2. GuardDuty no admite la ejecución de clústeres de Amazon EKS AWS Fargate.

Después de la configuración de Runtime Monitoring

Evalúe la cobertura del tiempo

Tras activar la supervisión del tiempo de ejecución y desplegar el agente de GuardDuty seguridad, le recomendamos que evalúe [de] forma continua el estado de cobertura del recurso en el que ha desplegado el agente de seguridad. El estado de la cobertura puede ser Saludable o Insalubre. Un estado de cobertura en buen estado indica que GuardDuty está recibiendo los eventos de tiempo de ejecución del recurso correspondiente cuando hay una actividad a nivel del sistema operativo.

Cuando el estado de cobertura pasa a ser Correcto para el recurso, GuardDuty puede recibir los eventos de tiempo de ejecución y analizarlos para detectar amenazas. Cuando GuardDuty detecta una posible amenaza a la seguridad en las tareas o aplicaciones que se ejecutan en las cargas de trabajo e instancias del contenedor, GuardDuty genera uno o más tipos de hallazgos de Runtime Monitoring.

[1] También puedes configurar un Amazon EventBridge (EventBridge) para que reciba una notificación cuando el estado de la cobertura cambie de Insalubre a Saludable o de otra manera.

Para obtener más información, consulte Evaluar la cobertura del tiempo de ejecución de sus recursos.

GuardDuty detecta posibles amenazas

A medida que GuardDuty comienza a recibir los eventos de tiempo de ejecución de su recurso, comienza a analizarlos. Cuando GuardDuty detecta una posible amenaza de seguridad en cualquiera de sus instancias de Amazon EC2, clústeres de Amazon ECS o clústeres de Amazon EKS, genera una o más. Tipos de búsqueda de Runtime Monitoring Puede acceder a los detalles de la búsqueda para ver los detalles de los recursos afectados.

¿Cómo funciona la prueba gratuita de 30 días en Runtime Monitoring

El período de prueba gratuito de 30 días funciona de forma diferente para las GuardDuty cuentas nuevas y las cuentas existentes que ya tenían habilitado EKS Runtime Monitoring antes de que la capacidad de Runtime Monitoring se extendiera a las instancias de Amazon EC2 y AWS Fargate (solo Amazon ECS).

Estoy utilizando el período de GuardDuty prueba o nunca he activado EKS Runtime Monitoring

La siguiente lista explica cómo funciona el período de prueba gratuito de 30 días si está utilizando el período de prueba de GuardDuty 30 días o si nunca ha activado EKS Runtime Monitoring:

- Cuando lo active GuardDuty por primera vez, Runtime Monitoring y EKS Runtime Monitoring no estarán habilitados de forma predeterminada.

  Al habilitar Runtime Monitoring para su cuenta u organización, asegúrese de configurar también el agente de GuardDuty seguridad del recurso que quiere monitorear para detectar amenazas. Por ejemplo, si desea utilizar Runtime Monitoring para sus instancias de Amazon EC2, después de habilitar Runtime Monitoring, también debe configurar el agente de seguridad para Amazon EC2. Puede elegir hacerlo de forma manual o automática de forma automática mediante. GuardDuty
- El plan de protección de Runtime Monitoring está activado a nivel de cuenta. El período de prueba gratuito de 30 días funciona a nivel de recursos. Una vez desplegado el agente de GuardDuty seguridad en un tipo de recurso específico, la prueba gratuita de 30 días comienza cuando se GuardDuty produce el primer evento de tiempo de ejecución asociado a este tipo de recurso. Por ejemplo, ha implementado el GuardDuty agente a nivel de recursos (para la instancia de Amazon EC2, el clúster de Amazon ECS y el clúster de Amazon EKS). Cuando GuardDuty reciba el primer evento de tiempo de ejecución de una instancia de Amazon EC2, la prueba gratuita de 30 días solo comenzará para Amazon EC2.
- Cuando desee habilitar únicamente la monitorización de tiempo de ejecución de EKS: cuando la active GuardDuty por primera vez, la supervisión de tiempo de ejecución de EKS no estará habilitada de forma predeterminada (después del lanzamiento de la supervisión de tiempo de ejecución). Deberá activar EKS Runtime Monitoring. Para utilizarlo de forma óptima, asegúrese de gestionar el agente de GuardDuty seguridad manualmente o de habilitar la configuración automática del agente para que GuardDuty gestione el agente en su nombre. El período de prueba

gratuito de 30 días de EKS Runtime Monitoring comienza cuando GuardDuty recibe su primer evento de tiempo de ejecución para el recurso Amazon EKS.

Habilité EKS Runtime Monitoring antes del lanzamiento de Runtime Monitoring

- En el caso de una GuardDuty cuenta existente que tenga activado el plan de protección de EKS Runtime Monitoring y utilice la experiencia de GuardDuty consola para utilizar este plan de protección, con el anuncio de Runtime Monitoring, la experiencia de consola de EKS Runtime Monitoring se ha consolidado en Runtime Monitoring. La configuración actual de EKS Runtime Monitoring sigue siendo la misma. Puede seguir utilizando el soporte de API/CLI para realizar las operaciones asociadas con EKS Runtime Monitoring.
- Para utilizar EKS Runtime Monitoring como parte de Runtime Monitoring, necesitará configurar Runtime Monitoring para su cuenta u organización. Para mantener la misma configuración para Runtime Monitoring, consulteMigración de EKS Runtime Monitoring a Runtime Monitoring. Sin embargo, esto no afectará a la prueba gratuita de 30 días del recurso Amazon EKS.
- El plan de protección Runtime Monitoring está activado a nivel de cuenta. Después de implementar el agente de GuardDuty seguridad en uno de los tipos de recursos especificados (instancia de Amazon EC2 y clúster de Amazon ECS), la prueba gratuita de 30 días comienza cuando se GuardDuty recibe el primer evento de tiempo de ejecución asociado al recurso. Hay una prueba gratuita de 30 días asociada a cada tipo de recurso.

  Por ejemplo, después de habilitar Runtime Monitoring, si decide implementar el GuardDuty agente solo en una instancia de Amazon EC2, la prueba gratuita de 30 días de este recurso solo se iniciará cuando GuardDuty reciba su primer evento de tiempo de ejecución para una instancia de Amazon EC2. Más adelante, cuando implemente el GuardDuty agente para Fargate (solo Amazon ECS), la prueba gratuita de 30 días de este recurso solo comenzará cuando GuardDuty reciba su primer evento de tiempo de ejecución para el clúster de Amazon ECS. Teniendo en cuenta que ya tiene activado EKS Runtime Monitoring en su cuenta, GuardDuty no restablece la prueba gratuita de 30 días de un recurso de Amazon EKS.

Requisitos previos para habilitar Runtime Monitoring

Para habilitar la supervisión en tiempo de ejecución y administrar el agente de GuardDuty seguridad, debe cumplir los requisitos previos de cada tipo de recurso que desee supervisar para detectar amenazas.

Contenido

Requisitos previos para la compatibilidad con instancias Amazon EC2

Requisito previo general

Las instancias de Amazon EC2 para las que desee GuardDuty supervisar los eventos de tiempo de ejecución deben estar gestionadas por SSM. Esto es independiente de si utiliza GuardDuty para administrar el agente de seguridad automáticamente o si lo administra manualmente (excepto Método 2: mediante scripts de instalación de RPM).

Para gestionar sus instancias de Amazon EC2 AWS Systems Manager, consulte Configuración de Systems Manager para instancias de Amazon EC2 en AWS Systems Manager la Guía del usuario.

Validación de los requisitos de arquitectura

La arquitectura de la distribución del sistema operativo puede afectar al comportamiento del agente GuardDuty de seguridad. Debe cumplir los siguientes requisitos antes de utilizar Runtime Monitoring para instancias de Amazon EC2:

- En la actualidad, la compatibilidad con Runtime Monitoring para Amazon EC2 solo está disponible para las versiones de Linux. Aunque el soporte para Ubuntu no está disponible en estos momentos, lo estará en un futuro próximo. Para recibir notificaciones sobre las actualizaciones de esta página, suscríbase a la fuente RSS.

  En la siguiente tabla se muestra la distribución del sistema operativo que se ha verificado para admitir el agente GuardDuty de seguridad para las instancias de Amazon EC2.

Distribución del sistema operativo	Versión del kernel	Compatibilidad del kernel	Arquitectura de la CPU	
			x64 (AMD64)	Graviton (ARM64)
AL2 y AL2023	5.4, 5.10, 5.15, 6.1	eBPF, Tracepoints, Kprobe	Soportado	Soportado

- Requisitos adicionales: solo si tiene Amazon ECS/Amazon EC2

  Para Amazon ECS/Amazon EC2, le recomendamos que utilice las últimas AMI optimizadas para Amazon ECS (con fecha del 29 de septiembre de 2023 o posterior) o que utilice la versión 1.77.0 del agente de Amazon ECS.

Cuando utilice la configuración de agentes automatizada

Para Utilice una configuración de agentes automatizada (recomendado) ello, Cuenta de AWS debe cumplir los siguientes requisitos previos:

- Cuando utilices etiquetas de inclusión con una configuración de agente automatizada, GuardDuty para crear una asociación de SSM para una nueva instancia, asegúrate de que la nueva instancia esté gestionada por SSM y aparezca en Fleet Manager en la consola https://console.aws.amazon.com/systems-manager/.
- Cuando utilice etiquetas de exclusión con una configuración de agente automatizada:
  - Añada la `false` etiqueta`GuardDutyManaged`: antes de configurar el agente GuardDuty automatizado para su cuenta.

    Asegúrese de añadir la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Al habilitar la configuración automática de agentes para Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión se incluirá en la configuración de agentes GuardDuty automatizada.
  - Para que las etiquetas de exclusión funcionen, actualice la configuración de la instancia para que el documento de identidad de la instancia esté disponible en el servicio de metadatos de la instancia (IMDS). El procedimiento para realizar este paso ya forma parte Habilitación de la supervisión del tiempo de tu cuenta.

Límite de CPU y memoria para el GuardDuty agente

Límite de CPU

El límite máximo de CPU para el agente de GuardDuty seguridad asociado a las instancias de Amazon EC2 es del 10 por ciento del total de núcleos de vCPU. Por ejemplo, si la instancia EC2 tiene 4 núcleos de vCPU, el agente de seguridad puede utilizar un máximo del 40 por ciento del 400 por ciento total disponible.

Memory limit (Límite de memoria)

De la memoria asociada a la instancia de Amazon EC2, hay una memoria limitada que el agente de GuardDuty seguridad puede utilizar.

En la siguiente tabla se muestra el límite de memoria.

Memoria de la instancia de Amazon EC2	Memoria máxima para el agente GuardDuty
Menos de 8 GB	128 MB
Menos de 32 GB	256 MB
Más o igual a 32 GB	1 GB

Siguiente paso

El siguiente paso es configurar Runtime Monitoring y también administrar el agente de seguridad (automática o manualmente). Para obtener más información, consulte Habilitación de la supervisión del tiempo.

Requisitos previos para la compatibilidad AWS Fargate (solo con Amazon ECS)

Validación de los requisitos de arquitectura

La plataforma que utilice puede afectar a la forma GuardDuty en que el agente GuardDuty de seguridad admite la recepción de los eventos de tiempo de ejecución de sus clústeres de Amazon ECS. Debe validar que esté utilizando una de las plataformas verificadas.

Consideraciones iniciales:

La AWS Fargate (Fargate) plataforma de los clústeres de Amazon ECS debe ser Linux. La versión de plataforma correspondiente debe ser como mínimo`1.4.0`, o`LATEST`. Para obtener más información sobre las versiones de la plataforma, consulte las versiones de la plataforma Linux en la Guía para desarrolladores de Amazon Elastic Container Service.

Las versiones de la plataforma Windows aún no son compatibles.

Plataformas verificadas

La distribución del sistema operativo y la arquitectura de la CPU afectan al soporte que proporciona el agente GuardDuty de seguridad. En la siguiente tabla se muestra la configuración verificada para implementar el agente GuardDuty de seguridad y configurar Runtime Monitoring.

Distribución del sistema operativo	Compatibilidad del kernel	Arquitectura de la CPU	
		x64 (AMD64)	Graviton (ARM64)
Linux	eBPF, Tracepoints, Kprobe	Supported	Supported

Proporcione los permisos de ECR y los detalles de la subred

Antes de habilitar Runtime Monitoring, debe proporcionar los siguientes detalles:

Proporcione una función de ejecución de tareas con permisos

La función de ejecución de tareas requiere que disponga de determinados permisos de Amazon Elastic Container Registry (Amazon ECR). Puede utilizar la política TaskExecutionRolePolicy gestionada por AmazonECS o añadir los siguientes permisos a su `TaskExecutionRole` política:

```
...
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
```

```
...
```

Para restringir aún más los permisos de Amazon ECR, puede añadir el URI del repositorio de Amazon ECR que aloja el agente de GuardDuty seguridad para (solo AWS Fargate Amazon ECS). Para obtener más información, consulte Repositorio para GuardDuty agentes en AWS Fargate (solo Amazon ECS).

Proporcione los detalles de la subred en la definición de la tarea

Puede proporcionar las subredes públicas como entrada en la definición de la tarea o crear un punto de enlace de VPC de Amazon ECR.

- Uso de la opción de definición de tareas: para ejecutar las UpdateServiceAPI CreateServicey en la referencia de API de Amazon Elastic Container Service, es necesario pasar la información de la subred. Para obtener más información, consulte las definiciones de tareas de Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.
- Uso de la opción de punto de conexión de VPC de Amazon ECR: proporcione una ruta de red a Amazon ECR; asegúrese de que el URI del repositorio de Amazon ECR que aloja el agente de seguridad sea accesible desde GuardDuty la red. Si sus tareas de Fargate se ejecutarán en una subred privada, Fargate necesitará la ruta de red para descargar el contenedor. GuardDuty

  Para obtener información sobre cómo habilitar Fargate para descargar el GuardDuty contenedor, consulte Uso de Amazon ECR con Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.

Límites de CPU y memoria

En la definición de tarea de Fargate, debe especificar el valor de la CPU y la memoria a nivel de la tarea. La siguiente tabla muestra las combinaciones válidas de valores de CPU y memoria a nivel de tarea y el límite máximo de memoria del agente de GuardDuty seguridad correspondiente para el contenedor. GuardDuty

Valor de CPU	Valor de memoria	GuardDuty límite máximo de memoria del agente
256 (0,25 vCPU)	512 MiB, 1 GB, 2 GB	128 MB
512 (0,5 vCPU)	1 GB, 2 GB, 3 GB, 4 GB	

Valor de CPU	Valor de memoria	GuardDuty límite máximo de memoria del agente
1024 (1 vCPU)	2 GB, 3 GB, 4 GB	
	5 GB, 6 GB, 7 GB, 8 GB	
2048 (2 vCPU)	Entre 4 GB y 16 GB en incrementos de 1 GB	
4096 (4 vCPU)	Entre 8 GB y 20 GB en incrementos de 1 GB	
8192 (8 vCPU)	Entre 16 GB y 28 GB en incrementos de 4 GB	256 MB
	Entre 32 GB y 60 GB en incrementos de 4 GB	512 MB
16384 (16 vCPU)	Entre 32 GB y 120 GB en incrementos de 8 GB	1 GB

Una vez que hayas activado Runtime Monitoring y hayas comprobado que el estado de cobertura del clúster es correcto, puedes configurar y ver las métricas de Container Insight. Para obtener más información, Configuración de la supervisión en el clúster de Amazon ECS.

El siguiente paso es configurar Runtime Monitoring y también administrar el agente de seguridad. Para obtener más información, consulte Habilitación de la supervisión del tiempo.

Requisitos previos para la compatibilidad con clústeres de Amazon EKS

Validación de los requisitos de arquitectura

La plataforma que utilice puede afectar a la forma GuardDuty en que el agente GuardDuty de seguridad admite la recepción de los eventos de tiempo de ejecución de sus clústeres de EKS. Debe validar que esté utilizando una de las plataformas verificadas. Si administra el GuardDuty agente manualmente, asegúrese de que la versión de Kubernetes sea compatible con la versión del GuardDuty agente que está en uso actualmente.

Plataformas verificadas

La distribución del sistema operativo, la versión del núcleo y la arquitectura de la CPU afectan al soporte que proporciona el agente de seguridad. GuardDuty La siguiente tabla muestra la configuración verificada para implementar el agente de GuardDuty seguridad y configurar EKS Runtime Monitoring.

Distribución del sistema operativo	Versión del kernel	Compatibilidad del kernel	Arquitectura de la CPU		Versión de Kubernetes compatible
			x64 (AMD64)	Graviton (ARM64) (Graviton2 y superiores) 1	
Ubuntu AL2	5.4, 5.10, 5.15, 6.1	Puntos de rastreo eBPF, sonda K	Soportado	Soportado	v1.21 - v1.29
Bottlerocket					v1.23 - v1.29

1. Runtime Monitoring para los clústeres de Amazon EKS no admite la instancia de Graviton de primera generación, como los tipos de instancia A1.

Versiones de Kubernetes compatibles con el agente de seguridad GuardDuty

En la siguiente tabla se muestran las versiones de Kubernetes para los clústeres de EKS compatibles con el agente de seguridad. GuardDuty

Versión de Kubernetes	Versión del agente de GuardDuty seguridad complementario Amazon EKS							
	v1.5.0	v1.4.1	v1.4.0	v1.3.1	v1.3.0	v1.2.0	v1.1.0	v1.0.0
1.29	Soportado	Soportado	Soportado	No admitido	No admitido	No admitido	No admitido	No admitido

1.28	Soportado	Soportado		
1.27			Compatible	
1.26				Compatible
1,25				Compatible
1,24				
1.23				
1.22				
1.21				

Algunas de las versiones del agente de GuardDuty seguridad llegarán al final del soporte estándar. Para obtener información sobre las versiones de lanzamiento del agente, consulteGuardDuty agente de seguridad para clústeres de Amazon EKS.

Límites de CPU y memoria

En la siguiente tabla se muestran los límites de CPU y memoria del complemento Amazon EKS para GuardDuty (`aws-guardduty-agent`).

Parámetro	Límite mínimo	Límite máximo
CPU	200m	1000m
Memoria	256 Mi	1024 Mi

Cuando utiliza la versión 1.5.0 o superior del complemento Amazon EKS, GuardDuty ofrece la posibilidad de configurar el esquema del complemento para los valores de CPU y memoria. Para obtener información sobre el rango configurable, consulteParámetros y valores configurables.

Después de habilitar la supervisión en tiempo de ejecución de EKS y evaluar el estado de la cobertura de sus clústeres de EKS, podrá configurar y ver las métricas de información de los contenedores. Para obtener más información, consulte Configuración de la supervisión de la CPU y la memoria.

Conceptos clave: enfoques para gestionar los agentes GuardDuty de seguridad

Tenga en cuenta los conceptos clave que le ayudarán a administrar el agente de seguridad en sus clústeres de Amazon EKS y Amazon ECS.

Contenido

Recurso de Fargate (solo Amazon ECS): enfoques para administrar GuardDuty un agente de seguridad

Runtime Monitoring le ofrece la opción de detectar posibles amenazas de seguridad en todos los clústeres de Amazon ECS (nivel de cuenta) o en clústeres selectivos (nivel de clúster) de su cuenta. Al habilitar la configuración automática de agentes para cada tarea de Amazon ECS Fargate que se vaya a ejecutar, GuardDuty añadirá un contenedor sidecar para cada carga de trabajo de contenedores incluida en esa tarea. El agente GuardDuty de seguridad se despliega en este contenedor de sidecar. Así es como GuardDuty obtiene visibilidad del comportamiento en tiempo de ejecución de los contenedores dentro de las tareas de Amazon ECS.

Actualmente, Runtime Monitoring admite la administración del agente de seguridad para sus clústeres de Amazon ECS (AWS Fargate) únicamente a través de GuardDuty. No se admite la administración manual del agente de seguridad en los clústeres de Amazon ECS.

Antes de configurar sus cuentas, evalúe cómo quiere administrar el agente de GuardDuty seguridad y, si es posible, supervise el comportamiento en tiempo de ejecución de los contenedores que pertenecen a las tareas de Amazon ECS. Tenga en cuenta los siguientes enfoques.

Temas

Gestione el agente GuardDuty de seguridad para todos los clústeres de Amazon ECS

Este enfoque le ayudará a detectar posibles amenazas de seguridad a nivel de cuenta. Utilice este enfoque cuando desee GuardDuty detectar posibles amenazas de seguridad para todos los clústeres de Amazon ECS que pertenecen a su cuenta.

Administre el agente de GuardDuty seguridad para la mayoría de los clústeres de Amazon ECS, pero excluya algunos de los clústeres de Amazon ECS

Utilice este enfoque cuando desee GuardDuty detectar posibles amenazas de seguridad para la mayoría de los clústeres de Amazon ECS de su AWS entorno, pero excluya algunos de ellos. Este enfoque le ayuda a supervisar el comportamiento en tiempo de ejecución de los contenedores dentro de sus tareas de Amazon ECS a nivel de clúster. Por ejemplo, el número de clústeres de Amazon ECS que pertenecen a su cuenta es 1000. Sin embargo, solo desea monitorizar 930 clústeres de Amazon ECS.

Este enfoque requiere que añada una GuardDuty etiqueta predefinida a los clústeres de Amazon ECS que no desee supervisar. Para obtener más información, consulte Gestión del agente de seguridad automatizado para Fargate (solo Amazon ECS).

Administre el agente GuardDuty de seguridad para clústeres selectivos de Amazon ECS

Utilice este enfoque cuando desee GuardDuty detectar posibles amenazas de seguridad para algunos de los clústeres de Amazon ECS. Este enfoque le ayuda a supervisar el comportamiento en tiempo de ejecución de los contenedores dentro de sus tareas de Amazon ECS a nivel de clúster. Por ejemplo, el número de clústeres de Amazon ECS que pertenecen a su cuenta es 1000. Sin embargo, solo desea monitorizar 230 clústeres.

Este enfoque requiere que añada una GuardDuty etiqueta predefinida a los clústeres de Amazon ECS que desee supervisar. Para obtener más información, consulte Gestión del agente de seguridad automatizado para Fargate (solo Amazon ECS).

Clústeres de Amazon EKS: enfoques para administrar los agentes GuardDuty de seguridad

GuardDuty Para consumir los eventos de tiempo de ejecución de sus clústeres de EKS a nivel de cuenta o de clúster, es necesario administrar el agente de GuardDuty seguridad de los clústeres correspondientes.

Enfoques para administrar los agentes GuardDuty de seguridad

Antes del 13 de septiembre de 2023, podía configurarlo GuardDuty para administrar el agente de seguridad a nivel de cuenta. Este comportamiento indicaba que, de forma predeterminada, GuardDuty administrará el agente de seguridad en todos los clústeres de EKS que pertenezcan a un Cuenta de AWS. Ahora, GuardDuty proporciona una capacidad granular que le ayuda a elegir los clústeres de EKS en los que GuardDuty desea administrar el agente de seguridad.

Si decide Administre el agente GuardDuty de seguridad manualmente, puede seguir seleccionando los clústeres de EKS que desee supervisar. Sin embargo, para administrar el agente de forma manual, es un requisito previo crear un punto de conexión de VPC de Amazon para la Cuenta de AWS .

> **Note**
>
> Independientemente del enfoque que utilice para administrar el agente de GuardDuty seguridad, EKS Runtime Monitoring siempre está activado a nivel de cuenta.

Temas

- Administre el agente de seguridad mediante GuardDuty
- Administre el agente GuardDuty de seguridad manualmente

Administre el agente de seguridad mediante GuardDuty

GuardDuty despliega y administra el agente de seguridad en su nombre. En cualquier momento, puede supervisar los clústeres de EKS de su cuenta con uno de los siguientes enfoques.

Temas

- Supervisión de todos los clústeres de EKS
- Supervisión de todos los clústeres de EKS y exclusión de determinados clústeres de EKS
- Supervisión de determinados clústeres de EKS

Supervisión de todos los clústeres de EKS

- Cuándo utilizar este enfoque: utilícelo cuando desee GuardDuty implementar y administrar el agente de seguridad para todos los clústeres de EKS de su cuenta. De forma predeterminada,

también GuardDuty implementará el agente de seguridad en un clúster de EKS potencialmente nuevo creado en su cuenta.

- Impacto del uso de este enfoque:
  - GuardDuty crea un punto final de Amazon Virtual Private Cloud (Amazon VPC) a través del cual el agente de GuardDuty seguridad envía los eventos de tiempo de ejecución. GuardDuty La creación del punto de conexión de Amazon VPC no conlleva ningún coste adicional si se gestiona el agente de seguridad a través de él. GuardDuty
  - Es necesario que el nodo de trabajo tenga una ruta de red válida a un punto final de `guardduty-data` VPC activo. GuardDuty despliega el agente de seguridad en sus clústeres de EKS. Amazon Elastic Kubernetes Service (Amazon EKS) coordinará la implementación del agente de seguridad en los nodos de los clústeres de EKS.
  - En función de la disponibilidad de IP, GuardDuty selecciona la subred para crear un punto final de VPC. Si utiliza topologías de red avanzadas, debe validar que la conectividad sea posible.
- Consideración: Actualmente, cuando se utiliza esta opción, la supervisión en tiempo de ejecución de EKS no crea una VPC compartida.

Supervisión de todos los clústeres de EKS y exclusión de determinados clústeres de EKS

- Cuándo usar este enfoque: utilícelo cuando desee administrar el agente de seguridad GuardDuty para todos los clústeres de EKS de su cuenta, pero excluya algunos clústeres de EKS. Este método utiliza un enfoque basado en etiquetas[1] en el que puede etiquetar los clústeres de EKS para los que no desea recibir los eventos de tiempo de ejecución. La etiqueta predefinida debe tener `GuardDutyManaged-false` como par de clave-valor.
- Impacto del uso de este enfoque:
  - Este enfoque requiere que habilite la administración automática de los GuardDuty agentes solo después de agregar etiquetas a los clústeres de EKS que desee excluir de la supervisión.

    Por lo tanto, el impacto que se produce al Administre el agente de seguridad mediante GuardDuty también se aplica este enfoque. Cuando añada etiquetas antes de habilitar la administración automática del GuardDuty agente, no GuardDuty implementará ni administrará el agente de seguridad para los clústeres de EKS que están excluidos de la supervisión.
- Consideraciones:
  - Debe añadir el par clave-valor de la siguiente maneraGuardDutyManaged: `false` para los clústeres de EKS selectivos antes de activar la configuración automática de agentes; de lo

contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS hasta que utilice la etiqueta.

- Debe impedir que se modifiquen las etiquetas, excepto por parte de identidades de confianza.

> **Important**
>
> Administre los permisos para modificar el valor de la etiqueta `GuardDutyManaged` de su clúster de EKS mediante políticas de control de servicios o políticas de IAM. Para obtener más información, consulte Políticas de control de servicios (SCP) en la Guía del AWS Organizations usuario o Control del acceso a AWS los recursos en la Guía del usuario de IAM.

- En el caso de un clúster de EKS potencialmente nuevo que no desee supervisar, asegúrese de agregar el par de clave-valor `GuardDutyManaged-false` al crear este clúster de EKS.
- Este enfoque también tendrá las mismas consideraciones que las especificadas para Supervisión de todos los clústeres de EKS.

Supervisión de determinados clústeres de EKS

- Cuándo usar este enfoque: utilícelo cuando desee GuardDuty implementar y administrar las actualizaciones del agente de seguridad solo para algunos clústeres de EKS de su cuenta. Este método utiliza un enfoque basado en etiquetas[1] en el que puede etiquetar el clúster de EKS para el que desea recibir los eventos de tiempo de ejecución.
- Impacto del uso de este enfoque:
  - Al usar etiquetas de inclusión, GuardDuty implementará y administrará automáticamente el agente de seguridad solo para los clústeres de EKS selectivos que estén etiquetados `GuardDutyManaged true` como par clave-valor.
  - El uso de este enfoque también tendrá el mismo impacto que el especificado para Supervisión de todos los clústeres de EKS.
- Consideraciones:
  - Si el valor de la etiqueta `GuardDutyManaged` no está establecido en `true`, la etiqueta de inclusión no funcionará como se esperaba y esto podría afectar a la supervisión del clúster de EKS.
  - Para asegurarse de que se estén supervisando determinados clústeres de EKS, debe evitar que las etiquetas se modifiquen, salvo por parte de identidades de confianza.

> **Important**
>
> Administre los permisos para modificar el valor de la etiqueta `GuardDutyManaged` de su clúster de EKS mediante políticas de control de servicios o políticas de IAM. Para obtener más información, consulte Políticas de control de servicios (SCP) en la Guía del AWS Organizations usuario o Control del acceso a AWS los recursos en la Guía del usuario de IAM.

- En el caso de un clúster de EKS potencialmente nuevo que no desee supervisar, asegúrese de agregar el par de clave-valor `GuardDutyManaged-false` al crear este clúster de EKS.
- Este enfoque también tendrá las mismas consideraciones que las especificadas para Supervisión de todos los clústeres de EKS.

[1] Para obtener más información sobre el etiquetado de determinados clústeres de EKS, consulte Etiquetado de los recursos de Amazon EKS en la Guía del usuario de Amazon EKS.

Administre el agente GuardDuty de seguridad manualmente

- Cuándo utilizar este enfoque: utilice este enfoque cuando desee implementar y administrar el agente de GuardDuty seguridad en todos los clústeres de EKS de forma manual. Asegúrese de que la supervisión en tiempo de ejecución de EKS esté habilitada en sus cuentas. Es posible que el agente de GuardDuty seguridad no funcione según lo esperado si no habilita EKS Runtime Monitoring.
- Impacto del uso de este enfoque: tendrá que coordinar la implementación del software del agente de GuardDuty seguridad en sus clústeres de EKS en todas las cuentas y Regiones de AWS donde esté disponible esta función.
- Consideraciones: Debe respaldar un flujo de datos seguro y, al mismo tiempo, supervisar y abordar las brechas de cobertura a medida que se implementan continuamente nuevos clústeres y nuevas cargas de trabajo.

Habilitación GuardDuty de la supervisión del tiempo

Antes de habilitar la supervisión del tiempo de ejecución en su cuenta, asegúrese de que el tipo de recurso para el que desea supervisar los eventos de tiempo de ejecución cumpla con los requisitos de la plataforma. Para obtener más información, consulte Requisitos previos.

Si utilizaba EKS Runtime Monitoring antes del lanzamiento de Runtime Monitoring, puede usar las API para comprobar y actualizar la configuración existente de EKS Runtime Monitoring. También puede migrar su configuración actual de EKS Runtime Monitoring a Runtime Monitoring. Para obtener más información, consulte Migración de EKS Runtime Monitoring a Runtime Monitoring.

> **Note**
>
> Actualmente, esta documentación proporciona los pasos para habilitar la monitorización del tiempo de ejecución para sus cuentas y su organización únicamente mediante consola. También puede habilitar la supervisión del tiempo de ejecución mediante API Actions o AWS CLI para GuardDuty.

Puede configurar la supervisión del tiempo de ejecución siguiendo los pasos de los siguientes temas.

Contenido

Habilitar la supervisión del tiempo de ejecución para una cuenta independiente

Console

1. Inicie sesión AWS Management Console y abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, selecciona Runtime Monitoring.
3. En la pestaña Configuración, seleccione Activar para activar la supervisión del tiempo de ejecución en su cuenta.
4. GuardDuty Para recibir los eventos de tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS), utilice las siguientes opciones para administrar el agente de seguridad de estos recursos:

   Para habilitar el agente GuardDuty de seguridad

   - Administración del agente de seguridad automatizado para la instancia de Amazon EC2

- Administración manual del agente de seguridad para la instancia de Amazon EC2
- Gestión del agente de seguridad automatizado para Fargate (solo Amazon ECS)
- Administración automática del agente de seguridad para los clústeres de Amazon EKS
- Administración manual del agente de seguridad para el clúster Amazon EKS

Para entornos con varias cuentas

En entornos con varias cuentas, solo la cuenta de GuardDuty administrador delegado puede habilitar o deshabilitar Runtime Monitoring para las cuentas de los miembros y administrar la configuración automatizada de los agentes para los tipos de recursos que pertenecen a las cuentas de los miembros de su organización. Las cuentas de GuardDuty los miembros no pueden modificar esta configuración desde sus cuentas. La cuenta de GuardDuty administrador delegado administra sus cuentas de miembros mediante AWS Organizations. Para más información sobre los entornos con varias cuentas, consulte Managing multiple accounts.

Para la cuenta de administrador delegado GuardDuty

Para habilitar Runtime Monitoring para la cuenta de administrador delegado GuardDuty

1. Inicie sesión AWS Management Console y abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, selecciona Runtime Monitoring.
3. En la pestaña Configuración, elija Editar en la sección de configuración de Runtime Monitoring.
4. Uso de Habilitar para todas las cuentas

   Si desea habilitar la supervisión en tiempo de ejecución para todas las cuentas que pertenecen a la organización, incluida la cuenta de GuardDuty administrador delegado, seleccione Habilitar para todas las cuentas.
5. Uso de Configurar cuentas manualmente

   Si desea activar Runtime Monitoring para cada cuenta de miembro de forma individual, elija Configurar las cuentas manualmente.

   - Seleccione Habilitar en la sección Administrador delegado (esta cuenta).
6. GuardDuty Para recibir los eventos de tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS), utilice las siguientes opciones para administrar el agente de seguridad de estos recursos:

Para habilitar el agente GuardDuty de seguridad

- Administración del agente de seguridad automatizado para la instancia de Amazon EC2
- Administración manual del agente de seguridad para la instancia de Amazon EC2
- Gestión del agente de seguridad automatizado para Fargate (solo Amazon ECS)
- Administración automática del agente de seguridad para los clústeres de Amazon EKS
- Administración manual del agente de seguridad para el clúster Amazon EKS

Para todas las cuentas de los miembros

Para habilitar Runtime Monitoring para todas las cuentas de los miembros de la organización

1. Inicie sesión en la GuardDuty consola AWS Management Console y ábrala en https://console.aws.amazon.com/guardduty/.

   Inicie sesión con la cuenta de GuardDuty administrador delegado.
2. En el panel de navegación, elija Runtime Monitoring.
3. En la página de supervisión del tiempo de ejecución, en la pestaña Configuración, seleccione Editar en la sección de configuración de la supervisión del tiempo de ejecución.
4. Elija Habilitar para todas las cuentas.
5. GuardDuty Para recibir los eventos de tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS), utilice las siguientes opciones para administrar el agente de seguridad de estos recursos:

   Para habilitar el agente GuardDuty de seguridad

   - Administración del agente de seguridad automatizado para la instancia de Amazon EC2
   - Administración manual del agente de seguridad para la instancia de Amazon EC2
   - Gestión del agente de seguridad automatizado para Fargate (solo Amazon ECS)
   - Administración automática del agente de seguridad para los clústeres de Amazon EKS
   - Administración manual del agente de seguridad para el clúster Amazon EKS

Para todas las cuentas de miembros activas existentes

Para habilitar Runtime Monitoring para las cuentas de miembros existentes en la organización

1. Inicie sesión AWS Management Console y abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Inicie sesión con la cuenta de GuardDuty administrador delegado de la organización.
2. En el panel de navegación, elija Runtime Monitoring.
3. En la página de supervisión del tiempo de ejecución, en la pestaña Configuración, puede ver el estado actual de la configuración de la supervisión del tiempo de ejecución.
4. En el panel Runtime Monitoring, en la sección Cuentas de miembros activos, selecciona Acciones.
5. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
6. Seleccione Confirmar.
7. GuardDuty Para recibir los eventos de tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS), utilice las siguientes opciones para administrar el agente de seguridad de estos recursos:

   Para habilitar el agente GuardDuty de seguridad

   - Administración del agente de seguridad automatizado para la instancia de Amazon EC2
   - Administración manual del agente de seguridad para la instancia de Amazon EC2
   - Gestión del agente de seguridad automatizado para Fargate (solo Amazon ECS)
   - Administración automática del agente de seguridad para los clústeres de Amazon EKS
   - Administración manual del agente de seguridad para el clúster Amazon EKS

> **Note**
>
> La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Habilite automáticamente la supervisión del tiempo de ejecución solo para las cuentas de los nuevos miembros

Para habilitar Runtime Monitoring para las nuevas cuentas de miembros de su organización

1. Inicie sesión en la GuardDuty consola AWS Management Console y ábrala en https://console.aws.amazon.com/guardduty/.

   Inicie sesión con la cuenta de GuardDuty administrador delegado designada de la organización.
2. En el panel de navegación, elija Runtime Monitoring
3. En la pestaña Configuración, elija Editar en la sección de configuración de Runtime Monitoring.
4. Elija Configurar cuentas manualmente.
5. Elija Habilitar automáticamente las cuentas de miembros nuevas.
6. GuardDuty Para recibir los eventos de tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS), utilice las siguientes opciones para administrar el agente de seguridad de estos recursos:

   Para habilitar el agente GuardDuty de seguridad

   - Administración del agente de seguridad automatizado para la instancia de Amazon EC2
   - Administración manual del agente de seguridad para la instancia de Amazon EC2
   - Gestión del agente de seguridad automatizado para Fargate (solo Amazon ECS)
   - Administración automática del agente de seguridad para los clústeres de Amazon EKS
   - Administración manual del agente de seguridad para el clúster Amazon EKS

Solo para cuentas de miembros activos selectivos

Para habilitar Runtime Monitoring para las cuentas individuales de los miembros activos

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Inicie sesión con las credenciales de la cuenta GuardDuty de administrador delegado.
2. En el panel de navegación, elija Accounts (Cuentas).
3. En la página Cuentas, revise los valores de las columnas Runtime Monitoring y Administrar el agente automáticamente. Estos valores indican si la supervisión del tiempo de ejecución y la administración de GuardDuty agentes están habilitadas o no para la cuenta correspondiente.

4. En la tabla Cuentas, seleccione la cuenta para la que desee habilitar Runtime Monitoring. Puede elegir varias cuentas a la vez.
5. Seleccione Confirmar.
6. Seleccione Editar planes de protección. Elija la acción apropiada.
7. Seleccione Confirmar.
8. GuardDuty Para recibir los eventos de tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS), utilice las siguientes opciones para administrar el agente de seguridad de estos recursos:

   Para habilitar el agente GuardDuty de seguridad

   - Administración del agente de seguridad automatizado para la instancia de Amazon EC2
   - Administración manual del agente de seguridad para la instancia de Amazon EC2
   - Gestión del agente de seguridad automatizado para Fargate (solo Amazon ECS)
   - Administración automática del agente de seguridad para los clústeres de Amazon EKS
   - Administración manual del agente de seguridad para el clúster Amazon EKS

Administrar agentes GuardDuty de seguridad

Puede administrar el agente de GuardDuty seguridad del recurso que desee supervisar. Si desea supervisar más de un tipo de recurso, asegúrese de administrar el GuardDuty agente de ese recurso.

> **Important**
>
> Al trabajar con un agente de GuardDuty seguridad para una instancia de Amazon EC2, puede instalar y usar el agente en el host subyacente dentro de un clúster de Amazon EKS. Si ya hubiera implementado un agente de seguridad en ese clúster de EKS, el mismo host podría tener dos agentes de seguridad ejecutándose al mismo tiempo. Para obtener información sobre cómo GuardDuty funciona en este escenario, consulteManejo de agentes de seguridad duales.

Los siguientes temas le ayudarán con los siguientes pasos para administrar el agente de seguridad.

Contenido

- Uso de una VPC compartida con agentes de seguridad automatizados

- Gestión de los agentes de seguridad duales instalados en un host
- Administración del agente de seguridad automatizado para la instancia de Amazon EC2
- Administración manual del agente de seguridad para la instancia de Amazon EC2
- Gestión del agente de seguridad automatizado para Fargate (solo Amazon ECS)
- Administración automática del agente de seguridad para los clústeres de Amazon EKS
- Administración manual del agente de seguridad para el clúster Amazon EKS

Uso de una VPC compartida con agentes de seguridad automatizados

Si GuardDuty decide administrar el agente de seguridad automáticamente, Runtime Monitoring admite el uso de una VPC compartida para las Cuentas de AWS que pertenecen a la misma organización. AWS Organizations En su nombre, GuardDuty puede configurar la política de puntos de conexión de Amazon VPC en función de los detalles asociados a la VPC compartida de su organización.

Antes de esta versión, solo se GuardDuty permitía el uso de VPC compartidas cuando se optaba por gestionar el agente de GuardDuty seguridad de forma manual.

Contenido

- Cómo funcionan
- Requisitos previos para usar una VPC compartida
- Preguntas frecuentes

Cómo funcionan

Cuando la cuenta de propietario de la VPC compartida habilita la supervisión del tiempo de ejecución y la configuración automática de los agentes para cualquiera de los recursos (Amazon EKS o (solo AWS Fargate Amazon ECS)), todas las VPC compartidas pueden instalarse automáticamente el punto de enlace de Amazon VPC compartido y el grupo de seguridad asociado en la cuenta de propietario de la VPC compartida. GuardDuty recupera el ID de la organización asociado a la Amazon VPC compartida.

Ahora, las Cuentas de AWS que pertenezcan a la misma organización que la cuenta de propietario de Amazon VPC compartida también pueden compartir el mismo punto de enlace de Amazon VPC. GuardDuty crea la VPC compartida cuando la cuenta del propietario de la VPC compartida

o la cuenta participante necesitan un punto de enlace de Amazon VPC. Algunos ejemplos de la necesidad de un punto de conexión de Amazon VPC incluyen la activación GuardDuty, la supervisión del tiempo de ejecución, la supervisión del tiempo de ejecución de EKS o el lanzamiento de una nueva tarea de Amazon ECS-Fargate. Cuando estas cuentas habilitan la monitorización del tiempo de ejecución y la configuración automática de agentes para cualquier tipo de recurso, GuardDuty crea un punto de enlace de Amazon VPC y establece la política de puntos de enlace con el mismo ID de organización que el de la cuenta de propietario de la VPC compartida. GuardDuty añade una `GuardDutyManaged` etiqueta y la establece `true` para el punto de enlace de Amazon VPC que GuardDuty crea. Si la cuenta de propietario de Amazon VPC compartida no ha habilitado la monitorización del tiempo de ejecución o la configuración automática de agentes para ninguno de los recursos, no GuardDuty establecerá la política de puntos de conexión de Amazon VPC. Para obtener información sobre la configuración de Runtime Monitoring y la administración automática del agente de seguridad en la cuenta de propietario de la VPC compartida, consulte. Habilitación GuardDuty de la supervisión del tiempo

Cada una de las cuentas que utilizan la misma política de puntos de conexión de Amazon VPC se denomina AWS cuenta participante de la Amazon VPC compartida asociada.

En el siguiente ejemplo, se muestra la política de punto final de la VPC predeterminada de la cuenta del propietario de la VPC compartida y de la cuenta del participante. `aws:PrincipalOrgID`Mostrará el ID de la organización asociado al recurso de VPC compartido. El uso de esta política se limita a las cuentas de los participantes presentes en la organización de la cuenta propietaria.

Example

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "*",
            "Resource": "*",
            "Effect": "Allow",
            "Principal": "*"
        },
        {
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalOrgID": "o-abcdef0123"
                }
            },
```

```
            "Action": "*",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "*"
        }
    ]
}
```

Requisitos previos para usar una VPC compartida

Requisitos previos para la configuración inicial

Realice los siguientes pasos cuando desee Cuenta de AWS que sea el propietario de la VPC compartida:

1. Crear una organización: cree una organización siguiendo los pasos que se indican en la Guía del AWS Organizations usuario sobre cómo crear y administrar una organización.

   Para obtener información sobre cómo agregar o eliminar cuentas de miembros, consulte Administrar Cuentas de AWS en su organización.
2. Creación de un recurso de VPC compartido: puede crear un recurso de VPC compartido desde la cuenta del propietario. Para obtener más información, consulte Compartir su VPC con otras cuentas en la Guía del usuario de Amazon VPC.

Requisitos previos específicos de la supervisión del tiempo de ejecución GuardDuty

La siguiente lista proporciona los requisitos previos específicos de: GuardDuty

- La cuenta de propietario de la VPC compartida y la cuenta participante pueden ser de diferentes organizaciones en. GuardDuty Sin embargo, deben pertenecer a la misma organización en AWS Organizations. Esto es necesario GuardDuty para crear un punto de enlace de Amazon VPC y un grupo de seguridad para la VPC compartida. Para obtener información sobre cómo funcionan las VPC compartidas, consulte Compartir su VPC con otras cuentas en la Guía del usuario de Amazon VPC.
- Habilite Runtime Monitoring o EKS Runtime Monitoring y GuardDuty automatice la configuración de agentes para cualquier recurso de la cuenta de propietario de la VPC compartida y de la cuenta de participante. Para obtener más información, consulte Habilitación de la supervisión del tiempo.

  Si ya ha completado estas configuraciones, continúe con el siguiente paso.

- Cuando trabaje con una tarea de Amazon EKS o una de Amazon ECS (AWS Fargate únicamente), asegúrese de elegir el recurso de VPC compartido asociado a la cuenta del propietario y de seleccionar sus subredes.

Preguntas frecuentes

La siguiente lista proporciona los pasos de solución de problemas relacionados con las preguntas más frecuentes cuando se utiliza un recurso de VPC compartido con la configuración de agentes GuardDuty automatizada habilitada en Runtime Monitoring:

Ya utilizo Runtime Monitoring (o EKS Runtime Monitoring). ¿Cómo habilito la VPC compartida?

Para obtener información sobre los requisitos previos para crear una VPC compartida, consulte. Requisitos previos

Cuando tanto la cuenta del propietario de la VPC compartida como la cuenta del participante cumplan los requisitos previos, GuardDuty intentarán establecer la política de puntos de conexión de Amazon VPC automáticamente.

Si antes de esta versión, Cuenta de AWS tuvo un problema de cobertura debido a que la VPC compartida no era compatible, siga los requisitos previos. Cuando su tipo de recurso (tarea de Amazon EKS o Amazon ECS (AWS Fargate única)) invoque el requisito de un punto de enlace de VPC compartido GuardDuty , intentará establecer la nueva política de punto de enlace de VPC.

Como cuenta de propietario de VPC compartida, quiero que la política de puntos finales de VPC compartida se restrinja a un subconjunto de cuentas de participantes de mi organización. ¿Cómo puedo hacerlo?

Si tiene una `true` etiqueta`GuardDutyManaged`: asociada al punto final, elimínela. Esto impide GuardDuty intentar modificar o anular la política de puntos finales de la VPC de la VPC compartida.

Para obtener más información, consulte Controlar el acceso a puntos de conexión de VPC con políticas de punto de conexión.

¿Por qué el punto final de la VPC compartido se modifica de a**`aws:PrincipalAccount`**? **`aws:PrincipalOrgId`** ¿Cómo puedo evitarlo?

Cuando GuardDuty detecta que varias cuentas de la misma organización comparten la VPC AWS Organizations, GuardDuty intenta modificar la política para especificar el ID de la organización.

Para evitarlo, elimina la `true` etiqueta`GuardDutyManaged`: del punto final de la VPC compartido. Esto impide GuardDuty intentar modificar o anular la política de puntos finales de la VPC de la VPC compartida.

¿Qué ocurre cuando la cuenta del propietario de la VPC compartida o una de las cuentas participantes deshabilita Runtime Monitoring (GuardDuty o EKS Runtime Monitoring)?

Cuando la cuenta de propietario de la VPC compartida inhabilita Runtime Monitoring (GuardDuty o EKS Runtime Monitoring), GuardDuty comprueba si algún tipo de recurso que pertenezca a la cuenta del participante ha utilizado el punto final de la VPC compartida o si alguna cuenta participante ha habilitado alguna vez la administración de GuardDuty agentes para algún tipo de recurso. En caso afirmativo, GuardDuty no eliminará el punto final de la VPC ni el grupo de seguridad.

Si la cuenta participante de la VPC compartida deshabilita GuardDuty Runtime Monitoring (o EKS Runtime Monitoring), la cuenta propietaria de la VPC compartida no se verá afectada y la cuenta propietaria no eliminará el recurso de VPC compartido ni el grupo de seguridad.

¿Cómo puedo eliminar el recurso de VPC compartido? ¿Cuál será su impacto?

Como cuenta de propietario de VPC compartida, puede eliminar el recurso de VPC compartido incluso cuando lo esté utilizando su cuenta o cualquiera de las cuentas participantes en Runtime Monitoring. Para obtener información sobre cómo eliminar la VPC compartida y comprender su impacto, consulte. To delete VPC endpoint

Gestión de los agentes de seguridad duales instalados en un host

Las instancias Amazon EC2 pueden admitir varios tipos de cargas de trabajo. Al configurar un agente de seguridad automatizado en una instancia de Amazon EC2, es posible que la misma instancia EC2 tenga otro agente de seguridad a través de EKS.

Información general

Considere un escenario en el que haya habilitado la monitorización del tiempo de ejecución. Ahora, habilita el agente automatizado para Amazon EKS mediante GuardDuty. También ha activado el agente automatizado para Amazon EC2. Puede ocurrir que el mismo host subyacente se instale con dos agentes de seguridad, uno para Amazon EKS y otro para Amazon EC2. Esto podría provocar que dos agentes de seguridad se ejecutaran dentro del mismo host y recopilaran los eventos en tiempo de ejecución y los enviaran a un servidor GuardDuty, lo que podría generar resultados duplicados.

Impact

- Si hay más de un agente de seguridad en ejecución en el mismo host, es posible que tu cuenta necesite el doble de procesamiento de CPU y memoria. Para obtener información sobre los límites de CPU y memoria para cada tipo de recurso, consulte Requisitos previos para ese recurso.
- GuardDuty ha diseñado la función de supervisión en tiempo de ejecución de forma que, aunque se superpongan dos agentes de seguridad que recopilen eventos en tiempo de ejecución del mismo host subyacente, solo se le cobre a su cuenta por una transmisión de eventos en tiempo de ejecución.

¿Cómo GuardDuty gestiona varios agentes

GuardDuty detecta cuando dos agentes de seguridad se están ejecutando en el mismo host y designa solo a uno de ellos como el agente de seguridad que recopila activamente los eventos de tiempo de ejecución. El segundo agente consumirá un mínimo de recursos del sistema para evitar cualquier impacto en el rendimiento de las aplicaciones.

GuardDuty considera los siguientes escenarios:

- Cuando una instancia de EC2 entra dentro del ámbito de los agentes de seguridad de Amazon EKS y Amazon EC2, el agente de seguridad de EKS tiene prioridad. Esto solo se aplicará cuando utilice el agente de seguridad v1.1.0 o superior para Amazon EC2. Las versiones anteriores del agente seguirán ejecutándose y recopilando eventos de tiempo de ejecución, ya que las versiones antiguas del agente no se ven afectadas por la priorización.
- Cuando Amazon EKS y Amazon EC2 hayan GuardDuty gestionado agentes de seguridad y su instancia de Amazon EC2 también esté gestionada por SSM, ambos agentes de seguridad se instalarán en el nivel de host. Una vez instalados los agentes, GuardDuty decide qué agente de seguridad seguirá ejecutándose. Cuando ambos agentes de seguridad estén en ejecución, eventualmente solo uno de ellos recopilará los eventos de tiempo de ejecución.
- Cuando los agentes de seguridad asociados a EC2 y EKS se ejecutan al mismo tiempo, es GuardDuty posible que solo se generen resultados duplicados durante el período de superposición.

  Esto puede ocurrir cuando:

  - Los agentes de seguridad para EC2 y EKS se configuran mediante GuardDuty (automáticamente), o
  - Su recurso de Amazon EKS tiene un agente de seguridad automatizado.

- Cuando el agente de seguridad de EKS ya está en ejecución, si lo implementa manualmente en el mismo host subyacente y cumple todos los requisitos previos, es GuardDuty posible que no instale un segundo agente de seguridad.

Administración del agente de seguridad automatizado para la instancia de Amazon EC2

Migración de un agente manual de Amazon EC2 a un agente automatizado

Esta sección se aplica a su Cuenta de AWS caso si anteriormente administraba el agente de seguridad de forma manual y ahora desea utilizar la configuración GuardDuty automática del agente. Si esto no es su caso, continúe configurando el agente de seguridad para su cuenta.

Cuando habilita el agente GuardDuty automatizado, GuardDuty administra el agente de seguridad en su nombre. Para obtener información sobre las medidas que se GuardDuty deben tomar, consulteUtilice una configuración de agentes automatizada (recomendado).

Eliminar recursos

Elimine la asociación SSM

- Elimine cualquier asociación de SSM que haya creado cuando administraba manualmente el agente de seguridad para Amazon EC2. Para obtener más información, consulte Eliminar asociaciones.
- Esto se hace para poder hacerse cargo de la gestión de las acciones de SSM, ya sea que utilice agentes automatizados a nivel de cuenta o de instancia (mediante etiquetas de inclusión o exclusión). GuardDuty Para obtener más información sobre las acciones que puede GuardDuty realizar el SSM, consulte. Permisos de rol vinculados al servicio para GuardDuty
- Al eliminar una asociación de SSM que se creó anteriormente para administrar el agente de seguridad de forma manual, es posible que se produzca un breve período de superposición cuando se GuardDuty cree una asociación de SSM para administrar el agente de seguridad automáticamente. Durante este período, es posible que se produzcan conflictos debido a la programación del SSM. Para obtener más información, consulte Programación de SSM en Amazon EC2.

Administre las etiquetas de inclusión y exclusión para sus instancias de Amazon EC2

- Etiquetas de inclusión: cuando no habilita la configuración GuardDuty automática del agente, pero etiqueta alguna de sus instancias de Amazon EC2 con una etiqueta de inclusión

(`GuardDutyManaged:true`), se GuardDuty crea una asociación SSM que instalará y administrará el agente de seguridad en las instancias de EC2 seleccionadas. Este es un comportamiento esperado que le ayuda a administrar el agente de seguridad solo en instancias de EC2 seleccionadas. Para obtener más información, consulte Cómo funciona Runtime Monitoring con las instancias de Amazon EC2.

Para GuardDuty evitar la instalación y la administración del agente de seguridad, elimine la etiqueta de inclusión de estas instancias de EC2. Para obtener más información, consulte Añadir y eliminar etiquetas en la Guía del usuario de Amazon EC2 para instancias de Linux.

- Etiquetas de exclusión: si desea habilitar la configuración GuardDuty automática de los agentes para todas las instancias de EC2 de su cuenta, asegúrese de que ninguna instancia de EC2 esté etiquetada con una etiqueta de exclusión (:)`GuardDutyManaged. false`

Configuración del GuardDuty agente para una cuenta independiente

Configure for all instances

Para configurar el agente GuardDuty de seguridad para todas las instancias de su cuenta independiente

1. Inicie sesión AWS Management Console y abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, selecciona Runtime Monitoring.
3. En la pestaña Configuración, seleccione Editar.
4. En la sección EC2, elija Activar.
5. Seleccione Guardar.
6. Puede comprobar que la asociación SSM que se GuardDuty crea instalará y administrará el agente de seguridad en todos los recursos de EC2 que pertenezcan a su cuenta.
   a. Abra la AWS Systems Manager consola en https://console.aws.amazon.com/systems-manager/.
   b. Abra la pestaña Objetivos de la asociación SSM (`GuardDutyRuntimeMonitoring-do-not-delete`). Observe que la clave de etiqueta aparece como InstanceIds.

Using inclusion tag in selected instances

Para configurar el agente GuardDuty de seguridad para instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. Añada la `true` etiqueta`GuardDutyManaged`: a las instancias que desee GuardDuty monitorear y detectar posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte Para agregar una etiqueta a un recurso individual.
3. Puede comprobar que la asociación SSM que se GuardDuty cree instalará y administrará el agente de seguridad únicamente en los recursos de EC2 que estén etiquetados con las etiquetas de inclusión.

   Abra la AWS Systems Manager consola en https://console.aws.amazon.com/systems-manager/.

   - Abra la pestaña Objetivos de la asociación SSM que se cree (`GuardDutyRuntimeMonitoring-do-not-delete`). La clave de etiqueta aparece como etiqueta: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Asegúrese de añadir la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Al habilitar la configuración automática de agentes para Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión se incluirá en la configuración de agentes GuardDuty automatizada.

Para configurar el agente GuardDuty de seguridad para instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.

2. Añada la `false` etiqueta`GuardDutyManaged`: a las instancias que no desee GuardDuty monitorear y detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte Para agregar una etiqueta a un recurso individual.
3. Para que las etiquetas de exclusión estén disponibles en los metadatos de la instancia, lleve a cabo los siguientes pasos:

   a. En la pestaña Detalles de la instancia, consulta el estado de Permitir etiquetas en los metadatos de la instancia.

      Si actualmente está deshabilitado, sigue estos pasos para cambiar el estado a Habilitado. De lo contrario, omita este paso.

   b. Seleccione la instancia para la que quiere permitir las etiquetas.

   c. En el menú Acciones, selecciona Configuración de instancia.

   d. Seleccione Permitir etiquetas en los metadatos de la instancia.

   e. En Acceso a las etiquetas de los metadatos de la instancia, selecciona Permitir.

   f. Seleccione Guardar.
4. Una vez que hayas agregado la etiqueta de exclusión, sigue los mismos pasos que se especificaron en la pestaña Configurar para todas las instancias.

Ahora puede evaluar el tiempo de ejecución. Cobertura para la instancia Amazon EC2

Configuración del GuardDuty agente en un entorno de cuentas múltiples

Para una cuenta de administrador delegado GuardDuty

Configure for all instances

Si seleccionó Activar Runtime Monitoring para todas las cuentas, elija una de las siguientes opciones para la cuenta de GuardDuty administrador delegado:

- Opción 1

  En Configuración automatizada de agentes, en la sección EC2, seleccione Activar para todas las cuentas.
- Opción 2
  - En Configuración automatizada de agentes, en la sección EC2, seleccione Configurar cuentas manualmente.

- En Administrador delegado (esta cuenta), elija Activar.
- Seleccione Guardar.

Si eligió Configurar las cuentas manualmente para la supervisión del tiempo de ejecución, lleve a cabo los siguientes pasos:

- En Configuración automatizada de agentes, en la sección EC2, seleccione Configurar cuentas manualmente.
- En Administrador delegado (esta cuenta), elija Activar.
- Seleccione Guardar.

Independientemente de la opción que elija para habilitar la configuración automática del agente para la cuenta de GuardDuty administrador delegado, puede comprobar que la asociación SSM que se GuardDuty cree instalará y gestionará el agente de seguridad en todos los recursos de EC2 que pertenezcan a esta cuenta.

1. Abra la AWS Systems Manager consola en https://console.aws.amazon.com/systems-manager/.
2. Abra la pestaña Objetivos de la asociación SSM (`GuardDutyRuntimeMonitoring-do-not-delete`). Observe que la clave de etiqueta aparece como InstanceIds.

Using inclusion tag in selected instances

Para configurar el GuardDuty agente para las instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. Añada la `true` etiqueta`GuardDutyManaged`: a las instancias que desee GuardDuty monitorear y detectar posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte Para agregar una etiqueta a un recurso individual.

   La adición de esta etiqueta permitirá GuardDuty instalar y administrar el agente de seguridad para estas instancias de EC2 seleccionadas. No es necesario habilitar la configuración automática del agente de forma explícita.

3. Puede comprobar que la asociación SSM que se GuardDuty cree instalará y administrará el agente de seguridad únicamente en los recursos de EC2 que estén etiquetados con las etiquetas de inclusión.

   Abra la AWS Systems Manager consola en https://console.aws.amazon.com/systems-manager/.

   - Abra la pestaña Objetivos de la asociación SSM que se cree (`GuardDutyRuntimeMonitoring-do-not-delete`). La clave de etiqueta aparece como etiqueta: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Asegúrese de añadir la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Al habilitar la configuración automática de agentes para Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión se incluirá en la configuración de agentes GuardDuty automatizada.

Para configurar el GuardDuty agente para las instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. Añada la `false` etiqueta`GuardDutyManaged`: a las instancias que no desee GuardDuty monitorear y detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte Para agregar una etiqueta a un recurso individual.
3. Para que las etiquetas de exclusión estén disponibles en los metadatos de la instancia, lleve a cabo los siguientes pasos:

   a. En la pestaña Detalles de la instancia, consulta el estado de Permitir etiquetas en los metadatos de la instancia.

      Si actualmente está deshabilitado, sigue estos pasos para cambiar el estado a Habilitado. De lo contrario, omita este paso.

   b. En el menú Acciones, seleccione Configuración de instancia.

   c. Seleccione Permitir etiquetas en los metadatos de la instancia.

4. Una vez que hayas agregado la etiqueta de exclusión, sigue los mismos pasos que se especificaron en la pestaña Configurar para todas las instancias.

Ahora puede evaluar el tiempo de ejecuciónCobertura para la instancia Amazon EC2.

Habilitación automática para todas las cuentas de los miembros

> **Note**
>
> La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Configure for all instances

En los siguientes pasos, se supone que seleccionó Activar para todas las cuentas en la sección Runtime Monitoring:

1. Seleccione Activar para todas las cuentas en la sección Configuración automática de agentes para Amazon EC2.
2. Puede comprobar que la asociación SSM que GuardDuty crea (`GuardDutyRuntimeMonitoring-do-not-delete`) instalará y administrará el agente de seguridad en todos los recursos de EC2 que pertenezcan a esta cuenta.
   a. Abra la AWS Systems Manager consola en https://console.aws.amazon.com/systems-manager/.
   b. Abra la pestaña Objetivos de la asociación SSM. Observe que la clave de etiqueta aparece como InstanceIds.

Using inclusion tag in selected instances

Para configurar el GuardDuty agente para las instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. Añada la `true` etiqueta`GuardDutyManaged`: a las instancias de EC2 que desee GuardDuty supervisar y detectar posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte Para agregar una etiqueta a un recurso individual.

La adición de esta etiqueta permitirá GuardDuty instalar y administrar el agente de seguridad para estas instancias de EC2 seleccionadas. No es necesario habilitar la configuración automática del agente de forma explícita.

3. Puede comprobar que la asociación SSM que se GuardDuty cree instalará y gestionará el agente de seguridad en todos los recursos de EC2 que pertenezcan a su cuenta.

   a. Abra la AWS Systems Manager consola en https://console.aws.amazon.com/systems-manager/.

   b. Abra la pestaña Objetivos de la asociación SSM (`GuardDutyRuntimeMonitoring-do-not-delete`). Observe que la clave de etiqueta aparece como InstanceIds.

Using exclusion tag in selected instances

> **Note**
>
> Asegúrese de añadir la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Al habilitar la configuración automática de agentes para Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión se incluirá en la configuración de agentes GuardDuty automatizada.

Para configurar el agente GuardDuty de seguridad para instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. Añada la `false` etiqueta`GuardDutyManaged`: a las instancias que no desee GuardDuty monitorear y detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte Para agregar una etiqueta a un recurso individual.
3. Para que las etiquetas de exclusión estén disponibles en los metadatos de la instancia, lleve a cabo los siguientes pasos:

   a. En la pestaña Detalles de la instancia, consulta el estado de Permitir etiquetas en los metadatos de la instancia.

      Si actualmente está deshabilitado, sigue estos pasos para cambiar el estado a Habilitado. De lo contrario, omita este paso.

b. En el menú Acciones, seleccione Configuración de instancia.

c. Seleccione Permitir etiquetas en los metadatos de la instancia.

4. Una vez que hayas agregado la etiqueta de exclusión, sigue los mismos pasos que se especificaron en la pestaña Configurar para todas las instancias.

Ahora puede evaluar el tiempo de ejecuciónCobertura para la instancia Amazon EC2.

Se habilita automáticamente solo para las cuentas de nuevos miembros

La cuenta de GuardDuty administrador delegado puede establecer la configuración del agente automatizado para el recurso de Amazon EC2 para que se habilite automáticamente para las cuentas de los nuevos miembros a medida que se unan a la organización.

Configure for all instances

En los siguientes pasos, se supone que ha seleccionado Activar automáticamente las cuentas de nuevos miembros en la sección Supervisión del tiempo de ejecución:

1. En el panel de navegación, selecciona Runtime Monitoring.
2. En la página Supervisión del tiempo de ejecución, seleccione Editar.
3. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que cada vez que se incorpore una nueva cuenta a su organización, la configuración automática de agentes para Amazon EC2 se habilite automáticamente para su cuenta. Solo la cuenta de GuardDuty administrador delegado de la organización puede modificar esta selección.
4. Seleccione Guardar.

Cuando un nuevo miembro se una a la organización, esta configuración se habilitará automáticamente para él. GuardDuty Para gestionar el agente de seguridad de las instancias de Amazon EC2 que pertenecen a esta nueva cuenta de miembro, asegúrese de que se cumplen todos los requisitos previosPara una instancia EC2.

Cuando se crea una asociación SSM (`GuardDutyRuntimeMonitoring-do-not-delete`), puede comprobar que la asociación SSM instalará y administrará el agente de seguridad en todas las instancias EC2 que pertenezcan a la nueva cuenta de miembro.

- Abra la AWS Systems Manager consola en https://console.aws.amazon.com/systems-manager/.

- Abra la pestaña Objetivos de la asociación SSM. Observe que la clave de etiqueta aparece como InstanceIds.

Using inclusion tag in selected instances

Para configurar el agente de GuardDuty seguridad para instancias seleccionadas de su cuenta

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. Añada la `true` etiqueta`GuardDutyManaged`: a las instancias que desee GuardDuty monitorear y detectar posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte Para agregar una etiqueta a un recurso individual.

   Agregar esta etiqueta permitirá GuardDuty instalar y administrar el agente de seguridad para estas instancias seleccionadas. No es necesario que habilite la configuración automática del agente de forma explícita.
3. Puede comprobar que la asociación SSM que se GuardDuty cree instalará y administrará el agente de seguridad únicamente en los recursos de EC2 que estén etiquetados con las etiquetas de inclusión.

   a. Abra la AWS Systems Manager consola en https://console.aws.amazon.com/systems-manager/.

   b. Abra la pestaña Objetivos de la asociación SSM que se va a crear. La clave de etiqueta aparece como etiqueta: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Asegúrese de añadir la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Al habilitar la configuración automática de agentes para Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión se incluirá en la configuración de agentes GuardDuty automatizada.

Para configurar el agente GuardDuty de seguridad para instancias específicas de su cuenta independiente

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. Añada la `false` etiqueta`GuardDutyManaged`: a las instancias que no desee GuardDuty monitorear y detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte Para agregar una etiqueta a un recurso individual.
3. Para que las etiquetas de exclusión estén disponibles en los metadatos de la instancia, lleve a cabo los siguientes pasos:

   a. En la pestaña Detalles de la instancia, consulta el estado de Permitir etiquetas en los metadatos de la instancia.

      Si actualmente está deshabilitado, sigue estos pasos para cambiar el estado a Habilitado. De lo contrario, omita este paso.

   b. En el menú Acciones, seleccione Configuración de instancia.

   c. Seleccione Permitir etiquetas en los metadatos de la instancia.
4. Una vez que hayas agregado la etiqueta de exclusión, sigue los mismos pasos que se especificaron en la pestaña Configurar para todas las instancias.

Ahora puede evaluar el tiempo de ejecuciónCobertura para la instancia Amazon EC2.

Solo cuentas de miembros selectivas

Configure for all instances

1. En la página Cuentas, seleccione una o más cuentas para las que desee habilitar la configuración de agentes automatizada de Runtime Monitoring (Amazon EC2). Asegúrese de que las cuentas que seleccione en este paso ya tengan activado Runtime Monitoring.
2. En Editar planes de protección, elija la opción adecuada para habilitar la configuración de agentes automatizada de Runtime Monitoring (Amazon EC2).
3. Seleccione Confirmar.

Using inclusion tag in selected instances

Para configurar el agente de GuardDuty seguridad para las instancias seleccionadas

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. Añada la `true` etiqueta`GuardDutyManaged`: a las instancias que desee GuardDuty monitorear y detectar posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte Para agregar una etiqueta a un recurso individual.

   Añadir esta etiqueta permitirá GuardDuty gestionar el agente de seguridad de las instancias etiquetadas de Amazon EC2. No es necesario que habilite explícitamente la configuración automática de los agentes (supervisión del tiempo de ejecución - Configuración automática de agentes (EC2).

Using exclusion tag in selected instances

> **Note**
>
> Asegúrese de añadir la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Al habilitar la configuración automática de agentes para Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión se incluirá en la configuración de agentes GuardDuty automatizada.

Para configurar el agente GuardDuty de seguridad para las instancias seleccionadas

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. Añada la `false` etiqueta`GuardDutyManaged`: a las instancias de EC2 que no desee GuardDuty supervisar o detectar posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte Para agregar una etiqueta a un recurso individual.
3. Para que las etiquetas de exclusión estén disponibles en los metadatos de la instancia, lleve a cabo los siguientes pasos:

   a. En la pestaña Detalles de la instancia, consulta el estado de Permitir etiquetas en los metadatos de la instancia.

Si actualmente está deshabilitado, sigue estos pasos para cambiar el estado a Habilitado. De lo contrario, omita este paso.

b. En el menú Acciones, seleccione Configuración de instancia.

c. Seleccione Permitir etiquetas en los metadatos de la instancia.

4. Una vez que hayas agregado la etiqueta de exclusión, sigue los mismos pasos que se especificaron en la pestaña Configurar para todas las instancias.

Ahora puede evaluarCobertura para la instancia Amazon EC2.

Administración manual del agente de seguridad para la instancia de Amazon EC2

Tras activar Runtime Monitoring, tendrá que instalar el agente de GuardDuty seguridad manualmente. Al instalar el agente, GuardDuty recibirá los eventos de tiempo de ejecución de las instancias de Amazon EC2.

Para administrar el agente GuardDuty de seguridad, debe crear un punto de conexión de Amazon VPC y, a continuación, seguir los pasos para instalar el agente de seguridad manualmente.

Creación manual de puntos de conexión de Amazon VPC

Antes de poder instalar el agente GuardDuty de seguridad, debe crear un punto final de Amazon Virtual Private Cloud (Amazon VPC). Esto ayudará a GuardDuty recibir los eventos de tiempo de ejecución de sus instancias de Amazon EC2.

> **Note**
>
> El uso del punto final de la VPC no conlleva ningún coste adicional.

Para crear un punto de conexión de Amazon VPC

1. Inicie sesión en la consola de Amazon VPC AWS Management Console y ábrala en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en Nube privada de VPC, selecciona Endpoints.
3. Seleccione Crear punto de conexión.
4. En la página Crear punto de conexión, en Categoría de servicio, elija Otros servicios de punto de conexión.

5. En Nombre del servicio, escriba **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

   Asegúrese de reemplazar *`us-east-1`* por su. Región de AWS Debe ser la misma región que la instancia de Amazon EC2 que pertenece a su ID de AWS cuenta.

6. Elija Verificar el servicio.

7. Una vez que el nombre del servicio se haya verificado correctamente, elija la VPC en la que reside la instancia. Añada la siguiente política para restringir el uso de puntos de conexión de Amazon VPC únicamente a la cuenta especificada. Con el valor de `Condition` de la organización que se indica debajo de esta política, puede actualizar la siguiente política para restringir el acceso a su punto de conexión. Para proporcionar el soporte del punto de enlace de Amazon VPC a los ID de cuenta específicos de su organización, consulte. Organization condition to restrict access to your endpoint

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
 ]
}
```

   El ID de cuenta de `aws:PrincipalAccount` debe coincidir con la cuenta que contiene la VPC y el punto de conexión de VPC. En la siguiente lista se muestra cómo compartir el punto final de la VPC con otros ID de AWS cuenta:

- Para especificar varias cuentas para acceder al punto final de la VPC, `"aws:PrincipalAccount: "111122223333"` sustitúyalo por el siguiente bloque:

```
"aws:PrincipalAccount": [
          "666666666666",
          "555555555555"
      ]
```

  Asegúrese de reemplazar los ID de AWS cuenta por los ID de cuenta de las cuentas que necesitan acceder al punto final de la VPC.

- Para permitir que todos los miembros de una organización accedan al punto final de la VPC, `"aws:PrincipalAccount: "111122223333"` sustitúyalo por la siguiente línea:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

  Asegúrese de reemplazar la organización *o-abcdef0123* por el ID de su organización.

- Para restringir el acceso a un recurso mediante un identificador de organización, añada el suyo a la política. `ResourceOrgID` Para obtener más información, consulte `aws:ResourceOrgID` en la Guía del usuario de IAM.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. En Configuración adicional, seleccione Habilitar nombre de DNS.
9. En Subredes, elige las subredes en las que reside la instancia.
10. En Grupos de seguridad, elija un grupo de seguridad que tenga el puerto de entrada 443 habilitado desde su VPC (o su instancia de Amazon EC2). Si aún no tiene un grupo de seguridad que tenga habilitado el puerto de entrada 443, consulte Crear un grupo de seguridad en la Guía del usuario de Amazon EC2 para instancias de Linux.

    Si se produce un problema al restringir los permisos de entrada a su VPC (o instancia), proporcione soporte al puerto 443 entrante desde cualquier dirección IP. `(0.0.0.0/0)`

Instalación manual del agente de seguridad

GuardDuty proporciona los dos métodos siguientes para instalar el agente GuardDuty de seguridad en las instancias de Amazon EC2:

- Método 1: Mediante el uso AWS Systems Manager : este método requiere que se gestione la instancia de Amazon EC2. AWS Systems Manager
- Método 2: Mediante scripts de instalación de RPM: puede utilizar este método independientemente de que sus instancias de Amazon EC2 estén AWS Systems Manager gestionadas o no.

Método 1: mediante el uso AWS Systems Manager

Para usar este método, asegúrese de que sus instancias de Amazon EC2 estén AWS Systems Manager administradas y, a continuación, instale el agente.

AWS Systems Manager instancia Amazon EC2 gestionada

Siga los siguientes pasos para gestionar sus instancias AWS Systems Manager de Amazon EC2.

- AWS Systems Managerle ayuda a administrar sus AWS aplicaciones y recursos end-to-end y a permitir operaciones seguras a escala.

  Para gestionar sus instancias de Amazon EC2 AWS Systems Manager, consulte Configuración de Systems Manager para instancias de Amazon EC2 en AWS Systems Manager la Guía del usuario.
- En la siguiente tabla se muestran los nuevos documentos GuardDuty gestionados AWS Systems Manager :

Nombre del documento	Tipo de documento	Finalidad
`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`	Distributor	Para empaquetar el agente GuardDuty de seguridad.
`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`	Comando	Ejecutar el script de instalación o desinstalación para instalar el GuardDuty agente de seguridad.

Para obtener más información al respecto AWS Systems Manager, consulte los documentos de Amazon EC2 Systems Manager en AWS Systems Manager la Guía del usuario.

Para instalar el GuardDuty agente para la instancia de Amazon EC2 mediante AWS Systems Manager

1. Abra la AWS Systems Manager consola en https://console.aws.amazon.com/systems-manager/.
2. En el panel de navegación, elija Documentos
3. En Propiedad de Amazon, seleccionaAmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin.
4. Elija Run Command (Ejecutar comando).
5. Introduzca los siguientes parámetros de ejecución del comando
   - Acción: selecciona Instalar.
   - Tipo de instalación: elija Instalar o Desinstalar.
   - Nombre: AmazonGuardDuty-RuntimeMonitoringSsmPlugin
   - Versión: si permanece vacío, obtendrá la última versión del agente de GuardDuty seguridad. Para obtener más información sobre las versiones de lanzamiento,GuardDuty agente de seguridad para instancias de Amazon EC2.
6. Seleccione la instancia Amazon EC2 de destino. Puede seleccionar una o más instancias de Amazon EC2. Para obtener más información, consulte AWS Systems Manager Ejecutar comandos desde la consola en la Guía del AWS Systems Manager usuario
7. Compruebe si la instalación del GuardDuty agente está en buen estado. Para obtener más información, consulte Validación del estado de instalación GuardDuty del agente de seguridad.

Método 2: mediante scripts de instalación de RPM

> **Important**
>
> Se recomienda encarecidamente comprobar la firma RPM del agente de GuardDuty seguridad antes de instalarlo en el equipo.

1. Compruebe la firma RPM del agente de GuardDuty seguridad

a. Descargue la clave pública correspondiente, la firma de x86_64 RPM, la firma de arm64 RPM y el enlace de acceso correspondiente a los scripts de RPM alojados en los buckets de Amazon S3

   Puede utilizar las siguientes plantillas para formar la clave pública, la firma de x86_64 RPM, la firma de arm64 RPM y el enlace de acceso correspondiente a los scripts de RPM. Sustituya el valor del Región de AWS identificador de AWS cuenta y la versión del GuardDuty agente para acceder a los scripts de RPM.

   - Clave pública:

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/publickey.pem
     ```

   - GuardDuty Firma RPM del agente de seguridad:

     Firma de x86_64 RPM

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/
     amazon-guardduty-agent-1.1.0.x86_64.sig
     ```

     Firma de arm64 RPM

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/
     amazon-guardduty-agent-1.1.0.arm64.sig
     ```

   - Acceda a los enlaces a los scripts RPM del bucket de Amazon S3:

     Enlace de acceso para x86_64 RPM

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/
     amazon-guardduty-agent-1.1.0.x86_64.rpm
     ```

     Enlace de acceso para arm64 RPM

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/
     amazon-guardduty-agent-1.1.0.arm64.rpm
     ```

   En el siguiente comando para descargar la clave pública correspondiente, la firma de x86_64 RPM, la firma de arm64 RPM y el enlace de acceso correspondiente a los scripts

RPM alojados en los buckets de Amazon S3, asegúrese de sustituir el ID de cuenta por el ID correspondiente y la región por su Cuenta de AWS región actual.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
x86_64/amazon-guardduty-agent-1.1.0.x86_64.rpm ./amazon-guardduty-
agent-1.1.0.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
x86_64/amazon-guardduty-agent-1.1.0.x86_64.sig ./amazon-guardduty-
agent-1.1.0.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
publickey.pem ./publickey.pem
```

Región de AWS	Nombre de la región	AWS ID de cuenta
eu-west-1	Europa (Irlanda)	694911143906
us-east-1	Este de EE. UU. (Norte de Virginia)	593207742271
us-west-2	Oeste de EE. UU. (Oregón)	733349766148
eu-west-3	Europa (París)	665651866788
us-east-2	Este de EE. UU. (Ohio)	307168627858
eu-central-1	Europa (Fráncfort)	323658145986
ap-northeast-2	Asia-Pacífico (Seúl)	914738172881
eu-north-1	Europa (Estocolmo)	591436053604
ap-east-1	Asia-Pacífico (Hong Kong)	258348409381
me-south-1	Medio Oriente (Baréin)	536382113932
eu-west-2	Europa (Londres)	892757235363
ap-northeast-1	Asia-Pacífico (Tokio)	533107202818
ap-southeast-1	Asia-Pacífico (Singapur)	174946120834

ap-south-1	Asia-Pacífico (Bombay)	251508486986
ap-southeast-3	Asia-Pacífico (Yakarta)	510637619217
sa-east-1	América del Sur (São Paulo)	758426053663
ap-northeast-3	Asia-Pacífico (Osaka)	273192626886
eu-south-1	Europa (Milán)	266869475730
af-south-1	África (Ciudad del Cabo)	197869348890
ap-southeast-2	Asia-Pacífico (Sídney)	005257825471
me-central-1	Medio Oriente (EAU)	000014521398
us-west-1	Oeste de EE. UU. (Norte de California)	684579721401
ca-central-1	Canadá (centro)	354763396469
ap-south-2	Asia-Pacífico (Hyderabad)	950823858135
eu-south-2	Europa (España)	919611009337
eu-central-2	Europa (Zúrich)	529164026651
ap-southeast-4	Asia-Pacífico (Melbourne)	251357961535
il-central-1	Israel (Tel Aviv)	870907303882

b. Importe la clave pública a la base de datos

```
gpg --import publickey.pem
```

gpg muestra que la importación se realizó correctamente

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

c. Verifique la firma

```
gpg --verify amazon-guardduty-agent-1.1.0.x86_64.sig amazon-guardduty-
agent-1.1.0.x86_64.rpm
```

Si se aprueba la verificación, verás un mensaje similar al resultado que se muestra a continuación. Ahora puede proceder a instalar el agente GuardDuty de seguridad mediante RPM.

Ejemplo de salida:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

Si la verificación falla, significa que es posible que la firma del RPM haya sido manipulada. Debe eliminar la clave pública de la base de datos y volver a intentar el proceso de verificación.

Ejemplo:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

d. Elimine la clave pública de la base de datos.

```
gpg --delete-keys AwsGuardDuty
```

2. Conéctate con SSH desde Linux o macOS.
3. Instale el agente GuardDuty de seguridad mediante el siguiente comando:

```
sudo rpm -ivh amazon-guardduty-agent-1.1.0.x86_64.rpm
```

4. Compruebe si la instalación del GuardDuty agente está en buen estado. Para obtener más información sobre los pasos, consulteValidación del estado de instalación GuardDuty del agente de seguridad.
5. (Opcional) elimine el agente de GuardDuty seguridad mediante el siguiente comando:

```
sudo rpm -ev amazon-guardduty-agent
```

Error de memoria insuficiente

Si se produce un `out-of-memory` error al instalar o actualizar manualmente el agente de GuardDuty seguridad para Amazon EC2, consulte. Solución de problemas de memoria insuficiente

Validación del estado de instalación GuardDuty del agente de seguridad

Para validar si el agente de GuardDuty seguridad está en buen estado

1. Conéctate con SSH desde Linux o macOS.
2. Ejecute el siguiente comando para comprobar el estado del agente de GuardDuty seguridad:

```
sudo systemctl status amazon-guardduty-agent
```

Si desea ver los registros de instalación del agente de seguridad, están disponibles en`/var/log/amzn-guardduty-agent/`.

Para ver los registros, haga lo siguiente`sudo journalctl -u amazon-guardduty-agent`.

Actualizar el agente GuardDuty de seguridad manualmente

Puede actualizar el agente GuardDuty de seguridad mediante el comando Ejecutar. Puede seguir los mismos pasos que utilizó para instalar el agente GuardDuty de seguridad.

Desinstalar el agente de seguridad manualmente

Al deshabilitar Runtime Monitoring, GuardDuty no elimina el agente de seguridad asociado a la instancia de Amazon EC2. Puede desinstalar el agente GuardDuty de seguridad para la instancia de Amazon EC2 mediante uno de los dos métodos siguientes.

Método 1: mediante el comando Ejecutar

Para desinstalar el agente GuardDuty de seguridad mediante el comando Ejecutar

1. Puede desinstalar el agente de GuardDuty seguridad siguiendo los pasos que se especifican en la sección AWS Systems Manager Ejecutar comando de la Guía del AWS Systems Manager

usuario. Utilice la acción Desinstalar en los parámetros para desinstalar el agente GuardDuty de seguridad.

En la sección Targets, asegúrese de que el impacto se produzca únicamente en las instancias de Amazon EC2 de las que desee desinstalar el agente de seguridad.

Utilice el siguiente GuardDuty documento y distribuidor:

- Nombre del documento: `AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`
- Distribuidor: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`

2. Tras proporcionar todos los detalles, al seleccionar Ejecutar, se elimina el agente de seguridad que se ha desplegado en las instancias de Amazon EC2 de destino.

   Para eliminar la configuración del punto de conexión de Amazon VPC, debe deshabilitar Runtime Monitoring y Amazon EKS Runtime Monitoring.

Método 2: mediante el script RPM

Para desinstalar el agente GuardDuty de seguridad mediante el rpm

1. Conéctate con SSH desde Linux o macOS.
2. El siguiente comando desinstalará el agente de GuardDuty seguridad de la instancia de Amazon EC2 a la que se conecte:

   ```
   sudo rpm -e amazon-guardduty-agent
   ```

   También puede comprobar los registros asociados a este comando.

Eliminar el punto de conexión de Amazon VPC

Si desea deshabilitar Runtime Monitoring o desinstalar el agente de GuardDuty seguridad de su cuenta, también puede optar por eliminar el punto de conexión de Amazon VPC que se creó manualmente ()Creación manual de puntos de conexión de Amazon VPC.

Para eliminar el punto de conexión de Amazon VPC mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.

3. Seleccione el punto final que se creó manualmente en el momento de habilitar Runtime Monitoring.
4. Elija Acciones, Eliminar puntos de conexión de VPC.
5. Cuando se le solicite confirmación, ingrese **`delete`**.
6. Elija Delete (Eliminar).

Para eliminar el punto de enlace de Amazon VPC mediante AWS CLI

- delete-vpc-endpoints (AWS Command Line Interface)
- VpcEndpoint Cmdlet Remove-EC2 (herramientas para Windows) PowerShell

Gestión del agente de seguridad automatizado para Fargate (solo Amazon ECS)

Configurar el GuardDuty agente para una cuenta independiente

Actualmente, Runtime Monitoring admite la administración del agente de seguridad para sus clústeres de Amazon ECS (AWS Fargate) únicamente a través de GuardDuty. No se admite la administración manual del agente de seguridad en los clústeres de Amazon ECS.

Console

1. Inicie sesión AWS Management Console y abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, selecciona Runtime Monitoring.
3. En la pestaña Configuración:

    a. Para gestionar la configuración de agentes automatizada para todos los clústeres de Amazon ECS (a nivel de cuenta)

    Seleccione Activar en la sección de configuración automática de agentes AWS Fargate (solo para ECS). Cuando se lance una nueva tarea de Fargate Amazon ECS, GuardDuty gestionará el despliegue del agente de seguridad.

    - Seleccione Guardar.

b. Para gestionar la configuración automática de los agentes excluyendo algunos de los clústeres de Amazon ECS (a nivel de clúster)

   i. Añada una etiqueta al clúster de Amazon ECS para la que desee excluir todas las tareas. El par clave-valor debe ser `GuardDutyManaged` -. `false`

   ii. Impida la modificación de estas etiquetas, excepto por parte de entidades de confianza. La política que se proporciona en Impedir que las etiquetas se modifiquen excepto según los principios autorizados en la Guía del AWS Organizations usuario se ha modificado para que sea aplicable aquí.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
```

```
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

iii. En la pestaña Configuración, seleccione Activar en la sección Configuración automática del agente.

> **Note**
>
> Añada siempre la etiqueta de exclusión a su clúster de Amazon ECS antes de habilitar la administración automática del GuardDuty agente en su cuenta; de lo contrario, el agente de seguridad se desplegará en todas las tareas que se lancen dentro del clúster de Amazon ECS correspondiente.

En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty gestionará el despliegue del agente de seguridad en el contenedor sidecar.

iv. Seleccione Guardar.

c. Para gestionar la configuración automatizada de los agentes mediante la inclusión de algunos de los clústeres de Amazon ECS (a nivel de clúster)

i. Añada una etiqueta a un clúster de Amazon ECS en el que desee incluir todas las tareas. El par clave-valor debe ser `GuardDutyManaged` -. `true`

ii. Impida la modificación de estas etiquetas, excepto por parte de entidades de confianza. La política que se proporciona en Impedir que las etiquetas se modifiquen excepto según los principios autorizados en la Guía del AWS Organizations usuario se ha modificado para que sea aplicable aquí.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

Configuración del GuardDuty agente para un entorno de múltiples cuentas

En un entorno de varias cuentas, solo la cuenta de GuardDuty administrador delegado puede habilitar o deshabilitar la configuración automatizada de agentes para las cuentas de los miembros y administrar la configuración automatizada de los agentes para los clústeres de Amazon ECS que pertenecen a las cuentas de los miembros de su organización. La cuenta de un GuardDuty miembro no puede modificar esta configuración. La cuenta de GuardDuty administrador delegado administra sus cuentas de miembros mediante AWS Organizations. Para obtener más información sobre los entornos de varias cuentas, consulte Administrar varias cuentas en. GuardDuty

Habilitar la configuración automática de agentes para la cuenta de administrador delegado GuardDuty

Manage for all Amazon ECS clusters (account level)

Si seleccionó Activar la supervisión en tiempo de ejecución para todas las cuentas, dispondrá de las siguientes opciones:

- Seleccione Activar para todas las cuentas en la sección de configuración automática del agente. GuardDuty desplegará y gestionará el agente de seguridad para todas las tareas de Amazon ECS que se inicien.
- Elija Configurar cuentas manualmente.

Si eligió Configurar las cuentas manualmente en la sección Supervisión del tiempo de ejecución, haga lo siguiente:

1. Elija Configurar las cuentas manualmente en la sección Configuración automatizada del agente.

2. Seleccione Activar en la sección de la cuenta de GuardDuty administrador delegado (esta cuenta).

Seleccione Guardar.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Añada una etiqueta a este clúster de Amazon ECS con el par clave-valor como `GuardDutyManaged` -. `false`
2. Impida la modificación de las etiquetas, excepto por parte de las entidades de confianza. La política que se proporciona en Impedir que las etiquetas se modifiquen excepto según los principios autorizados en la Guía del AWS Organizations usuario se ha modificado para que sea aplicable aquí.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
```

```
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
4. En el panel de navegación, elija Runtime Monitoring.
5.
> **Note**
>
> Añada siempre la etiqueta de exclusión a sus clústeres de Amazon ECS antes de activar la configuración automática de agentes en su cuenta; de lo contrario, el contenedor GuardDuty sidecar se adjuntará a todos los contenedores de las tareas de Amazon ECS que se lancen.

   En la pestaña Configuración, seleccione Activar en la configuración del agente automatizado.

   En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty gestionará el despliegue del agente de seguridad en el contenedor sidecar.
6. Seleccione Guardar.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Añada una etiqueta a un clúster de Amazon ECS en el que desee incluir todas las tareas. El par clave-valor debe ser `GuardDutyManaged` -. `true`
2. Impida la modificación de estas etiquetas, excepto por parte de entidades de confianza. La política que se proporciona en Impedir que las etiquetas se modifiquen excepto según los principios autorizados en la Guía del AWS Organizations usuario se ha modificado para que sea aplicable aquí.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
```

```
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
```

```
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Al utilizar etiquetas de inclusión para sus clústeres de Amazon ECS, no necesita habilitar el GuardDuty agente mediante la configuración automática de agentes de forma explícita.

Se habilita automáticamente para todas las cuentas de los miembros

Manage for all Amazon ECS clusters (account level)

En los siguientes pasos, se supone que seleccionó Activar para todas las cuentas en la sección Supervisión del tiempo de ejecución.

1. Seleccione Activar para todas las cuentas en la sección de configuración automática del agente. GuardDuty desplegará y gestionará el agente de seguridad para todas las tareas de Amazon ECS que se inicien.
2. Seleccione Guardar.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Añada una etiqueta a este clúster de Amazon ECS con el par clave-valor como `GuardDutyManaged` -. `false`

2. Impida la modificación de las etiquetas, excepto por parte de las entidades de confianza. La política que se proporciona en Impedir que las etiquetas se modifiquen excepto según los principios autorizados en la Guía del AWS Organizations usuario se ha modificado para que sea aplicable aquí.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
4. En el panel de navegación, elija Runtime Monitoring.
5.

> **Note**
>
> Añada siempre la etiqueta de exclusión a sus clústeres de Amazon ECS antes de activar la configuración automática de agentes en su cuenta; de lo contrario, el

contenedor GuardDuty sidecar se adjuntará a todos los contenedores de las tareas de Amazon ECS que se lancen.

En la pestaña Configuración, selecciona Editar.

6. Seleccione Activar para todas las cuentas en la sección de configuración automatizada del agente

   En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty gestionará el despliegue del agente de seguridad en el contenedor sidecar.

7. Seleccione Guardar.

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Independientemente de cómo elija habilitar Runtime Monitoring, los siguientes pasos le ayudarán a supervisar tareas selectivas de Amazon ECS Fargate para todas las cuentas de los miembros de su organización.

1. No habilite ninguna configuración en la sección de configuración automática de los agentes. Mantenga la configuración de Runtime Monitoring igual a la que seleccionó en el paso anterior.
2. Seleccione Guardar.
3. Impida la modificación de estas etiquetas, excepto por parte de entidades de confianza. La política que se proporciona en Impedir que las etiquetas se modifiquen excepto según los principios autorizados en la Guía del AWS Organizations usuario se ha modificado para que sea aplicable aquí.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
```

```
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
```

```
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Al usar etiquetas de inclusión para sus clústeres de Amazon ECS, no necesita habilitar la administración automática de GuardDuty agentes de forma explícita.

Habilitar la configuración automática de los agentes para las cuentas de miembros activos existentes

Manage for all Amazon ECS clusters (account level)

1. En la página de supervisión del tiempo de ejecución, en la pestaña Configuración, puede ver el estado actual de la configuración de los agentes automatizados.
2. En el panel de configuración de agentes automatizados, en la sección Cuentas de miembros activos, seleccione Acciones.
3. En Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
4. Seleccione Confirmar.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Añada una etiqueta a este clúster de Amazon ECS con el par clave-valor como `GuardDutyManaged` -. `false`

2. Impida la modificación de las etiquetas, excepto por parte de las entidades de confianza. La política que se proporciona en Impedir que las etiquetas se modifiquen excepto según los principios autorizados en la Guía del AWS Organizations usuario se ha modificado para que sea aplicable aquí.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
4. En el panel de navegación, elija Runtime Monitoring.
5.

> **Note**
>
> Añada siempre la etiqueta de exclusión a sus clústeres de Amazon ECS antes de activar la configuración automática de agentes en su cuenta; de lo contrario, el

contenedor GuardDuty sidecar se adjuntará a todos los contenedores de las tareas de Amazon ECS que se lancen.

En la pestaña Configuración, en la sección Configuración automatizada de agentes, en Cuentas de miembros activos, selecciona Acciones.

6. En Acciones, seleccione Habilitar para todas las cuentas de miembros activas.

   En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty gestionará el despliegue del agente de seguridad en el contenedor sidecar.

7. Seleccione Confirmar.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Añada una etiqueta a un clúster de Amazon ECS en el que desee incluir todas las tareas. El par clave-valor debe ser `GuardDutyManaged` -. `true`
2. Impida la modificación de estas etiquetas, excepto por parte de entidades de confianza. La política que se proporciona en Impedir que las etiquetas se modifiquen excepto según los principios autorizados en la Guía del AWS Organizations usuario se ha modificado para que sea aplicable aquí.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Al utilizar etiquetas de inclusión para sus clústeres de Amazon ECS, no necesita habilitar la configuración automática de agentes de forma explícita.

Habilite automáticamente la configuración automática de agentes para los nuevos miembros

Manage for all Amazon ECS clusters (account level)

1. En la página Runtime Monitoring, seleccione Editar para actualizar la configuración existente.
2. En la sección Configuración automatizada del agente, seleccione Activar automáticamente las cuentas de los nuevos miembros.
3. Seleccione Guardar.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Añada una etiqueta a este clúster de Amazon ECS con el par clave-valor como `GuardDutyManaged` -. `false`
2. Impida la modificación de las etiquetas, excepto por parte de las entidades de confianza. La política que se proporciona en Impedir que las etiquetas se modifiquen excepto según los principios autorizados en la Guía del AWS Organizations usuario se ha modificado para que sea aplicable aquí.

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

```
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
```

```
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
4. En el panel de navegación, elija Runtime Monitoring.
5.

> **Note**
>
> Añada siempre la etiqueta de exclusión a sus clústeres de Amazon ECS antes de activar la configuración automática de agentes en su cuenta; de lo contrario, el contenedor GuardDuty sidecar se adjuntará a todos los contenedores de las tareas de Amazon ECS que se lancen.

   En la pestaña Configuración, seleccione Activar automáticamente las cuentas de nuevos miembros en la sección Configuración automática de agentes.

   En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty gestionará el despliegue del agente de seguridad en el contenedor sidecar.
6. Seleccione Guardar.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Añada una etiqueta a un clúster de Amazon ECS en el que desee incluir todas las tareas. El par clave-valor debe ser `GuardDutyManaged` -. `true`
2. Impida la modificación de estas etiquetas, excepto por parte de entidades de confianza. La política que se proporciona en Impedir que las etiquetas se modifiquen excepto según los principios autorizados en la Guía del AWS Organizations usuario se ha modificado para que sea aplicable aquí.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
```

```
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Al utilizar etiquetas de inclusión para sus clústeres de Amazon ECS, no necesita habilitar la configuración automática de agentes de forma explícita.

Habilitar la configuración automática de agentes para las cuentas de los miembros activos de forma selectiva

Manage for all Amazon ECS (account level)

1. En la página Cuentas, seleccione las cuentas para las que desee habilitar la configuración automatizada de agentes de Runtime Monitoring (ECS-Fargate). Puede seleccionar varias cuentas. Asegúrese de que las cuentas que seleccione en este paso ya estén habilitadas con Runtime Monitoring.
2. En Editar planes de protección, elija la opción adecuada para habilitar la configuración automática de agentes de Runtime Monitoring (ECS-Fargate).
3. Seleccione Confirmar.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Añada una etiqueta a este clúster de Amazon ECS con el par clave-valor como `GuardDutyManaged` -. `false`
2. Impida la modificación de las etiquetas, excepto por parte de las entidades de confianza. La política que se proporciona en Impedir que las etiquetas se modifiquen excepto según los principios autorizados en la Guía del AWS Organizations usuario se ha modificado para que sea aplicable aquí.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
```

```
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
```

```
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
4. En el panel de navegación, elija Runtime Monitoring.
5.

> **Note**
>
> Añada siempre la etiqueta de exclusión a sus clústeres de Amazon ECS antes de habilitar la administración automática de GuardDuty agentes en su cuenta; de lo contrario, el contenedor GuardDuty sidecar se adjuntará a todos los contenedores de las tareas de Amazon ECS que se lancen.

   En la página Cuentas, seleccione las cuentas para las que desee habilitar la configuración automatizada de agentes de Runtime Monitoring (ECS-Fargate). Puede seleccionar varias cuentas. Asegúrese de que las cuentas que seleccione en este paso ya estén habilitadas con Runtime Monitoring.

   En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty gestionará el despliegue del agente de seguridad en el contenedor sidecar.
6. En Editar planes de protección, elija la opción adecuada para habilitar la configuración automática de agentes de Runtime Monitoring (ECS-Fargate).
7. Seleccione Guardar.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Asegúrese de no habilitar la configuración automatizada de agentes (o Runtime Monitoring-Automated Agent Configuration (ECS-Fargate)) para las cuentas seleccionadas que tienen los clústeres de Amazon ECS que desea monitorear.
2. Añada una etiqueta a un clúster de Amazon ECS en el que desee incluir todas las tareas. El par clave-valor debe ser `GuardDutyManaged` -. `true`
3. Impida la modificación de estas etiquetas, excepto por parte de entidades de confianza. La política que se proporciona en Impedir que las etiquetas se modifiquen excepto según los principios autorizados en la Guía del AWS Organizations usuario se ha modificado para que sea aplicable aquí.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
```

```
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Al utilizar etiquetas de inclusión para sus clústeres de Amazon ECS, no necesita habilitar la configuración automática de agentes de forma explícita.

Administración automática del agente de seguridad para los clústeres de Amazon EKS

Configuración del agente automatizado para una cuenta independiente

1. Inicie sesión en la GuardDuty consola AWS Management Console y ábrala en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, selecciona Runtime Monitoring.
3. En la pestaña Configuración, seleccione Habilitar para habilitar la configuración automática de agentes para su cuenta.

Método preferido para implementar un agente GuardDuty de seguridad	Pasos
Administre el agente de seguridad mediante GuardDuty (Supervisión de todos los clústeres de EKS)	1. Seleccione Activar en la sección de configuración automática del agente. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de EKS existentes y potencialmente nuevos de su cuenta. 2. Seleccione Guardar.
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	De los siguientes procedimientos, elija uno de los escenarios que le corresponda. Excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad no se haya desplegado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como `GuardDutyManaged` y su valor como `false`.

Método preferido para implementar un agente GuardDuty de seguridad	Pasos
	Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDuty Managed` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Abra la consola en https://console.aws.amazon.com/guardduty/ GuardDuty .

Método preferido para implementar un agente GuardDuty de seguridad	Pasos
	4. En el panel de navegación, elija Runtime Monitoring. **Note** Añada siempre la etiqueta de exclusión a sus clústeres de EKS antes de habilitar la administración automática del GuardDuty agente en su cuenta; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta. 5. En la pestaña Configuración, seleccione Activar en la sección de administración de GuardDuty agentes. En el caso de los clústeres de EKS que no se hayan excluido de la supervisión, GuardDuty gestionará el despliegue y las actualizaciones del agente GuardDuty de seguridad. 6. Seleccione Guardar. Excluir un clúster de EKS de la supervisión después de que el agente de GuardDuty seguridad ya se haya desplegado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como `GuardDutyManaged` y su valor como `false`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS.

Método preferido para implementar un agente GuardDuty de seguridad	Pasos
	Tras este paso, no GuardDuty actualizará el agente de seguridad de este clúster. Sin embargo, el agente de seguridad permanecerá desplegado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDuty Managed` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Método preferido para implementar un agente GuardDuty de seguridad	Pasos
	3. Para dejar de recibir eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado de este clúster de EKS. Para obtener más información acerca de la eliminación del agente de seguridad implementado, consulte Limpiar los recursos de los agentes de seguridad GuardDuty .

Método preferido para implementar un agente GuardDuty de seguridad	Pasos
Supervisión de determinados clústeres de EKS mediante etiquetas de inclusión	1. Asegúrese de seleccionar Inhabilitar en la sección de configuración automática del agente. Mantenga habilitada la supervisión del tiempo de ejecución. 2. Seleccione Guardar. 3. Agregue una etiqueta a este clúster de EKS con la clave como `GuardDutyManaged` y su valor como `true`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para los clústeres de EKS selectivos que desee supervisar. 4. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDutyManaged` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza.

Método preferido para implementar un agente GuardDuty de seguridad	Pasos
	Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Administración manual del agente	1. Asegúrese de seleccionar Inhabilitar en la sección de configuración automática del agente. Mantenga habilitada la supervisión del tiempo de ejecución. 2. Seleccione Guardar. 3. Para administrar el agente de seguridad, consulte Administración manual del agente de seguridad para el clúster Amazon EKS.

Configuración del agente automatizado para entornos con varias cuentas

En entornos con varias cuentas, solo la cuenta de GuardDuty administrador delegado puede habilitar o deshabilitar la configuración automática de agentes para las cuentas de los miembros y administrar el agente automatizado para los clústeres de EKS que pertenecen a las cuentas de los miembros de su organización. Las cuentas de GuardDuty los miembros no pueden modificar esta configuración desde sus cuentas. La cuenta de GuardDuty administrador delegado administra sus cuentas de miembros mediante AWS Organizations. Para más información sobre los entornos con varias cuentas, consulte Managing multiple accounts.

Configuración de la configuración automática del agente para la cuenta de administrador delegado GuardDuty

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
Administre el agente de seguridad mediante GuardDuty (Supervisión de todos los clústeres de EKS)	Si seleccionó Activar para todas las cuentas en la sección Supervisión del tiempo de ejecución, dispondrá de las siguientes opciones: • Seleccione Activar para todas las cuentas en la sección de configuración automatizada del agente. GuardDuty desplegará y gestionará el agente de seguridad para todos los clústeres de EKS que pertenezcan a la cuenta de GuardDuty administrador delegado y también para todos los clústeres de EKS que pertenezcan a todas las cuentas de miembros existentes y potencialmente nuevas de la organización. • Elija Configurar cuentas manualmente. Si seleccionó Configurar las cuentas manualmente en la sección Supervisión del tiempo de ejecución, haga lo siguiente: 1. Elija Configurar las cuentas manualmente en la sección Configuración automatizada del agente. 2. Seleccione Activar en la sección de la cuenta de GuardDuty administrador delegado (esta cuenta). Seleccione Guardar.
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante etiquetas de exclusión)	De los siguientes procedimientos, elija uno de los escenarios que se aplique a su situación. Para excluir un clúster de EKS de la supervisión cuando el agente GuardDuty de seguridad no se ha desplegado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como `GuardDutyManaged` y su valor como `false`.

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos

Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS.

2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes:

   - Sustituya *ec2: CreateTags* por. `eks:TagResource`
   - Sustituya *ec2: DeleteTags* por. `eks:UntagResource`
   - Sustituya *access-project* por `GuardDutyManaged` .
   - Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza.

     Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` :

     ```
     "aws:PrincipalArn":["arn:aws:iam::12345678901
     2:role/org-admins/iam-admin", "arn:aws:iam::1234
     56789012:role/org-admins/iam-admin", "arn:aws:
     iam::123456789012:role/org-admins/iam-admin"]
     ```

3. Abra la consola en https://console.aws.amazon.com/guardduty/ GuardDuty .
4. En el panel de navegación, elija Runtime Monitoring.

   > **Note**
   >
   > Añada siempre la etiqueta de exclusión a sus clústeres de EKS antes de habilitar la administración automática del GuardDuty agente en su cuenta; de lo contrario, el

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
	agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta. 5. En la pestaña Configuración, seleccione Activar en la sección de administración de GuardDuty agentes. En el caso de los clústeres de EKS que no se hayan excluido de la supervisión, GuardDuty gestionará el despliegue y las actualizaciones del agente GuardDuty de seguridad. 6. Seleccione Guardar. Excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad se ha desplegado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como `GuardDutyManaged` y su valor como `false`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *`ec2: CreateTags`* por. `eks:TagResource` • Sustituya *`ec2: DeleteTags`* por. `eks:UntagResource` • Sustituya *`access-project`* por `GuardDutyManaged` . • Sustituya *`123456789012`* por el Cuenta de AWS ID de la entidad de confianza.

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
	Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Si tenía el agente automatizado habilitado para este clúster de EKS, después de este paso, no GuardDuty actualizará el agente de seguridad de este clúster. Sin embargo, el agente de seguridad permanecerá desplegado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso. Para dejar de recibir eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado de este clúster de EKS. Para obtener más información sobre la eliminación del agente de seguridad implementado, consulte Limpiar los recursos de los agentes de seguridad GuardDuty . 4. Si administraba el agente de GuardDuty seguridad de este clúster de EKS de forma manual, consulteLimpiar los recursos de los agentes de seguridad GuardDuty .

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
Supervisión de determina dos clústeres de EKS mediante etiquetas de inclusión	Independientemente de cómo haya activado Runtime Monitoring, los siguientes pasos le ayudarán a monitorear algunos clústeres de EKS en su cuenta: 1. Asegúrese de seleccionar Inhabilitar la cuenta de GuardDuty administrador delegado (esta cuenta) en la sección Configura ción automática de agentes. Mantenga la configuración de Runtime Monitoring igual a la configurada en el paso anterior. 2. Seleccione Guardar. 3. Agregue una etiqueta a su clúster de EKS con la clave como `GuardDutyManaged` y su valor como `true`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturaci ón en la Guía del usuario de Amazon EKS. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para los clústeres de EKS selectivos que desee supervisar. 4. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *`ec2: CreateTags`* por. `eks:TagResource` • Sustituya *`ec2: DeleteTags`* por. `eks:UntagResource` • Sustituya *`access-project`* por `GuardDutyManaged` . • Sustituya *`123456789012`* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` :

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
	`"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Administre el agente de seguridad manualmente GuardDuty	Independientemente de cómo elija habilitar Runtime Monitoring, puede administrar el agente de seguridad manualmente para sus clústeres de EKS. 1. Asegúrese de seleccionar Inhabilitar la cuenta de GuardDuty administrador delegado (esta cuenta) en la sección de configuración automática del agente. Mantenga la configuración de Runtime Monitoring igual a la configurada en el paso anterior. 2. Seleccione Guardar. 3. Para administrar el agente de seguridad, consulte Administración manual del agente de seguridad para el clúster Amazon EKS.

Habilite automáticamente el agente automatizado para todas las cuentas de los miembros

> **Note**
>
> La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
Administre el agente de seguridad mediante GuardDuty (Supervisión de todos los clústeres de EKS)	En este tema se trata de habilitar la supervisión del tiempo de ejecución para todas las cuentas de los miembros y, por lo tanto, en los siguientes pasos se supone que debe haber elegido la opción Habilitar para todas las cuentas en la sección Supervisión del tiempo de ejecución. 1. Seleccione Activar para todas las cuentas en la sección de configuración automática del agente. GuardDuty desplegará y gestionará el agente de seguridad para todos los clústeres de EKS que pertenezcan a la cuenta de GuardDuty administr ador delegado y también para todos los clústeres de EKS que pertenezcan a todas las cuentas de miembros existentes y potencialmente nuevas de la organización. 2. Seleccione Guardar.
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante etiquetas de exclusión)	De los siguientes procedimientos, elija uno de los escenarios que se aplique a su situación. Excluir un clúster de EKS de la supervisión cuando el agente GuardDuty de seguridad no se haya desplegado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como `GuardDutyManaged` y su valor como `false`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource`

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos

- Sustituya *ec2: DeleteTags* por. `eks:UntagResource`
- Sustituya *access-project* por `GuardDutyManaged` .
- Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza.

  Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` :

```
"aws:PrincipalArn":["arn:aws:iam::12345678901
2:role/org-admins/iam-admin", "arn:aws:iam::1234
56789012:role/org-admins/iam-admin", "arn:aws:
iam::123456789012:role/org-admins/iam-admin"]
```

3. Abra la consola en https://console.aws.amazon.com/guardduty/ GuardDuty .
4. En el panel de navegación, elija Runtime Monitoring.

   > **Note**
   >
   > Añada siempre la etiqueta de exclusión a sus clústeres de EKS antes de activar el agente automatizado en su cuenta; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta.

5. En la pestaña Configuración, selecciona Editar en la sección de configuración de Runtime Monitoring.
6. Seleccione Activar para todas las cuentas en la sección de configuración automatizada del agente. En el caso de los clústeres de EKS que no se hayan excluido de la supervisión, GuardDuty gestionará el despliegue y las actualizaciones del agente GuardDuty de seguridad.
7. Seleccione Guardar.

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
	Excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad se ha desplegado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como `GuardDutyManaged` y su valor como `false`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. 2. Si tenía habilitada la configuración automática del agente para este clúster de EKS, después de este paso, no GuardDuty se actualizará el agente de seguridad de este clúster. Sin embargo, el agente de seguridad permanecerá desplegado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso. Para dejar de recibir eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado de este clúster de EKS. Para obtener más información sobre la eliminación del agente de seguridad implementado, consulte Limpiar los recursos de los agentes de seguridad GuardDuty . 3. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *`ec2: CreateTags`* por. `eks:TagResource` • Sustituya *`ec2: DeleteTags`* por. `eks:UntagResource` • Sustituya *`access-project`* por `GuardDutyManaged` . • Sustituya *`123456789012`* por el Cuenta de AWS ID de la entidad de confianza.

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
	Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 4. Si administraba el agente de GuardDuty seguridad de este clúster de EKS de forma manual, consulte. Limpiar los recursos de los agentes de seguridad GuardDuty

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
Supervisión de determina dos clústeres de EKS mediante etiquetas de inclusión	Independientemente de cómo haya activado Runtime Monitoring, los siguientes pasos le ayudarán a monitorear algunos clústeres de EKS para todas las cuentas de los miembros de su organización: 1. No habilite ninguna configuración en la sección de configura ción automatizada de agentes. Mantenga la configuración de Runtime Monitoring igual a la configurada en el paso anterior. 2. Seleccione Guardar. 3. Agregue una etiqueta a su clúster de EKS con la clave como `GuardDutyManaged` y su valor como `true`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturaci ón en la Guía del usuario de Amazon EKS. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para los clústeres de EKS selectivos que desee supervisar. 4. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *`ec2: CreateTags`* por. `eks:TagResource` • Sustituya *`ec2: DeleteTags`* por. `eks:UntagResource` • Sustituya *`access-project`* por `GuardDutyManaged` . • Sustituya *`123456789012`* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` :

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
	`"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Administre el agente de seguridad manualmente GuardDuty	Independientemente de cómo elija habilitar Runtime Monitoring, puede administrar el agente de seguridad manualmente para sus clústeres de EKS. 1. No habilite ninguna configuración en la sección de configuración automatizada del agente. Mantenga la configuración de Runtime Monitoring igual a la configurada en el paso anterior. 2. Seleccione Guardar. 3. Para administrar el agente de seguridad, consulte Administración manual del agente de seguridad para el clúster Amazon EKS.

Habilitar el agente automatizado para todas las cuentas de miembros activos existentes

> **Note**
>
> La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Para administrar el agente GuardDuty de seguridad para las cuentas de miembros activos existentes en su organización

- GuardDuty Para recibir los eventos en tiempo de ejecución de los clústeres de EKS que pertenecen a las cuentas de los miembros activos existentes en la organización, debe elegir el enfoque que prefiera para administrar el agente de GuardDuty seguridad de estos clústeres de

EKS. Para obtener más información acerca de cada uno de estos métodos, consulte Enfoques para administrar los agentes GuardDuty de seguridad.

Método preferido para administrar los agentes GuardDuty de seguridad	Pasos
Administre el agente de seguridad mediante GuardDuty (Supervisión de todos los clústeres de EKS)	Supervisión de todos los clústeres de EKS para todas las cuentas de miembros activas existentes 1. En la página de supervisión del tiempo de ejecución , en la pestaña Configuración, puede ver el estado actual de la configuración del agente automatizado. 2. En el panel de configuración de agentes automatizados, en la sección Cuentas de miembros activos, seleccione Acciones. 3. En Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes. 4. Seleccione Confirmar.

Método preferido para administrar los agentes GuardDuty de seguridad	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	De los siguientes procedimientos, elija uno de los escenarios que se aplique a su situación. Para excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad no se ha desplegado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como `GuardDutyManaged` y su valor como `false`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *`ec2: CreateTags`* por. `eks:TagResource` • Sustituya *`ec2: DeleteTags`* por. `eks:UntagResource` • Sustituya *`access-project`* por `GuardDutyManaged` . • Sustituya *`123456789012`* por el Cuenta de AWS ID de la entidad de confianza.

Método preferido para administrar los agentes GuardDuty de seguridad	Pasos
	Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Abra la consola en https://console.aws.amazon.com/guardduty/ GuardDuty . 4. En el panel de navegación, elija Runtime Monitoring. **Note** Añada siempre la etiqueta de exclusión a sus clústeres de EKS antes de activar la configuración automática de agentes en su cuenta; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta. 5. En la pestaña Configuración, en el panel de configuración automática del agente, en Cuentas de miembros activos, selecciona Acciones. 6. En Acciones, seleccione Habilitar para todas las cuentas de miembros activas. 7. Seleccione Confirmar.

Método preferido para administrar los agentes GuardDuty de seguridad	Pasos
	Para excluir un clúster de EKS de la supervisión después de que el agente de GuardDuty seguridad ya se haya desplegado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como `GuardDutyManaged` y su valor como `false`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. Tras este paso, no GuardDuty actualizará el agente de seguridad de este clúster. Sin embargo, el agente de seguridad permanecerá desplegado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDutyManaged` .

Método preferido para administrar los agentes GuardDuty de seguridad	Pasos
	• Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Independientemente de cómo administre el agente de seguridad (de forma manual GuardDuty o manual), para dejar de recibir los eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad desplegado de este clúster de EKS. Para obtener más información acerca de la eliminación del agente de seguridad implementado, consulte Limpiar los recursos de los agentes de seguridad GuardDuty .

Método preferido para administrar los agentes GuardDuty de seguridad	Pasos
Supervisión de determinados clústeres de EKS mediante etiquetas de inclusión	1. En la página Cuentas, después de activar la supervisión del tiempo de ejecución, no active la supervisión del tiempo de ejecución: configuración automática del agente. 2. Agregue una etiqueta al clúster de EKS que pertenezca a la cuenta seleccionada que desee supervisar. El par de clave-valor de la etiqueta debe ser `GuardDutyManaged -true`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para los clústeres de EKS selectivos que desee supervisar. 3. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDutyManaged` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza.

Método preferido para administrar los agentes GuardDuty de seguridad	Pasos
	Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Administre el agente de seguridad manualmente GuardDuty	1. Asegúrese de no seleccionar Activar en la sección de configuración automática del agente. Mantenga habilitada la supervisión del tiempo de ejecución. 2. Seleccione Guardar. 3. Para administrar el agente de seguridad, consulte Administración manual del agente de seguridad para el clúster Amazon EKS.

Habilite automáticamente la configuración automática de los agentes para los nuevos miembros

Enfoque preferido para administrar los agentes GuardDuty de seguridad	Pasos
Administre el agente de seguridad mediante GuardDuty (Supervisión de todos los clústeres de EKS)	1. En la página de supervisión del tiempo de ejecución , seleccione Editar para actualizar la configuración existente. 2. En la sección Configuración automatizada del agente, seleccione Activar automáticamente las cuentas de los nuevos miembros.

Enfoque preferido para administrar los agentes GuardDuty de seguridad	Pasos
	3. Seleccione Guardar.

Enfoque preferido para administrar los agentes GuardDuty de seguridad	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante etiquetas de exclusión)	De los siguientes procedimientos, elija uno de los escenarios que se aplique a su situación. Para excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad no se ha desplegado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como `GuardDutyManaged` y su valor como `false`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDutyManaged` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza.

Enfoque preferido para administrar los agentes GuardDuty de seguridad	Pasos

Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` :

```
"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
```

3. Abra la consola en https://console.aws.amazon.com/guardduty/ GuardDuty .
4. En el panel de navegación, elija Runtime Monitoring.

> **Note**
>
> Añada siempre la etiqueta de exclusión a sus clústeres de EKS antes de activar la configuración automática de agentes en su cuenta; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta.

5. En la pestaña Configuración, selecciona Activar automáticamente las cuentas de nuevos miembros en la sección de administración de GuardDuty agentes.

   En el caso de los clústeres de EKS que no se hayan excluido de la supervisión, GuardDuty gestionará el despliegue y las actualizaciones del agente GuardDuty de seguridad.
6. Seleccione Guardar.

Enfoque preferido para administrar los agentes GuardDuty de seguridad	Pasos
	Excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad se ha desplegado en este clúster 1. Independientemente de si administra el agente de GuardDuty seguridad de forma automática GuardDuty o manual, añada una etiqueta a este clúster de EKS con la clave como `GuardDutyManaged` y su valor como`false`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. Si tenía el agente automatizado habilitado para este clúster de EKS, después de este paso, no GuardDuty actualizará el agente de seguridad de este clúster. Sin embargo, el agente de seguridad permanece rá desplegado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso. Para dejar de recibir eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado de este clúster de EKS. Para obtener más información sobre la eliminación del agente de seguridad implementado, consulte Limpiar los recursos de los agentes de seguridad GuardDuty . 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la

Enfoque preferido para administrar los agentes GuardDuty de seguridad	Pasos
	Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDuty Managed` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Si administraba el agente de GuardDuty seguridad de este clúster de EKS de forma manual, consulte. Limpiar los recursos de los agentes de seguridad GuardDuty

Enfoque preferido para administrar los agentes GuardDuty de seguridad	Pasos
Supervisión de determinados clústeres de EKS mediante etiquetas de inclusión	Independientemente de cómo haya activado Runtime Monitoring, los siguientes pasos le ayudarán a monitorear algunos clústeres de EKS para las nuevas cuentas de los miembros de su organización. 1. Asegúrese de desactivar la opción Activar automáticamente las cuentas de nuevos miembros en la sección Configuración automática de agentes. Mantenga la configuración de Runtime Monitoring igual a la configurada en el paso anterior. 2. Seleccione Guardar. 3. Agregue una etiqueta a su clúster de EKS con la clave como `GuardDutyManaged` y su valor como `true`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para los clústeres de EKS selectivos que desee supervisar. 4. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource`

Enfoque preferido para administrar los agentes GuardDuty de seguridad	Pasos
	• Sustituya *access-project* por `GuardDuty Managed` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Administre el agente de seguridad manualmente GuardDuty	Independientemente de cómo elija habilitar Runtime Monitoring, puede administrar el agente de seguridad manualmente para sus clústeres de EKS. 1. Asegúrese de desactivar la casilla Activar automáticamente las cuentas de nuevos miembros en la sección Configuración automática de agentes. Mantenga la configuración de Runtime Monitoring igual a la configurada en el paso anterior. 2. Seleccione Guardar. 3. Para administrar el agente de seguridad, consulte Administración manual del agente de seguridad para el clúster Amazon EKS.

Configurar el agente automatizado para las cuentas de los miembros activos de forma selectiva

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
Administre el agente de seguridad mediante GuardDuty (Supervisión de todos los clústeres de EKS)	1. En la página Cuentas, seleccione las cuentas para las que desee habilitar la configuración automática del agente. Puede seleccionar más de una cuenta a la vez. Asegúrese de que las cuentas que seleccione en este paso ya tengan habilitada la supervisión en tiempo de ejecución de EKS. 2. En los planes de Edit Protection, elija la opción adecuada para activar la supervisión del tiempo de ejecución: configuración automática de agentes. 3. Seleccione Confirmar.
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante etiquetas de exclusión)	De los siguientes procedimientos, elija uno de los escenarios que se aplique a su situación. Para excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad no se ha desplegado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como `GuardDutyManaged` y su valor como `false`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDutyManaged` .

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos

- Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza.

  Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` :

  ```
  "aws:PrincipalArn":["arn:aws:iam::12345678901
  2:role/org-admins/iam-admin", "arn:aws:iam::1234
  56789012:role/org-admins/iam-admin", "arn:aws:
  iam::123456789012:role/org-admins/iam-admin"]
  ```

3. Abra la consola en https://console.aws.amazon.com/guardduty/ GuardDuty .

   > **Note**
   >
   > Añada siempre la etiqueta de exclusión a sus clústeres de EKS antes de activar la configuración automátic a del agente en su cuenta; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta.

4. En la página Cuentas, seleccione la cuenta para la que desee habilitar Administrar agente automáticamente. Puede seleccion ar más de una cuenta a la vez.
5. En Editar planes de protección, elija la opción adecuada para habilitar la configuración automática de agentes de Runtime Monitoring para la cuenta seleccionada.

   En el caso de los clústeres de EKS que no se hayan excluido de la supervisión, GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad. GuardDuty
6. Seleccione Guardar.

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
	Excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad se ha desplegado en este clúster 1. Agregue una etiqueta a este clúster de EKS con la clave como `GuardDutyManaged` y su valor como `false`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. Si anteriormente tenía habilitada la configuración del agente automatizado para este clúster de EKS, después de este paso, no GuardDuty actualizará el agente de seguridad de este clúster. Sin embargo, el agente de seguridad permanecerá desplegado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso. Para dejar de recibir eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado de este clúster de EKS. Para obtener más información sobre la eliminación del agente de seguridad implementado, consulte Limpiar los recursos de los agentes de seguridad GuardDuty . 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *`ec2: CreateTags`* por. `eks:TagResource` • Sustituya *`ec2: DeleteTags`* por. `eks:UntagResource` • Sustituya *`access-project`* por `GuardDutyManaged` . • Sustituya *`123456789012`* por el Cuenta de AWS ID de la entidad de confianza.

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
	Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Si administraba el agente de GuardDuty seguridad de este clúster de EKS de forma manual, debe eliminarlo. Para obtener más información, consulte Limpiar los recursos de los agentes de seguridad GuardDuty .

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
Supervisión de determina dos clústeres de EKS mediante etiquetas de inclusión	Independientemente de cómo haya activado Runtime Monitoring, los siguientes pasos le ayudarán a monitorear algunos clústeres de EKS que pertenecen a las cuentas seleccionadas: 1. Asegúrese de no habilitar la configuración de agentes automatizada de Runtime Monitoring para las cuentas seleccionadas que tienen los clústeres de EKS que desea monitorear. 2. Agregue una etiqueta a su clúster de EKS con la clave como `GuardDutyManaged` y su valor como `true`. Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte Etiquetado de los recursos para facturación en la Guía del usuario de Amazon EKS. Tras añadir la etiqueta, GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para los clústeres de EKS selectivos que desee supervisar. 3. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *`ec2: CreateTags`* por. `eks:TagResource` • Sustituya *`ec2: DeleteTags`* por. `eks:UntagResource` • Sustituya *`access-project`* por `GuardDutyManaged` . • Sustituya *`123456789012`* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` :

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
	`"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Administre el agente de seguridad manualmente GuardDuty	1. Mantenga la configuración de Runtime Monitoring igual a la configurada en el paso anterior. Asegúrese de no habilitar la configuración del agente Runtime Monitoring: Automated para ninguna de las cuentas seleccionadas. 2. Seleccione Confirmar. 3. Para administrar el agente de seguridad, consulte Administración manual del agente de seguridad para el clúster Amazon EKS.

Administración manual del agente de seguridad para el clúster Amazon EKS

En esta sección se describe cómo puede gestionar su agente complementario (GuardDuty agente) de Amazon EKS después de activar Runtime Monitoring. Para usar Runtime Monitoring, debe habilitar Runtime Monitoring y configurar el complemento Amazon EKS,`aws-guardduty-agent`. Realizar solo uno de estos dos pasos no ayudará a GuardDuty detectar posibles amenazas ni a generar hallazgos.

Requisitos previos para implementar un agente GuardDuty de seguridad

En esta sección se describen los requisitos previos para implementar manualmente el agente GuardDuty de seguridad en los clústeres de EKS. Antes de continuar, asegúrese de haber configurado Runtime Monitoring para sus cuentas. El agente GuardDuty de seguridad (complemento EKS) no funcionará si no configura Runtime Monitoring. Para obtener más información, consulte Habilitación GuardDuty de la supervisión del tiempo. Después de completar los siguientes pasos, consulte Implementación de un agente de seguridad GuardDuty .

Elija el método de acceso que prefiera para crear un punto de conexión de VPC de Amazon.

Console

Creación de un punto de conexión de VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en Nube virtual privada, seleccione Puntos de conexión.
3. Seleccione Crear punto de conexión.
4. En la página Crear punto de conexión, en Categoría de servicio, elija Otros servicios de punto de conexión.
5. En Nombre del servicio, escriba **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

   Asegúrese de sustituir *`us-east-1`* por la región correcta. Debe ser la misma región que el clúster de EKS que pertenece a su Cuenta de AWS ID.
6. Elija Verificar el servicio.
7. Una vez que el nombre del servicio se haya verificado correctamente, elija la VPC en la que reside el clúster. Agregue la siguiente política para restringir el uso de los puntos de conexión de VPC únicamente a la cuenta especificada. Con el valor de `Condition` de la organización que se indica debajo de esta política, puede actualizar la siguiente política para restringir el acceso a su punto de conexión. Para proporcionar compatibilidad con puntos de conexión de VPC a ID de cuentas específicos de su organización, consulte Organization condition to restrict access to your endpoint.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
```

```
    "Effect": "Deny",
    "Principal": "*"
  }
 ]
}
```

El ID de cuenta de `aws:PrincipalAccount` debe coincidir con la cuenta que contiene la VPC y el punto de conexión de VPC. En la siguiente lista se muestra cómo compartir el punto de conexión de VPC con otros ID de Cuenta de AWS :

Condición de la organización para restringir el acceso a su punto de conexión

- Si quiere especificar varias cuentas para acceder al punto de conexión de VPC, sustituya `"aws:PrincipalAccount": "111122223333"` por lo siguiente:

```
"aws:PrincipalAccount": [
          "666666666666",
          "555555555555"
    ]
```

- Para permitir que todos los miembros de una organización accedan al punto de conexión de VPC, sustituya `"aws:PrincipalAccount": "111122223333"` por lo siguiente:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- Para restringir el acceso a un recurso a un ID de organización, agregue su `ResourceOrgID` a la política.

  Para obtener más información, consulte ResourceOrgID.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. En Configuración adicional, seleccione Habilitar nombre de DNS.
9. En Subredes, elija las subredes en las que reside el clúster.
10. En Grupos de seguridad, elija un grupo de seguridad que tenga el puerto de entrada 443 habilitado desde su VPC (o su clúster de EKS). Si aún no tiene ningún grupo de seguridad que tenga habilitado el puerto de entrada 443, cree un grupo de seguridad.

Si se produce un problema al restringir los permisos de entrada a su VPC (o clúster), proporcione compatibilidad con el puerto de entrada 443 desde cualquier dirección IP (`0.0.0.0/0`).

API/CLI

- Invocar. CreateVpcEndpoint
- Utilice los siguientes valores para los parámetros:
  - En Nombre del servicio, escriba **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

    Asegúrese de sustituir *`us-east-1`* por la región correcta. Debe ser la misma región que el clúster de EKS que pertenece a su Cuenta de AWS ID.
  - Para DNSOptions, establezca la opción de DNS privado en `true` para habilitarla.
- Para ver AWS Command Line Interface, consulte create-vpc-endpoint.

Configurar los parámetros del agente de GuardDuty seguridad (complemento) para Amazon EKS

Puede configurar parámetros específicos de su agente de GuardDuty seguridad para Amazon EKS. Este soporte está disponible para la versión 1.5.0 y superior del agente de GuardDuty seguridad. Para obtener información sobre las últimas versiones de los complementos, consulteGuardDuty agente de seguridad para clústeres de Amazon EKS.

¿Por qué debo actualizar el esquema de configuración del agente de seguridad

El esquema de configuración del agente GuardDuty de seguridad es el mismo en todos los contenedores de los clústeres de Amazon EKS. Cuando los valores predeterminados no coincidan con las cargas de trabajo asociadas y el tamaño de la instancia, considere la posibilidad de configurar los ajustes de la CPU, la memoria y los `dnsPolicy` ajustes. `PriorityClass` Independientemente de cómo administre el GuardDuty agente para sus clústeres de Amazon EKS, puede configurar o actualizar la configuración existente de estos parámetros.

Comportamiento automatizado de la configuración del agente con parámetros configurados

Cuando GuardDuty administra el agente de seguridad (complemento EKS) en su nombre, actualiza el complemento según sea necesario. GuardDuty establecerá el valor de los parámetros

configurables en un valor predeterminado. Sin embargo, aún puede actualizar los parámetros al valor deseado. Si esto provoca un conflicto, la opción predeterminada para ResolveConflicts es. None

Parámetros y valores configurables

Para obtener información sobre los pasos para configurar los parámetros del complemento, consulte:

- Implementación de un agente de seguridad GuardDuty o
- Actualizar el agente de seguridad manualmente

Las siguientes tablas proporcionan los rangos y valores que puede usar para implementar el complemento Amazon EKS manualmente o actualizar la configuración del complemento existente.

Configuración de la CPU

Parámetros	Valor predeterminado	Rango configurable
Solicitudes	200m	Entre 200 m y 10000 m, ambos inclusive
Límites	1000m	

Ajustes de memoria

Parámetros	Valor predeterminado	Rango configurable
Solicitudes	256 Mi	Entre 256 Mi y 20000 Mi, ambos inclusive
Límites	1024 millas	

Configuración de **`PriorityClass`**

Cuando GuardDuty crea un complemento de Amazon EKS para usted, el asignado `PriorityClass` es`aws-guardduty-agent.priorityclass`. Esto significa que no se realizará ninguna acción en función de la prioridad del pod de agentes. Puede configurarlo eligiendo una de las siguientes `PriorityClass` opciones:

Configurable **`PriorityClass`**	Valor de **`preemptionPolicy`**	**`preemptionPolicy`** descripción	Valor del pod
`aws-guardduty-agent.priorityclass`	`Never`	Sin acciones	1000000
`aws-guardduty-agent.priorityclass-high`	`PreemptLowerPriority`	Al asignar este valor, se evitará que un pod se ejecute con un valor de prioridad inferior al valor del pod del agente.	100000000
`system-cluster-critical` [1]	`PreemptLowerPriority`		2000000000
`system-node-critical` [1]	`PreemptLowerPriority`		2000001000

[1] Kubernetes ofrece estas dos opciones: y. `PriorityClass` `system-cluster-critical` `system-node-critical` Para obtener más información, consulte la documentación de PriorityClassKubernetes.

Configuración de **`dnsPolicy`**

Elige una de las siguientes opciones de política de DNS compatibles con Kubernetes. Si no se especifica ninguna configuración, `ClusterFirst` se usa como valor predeterminado.

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

Para obtener información sobre estas políticas, consulta la Política de DNS de Pod en la documentación de Kubernetes.

Implementación de un agente de seguridad GuardDuty

En esta sección, se describe cómo implementar el agente GuardDuty de seguridad por primera vez en clústeres de EKS específicos. Antes de continuar con esta sección, asegúrese de haber configurado los requisitos previos y de haber activado Runtime Monitoring para sus cuentas. El agente GuardDuty de seguridad (complemento EKS) no funcionará si no habilita Runtime Monitoring.

Elija el método de acceso que prefiera para implementar el agente de GuardDuty seguridad por primera vez.

Console

1. Abra la consola de Amazon EKS en https://console.aws.amazon.com/eks/home#/clusters.
2. Elija un nombre para el clúster.
3. Elija la pestaña Complementos.
4. Escoja Obtener más complementos.
5. En la página Seleccionar complementos, selecciona Amazon GuardDuty Runtime Monitoring.
6. En la página Definir configuración del complemento seleccionado, utilice la configuración predeterminada. Si el estado de su complemento de EKS es Requiere activación, seleccione Activar GuardDuty. Esta acción abrirá la GuardDuty consola para configurar Runtime Monitoring para sus cuentas.
7. Una vez que haya configurado Runtime Monitoring para sus cuentas, vuelva a la consola Amazon EKS. El estado de su complemento de EKS debería haber cambiado a Listo para instalar.
8. (Opcional) Proporcionar el esquema de configuración del complemento EKS

   Para la versión complementaria, si elige la v1.5.0 o superior, Runtime Monitoring permite configurar parámetros específicos del GuardDuty agente. Para obtener información sobre los rangos de parámetros, consulte. Configure los parámetros del complemento EKS

   a. Amplíe los ajustes de configuración opcionales para ver los parámetros configurables y su valor y formato esperados.
   b. Defina los parámetros. Los valores deben estar en el rango indicado enConfigure los parámetros del complemento EKS.
   c. Seleccione Guardar cambios para crear el complemento en función de la configuración avanzada.

d. Para el método de resolución de conflictos, la opción que elija se utilizará para resolver un conflicto al actualizar el valor de un parámetro a un valor no predeterminado. Para obtener más información sobre las opciones de la lista, consulte ResolveConflicts en la referencia de la API de Amazon EKS.

9. Elija Siguiente.
10. En la página Revisar y crear, compruebe todos los detalles y elija Crear.
11. Vuelva a los detalles del clúster y elija la pestaña Recursos.
12. Puede ver los nuevos pods con el prefijo. aws-guardduty-agent

API/CLI

Puede configurar el agente del complemento de Amazon EKS (`aws-guardduty-agent`) mediante una de las siguientes opciones:

- Dirígete CreateAddona tu cuenta.
-

> **Note**
>
> En el caso del complemento`version`, si elige la versión 1.5.0 o superior, Runtime Monitoring permite configurar parámetros específicos del GuardDuty agente. Para obtener más información, consulte Configure los parámetros del complemento EKS.

Utilice los siguientes valores para los parámetros de la solicitud:

- En `addonName`, introduzca `aws-guardduty-agent`.

Puede usar el siguiente AWS CLI ejemplo cuando utilice valores configurables compatibles con las versiones del complemento v1.5.0 y posteriores. Asegúrese de reemplazar los valores marcadores de posición resaltados en rojo y los asociados a los valores `Example.json` configurados.

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

Example Ejemplo.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

- Para obtener más información sobre los valores de `addonVersion` admitidos, consulte Versiones de Kubernetes compatibles con el agente de seguridad GuardDuty .

- Como alternativa, puede usar. AWS CLI Para obtener más información, consulte create-addon.

Actualizar el agente de seguridad manualmente

Cuando gestionas el agente de GuardDuty seguridad manualmente, eres responsable de actualizarlo para tu cuenta. Para recibir notificaciones sobre nuevas versiones del agente, puede suscribirse a una fuente RSS enGuardDuty historial de versiones del agente.

Puede actualizar el agente de seguridad a la última versión para beneficiarse del soporte y las mejoras adicionales. Si su versión actual del agente está agotando el soporte estándar, para seguir utilizando Runtime Monitoring (o EKS Runtime Monitoring), debe actualizar su versión actual del agente. Para obtener información sobre las versiones de lanzamiento, consulteGuardDuty agente de seguridad para clústeres de Amazon EKS.

Requisito previo

Antes de actualizar la versión del agente de seguridad, asegúrese de que la versión del agente que planea usar ahora sea compatible con su versión de Kubernetes. Para obtener más información, consulte Versiones de Kubernetes compatibles con el agente de seguridad GuardDuty .

Console

1. Abra la consola de Amazon EKS en https://console.aws.amazon.com/eks/home#/clusters.
2. Elija un nombre para el clúster.
3. Selecciona Complementos.
4. En Complementos, selecciona Supervisión del GuardDuty tiempo de ejecución.
5. Seleccione Editar para actualizar los detalles del agente.
6. En la página Configurar la supervisión del GuardDuty tiempo de ejecución, actualice los detalles.
7. (Opcional) Actualizar los parámetros de configuración del complemento

   Si la versión del complemento EKS es la 1.5.0 o superior, también puede actualizar los ajustes de configuración del complemento.

   a. Amplíe los ajustes de configuración opcionales para ver el esquema de configuración.
   b. Actualice los valores de los parámetros en función del rango proporcionado enConfigure los parámetros del complemento EKS.
   c. Elija Guardar cambios para iniciar la actualización.
   d. En el caso del método de resolución de conflictos, la opción que elija se utilizará para resolver un conflicto al actualizar el valor de un parámetro a un valor no predeterminado. Para obtener más información sobre las opciones de la lista, consulte ResolveConflicts en la referencia de la API de Amazon EKS.

API/CLI

Para actualizar el agente GuardDuty de seguridad de sus clústeres de Amazon EKS, consulte Actualización de un complemento.

> **Note**
>
> Para el complemento`version`, si elige la versión 1.5.0 o superior, Runtime Monitoring permite configurar parámetros específicos del GuardDuty agente. Para obtener información sobre los rangos de parámetros, consulte. Configure los parámetros del complemento EKS

Puede utilizar el siguiente AWS CLI ejemplo cuando utilice valores configurables compatibles con las versiones del complemento v1.5.0 y posteriores. Asegúrese de reemplazar los valores marcadores de posición resaltados en rojo y los asociados a los valores `Example.json` configurados.

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

Example Ejemplo.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

Si la versión del complemento Amazon EKS es 1.5.0 o superior y ha configurado el esquema del complemento, puede comprobar si los valores aparecen correctamente o no en su clúster. Para obtener más información, consulte Verificar las actualizaciones del esquema de configuración.

Verificar las actualizaciones del esquema de configuración

Una vez configurados los parámetros, lleve a cabo los siguientes pasos para comprobar que el esquema de configuración se ha actualizado:

1. Abra la consola de Amazon EKS en https://console.aws.amazon.com/eks/home#/clusters.
2. En el panel de navegación, seleccione Clusters (Clústeres).
3. En la página Clústeres, seleccione el nombre del clúster cuyas actualizaciones desee comprobar.

4. Elija la pestaña Recursos.
5. En el panel Tipos de recursos, en Cargas de trabajo, elija DaemonSets.
6. Seleccione aws-guardduty-agent.
7. En la aws-guardduty-agentpágina, elija Vista sin procesar para ver la respuesta JSON sin formato. Compruebe que los parámetros configurables muestran el valor que ha proporcionado.

Tras la verificación, cambie a la GuardDuty consola. Seleccione el correspondiente Región de AWS y consulte el estado de cobertura de sus clústeres de Amazon EKS. Para obtener más información, consulte Cobertura para clústeres de Amazon EKS.

Configuración de EKS Runtime Monitoring (solo API)

Antes de configurar la supervisión en tiempo de ejecución de EKS en su cuenta, asegúrese de utilizar una de las plataformas verificadas que son compatibles con la versión de Kubernetes que se utiliza actualmente. Para obtener más información, consulte Validación de los requisitos de arquitectura.

Configuración de la supervisión en tiempo de ejecución de EKS para una cuenta independiente

Consulte las cuentas asociadas a AWS Organizations en Configuración de la supervisión en tiempo de ejecución de EKS para entornos con varias cuentas.

Elija su método de acceso preferido para habilitar la supervisión en tiempo de ejecución de EKS en su cuenta.

API/CLI

Según los Enfoques para administrar los agentes GuardDuty de seguridad, puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
Gestione el agente de seguridad mediante GuardDuty (supervise todos los clústeres de EKS)	1. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto `features`como `EKS_RUNTIME_MONITORING` y el estado como `ENABLED`. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta. 2. Como alternativa, puede usar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el ejemplo siguiente se habilita `EKS_RUNTIME_MONITORING` y `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es `GuardDutyManaged -false`. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS.

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
	2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDuty Managed` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** Añada siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor `STATUS` de `EKS_RUNTIME_MONITORING` en`ENABLED`; de lo contrario, el agente de

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
	GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto `features`como `EKS_RUNTIME_MONITORING` y el estado como `ENABLED`. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el ejemplo siguiente se habilita `EKS_RUNTIME_MONITORING` y `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
Supervisión de determinados clústeres de EKS (mediante una etiqueta de inclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es `GuardDutyManaged -true`. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDutyManaged` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
	3. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto `features`como `EKS_RUNTIME_MONITORING` y el estado como `ENABLED`. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `DISABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que se hayan etiquetado con el `true` par `GuardDutyManaged` -. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el siguiente ejemplo se habilita `EKS_RUNTIME_MONITORING` y se deshabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Enfoque preferido para administrar el agente GuardDuty de seguridad	Pasos
Administración manual del agente de seguridad	1. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto `features`como `EKS_RUNTIME_MONITORING` y el estado como `ENABLED`. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el siguiente ejemplo se habilita `EKS_RUNTIME_MONITORING` y se deshabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` 2. Para administrar el agente de seguridad, consulte Administración manual del agente de seguridad para el clúster Amazon EKS.

Configuración de la supervisión en tiempo de ejecución de EKS para entornos con varias cuentas

En entornos con varias cuentas, solo la cuenta de GuardDuty administrador delegado puede activar o desactivar EKS Runtime Monitoring para las cuentas de los miembros y gestionar la gestión de los GuardDuty agentes de los clústeres de EKS que pertenecen a las cuentas de los miembros de su organización. Las cuentas de GuardDuty los miembros no pueden modificar esta configuración desde sus cuentas. La cuenta de GuardDuty administrador delegado administra sus cuentas de miembros mediante AWS Organizations. Para más información sobre los entornos con varias cuentas, consulte Managing multiple accounts.

Configuración de EKS Runtime Monitoring para la cuenta de administrador delegado GuardDuty

Elija el método de acceso que prefiera para habilitar EKS Runtime Monitoring y administrar el agente de GuardDuty seguridad para los clústeres de EKS que pertenecen a la cuenta de GuardDuty administrador delegado.

API/CLI

Según los Enfoques para administrar los agentes GuardDuty de seguridad, puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
Gestione el agente de seguridad mediante GuardDuty (supervise todos los clústeres de EKS)	Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto `features`como `EKS_RUNTIME_MONITORING` y el estado como `ENABLED`. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta.

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
	Como alternativa, puede usar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el ejemplo siguiente se habilita `EKS_RUNTIME_MONITORING` y `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es `GuardDutyManaged -false`. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDuty Managed` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
	3. **Note** Añada siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor `STATUS` de `EKS_RUNTIME_MONITORING` en`ENABLED`; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto `features`como `EKS_RUNTIME_MONITORING` y el estado como `ENABLED`. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el ejemplo siguiente se habilita `EKS_RUNTIME_MONITORING` y `EKS_ADDON_MANAGEMENT` :

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
	`aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
Supervisión de determinados clústeres de EKS (mediante una etiqueta de inclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es `GuardDutyManaged -true`. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDuty Managed` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
	3. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto `features`como `EKS_RUNTIME_MONITORING` y el estado como `ENABLED`. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `DISABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que se hayan etiquetado con el `true` par `GuardDutyManaged` -. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el siguiente ejemplo se habilita `EKS_RUNTIME_MONITORING` y se deshabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
Administración manual del agente de seguridad	1. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto `features`como `EKS_RUNTIME_MONITORING` y el estado como `ENABLED`. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el siguiente ejemplo se habilita `EKS_RUNTIME_MONITORING` y se deshabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'` 2. Para administrar el agente de seguridad, consulte Administración manual del agente de seguridad para el clúster Amazon EKS.

Habilitación automática de la supervisión en tiempo de ejecución de EKS para todas las cuentas de miembros

Elija su método de acceso preferido para habilitar la supervisión en tiempo de ejecución de EKS en todas las cuentas de miembros. Esto incluye la cuenta de GuardDuty administrador delegado, las cuentas de los miembros existentes y las nuevas cuentas que se unen a la organización. Elija el enfoque que prefiera para administrar los agentes GuardDuty de seguridad de los clústeres de EKS que pertenecen a estas cuentas de miembros.

API/CLI

Según los Enfoques para administrar los agentes GuardDuty de seguridad, puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

Método preferido para administrar los agentes GuardDuty de seguridad	Pasos
Gestione el agente de seguridad mediante GuardDuty (supervise todos los clústeres de EKS)	Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio *ID de detector*. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta. Como alternativa, puede usar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el ejemplo siguiente se habilita `EKS_RUNTIME_MONITORING` y `EKS_ADDON_MANAGEMENT` :

Método preferido para administrar los agentes GuardDuty de seguridad	Pasos

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0    --account-
ids 111122223333  --features '[{"Name" : "EKS_RUNT
IME_MONITORING", "Status" : "  ENABLED", "Addition
alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT",
 "Status" : "ENABLED"}] ]'
```

> **Note**
>
> También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Método preferido para administrar los agentes GuardDuty de seguridad	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es `GuardDuty Managed -false`. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:Untag Resource` • Sustituya *access-project* por `GuardDutyManaged` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** Añada siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor `STATUS` de `EKS_RUNTIME_MONITORING` en`ENABLED`; de

Método preferido para administrar los agentes GuardDuty de seguridad	Pasos
	lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto `features`como `EKS_RUNTIME_MONITORING` y el estado como `ENABLED`. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el ejemplo siguiente se habilita `EKS_RUNTIME_MONITORING` y `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Método preferido para administrar los agentes GuardDuty de seguridad	Pasos
	> **Note** > También puede pasar una lista de ID de cuentas separadas por un espacio. Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Método preferido para administrar los agentes GuardDuty de seguridad	Pasos
Supervisión de determinados clústeres de EKS (mediante una etiqueta de inclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es `GuardDuty Managed -true`. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:Untag Resource` • Sustituya *access-project* por `GuardDutyManaged` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto `features`como `EKS_RUNTIME_MONITORING` y el estado como `ENABLED`. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `DISABLED`.

Método preferido para administrar los agentes GuardDuty de seguridad	Pasos
	GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que se hayan etiquetado con el `true` par `GuardDuty Managed` -. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el siguiente ejemplo se habilita `EKS_RUNTIME_MONITORING` y se deshabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** También puede pasar una lista de ID de cuentas separadas por un espacio. Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Método preferido para administrar los agentes GuardDuty de seguridad	Pasos
Administración manual del agente de seguridad	1. Ejecute la API updateDetector con su propio ID de detector regional y pase el nombre del objeto `features`como `EKS_RUNTIME_MONITORING` y el estado como `ENABLED`. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el siguiente ejemplo se habilita `EKS_RUNTIME_MONITORING` y se deshabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. Para administrar el agente de seguridad, consulte Administración manual del agente de seguridad para el clúster Amazon EKS.

Configuración de la supervisión en tiempo de ejecución de EKS para todas las cuentas de miembros activas existentes

Elija el método de acceso que prefiera para habilitar EKS Runtime Monitoring y administrar el agente de GuardDuty seguridad para las cuentas de los miembros activos existentes en su organización.

API/CLI

Según los Enfoques para administrar los agentes GuardDuty de seguridad, puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
Gestione el agente de seguridad mediante GuardDuty (supervise todos los clústeres de EKS)	Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio *ID de detector*. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta. Como alternativa, puede usar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el ejemplo siguiente se habilita `EKS_RUNTIME_MONITORING` y `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
	Note También puede pasar una lista de ID de cuentas separadas por un espacio. Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es `GuardDuty Managed -false`. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:Untag Resource` • Sustituya *access-project* por `GuardDutyManaged` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** Añada siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor `STATUS` de `EKS_RUNTIME_MONITORING` en`ENABLED`; de

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
	lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta. Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio *ID de detector*. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el ejemplo siguiente se habilita `EKS_RUNTIME_MONITORING` y `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
	> **Note** > También puede pasar una lista de ID de cuentas separadas por un espacio. Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
Supervisión de determinados clústeres de EKS (mediante una etiqueta de inclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es `GuardDuty Managed -true`. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:Untag Resource` • Sustituya *access-project* por `GuardDutyManaged` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio *ID de detector*.

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
	Establezca el estado de `EKS_ADDON_MANAGEMENT` como `DISABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que se hayan etiquetado con el `true` par `GuardDuty Managed` -. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el siguiente ejemplo se habilita `EKS_RUNTIME_MONITORING` y se deshabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** También puede pasar una lista de ID de cuentas separadas por un espacio. Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del

Método preferido para gestionar el agente GuardDuty de seguridad	Pasos
	detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.
Administración manual del agente de seguridad	1. Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio *ID de detector*. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el siguiente ejemplo se habilita `EKS_RUNTIME_MONITORING` y se deshabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. Para administrar el agente de seguridad, consulte Administración manual del agente de seguridad para el clúster Amazon EKS.

Habilitación automática de la supervisión en tiempo de ejecución de EKS para los nuevos miembros

La cuenta de GuardDuty administrador delegado puede habilitar automáticamente EKS Runtime Monitoring y elegir un enfoque para administrar el agente de GuardDuty seguridad para las nuevas cuentas que se unan a su organización.

API/CLI

Según los Enfoques para administrar los agentes GuardDuty de seguridad, puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

Método preferido para gestionar el agente de seguridad GuardDuty	Pasos
Gestione el agente de seguridad mediante GuardDuty (supervise todos los clústeres de EKS)	Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para las nuevas cuentas, invoque la operación de la API UpdateOrganizationConfiguration con su propio *ID de detector*. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta. Como alternativa, puede usar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el siguiente ejemplo se habilitan `EKS_RUNTIME_MONITORING` y `EKS_ADDON_MANAGEMENT` para una sola cuenta. También puede pasar una lista de ID de cuentas separadas por un espacio. Para encontrar la correspondiente `detectorId` a tu cuenta y a la región actual, consulta la página de

Método preferido para gestionar el agente de seguridad GuardDuty	Pasos
	configuración de la consola https://console.aws.amazon.com/guardduty/. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Método preferido para gestionar el agente de seguridad GuardDuty	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es `GuardDutyManaged -false`. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDutyManaged` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Método preferido para gestionar el agente de seguridad GuardDuty	Pasos
	3. **Note** Añada siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor `STATUS` de `EKS_RUNTIME_MONITORING` en`ENABLED`; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta. Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para las nuevas cuentas, invoque la operación de la API UpdateOrganizationConfiguration con su propio *`ID de detector`*. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el siguiente ejemplo se habilitan `EKS_RUNTIME_MONITORING` y `EKS_ADDON_MANAGEMENT`

Método preferido para gestionar el agente de seguridad GuardDuty	Pasos
	para una sola cuenta. También puede pasar una lista de ID de cuentas separadas por un espacio. Para encontrar la correspondiente `detectorId` a tu cuenta y a la región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Método preferido para gestionar el agente de seguridad GuardDuty	Pasos
Supervisión de determinados clústeres de EKS (mediante una etiqueta de inclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es `GuardDutyManaged -true`. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDutyManaged` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Método preferido para gestionar el agente de seguridad GuardDuty	Pasos
	3. Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para las nuevas cuentas, invoque la operación de la API UpdateOrganizationConfiguration con su propio *ID de detector*. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `DISABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que se hayan etiquetado con el `true` par `GuardDutyManaged` -. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el siguiente ejemplo se habilita `EKS_RUNTIME_MONITORING` y se deshabilita `EKS_ADDON_MANAGEMENT` para una sola cuenta. También puede pasar una lista de ID de cuentas separadas por un espacio. Para encontrar la correspondiente `detectorId` a tu cuenta y a la región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --feature`

Método preferido para gestionar el agente de seguridad GuardDuty	Pasos
	s '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}]]' Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Método preferido para gestionar el agente de seguridad GuardDuty	Pasos
Administración manual del agente de seguridad	1. Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para las nuevas cuentas, invoque la operación de la API UpdateOrganizationConfiguration con su propio *ID de detector*. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el siguiente ejemplo se habilita `EKS_RUNTIME_MONITORING` y se deshabilita `EKS_ADDON_MANAGEMENT` para una sola cuenta. También puede pasar una lista de ID de cuentas separadas por un espacio. Para encontrar la correspondiente `detectorId` a tu cuenta y a la región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'`

Método preferido para gestionar el agente de seguridad GuardDuty	Pasos
	Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema. 2. Para administrar el agente de seguridad, consulte Administración manual del agente de seguridad para el clúster Amazon EKS.

Habilitación de la Supervisión en tiempo de ejecución de EKS para cuentas de miembros activas individuales

API/CLI

Según los Enfoques para administrar los agentes GuardDuty de seguridad, puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

Método preferido para administrar el agente GuardDuty de seguridad	Pasos
Gestione el agente de seguridad mediante GuardDuty (supervise todos los clústeres de EKS)	Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio *`ID de detector`*. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta.

Método preferido para administrar el agente GuardDuty de seguridad	Pasos
	Como alternativa, puede usar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el ejemplo siguiente se habilita `EKS_RUNTIME_MONITORING` y `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'` **Note** También puede pasar una lista de ID de cuentas separadas por un espacio. Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Método preferido para administrar el agente GuardDuty de seguridad	Pasos
Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es `GuardDutyManaged -false`. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDuty Managed` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Método preferido para administrar el agente GuardDuty de seguridad	Pasos
	3. **Note** Añada siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor `STATUS` de `EKS_RUNTIME_MONITORING` en`ENABLED`; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta. Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio *`ID de detector`*. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el ejemplo siguiente se habilita `EKS_RUNTIME_MONITORING` y `EKS_ADDON_MANAGEMENT` :

Método preferido para administrar el agente GuardDuty de seguridad	Pasos
	`aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'` **Note** También puede pasar una lista de ID de cuentas separadas por un espacio. Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Método preferido para administrar el agente GuardDuty de seguridad	Pasos
Supervisión de determinados clústeres de EKS (mediante una etiqueta de inclusión)	1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es `GuardDutyManaged -true`. Para obtener más información sobre cómo agregar la etiqueta, consulte Uso de etiquetas mediante la CLI, la API o eksctl en la Guía del usuario de Amazon EKS. 2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en Impedir que las etiquetas se modifiquen excepto por entidades autorizadas en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: • Sustituya *ec2: CreateTags* por. `eks:TagResource` • Sustituya *ec2: DeleteTags* por. `eks:UntagResource` • Sustituya *access-project* por `GuardDutyManaged` . • Sustituya *123456789012* por el Cuenta de AWS ID de la entidad de confianza. Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Método preferido para administrar el agente GuardDuty de seguridad	Pasos
	3. Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio *ID de detector*. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `DISABLED`. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que se hayan etiquetado con el `true` par `GuardDutyManaged` -. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el siguiente ejemplo se habilita `EKS_RUNTIME_MONITORING` y se deshabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Método preferido para administrar el agente GuardDuty de seguridad	Pasos
	> **Note** > También puede pasar una lista de ID de cuentas separadas por un espacio. Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Método preferido para administrar el agente GuardDuty de seguridad	Pasos
Administración manual del agente de seguridad	1. Para habilitar o deshabilitar la supervisión en tiempo de ejecución de EKS de forma selectiva para sus cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio *ID de detector*. Establezca el estado de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. En el siguiente ejemplo se habilita `EKS_RUNTIME_MONITORING` y se deshabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. Para administrar el agente de seguridad, consulte Administración manual del agente de seguridad para el clúster Amazon EKS.

Migración de EKS Runtime Monitoring a Runtime Monitoring

Con el lanzamiento de GuardDuty Runtime Monitoring, la cobertura de detección de amenazas se ha ampliado a los contenedores de Amazon ECS y a las instancias de Amazon EC2. El monitoreo en tiempo de ejecución de EKS ahora se ha consolidado en Runtime Monitoring. Puede habilitar Runtime Monitoring y administrar agentes de GuardDuty seguridad individuales para cada tipo de recurso (instancia de Amazon EC2, clúster de Amazon ECS y clúster de Amazon EKS) cuyo comportamiento en tiempo de ejecución desee supervisar.

No existe una experiencia de GuardDuty consola independiente para EKS Runtime Monitoring. Para seguir utilizando EKS Runtime Monitoring, debe configurarlo mediante las API o el AWS Command Line Interface.

Para migrar de EKS Runtime Monitoring a Runtime Monitoring

1. La GuardDuty consola es compatible con EKS Runtime Monitoring como parte de Runtime Monitoring.

   Puede empezar a utilizar Runtime Monitoring desde su organización y sus cuentas. Comprobación del estado de configuración de EKS Runtime Monitoring

   Asegúrese de no deshabilitar EKS Runtime Monitoring antes de activar Runtime Monitoring. Si deshabilita EKS Runtime Monitoring, también se deshabilitará la administración de complementos de Amazon EKS. Continúe con los siguientes pasos en el orden indicado.
2. Asegúrese de cumplir con todos losRequisitos previos para habilitar Runtime Monitoring.
3. Habilite el monitoreo del tiempo de ejecución replicando los mismos ajustes de configuración de la organización para el monitoreo del tiempo de ejecución que tiene para el monitoreo del tiempo de ejecución de EKS. Para obtener más información, consulte Habilitación de la supervisión del tiempo.
   - Si tiene una cuenta independiente, debe habilitar Runtime Monitoring.

     Si su agente de GuardDuty seguridad ya está desplegado, los ajustes correspondientes se replican automáticamente y no es necesario volver a configurarlos.
   - Si tiene una organización con una configuración de activación automática, asegúrese de replicar la misma configuración de activación automática para Runtime Monitoring.
   - Si tiene una organización con ajustes configurados individualmente para las cuentas de los miembros activos existentes, asegúrese de habilitar Runtime Monitoring y configurar el agente de GuardDuty seguridad para estos miembros de forma individual.

4. Una vez que se haya asegurado de que la configuración de Runtime Monitoring y del agente de GuardDuty seguridad es correcta, desactive EKS Runtime Monitoring mediante la API o el AWS CLI comando.
5. (Opcional) si desea limpiar cualquier recurso asociado al agente GuardDuty de seguridad, consulteLimpiar los recursos de los agentes de seguridad GuardDuty .

Si desea seguir utilizando EKS Runtime Monitoring sin activar Runtime Monitoring, consulteConfiguración de EKS Runtime Monitoring (solo API).

Comprobación del estado de configuración de EKS Runtime Monitoring

Utilice las siguientes API o AWS CLI comandos para comprobar el estado de configuración actual de EKS Runtime Monitoring.

Para comprobar el estado de configuración actual de EKS Runtime Monitoring en su cuenta

- Ejecute GetDetectorpara comprobar el estado de configuración de su propia cuenta.
- Como alternativa, puede ejecutar el siguiente comando mediante AWS CLI:

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1
```

  Asegúrese de reemplazar el ID del detector de su región Cuenta de AWS y el de la región actual. Para encontrar el `detectorId` de su cuenta y su región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

Para comprobar el estado de la configuración actual de EKS Runtime Monitoring en su organización (solo como cuenta de GuardDuty administrador delegado)

- Ejecute DescribeOrganizationConfigurationpara comprobar el estado de configuración de su organización.

  Como alternativa, puede ejecutar el siguiente comando mediante AWS CLI:

```
aws guardduty describe-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

Asegúrese de sustituir el ID del detector por el ID del detector de su cuenta de GuardDuty administrador delegado y la región por la región actual. Para encontrar el de `detectorId` su cuenta y su región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

Desactivar EKS Runtime Monitoring después de migrar a Runtime Monitoring

Una vez que se haya asegurado de que la configuración existente de su cuenta u organización se ha replicado en Runtime Monitoring, puede deshabilitar EKS Runtime Monitoring.

Para deshabilitar EKS Runtime Monitoring

- Para deshabilitar EKS Runtime Monitoring en su propia cuenta

  Ejecute la UpdateDetectorAPI con su propio identificador de *detector regional.*

  Como alternativa, puedes usar el siguiente AWS CLI comando. *Sustituya 12abc34d567e8fa901bc2d34e56789f0 por su propio identificador de detector regional.*

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "DISABLED"}]'
```

- Para deshabilitar EKS Runtime Monitoring para las cuentas de los miembros de su organización

  Ejecute la UpdateMemberDetectorsAPI con el *identificador de detector regional* de la cuenta de GuardDuty administrador delegado de la organización.

  Como alternativa, puede usar el siguiente comando. AWS CLI *Sustituya 12abc34d567e8fa901bc2d34e56789f0 por el identificador del detector regional de la cuenta de administrador delegado GuardDuty de la organización y 111122223333 por el ID de la cuenta de miembro para la que desea deshabilitar esta función.* Cuenta de AWS

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
 "Status" : "DISABLED"}]'
```

- Para actualizar la configuración de EKS Runtime Monitoring para su organización, active automáticamente

  Realice el siguiente paso solo si ha configurado los ajustes de activación automática de EKS Runtime Monitoring para las cuentas de miembros nuevas (`NEW`) o todas (`ALL`) de la organización. Si ya lo ha configurado como`NONE`, puede omitir este paso.

  > **Note**
  >
  > Establecer la configuración de activación automática de EKS Runtime Monitoring `NONE` significa que EKS Runtime Monitoring no se habilitará automáticamente para ninguna cuenta de miembro existente o cuando una nueva cuenta de miembro se una a su organización.

  Ejecute la UpdateOrganizationConfigurationAPI con el *`identificador de detección`* regional de la cuenta de GuardDuty administrador delegado de la organización.

  Como alternativa, puede usar el siguiente comando. AWS CLI *`Sustituya 12abc34d567e8fa901bc2d34e56789f0 por el identificador de detector regional de la cuenta de administrador delegado de la organización.`* GuardDuty Sustituya el *`EXISTING_VALUE`* por su configuración actual para la activación automática. GuardDuty

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
   --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
  ```

Limpiar los recursos de los agentes de seguridad GuardDuty

Debe limpiar los recursos en los escenarios siguientes:

Al deshabilitar la configuración automática de los agentes

GuardDuty no elimina el agente de seguridad que está desplegado en el recurso. Sin embargo, GuardDuty dejará de administrar las actualizaciones del agente de seguridad.

GuardDuty sigue recibiendo los eventos de tiempo de ejecución de su tipo de recurso. Para evitar que sus estadísticas de uso se vean afectadas, asegúrese de eliminar el agente de GuardDuty seguridad del recurso.

Ya sea que Cuenta de AWS utilice o no un punto de enlace de VPC compartido, GuardDuty no elimina el punto de enlace de VPC. Si es necesario, tendrá que eliminar el punto final de la VPC manualmente.

Al deshabilitar Runtime Monitoring o EKS Runtime Monitoring

En general, GuardDuty elimina el punto final de la VPC que había creado. GuardDuty los etiqueta como`GuardDutyManaged`:. `true` Sin embargo, al deshabilitar Runtime Monitoring o EKS Runtime Monitoring para una cuenta participante de VPC compartida, si el punto final de VPC compartido lo ha utilizado al menos una cuenta participante, no se GuardDuty elimina el punto final de VPC ni el grupo de seguridad asociado al recurso de VPC compartido.

Cuando dejas de administrar el agente de seguridad manualmente

Independientemente del enfoque que utilice para implementar y administrar el agente de GuardDuty seguridad, para dejar de supervisar los eventos de tiempo de ejecución en su recurso, debe eliminar el agente GuardDuty de seguridad. Si desea dejar de monitorizar los eventos de tiempo de ejecución desde un tipo de recurso de una cuenta, también puede eliminar el punto de enlace de Amazon VPC.

Proceso para limpiar los recursos de los agentes de seguridad

Eliminación del punto de conexión de VPC de Amazon

- Sin una VPC compartida: cuando ya no desee supervisar un recurso de una cuenta, considere la posibilidad de eliminar el punto de enlace de Amazon VPC.
- Con una VPC compartida: cuando la cuenta de propietario de la VPC compartida elimina el recurso de la VPC compartida, cualquier cuenta de participante que utilice actualmente el punto de enlace de la VPC compartida, el estado de cobertura de Runtime Monitoring para los recursos de su cuenta de propietario de la VPC compartida y la cuenta participante puede dejar de estar en buen estado. Para obtener más información, consulte Evaluar la cobertura del tiempo de ejecución de sus recursos.

Para obtener más información, consulte Eliminación de un punto de conexión de interfaz.

Para eliminar el grupo de seguridad

- Sin una VPC compartida: cuando ya no desee supervisar un tipo de recurso en una cuenta, considere la posibilidad de eliminar el grupo de seguridad asociado a la Amazon VPC.
- Con una VPC compartida: cuando la cuenta del propietario de la VPC compartida elimina el grupo de seguridad, cualquier cuenta participante que utilice actualmente el grupo de seguridad asociado a la VPC compartida, el estado de cobertura de Runtime Monitoring para los recursos de su cuenta de propietario de la VPC compartida y la cuenta participante pueden dejar de estar en buen estado. Para obtener más información, consulte Evaluar la cobertura del tiempo de ejecución de sus recursos.

Para obtener más información, consulte Eliminar un grupo de seguridad.

Para eliminar el agente GuardDuty de seguridad de un clúster de EKS

Para eliminar el agente de seguridad del clúster de EKS que ya no desea supervisar, consulte Eliminar un complemento.

Al eliminar el agente del complemento de EKS, no se elimina el espacio de nombres `amazon-guardduty` del clúster de EKS. Para eliminar el espacio de nombres `amazon-guardduty`, consulte Deleting a namespace.

Para eliminar el espacio de **`amazon-guardduty`** nombres (clúster EKS)

Al deshabilitar la configuración automática del agente, no se elimina automáticamente el espacio de `amazon-guardduty` nombres del clúster de EKS. Para eliminar el espacio de nombres `amazon-guardduty`, consulte Deleting a namespace.

Evaluar la cobertura del tiempo de ejecución de sus recursos

Tras activar Runtime Monitoring y desplegar el agente de GuardDuty seguridad en el recurso, GuardDuty proporciona estadísticas de cobertura para el tipo de recurso correspondiente y el estado de cobertura individual de los recursos que pertenecen a su cuenta. El estado de la cobertura se determina asegurándose de que ha habilitado Runtime Monitoring, de que se ha creado su punto de enlace de Amazon VPC y de que se ha implementado el agente de GuardDuty seguridad del recurso correspondiente. Un estado de cobertura en buen estado indica que, cuando hay un evento de tiempo de ejecución relacionado con su recurso, GuardDuty puede recibir dicho evento de tiempo de ejecución a través del punto de enlace de Amazon VPC y monitorear el comportamiento. Si se produjo un problema al configurar Runtime Monitoring, crear un punto de enlace de Amazon VPC

o implementar el agente de GuardDuty seguridad, el estado de la cobertura aparece como En mal estado. Cuando el estado de la cobertura no sea adecuado, no GuardDuty podrá recibir ni monitorear el comportamiento en tiempo de ejecución del recurso correspondiente ni generar ningún resultado de monitorización del tiempo de ejecución.

Los siguientes temas le ayudarán a revisar las estadísticas de cobertura, configurar EventBridge las notificaciones y solucionar los problemas de cobertura de un tipo de recurso específico.

Contenido

Cobertura para la instancia Amazon EC2

En el caso de un recurso de Amazon EC2, la cobertura del tiempo de ejecución se evalúa a nivel de instancia. Sus instancias de Amazon EC2 pueden ejecutar varios tipos de aplicaciones y cargas de trabajo, entre otros, en su entorno. AWS Esta función también es compatible con las instancias Amazon EC2 administradas por Amazon ECS y, si tiene clústeres de Amazon ECS ejecutándose en una instancia de Amazon EC2, los problemas de cobertura a nivel de instancia se mostrarán en la cobertura de tiempo de ejecución de Amazon EC2.

Temas

Revisión de las estadísticas de cobertura

Las estadísticas de cobertura de las instancias de Amazon EC2 asociadas a sus propias cuentas o a las cuentas de sus miembros representan el porcentaje de instancias EC2 en buen estado entre todas las instancias de EC2 seleccionadas. Región de AWS La siguiente ecuación lo representa de la siguiente manera:

(Instancias en buen estado o todas las instancias) *100

Si también ha implementado el agente de GuardDuty seguridad para sus clústeres de Amazon ECS, cualquier problema de cobertura a nivel de instancia asociado a los clústeres de Amazon ECS que se ejecuten en una instancia de Amazon EC2 aparecerá como un problema de cobertura del tiempo de ejecución de una instancia de Amazon EC2.

Elija uno de los métodos de acceso para revisar las estadísticas de cobertura de sus cuentas.

Console

- Inicie sesión en la GuardDuty consola AWS Management Console y ábrala en https://console.aws.amazon.com/guardduty/.
- En el panel de navegación, selecciona Runtime Monitoring.
- Seleccione la pestaña Cobertura del tiempo de ejecución.
- En la pestaña Cobertura del tiempo de ejecución de la instancia EC2, puede ver las estadísticas de cobertura agregadas por el estado de cobertura de cada instancia de Amazon EC2 que está disponible en la tabla de lista de instancias.
  - Puede filtrar la tabla de listas de instancias por las siguientes columnas:
    - ID de cuenta
    - Tipo de administración del agente
    - Versión del agente
    - Estado de la cobertura
    - ID de instancia
    - ARN de clúster
- Si alguna de sus instancias EC2 tiene el estado de cobertura en mal estado, la columna Problema incluye información adicional sobre el motivo del estado en mal estado.

API/CLI

- Ejecute la ListCoverageAPI con su propio ID de detector válido, la región actual y el punto de conexión del servicio. Puedes filtrar y ordenar la lista de instancias con esta API.
  - Puede cambiar el ejemplo de `filter-criteria` con una de las siguientes opciones para `CriterionKey`:
    - `ACCOUNT_ID`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`

    - AGENT_VERSION
    - MANAGEMENT_TYPE
    - INSTANCE_ID
    - CLUSTER_ARN
  - Cuando se `filter-criteria` incluye `RESOURCE_TYPE` como EC2, Runtime Monitoring no admite el uso de ISSUE como. `AttributeName` Si lo usa, la respuesta de la API generará. `InvalidInputException`

    Puede cambiar el ejemplo de `AttributeName` en `sort-criteria` con las siguientes opciones:

    - ACCOUNT_ID
    - COVERAGE_STATUS
    - INSTANCE_ID
    - UPDATED_AT
  - Puede cambiar el valor de *`max-results`* (hasta 50).
  - Para encontrar la correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Ejecute la GetCoverageStatisticsAPI para recuperar las estadísticas agregadas de cobertura basadas en`statisticsType`.
  - Puede cambiar el ejemplo de `statisticsType` a una de las siguientes opciones:
    - COUNT_BY_COVERAGE_STATUS: representa las estadísticas de cobertura de los clústeres de EKS agregadas por estado de cobertura.
    - COUNT_BY_RESOURCE_TYPE— Estadísticas de cobertura agregadas en función del tipo de AWS recurso de la lista.
    - Puede cambiar el ejemplo de `filter-criteria` en el comando. Puede usar las siguientes opciones para `CriterionKey`:
      - ACCOUNT_ID

- `RESOURCE_TYPE`
- `COVERAGE_STATUS`
- `AGENT_VERSION`
- `MANAGEMENT_TYPE`
- `INSTANCE_ID`
- `CLUSTER_ARN`

- Para encontrar las correspondientes `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Si el estado de cobertura de su instancia EC2 es Incorrecto, consulteSolución de problemas de cobertura.

Configuración de las notificaciones de cambio de estado de cobertura

El estado de cobertura de su instancia de Amazon EC2 puede aparecer como En mal estado. Para saber cuándo cambia el estado de la cobertura, le recomendamos que supervise el estado de la cobertura periódicamente y que solucione los problemas si el estado pasa a ser insalubre. Como alternativa, puedes crear una EventBridge regla de Amazon para recibir una notificación cuando el estado de la cobertura cambie de Insalubre a Saludable o no. De forma predeterminada, la GuardDuty publica en el EventBridge bus de tu cuenta.

Ejemplo de esquema de notificaciones

Como EventBridge regla general, puede utilizar los ejemplos de eventos y patrones de eventos predefinidos para recibir la notificación del estado de la cobertura. Para obtener más información sobre cómo crear una EventBridge regla, consulta Crear regla en la Guía del EventBridge usuario de Amazon.

Además, puede crear un patrón de eventos personalizado mediante el siguiente ejemplo de esquema de notificaciones. Asegúrese de sustituir los valores de su cuenta. Para recibir una notificación cuando el estado de cobertura de su instancia de Amazon EC2 cambie de `Healthy` aUnhealthy, `detail-type` debería indicar *`GuardDuty Runtime Protection`* Unhealthy. Para

recibir una notificación cuando el estado de la cobertura cambie de `Unhealthy` a`Healthy`, sustituya el valor de `detail-type` por *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Cuenta de AWS ID",
  "time": "event timestamp (string)",
  "region": "Región de AWS",
  "resources": [
      ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EC2",
        "ec2InstanceDetails": {
          "instanceId":"",
          "instanceType":"",
          "clusterArn": "",
          "agentDetails": {
            "version":""
          },
          "managementType":""
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Solución de problemas de cobertura

Si el estado de la cobertura de su instancia de Amazon EC2 es Incorrecto, puede ver el motivo en la columna Problema.

En la siguiente tabla se enumeran los tipos de problemas y los pasos de solución de problemas correspondientes.

Tipo de problema	Mensaje de emisión	Pasos para la solución de problemas
No hay ningún agente que denuncie	Esperando la notificación de SSM	Asegúrese de que la instancia de Amazon EC2 ya esté gestionada por SSM. La recepción de la notificación de SSM puede tardar unos minutos.
	(Vacía a propósito)	Si administra el agente GuardDuty de seguridad manualmente, esto no es posible.
		Si ha activado la configuración automática del agente: • Su instancia EC2 está gestionada por SSM. • Consulte periódicamente el estado de su agente de seguridad. Para obtener más información, consulte Validación del estado de instalación GuardDuty del agente de seguridad.
	Agente desconectado	• Vea el estado de su agente de seguridad. Para obtener más información, consulte Validación del estado de instalación GuardDuty del agente de seguridad. • Consulte los registros de los agentes de seguridad para identificar la posible causa raíz. Los registros proporcionan errores detallados que puede utilizar para solucionar el problema usted mismo. Los archivos de registro están disponibles en. `/var/log/amzn-guardduty-agent/` Realice `sudo journalctl -u amazon-guardduty-agent` .
Falló la creación de la asociación SSM	GuardDuty La asociación SSM ya existe en su cuenta	1. Elimine la asociación existente manualmente. Para obtener más información, consulte Eliminar asociaciones en la Guía del AWS Systems Manager usuario. 2. Tras eliminar la asociación, deshabilite y vuelva a habilitar la configuración GuardDuty automática del agente para Amazon EC2.

Tipo de problema	Mensaje de emisión	Pasos para la solución de problemas
	Su cuenta tiene demasiadas asociaciones de SSM	Elige una de las dos opciones siguientes: • Elimine las asociaciones de SSM que no se utilicen. Para obtener más información, consulte Eliminar asociaciones en la Guía del AWS Systems Manager usuario. • Compruebe si su cuenta es apta para un aumento de cuota. Para obtener más información, consulte Cuotas de Systems Manager Service en Referencia general de AWS.
Falló la actualización de la asociación de SSM	GuardDuty La asociación SSM no existe en su cuenta	Falta la asociación SSM. Deshabilite y, a continuación, vuelva a activar Runtime Monitoring.
Falló la eliminación de la asociación SSM	GuardDuty La asociación SSM no existe en su cuenta	Falta la asociación SSM. Esto no es procesable.

Tipo de problema	Mensaje de emisión	Pasos para la solución de problemas
Falló la ejecución de la asociación de instancias de SSM	No se cumplen los requisitos arquitectónicos u otros requisitos previos.	Para obtener información sobre las distribuciones de sistemas operativos verificadas, consulte. Requisitos previos para la compatibilidad con instancias Amazon EC2 Si sigue teniendo este problema, los siguientes pasos le ayudarán a identificarlo y, si es posible, a resolverlo: 1. Abre la AWS Systems Manager consola en https://console.aws.amazon.com/systems-manager/. 2. En el panel de navegación, en Administración de nodos, seleccione State Manager. 3. Filtre por propiedad de nombre de documento e introdúzcala AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin. 4. Seleccione el ID de asociación correspondiente y consulte su historial de ejecución. 5. Utilice el historial de ejecución para ver los errores, identificar la posible causa raíz e intentar resolverla.
No se pudo crear el punto final de la VPC	No se admite la creación de puntos de conexión de VPC para la VPC compartida *vpcId*	Runtime Monitoring admite el uso de una VPC compartida dentro de una organización. Para obtener más información, consulte Uso de una VPC compartida con agentes de seguridad automatizados.

Tipo de problema	Mensaje de emisión	Pasos para la solución de problemas
	Solo cuando se utiliza una VPC compartida con una configuración de agente automatizada El ID de cuenta de propietario *111122223333* de la VPC compartida (*vPCid*) *no tiene habilitada* la supervisión del tiempo de ejecución, la configuración automática de agentes o ambas	La cuenta de propietario de la VPC compartida debe habilitar la supervisión del tiempo de ejecución y la configuración automática de los agentes para al menos un tipo de recurso (Amazon EKS o Amazon ECS (AWS Fargate)). Para obtener más información, consulte Requisitos previos específicos de la supervisión del tiempo de ejecución GuardDuty.

Tipo de problema	Mensaje de emisión	Pasos para la solución de problemas
	La habilitación del DNS privado requiere que los atributos de VPC `enableDnsSupport` y `enableDnsHostnames` estén establecidos en `true` para *`vpcId`* (Servicio: Ec2, Código de estado: 400, ID de solicitud: *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*).	Asegúrese de que los siguientes atributos de VPC estén establecidos en `true` - `enableDnsSupport` y `enableDnsHostnames` . Para obtener más información, consulte Atributos DNS para la VPC. Si utiliza la consola de Amazon VPC en https://console.aws.amazon.com/vpc/ para crear la VPC de Amazon, asegúrese de seleccionar Habilitar nombres de host DNS y Habilitar la resolución de DNS. Para obtener más información, consulte Opciones de configuración de la VPC.

Tipo de problema	Mensaje de emisión	Pasos para la solución de problemas
No se pudo eliminar el punto final de VPC compartido	*No se permite eliminar el punto final de la VPC compartid a para el ID de cuenta 111122223 333, el vPCid de la VPC compartida y el ID de cuenta del propietario 555555555 555.*	Posibles pasos: • La desactivación del estado de supervisión del tiempo de ejecución de la cuenta participante de la VPC compartida no afecta a la política de puntos finales de la VPC compartida ni al grupo de seguridad que existe en la cuenta propietaria. Para eliminar el punto final de la VPC y el grupo de seguridad compartidos, debe deshabilitar Runtime Monitoring o el estado de configuración automátic a del agente en la cuenta del propietario de la VPC compartida. • La cuenta de participante de la VPC compartida no puede eliminar el punto final de la VPC compartida ni el grupo de seguridad alojados en la cuenta del propietar io de la VPC compartida.
El agente no presenta informes	(Vacío a propósito)	El tipo de problema ha llegado al final del soporte. Si sigue teniendo este problema y aún no lo ha hecho, active el agente GuardDuty automatizado para Amazon EC2. Si el problema persiste, considere la posibilidad de deshabilitar Runtime Monitoring durante unos minutos y, a continuación, volver a habilitarlo.

Cobertura del recurso Fargate (solo Amazon ECS)

En el caso de un clúster de Amazon ECS que se ejecuta en Fargate, la cobertura del tiempo de ejecución se evalúa a nivel de tarea. La cobertura del tiempo de ejecución de los clústeres de ECS

incluye las tareas de Fargate que comenzaron a ejecutarse después de habilitar la supervisión del tiempo de ejecución y la configuración automática de los agentes.

Si su tarea de Fargate ya se estaba ejecutando cuando habilitó la supervisión del tiempo de ejecución, esta tarea no se considerará para evaluar la cobertura del tiempo de ejecución de los clústeres de ECS. Para incluir una tarea de Fargate de este tipo, tendrás que detenerla y volver a ejecutarla.

Revisión de las estadísticas de cobertura

Las estadísticas de cobertura de los recursos AWS Fargate (solo de Amazon ECS) asociados a sus propias cuentas o a las cuentas de sus miembros representan el porcentaje de los clústeres de Amazon ECS en buen estado entre todos los clústeres de Amazon ECS de los seleccionados Región de AWS. La siguiente ecuación lo representa de la siguiente manera:

(Clústeres en buen estado/Todos los clústeres)*100

Las estadísticas de cobertura incluyen las tareas de Fargate que están en ejecución o que han terminado de ejecutarse recientemente.

Elija uno de los métodos de acceso para revisar las estadísticas de cobertura de sus cuentas.

Console

- Inicie sesión en la GuardDuty consola AWS Management Console y ábrala en https://console.aws.amazon.com/guardduty/.
- En el panel de navegación, selecciona Runtime Monitoring.
- Seleccione la pestaña Cobertura del tiempo de ejecución.
- En la pestaña de cobertura de tiempo de ejecución de los clústeres de ECS, puede ver las estadísticas de cobertura agregadas por el estado de cobertura de cada clúster de Amazon ECS que está disponible en la tabla de listas de clústeres.
  - Puede filtrar la tabla de listas de clústeres por las siguientes columnas:
    - ID de cuenta
    - Nombre del clúster
    - Tipo de administración del agente
    - Estado de la cobertura
- Si alguno de sus clústeres de ECS tiene el estado de cobertura en mal estado, la columna Problema incluye información adicional sobre el motivo del estado en mal estado.

API/CLI

- Ejecute la ListCoverageAPI con su propio ID de detector válido, la región actual y el punto de conexión del servicio. Puedes filtrar y ordenar la lista de instancias con esta API.
  - Puede cambiar el ejemplo de `filter-criteria` con una de las siguientes opciones para `CriterionKey`:
    - `ACCOUNT_ID`
    - `ECS_CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `MANAGEMENT_TYPE`
  - Puede cambiar el ejemplo de `AttributeName` en `sort-criteria` con las siguientes opciones:
    - `ACCOUNT_ID`
    - `COVERAGE_STATUS`
    - `ISSUE`
    - `ECS_CLUSTER_NAME`
    - `UPDATED_AT`

      El campo se actualiza solo cuando se crea una nueva tarea en el clúster de Amazon ECS asociado o cuando se produce un cambio en el estado de cobertura correspondiente.
  - Puede cambiar el valor de *`max-results`* (hasta 50).
  - Para encontrar el `detectorId` de su cuenta y su región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Ejecute la GetCoverageStatisticsAPI para recuperar las estadísticas agregadas de cobertura basadas en`statisticsType`.
  - Puede cambiar el ejemplo de `statisticsType` a una de las siguientes opciones:
    - `COUNT_BY_COVERAGE_STATUS`— Representa las estadísticas de cobertura de los clústeres de ECS agregadas por estado de cobertura.

- `COUNT_BY_RESOURCE_TYPE`— Estadísticas de cobertura agregadas en función del tipo de AWS recurso de la lista.
- Puede cambiar el ejemplo de `filter-criteria` en el comando. Puede usar las siguientes opciones para `CriterionKey`:
  - `ACCOUNT_ID`
  - `ECS_CLUSTER_NAME`
  - `COVERAGE_STATUS`
  - `MANAGEMENT_TYPE`
  - `INSTANCE_ID`
- Para encontrar las correspondientes `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Para obtener más información sobre los problemas de cobertura, consulteSolución de problemas de cobertura.

Configuración de las notificaciones de cambio de estado de cobertura

El estado de cobertura de su clúster de Amazon ECS puede aparecer como Insalubre. Para saber cuándo cambia el estado de la cobertura, le recomendamos que supervise el estado de la cobertura periódicamente y solucione los problemas si el estado pasa a ser insalubre. Como alternativa, puedes crear una EventBridge regla de Amazon para recibir una notificación cuando el estado de la cobertura cambie de Insalubre a Saludable o no. De forma predeterminada, la GuardDuty publica en el EventBridge bus de tu cuenta.

Ejemplo de esquema de notificaciones

Como EventBridge regla general, puede utilizar los ejemplos de eventos y patrones de eventos predefinidos para recibir la notificación del estado de la cobertura. Para obtener más información sobre cómo crear una EventBridge regla, consulta Crear regla en la Guía del EventBridge usuario de Amazon.

Además, puede crear un patrón de eventos personalizado mediante el siguiente ejemplo de esquema de notificaciones. Asegúrese de sustituir los valores de su cuenta. Para recibir una notificación cuando el estado de cobertura de su clúster de Amazon ECS cambie de `Healthy` a`Unhealthy`, `detail-type` debería indicar *`GuardDuty Runtime Protection Unhealthy`*. Para recibir una notificación cuando el estado de la cobertura cambie de `Unhealthy` a`Healthy`, sustituya el valor de `detail-type` por *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Cuenta de AWS ID",
  "time": "event timestamp (string)",
  "region": "Región de AWS",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "ECS",
        "ecsClusterDetails": {
          "clusterName":"",
          "fargateDetails":{
            "issues":[],
            "managementType":""
          },
          "containerInstanceDetails":{
            "coveredContainerInstances":int,
            "compatibleContainerInstances":int
          }
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Solución de problemas de cobertura

Si el estado de la cobertura de su clúster de Amazon ECS es Incorrecto, puede ver el motivo en la columna Problema.

La siguiente tabla proporciona los pasos de solución de problemas recomendados para los problemas de Fargate (solo Amazon ECS).

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas
El agente no informa	El agente no se presenta para realizar tareas en `TaskDefinition - '`*`TASK_DEFINITION`*` '`	Valide que la configuración del punto de conexión de Amazon VPC sea correcta.
	`VPC_ISSUE` `; for task in TaskDefinition - '` *`TASK_DEFINITION`*` '`	Consulta los detalles del problema de la VPC en la información adicional.
El agente ha salido	ExitCode: `EXIT_CODE` para tareas en `TaskDefinition - '`*`TASK_DEFINITION`*` '`	Consulta los detalles del problema en la información adicional.
	Motivo: *`MOTIVO`* de las tareas en `TaskDefinition - '` *`TASK_DEFINITION`*` '`	
	ExitCode: `EXIT_CODE` con el motivo: *`'EXIT_CODE '`* para las tareas en `TaskDefinition - '` *`TASK_DEFINITION`*` '`	

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas

	El agente salió: MotivoCannotPullContainerError : se ha vuelto a intentar extraer el manifiesto de imagen...	La función de ejecución de tareas debe tener los siguientes permisos de Amazon Elastic Container Registry (Amazon ECR):
		`...`
		`"ecr:GetAuthorizationToken",`
		`"ecr:BatchCheckLayerAvailability",`
		`"ecr:GetDownloadUrlForLayer",`
		`"ecr:BatchGetImage",`
		`...`
		Para obtener más información, consulte Proporcione los permisos de ECR y los detalles de la subred.
		Tras añadir los permisos de Amazon ECR, debe reiniciar la tarea.
		Si el problema persiste, consulteMi AWS Step Functions flujo de trabajo está fallando inesperadamente.

ExitCode: EXIT_CODE para tareas en TaskDefinition - 'TASK_DEFINITION '	Consulta los detalles del problema en la información adicional.	

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas
ExitCode: `EXIT_CODE` con el motivo: '*`EXIT_CODE`* ' para las tareas en `TaskDefinition` - ' *`TASK_DEFINITION`* '		
Motivo: *`MOTIVO de las tareas`* en `TaskDefinition` - ' *`TASK_DEFINITION`* '		
El agente no se presenta	El agente no se presenta para realizar tareas en `TaskDefinition` - '*`TASK_DEFINITION`* '	Valide que la configuración del punto de conexión de Amazon VPC sea correcta.
	`VPC_ISSUE` ; `for task in TaskDefinition` - ' *`TASK_DEFINITION`* '	Consulta los detalles del problema de la VPC en la información adicional.

<table>
<tr><th>Tipo de problema</th><th>Información adicional</th><th>Pasos recomendados de solución de problemas</th></tr>
<tr><td>Otros o el agente no están aprovisionados</td><td>Problema no identificado, relacionado con tareas en <code>TaskDefinition - 'TASK_DEFINITION '</code></td><td>Utilice las siguientes preguntas para identificar la causa raíz del problema:

<table><tr><th>Pregunta</th><th>Explicación</th></tr><tr><td>¿Se inició la tarea antes de activar Runtime Monitoring?</td><td>En Amazon ECS, las tareas son inmutables. Para evaluar el comportamiento en tiempo de ejecución de una tarea de Fargate en ejecución, asegúrese de que Runtime Monitoring ya esté habilitada y, a continuación, reinicie la tarea GuardDuty para añadir el sidecar del contenedor.</td></tr><tr><td>¿La tarea fue lanzada por un servicio no compatible?</td><td>Actualmente, Runtime Monitoring no admite las tareas lanzadas por AWS Batch y AWS CodePipeline.</td></tr></table></td></tr>
</table>

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas	
		Pregunta	Explicación
		¿Esta tarea forma parte de la implementación de un servicio que se inició antes de activar Runtime Monitoring?	En caso afirmativo, puede reiniciar el servicio o actualizarlo `forceNewDeployment` mediante los pasos que se indican en Actualización de un servicio. También puedes usar UpdateService o AWS CLI.
		¿Se inició la tarea después de excluir el clúster de ECS de Runtime Monitoring?	Si cambias la GuardDuty etiqueta predefinida de `GuardDutyManaged - true` a `GuardDutyManaged -false`, no GuardDuty recibirá los eventos de tiempo de ejecución del clúster de ECS.

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas	
		Pregunta	Explicación
		¿Falta un? `TaskExecutionRole`	Es obligatorio añadir un `TaskExecutionRole` porque GuardDuty necesita permisos para descargar el GuardDuty contenedor del repositorio de ECR. Para obtener más información, consulte Proporcione los permisos de ECR y los detalles de la subred.
		¿Su servicio contiene una tarea que tiene un formato antiguo de? `taskArn`	GuardDuty Runtime Monitoring no admite la cobertura de tareas que tienen el formato anterior de `taskArn`.

Tipo de problema	Información adicional	Pasos recomendados de solución de problemas	
		Pregunta	Explicación
			Para obtener información sobre los nombres de recursos de Amazon (ARN) para los recursos de Amazon ECS, consulte Nombres e ID de recursos de Amazon (ARN).

Cobertura para clústeres de Amazon EKS

Revisión de las estadísticas de cobertura

Las estadísticas de cobertura de los clústeres de EKS asociados a sus propias cuentas o a las de sus miembros representan el porcentaje de los clústeres de EKS en buen estado con respecto a todos los clústeres de EKS de la Región de AWS seleccionada. La siguiente ecuación lo representa de la siguiente manera:

(Clústeres en buen estado/Todos los clústeres)*100

Elija uno de los métodos de acceso para revisar las estadísticas de cobertura de sus cuentas.

Console

- Inicie sesión AWS Management Console y abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
- En el panel de navegación, selecciona Runtime Monitoring.
- Seleccione la pestaña Cobertura del tiempo de ejecución de los clústeres de EKS.

- En la pestaña Cobertura del tiempo de ejecución de los clústeres de EKS, puede ver las estadísticas de cobertura agregadas por el estado de cobertura que está disponible en la tabla Lista de clústeres.
  - Puede filtrar la tabla Lista de clústeres por las siguientes columnas:
    - Cluster name (Nombre del clúster)
    - ID de cuenta
    - Tipo de administración del agente
    - Estado de la cobertura
    - Versión del complemento
- Si el valor de Estado de la cobertura de alguno de sus clústeres de EKS es En mal estado, en la columna Problema se puede incluir información adicional sobre el motivo del estado En mal estado.

API/CLI

- Ejecute la ListCoverageAPI con su propio ID de detector, región y punto final de servicio válidos. Puede filtrar y ordenar la lista de clústeres con esta API.
  - Puede cambiar el ejemplo de `filter-criteria` con una de las siguientes opciones para `CriterionKey`:
    - `ACCOUNT_ID`
    - `CLUSTER_NAME`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `ADDON_VERSION`
    - `MANAGEMENT_TYPE`
  - Puede cambiar el ejemplo de `AttributeName` en `sort-criteria` con las siguientes opciones:
    - `ACCOUNT_ID`
    - `CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `ISSUE`
    - `ADDON_VERSION`

    - UPDATED_AT
  - Puede cambiar el valor de *max-results* (hasta 50).
  - Para encontrar los detectorId valores de tu cuenta y región actuales, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Ejecute la GetCoverageStatisticsAPI para recuperar las estadísticas agregadas de cobertura basadas enstatisticsType.
  - Puede cambiar el ejemplo de statisticsType a una de las siguientes opciones:
    - COUNT_BY_COVERAGE_STATUS: representa las estadísticas de cobertura de los clústeres de EKS agregadas por estado de cobertura.
    - COUNT_BY_RESOURCE_TYPE— Estadísticas de cobertura agregadas en función del tipo de AWS recurso de la lista.
    - Puede cambiar el ejemplo de filter-criteria en el comando. Puede usar las siguientes opciones para CriterionKey:
      - ACCOUNT_ID
      - CLUSTER_NAME
      - RESOURCE_TYPE
      - COVERAGE_STATUS
      - ADDON_VERSION
      - MANAGEMENT_TYPE
  - Para encontrar las correspondientes detectorId a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Si el estado de cobertura de su clúster de EKS es En mal estado, consulte Solución de problemas de cobertura de EKS.

Configuración de las notificaciones de cambio de estado de cobertura

El estado de cobertura de un clúster de EKS de su cuenta puede aparecer como En mal estado. Para detectar cuándo el estado de cobertura pasa a ser En mal estado, le recomendamos que supervise el estado de cobertura periódicamente y que solucione los problemas si el estado es En mal estado. Como alternativa, puedes crear una EventBridge regla de Amazon que te notifique cuando el estado de la cobertura cambie de `Unhealthy` a `Healthy` o no. De forma predeterminada, la GuardDuty publica en el EventBridgebus de tu cuenta.

Ejemplo de esquema de notificaciones

Como EventBridge regla general, puede utilizar los ejemplos de eventos y patrones de eventos predefinidos para recibir la notificación del estado de la cobertura. Para obtener más información sobre cómo crear una EventBridge regla, consulta Crear regla en la Guía del EventBridge usuario de Amazon.

Además, puede crear un patrón de eventos personalizado mediante el siguiente ejemplo de esquema de notificaciones. Asegúrese de sustituir los valores de su cuenta. Para recibir una notificación cuando el estado de cobertura de su clúster de Amazon EKS cambie de `Healthy` a`Unhealthy`, `detail-type` debería indicar *`GuardDuty Runtime Protection Unhealthy`*. Para recibir una notificación cuando el estado de la cobertura cambie de `Unhealthy` a`Healthy`, sustituya el valor de `detail-type` por *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Cuenta de AWS ID",
  "time": "event timestamp (string)",
  "region": "Región de AWS",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
```

```
    "resourceDetails": {
        "resourceType": "EKS",
        "eksClusterDetails": {
            "clusterName": "string",
            "availableNodes": "string",
             "desiredNodes": "string",
             "addonVersion": "string"
         }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Solución de problemas de cobertura de EKS

Si el estado de cobertura de su clúster EKS es`Unhealthy`, puede ver el error correspondiente en la columna Problema de la GuardDuty consola o utilizando el tipo de CoverageResourcedatos.

Cuando trabaje con etiquetas de inclusión o exclusión para supervisar los clústeres de EKS de forma selectiva, es posible que las etiquetas tarden algún tiempo en sincronizarse. Esto puede afectar al estado de cobertura del clúster de EKS asociado. Puede intentar eliminar y volver a agregar la etiqueta correspondiente (inclusión o exclusión). Para obtener más información, consulte Etiquetado de los recursos de Amazon EKS en la Guía del usuario de Amazon EKS.

La estructura de un problema de cobertura es `Issue type:Extra information`. Por lo general, los problemas tienen información adicional opcional que puede incluir una excepción específica del cliente o una descripción del problema. En función de la información adicional, en las siguientes tablas se proporcionan los pasos recomendados para solucionar los problemas de cobertura de los clústeres de EKS.

Tipo de problema (prefijo)	Información adicional	Pasos recomendados de solución de problemas
Error de creación del complemento	El complemento no `aws-guardduty-agent` es compatible con la versión actual del clúster. *`ClusterName`* No se	Asegúrese de utilizar una de esas versiones de Kubernetes que admiten la implementación del complemento de EKS `aws-guardduty-agen`

Tipo de problema (prefijo)	Información adicional	Pasos recomendados de solución de problemas
	admite el complemento especificado.	`t` . Para obtener más información, consulte Versiones de Kubernetes compatibles con el agente de seguridad GuardDuty . Para obtener información sobre cómo actualizar su versión de Kubernetes, consulte Actualización de una versión de Kubernetes de clúster de Amazon EKS.
Error de creación del complemento Falló la actualización del complemento Complemento en mal estado	Problema con el complemento de EKS: `AddonIssueCode` : `AddonIssueMessage`	Para obtener información sobre los pasos recomendados para un código de problema de complemento específico, consulte. Troubleshooting steps for Addon creation/updatation error with Addon issue code Para obtener una lista de los códigos de problemas relacionados con los complementos que podrían producirse en este problema, consulte AddonIssue.

Tipo de problema (prefijo)	Información adicional	Pasos recomendados de solución de problemas
Error al crear el punto de conexión de VPC	*No se admite la creación de puntos de conexión de VPC para VPC compartidos*	La supervisión del tiempo de ejecución ahora admite el uso de una VPC compartida dentro de una organización. Asegúrese de que sus cuentas cumplen todos los requisitos previos. Para obtener más información, consulte Requisitos previos para usar una VPC compartida.
	Solo cuando se utiliza una VPC compartida con una configuración de agente automatizada El ID de la cuenta de propietario *111122223333* de la VPC compartida no tiene *habilitada la* supervisión del tiempo de ejecución, la configuración automática de agentes o ambas.	La cuenta de propietario de la VPC compartida debe habilitar la supervisión del tiempo de ejecución y la configuración automática de los agentes para al menos un tipo de recurso (Amazon EKS o Amazon ECS (AWS Fargate)). Para obtener más información, consulte Requisitos previos específicos de la supervisión del tiempo de ejecución GuardDuty.

Tipo de problema (prefijo)	Información adicional	Pasos recomendados de solución de problemas
	La habilitación del DNS privado requiere que los atributos de VPC `enableDnsSupport` y `enableDnsHostnames` estén establecidos en `true` para *`vpcId`* (Servicio: Ec2, Código de estado: 400, ID de solicitud: *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*).	Asegúrese de que los siguientes atributos de VPC estén establecidos en `true` - `enableDnsSupport` y `enableDnsHostnames`. Para obtener más información, consulte Atributos DNS para la VPC. Si utiliza la consola de Amazon VPC en https://console.aws.amazon.com/vpc/ para crear la VPC de Amazon, asegúrese de seleccionar Habilitar nombres de host DNS y Habilitar la resolución de DNS. Para obtener más información, consulte Opciones de configuración de la VPC.

Tipo de problema (prefijo)	Información adicional	Pasos recomendados de solución de problemas
No se pudo eliminar el punto final de la VPC compartido	*No se permite eliminar el punto final de la VPC compartida para el ID de cuenta 111122223333, el vPCid de la VPC compartida y el ID de cuenta del propietario 555555555555.*	Posibles pasos: • La desactivación del estado de supervisión del tiempo de ejecución de la cuenta participante de la VPC compartida no afecta a la política de puntos finales de la VPC compartida ni al grupo de seguridad que existe en la cuenta propietaria. Para eliminar el punto final de la VPC y el grupo de seguridad compartidos, debe deshabilitar Runtime Monitoring o el estado de configuración automática del agente en la cuenta del propietario de la VPC compartida. • La cuenta de participante de la VPC compartida no puede eliminar el punto final de la VPC compartida ni el grupo de seguridad alojados en la cuenta del propietar

Tipo de problema (prefijo)	Información adicional	Pasos recomendados de solución de problemas
		io de la VPC compartid a.
Clústeres de EKS locales	Los complementos de EKS no se admiten en los clústeres de Outposts locales.	No se puede procesar. Para obtener más información, consulte Amazon EKS en AWS Outposts.
No se ha concedido el permiso de habilitación de la supervisión en tiempo de ejecución de EKS	(puede o no mostrar información adicional)	1. Si hay información adicional disponible sobre este problema, corrija la causa raíz y avance al siguiente paso. 2. Desactive la supervisión en tiempo de ejecución de EKS y vuelva a activarla . Asegúrese de que el GuardDuty agente también se despliegue, ya sea de forma automática GuardDuty o manual.

Tipo de problema (prefijo)	Información adicional	Pasos recomendados de solución de problemas
Aprovisionamiento de recursos de habilitación de la supervisión en tiempo de ejecución de EKS en curso.	(puede o no mostrar información adicional)	No se puede procesar. Después de habilitar la supervisión en tiempo de ejecución de EKS, el estado de cobertura puede seguir siendo `Unhealthy` hasta que se complete el paso de aprovisionamiento de recursos. El estado de cobertura se supervisa y actualiza periódicamente.
Otros (cualquier otro problema)	Error debido a un error de autorización	Desactive la supervisión en tiempo de ejecución de EKS y vuelva a activarla. Asegúrese de que el GuardDuty agente también se despliegu e, de forma automática GuardDuty o manual.

Error de creación o actualización del complemento	Pasos para la solución de problemas
Problema con el complemento EKS`InsufficientNumberOfReplicas` : el complemento no está en buen estado porque no tiene el número deseado de réplicas.	Con el mensaje del problema, puede identificar y corregir la causa raíz. Puede empezar por describir su clúster. Por ejemplo, `kubectl describe pods`utilícelo para identificar la causa principal del fallo del pod.

Error de creación o actualización del complemento	Pasos para la solución de problemas
	Tras corregir la causa principal, vuelve a intentar el paso (creación o actualización del complemento).
Problema con el complemento EKS`AdmissionRequestDenied` : webhook de admisión `"validate.kyverno.svc-fail"` denegó la solicitud: política de infracción `DaemonSet/amazon-guardduty/aws-guardduty-agent` de recursos:::... restrict-image-registries `autogen-validate-registries`	1. El clúster Amazon EKS o el administrador de seguridad deben revisar la política de seguridad que bloquea la actualización del complemento. 2. Debe deshabilitar el controlador (`webhook`) o hacer que el controlador acepte las solicitudes de Amazon EKS.
Problema con el complemento EKS`ConfigurationConflict` : Se encontraron conflictos al intentar aplicarlo. No continuará debido al modo de resolución de conflictos. `Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.template.spec.containers[name="aws-guardduty-agent"].image`	Al crear o actualizar el complemento, proporciona el indicador de `OVERWRITE` resolución de conflictos. Esto podría sobrescribir cualquier cambio que se haya realizado directamente en los recursos relacionados de Kubernetes mediante la API de Kubernetes. Primero puedes eliminar el complemento y, después, volver a instalarlo.

Error de creación o actualización del complemento	Pasos para la solución de problemas

Problema con el complemento EKS - `AccessDenied: priorityclasses.scheduling.k8s.io "aws-guardduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope`	Debe añadir el permiso que falta al `eks:addon-cluster-admin ClusterRoleBinding` manual. Añada lo siguiente `yaml aeks:addon-cluster-admin` :
	
	`---`
	`kind: ClusterRoleBinding`
	`apiVersion: rbac.authorization.k8s.io/v1`
	`metadata:`
	`  name: eks:addon-cluster-admin`
	`subjects:`
	`- kind: User`
	`  name: eks:addon-manager`
	`  apiGroup: rbac.authorization.k8s.io`
	`roleRef:`
	`  kind: ClusterRole`
	`  name: cluster-admin`
	`  apiGroup: rbac.authorization.k8s.io`
	`---`
	
	Ahora puede aplicarlo `yaml` a su clúster de Amazon EKS mediante el siguiente comando:
	
	`kubectl apply -f eks-addon-cluster-admin.yaml`

Problema con el complemento EKS - `AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label`	Debe deshabilitar el controlador o hacer que el controlador acepte las solicitudes del clúster de Amazon EKS. Antes de crear o actualizar el complemento, también puede crear un espacio de GuardDuty nombres y etiquetarlo como. `owner`

Preguntas frecuentes

Contenido

¿Por qué el estado de cobertura de mi recurso se mantiene **`Unhealthy`** incluso después de activar Runtime Monitoring, implementar el agente de GuardDuty seguridad y cumplir todos los requisitos previos?

Si acaba de implementar el agente de GuardDuty seguridad (ya sea mediante una configuración automática del agente o manualmente) o ha seguido los pasos recomendados para solucionar un problema de cobertura, es posible que el estado de la cobertura tarde unos minutos en recuperarse. Puedes comprobar el estado de la cobertura periódicamente o configurar Amazon EventBridge (EventBridge) para que reciba una notificación cuando cambie el estado de la cobertura.

¿Quién puede ver el estado de cobertura en tiempo de ejecución de un recurso que me pertenece Cuenta de AWS?

Como cuenta de miembro o cuenta independiente, puede ver las estadísticas de cobertura de los recursos asociados a sus propias cuentas. Como cuenta de GuardDuty administrador delegado de una organización, puede ver las estadísticas de cobertura de los recursos asociados a su cuenta y de las cuentas de los miembros que pertenecen a su organización.

Configuración de la supervisión de la CPU y la memoria

Después de activar Runtime Monitoring y evaluar si el estado de cobertura del clúster es correcto, puede configurar y ver las métricas de información.

Los siguientes temas pueden ayudarle a evaluar el rendimiento del agente desplegado en comparación con los límites de CPU y memoria del GuardDuty agente.

Configuración de la supervisión en el clúster de Amazon ECS

Los siguientes pasos de la Guía del CloudWatch usuario de Amazon pueden ayudarle a evaluar el rendimiento del agente desplegado en comparación con los límites de CPU y memoria del GuardDuty agente:

1. Configuración de Container Insights en Amazon ECS para métricas a nivel de clúster y servicio
2. Métricas de Amazon ECS Container Insights

Configuración de la supervisión en el clúster Amazon EKS

Una vez que se haya desplegado el agente de GuardDuty seguridad y hayas evaluado que el estado de cobertura del clúster es correcto, puedes configurar y ver las métricas de Container Insight.

Evalúe el rendimiento del agente de seguridad

1. Configuración de Container Insights en Amazon EKS y Kubernetes en la Guía del usuario de Amazon CloudWatch
2. Métricas de Amazon EKS y Kubernetes Container Insights en la Guía del usuario de Amazon CloudWatch

Gestione el rendimiento con el agente de seguridad v1.5.0 y versiones posteriores

> Con el agente de seguridad v1.5.0 y versiones posteriores, cuando los datos indican que el GuardDuty agente asociado está alcanzando los límites asignados, puede configurar parámetros específicos. Para obtener más información, consulte Configure los parámetros del complemento EKS.

Tipos de eventos de tiempo de ejecución recopilados que utilizan GuardDuty

El agente GuardDuty de seguridad recopila los siguientes tipos de eventos y los envía al GuardDuty backend para detectar y analizar las amenazas. GuardDuty no hace que estos eventos sean accesibles para usted. Si GuardDuty detecta una amenaza potencial y genera un resultado de Runtime Monitoring, puede ver los detalles del hallazgo correspondiente. Para obtener más información sobre cómo se GuardDuty utilizan los tipos de eventos recopilados, consulteOptar por no utilizar sus datos para mejorar el servicio.

Eventos de procesos

Nombre del campo	Descripción
Process name (Nombre del proceso)	Nombre del proceso observado.
Ruta de proceso	Ruta absoluta del ejecutable del proceso.
ID de proceso	ID asignado al proceso por el sistema operativo .
PID de espacio de nombres	ID del proceso en un espacio de nombres de PID secundario distinto del espacio de nombres de PID de nivel de host. En el caso de los procesos dentro de un contenedor, es el ID de proceso observado dentro del contenedor.
ID de usuario del proceso	ID único del usuario que ha ejecutado el proceso.
UUID de proceso	El identificador único asignado al proceso por GuardDuty.
GID de proceso	ID del proceso del grupo de procesos.
EGID de proceso	ID del grupo efectivo del grupo de procesos.
EUID de proceso	ID del usuario efectivo del proceso.
Nombre de usuario de proceso	Nombre del usuario que ha ejecutado el proceso.
Hora de inicio de proceso	Hora de creación del proceso. Este campo está en formato de cadena de fecha UTC (`2023-03-22T19:37:20.168Z`).
SHA-256 de ejecutable de proceso	Hash `SHA256` del ejecutable del proceso.
Ruta de script de proceso	Ruta del archivo del script que se ha ejecutado.

Nombre del campo	Descripción
Variable de entorno de proceso	Variable de entorno puesta a disposición del proceso. Solo se recopilan `LD_PRELOAD` y `LD_LIBRARY_PATH` .
Directorio de trabajo actual (PWD) de proceso	Directorio de trabajo actual del proceso.
Proceso principal	Detalles del proceso principal. Un proceso principal es un proceso que creó el proceso observado.
Argumentos de línea de comandos Actualmente, este campo está limitado a versiones de agentes específicas correspon dientes al tipo de recurso: • Fargate (solo Amazon ECS) con agente de GuardDuty seguridad v1.0.0 y versiones posteriores. • Instancias de Amazon EC2 con agente de GuardDuty seguridad v1.0.0 y versiones posteriores. • Amazon EKS se agrupa con el agente de seguridad v1.4.0 y versiones posteriores. Para obtener más información, consulte GuardDuty historial de versiones del agente.	Argumentos de línea de comandos proporcio nados en el momento de la ejecución del proceso. Este campo puede contener datos confidenciales de los clientes.

Eventos de contenedores

Nombre del campo	Descripción
Nombre de contenedor	Nombre del contenedor.

Nombre del campo	Descripción
	Cuando está disponible, este campo muestra el valor de la etiqueta `io.kubenetes.container.name` .
UID de contenedor	ID único del contenedor asignado por el tiempo de ejecución del contenedor.
Tiempo de ejecución de contenedor	Tiempo de ejecución del contenedor (por ejemplo, `docker` o `containerd`) utilizado para ejecutar el contenedor.
ID de imagen de contenedor	ID de la imagen del contenedor.
Nombre de imagen de contenedor	Nombre de la imagen del contenedor.

AWS Fargate Eventos de tareas (solo en Amazon ECS)

Nombre del campo	Descripción
Nombre de recurso de Amazon (ARN) de la tarea	El ARN de la tarea.
Nombre del clúster	El nombre del clúster de Amazon ECS.
Apellido	Apellido de la definición de la tarea. Se `family` utiliza como nombre para la definición de tarea que se utiliza para iniciar la tarea.
Nombre del servicio	El nombre del servicio Amazon ECS, si la tarea se lanzó como parte de un servicio.
Tipo de lanzamiento	La infraestructura en la que se ejecuta la tarea. En el caso de la supervisión del tiempo de ejecución con el tipo de recurso como`ECSCluster` , el tipo de lanzamiento podría ser uno `EC2` o dos`FARGATE`.

Nombre del campo	Descripción
CPU	El número de unidades de CPU utilizadas por la tarea, tal como se expresa en la definición de la tarea.

Eventos de pod de Kubernetes

Nombre del campo	Descripción
ID de pod	ID del pod de Kubernetes.
Nombre de pod	Nombre del pod de Kubernetes.
Espacio de nombres de pod	Nombre del espacio de nombres de Kubernetes al que pertenece la carga de trabajo de Kubernetes.
Nombre de clúster de Kubernetes	Nombre del clúster de Kubernetes.

Eventos de DNS

Nombre del campo	Descripción
Tipo de socket	Tipo de socket para indicar la semántica de la comunicación. Por ejemplo, `SOCK_RAW`.
Familia de direcciones	Representa el protocolo de comunicación asociado a la dirección. Por ejemplo, la familia de direcciones `AF_INET` se utiliza para el protocolo IP v4.
ID de dirección	ID de la dirección de conexión.
Número de protocolo	Número de protocolo de capa 4 (por ejemplo, 17 para UDP y 6 para TCP).

Nombre del campo	Descripción
IP de punto de conexión remoto de DNS	IP remota de la conexión.
Puerto de punto de conexión remoto de DNS	Número del puerto de la conexión.
IP de punto de conexión local de DNS	IP local de la conexión.
Puerto de punto de conexión local de DNS	Número del puerto de la conexión.
Carga de DNS	Carga de los paquetes de DNS que contiene consultas y respuestas de DNS.

Eventos abiertos

Nombre del campo	Descripción
Ruta de archivo	Ruta del archivo que se abre en este evento.
Indicadores	Describe el modo de acceso a archivos, como solo lectura, solo escritura y lectura-escritura.

Evento de carga de módulo

Nombre del campo	Descripción
Nombre de módulo	Nombre del módulo cargado en el kernel.

Eventos de Mprotect

Nombre del campo	Descripción
Rango de direcciones	Rango de direcciones para el que se modificaron las protecciones de acceso.
Regiones de memoria	Especifica la región del espacio de direcciones de un proceso, como la pila y el montón.
Indicadores	Representa las opciones que controlan el comportamiento de este evento.

Eventos de montaje

Nombre del campo	Descripción
Destino de montaje	Ruta en la que se monta el origen del montaje.
Origen de montaje	Ruta del host que se monta en el destino de montaje.
Tipo de sistema de archivos	Representa el tipo de sistema de archivos montado.
Indicadores	Representa las opciones que controlan el comportamiento de este evento.

Eventos de enlace

Nombre del campo	Descripción
Ruta de enlace	Ruta en la que se crea el enlace físico.
Ruta de destino	Ruta del archivo al que apunta el enlace físico.

Eventos de enlace simbólico

Nombre del campo	Descripción
Ruta de enlace	Ruta en la que se crea el enlace simbólico.
Ruta de destino	Ruta del archivo al que apunta el enlace simbólico.

Eventos duplicados

Nombre del campo	Descripción
Descriptor de archivo antiguo	Descriptor de archivo que representa un objeto de archivo abierto.
Descriptor de archivo nuevo	Descriptor de archivo nuevo que es un duplicado del descriptor de archivo antiguo. Tanto el descriptor de archivo antiguo como el nuevo representan el mismo objeto de archivo abierto.
IP de punto de conexión remoto de duplicación	Dirección IP remota del socket de red que representa el descriptor de archivo antiguo. Solo se aplica cuando el descriptor de archivo antiguo representa un socket de red.
Puerto de punto de conexión remoto de duplicación	Puerto remoto del socket de red que representa el descriptor de archivo antiguo. Solo se aplica cuando el descriptor de archivo antiguo representa un socket de red.
IP de punto de conexión local de duplicación	Dirección IP local del socket de red que representa el descriptor de archivo antiguo. Solo se aplica cuando el descriptor de archivo antiguo representa un socket de red.
Puerto de punto de conexión local de duplicación	Puerto local del socket de red que representa el descriptor de archivo antiguo. Solo se aplica cuando el descriptor de archivo antiguo representa un socket de red.

Evento de mapa de memoria

Nombre del campo	Descripción
Ruta de archivo	Ruta del archivo al que se asigna la memoria.

Eventos de socket

Nombre del campo	Descripción
Familia de direcciones	Representa el protocolo de comunicación asociado a la dirección. Por ejemplo, la familia de direcciones `AF_INET` se utiliza para la versión de IP del protocolo 4.
Tipo de socket	Tipo de socket para indicar la semántica de la comunicación. Por ejemplo, `SOCK_RAW`.
Número de protocolo	Especifica un protocolo concreto de la familia de direccion es. Por lo general, hay un único protocolo en las familias de direcciones. Por ejemplo, la familia de direcciones `AF_INET` solo tiene el protocolo de IP.

Eventos de conexión

Nombre del campo	Descripción
Familia de direcciones	Representa el protocolo de comunicación asociado a la dirección. Por ejemplo, la familia de direcciones `AF_INET` se utiliza para el protocolo IP v4.
Tipo de socket	Tipo de socket para indicar la semántica de la comunicación. Por ejemplo, `SOCK_RAW`.
Número de protocolo	Especifica un protocolo concreto de la familia de direccion es. Por lo general, hay un único protocolo en las familias de

Nombre del campo	Descripción
	direcciones. Por ejemplo, la familia de direcciones `AF_INET` solo tiene el protocolo de IP.
Ruta de archivo	Ruta del archivo de socket si la familia de direcciones es `AF_UNIX`.
IP de punto de conexión remoto	IP remota de la conexión.
Puerto de punto de conexión remoto	Número del puerto de la conexión.
IP de punto de conexión local	IP local de la conexión.
Puerto de punto de conexión local	Número del puerto de la conexión.

Eventos de Readv de VM de proceso

Nombre del campo	Descripción
Indicadores	Representa las opciones que controlan el comportamiento de este evento.
PID de destino	ID del proceso desde el que se lee la memoria.
UUID de proceso de destino	ID único del proceso de destino.
Ruta de ejecutable de destino	Ruta absoluta del archivo ejecutable del proceso de destino.

Eventos de Writev de VM de proceso

Nombre del campo	Descripción
Indicadores	Representa las opciones que controlan el comportamiento de este evento.
PID de destino	ID del proceso en el que se escribe la memoria.
UUID de proceso de destino	ID único del proceso de destino.
Ruta de ejecutable de destino	Ruta absoluta del archivo ejecutable del proceso de destino.

Eventos de Ptrace

Nombre del campo	Descripción
PID de destino	ID del proceso de destino.
UUID de proceso de destino	ID único del proceso de destino.
Ruta de ejecutable de destino	Ruta absoluta del archivo ejecutable del proceso de destino.
Indicadores	Representa las opciones que controlan el comportamiento de este evento.

Eventos de enlace

Nombre del campo	Descripción
Familia de direcciones	Representa el protocolo de comunicación asociado a la dirección. Por ejemplo, la familia de direcciones `AF_INET` se utiliza para el protocolo IP v4.
Tipo de enchufe	Tipo de socket para indicar la semántica de la comunicación. Por ejemplo, `SOCK_RAW`.

Nombre del campo	Descripción
Número de protocolo	Número de protocolo de capa 4 (por ejemplo, 17 para UDP y 6 para TCP).
IP del punto final local	IP local de la conexión.
Puerto de punto final local	Número del puerto de la conexión.

Escuche los eventos

Nombre del campo	Descripción
Familia de direcciones	Representa el protocolo de comunicación asociado a la dirección. Por ejemplo, la familia de direcciones `AF_INET` se utiliza para el protocolo IP v4.
Tipo de enchufe	Tipo de socket para indicar la semántica de la comunicación. Por ejemplo, `SOCK_RAW`.
Número de protocolo	Número de protocolo de capa 4 (por ejemplo, 17 para UDP y 6 para TCP).
IP del punto final local	IP local de la conexión.
Puerto de punto final local	Número del puerto de la conexión.

Cambie el nombre de los eventos

Nombre del campo	Descripción
Ruta de archivo	Ruta donde se encuentra el archivo al que se cambia el nombre.
Destino	La nueva ruta del archivo.

Configure los eventos de UID

Nombre del campo	Descripción
Nuevo EUID	El nuevo seudónimo efectivo del proceso.
Nuevo UID	El nuevo ID de usuario del proceso.

Eventos de Chmod

Nombre del campo	Descripción
Ruta de archivo	Ruta del archivo que invoca este evento.
Modo de archivo	Los permisos de acceso actualizados para el archivo asociado.

Agente de alojamiento GuardDuty de repositorios Amazon ECR

En las siguientes secciones se enumeran los repositorios de Amazon Elastic Container Registry (Amazon ECR) GuardDuty donde se aloja el agente de seguridad que se implementa en los clústeres de Amazon EKS y Amazon ECS.

Contenido

Repositorio para GuardDuty agentes en clústeres de Amazon EKS

En la siguiente tabla se muestran los repositorios de Amazon ECR que alojan el agente complementario Amazon EKS para GuardDuty (`aws-guardduty-agent`) para cada uno de ellos.
Región de AWS

Región de AWS	URI del repositorio de Amazon ECR
Oeste de EE. UU. (Oregón)	039403964562.dkr.ecr.us-west-2.amazonaws.com
Europa (París)	113643092156.dkr.ecr.eu-west-3.amazonaws.com
Asia-Pacífico (Bombay)	610108029387.dkr.ecr.ap-south-1.amazonaws.com
Asia-Pacífico (Hyderabad)	618745550137.dkr.ecr.ap-south-2.amazonaws.com
Canadá (centro)	001188825231.dkr.ecr.ca-central-1.amazonaws.com
Medio Oriente (EAU)	601769779514.dkr.ecr.me-central-1.amazonaws.com
Europa (Londres)	109118265657.dkr.ecr.eu-west-2.amazonaws.com
Europa (Irlanda)	373421517865.dkr.ecr.us-west-1.amazonaws.com
Este de EE. UU. (Norte de Virginia)	031903291036.dkr.ecr.us-east-1.amazonaws.com
Este de EE. UU. (Ohio)	591382732059.dkr.ecr.us-east-2.amazonaws.com
Europa (Irlanda)	673884943994.dkr.ecr.eu-west-1.amazonaws.com
América del Sur (São Paulo)	941219317354.dkr.ecr.sa-east-1.amazonaws.com
Europa (Estocolmo)	366771026645.dkr.ecr.eu-north-1.amazonaws.com
Europa (Fráncfort)	409493279830.dkr.ecr.eu-central-1.amazonaws.com

Región de AWS	URI del repositorio de Amazon ECR
Europa (Zúrich)	718440343717.dkr.ecr.eu-central-2.amazonaws.com
Asia-Pacífico (Singapur)	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
Asia-Pacífico (Sídney)	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Asia-Pacífico (Yakarta)	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
Asia-Pacífico (Tokio)	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
Asia-Pacífico (Seúl)	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asia-Pacífico (Osaka)	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Asia-Pacífico (Hong Kong)	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Medio Oriente (Baréin)	541829937850.dkr.ecr.me-south-1.amazonaws.com
Europa (Milán)	528450769569.dkr.ecr.eu-south-1.amazonaws.com
Europa (España)	531047660167.dkr.ecr.eu-south-2.amazonaws.com
África (Ciudad del Cabo)	379032919888.dkr.ecr.af-south-1.amazonaws.com
Asia-Pacífico (Melbourne)	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com
Israel (Tel Aviv)	292660727137.dkr.ecr.il-central-1.amazonaws.com

Repositorio para GuardDuty agentes en AWS Fargate (solo Amazon ECS)

En la siguiente tabla se muestran los repositorios de Amazon ECR que alojan el GuardDuty agente para cada uno de ellos (solo AWS Fargate Amazon ECS). Región de AWS

Región de AWS	URI del repositorio de Amazon ECR
Oeste de EE. UU. (Oregón)	`733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-fargate`
Europa (París)	`665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-fargate`
Asia-Pacífico (Bombay)	`251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Asia-Pacífico (Hyderabad)	`950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-fargate`
Canadá (centro)	`354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Medio Oriente (EAU)	`000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Londres)	`892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Irlanda)	`684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-fargate`
Este de EE. UU. (Norte de Virginia)	`593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-fargate`
Este de EE. UU. (Ohio)	`307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-fargate`

Región de AWS	URI del repositorio de Amazon ECR
Europa (Irlanda)	694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-fargate
América del Sur (São Paulo)	758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Estocolmo)	591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Fráncfort)	323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Zúrich)	529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Singapur)	174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Sídney)	005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Yakarta)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Tokio)	533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Seúl)	914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Osaka)	273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asia-Pacífico (Hong Kong)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate
Medio Oriente (Baréin)	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate

Región de AWS	URI del repositorio de Amazon ECR
Europa (Milán)	`266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (España)	`919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate`
África (Ciudad del Cabo)	`197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Asia-Pacífico (Melbourne)	`251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate`
Israel (Tel Aviv)	`870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate`

GuardDuty historial de versiones del agente

En las siguientes secciones se proporciona la versión de lanzamiento del GuardDuty agente que se implementa en las instancias de Amazon EC2, los clústeres de Amazon ECS y los clústeres de Amazon EKS.

GuardDuty agente de seguridad para instancias de Amazon EC2

Versión del agente	Notas de la versión	Fecha de disponibilidad
v1.1.0	Admite la configuración GuardDuty automática de agentes en Runtime Monitoring para instancias de Amazon EC2. Es compatible con las nuevas señales y hallazgos de seguridad publicados con el anuncio de la disponibilidad	26 de marzo de 2024

Versión del agente	Notas de la versión	Fecha de disponibilidad
	general de Runtime Monitoring para las instancias EC2. Mejora general del rendimien to.	
v1.0.2	Es compatible con las últimas AMI de Amazon ECS.	2 de febrero de 2024
v1.0.1	Ajustes y mejoras generales del rendimiento Las versiones de agente publicadas antes de la v1.0.2 son incompatibles con las AMI de Amazon ECS lanzadas después del 31 de enero de 2024.	23 de enero de 2024
v1.0.0	Versión inicial de la instalación del RPM. Las versiones de agente publicadas antes de la v1.0.2 son incompatibles con las AMI de Amazon ECS lanzadas después del 31 de enero de 2024.	26 de noviembre de 2023

La clave pública, la firma de x86_64 RPM, la firma de arm64 RPM y el enlace de acceso correspondiente a los scripts RPM alojados en los buckets de Amazon S3 se pueden formar a partir de las siguientes plantillas. Sustituya el valor del Región de AWS ID de AWS cuenta y la versión del GuardDuty agente para acceder a los scripts de RPM. Las siguientes plantillas incluyen la versión más reciente del agente para las instancias de Amazon EC2.

- Clave pública:

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/publickey.pem
```

- GuardDuty Firma RPM del agente de seguridad:

  Firma de x86_64 RPM

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/amazon-guardduty-agent-1.1.0.x86_64.sig
  ```

  Firma de arm64 RPM

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/amazon-guardduty-agent-1.1.0.arm64.sig
  ```

- Acceda a los enlaces a los scripts RPM del bucket de Amazon S3:

  Enlace de acceso para x86_64 RPM

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/amazon-guardduty-agent-1.1.0.x86_64.rpm
  ```

  Enlace de acceso para arm64 RPM

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/amazon-guardduty-agent-1.1.0.arm64.rpm
  ```

Región de AWS	Nombre de la región	AWS ID de cuenta
eu-west-1	Europa (Irlanda)	694911143906
us-east-1	Este de EE. UU. (Norte de Virginia)	593207742271
us-east-2	Este de EE. UU. (Ohio)	733349766148
eu-west-3	Europa (París)	665651866788
us-east-2	Este de EE. UU. (Ohio)	307168627858

eu-central-1	Europa (Fráncfort)	323658145986
ap-northeast-2	Asia-Pacífico (Seúl)	914738172881
eu-north-1	Europa (Estocolmo)	591436053604
ap-east-1	Asia-Pacífico (Hong Kong)	258348409381
me-south-1	Medio Oriente (Baréin)	536382113932
eu-west-2	Europa (Londres)	892757235363
ap-northeast-1	Asia-Pacífico (Tokio)	533107202818
ap-southeast-1	Asia-Pacífico (Singapur)	174946120834
ap-south-1	Asia-Pacífico (Bombay)	251508486986
ap-southeast-3	Asia-Pacífico (Yakarta)	510637619217
sa-east-1	América del Sur (São Paulo)	758426053663
ap-northeast-3	Asia-Pacífico (Osaka)	273192626886
eu-south-1	Europa (Milán)	266869475730
af-south-1	África (Ciudad del Cabo)	197869348890
ap-southeast-2	Asia-Pacífico (Sídney)	005257825471
me-central-1	Medio Oriente (EAU)	000014521398
us-west-1	Oeste de EE. UU. (Norte de California)	684579721401
ca-central-1	Canadá (centro)	354763396469
ap-south-2	Asia-Pacífico (Hyderabad)	950823858135
eu-south-2	Europa (España)	919611009337
eu-central-2	Europa (Zúrich)	529164026651

ap-southeast-4	Asia-Pacífico (Melbourne)	251357961535
il-central-1	Israel (Tel Aviv)	870907303882

GuardDuty agente de seguridad para AWS Fargate (solo Amazon ECS)

En la siguiente tabla se muestra el historial de versiones del agente de GuardDuty seguridad de Fargate (solo en Amazon ECS).

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad
v1.0.0	x86_64 (AMD64): sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017 Graviton (ARM64): sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984	Versión inicial del agente de GuardDuty seguridad para AWS Fargate (solo Amazon ECS).	26 de noviembre de 2023

GuardDuty agente de seguridad para clústeres de Amazon EKS

En la siguiente tabla se muestra el historial de versiones del GuardDuty agente de complementos de Amazon EKS.

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Fin del soporte estándar ([1]).
v1.5.0	x86_64 (AMD64): sha256:66d491927763742660faa87cc2c39bb97b7873	• Ajustes y mejoras generales	7 de marzo de 2024	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Fin del soporte estándar ([1]).
	`039157ae8b90bc999cb73d0b9c` Graviton (ARM64): `sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dffe0792c9e6d0778b40`	del rendimiento. • Mejoras de seguridad, incluidos nuevos tipos de eventos en Tipos de eventos de tiempo de ejecución recopilados. • Mejoras de rendimiento en relación con el uso de la CPU.		
v1.4.1	x86_64 (AMD64): `sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c` Graviton (ARM64): `sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dffe0792c9e6d0778b40`	Ajustes y mejoras generales del rendimiento.	16 de enero de 2024	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Fin del soporte estándar ([1]).
v1.4.0	x86_64 (AMD64): `sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f` Graviton (ARM64): `sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e`	El punto de montaje manifiesto permite una mejor recopilación de datos AppArmor configuración en el manifiesto Recoja el argumento de la línea de comandos Ajustes y mejoras generales del rendimiento	21 de diciembre de 2023	–
v1.3.1	x86_64 (AMD64): `sha256:555578fcb7b73097ade5c8404390ef16cf76a7b568490abaae01ac75992b3ea29` Graviton (ARM64): `sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd`	Actualizaciones y revisiones de seguridad importantes.	23 de octubre de 2023	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Fin del soporte estándar ([1]).
v1.3.0	x86_64 (AMD64): `sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbe69530bfbd46c694` Graviton (ARM64): `sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb`	Compatible con la plataforma Ubuntu Compatible con la versión 1.28 de Kubernetes Mejoras generales de rendimiento y de estabilidad.	5 de octubre de 2023	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Fin del soporte estándar ([1]).
v1.2.0	x86_64 (AMD64): `sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3` Graviton (ARM64): `sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa`	Además de las instancias basadas en AMD64, la versión 1.2.0 ahora también admite las instancias basadas en ARM64. Se ha agregado compatibilidad con Bottlerocket y se ha verificado. Compatible con la versión 1.27 de Kubernetes Mejoras generales de rendimiento y de estabilidad.	16 de junio de 2023	–

Versión del agente	Imagen de contenedor	Notas de la versión	Fecha de disponibilidad	Fin del soporte estándar ([1]).
v1.1.0	`sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c`	Además de las Versiones de Kubernetes compatibles con el agente de seguridad GuardDuty , esta versión del agente también es compatible con la versión 1.26 de Kubernetes. Mejoras generales de rendimiento y de estabilidad.	2 de mayo de 2023	14 de mayo de 2024
v1.0.0	`sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e`	Versión inicial del agente del complemento de Amazon EKS.	30 de marzo de 2023	14 de mayo de 2024

- [1] Para obtener información sobre cómo actualizar la versión actual del agente que está a punto de finalizar el soporte estándar, consulteActualizar el agente de seguridad manualmente.

Protección de Amazon S3 en Amazon GuardDuty

S3 Protection ayuda a Amazon a GuardDuty supervisar AWS CloudTrail los eventos de datos de Amazon Simple Storage Service (Amazon S3), que incluyen operaciones de API a nivel de objeto para identificar posibles riesgos de seguridad para los datos contenidos en sus buckets de Amazon S3.

GuardDuty monitorea tanto los eventos de AWS CloudTrail administración como los eventos de datos de AWS CloudTrail S3 para identificar posibles amenazas en sus recursos de Amazon S3. Los dos orígenes de datos supervisan diferentes tipos de actividades. Algunos ejemplos de eventos de CloudTrail administración para S3 incluyen operaciones que muestran o configuran buckets de Amazon S3, como `ListBucketsDeleteBuckets`, y`PutBucketReplication`. Entre los ejemplos de eventos de CloudTrail datos para S3 se incluyen las operaciones de API a nivel de objeto, como`GetObject`,`ListObjects`, `DeleteObject` y. `PutObject`

Cuando habilitas Amazon GuardDuty para un Cuenta de AWS, GuardDuty comienza a monitorear los eventos CloudTrail de administración. No necesita habilitar ni configurar manualmente el registro de eventos de datos de S3 AWS CloudTrail. Puedes activar la función S3 Protection (que monitorea CloudTrail los eventos de datos de S3) para cualquier cuenta en cualquier Región de AWS lugar en el que esta función esté disponible en Amazon GuardDuty y en cualquier momento. Si Cuenta de AWS ya está habilitada GuardDuty, puede activar S3 Protection por primera vez con un período de prueba gratuito de 30 días. Si Cuenta de AWS se activa GuardDuty por primera vez, S3 Protection ya está activado e incluido en esta prueba gratuita de 30 días. Para obtener más información, consulte Estimación de costos GuardDuty .

Le recomendamos que active S3 Protection en GuardDuty. Si esta función no está habilitada, no GuardDuty podrá monitorizar completamente sus depósitos de Amazon S3 ni generar información sobre el acceso sospechoso a los datos almacenados en sus depósitos de S3.

¿Cómo GuardDuty utiliza los eventos de datos de S3

Cuando habilita los eventos de datos de S3 (protección de S3), GuardDuty comienza a analizar los eventos de datos de S3 de todos sus buckets de S3 y los monitorea para detectar actividades maliciosas o sospechosas. Para obtener más información, consulte AWS CloudTrail eventos de datos para S3.

Cuando un usuario no autenticado accede a un objeto de S3, significa que el objeto de S3 es de acceso público. Por lo tanto, GuardDuty no procesa dichas solicitudes. GuardDuty procesa las

solicitudes realizadas a los objetos S3 mediante credenciales de IAM (AWS Identity and Access Management) o AWS STS (AWS Security Token Service) válidas.

Cuando GuardDuty detecta una amenaza potencial en función de la supervisión de eventos de datos de S3, genera una comprobación de seguridad. Para obtener información sobre los tipos de hallazgos que GuardDuty se pueden generar para los buckets de Amazon S3, consulteGuardDuty Tipos de búsqueda S3.

Si deshabilita S3 Protection, GuardDuty detiene la supervisión de los eventos de datos de S3 de los datos almacenados en sus buckets de S3.

Configuración de la protección de S3 para una cuenta independiente

En el caso de las cuentas asociadas por AWS Organizations, este proceso se puede automatizar mediante la configuración de la consola. Para obtener más información, consulte Configuración de la protección de S3 en entornos con varias cuentas.

Habilitación o deshabilitación de la protección de S3

Elija el método de acceso que prefiera para configurar la protección de S3 para una cuenta independiente.

Console

1. Inicie sesión en la GuardDuty consola AWS Management Console y ábrala en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, elija Protección de S3.
3. En la página Protección de S3 se indica el estado actual de la protección de S3 de su cuenta. Seleccione Habilitar o Deshabilitar para habilitar o deshabilitar la protección de S3 en cualquier momento.
4. Elija Confirmar para confirmar su selección.

API/CLI

1. Ejecute updateDetector con su ID de detector válido para la región actual y transfiera el valor de `name` del objeto `features` como `S3_DATA_EVENTS` establecido en `ENABLED` o `DISABLED` para habilitar lo deshabilitar la protección de S3, respectivamente.

> **Note**
>
> Para encontrar la correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

2. Como alternativa, puede utilizar AWS Command Line Interface. Para habilitar la protección de S3, ejecute el siguiente comando y asegúrese de utilizar su propio ID de detector válido.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

   Para deshabilitar la protección de S3, sustituya `ENABLED` por `DISABLED` en el ejemplo.

Configuración de la protección de S3 en entornos con varias cuentas

En un entorno con varias cuentas, solo la cuenta de GuardDuty administrador delegado tiene la opción de configurar (activar o desactivar) S3 Protection para las cuentas de los miembros de su AWS organización. Las cuentas de GuardDuty los miembros no pueden modificar esta configuración desde sus cuentas. La cuenta de GuardDuty administrador delegado administra sus cuentas de miembros mediante AWS Organizations. La cuenta de GuardDuty administrador delegado puede elegir que S3 Protection se active automáticamente en todas las cuentas, solo en las cuentas nuevas o en ninguna cuenta de la organización. Para obtener más información, consulte Administración de cuentas con AWS Organizations.

Configuración de S3 Protection para la cuenta de administrador delegado GuardDuty

Elija su método de acceso preferido para configurar S3 Protection para la cuenta de GuardDuty administrador delegado.

Console

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de administración.
2. En el panel de navegación, elija Protección de S3.
3. En la página Protección de S3, seleccione Editar.

4. Realice una de las acciones siguientes:

   Uso de Habilitar para todas las cuentas

   - Elija Habilitar para todas las cuentas. Esto habilitará el plan de protección para todas las GuardDuty cuentas activas de su AWS organización, incluidas las cuentas nuevas que se unan a la organización.
   - Seleccione Guardar.

   Uso de Configurar cuentas manualmente

   - Para habilitar el plan de protección solo para la cuenta de GuardDuty administrador delegado, elija Configurar las cuentas manualmente.
   - Seleccione Activar en la sección de la cuenta de GuardDuty administrador delegado (esta cuenta).
   - Seleccione Guardar.

API/CLI

updateDetectorPara ello, utilice el identificador de detector de la cuenta de GuardDuty administrador delegado para la región actual y pase el `features` objeto `name` como `S3_DATA_EVENTS` y `status` como `ENABLED` o. `DISABLED`

Como alternativa, puede configurar S3 Protection mediante AWS Command Line Interface. *Ejecute el siguiente comando y asegúrese de sustituir 12abc34d567e8fa901bc2d34e56789f0 por el ID de detector de la cuenta de administrador delegado de la región actual y 555555555555 por el ID de la cuenta de administrador delegado. GuardDuty* Cuenta de AWS GuardDuty

Para encontrar el de su cuenta y su región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/. **`detectorId`**

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 555555555555 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

Habilitación automática de la protección de S3 para todas las cuentas de miembros de la organización

Console

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Inicie sesión con su cuenta de administrador.

2. Realice una de las acciones siguientes:

   Uso de la página Protección de S3

   1. En el panel de navegación, elija Protección de S3.
   2. Elija Habilitar para todas las cuentas. Esta acción habilita automáticamente la protección de S3 para las cuentas nuevas y existentes de la organización.
   3. Seleccione Guardar.

   > **Note**
   >
   > La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

   Uso de la página Cuentas

   1. En el panel de navegación, elija Accounts (Cuentas).
   2. En la página Cuentas, seleccione las preferencias para Habilitar automáticamente antes de Agregar cuentas mediante invitación.
   3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para todas las cuentas en Protección de S3.
   4. Seleccione Guardar.

   Si no puede utilizar la opción Habilitar para todas las cuentas, consulte Habilitación o deshabilitación selectiva de la protección de S3 para las cuentas de miembros.

API/CLI

- Para habilitar o deshabilitar la protección de S3 de forma selectiva para las cuentas de miembros, invoque la operación de la API updateMemberDetectors con su propio *ID de detector*.
- En el siguiente ejemplo se muestra cómo se puede habilitar la protección de S3 para una sola cuenta de miembro. *Asegúrese de sustituir 12abc34d567e8fa901bc2d34e56789f0 por la cuenta de administrador delegado y 111122223333. detector-id GuardDuty* Para deshabilitar la protección de S3, sustituya `ENABLED` por `DISABLED`.

  Para `detectorId` encontrar la correspondiente a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación de la protección de S3 para todas las cuentas de miembros activas existentes

Elija su método de acceso preferido para habilitar la protección de S3 en todas las cuentas de miembros activas existentes de la organización.

Console

1. Inicia sesión en la GuardDuty consola AWS Management Console y ábrela en https://console.aws.amazon.com/guardduty/.

   Inicie sesión con las credenciales de la cuenta GuardDuty de administrador delegado.
2. En el panel de navegación, elija Protección de S3.

3. En la página Protección de S3, puede ver el estado actual de la configuración. En la sección Cuentas de miembros activas, seleccione Acciones.
4. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
5. Seleccione Confirmar.

API/CLI

- Para habilitar o deshabilitar la protección de S3 de forma selectiva para las cuentas de miembros, invoque la operación de la API updateMemberDetectors con su propio *ID de detector*.
- En el siguiente ejemplo se muestra cómo se puede habilitar la protección de S3 para una sola cuenta de miembro. *Asegúrese de sustituir 12abc34d567e8fa901bc2d34e56789f0 por la cuenta de administrador delegado y 111122223333. detector-id GuardDuty* Para deshabilitar la protección de S3, sustituya `ENABLED` por `DISABLED`.

  Para `detectorId` encontrar la correspondiente a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación automática de la protección de S3 para las cuentas de nuevos miembros

Elija su método de acceso preferido para habilitar la protección de S3 para las cuentas nuevas que se unan a la organización.

Console

La cuenta de GuardDuty administrador delegado puede habilitar nuevas cuentas de miembros en una organización a través de la consola, desde la página de Protección de S3 o desde la página de Cuentas.

Habilitación automática de la protección de S3 para las cuentas de nuevos miembros

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.
2. Realice una de las acciones siguientes:
   - Uso de la página Protección de S3:
     1. En el panel de navegación, elija Protección de S3.
     2. En la página Protección de S3, seleccione Editar.
     3. Elija Configurar cuentas manualmente.
     4. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que cada vez que una nueva cuenta se una a su organización, la protección de S3 se habilitará automáticamente para la cuenta. Solo la cuenta de GuardDuty administrador delegado de la organización puede modificar esta configuración.
     5. Seleccione Guardar.
   - Mediante la página Cuentas:
     1. En el panel de navegación, elija Accounts (Cuentas).
     2. En la página Cuentas, seleccione Habilitar automáticamente las preferencias.
     3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para las nuevas cuentas en Protección de S3.
     4. Seleccione Guardar.

API/CLI

- Para habilitar o deshabilitar la protección de S3 de forma selectiva para las cuentas de miembros, invoque la operación de la API UpdateOrganizationConfiguration con su propio *ID de detector*.

- En el siguiente ejemplo se muestra cómo se puede habilitar la protección de S3 para una sola cuenta de miembro. Para deshabilitar esta característica, consulte Activación o desactivación de la Protección de RDS para las cuentas de miembros de forma selectiva. Establezca las preferencias para habilitar o deshabilitar automáticamente el plan de protección en esa región para las nuevas cuentas (`NEW`) que se unan a la organización, todas las cuentas (`ALL`) o ninguna de las cuentas (`NONE`) de la organización. Para obtener más información, consulte autoEnableOrganizationMiembros. Según sus preferencias, es posible que deba sustituir `NEW` por `ALL` o `NONE`.

  Para encontrar la correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
   "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
  ```

  > **Note**
  >
  > También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilitación o deshabilitación selectiva de la protección de S3 para las cuentas de miembros

Elija el método de acceso que prefiera para habilitar o deshabilitar de forma selectiva la protección de S3 en las cuentas de miembros.

Console

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. En el panel de navegación, elija Accounts (Cuentas).

En la página Cuentas, revise la columna Protección de S3 para ver el estado de su cuenta de miembro.

3. Habilitación o deshabilitación selectiva de la protección de S3

   Seleccione la cuenta para la que desee configurar la protección de S3. Puede seleccionar varias cuentas de manera simultánea. En el menú desplegable Editar planes de protección, seleccione S3Pro y, a continuación, elija la opción adecuada.

API/CLI

Para habilitar o deshabilitar la protección de S3 de forma selectiva para las cuentas de miembros, ejecute la operación de la API updateMemberDetectors con su propio ID de detector. En el siguiente ejemplo se muestra cómo se puede habilitar la protección de S3 para una sola cuenta de miembro. Para desactivarlo, sustituya `true` por `false`.

Para encontrar las de `detectorId` su cuenta y su región actual, consulte la página de configuración en la consola https://console.aws.amazon.com/guardduty/.

```
 aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features
 '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

> **Note**
>
> También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

> **Note**
>
> Si utiliza scripts para incorporar nuevas cuentas y desea deshabilitar la protección de S3 en sus nuevas cuentas, puede modificar la operación de la API createDetector con el objeto `dataSources` opcional, tal y como se describe en este tema.

Desactivar automáticamente S3 Protection para cuentas nuevas GuardDuty

> **Important**
>
> De forma predeterminada, la protección de S3 se habilita automáticamente para Cuentas de AWS esa unión GuardDuty por primera vez.

Si es GuardDuty administrador y habilita una cuenta nueva GuardDuty por primera vez y no quiere que S3 Protection esté habilitada de forma predeterminada, puede deshabilitarla modificando la operación de la createDetectorAPI con el `features` objeto opcional. En el siguiente ejemplo, se utiliza AWS CLI para activar un GuardDuty detector nuevo con la protección S3 desactivada.

```
aws guardduty create-detector --enable --features '[{"Name" : "S3_DATA_EVENTS",
"Status" : "DISABLED"}]'
```

Característica en la protección de S3

AWS CloudTrail eventos de datos para S3

En los eventos de datos, también conocidos como operaciones del plano de datos, se muestra información sobre las operaciones de recursos llevadas a cabo en un recurso determinado. Suelen ser actividades de gran volumen.

Los siguientes son ejemplos de eventos de CloudTrail datos para S3 que GuardDuty se pueden monitorear:

- Operaciones de la API de `GetObject`
- Operaciones de la API de `PutObject`
- Operaciones de la API de `ListObjects`
- Operaciones de la API de `DeleteObject`

Cuando se activa GuardDuty por primera vez, S3 Protection está activado de forma predeterminada y también se incluye en el período de prueba gratuito de 30 días. Sin embargo, esta característica es opcional y puede habilitarla o deshabilitarla para cualquier cuenta o región en cualquier momento. Para obtener más información sobre cómo configurar Amazon S3 como una característica, consulte GuardDuty Protección S3.

Entender los GuardDuty hallazgos de Amazon

Un GuardDuty hallazgo representa un posible problema de seguridad detectado en su red. GuardDutygenera un hallazgo cada vez que detecta una actividad inesperada y potencialmente maliciosa en su AWS entorno.

Puede ver y gestionar sus GuardDuty hallazgos en la página Hallazgos de la GuardDuty consola o mediante las AWS CLI operaciones de la API. Para obtener información general de las formas en las que puede administrar los resultados, consulte Gestión de los GuardDuty hallazgos de Amazon.

Temas:

Detalles de los resultados

En la GuardDuty consola de Amazon, puedes ver los detalles de búsqueda en la sección de resumen de búsquedas. Los detalles de los resultados varían según el tipo de resultado.

Hay dos detalles principales que determinarán qué tipo de información está disponibles para cualquier resultado. El primero es el tipo de recurso, que puede ser `Instance`, `AccessKey`, `S3Bucket`, `Kubernetes cluster`, `ECS cluster`, `Container`, `RDSDBInstance` o `Lambda`. El segundo detalle que determina la información de los resultados es el rol del recurso. El rol del

recurso puede ser `Target` para las claves de acceso, lo que significa que el recurso fue objeto de una actividad sospechosa. En el caso de resultados por tipo de instancia, el rol del recurso también puede ser `Actor`, lo que significa que el recurso fue el actor que ha llevado a cabo la actividad sospechosa. En este tema, se describen algunos de los detalles de los resultados que se encuentran disponibles con más frecuencia.

Información general de los resultados

La sección Información general de un resultado contiene las características identificativas más básicas del resultado, incluida la siguiente información:

- ID de cuenta: el ID de la AWS cuenta en la que se llevó GuardDuty a cabo la actividad que provocó la generación de este hallazgo.
- Recuento: el número de veces que GuardDuty se ha agregado una actividad que coincide con este patrón con este identificador de búsqueda.
- Hora de creación: fecha y hora en que se ha creado este resultado por primera vez. Si este valor difiere de Hora de actualización, indica que la actividad se ha producido varias veces y es un problema continuo.

> **Note**
>
> Las marcas de tiempo de las búsquedas en la GuardDuty consola aparecen en la zona horaria local, mientras que las exportaciones de JSON y las salidas de CLI muestran las marcas de tiempo en UTC.

- ID de resultado: un identificador único para este tipo de resultado y conjunto de parámetros. Las nuevas ocurrencias de actividad que coincidan con este patrón se añadirán al mismo ID.
- Tipo de resultado: una cadena formateada que representa el tipo de actividad que ha desencadenado el resultado. Para obtener más información, consulte Formato de búsqueda GuardDuty.
- Región: la AWS región en la que se generó el hallazgo. Para obtener más información acerca de las regiones admitidas, consulte Regiones y puntos de conexión
- ID de recurso: el ID del AWS recurso con el que se llevó GuardDuty a cabo la actividad que provocó la generación de este hallazgo.
- ID de escaneo: se aplica a los hallazgos cuando la protección contra GuardDuty malware está habilitada y es un identificador del escaneo de malware que se ejecuta en los volúmenes de

EBS conectados a la carga de trabajo de la instancia EC2 o del contenedor potencialmente comprometida. Para obtener más información, consulte Detalles de los resultados de la protección contra malware.

- Gravedad: un nivel de gravedad alta, mediana o baja asignado al resultado. Para obtener más información, consulte Niveles de gravedad de GuardDuty los hallazgos.
- Actualizado el: la última vez que se actualizó este hallazgo con una nueva actividad que coincidía con el patrón que llevó GuardDuty a generar este hallazgo.

Recurso

El recurso afectado proporciona detalles sobre el AWS recurso al que se dirigió la actividad iniciadora. La información disponible variará según el tipo de recurso y el tipo de acción.

Función de recurso: la función del AWS recurso que inició la búsqueda. Este valor puede ser TARGET o ACTOR y representa si su recurso era el objetivo de la actividad sospechosa o si era el actor que ha llevado a cabo la actividad sospechosa, respectivamente.

Tipo de recurso: el tipo del recurso afectado. Si estuvieron involucrados varios recursos, un resultado puede incluir varios tipos de recursos. Los tipos de recursos son Instance, S3Bucket AccessKey, ECSCluster KubernetesCluster, Container, RDSDBInstance y Lambda. En función del tipo de recurso, habrá distintos detalles disponibles sobre el resultado. Seleccione una pestaña de opciones de recurso para obtener información sobre los detalles disponibles de ese recurso.

Instance

Detalles de la instancia:

> **Note**
>
> Es posible que falten algunos detalles de la instancia si esta ya se ha detenido o si la invocación a la API subyacente se ha originado en una instancia de EC2 en una región diferente al hacer una llamada a la API entre regiones.

- ID de instancia: el ID de la instancia de EC2 implicada en la actividad que provocó la generación del hallazgo. GuardDuty
- Tipo de instancia: el tipo de instancia de EC2 implicada en el resultado.

- Hora de lanzamiento: la fecha y hora en que se lanzó la instancia.
- Outpost ARN: el nombre del recurso de Amazon (ARN) de. AWS Outposts Solo se aplica a las instancias. AWS Outposts Para obtener más información, consulte ¿Qué es AWS Outposts?
- Nombre del grupo de seguridad: el nombre del grupo de seguridad asociado a la instancia en cuestión.
- ID del grupo de seguridad: el ID del grupo de seguridad asociado a la instancia en cuestión.
- Estado de la instancia: el estado actual de la instancia afectada.
- Zona de disponibilidad: la zona de disponibilidad de la región de AWS en la que se encuentra la instancia en cuestión.
- ID de imagen: el ID de la imagen de máquina de Amazon utilizada para crear la instancia implicada en la actividad.
- Descripción de la imagen: una descripción del ID de la imagen de máquina de Amazon utilizada para crear la instancia implicada en la actividad.
- Etiquetas: una lista de etiquetas adjuntas a este recurso, enumeradas en el formato de `key-value`.

AccessKey

Detalles de la clave de acceso:

- ID de clave de acceso: ID de clave de acceso del usuario que participó en la actividad GuardDuty que provocó la generación del hallazgo.
- ID principal: el ID principal del usuario que participó en la actividad que provocó GuardDuty la generación del hallazgo.
- Tipo de usuario: el tipo de usuario que participó en la actividad que provocó GuardDuty la generación del hallazgo. Para obtener más información, consulte Elemento userIdentity de CloudTrail .
- Nombre de usuario: el nombre del usuario que participó en la actividad que provocó GuardDuty la generación del hallazgo.

S3Bucket

Detalles del bucket de Amazon S3:

- Nombre: el nombre del bucket implicado en el resultado.

- ARN: el ARN del bucket implicado en el resultado.
- Propietario: el ID canónico del usuario propietario del bucket implicado en el resultado. Para más información acerca de los ID de usuario canónico, consulte AWS account identifiers.
- Tipo: el tipo de resultado del bucket, que puede ser de Destino o de Origen.
- Cifrado predeterminado del servidor: los detalles de cifrado del bucket.
- Etiquetas del bucket: una lista de etiquetas asociadas a este recurso, enumeradas en el formato de `key-value`.
- Permisos efectivos: una evaluación de todos los permisos y políticas efectivos del bucket que indica si el bucket en cuestión está expuesto públicamente. Los valores pueden ser Público o No público.

EKSCluster

Detalles del clúster de Kubernetes:

- Nombre: el nombre del clúster de Kubernetes.
- ARN: el ARN que identifica al clúster.
- Hora de creación: fecha y hora en que se ha creado este clúster.

> **Note**
>
> Las marcas de tiempo de las búsquedas en la GuardDuty consola aparecen en la zona horaria local, mientras que las exportaciones de JSON y las salidas de CLI muestran las marcas de tiempo en UTC.

- ID de VPC: el ID de la VPC asociada al clúster.
- Estado: el estado actual del clúster.
- Etiquetas: los metadatos que se aplican a los clústeres para ayudarle a categorizarlos y organizarlos. Cada etiqueta consta de una clave y un valor opcional, mostrada en el formato `key-value`. Puede definir tanto la clave como el valor.

  Las etiquetas del clúster no se propagan a ningún otro recurso asociado al clúster.

Detalles de la carga de trabajo de Kubernetes:

- Tipo: el tipo de carga de trabajo de Kubernetes, como el pod, la implementación y el trabajo.

- Nombre: el nombre de la carga de trabajo de Kubernetes.
- Uid: el ID único de la carga de trabajo de Kubernetes.
- Hora de creación: fecha y hora en que se ha creado esta carga de trabajo.
- Etiquetas: los pares de clave-valor asociados a la carga de trabajo de Kubernetes.
- Contenedores: los detalles del contenedor que se ejecuta como parte de la carga de trabajo de Kubernetes.
- Espacio de nombres: la carga de trabajo pertenece a este espacio de nombres de Kubernetes.
- Volúmenes: los volúmenes que utiliza la carga de trabajo de Kubernetes.
  - Ruta del host: representa un archivo o directorio preexistente en la máquina host al que se asigna el volumen.
  - Nombre: el nombre del volumen.
- Contexto de seguridad del pod: define la configuración de privilegios y control de acceso para todos los contenedores de un pod.
- Red de host: se establece como `true` si los pods se han incluido en la carga de trabajo de Kubernetes.

Detalles de usuario de Kubernetes:

- Grupos: grupos de RBAC (control basado en el acceso a roles) de Kubernetes del usuario que ha participado en la actividad que generó el resultado.
- ID: el ID única del usuario de Kubernetes.
- Nombre de usuario: nombre del usuario de Kubernetes que ha participado en la actividad que generó el resultado.
- Nombre de sesión: entidad que ha asumido el rol de IAM con los permisos de RBAC de Kubernetes.

ECSCluster

Detalles del clúster de ECS:

- ARN: el ARN que identifica al clúster.
- Nombre: el nombre del clúster.
- Estado: el estado actual del clúster.

- Recuento de servicios activos: la cantidad de servicios que se ejecutan en el clúster en un estado `ACTIVE`. Puedes ver estos servicios con ListServices
- Recuento de instancias de contenedor registradas: el número de instancias de contenedor registradas en el clúster. Esto incluye las instancias de contenedor tanto en estado `ACTIVE` como `DRAINING`.
- Recuento de tareas en ejecución: el número de tareas del clúster que se encuentran en estado `RUNNING`.
- Etiquetas: los metadatos que se aplican a los clústeres para ayudarle a categorizarlos y organizarlos. Cada etiqueta consta de una clave y un valor opcional, mostrada en el formato `key-value`. Puede definir tanto la clave como el valor.
- Contenedores: los detalles sobre el contenedor asociado a la tarea:
  - Nombre del contenedor: el nombre del contenedor.
  - Imagen del contenedor: la imagen del contenedor.
- Detalles de la tarea: los detalles de una tarea en un clúster.
  - ARN: el nombre de recurso de Amazon (ARN) de la tarea.
  - ARN de definición: el nombre de recurso de Amazon (ARN) de la definición de tarea que crea esta.
  - Versión: el contador de versiones de la tarea.
  - Hora de creación de la tarea: la marca de tiempo de Unix en la que se ha creado la tarea.
  - Hora de inicio de la tarea: la marca de tiempo de Unix cuando se ha iniciado la tarea.
  - Tarea iniciada por: la etiqueta especificada cuando se inicia una tarea.

Container

Detalles del contenedor:

- Tiempo de ejecución del contenedor: el tiempo de ejecución del contenedor (por ejemplo, `docker` o `containerd`) utilizado para ejecutar el contenedor.
- ID: el ID de la instancia de contenedor o las entradas de ARN completas de la instancia de contenedor.
- Nombre: el nombre del contenedor.

  Cuando está disponible, este campo muestra el valor de la etiqueta `io.kubenetes.container.name`.

- Imagen: la imagen de la instancia de contenedor.
- Monturas de volumen: lista de monturas de volumen de contenedores. Un contenedor puede montar un volumen en su sistema de archivos.
- Contexto de seguridad: el contexto de seguridad de contenedor define la configuración de privilegios y control de acceso de un contenedor.
- Detalles del proceso: describe los detalles del proceso asociado al resultado.

RDSDBInstance

Detalles de RDSDBInstance:

> **Note**
>
> Este recurso está disponible en los resultados de la protección de RDS relacionados con la instancia de base de datos.

- ID de instancia de base de datos: el identificador asociado a la instancia de base de datos que participó en la GuardDuty búsqueda.
- Motor: el nombre del motor de base de datos de la instancia de base de datos implicada en el resultado. Los valores posibles son Compatible con Aurora MySQL o Compatible con Aurora PostgreSQL.
- Versión del motor: la versión del motor de base de datos que participó en la GuardDuty búsqueda.
- ID del clúster de base de datos: el identificador del clúster de base de datos que contiene el ID de la instancia de base de datos implicada en la GuardDuty búsqueda.
- ARN de instancia de base de datos: el ARN que identifica la instancia de base de datos implicada en el hallazgo. GuardDuty

Lambda

Detalles de la función de Lambda

- Nombre de la función: el nombre de la función de Lambda implicada en el resultado.
- Versión de la función: la versión de la función de Lambda implicada en el resultado.

- Descripción de la función: una descripción de la función de Lambda implicada en el resultado.
- ARN de la función: el nombre de recurso de Amazon (ARN) de la función de Lambda implicada en el resultado.
- ID de revisión: el ID de revisión de la versión de la función de Lambda.
- Rol: el rol de ejecución de la función de Lambda implicada en el resultado.
- Configuración de VPC: la configuración de Amazon VPC, que incluye el ID de VPC, el grupo de seguridad y los ID de subred asociados a la función de Lambda.
- ID de VPC: el ID de Amazon VPC asociada a la función de Lambda implicada en el resultado.
- ID de subred: los ID de las subredes asociadas a la función de Lambda.
- Grupo de seguridad: el grupo de seguridad asociado a la función de Lambda implicada. Esto incluye el nombre del grupo de seguridad y el ID de grupo.
- Etiquetas: una lista de etiquetas adjuntas a este recurso, con el formato de pares de `key-value`.

Detalles de usuario de la base de datos (DB) de RDS

> **Note**
>
> Esta sección se aplica a los hallazgos cuando se habilita la función de protección RDS en. GuardDuty Para obtener más información, consulte GuardDuty Protección RDS.

El GuardDuty hallazgo proporciona los siguientes detalles de usuario y autenticación de la base de datos potencialmente comprometida.

- Usuario: el nombre de usuario utilizado para llevar a cabo el intento de inicio de sesión anómalo.
- Aplicación: el nombre de la aplicación utilizada para llevar a cabo el intento de inicio de sesión anómalo.
- Base de datos: el nombre de la instancia de base de datos implicada en el intento de inicio de sesión anómalo.
- SSL: la versión de capa de sockets seguros (SSL) utilizada para la red.
- Método de autenticación: el método de autenticación utilizado por el usuario implicado en el resultado.

Detalles de búsqueda de Runtime Monitoring

> **Note**
>
> Es posible que estos detalles estén disponibles solo si GuardDuty genera uno de los[Tipos de búsqueda de Runtime Monitoring](#).

Esta sección contiene los detalles del tiempo de ejecución, como los detalles del proceso y cualquier contexto necesario. Los detalles del proceso describen la información sobre el proceso observado y el contexto del tiempo de ejecución describe cualquier información adicional sobre la actividad potencialmente sospechosa.

Detalles del proceso

- Nombre: el nombre del proceso.
- Ruta ejecutable: la ruta absoluta del archivo ejecutable del proceso.
- SHA-256 ejecutable: el hash SHA256 del ejecutable del proceso.
- PID del espacio de nombres: el ID del proceso en un espacio de nombres de PID secundario distinto del espacio de nombres de PID del host. En el caso de los procesos dentro de un contenedor, es el ID de proceso observado dentro del contenedor.
- Directorio de trabajo actual: el directorio de trabajo actual del proceso.
- ID del proceso: el ID asignado al proceso por el sistema operativo.
- startTime: la hora en la que se ha iniciado el proceso. Está en formato de cadena de fecha UTC (`2023-03-22T19:37:20.168Z`).
- UUID: el identificador único asignado al proceso por GuardDuty.
- UUID principal: el ID único del proceso principal. Este ID lo asigna al proceso principal. GuardDuty
- Usuario: el usuario que ha ejecutado el proceso.
- ID del usuario: el ID del usuario que ha ejecutado el proceso.
- ID del usuario efectivo: el ID del usuario efectivo del proceso en el momento del evento.
- Linaje: información sobre los antepasados del proceso.
  - ID del proceso: el ID asignado al proceso por el sistema operativo.
  - UUID: el identificador único asignado al proceso por GuardDuty.

- Ruta ejecutable: la ruta absoluta del archivo ejecutable del proceso.
- ID del usuario efectivo: el ID del usuario efectivo del proceso en el momento del evento.
- UUID principal: el ID único del proceso principal. Este ID lo asigna al proceso principal. GuardDuty
- Hora de inicio: la hora en la que se ha iniciado el proceso.
- PID del espacio de nombres: el ID del proceso en un espacio de nombres de PID secundario distinto del espacio de nombres de PID del host. En el caso de los procesos dentro de un contenedor, es el ID de proceso observado dentro del contenedor.
- ID del usuario: el ID del usuario que ejecutó el proceso.
- Nombre: el nombre del proceso.

Contexto del tiempo de ejecución

De los siguientes campos, un resultado generado puede incluir solo los campos que son relevantes para el tipo de resultado.

- Origen de la montura: la ruta en el host que monta el contenedor.
- Destino de la montura: la ruta del contenedor que está asignada al directorio del host.
- Tipo de sistema de archivos: representa el tipo de sistema de archivos montado.
- Marcas: representan las opciones que controlan el comportamiento del evento implicado en este resultado.
- Proceso de modificación: información sobre el proceso que ha creado o modificado un binario, un script o una biblioteca dentro de un contenedor en tiempo de ejecución.
- Modificado el: la marca de tiempo en la que el proceso ha creado o modificado un binario, un script o una biblioteca dentro de un contenedor en tiempo de ejecución. Este campo está en formato de cadena de fecha UTC (`2023-03-22T19:37:20.168Z`).
- Ruta de la biblioteca: la ruta a la nueva biblioteca que se ha cargado.
- Valor de precarga de LD: el valor de la variable de entorno `LD_PRELOAD`.
- Ruta del socket: la ruta al socket de Docker al que se accedió.
- Ruta al binario Runc: la ruta al binario `runc`.
- Ruta del agente de lanzamiento: la ruta al archivo del agente de lanzamiento del `cgroup`.
- Ejemplo de línea de comandos: ejemplo de la línea de comandos implicada en la actividad potencialmente sospechosa.

- Categoría de herramienta: categoría a la que pertenece la herramienta. Algunos de los ejemplos son Backdoor Tool, Pentest Tool, Network Scanner y Network Sniffer.
- Nombre de la herramienta: el nombre de la herramienta potencialmente sospechosa.
- Ruta del script: la ruta al script ejecutado que generó el hallazgo.
- Ruta del archivo de amenazas: la ruta sospechosa en la que se encontraron los detalles de la inteligencia de amenazas.
- Nombre del servicio: el nombre del servicio de seguridad que se ha desactivado.

Detalles del análisis de volúmenes de EBS

> **Note**
>
> Esta sección se aplica a los hallazgos al activar el análisis GuardDuty de malware iniciado. GuardDuty Protección contra malware

El análisis de volúmenes de EBS proporciona detalles sobre el volumen de EBS asociado a la carga de trabajo del contenedor o la instancia de EC2 potencialmente afectada.

- ID de análisis: el identificador del análisis de malware.
- Análisis iniciado el: la fecha y hora en que inició el análisis de malware.
- Análisis completado el: la fecha y la hora en que se completó el análisis de malware.
- Identificador de búsqueda de activación: el identificador de GuardDuty búsqueda del descubrimiento que inició este análisis de malware.
- Orígenes: los valores posibles son `Bitdefender` y `AWS`.
- Detecciones de análisis: la vista completa de los detalles y los resultados de cada análisis de malware.
  - Recuento de elementos analizados: el número total de archivos analizados. Proporciona detalles como `totalGb`, `files` y `volumes`.
  - Recuento de elementos de amenazas detectadas: el número total de `files` maliciosos detectados durante el análisis.
  - Detalles de las amenazas de mayor gravedad: los detalles de la amenaza de mayor gravedad detectada durante el análisis y el número de archivos maliciosos. Proporciona detalles como `severity`, `threatName` y `count`.

- Amenazas detectadas por nombre: el elemento del contenedor que agrupa las amenazas de todos los niveles de gravedad. Proporciona detalles como `itemCount`, `uniqueThreatNameCount`, `shortened` y `threatNames`.

Detalles de los resultados de la protección contra malware

> **Note**
>
> Esta sección se aplica a los datos detectados al activar el análisis GuardDuty de malware iniciado. GuardDuty Protección contra malware

Cuando el análisis de Protección contra malware detecte malware, podrá ver los detalles del análisis al seleccionar el resultado correspondiente en la página Resultados de la consola https://console.aws.amazon.com/guardduty/. La gravedad del hallazgo de protección contra malware depende de la gravedad del GuardDuty hallazgo.

> **Note**
>
> La etiqueta `GuardDutyFindingDetected` especifica que las instantáneas contienen malware.

La siguiente información está disponible en la sección Amenazas detectadas del panel de detalles.

- Nombre: el nombre de la amenaza, obtenido al agrupar los archivos por detección.
- Gravedad: el nivel de gravedad de la amenaza detectada.
- Hash: el SHA-256 del archivo.
- Ruta de archivo: la ubicación del archivo malicioso en el volumen de EBS.
- Nombre de archivo: el nombre del archivo en el que se detectó la amenaza.
- ARN del volumen: el ARN de los volúmenes de EBS analizados.

La siguiente información está disponible en la sección Detalles del análisis de malware del panel de detalles.

- ID de análisis: el ID del análisis de malware.

- Análisis iniciado el: la fecha y hora en que inició el análisis.
- Análisis completado el: la fecha y la hora en que se completó el análisis.
- Archivos analizados: el número total de archivos y directorios analizados.
- Total de GB analizados: la cantidad de almacenamiento analizada durante el proceso.
- Identificador de detección del disparador: el identificador de GuardDuty búsqueda del hallazgo que inició este análisis de malware.
- La siguiente información está disponible en la sección Detalles del volumen del panel de detalles.
  - ARN del volumen: el nombre de recurso de Amazon (ARN) del volumen.
  - SnapshotARN: el ARN de la instantánea del volumen de EBS.
  - Estado: el estado de análisis del volumen, como `Running`, `Skipped` y `Completed`.
  - Tipo de cifrado: el tipo de cifrado utilizado en el volumen. Por ejemplo, `CMCMK`.
  - Nombre del dispositivo: el nombre del dispositivo. Por ejemplo, `/dev/xvda`.

Acción

La acción de un resultado proporciona detalles sobre el tipo de actividad que desencadenó el resultado. La información disponible variará en función del tipo de acción.

Tipo de acción: el tipo de actividad del resultado. Este valor puede ser NETWORK_CONNECTION, PORT_PROBE, DNS_REQUEST, AWS_API_CALL o RDS_LOGIN_ATTEMPT. La información disponible variará en función del tipo de acción:

- NETWORK_CONNECTION: indica que hubo un intercambio de tráfico de la red entre la instancia de EC2 identificada y el host remoto. Este tipo de acción presenta la siguiente información adicional:
  - Dirección de conexión: la dirección de conexión de red observada en la actividad GuardDuty que provocó la detección. Puede ser uno de los siguientes valores:
    - INBOUND: indica que un host remoto inició una conexión con un puerto local en la instancia de EC2 identificada en su cuenta.
    - OUTBOUND: indica que la instancia de EC2 identificada inició una conexión a un host remoto.
    - Desconocido: indica que no se GuardDuty pudo determinar la dirección de la conexión.
  - Protocolo: el protocolo de conexión de red observado en la actividad que provocó GuardDuty la generación del hallazgo.

  - IP local: la dirección IP de origen original del tráfico que activó el resultado. Se puede usar esta información para distinguir entre la dirección IP de una capa intermedia a través de la que fluye el tráfico y la dirección IP de origen original del tráfico que desencadenó la búsqueda. Por ejemplo, la dirección IP de un pod EKS en lugar de la dirección IP de la instancia en la que se ejecuta el pod EKS.
  - Bloqueado: indica si el puerto objetivo está bloqueado.
- PORT_PROBE: indica que un host remoto sondeó la instancia de EC2 identificada en varios puertos abiertos. Este tipo de acción presenta la siguiente información adicional:
  - IP local: la dirección IP de origen original del tráfico que activó el resultado. Se puede usar esta información para distinguir entre la dirección IP de una capa intermedia a través de la que fluye el tráfico y la dirección IP de origen original del tráfico que desencadenó la búsqueda. Por ejemplo, la dirección IP de un pod EKS en lugar de la dirección IP de la instancia en la que se ejecuta el pod EKS.
  - Bloqueado: indica si el puerto objetivo está bloqueado.
- DNS_REQUEST: indica que la instancia de EC2 identificada consultó un nombre de dominio. Este tipo de acción presenta la siguiente información adicional:
  - Protocolo: el protocolo de conexión de red observado en la actividad que provocó GuardDuty la generación del hallazgo.
  - Bloqueado: indica si el puerto objetivo está bloqueado.
- AWS_API_CALL: indica que se ha invocado una API de AWS . Este tipo de acción presenta la siguiente información adicional:
  - API: el nombre de la operación de API que se invocó y, por lo tanto, se GuardDuty le pidió que generara este hallazgo.

    > **Note**
    >
    > Estas operaciones también pueden incluir eventos que no pertenecen a la API capturados por AWS CloudTrail. Para obtener más información, consulte Eventos ajenos a la API capturados por CloudTrail.

  - Agente de usuario: el agente de usuario que hizo la solicitud de API. Este valor indica si la llamada se realizó desde AWS Management Console, un AWS servicio, los AWS SDK o el. AWS CLI
  - CÓDIGO DE ERROR: si una llamada fallida a la API ha desencadenado el resultado, se muestra el código de error de esa llamada.

  - Nombre del servicio: el nombre de DNS del servicio que ha intentado hace la llamada a la API que desencadenó el resultado.
- RDS_LOGIN_ATTEMPT: indica que se intentó iniciar sesión en la base de datos potencialmente afectada desde una dirección IP remota.
  - Dirección IP: la dirección IP remota que se utilizó para llevar a cabo el intento de inicio de sesión potencialmente sospechoso.

Actor u objetivo

Un resultado tendrá una sección Actor si el Rol de recurso era `TARGET`. Esto indica que su recurso fue objeto de actividad sospechosa y la sección Actor contendrá detalles sobre la entidad que tenía el recurso como objetivo.

Un resultado tendrá una sección Objetivo si el Rol de recurso era `ACTOR`. Esto indica que su recurso estuvo involucrado en actividad sospechosa contra un host remoto y esta sección contendrá información sobre la IP o el dominio que era el objetivo de su recurso.

La información disponible en la sección Actor u Objetivo puede incluir lo siguiente:

- Afiliado: detalla si la AWS cuenta de la persona que llama a la API remota está relacionada con su GuardDuty entorno. Si este valor es `true`, la persona que llama a la API está afiliada a su cuenta de alguna manera; si es `false`, la persona que llama a la API es ajena a su entorno.
- ID de cuenta remota: el ID de cuenta propietario de la dirección IP saliente que se utilizó para acceder al recurso en la red final.
- Dirección IP: la dirección IP implicada en la actividad que provocó GuardDuty la generación del hallazgo.
- Ubicación: información de ubicación de la dirección IP implicada en la actividad que provocó GuardDuty la generación del hallazgo.
- Organización: información de la organización del ISP sobre la dirección IP implicada en la actividad que motivó GuardDuty la generación del hallazgo.
- Puerto: el número de puerto implicado en la actividad que motivó GuardDuty la generación del hallazgo.
- Dominio: el dominio implicado en la actividad que motivó GuardDuty la generación del hallazgo.
- Dominio con sufijo: el dominio de segundo y superior nivel implicado en una actividad que podría provocar la generación del hallazgo. GuardDuty Para obtener una lista de los dominios de nivel superior y segundo nivel, consulte la lista de sufijos públicos.

Información adicional

Todos los resultados tienen una sección de Información adicional donde se puede encontrar la siguiente información:

- Nombre de la lista de amenazas: el nombre de la lista de amenazas que incluye la dirección IP o el nombre de dominio implicados en la actividad que provocó la GuardDuty búsqueda.
- Muestra: un valor verdadero o falso que indica si se trata de un resultado de muestra.
- Archivado: un valor verdadero o falso que indica si el resultado se ha archivado.
- Inusual: detalles de las actividades que no se han observado históricamente. Pueden incluir cualquier usuario, hora, ubicación, bucket, comportamiento de inicio de sesión u organización de ASN inusuales (no observados previamente).
- Protocolo inusual: el protocolo de conexión de red implicado en la actividad GuardDuty que provocó la generación del hallazgo.
- Detalles del agente: detalles sobre el agente de seguridad que está implementado actualmente en el clúster de EKS de su Cuenta de AWS. Esto solo se aplica a los tipos de resultados de la Supervisión en tiempo de ejecución de EKS.
  - Versión del agente: la versión del agente GuardDuty de seguridad.
  - ID del agente: el identificador único del agente GuardDuty de seguridad.

Evidencia

Los resultados que se obtienen mediante la inteligencia sobre amenazas tienen una sección de Evidencia que incluye la siguiente información:

- Detalles de inteligencia sobre amenazas: nombre de la lista de amenazas en la que `Threat name` aparece lo reconocido.
- Nombre de la amenaza: el nombre de la familia de malware u otro identificador asociado a la amenaza.
- Archivo de amenaza SHA256: SHA256 del archivo que generó el hallazgo.

Comportamiento anómalo

Los tipos de hallazgos que terminan con «» AnomalousBehaviorindican que el hallazgo se generó mediante el modelo de aprendizaje automático (ML) para la detección de GuardDuty anomalías.

El modelo de ML evalúa todas las solicitudes de API a su cuenta e identifica los eventos anómalos relacionados con las tácticas utilizadas por los adversarios. El modelo de ML da seguimiento a varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó.

Los detalles sobre los factores de la solicitud de API que son inusuales para la identidad del CloudTrail usuario que invocó la solicitud se encuentran en los detalles de la búsqueda. Las identidades las define el elemento CloudTrail UserIdentity y los valores posibles son`Root`:,,`IAMUser`,, `AssumedRole` o. `FederatedUser` `AWSAccount` `AWSService`

Además de los detalles disponibles para todos los GuardDuty hallazgos relacionados con la actividad de la API, AnomalousBehaviorlos hallazgos tienen detalles adicionales que se describen en la siguiente sección. Estos detalles se pueden ver en la consola y también están disponibles en el JSON de los resultados.

- API anómalas: lista de solicitudes de API invocadas por la identidad del usuario cerca de la solicitud de API principal asociada al resultado. En este panel se desglosan en profundidad los detalles del evento de la API de las siguientes maneras.
  - La primera API de la lista es la API principal, que es la solicitud de API asociada a la actividad observada de mayor riesgo. Esta es la API que ha desencadenado el resultado y se correlaciona con la fase de ataque del tipo de resultado. Esta es también la API que se detalla en la sección Acción de la consola y en el JSON del resultado.
  - Todas las demás API de la lista son API anómalas adicionales a la identidad de usuario de la lista observadas cerca de la API principal. Si solo hay una API en la lista, el modelo de ML no ha identificado como anómala ninguna solicitud de API adicional procedente de esa identidad de usuario.
  - La lista de API se divide en función de si una API se llamó correctamente o si se llamó de forma incorrecta, lo que significa que se recibió una respuesta de error. El tipo de respuesta de error recibida aparece encima de cada API llamada incorrectamente. Los posibles tipos de respuesta de error son: `access denied`, `access denied exception`, `auth failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found` y `operation not permitted`.
  - Las API se clasifican según su servicio asociado.

> **Note**
>
> Para obtener más contexto, seleccione API históricas para ver los detalles sobre las API principales, hasta un máximo de 20, que normalmente se muestran tanto para la identidad del usuario como para todos los usuarios de la cuenta. Las API se marcan como Raro (menos de una vez al mes), Poco frecuente (varias veces al mes) o Frecuente (diario o semanal), en función de la frecuencia con la que se usen en la cuenta.

- Comportamiento inusual (cuenta): en esta sección, se proporcionan detalles adicionales sobre el comportamiento perfilado de su cuenta. La información rastreada en este panel incluye:
  - Organización de ASN: la organización de ASN desde la que se hizo la llamada anómala a la API.
  - Nombre de usuario: el nombre del usuario que hizo la llamada anómala a la API.
  - Agente de usuario: el agente de usuario utilizado para hacer la llamada anómala a la API. El agente de usuario es el método utilizado para hacer la llamada, por ejemplo, `aws-cli` o `Botocore`.
  - Tipo de usuario: el tipo de usuario que hizo la llamada anómala a la API. Los valores posibles son `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` o `ROLE`.
  - Bucket: el nombre del bucket de S3 al que se ha accedido.
- Comportamiento inusual (identidad de usuario): en esta sección se proporcionan detalles adicionales sobre el comportamiento perfilado de la identidad de usuario implicado en el resultado. Cuando un comportamiento no se identifica como histórico, significa que el modelo de aprendizaje GuardDuty automático no había visto anteriormente esta identidad de usuario realizando esta llamada a la API de esta manera durante el período de formación. Los siguientes detalles adicionales sobre la identidad de usuario están disponibles:
  - Organización de ASN: la organización de ASN desde la que se hizo la llamada anómala a la API.
  - Agente de usuario: el agente de usuario utilizado para hacer la llamada anómala a la API. El agente de usuario es el método utilizado para hacer la llamada, por ejemplo, `aws-cli` o `Botocore`.
  - Bucket: el nombre del bucket de S3 al que se ha accedido.
- Comportamiento inusual (bucket): en esta sección, se proporcionan detalles adicionales sobre el comportamiento perfilado del bucket de S3 asociado al resultado. Cuando un comportamiento no se identifica como histórico, significa que en el modelo de aprendizaje GuardDuty automático no

se habían realizado anteriormente llamadas a la API a este segmento de esta manera durante el período de formación. La información rastreada en esta sección incluye:

- Organización de ASN: la organización de ASN desde la que se hizo la llamada anómala a la API.
- Nombre de usuario: el nombre del usuario que hizo la llamada anómala a la API.
- Agente de usuario: el agente de usuario utilizado para hacer la llamada anómala a la API. El agente de usuario es el método utilizado para hacer la llamada, por ejemplo, `aws-cli` o `Botocore`.
- Tipo de usuario: el tipo de usuario que hizo la llamada anómala a la API. Los valores posibles son `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` o `ROLE`.

> **Note**
>
> Para más información sobre los comportamientos históricos, seleccione Comportamiento histórico en las secciones Comportamiento inusual (cuenta), ID de usuario o Bucket para ver detalles sobre el comportamiento esperado de su cuenta en cada una de las siguientes categorías: Raro (menos de una vez al mes), Poco frecuente (varias veces al mes) o Frecuente (diario o semanal), según la frecuencia con la que se usen en la cuenta.

- Comportamiento inusual (base de datos): en esta sección, se proporcionan detalles adicionales sobre el comportamiento perfilado de la instancia de base de datos asociada al resultado. Cuando un comportamiento no se identifica como histórico, significa que el modelo de aprendizaje GuardDuty automático no ha visto ningún intento de inicio de sesión en esta instancia de base de datos de esta manera durante el período de entrenamiento. La información recopilada en esta sección del panel de resultados incluye:
  - Nombre de usuario: el nombre de usuario utilizado para llevar a cabo el intento de inicio de sesión anómalo.
  - Organización de ASN: la organización de ASN desde la que se hizo el intento de inicio de sesión anómalo.
  - Nombre de la aplicación: el nombre de la aplicación utilizada para llevar a cabo el intento de inicio de sesión anómalo.
  - Nombre de base de datos: el nombre de la instancia de base de datos implicada en el intento de inicio de sesión anómalo.

> **Note**
>
> La sección Comportamiento histórico proporciona más contexto sobre los Nombres de usuario, Organizaciones de ASN, Nombres de las aplicaciones y Nombres de bases de datos observados anteriormente para la base de datos asociada. Cada valor único tiene un recuento asociado que representa el número de veces que se observó este valor en un evento de inicio de sesión exitoso.

- Comportamiento inusual (cuenta, clúster de Kubernetes, espacio de nombres de Kubernetes y nombre de usuario de Kubernetes): en esta sección se proporcionan detalles adicionales sobre el comportamiento perfilado del clúster y el espacio de nombres de Kubernetes asociado al hallazgo. Cuando un comportamiento no se identifica como histórico, significa que el modelo de aprendizaje automático no ha observado previamente esta cuenta, clúster, espacio de nombres o nombre de usuario de GuardDuty esta manera. La información recopilada en esta sección del panel de resultados incluye:
  - Nombre de usuario: el usuario que llamó a la API de Kubernetes asociada al hallazgo.
  - Nombre de usuario suplantado: el usuario al que se hace pasar por. `username`
  - Espacio de nombres: el espacio de nombres de Kubernetes dentro del clúster de Amazon EKS en el que se produjo la acción.
  - Agente de usuario: el agente de usuario asociado a la llamada a la API de Kubernetes. El agente de usuario es el método utilizado para realizar la llamada, por ejemplo. `kubectl`
  - API: la API de Kubernetes llamada desde `username` el clúster de Amazon EKS.
  - Información de ASN: la información de ASN, como la organización y el ISP, asociada a la dirección IP del usuario que realiza esta llamada.
  - Día de la semana: el día de la semana en que se realizó la llamada a la API de Kubernetes.
  - Permiso [1]: Se comprueba el acceso al verbo y al recurso de Kubernetes para indicar si pueden o no utilizar la API de Kubernetes. `username`
  - Nombre de la cuenta de servicio [1]: la cuenta de servicio asociada a la carga de trabajo de Kubernetes que proporciona una identidad a la carga de trabajo.
  - Registro [1]: el registro del contenedor asociado a la imagen del contenedor que se implementa en la carga de trabajo de Kubernetes.
  - Imagen [1]: la imagen del contenedor, sin las etiquetas ni el resumen asociados, que se despliega en la carga de trabajo de Kubernetes.

- Image Prefix Config [1]: el prefijo de la imagen con la configuración de seguridad del contenedor y la carga de trabajo habilitada, por ejemplo`privileged`, `hostNetwork` o, para el contenedor que usa la imagen.
- Nombre del sujeto [1]: los sujetos, como un `usergroup`, o `serviceAccountName` que están vinculados a un rol de referencia en un `RoleBinding` o. `ClusterRoleBinding`
- Nombre del rol [1]: el nombre del rol que interviene en la creación o modificación de los roles o de la `roleBinding` API.

Anomalías basadas en el volumen de S3

En esta sección, se detalla la información contextual de las anomalías basadas en el volumen de S3. El resultado basado en el volumen (Exfiltration:S3/AnomalousBehavior) supervisa un número inusual de llamadas a la API de S3 hechas por los usuarios a los buckets de S3, lo que indica una posible exfiltración de datos. Las siguientes llamadas a la API de S3 se supervisan para detectar anomalías basadas en el volumen.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

Las siguientes métricas ayudarían a crear una referencia del comportamiento habitual cuando una entidad de IAM accede a un bucket de S3. Para detectar la exfiltración de datos, el resultado de la detección de anomalías basada en el volumen evalúa todas las actividades con respecto a la referencia de comportamiento habitual. Seleccione Comportamiento histórico en las secciones Comportamiento inusual (identidad de usuario), Volumen observado (identidad de usuario) y Volumen observado (bucket) para ver las siguientes métricas, respectivamente.

- Número de llamadas a la API `s3-api-name` invocadas por el usuario de IAM o rol de IAM (depende de cuál se haya emitido) asociados al bucket de S3 afectado en las últimas 24 horas.
- Número de llamadas a la API `s3-api-name` invocadas por el usuario de IAM o rol de IAM (depende de cuál se haya emitido) asociados a todos los buckets de S3 afectados en las últimas 24 horas.
- Número de llamadas a la API `s3-api-name` en todos los usuarios de IAM o roles de IAM (depende de cuál se haya emitido) asociados al bucket de S3 afectado en las últimas 24 horas.

Anomalías basadas en la actividad de inicio de sesión en RDS

En esta sección, se detalla el recuento de los intentos de inicio de sesión de un actor inusual y se agrupa por el resultado de los intentos de inicio de sesión. Tipos de búsqueda de RDS Protection identifica el comportamiento anómalo mediante la supervisión de los eventos de inicio de sesión para detectar patrones inusuales de `successfulLoginCount`, `failedLoginCount` y `incompleteConnectionCount`.

- successfulLoginCount— Este contador representa la suma de las conexiones correctas (combinación correcta de los atributos de inicio de sesión) realizadas a la instancia de base de datos por un actor inusual. Los atributos de inicio de sesión incluyen el nombre de usuario, la contraseña y el nombre de la base de datos.
- failedLoginCount— Este contador representa la suma de los intentos de inicio de sesión fallidos (fallidos) realizados para establecer una conexión con la instancia de base de datos. Esto indica que uno o varios atributos de la combinación de inicio de sesión, como el nombre de usuario, la contraseña o el nombre de la base de datos, eran incorrectos.
- incompleteConnectionCount— Este contador representa el número de intentos de conexión que no se pueden clasificar como exitosos o fallidos. Estas conexiones se cierran antes de que la base de datos proporcione una respuesta. Por ejemplo, se analiza un puerto cuando el puerto de la base de datos está conectado, pero no se envía ningún dato a la base de datos o cuando la conexión se interrumpió antes de que se completara el inicio de sesión en un intento exitoso o fallido.

Formato de búsqueda GuardDuty

Cuando AWS detecta un comportamiento inesperado o sospechoso en el entorno de AWS, genera un resultado. Un resultado es una notificación que contiene detalles sobre un problema potencial de seguridad descubierto por . Los detalles de los resultados incluyen información sobre lo que ha sucedido, los recursos de AWS implicados en la actividad sospechosa, cuándo se ha producido, etc.

Uno de los datos más útiles de los detalles de los resultados es el tipo de resultado. El objetivo del tipo de resultado es proporcionar una descripción concisa pero comprensible del posible problema de seguridad. Por ejemplo, el tipo de resultado Recon:EC2/PortProbeUnprotectedPort de AWS le informa inmediatamente de que en algún lugar del entorno de AWS hay una instancia EC2 con un puerto sin protección que un posible atacante está sondeando.

utiliza el formato siguiente para los distintos tipos de resultados que genera:

Propósito de la amenaza: ResourceTypeAffect/ThreatFamilyName.Mecanismo de detección Artefacto

Cada parte de este formato representa un aspecto de un tipo de hallazgo. Estos aspectos tienen las siguientes explicaciones:

- ThreatPurpose: describe el objetivo principal de una amenaza o un posible ataque. Consulte la siguiente sección para obtener una lista completa de los propósitos de las amenazas de GuardDuty.
- ResourceTypeAffected: describe el recurso de AWS que se ha identificado en este resultado como el posible destino de un ataque. Actualmente, GuardDuty puede generar conclusiones para los recursos de EC2, S3, IAM y EKS.
- ThreatFamilyName: describe la amenaza general o la posible actividad malintencionada que está detectando. Por ejemplo, el valor NetworkPortUnusual indica que una instancia EC2 identificada en el resultado de no tiene historial previo de comunicaciones en un determinado puerto remoto que también se identifica en el resultado.
- DetectionMechanism: describe el método con el que GuardDuty detectó el hallazgo. Esto se puede usar para indicar una variación de un tipo de hallazgo común o un hallazgo que GuardDuty utilizó un mecanismo específico para detectar. Por ejemplo, Backdoor:EC2/denialOfService.tcp indica que la denegación de servicio (DoS) se detectó a través de TCP. La variante UDP es Backdoor:EC2/denialOfService.udp.

  Un valor de .Custom indica que GuardDuty detectó el hallazgo en función de sus listas de amenazas personalizadas, mientras que .Reputation indica que GuardDuty detectó el hallazgo mediante un modelo de puntuación de reputación de dominio.
- Artifact: describe un recurso específico que es propiedad de una herramienta que se usa en el ataque. Por ejemplo, DNS en el tipo de resultado CryptoCurrency:EC2/BitcoinTool.B!DNS informa de que una instancia EC2 se está comunicando con un dominio conocido relacionado con Bitcoin.

PROPÓSITO DE LA AMENAZA

En GuardDuty, el propósito de una amenaza describe el propósito principal de una amenaza, un tipo de ataque o una fase de un posible ataque. Por ejemplo, algunos propósitos de amenaza, como Backdoor, indican un tipo de ataque. Sin embargo, algunos propósitos de amenaza, como Impact, se alinean con las tácticas de MITRE ATT&CK. Las tácticas de MITRE ATT&CK indican distintas fases en el ciclo de ataque del adversario. En la versión actual de , ThreatPurpose puede tener los valores siguientes:

Backdoor

Backdoor: este valor indica que el ataque ha comprometido un recurso de AWS y de que es capaz de ponerse en contacto con su propio servidor de comando y control (C&C) con objeto de recibir más instrucciones para llevar a cabo actividades malintencionadas.

Comportamiento

Behavior: este valor indica que está detectando actividad o patrones de actividad distintos de la referencia establecida para un recurso de AWS determinado.

Acceso con credenciales

Este valor indica que GuardDuty ha detectado patrones de actividad que un adversario podría utilizar para robar credenciales, como identificadores de cuentas o contraseñas, de su entorno. El objetivo de esta amenaza se basa en las tácticas de MITRE ATT&CK

Cryptocurrency

Este valor indica que GuardDuty ha detectado que AWS un recurso de su entorno aloja software asociado a criptomonedas (por ejemplo, Bitcoin).

Defensa y evasión

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que un adversario puede utilizar para evitar ser detectado mientras se infiltra en su entorno. El objetivo de esta amenaza se basa en las tácticas de MITRE ATT&CK

Discovery

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que un adversario podría utilizar para ampliar su conocimiento de sus sistemas y redes internas. El objetivo de esta amenaza se basa en las tácticas de MITRE ATT&CK.

Ejecución

Este valor indica que GuardDuty ha detectado que un adversario podría intentar ejecutar código malicioso para explorar la red o robar datos. El objetivo de esta amenaza se basa en las tácticas de MITRE ATT&CK.

Exfiltración

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que un adversario podría utilizar al intentar robar datos de su red. El objetivo de esta amenaza se basa en las tácticas de MITRE ATT&CK.

Impact

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que sugieren que un adversario está intentando manipular, interrumpir o destruir sus sistemas y datos. El objetivo de esta amenaza se basa en las tácticas de MITRE ATT&CK

Acceso inicial

El propósito de esta amenaza se basa en las tácticas de MITRE ATT&CK

PenTest

PentestAWS: a veces, los propietarios de recursos de AWS o sus representantes autorizados ejecutan intencionadamente pruebas en las aplicaciones de AWS para descubrir vulnerabilidades, como grupos de seguridad abiertos o claves de acceso demasiado permisivas. Estas pruebas de intrusión son un intento de identificar y bloquear los recursos vulnerables antes de que los descubran los atacantes. Sin embargo, algunas de las herramientas que se utilizan para las pruebas de intrusión autorizadas están disponibles de forma gratuita y, por tanto, los usuarios no autorizados o los atacantes pueden usarlas para llevar a cabo pruebas de sondeo. Aunque no puede identificar el verdadero propósito de este tipo de actividad, el valor Pentest indica que está detectando dicha actividad y que esta es similar a la generada por las herramientas de pruebas de intrusión conocidas.

Persistencia

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que un adversario podría utilizar para intentar mantener el acceso a sus sistemas incluso si su ruta de acceso inicial está cortada. Por ejemplo, esto podría incluir la creación de un nuevo usuario de IAM después de obtener acceso a través de las credenciales comprometidas de un usuario existente. Cuando se eliminen las credenciales del usuario existente, el adversario conservará el acceso al nuevo usuario que no se haya detectado como parte del evento original. El objetivo de esta amenaza se basa en las tácticas de MITRE ATT&CK.

Auto Scaling

Policy: este valor indica que la cuenta de AWS está registrando un comportamiento que infringe las prácticas de seguridad recomendadas.

PrivilegeEscalation

Este valor le informa de que el responsable implicado de su AWS entorno presenta un comportamiento que un adversario podría utilizar para obtener permisos de nivel superior para acceder a su red. El objetivo de esta amenaza se basa en las tácticas de MITRE ATT&CK.

Recon

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que un adversario puede utilizar al realizar un reconocimiento de su red para determinar cómo puede ampliar su acceso o utilizar sus recursos. Por ejemplo, esta actividad puede incluir la detección de vulnerabilidades en su AWS entorno mediante el sondeo de los puertos, la lista de usuarios, las tablas de bases de datos, etc.

Stealth

Este valor indica que un adversario está intentando ocultar sus acciones de forma activa. Por ejemplo, podrían utilizar un servidor proxy anonimizador, lo que dificultaría enormemente evaluar la verdadera naturaleza de la actividad.

Trojan

Trojan: este valor indica que un ataque está utilizando programas troyanos que desarrollan en silencio actividad malintencionada. En ocasiones, este software tiene el aspecto de un programa legítimo. A veces, los usuarios ejecutan accidentalmente este software. Otras veces, este software puede ejecutarse automáticamente mediante la explotación de una vulnerabilidad.

UnauthorizedAccess

UnauthorizedAccess: este valor indica que está detectando actividades sospechosas o un patrón de actividades sospechosas por parte de un individuo no autorizado.

Generación de hallazgos de muestra en GuardDuty

Puedes generar ejemplos de hallazgos con Amazon GuardDuty para ayudarte a visualizar y comprender los distintos tipos de hallazgos que GuardDuty se pueden generar. Cuando generas muestras de resultados, GuardDuty rellena tu lista de hallazgos actual con una muestra de hallazgo por cada tipo de hallazgo compatible.

Las muestras generadas son aproximaciones rellenadas con valores de marcador de posición. Es posible que estas muestras tengan un aspecto diferente al de los resultados reales de su entorno, pero puede utilizarlas para probar diversas configuraciones GuardDuty, como sus CloudWatch eventos o filtros. Para obtener una lista de los valores disponibles para los tipos de resultados, consulte la tabla Tipos de resultados.

Para generar algunos resultados comunes en función de la actividad simulada dentro de su entorno, consulte Generación automática de GuardDuty hallazgos comunes a continuación.

Generar ejemplos de resultados a través de la GuardDuty consola o la API

Elija el método de acceso que prefiera para generar resultados de muestra.

> **Note**
>
> El método de consola genera uno para cada tipo de resultado. Los resultados de una sola muestra solo se pueden generar a través de la API.

Console

Use el procedimiento siguiente para generar resultados de muestra. Este proceso genera un hallazgo de muestra para cada tipo de GuardDuty hallazgo.

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, seleccione Configuración.
3. En la página Settings, en Sample findings, elija Generate sample findings.
4. En el panel de navegación, seleccione Findings (resultados). Los resultados de muestra se muestran en la página Resultados actuales con el prefijo [SAMPLE].

API/CLI

Puede generar una única búsqueda de muestra que coincida con cualquiera de los tipos de GuardDuty búsqueda a través de la CreateSampleFindingsAPI; los valores disponibles para los tipos de búsqueda se muestran en Tipos de resultados la tabla.

Esto resulta útil para probar las reglas de los CloudWatch eventos o para automatizarlas en función de los resultados. En el siguiente ejemplo, se muestra cómo generar un solo resultado de muestra del tipo `Backdoor:EC2/DenialOfService.Tcp` con la AWS CLI.

Para encontrar la correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --finding-types Backdoor:EC2/DenialOfService.Tcp
```

El título de los resultados de muestra generados mediante estos métodos siempre comienza con [SAMPLE] en la consola. Los resultados de muestra tienen un valor `"sample": true` en la sección additionalInfo de los detalles de los resultados de JSON.

Generación automática de GuardDuty hallazgos comunes

Puede utilizar los siguientes scripts para generar automáticamente varios GuardDuty hallazgos comunes. El guardduty-tester.template se utiliza AWS CloudFormation para crear un entorno aislado con un host bastión, una instancia Amazon EC2 de prueba a la que se puede acceder a través de SSH y dos instancias EC2 de destino. A continuación, puede ejecutar guardduty_tester.sh para iniciar una interacción entre la instancia EC2 de prueba, la instancia EC2 de Windows de destino y la instancia EC2 de Linux de destino, a fin de simular cinco tipos de ataques comunes que pueden detectarlos y notificarle con los resultados generados. GuardDuty

1. Como requisito previo, debe habilitar guardduty-tester.template y guardduty_tester.sh GuardDuty en la cuenta y la región en las que desee ejecutar. Para obtener más información sobre la activación, consulte. GuardDuty Empezar con GuardDuty

   También debe generar un nuevo par de claves de EC2 (o utilizar uno que ya esté disponible) en cada región en la que desea ejecutar estos scripts. Este par de claves EC2 se utiliza como parámetro en el script guardduty-tester.template que se utiliza para crear una pila nueva. CloudFormation Para obtener más información acerca de la generación de pares de claves, consulte Pares de claves de Amazon EC2.
2. Cree una pila nueva con guardduty-tester.template. CloudFormation Para obtener instrucciones detalladas sobre cómo crear una pila, consulte Creación de una pila. Antes de ejecutar guardduty-tester.template, modifíquelo con valores en los siguientes parámetros: Stack Name (nombre para identificar la nueva pila), Availability Zone (zona de disponibilidad donde desea ejecutar la pila) y Key Pair (par de claves que puede utilizar para lanzar las instancias EC2). A continuación, puede utilizar la clave privada correspondiente para acceder a las instancias de EC2 a través de SSH.

   La guardduty-tester.template tarda alrededor de 10 minutos en ejecutarse y finalizar. Crea el entorno y copia guardduty_tester.sh en la instancia EC2 de prueba.
3. En la AWS CloudFormation consola, selecciona la casilla de verificación situada junto a tu nueva pila en ejecución. AWS CloudFormation En el conjunto de pestañas que se muestra, seleccione la pestaña Output (Salida). Tome nota de las direcciones IP asignadas al host bastión y a la instancia EC2 de prueba. Necesita ambas direcciones IP para acceder a la instancia de EC2 de comprobación a través de SSH.

4. Cree la siguiente entrada en el archivo ~/.ssh/config para iniciar sesión en la instancia a través del host bastión.

```
Host bastion
        HostName {Elastic IP Address of Bastion}
        User ec2-user
        IdentityFile ~/.ssh/{your-ssh-key.pem}
Host tester
        ForwardAgent yes
        HostName {Local IP Address of RedTeam Instance}
        User ec2-user
        IdentityFile ~/.ssh/{your-ssh-key.pem}
        ProxyCommand ssh bastion nc %h %p
        ServerAliveInterval 240
```

   Ahora puede hacer una llamada a $ ssh tester para iniciar sesión en la instancia de EC2 de destino. Para obtener más información sobre la configuración y la conexión a las instancias de EC2 a través de hosts bastiones, consulte https://aws.amazon.com/blogs/security/ securely-connect-to-linux - -instances-running-in-a/. private-amazon-vpc

5. Tras conectarse a la instancia EC2 de prueba, ejecute guardduty_tester.sh para iniciar la interacción entre la instancia de EC2 de destino y la de prueba, simular ataques y generar resultados. GuardDuty

Niveles de gravedad de GuardDuty los hallazgos

Cada GuardDuty hallazgo tiene un nivel de gravedad y un valor asignados que reflejan el riesgo potencial que el hallazgo podría suponer para su red, según determinaron nuestros ingenieros de seguridad. El valor de la gravedad puede estar comprendido en cualquier lugar dentro del intervalo de 1,0 a 8,9, donde los valores superiores indican un mayor riesgo de seguridad. Para ayudarle a determinar la respuesta a un posible problema de seguridad que se ponga de manifiesto en un hallazgo, GuardDuty desglosa este rango en niveles de gravedad alta, media y baja.

> **Note**
>
> Los valores 0 y entre 9,0 y 10,0 están reservados actualmente para uso futuro.

A continuación se indican los valores y niveles de gravedad definidos actualmente para los GuardDuty hallazgos, así como las recomendaciones generales para cada uno de ellos:

Nivel de gravedad	Rango de valor
Alta	7,0 - 8,9
Un nivel de seguridad alto indica que el recurso en cuestión (una instancia de EC2 o un conjunto de credenciales de inicio de sesión de usuarios de IAM) está en peligro y que se está utilizando activamente para fines no autorizados. Le recomendamos que trate cualquier problema de seguridad con un resultado de gravedad alta como una prioridad y que tome medidas de corrección inmediatas para evitar el uso no autorizad o de sus recursos. Por ejemplo, limpie la instancia de EC2 o termínela, o rote las credenciales de IAM. Consulte Medidas de corrección para obtener más detalles.	
Medio	4,0 - 6,9
Un nivel de gravedad mediano indica una actividad sospechosa que se desvía del comportam iento observado normalmente y, en función de su caso de uso, puede ser indicativo de un peligro para los recursos. Recomendamos que investigue el recurso implicado tan pronto como sea posible. Las medidas de corrección variarán según el recurso y la familia de resultados, pero, en general, debería tratar de confirmar que la actividad está autorizada y es coherente con su caso de uso. Si no puede identificar la causa o confirmar que la actividad está autorizada, debería considerar el recurso como afectado y seguir los Pasos de corrección para proteger el recurso. Estas son algunas cosas a tener en cuenta al revisar un resultado de nivel mediano: • Compruebe si un usuario autorizado ha instalado nuevo software que haya cambiado el comportamiento de un recurso (por ejemplo, permitir un tráfico superior al normal o habilitar la comunicación en un nuevo puerto). • Compruebe si un usuario autorizado ha modificado la configuración del panel de control, por ejemplo, ha modificado la configuración de un grupo de seguridad • Ejecute un examen antivirus en el recurso implicado para detectar software no autorizado. • Verifique los permisos asociados al rol de IAM, usuario, grupo o conjunto de credenciales implicados. Tal vez sea necesario cambiarlos o moverlos.	

Nivel de gravedad	Rango de valor
Baja	1,0 - 3,9

Un nivel de gravedad bajo indica un intento de actividad sospechosa que no puso en peligro la red, por ejemplo, un análisis de puerto o un intento de intrusión que ha producido error.

No hay ninguna acción recomendada inmediata, pero vale la pena tomar nota de esta información ya que puede indicar que alguien está buscando puntos débiles en su red.

GuardDuty encontrar agregación

Todos los hallazgos son dinámicos, lo que significa que, si GuardDuty detecta una nueva actividad relacionada con el mismo problema de seguridad, actualizará el hallazgo original con la nueva información, en lugar de generar un nuevo hallazgo. Este comportamiento le permite identificar problemas en curso sin necesidad de revisar varios informes similares y reduce el ruido general de los problemas de seguridad que ya conoce.

Por ejemplo, para un resultado `UnauthorizedAccess:EC2/SSHBruteForce`, se agregarán varios intentos de acceso contra la instancia al mismo ID de resultado, lo que aumentará el número de recuento en los detalles del resultado. Esto se debe a que ese resultado representa un único problema de seguridad con la instancia que indica que el puerto SSH de la instancia no está protegido adecuadamente contra este tipo de actividad. Sin embargo, si GuardDuty detecta una actividad de acceso a SSH dirigida a una nueva instancia de su entorno, creará un nuevo hallazgo con un identificador de búsqueda único para avisarle de que hay un problema de seguridad asociado al nuevo recurso.

Cuando se agrega un resultado, se actualiza con la información del último caso de esa actividad. Esto significa que, en el ejemplo anterior, si su instancia es el objetivo de un intento de fuerza bruta de un nuevo actor, los detalles del resultado se actualizarán para reflejar la IP remota del origen más reciente y se sustituirá la información más antigua. La información completa sobre los intentos de actividad individuales seguirá estando disponible en tus registros de flujo CloudTrail o en los de VPC.

Los criterios que permiten GuardDuty generar un nuevo hallazgo en lugar de agregar uno existente dependen del tipo de hallazgo. Nuestros ingenieros de seguridad determinan los criterios de agregación para cada tipo de resultado para ofrecerle la mejor información general de los distintos problemas de seguridad dentro de su cuenta.

Localizar y analizar los hallazgos GuardDuty

Utilice el siguiente procedimiento para ver y analizar sus GuardDuty hallazgos.

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. Elija Hallazgos y, a continuación, seleccione un resultado específico para consultar sus detalles.

   Los detalles de cada resultado variarán en función del tipo de resultado, los recursos implicados y la naturaleza de la actividad. Para obtener más información sobre los campos de resultado disponibles, consulte Detalles de los resultados.
3. (Opcional) Si desea archivar un resultado, selecciónelo de la lista de resultados y, a continuación, elija el menú Acciones. A continuación, elija Archivar.

   Para consultar los resultados archivados, puede elegir Archivado en el menú desplegable Actual.

   Actualmente, los GuardDuty usuarios de las cuentas de los GuardDuty miembros no pueden archivar las conclusiones.

   > **Important**
   >
   > Si archiva un resultado manualmente utilizando el procedimiento anterior, todos los casos posteriores de este resultado (generados una vez completado el archivado) se añaden a la lista de sus resultados actuales. Para no ver nunca este resultado en su lista actual, puede utilizar el archivado automático. Para obtener más información, consulte Reglas de supresión.
4. (Opcional) Para descargar un resultado, selecciónelo de la lista de resultados y, a continuación, elija el menú Acciones. A continuación, elija Exportar. Cuando se exporta un resultado con Export (Exportar), puede ver su documento JSON completo.

   > **Note**
   >
   > En algunos casos, GuardDuty se da cuenta de que ciertos resultados son falsos positivos una vez generados. GuardDuty proporciona un campo de confianza en el JSON del hallazgo y establece su valor en cero. De esta GuardDuty forma, sabrá que puede ignorar estos hallazgos de forma segura.

Tipos de resultados

Para obtener información sobre los cambios importantes en los tipos de GuardDuty búsqueda, incluidos los tipos de búsqueda recién agregados o retirados, consulteHistorial de documentos de Amazon GuardDuty.

Para obtener información sobre tipos de resultados que ya se han retirado, consulte Tipos de resultados retirados.

GuardDuty Tipos de búsqueda de EC2

Los siguientes resultados son específicos de los recursos de Amazon EC2 y siempre tendrán un tipo de recurso de `Instance`. La gravedad y los detalles de los resultados variarán en función del rol de recurso que indicará si la instancia de EC2 fue objeto de actividad sospechosa o el agente que llevó a cabo la actividad.

Los resultados que se muestran aquí incluyen los orígenes de datos y los modelos utilizados para generar ese tipo de resultado. Para más información sobre los orígenes de datos y modelos, consulte Orígenes de datos fundamentales.

> **Note**
>
> Es posible que falten detalles de la instancia de algunos resultados de EC2 si la instancia ya se ha terminado o si la llamada a la API subyacente fue parte de una llamada a la API entre regiones que se ha originado en una instancia de EC2 en una región diferente.

Para todos los resultados de EC2, se recomienda examinar el recurso en cuestión para determinar si se comporta de la manera esperada. Si la actividad está autorizada, puede utilizar reglas de supresión o listas de IP confiables para evitar las notificaciones de falsos positivos para ese recurso. Si la actividad es inesperada, la práctica recomendada de seguridad consiste en asumir que la instancia se ha visto afectada y llevar a cabo las acciones detalladas en Corregir una instancia de Amazon EC2 potencialmente comprometida.

Temas

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS

- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- Behavior:EC2/NetworkPortUnusual
- Behavior:EC2/TrafficVolumeUnusual
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- DefenseEvasion:EC2/UnusualDNSResolver
- DefenseEvasion:EC2/UnusualDoHActivity
- DefenseEvasion:EC2/UnusualDoTActivity
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce
- Recon:EC2/PortProbeEMRUnprotectedPort
- Recon:EC2/PortProbeUnprotectedPort
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS

- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/MetadataDNSRebind
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:EC2/SSHBruteForce
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay

Backdoor:EC2/C&CActivity.B

Una instancia de EC2 está consultando una IP que está asociada a un servidor de comando y control conocido.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que hay una instancia que aparece en la lista dentro del entorno de AWS que está consultando a una IP asociada con un servidor de comando y control (C&C) conocido. La instancia de la lista podría haberse visto afectada. Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet.

Un botnet es una colección de dispositivos conectados a Internet (que pueden incluir PC, servidores, dispositivos móviles y dispositivos de Internet de las cosas) que están infectados y controlados por un tipo común de malware. A menudo, los botnets se utilizan para distribuir malware y recopilar información obtenida de forma indebida, como números de tarjetas de crédito. Dependiendo de la finalidad y la estructura del botnet, el servidor C&C también puede enviar comandos para comenzar un ataque de denegación de servicio distribuido (DDoS).

> **Note**
>
> Si la IP consultada está relacionada con log4j, los campos del resultado asociado incluirán los siguientes valores:
>
> - Servicio. Información adicional. threatListName = Amazon

- service.additionalInfo.threatName = Log4j Related

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Backdoor:EC2/C&CActivity.B!DNS

La instancia de EC2 está consultando un nombre de dominio que está asociado a un servidor de comando y control conocido.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia que se muestra en la lista dentro del entorno de AWS que está consultando a un nombre de dominio asociado con un servidor de comando y control (C&C) conocido. La instancia de la lista podría haberse visto afectada. Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet.

Un botnet es una colección de dispositivos conectados a Internet (que pueden incluir PC, servidores, dispositivos móviles y dispositivos de Internet de las cosas) que están infectados y controlados por un tipo común de malware. A menudo, los botnets se utilizan para distribuir malware y recopilar información obtenida de forma indebida, como números de tarjetas de crédito. Dependiendo de la finalidad y la estructura del botnet, el servidor C&C también puede enviar comandos para comenzar un ataque de denegación de servicio distribuido (DDoS).

> **Note**
>
> Si el nombre de dominio consultado está relacionado con log4j, los campos del resultado asociado incluirán los siguientes valores:
>
> - Servicio.Información adicional. threatListName = Amazon
> - service.additionalInfo.threatName = Log4j Related

> **Note**
>
> Para comprobar cómo se GuardDuty genera este tipo de búsqueda, puedes realizar una solicitud de DNS desde tu instancia (`dig`para Linux o `nslookup` Windows) y compararla con un dominio de prueba`guarddutyc2activityb.com`.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Backdoor:EC2/DenialOfService.Dns

Una instancia EC2 tiene un comportamiento que puede indicar que se está utilizando para llevar a cabo un ataque de denegación de servicio (DoS) mediante el protocolo DNS.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS está generando un gran volumen de tráfico DNS saliente. Esto puede indicar que la instancia de la lista está comprometida y se está utilizando para realizar ataques denial-of-service (DoS) mediante el protocolo DNS.

> **Note**
>
> Este resultado solo detecta los ataques DoS contra direcciones IP direccionables públicamente, que son los objetivos principales de este tipo de ataques.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Backdoor:EC2/DenialOfService.Tcp

Una instancia EC2 se comporta de una manera que indica que se está utilizando para realizar un ataque de denegación de servicio (DoS) mediante el protocolo TCP.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS está generando un gran volumen de tráfico TCP saliente. Esto puede indicar que la instancia está comprometida y que se está utilizando para realizar ataques denial-of-service (DoS) mediante el protocolo TCP.

> **Note**
>
> Este resultado solo detecta los ataques DoS contra direcciones IP direccionables públicamente, que son los objetivos principales de este tipo de ataques.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Backdoor:EC2/DenialOfService.Udp

Una instancia EC2 se comporta de una manera que indica que se está utilizando para realizar un ataque de denegación de servicio (DoS) mediante el protocolo UDP.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS está generando un gran volumen de tráfico UDP saliente. Esto puede indicar que la instancia

de la lista está comprometida y se está utilizando para realizar ataques denial-of-service (DoS) mediante el protocolo UDP.

> **Note**
>
> Este resultado solo detecta los ataques DoS contra direcciones IP direccionables públicamente, que son los objetivos principales de este tipo de ataques.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Una instancia EC2 tiene un comportamiento que puede indicar que se está utilizando para llevar a cabo un ataque de denegación de servicio (DoS) mediante el protocolo UDP en un puerto TCP.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS está generando un gran volumen de tráfico UDP saliente cuyo objetivo es un puerto que usualmente se utiliza para la comunicación mediante TCP. Esto puede indicar que la instancia de la lista está comprometida y se está utilizando para realizar un ataque denial-of-service (DoS) mediante el protocolo UDP en un puerto TCP.

> **Note**
>
> Este resultado solo detecta los ataques DoS contra direcciones IP direccionables públicamente, que son los objetivos principales de este tipo de ataques.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Backdoor:EC2/DenialOfService.UnusualProtocol

Una instancia EC2 tiene un comportamiento que puede indicar que se está utilizando para llevar a cabo un ataque de denegación de servicio (DoS) utilizando un protocolo inusual.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS está generando un gran volumen de tráfico saliente mediante un tipo de protocolo inusual que no suelen utilizar las instancias de EC2 (por ejemplo, el protocolo de administración de grupos de Internet). Esto puede indicar que la instancia está comprometida y se está utilizando para realizar ataques denial-of-service (DoS) mediante un protocolo inusual. Este resultado solo detecta los ataques DoS contra direcciones IP direccionables públicamente, que son los objetivos principales de este tipo de ataques.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Backdoor:EC2/Spambot

Una instancia de EC2 exhibe un comportamiento inusual al comunicarse con un host remoto en el puerto 25.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS se está comunicando con un host remoto en el puerto 25. Este comportamiento es inusual, ya

que esta instancia EC2 no tiene un historial previo de comunicaciones en el puerto 25. El puerto 25 lo utilizan tradicionalmente los servidores de correo para las comunicaciones SMTP. Este resultado indica que la instancia EC2 es posible que se vea comprometida para su uso en el envío de spam.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Behavior:EC2/NetworkPortUnusual

Una instancia EC2 se comunica con un host remoto en un puerto de servidor inusual.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS se está comportando de una manera que se desvía de la referencia establecida. Esta instancia EC2 no tiene historial previo de comunicaciones en este puerto remoto.

> **Note**
>
> Si la instancia de EC2 se ha comunicado en los puertos 389 o 1389, la gravedad del resultado asociado se modificará a Alta y los campos del resultado incluirán el siguiente valor:
>
> - service.additionalInfo.context = Possible log4j callback

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Behavior:EC2/TrafficVolumeUnusual

Una instancia EC2 genera una cantidad inusualmente elevada de tráfico de red a un host remoto.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS se está comportando de una manera que se desvía de la referencia establecida. Esta instancia EC2 no tiene historial previo de envío de esta cantidad de tráfico a este host remoto.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

CryptoCurrency:EC2/BitcoinTool.B

Una instancia EC2 consulta una dirección IP asociada con una actividad relacionada con una criptomoneda.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está consultando una dirección IP que está asociada con actividades relacionadas con Bitcoin u otras criptomonedas. Bitcoin es una criptomoneda mundial y un sistema de pago digital que se puede cambiar por otras monedas, productos y servicios. Bitcoin es una recompensa por la extracción de bitcoins y es muy solicitado por los actores de amenazas.

Recomendaciones de corrección:

Si utiliza esta instancia de EC2 para extraer o administrar criptomonedas, o esta instancia está involucrada de otra manera en la actividad de cadena de bloques, este resultado podría ser la actividad esperada para su entorno. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `CryptoCurrency:EC2/BitcoinTool.B`. El segundo criterio de filtro debe ser el ID de instancia de la instancia involucrada en la actividad de blockchain. Para obtener más información sobre la creación de reglas de supresión, consulte Reglas de supresión.

Si esta actividad es inesperada, puede que su instancia esté comprometida; consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

CryptoCurrency:EC2/BitcoinTool.B!DNS

Una instancia EC2 consulta un nombre de dominio asociado con la actividad relacionada con la criptomoneda.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está consultando un nombre de dominio que está asociado con actividades relacionadas con Bitcoin u otras criptomonedas. Bitcoin es una criptomoneda mundial y un sistema de pago digital que se puede cambiar por otras monedas, productos y servicios. Bitcoin es una recompensa por la extracción de bitcoins y es muy solicitado por los actores de amenazas.

Recomendaciones de corrección:

Si utiliza esta instancia de EC2 para extraer o administrar criptomonedas, o esta instancia está involucrada de otra manera en la actividad de cadena de bloques, este resultado podría ser la actividad esperada para su entorno. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `CryptoCurrency:EC2/BitcoinTool.B!DNS`. El segundo criterio de filtro debe ser el ID de instancia de la instancia involucrada en la actividad de blockchain. Para obtener más información sobre la creación de reglas de supresión, consulte Reglas de supresión.

Si esta actividad es inesperada, puede que su instancia esté comprometida; consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

DefenseEvasion:EC2/UnusualDNSResolver

Una instancia de Amazon EC2 se está comunicando con un solucionador de DNS público inusual.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista del entorno de AWS se está comportando de una manera que se desvía de la referencia establecida. Esta instancia de EC2 no tiene un historial reciente de comunicación con este solucionador de DNS público. El campo Insólito del panel de detalles de búsqueda de la GuardDuty consola puede proporcionar información sobre la resolución de DNS consultada.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

DefenseEvasion:EC2/UnusualDoHActivity

Una instancia de Amazon EC2 se comunica de manera inusual con un DNS a través de HTTPS (DoH).

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS se está comportando de una manera que se desvía de la referencia establecida. Esta instancia de EC2 no tiene ningún historial reciente de comunicaciones de DNS a través de HTTPS (DoH) con este servidor DoH público. El campo Inusual de los detalles de resultado puede proporcionar información sobre el servidor de DoH consultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

DefenseEvasion:EC2/UnusualDoTActivity

Una instancia de Amazon EC2 se está comunicando de manera inusual con un DNS a través de TLS (DoT).

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS se está comportando de una manera que se desvía de la referencia establecida. Esta instancia de EC2 no tiene ningún historial reciente de comunicaciones de DNS a través de TLS (DoT) con este servidor DoT público. El campo Inusual del panel de detalles de resultado puede proporcionar información sobre el servidor DoT consultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Impact:EC2/AbusedDomainRequest.Reputation

Una instancia de EC2 consulta un nombre de dominio de baja reputación que está asociado a dominios que se sabe que se han utilizado indebidamente.

Gravedad predeterminada: media

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación asociado a dominios o direcciones IP de los que se sabe que se han utilizado indebidamente. Algunos ejemplos de dominios utilizados indebidamente son los nombres de dominio de nivel superior (TLD) y los nombres de dominio de segundo nivel (2LD), que proporcionan registros de subdominios gratuitos, así como proveedores de DNS dinámicos. Los actores de amenazas suelen utilizar estos servicios para registrar dominios de forma gratuita o a un bajo costo. Los dominios de baja reputación de esta categoría también pueden ser dominios caducados que se resuelven en la dirección IP de estacionamiento de un registrador y, por lo tanto, es posible que ya no estén activos. Una IP de estacionamiento es el lugar al que un registrador dirige el tráfico de dominios que no se han vinculado a ningún servicio. La instancia de Amazon EC2 que aparece en la lista puede haberse visto afectada, ya que los actores de amenazas suelen utilizar estos registradores o servicios para la distribución de C&C y malware.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Impact:EC2/BitcoinDomainRequest.Reputation

Una instancia de EC2 consulta un nombre de dominio de baja reputación que está asociado a la actividad relacionada con criptomonedas.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio que está asociado con actividades relacionadas con Bitcoin u otras criptomonedas. Bitcoin es una criptomoneda mundial y un sistema de pago digital que se puede cambiar por otras monedas, productos y servicios. Bitcoin es una recompensa por la extracción de bitcoins y es muy solicitado por los actores de amenazas.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

Recomendaciones de corrección:

Si utiliza esta instancia de EC2 para extraer o administrar criptomonedas, o esta instancia está involucrada de otra manera en la actividad de cadena de bloques, este resultado podría representar la actividad esperada para su entorno. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `Impact:EC2/BitcoinDomainRequest.Reputation`. El segundo criterio de filtro debe ser el ID de instancia de la instancia involucrada en la actividad de blockchain. Para obtener más información sobre la creación de reglas de supresión, consulte Reglas de supresión.

Si esta actividad es inesperada, puede que su instancia esté comprometida; consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Impact:EC2/MaliciousDomainRequest.Reputation

Una instancia de EC2 consulta un dominio de baja reputación que está asociado a dominios maliciosos conocidos.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación asociado a dominios o direcciones IP de los que se sabe que son maliciosos. Por ejemplo, los dominios pueden estar asociados a una dirección IP conocida como oculta. Los dominios ocultos son aquellos que anteriormente estaban controlados por un agente de amenazas y las solicitudes que se les hagan pueden indicar que la instancia se ha visto afectada. Estos dominios también pueden estar correlacionados con campañas o algoritmos de generación de dominios maliciosos conocidos.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Impact:EC2/PortSweep

Una instancia de EC2 está sondeando un puerto en un gran número de direcciones IP.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está sondeando un puerto en un gran número de direcciones IP direccionables públicamente. Este tipo de actividad se suele utilizar para encontrar hosts vulnerables y explotarlos. En el panel de detalles de búsqueda de la GuardDuty consola, solo se muestra la dirección IP remota más reciente

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Impact:EC2/SuspiciousDomainRequest.Reputation

Una instancia de EC2 consulta un nombre de dominio de baja reputación que resulta sospechoso por naturaleza debido a su antigüedad o a su baja popularidad.

Gravedad predeterminada: baja

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación que se sospecha que es malicioso. Se observaron características de este dominio que eran consistentes con las de dominios maliciosos observados anteriormente; sin embargo, nuestro modelo de reputación no pudo relacionarlo definitivamente con una amenaza conocida. Por lo general, estos dominios se han detectado recientemente o reciben poco tráfico.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Impact:EC2/WinRMBruteForce

Una instancia de EC2 está realizando un ataque de fuerza bruta saliente con Windows Remote Management.

Gravedad predeterminada: baja*

> **Note**
>
> La gravedad de este resultado es baja si su instancia de EC2 era el objetivo de un ataque de fuerza bruta. La gravedad de este resultado es alta si su instancia de EC2 es el actor que se utiliza para llevar a cabo el ataque de fuerza bruta.

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que hay una instancia de EC2 en el entorno de AWS que está llevando a cabo un ataque de Windows Remote Management (WinRM) con fuerza bruta con el objetivo de obtener acceso al servicio de Windows Remote Management en sistemas basados en Windows.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Recon:EC2/PortProbeEMRUnprotectedPort

Una instancia de EC2 tiene un puerto relacionado con EMR desprotegido sondeado por un host malicioso conocido.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este hallazgo le informa de que un puerto confidencial relacionado con el EMR de la instancia EC2 de la lista que forma parte de un clúster de su AWS entorno no está bloqueado por un grupo de seguridad, una lista de control de acceso (ACL) o un firewall del host, como IPTables de Linux. Este hallazgo también indica que los escáneres conocidos de Internet están inspeccionando activamente este puerto. Los puertos que pueden desencadenar este resultado, como el puerto 8088 (puerto de IU web de YARN), se pueden utilizar potencialmente para la ejecución de código remoto.

Recomendaciones de corrección:

Debería bloquear el acceso libre a los puertos en los clústeres desde Internet y restringir el acceso solo a direcciones IP específicas que requieren acceso a estos puertos. Para obtener más información, consulte Grupos de seguridad para clústeres de EMR.

Recon:EC2/PortProbeUnprotectedPort

Una instancia EC2 tiene un puerto sin protección que un host malintencionado conocido está sondeando.

Gravedad predeterminada: baja*

> **Note**
>
> La gravedad predeterminada de este resultado es Baja. Sin embargo, si Elasticsearch (9200 o 9300) utiliza el puerto que se está sondeando, la gravedad del hallazgo es alta.

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que un puerto en la instancia de EC2 que aparece en la lista del entorno de AWS no está bloqueado por un grupo de seguridad, una lista de control de acceso (ACL) o un firewall del host (por ejemplo, IPTables) y está siendo sondeado activamente por análisis conocidos en Internet.

Si el puerto desprotegido identificado es 22 o 3389 y utiliza estos puertos para conectarse a su instancia, aún puede limitar la exposición permitiendo el acceso a estos puertos solo a las direcciones IP desde el espacio de direcciones IP de su red corporativa. Para restringir el acceso al puerto 22 en Linux, consulte Autorización del tráfico de entrada para sus instancias de Linux. Para restringir el acceso al puerto 3389 en Windows, consulte Autorización del tráfico de entrada para sus instancias de Windows.

GuardDuty no genera este resultado para los puertos 443 y 80.

Recomendaciones de corrección:

Puede haber casos en los que las instancias se exponen de forma intencionada, por ejemplo, si están alojando servidores web. Si este es el caso en su entorno de AWS, le recomendamos que

configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `Recon:EC2/PortProbeUnprotectedPort`. El segundo criterio de filtro debe coincidir con la instancia o instancias que sirven como host de bastión. Puede utilizar el atributo ID de imagen de instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. Para más información sobre la creación de reglas de supresión, consulte Reglas de supresión.

Si esta actividad es inesperada, puede que su instancia esté comprometida; consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Recon:EC2/Portscan

Una instancia EC2 realiza exploraciones de puertos salientes a un host remoto.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está involucrada en un posible ataque de análisis de puertos porque está intentando conectarse a varios puertos en un período corto de tiempo. El objetivo de un ataque de análisis de puertos es localizar puertos abiertos para detectar los servicios que está ejecutando el equipo e identificar su sistema operativo.

Recomendaciones de corrección:

Este resultado puede ser un falso positivo cuando se implementan aplicaciones de evaluación de vulnerabilidades en instancias de EC2 en su entorno, ya que estas aplicaciones analizan los puertos para alertarle sobre puertos abiertos mal configurados. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `Recon:EC2/Portscan`. El segundo criterio de filtro debe coincidir con la instancia o instancias que alojan estas herramientas de evaluación de vulnerabilidades. Puede utilizar el atributo ID de imagen de instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. Para más información sobre la creación de reglas de supresión, consulte Reglas de supresión.

Si esta actividad es inesperada, puede que su instancia esté comprometida; consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Trojan:EC2/BlackholeTraffic

Una instancia EC2 intenta comunicarse con una dirección IP de un host remoto que es un agujero negro conocido.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS podría haberse visto afectada, ya que está intentando comunicarse con una dirección IP de agujero negro (u oculta). Los agujeros negros hacen referencia a lugares de la red donde el tráfico entrante o saliente se descarta silenciosamente sin informar al origen de que los datos no llegaron a su destinatario esperado. Una dirección IP de agujero negro especifica una máquina host que no se está ejecutando o una dirección a la que no se le ha asignado ningún host.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Trojan:EC2/BlackholeTraffic!DNS

Una instancia EC2 consulta un nombre de dominio que se está redireccionando a una dirección IP de agujero negro.

Gravedad predeterminada: media

- Origen de datos: registros de DNS

Este resultado le informa de que una instancia de EC2 que aparece en la lista del entorno de AWS podría haberse visto afectada, ya que está consultando un nombre de dominio que se está redireccionando a una dirección IP de agujero negro. Los agujeros negros hacen referencia a lugares de la red donde el tráfico entrante o saliente se descarta silenciosamente sin informar al origen de que los datos no llegaron a su destinatario esperado.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Trojan:EC2/DGADomainRequest.B

Una instancia EC2 consulta dominios generados mediante algoritmo. El malware suele utilizar dichos dominios y podría indicar una instancia EC2 comprometida.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está intentando hacer consultas en dominios de algoritmos de generación de dominios (DGA). La instancia EC2 podría estar comprometida.

Los dominios DGA se utilizan para generar de forma periódica una gran cantidad de nombres de dominio que se pueden usar como puntos de encuentro con sus servidores de comando y control (C & C). Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet, que es una colección de dispositivos conectados a Internet que están infectados y son controlados por un tipo común de malware. El gran número de posibles puntos de encuentro dificulta un apagado eficaz de los botnets, ya que los equipos infectados intentan ponerse en contacto con algunos de estos nombres de dominio cada día para recibir actualizaciones o comandos.

> **Note**
>
> Este resultado se basa en el análisis de nombres de dominio mediante heurística avanzada, por lo que podría identificar nuevos dominios de DGA que no están presentes en fuentes de información de amenazas.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Trojan:EC2/DGADomainRequest.C!DNS

Una instancia EC2 consulta dominios generados mediante algoritmo. El malware suele utilizar dichos dominios y podría indicar una instancia EC2 comprometida.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está intentando hacer consultas en dominios de algoritmos de generación de dominios (DGA). La instancia EC2 podría estar comprometida.

Los dominios DGA se utilizan para generar de forma periódica una gran cantidad de nombres de dominio que se pueden usar como puntos de encuentro con sus servidores de comando y control (C & C). Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet, que es una colección de dispositivos conectados a Internet que están infectados y son controlados por un tipo común de malware. El gran número de posibles puntos de encuentro dificulta un apagado eficaz de los botnets, ya que los equipos infectados intentan ponerse en contacto con algunos de estos nombres de dominio cada día para recibir actualizaciones o comandos.

> **Note**
>
> Este hallazgo se basa en los dominios de DGA conocidos de las fuentes de inteligencia sobre amenazas GuardDuty de las que dispone.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Trojan:EC2/DNSDataExfiltration

Una instancia EC2 sustrae datos a través de consultas de DNS.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está ejecutando malware que utiliza consultas de DNS para transferencias de datos salientes. Este tipo de transferencia de datos indica que se trata de una instancia afectada y podría provocar la exfiltración de datos. Por lo general, el tráfico de DNS no está bloqueado por los firewalls. Por ejemplo, el malware de una instancia EC2 comprometida puede codificar datos (como el número de su tarjeta de crédito) en una consulta de DNS y enviarlos a un servidor DNS remoto controlado por un atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Trojan:EC2/DriveBySourceTraffic!DNS

Una instancia EC2 consulta un nombre de dominio de un host remoto que es una fuente conocida de ataques de descarga Drive-By.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS podría haberse visto afectada, ya que está consultando un nombre de dominio de un host remoto que es un origen conocido de ataques de descargas Drive-By. Se trata de descargas no deseadas de software informático desde Internet que pueden desencadenar la instalación automática de un virus, spyware o malware.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Trojan:EC2/DropPoint

Una instancia EC2 está intentando comunicarse con una dirección IP de un host remoto que se sabe que mantiene credenciales y otros datos robados capturados por malware.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que una instancia de EC2 de su entorno de AWS está intentando comunicarse con una dirección IP de un host remoto que se sabe que conserva credenciales y otros datos robados capturados por malware.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Trojan:EC2/DropPoint!DNS

Una instancia EC2 está consultando un nombre de dominio de un host remoto que se conoce que mantiene credenciales y otros datos robados capturados por malware.

Gravedad predeterminada: media

- Origen de datos: registros de DNS

Este resultado le informa de que una instancia de EC2 de su entorno de AWS está consultando un nombre de dominio de un host remoto que se sabe que conserva credenciales y otros datos robados capturados por malware.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Trojan:EC2/PhishingDomainRequest!DNS

Una instancia EC2 consulta dominios implicados en ataques de phishing. La instancia EC2 podría estar comprometida.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que hay una instancia de EC2 en el entorno de AWS que está intentando hacer consultas a un dominio implicado en ataques de suplantación de identidad. Los dominios de suplantación de identidad los configura alguien que se presenta como una institución legítima para inducir a las personas a proporcionar información confidencial, como información de identificación personal, datos bancarios y de tarjetas de crédito, y contraseñas. Es posible que su instancia de EC2 esté intentando recuperar datos confidenciales almacenados en un sitio web de suplantación de identidad o que esté intentando configurar un sitio web de este tipo. La instancia EC2 podría estar comprometida.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Una instancia de EC2 establece conexiones con una dirección IP en una lista de amenazas personalizada.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que una instancia de EC2 del entorno de AWS se está comunicando con una dirección IP incluida en una lista de amenazas que ha cargado. En GuardDuty, una lista de amenazas consta de direcciones IP malintencionadas. GuardDuty genera resultados en función de las listas de amenazas cargadas. La lista de amenazas utilizada para generar este resultado se mostrará en los detalles del resultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

UnauthorizedAccess:EC2/MetadataDNSRebind

Una instancia de EC2 está haciendo búsquedas de DNS que se resuelven en el servicio de metadatos de la instancia.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que una instancia de EC2 del entorno de AWS está consultando un dominio que se resuelve en la dirección IP de metadatos de EC2 (169.254.169.254). Una consulta de DNS de este tipo puede indicar que la instancia es el objetivo de una técnica de reenlace de DNS. Esta técnica se puede utilizar para obtener metadatos de una instancia de EC2, que incluye las credenciales de IAM asociadas a la instancia.

El reenlace de DNS implica engañar a una aplicación que se ejecuta en la instancia de EC2 para que cargue datos devueltos desde una URL, de tal forma que el nombre de dominio de la URL se resuelve en la dirección IP de metadatos de EC2 (169.254.169.254). Esto hace que la aplicación obtenga acceso a los metadatos de EC2 y, posiblemente, los ponga a disposición del atacante.

Solo se puede obtener acceso a los metadatos de EC2 mediante el reenlace de DNS si la instancia de EC2 ejecuta una aplicación vulnerable que permite la inserción de URL o si un usuario obtiene acceso a la URL en un navegador web que se ejecuta en la instancia de EC2.

Recomendaciones de corrección:

En respuesta a este resultado, es importante evaluar si hay alguna aplicación vulnerable que se esté ejecutando en la instancia de EC2 o si un usuario ha utilizado un navegador para acceder al dominio identificado en el resultado. Si la causa raíz es una aplicación vulnerable, debe corregir la vulnerabilidad. Si un usuario ha navegado por el dominio identificado, debe bloquear el dominio o impedir que los usuarios puedan acceder a él. Si determina que el resultado está relacionado con cualquiera de los casos anteriores, debe revocar la sesión asociada a la instancia de EC2.

Algunos clientes de AWS asignan deliberadamente la dirección IP de metadatos a un nombre de dominio en sus servidores DNS autorizados. Si este es el caso en su entorno de , le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `UnauthorizedAccess:EC2/MetaDataDNSRebind`. El segundo criterio de filtro debe ser Dominio de la solicitud DNS y el valor debe coincidir con el dominio que ha mapeado a la dirección IP de metadatos (169.254.169.254). Para obtener más información sobre la creación de reglas de supresión, consulte Reglas de supresión.

UnauthorizedAccess:EC2/RDPBruteForce

Una instancia EC2 se ve implicada en ataques de fuerza bruta RDP.

Gravedad predeterminada: baja*

> **Note**
>
> La gravedad de este resultado es baja si su instancia de EC2 era el objetivo de un ataque de fuerza bruta. La gravedad de este resultado es alta si su instancia de EC2 es el actor que se utiliza para llevar a cabo el ataque de fuerza bruta.

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que una instancia de EC2 del entorno de AWS se ha visto envuelta en un ataque de fuerza bruta cuyo objetivo ha sido obtener contraseñas de servicios de RDP en sistemas basados en Windows. Esto puede significar un acceso no autorizado a los recursos de AWS.

Recomendaciones de corrección:

Si el Rol de recurso de su instancia es `ACTOR`, indica que su instancia se ha utilizado para llevar a cabo ataques de fuerza bruta a RDP. A no ser que esta instancia tenga un motivo legítimo para contactar con la dirección IP mostrada en la lista como `Target`, se recomienda que asuma que su instancia se ha visto afectada y lleve a cabo las acciones que aparecen en Corregir una instancia de Amazon EC2 potencialmente comprometida.

Si el Rol de recurso de su instancia es TARGET, este resultado puede corregirse mediante la delegación de la protección de su puerto RDP solo a direcciones IP de confianza a través de grupos de seguridad, ACL o firewalls. Para obtener más información, consulte Tips for securing your EC2 instances (Linux).

UnauthorizedAccess:EC2/SSHBruteForce

Una instancia EC2 se ve implicada en ataques de fuerza bruta SSH.

Gravedad predeterminada: baja*

> **Note**
>
> La gravedad de este resultado es baja si se dirige un ataque de fuerza a una de las instancias de EC2. La gravedad de este resultado es alta si la instancia de EC2 se está utilizando para llevar a cabo el ataque de fuerza bruta.

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que una instancia de EC2 del entorno de AWS se ha visto envuelta en un ataque de fuerza bruta cuyo objetivo ha sido obtener contraseñas de servicios de SSH en sistemas basados en Linux. Esto puede significar un acceso no autorizado a los recursos de AWS.

> **Note**
>
> Este resultado solo se genera mediante el monitoreo del tráfico en el puerto 22 por parte de . Si los servicios de SSH están configurados para usar otros puertos, no se genera este resultado.

Recomendaciones de corrección:

Si el objetivo del intento de fuerza bruta es un host bastión, esto podría representar el comportamiento esperado para su entorno de AWS. Si este es el caso, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos

criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `UnauthorizedAccess:EC2/SSHBruteForce`. El segundo criterio de filtro debe coincidir con la instancia o instancias que sirven como host de bastión. Puede utilizar el atributo ID de imagen de la instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. Para más información sobre la creación de reglas de supresión, consulte Reglas de supresión.

Si esta actividad no se espera en su entorno y el Rol de recurso de su instancia es `TARGET`, este resultado puede corregirse mediante la delegación de la protección de su puerto SSH solo a direcciones IP de confianza a través de grupos de seguridad, ACL o firewalls. Para obtener más información, consulte Tips for securing your EC2 instances (Linux).

Si el Rol de recurso de su instancia es `ACTOR`, indica que la instancia se ha utilizado para llevar a cabo ataques de fuerza bruta a SSH. A no ser que esta instancia tenga un motivo legítimo para contactar con la dirección IP mostrada en la lista como `Target`, se recomienda que asuma que su instancia se ha visto afectada y lleve a cabo las acciones que aparecen en Corregir una instancia de Amazon EC2 potencialmente comprometida.

UnauthorizedAccess:EC2/TorClient

La instancia EC2 está estableciendo conexiones con un guardia Tor o un nodo Authority.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que una instancia de EC2 del entorno de AWS está estableciendo conexiones con un nodo Authority o Guard de Tor. Tor es un software que permite las comunicaciones anónimas. Los guardias Tor y los nodos Authority actúan como gateways a una red Tor. Este tráfico puede indicar que esta instancia de EC2 se ha visto afectada y está actuando como cliente en una red de Tor. Este resultado puede significar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

UnauthorizedAccess:EC2/TorRelay

La instancia EC2 establece conexiones a una red Tor como repetidor Tor.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que una instancia de EC2 del entorno de AWS está estableciendo conexiones con una red de Tor de una forma que sugiere que actúa como un relé de Tor. Tor es un software que permite las comunicaciones anónimas. Tor incrementa el anonimato en la comunicación, ya que reenvía el tráfico potencialmente ilícito del cliente de un relé de Tor a otro.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

GuardDuty Tipos de búsqueda de IAM

Los siguientes resultados son específicos de las entidades y claves de acceso de IAM y siempre tendrán un Tipo de recurso de `AccessKey`. La gravedad y los detalles de los resultados varían en función del tipo de resultado.

Los resultados que se muestran aquí incluyen los orígenes de datos y los modelos utilizados para generar ese tipo de resultado. Para obtener más información, consulte Orígenes de datos fundamentales.

En el caso de todos los resultados relacionados con IAM, se recomienda que examine la entidad en cuestión y se asegure de que sus permisos sigan las prácticas recomendadas de privilegio mínimo. Si la actividad es inesperada, las credenciales pueden verse afectadas. Para obtener más información sobre los resultados de corrección, consulte Corregir las credenciales potencialmente comprometidas AWS.

Temas

- CredentialAccess:IAMUser/AnomalousBehavior
- DefenseEvasion:IAMUser/AnomalousBehavior

- Discovery:IAMUser/AnomalousBehavior
- Exfiltration:IAMUser/AnomalousBehavior
- Impact:IAMUser/AnomalousBehavior
- InitialAccess:IAMUser/AnomalousBehavior
- PenTest:IAMUser/KaliLinux
- PenTest:IAMUser/ParrotLinux
- PenTest:IAMUser/PentooLinux
- Persistence:IAMUser/AnomalousBehavior
- Policy:IAMUser/RootCredentialUsage
- PrivilegeEscalation:IAMUser/AnomalousBehavior
- Recon:IAMUser/MaliciousIPCaller
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/TorIPCaller

CredentialAccess:IAMUser/AnomalousBehavior

Una API utilizada para acceder a un AWS entorno se invocó de forma anómala.

Gravedad predeterminada: media

- Fuente de datos: evento CloudTrail de gestión

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas

que haya hecho en proximidad una sola identidad de usuario. La API observada suele asociarse a la fase de acceso a las credenciales en un ataque, donde un adversario intenta recopilar contraseñas, nombres de usuario y claves de acceso de su entorno. Las API de esta categoría son `GetPasswordData`, `GetSecretValue` y `GenerateDbAuthToken`.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los detalles del resultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

DefenseEvasion:IAMUser/AnomalousBehavior

Se ha invocado de forma anómala una API utilizada para evadir las medidas defensivas.

Gravedad predeterminada: media

- Fuente de datos: evento de gestión CloudTrail

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas que haya hecho en proximidad una sola identidad de usuario. La API observada suele asociarse a las tácticas de evasión de la defensa, en las que un adversario intenta ocultar sus rastros para evitar ser detectado. Las API de esta categoría suelen eliminar, deshabilitar o detener operaciones, como `DeleteFlowLogs`, `DisableAlarmActions` o `StopLogging`.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la

solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los detalles del resultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Discovery:IAMUser/AnomalousBehavior

Se ha invocado de forma anómala una API que se utiliza habitualmente para detectar recursos.

Gravedad predeterminada: baja

- Fuente de datos: evento de gestión CloudTrail

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas que haya hecho en proximidad una sola identidad de usuario. La API observada suele asociarse a la etapa de descubrimiento de un ataque, cuando un adversario recopila información para determinar si su AWS entorno es susceptible a un ataque más amplio. Las API de esta categoría suelen obtener, describir o enumerar operaciones, como `DescribeInstances`, `GetRolePolicy` o `ListAccessKeys`.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los detalles del resultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Exfiltration:IAMUser/AnomalousBehavior

Una API que se utiliza habitualmente para recopilar datos de un AWS entorno se invocó de forma anómala.

Gravedad predeterminada: alta

- Fuente de datos: evento CloudTrail de gestión

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas que haya hecho en proximidad una sola identidad de usuario. La API observada suele asociarse a tácticas de exfiltración, en las que un adversario intenta recopilar datos de su red mediante el empaquetado y el cifrado para evitar ser detectado. Las API para este tipo de resultado son únicamente operaciones de administración (plano de control) y, por lo general, están relacionadas con S3, instantáneas y bases de datos, como `PutBucketReplication`, `CreateSnapshot` o `RestoreDBInstanceFromDBSnapshot`.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los detalles del resultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Impact:IAMUser/AnomalousBehavior

Una API que se utiliza habitualmente para manipular datos o procesos en un AWS entorno se invocó de forma anómala.

Gravedad predeterminada: alta

- Fuente de datos: evento de gestión CloudTrail

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas que haya hecho en proximidad una sola identidad de usuario. La API observada suele asociarse a tácticas de impacto, en las que un adversario intenta interrumpir las operaciones y manipular, interrumpir o destruir los datos de la cuenta. Las API para este tipo de resultado suelen eliminar, actualizar o preparar operaciones, como `DeleteSecurityGroup`, `UpdateUser` o `PutBucketPolicy`.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los detalles del resultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

InitialAccess:IAMUser/AnomalousBehavior

Una API que se utiliza habitualmente para obtener acceso no autorizado a un AWS entorno se invocó de forma anómala.

Gravedad predeterminada: media

- Fuente de datos: evento CloudTrail de gestión

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas que haya hecho en proximidad una sola identidad de usuario. La API observada suele asociarse a la fase de acceso inicial de un ataque, cuando un adversario intenta establecer acceso a su entorno. Las API de esta categoría suelen obtener operaciones de token o de sesión, como `GetFederationToken`, `StartSession` o `GetAuthorizationToken`.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los detalles del resultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

PenTest:IAMUser/KaliLinux

Se invocó una API desde una máquina Kali Linux.

Gravedad predeterminada: media

- Fuente de datos: evento CloudTrail de administración

Este hallazgo le informa de que una máquina que ejecuta Kali Linux realiza llamadas a la API con credenciales que pertenecen a la AWS cuenta indicada en su entorno. Kali Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para detectar puntos débiles en la configuración de EC2 y obtener acceso no autorizado a su AWS entorno.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

PenTest:IAMUser/ParrotLinux

Se ha invocado una API desde una máquina Parrot Security Linux.

Gravedad predeterminada: media

- Fuente de datos: evento CloudTrail de administración

Este hallazgo le informa de que un equipo que ejecuta Parrot Security Linux realiza llamadas a la API con credenciales que pertenecen a la AWS cuenta indicada en su entorno. Parrot Security Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para detectar puntos débiles en la configuración de EC2 y obtener acceso no autorizado a su AWS entorno.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

PenTest:IAMUser/PentooLinux

Se ha invocado una API desde una máquina Pentoo Linux.

Gravedad predeterminada: media

- Fuente de datos: evento CloudTrail de administración

Este hallazgo le informa de que una máquina que ejecuta Pentoo Linux está realizando llamadas a la API con credenciales que pertenecen a la AWS cuenta indicada en su entorno. Pentoo Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para detectar puntos débiles en la configuración de EC2 y obtener acceso no autorizado a su AWS entorno.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Persistence:IAMUser/AnomalousBehavior

Se invocó de forma anómala una API que se utiliza habitualmente para mantener el acceso no autorizado a un AWS entorno.

Gravedad predeterminada: media

- Fuente de datos: evento CloudTrail de gestión

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas que haya hecho en proximidad una sola identidad de usuario. La API observada suele asociarse a tácticas de persistencia, en las que un adversario ha logrado acceder a su entorno e intenta conservar ese acceso. Las API de esta categoría suelen crear, importar o modificar operaciones, como `CreateAccessKey`, `ImportKeyPair` o `ModifyInstanceAttribute`.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los detalles del resultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Policy:IAMUser/RootCredentialUsage

Se ha invocado una API mediante credenciales de inicio de sesión del usuario raíz.

Gravedad predeterminada: baja

- Fuente de datos: eventos CloudTrail de administración o CloudTrail eventos de datos

Este resultado le informa de que las credenciales de inicio de sesión del usuario raíz de la Cuenta de AWS que aparece en la lista de su entorno se están utilizando para hacer solicitudes a los servicios de AWS . Se recomienda que los usuarios nunca utilicen las credenciales de inicio de sesión del usuario raíz para acceder a AWS los servicios. En su lugar, se debe acceder a los AWS servicios con credenciales temporales con privilegios mínimos de AWS Security Token Service (STS). En los

casos donde no se admite AWS STS , se recomienda utilizar las credenciales de usuario de IAM. Para obtener más información, consulte las prácticas recomendadas de IAM.

> **Note**
>
> Si la detección de amenazas de S3 está habilitada para la cuenta, este resultado puede generarse en respuesta a los intentos de ejecutar operaciones del plano de datos de S3 en los recursos de S3 mediante las credenciales de inicio de sesión del usuario raíz de la Cuenta de AWS. La llamada a la API utilizada se mostrará en los detalles de resultado. Si la detección de amenazas de S3 no está habilitada, solo las API de registro de eventos pueden activar este resultado. Para obtener más información acerca de la detección de amenazas de S3, consulte S3 protection.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

PrivilegeEscalation:IAMUser/AnomalousBehavior

Una API que se utiliza habitualmente para obtener permisos de alto nivel para un AWS entorno se invocó de forma anómala.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de administración

Este resultado le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas que haya hecho en proximidad una sola identidad de usuario. La API observada suele asociarse a tácticas de derivación de privilegios, en las que un adversario intenta obtener permisos de nivel superior para acceder a un entorno. Las API de esta categoría suelen implicar operaciones que cambian las políticas, los roles y los usuarios de IAM, como `AssociateIamInstanceProfile`, `AddUserToGroup` o `PutUserPolicy`.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta

e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los detalles del resultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Recon:IAMUser/MaliciousIPCaller

Se ha invocado una API desde una dirección IP malintencionada conocida.

Gravedad predeterminada: media

- Fuente de datos: eventos de gestión CloudTrail

Este resultado le informa de que una operación de API que puede enumerar o describir los recursos de AWS se ha invocado desde una dirección IP que aparece en una lista de amenazas. Un atacante puede utilizar credenciales robadas para realizar este tipo de reconocimiento de sus AWS recursos con el fin de encontrar credenciales más valiosas o determinar las capacidades de las credenciales que ya tiene.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Recon:IAMUser/MaliciousIPCaller.Custom

Se ha invocado una API desde una dirección IP malintencionada conocida.

Gravedad predeterminada: media

- Fuente de datos: eventos de gestión CloudTrail

Este resultado le informa de que una operación de API que puede enumerar o describir los recursos de AWS en una cuenta dentro de su entorno se ha invocado desde una dirección IP que aparece en una lista de amenazas personalizada. La lista de amenazas utilizada se mostrará en los detalles del resultado. Un atacante podría utilizar credenciales robadas para realizar este tipo de reconocimiento de sus AWS recursos con el fin de encontrar credenciales más valiosas o determinar las capacidades de las credenciales que ya tiene.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Recon:IAMUser/TorIPCaller

Se ha invocado una API desde una dirección IP de un nodo de salida de Tor.

Gravedad predeterminada: media

- Fuente de datos: eventos de administración CloudTrail

Este resultado le informa de que una operación de API que puede enumerar o describir los recursos de AWS de una cuenta dentro de su entorno se ha invocado desde una dirección IP de nodo de salida de Tor. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Un atacante utilizaría Tor para ocultar su verdadera identidad.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail el registro estaba deshabilitado.

Gravedad predeterminada: baja

- Fuente de datos: eventos CloudTrail de administración

Este hallazgo le informa de que se ha desactivado un CloudTrail sendero de su AWS entorno. Puede tratarse del intento por parte de un atacante de desactivar el registro para cubrir sus rastros mediante la eliminación de cualquier indicio de su actividad y, a su vez, la obtención de acceso a los recursos de AWS con fines maliciosos. Este resultado se puede activar mediante una eliminación o actualización correcta de un registro de seguimiento. Este hallazgo también se puede provocar si se elimina correctamente un depósito de S3 que almacena los registros de un rastro al que está asociado GuardDuty.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Stealth:IAMUser/PasswordPolicyChange

La política de contraseñas de la cuenta se ha debilitado.

Gravedad predeterminada: baja*

> **Note**
>
> La gravedad de este resultado puede ser baja, media o alta, según la gravedad de los cambios hechos en la política de contraseñas.

- Fuente de datos: eventos CloudTrail de administración

La política de contraseñas de AWS cuentas se debilitó en la cuenta incluida en la lista de su AWS entorno. Por ejemplo, se ha eliminado o actualizado para exigir menos caracteres, no requerir símbolos y números, o se ha requerido la ampliación del período de vencimiento de la contraseña. Este descubrimiento también puede deberse a un intento de actualizar o eliminar la política de contraseñas de su AWS cuenta. La política de contraseñas de las AWS cuentas define las reglas que rigen los tipos de contraseñas que se pueden configurar para los usuarios de IAM. Una política de contraseñas más débil permite la creación de contraseñas que son fáciles de recordar y potencialmente más fáciles de adivinar, y que suponen un riesgo para la seguridad.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Se han observado varios inicios de sesión correctos en la consola desde distintos lugares del mundo.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de gestión

Este resultado le informa de que se han observado varios inicios de sesión correctos en la consola para el mismo usuario de IAM aproximadamente al mismo tiempo en diversas ubicaciones geográficas. Estos patrones de ubicación de acceso anómalos y riesgosos indican un posible acceso no autorizado a sus AWS recursos.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

Se están utilizando las credenciales creadas exclusivamente para una instancia de EC2 a través de un rol de lanzamiento de instancias desde otra cuenta dentro de AWS.

Gravedad predeterminada: alta*

> **Note**
>
> La gravedad predeterminada de este resultado es alta. Sin embargo, si la API la ha invocado una cuenta afiliada a su AWS entorno, la gravedad es media.

- Fuente de datos: eventos CloudTrail de administración o eventos de datos de S3

Este hallazgo le informa cuando las credenciales de la instancia de EC2 se utilizan para invocar las API desde una dirección IP que pertenece a una AWS cuenta diferente a la que se ejecuta la instancia de EC2 asociada.

AWS no recomienda redistribuir las credenciales temporales fuera de la entidad que las creó (por ejemplo, AWS aplicaciones, EC2 o Lambda). Sin embargo, los usuarios autorizados pueden exportar credenciales desde sus instancias EC2 para realizar llamadas a la API legítimas. Si el `remoteAccountDetails.Affiliated` campo es, `True` la API se invocó desde una cuenta asociada a su entorno. AWS Para descartar un posible ataque y verificar la legitimidad de la actividad, póngase en contacto con el usuario de IAM al que se han asignado estas credenciales.

> **Note**
>
> Si GuardDuty observa una actividad continua desde una cuenta remota, su modelo de aprendizaje automático (ML) identificará este comportamiento como esperado. Por lo tanto, GuardDuty dejará de generar este resultado para la actividad de esa cuenta remota. GuardDuty seguirá recopilando información sobre el nuevo comportamiento de otras cuentas remotas y volverá a evaluar las cuentas remotas detectadas a medida que el comportamiento vaya cambiando con el tiempo.

Recomendaciones de corrección:

En respuesta a este resultado, puede utilizar el siguiente flujo de trabajo para determinar el curso de acción:

1. Identifique la cuenta remota implicada en el campo `service.action.awsApiCallAction.remoteAccountDetails.accountId`.
2. A continuación, determine si esa cuenta está afiliada a su GuardDuty entorno desde el `service.action.awsApiCallAction.remoteAccountDetails.affiliated` terreno.
3. Si la cuenta está afiliada, contacte con el propietario de la cuenta remota y con el propietario de las credenciales de la instancia de EC2 para investigar.
4. Si la cuenta no está afiliada, primero evalúe si la cuenta está asociada a su organización pero no forma parte de la configuración de GuardDuty varias cuentas o si GuardDuty aún no está

habilitada en la cuenta. De lo contrario, contacte con el propietario de las credenciales de EC2 para determinar si existe algún caso de uso para que una cuenta remota utilice estas credenciales.

5. Si el propietario de las credenciales no reconoce la cuenta remota, es posible que un actor de amenazas que opere dentro de AWShaya puesto en peligro las credenciales. Debe seguir las medidas recomendadas en Corregir una instancia de Amazon EC2 potencialmente comprometida para proteger su entorno. Además, puedes enviar una denuncia de abuso al equipo de AWS Confianza y Seguridad para iniciar una investigación sobre la cuenta remota. Cuando envíe su informe al equipo de Seguridad y confianza de AWS , incluya todos los detalles del resultado en JSON.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Las credenciales creadas exclusivamente para una instancia EC2 a través de un rol de lanzamiento de instancias se utilizan desde una dirección IP externa.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de administración o eventos de datos de S3

Este hallazgo le informa de que un host externo AWS ha intentado ejecutar operaciones de AWS API con AWS credenciales temporales que se crearon en una instancia de EC2 de su AWS entorno. La instancia de EC2 que aparece en la lista podría estar comprometida y las credenciales temporales de esta instancia podrían haberse filtrado a un host remoto externo. AWS AWS no recomienda redistribuir las credenciales temporales fuera de la entidad que las creó (por ejemplo, AWS aplicaciones, EC2 o Lambda). Sin embargo, los usuarios autorizados pueden exportar credenciales desde sus instancias EC2 para realizar llamadas a la API legítimas. Para descartar un posible ataque y verificar la legitimidad de la actividad, valide si se espera el uso de credenciales de instancia por parte de la IP remota en el resultado.

> **Note**
>
> Si GuardDuty observa una actividad continua desde una cuenta remota, su modelo de aprendizaje automático (ML) identificará este comportamiento como esperado. Por lo tanto, GuardDuty dejará de generar este resultado para la actividad de esa cuenta remota. GuardDuty seguirá recopilando información sobre el nuevo comportamiento de otras cuentas

remotas y volverá a evaluar las cuentas remotas detectadas a medida que el comportamiento vaya cambiando con el tiempo.

Recomendaciones de corrección:

Este resultado se genera cuando la red está configurada para dirigir el tráfico de Internet de tal forma que salga por una puerta de enlace en las instalaciones y no por una puerta de enlace de Internet (IGW) de la VPC. Las configuraciones comunes, como el uso de AWS Outposts o de conexiones de VPN de la VPC, pueden generar tráfico dirigido de esta manera. Si se trata de un comportamiento esperado, se recomienda utilizar reglas de supresión y crear una regla que conste de dos criterios de filtrado. El primer criterio es Tipo de resultado, que debería ser `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. El segundo criterio de filtro es la Dirección IPv4 de la persona que llama a la API con el rango de direcciones IP o CIDR de su puerta de enlace de Internet en las instalaciones. Para obtener más información sobre la creación de reglas de supresión, consulte Reglas de supresión.

> **Note**
>
> Si GuardDuty observa la actividad continua de una fuente externa, su modelo de aprendizaje automático identificará este comportamiento como esperado y dejará de generar este resultado para la actividad de esa fuente. GuardDuty seguirá buscando nuevos comportamientos a partir de otras fuentes y reevaluará las fuentes aprendidas a medida que el comportamiento vaya cambiando con el tiempo.

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte Corregir las credenciales potencialmente comprometidas AWS.

UnauthorizedAccess:IAMUser/MaliciousIPCaller

Se ha invocado una API desde una dirección IP malintencionada conocida.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de gestión

Este hallazgo indica que se ha invocado una operación de API (por ejemplo, un intento de lanzar una instancia EC2, crear un nuevo usuario de IAM o modificar sus AWS privilegios) desde una dirección IP maliciosa conocida. Esto puede indicar un acceso no autorizado a AWS los recursos de su entorno.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

Se ha invocado una API desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de administración

Este hallazgo indica que se ha invocado una operación de API (por ejemplo, un intento de lanzar una instancia EC2, crear un nuevo usuario de IAM o modificar AWS privilegios) desde una dirección IP incluida en una lista de amenazas que usted ha subido. En , una lista de amenazas está formada por direcciones IP malintencionadas conocidas. Esto puede indicar un acceso no autorizado a AWS los recursos de su entorno.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

UnauthorizedAccess:IAMUser/TorIPCaller

Se ha invocado una API desde una dirección IP de un nodo de salida de Tor.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de administración

Este resultado le informa de que una operación de la API (por ejemplo, un intento de lanzar una instancia de EC2, crear un nuevo usuario de IAM o modificar los privilegios de AWS) se ha invocado desde una dirección IP de nodo de salida de Tor. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Tipos de resultados de registros de auditoría de Kubernetes

Los siguientes resultados son específicos de los recursos de Kubernetes y siempre tendrán un resource_type de `EKSCluster`. La gravedad y los detalles de los resultados varían en función del tipo de resultado.

Para todos los resultados de tipo Kubernetes, se recomienda que examine el recurso en cuestión para determinar si la actividad es esperada o potencialmente maliciosa. Para obtener orientación sobre cómo corregir un recurso de Kubernetes comprometido identificado mediante un hallazgo, consulte. GuardDuty Corrección de los resultados de la supervisión de registros de auditoría de EKS

> **Note**
>
> Si se espera la actividad por la que se generan estos resultados, considere agregar Reglas de supresión para evitar futuras alertas.

Temas

- CredentialAccess:Kubernetes/MaliciousIPCaller
- CredentialAccess:Kubernetes/MaliciousIPCaller.Custom
- CredentialAccess:Kubernetes/SuccessfulAnonymousAccess
- CredentialAccess:Kubernetes/TorIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller

- DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom
- DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess
- DefenseEvasion:Kubernetes/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom
- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Impact:Kubernetes/SuccessfulAnonymousAccess
- Impact:Kubernetes/TorIPCaller
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Persistence:Kubernetes/MaliciousIPCaller
- Persistence:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/SuccessfulAnonymousAccess
- Persistence:Kubernetes/TorIPCaller
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/KubeflowDashboardExposed
- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

> **Note**
>
> Antes de la versión 1.14 de Kubernetes, el grupo estaba asociado a Kubernetes y de forma predeterminada`system:unauthenticated`. `system:discovery` `system:basic-user` ClusterRoles Esta asociación puede permitir el acceso no deseado de usuarios anónimos. Las actualizaciones del clúster no revocan estos permisos. Aunque se haya actualizado el clúster a la versión 1.14 o posterior, es posible que estos permisos sigan habilitados. Se recomienda que desasocie estos permisos del grupo `system:unauthenticated`. Para obtener orientación sobre la revocación de estos permisos, consulte las prácticas recomendadas de seguridad para Amazon EKS en la Guía del usuario de Amazon EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller

Se ha invocado una API que se suele utilizar para acceder a las credenciales o los secretos de un clúster de Kubernetes desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha invocado una operación de API desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a las tácticas de acceso a las credenciales, en las que un adversario intenta recopilar contraseñas, nombres de usuario y claves de acceso de su clúster de Kubernetes.

Recomendaciones de corrección:

Si el usuario mencionado en la conclusión de la `KubernetesUserDetails` sección es`system:anonymous`, investigue por qué se le permitió al usuario anónimo invocar la API y revocar los permisos, si fuera necesario, siguiendo las instrucciones de las prácticas recomendadas de seguridad para Amazon EKS de la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investíguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue

maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Se ha invocado una API que se utiliza habitualmente para acceder a las credenciales o los secretos de un clúster de Kubernetes desde una dirección IP en una lista de amenazas personalizada.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha invocado una operación de la API desde una dirección IP que aparece en una lista de amenazas que se ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. La API observada suele asociarse a las tácticas de acceso a las credenciales, en las que un adversario intenta recopilar contraseñas, nombres de usuario y claves de acceso de su clúster de Kubernetes.

Recomendaciones de corrección:

Si el usuario mencionado en la conclusión de la `KubernetesUserDetails` sección `essystem:anonymous`, investigue por qué se le permitió al usuario anónimo invocar la API y revocar los permisos, si fuera necesario, siguiendo las instrucciones de las prácticas recomendadas de seguridad para Amazon EKS de la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investíguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

Un usuario no autenticado ha invocado una API que se suele utilizar para acceder a las credenciales o los secretos de un clúster de Kubernetes.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que el usuario `system:anonymous` ha invocado correctamente una operación de la API. No se han autenticado las llamadas a la API que ha hecho `system:anonymous`. La API observada suele asociarse a las tácticas de acceso a las credenciales, en las que un adversario intenta recopilar contraseñas, nombres de usuario y claves de acceso de su clúster de Kubernetes. Esta actividad indica que se permite el acceso anónimo o no autenticado a la acción de la API descrita en el resultado y que se puede permitir a otras acciones. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` en su clúster y asegurarse de que todos los permisos sean necesarios. Si los permisos se han concedido por error o de forma maliciosa, debe revocar el acceso del usuario y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte Prácticas recomendadas de seguridad para Amazon EKS en la Guía del usuario de Amazon EKS.

Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

CredentialAccess:Kubernetes/TorIPCaller

Se ha invocado una API que se suele utilizar para acceder a las credenciales o los secretos de un clúster de Kubernetes desde una dirección IP de un nodo de salida de Tor.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha invocado una API desde una dirección IP de un nodo de salida de Tor. La API observada suele asociarse a las tácticas de acceso a las credenciales, en las que un adversario intenta recopilar contraseñas, nombres de usuario y claves de acceso de su clúster de Kubernetes. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El

último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos del clúster de Kubernetes con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si el usuario mencionado en la conclusión de la `KubernetesUserDetails` sección `essystem:anonymous`, investigue por qué se le permitió al usuario anónimo invocar la API y revocar los permisos, si fuera necesario, siguiendo las instrucciones de las prácticas recomendadas de seguridad para Amazon EKS de la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investíguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller

Se ha invocado una API que se suele utilizar para evadir medidas defensivas desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha invocado una operación de API desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a las tácticas de evasión de la defensa, en las que un adversario intenta ocultar sus acciones para evitar ser detectado.

Recomendaciones de corrección:

Si el usuario mencionado en la conclusión de la `KubernetesUserDetails` sección `essystem:anonymous`, investigue por qué se le permitió al usuario anónimo invocar la API y revocar los permisos, si fuera necesario, siguiendo las instrucciones de las prácticas recomendadas de seguridad para Amazon EKS de la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investíguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

Se ha invocado una API que se suele utilizar para evadir medidas de defensa desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha invocado una operación de la API desde una dirección IP que aparece en una lista de amenazas que se ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. La API observada suele asociarse a las tácticas de evasión de la defensa, en las que un adversario intenta ocultar sus acciones para evitar ser detectado.

Recomendaciones de corrección:

Si el usuario mencionado en la conclusión de la `KubernetesUserDetails` sección es`system:anonymous`, investigue por qué se le permitió al usuario anónimo invocar la API y revocar los permisos, si fuera necesario, siguiendo las instrucciones de las prácticas recomendadas de seguridad para Amazon EKS de la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investíguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

Un usuario no autenticado ha invocado una API que se suele utilizar para evadir medidas defensivas.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que el usuario `system:anonymous` ha invocado correctamente una operación de la API. No se han autenticado las llamadas a la API que ha hecho

`system:anonymous`. La API observada suele asociarse a las tácticas de evasión de la defensa, en las que un adversario intenta ocultar sus acciones para evitar ser detectado. Esta actividad indica que se permite el acceso anónimo o no autenticado a la acción de la API descrita en el resultado y que se puede permitir a otras acciones. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` en su clúster y asegurarse de que todos los permisos sean necesarios. Si los permisos se han concedido por error o de forma maliciosa, debe revocar el acceso del usuario y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte Prácticas recomendadas de seguridad para Amazon EKS en la Guía del usuario de Amazon EKS.

Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

DefenseEvasion:Kubernetes/TorIPCaller

Se ha invocado una API que se suele utilizar para evadir medidas defensivas desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha invocado una API desde una dirección IP de un nodo de salida de Tor. La API observada suele asociarse a las tácticas de evasión de la defensa, en las que un adversario intenta ocultar sus acciones para evitar ser detectado. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado al clúster de Kubernetes con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si el usuario mencionado en la conclusión de la `KubernetesUserDetails` sección es`system:anonymous`, investigue por qué se le permitió al usuario anónimo invocar la API y

revocar los permisos, si fuera necesario, siguiendo las instrucciones de las prácticas recomendadas de seguridad para Amazon EKS de la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investíguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Discovery:Kubernetes/MaliciousIPCaller

Se ha invocado una API que se suele utilizar para descubrir recursos en un clúster de Kubernetes desde una dirección IP.

Gravedad predeterminada: media

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha invocado una operación de API desde una dirección IP asociada a una actividad maliciosa conocida. La API observada se suele utilizar en la fase de detección de un ataque, en la que un atacante recopila información para determinar si el clúster de Kubernetes es susceptible a un ataque más amplio.

Recomendaciones de corrección:

Si el usuario mencionado en la conclusión de la `KubernetesUserDetails` sección `essystem:anonymous`, investigue por qué se le permitió al usuario anónimo invocar la API y revocar los permisos, si fuera necesario, siguiendo las instrucciones de las prácticas recomendadas de seguridad para Amazon EKS de la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investíguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Discovery:Kubernetes/MaliciousIPCaller.Custom

Se ha invocado una API que se suele utilizar para detectar recursos en un clúster de Kubernetes desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: media

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha invocado una API desde una dirección IP que aparece en una lista de amenazas que se ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. La API observada se suele utilizar en la fase de detección de un ataque, en la que un atacante recopila información para determinar si el clúster de Kubernetes es susceptible a un ataque más amplio.

Recomendaciones de corrección:

Si el usuario mencionado en la conclusión de la `KubernetesUserDetails` sección es`system:anonymous`, investigue por qué se le permitió al usuario anónimo invocar la API y revocar los permisos, si fuera necesario, siguiendo las instrucciones de las prácticas recomendadas de seguridad para Amazon EKS de la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investíguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Discovery:Kubernetes/SuccessfulAnonymousAccess

Un usuario no autenticado ha invocado una API que se suele utilizar para descubrir recursos en un clúster de Kubernetes.

Gravedad predeterminada: media

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que el usuario `system:anonymous` ha invocado correctamente una operación de la API. No se han autenticado las llamadas a la API que ha hecho `system:anonymous`. La API observada suele asociarse a la fase de detección de un ataque, cuando un adversario recopila información sobre el clúster de Kubernetes. Esta actividad indica que se permite el acceso anónimo o no autenticado a la acción de la API descrita en el resultado y que se puede permitir a otras acciones. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` en su clúster y asegurarse de que todos los permisos sean necesarios. Si los permisos se han concedido por error o de forma maliciosa, debe revocar el acceso del usuario y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte Prácticas recomendadas de seguridad para Amazon EKS en la Guía del usuario de Amazon EKS.

Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Discovery:Kubernetes/TorIPCaller

Se ha invocado una API que se suele utilizar para detectar recursos en un clúster de Kubernetes desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: media

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha invocado una API desde una dirección IP de un nodo de salida de Tor. La API observada se suele utilizar en la fase de detección de un ataque, en la que un atacante recopila información para determinar si el clúster de Kubernetes es susceptible a un ataque más amplio. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado al clúster de Kubernetes con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si el usuario mencionado en la conclusión de la `KubernetesUserDetails` sección `essystem:anonymous`, investigue por qué se le permitió al usuario anónimo invocar la API y revoque los permisos, si fuera necesario, siguiendo las instrucciones de las prácticas recomendadas de seguridad para Amazon EKS de la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investíguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Execution:Kubernetes/ExecInKubeSystemPod

Se ha ejecutado un comando en un pod dentro del espacio de nombres **`kube-system`**

Gravedad predeterminada: media

- Característica: registros de auditoría de Kubernetes

Este resultado indica que se ha ejecutado un comando en un pod dentro del espacio de nombres `kube-system` mediante la API exec de Kubernetes. El espacio de nombres `kube-system` es un espacio de nombres predeterminado, que se utiliza principalmente para componentes de nivel de sistema, como `kube-dns` y `kube-proxy`. Es muy poco común ejecutar comandos dentro de pods o contenedores de un espacio de nombres `kube-system`, lo que puede indicar una actividad sospechosa.

Recomendaciones de corrección:

Si la ejecución de este comando es inesperada, es posible que las credenciales de identidad de usuario utilizada para ejecutar el comando se hayan visto afectadas. Revoque el acceso del usuario y anule cualquier cambio que haya hecho un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Impact:Kubernetes/MaliciousIPCaller

Se ha invocado una API que se suele utilizar para manipular recursos en un clúster de Kubernetes desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha invocado una operación de API desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a tácticas de impacto, en las que un adversario intenta manipular, interrumpir o destruir los datos de su entorno. AWS

Recomendaciones de corrección:

Si el usuario mencionado en la conclusión de la `KubernetesUserDetails` sección `essystem:anonymous`, investigue por qué se le permitió al usuario anónimo invocar la API y revocar los permisos, si fuera necesario, siguiendo las instrucciones de las prácticas recomendadas de seguridad para Amazon EKS de la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investíguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Impact:Kubernetes/MaliciousIPCaller.Custom

Se ha invocado una API que se suele utilizar para manipular los recursos de un clúster de Kubernetes desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha invocado una operación de la API desde una dirección IP que aparece en una lista de amenazas que se ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. La API observada suele asociarse a tácticas de impacto, en las que un adversario intenta manipular, interrumpir o destruir los datos de su entorno. AWS

Recomendaciones de corrección:

Si el usuario mencionado en la conclusión de la `KubernetesUserDetails` sección `essystem:anonymous`, investigue por qué se le permitió al usuario anónimo invocar la API y revocar los permisos, si fuera necesario, siguiendo las instrucciones de las prácticas recomendadas de seguridad para Amazon EKS de la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investíguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Impact:Kubernetes/SuccessfulAnonymousAccess

Un usuario no autenticado ha invocado una API que se suele utilizar para manipular los recursos de un clúster de Kubernetes.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que el usuario `system:anonymous` ha invocado correctamente una operación de la API. No se han autenticado las llamadas a la API que ha hecho `system:anonymous`. La API observada suele asociarse a la fase de impacto de un ataque, cuando un adversario está manipulando los recursos del clúster. Esta actividad indica que se permite el acceso anónimo o no autenticado a la acción de la API descrita en el resultado y que se puede permitir a otras acciones. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` en su clúster y asegurarse de que todos los permisos sean necesarios. Si los permisos se han concedido por error o de forma maliciosa, debe revocar el acceso del usuario y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte Prácticas recomendadas de seguridad para Amazon EKS en la Guía del usuario de Amazon EKS.

Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Impact:Kubernetes/TorIPCaller

Se ha invocado una API que se suele utilizar para manipular los recursos de un clúster de Kubernetes desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha invocado una API desde una dirección IP de un nodo de salida de Tor. La API observada suele asociarse a tácticas de impacto, en las que un adversario intenta manipular, interrumpir o destruir los datos que están dentro de su entorno de AWS . Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado al clúster de Kubernetes con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si el usuario mencionado en la conclusión de la `KubernetesUserDetails` sección `essystem:anonymous`, investigue por qué se le permitió al usuario anónimo invocar la API y revocar los permisos, si fuera necesario, siguiendo las instrucciones de las prácticas recomendadas de seguridad para Amazon EKS de la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investíguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Persistence:Kubernetes/ContainerWithSensitiveMount

Se ha lanzado un contenedor con una ruta de host externa confidencial montada en su interior.

Gravedad predeterminada: media

- Característica: registros de auditoría de Kubernetes

Este resultado indica que se ha lanzado un contenedor con una configuración que incluía una ruta de host confidencial con acceso de escritura en la sección `volumeMounts`. Esto hace que la ruta confidencial del host sea accesible y se pueda sobrescribir desde el interior del contenedor. Los adversarios suelen utilizar esta técnica para acceder al sistema de archivos del host.

Recomendaciones de corrección:

Si el lanzamiento de este contenedor es inesperado, es posible que las credenciales de identidad de usuario utilizadas para lanzarlo se hayan visto afectadas. Revoque el acceso del usuario y anule cualquier cambio que haya hecho un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Si el lanzamiento de este contenedor es esperado, se recomienda utilizar una regla de supresión que consista en un criterio de filtrado basado en el campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. En los criterios de filtrado, el campo `imagePrefix` debe ser el mismo que el `imagePrefix` especificado en el resultado. Para obtener más información sobre la creación de reglas de supresión, consulte Reglas de supresión.

Persistence:Kubernetes/MaliciousIPCaller

Se ha invocado una API que se suele utilizar para acceder a un clúster de Kubernetes desde una dirección IP maliciosa conocida.

Gravedad predeterminada: media

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha invocado una operación de API desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a tácticas de persistencia, en las que un adversario ha logrado acceder al clúster de Kubernetes e intenta conservar ese acceso.

Recomendaciones de corrección:

Si el usuario mencionado en la conclusión de la `KubernetesUserDetails` sección `essystem:anonymous`, investigue por qué se le permitió al usuario anónimo invocar la API y revocar los permisos, si fuera necesario, siguiendo las instrucciones de las prácticas recomendadas de seguridad para Amazon EKS de la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investíguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Persistence:Kubernetes/MaliciousIPCaller.Custom

Se ha invocado una API que se suele utilizar para obtener acceso persistente a un clúster de Kubernetes desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: media

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha invocado una operación de la API desde una dirección IP que aparece en una lista de amenazas que se ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. La API observada suele asociarse a tácticas de persistencia, en las que un adversario ha logrado acceder al clúster de Kubernetes e intenta conservar ese acceso.

Recomendaciones de corrección:

Si el usuario mencionado en la conclusión de la `KubernetesUserDetails` sección es`system:anonymous`, investigue por qué se le permitió al usuario anónimo invocar la API y revocar los permisos, si fuera necesario, siguiendo las instrucciones de las prácticas recomendadas de seguridad para Amazon EKS de la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investíguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Persistence:Kubernetes/SuccessfulAnonymousAccess

Un usuario no autenticado ha invocado una API que se suele utilizar para obtener permisos de nivel superior a un clúster de Kubernetes.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que el usuario `system:anonymous` ha invocado correctamente una operación de la API. No se han autenticado las llamadas a la API que ha hecho `system:anonymous`. La API observada suele asociarse a tácticas de persistencia, en las que un adversario ha logrado acceder al clúster e intenta conservar ese acceso. Esta actividad indica que se permite el acceso anónimo o no autenticado a la acción de la API descrita en el resultado y que se puede permitir a otras acciones. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` en su clúster y asegurarse de que todos los permisos sean necesarios. Si los permisos se han concedido por error o de forma maliciosa, debe revocar el acceso del usuario y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte Prácticas recomendadas de seguridad para Amazon EKS en la Guía del usuario de Amazon EKS.

Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Persistence:Kubernetes/TorIPCaller

Se ha invocado una API que se suele utilizar para acceder a un clúster de Kubernetes desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: media

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha invocado una API desde una dirección IP de un nodo de salida de Tor. La API observada suele asociarse a tácticas de persistencia, en las que un adversario ha logrado acceder al clúster de Kubernetes e intenta conservar ese acceso. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a sus AWS recursos con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si el usuario mencionado en la conclusión de la `KubernetesUserDetails` sección `essystem:anonymous`, investigue por qué se le permitió al usuario anónimo invocar la API y revocar los permisos, si fuera necesario, siguiendo las instrucciones de las prácticas recomendadas de seguridad para Amazon EKS de la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investíguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

Se concedieron privilegios de administrador en un clúster de Kubernetes a la cuenta de servicio predeterminada.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se han concedido privilegios de administrador a la cuenta de servicio predeterminada de un espacio de nombres de su clúster de Kubernetes. Kubernetes crea una cuenta de servicio predeterminada para todos los espacios de nombres del clúster. Asigna automáticamente la cuenta de servicio predeterminada como identidad a los pods que no se han asociado explícitamente a otra cuenta de servicio. Si la cuenta de servicio predeterminada tiene privilegios de administrador, es posible que los pods se inicien involuntariamente con privilegios de administrador. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

No debe utilizar la cuenta de servicio predeterminada para conceder permisos a los pods. En su lugar, debe crear una cuenta de servicio dedicada para cada carga de trabajo y conceder el permiso a esa cuenta en función de sus necesidades. Para solucionar este problema, debe crear cuentas de servicio dedicadas para todos sus pods y cargas de trabajo, además de actualizar los pods y las cargas de trabajo para migrarlos de la cuenta de servicio predeterminada a sus cuentas dedicadas. A continuación, debe eliminar el permiso de administrador de la cuenta de servicio predeterminada. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Policy:Kubernetes/AnonymousAccessGranted

Se ha concedido un permiso de API al usuario **`system:anonymous`** en un clúster de Kubernetes.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que un usuario de su clúster de Kubernetes ha creado correctamente un `ClusterRoleBinding` o `RoleBinding` para enlazar al usuario `system:anonymous` a un rol. Esto permite el acceso no autenticado a las operaciones de la API permitidas por el rol. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` o grupo `system:unauthenticated` en su clúster y revocar el acceso anónimo innecesario. Para obtener más información, consulte Prácticas recomendadas de seguridad para Amazon EKS en la Guía del usuario de Amazon EKS. Si los permisos se han concedido de forma maliciosa, debe revocar el acceso del usuario que concedió los permisos y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Policy:Kubernetes/ExposedDashboard

El panel de un clúster de Kubernetes estaba expuesto a Internet

Gravedad predeterminada: media

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que el servicio de equilibrador de carga ha expuesto el panel de Kubernetes de su clúster a Internet. Un panel expuesto hace que la interfaz de administración del clúster sea accesible desde Internet y permite a los adversarios aprovechar cualquier brecha de autenticación y control de acceso que pueda existir.

Recomendaciones de corrección:

Debe asegurarse de que se apliquen una autenticación y una autorización sólidas en el panel de Kubernetes. También debe implementar un control de acceso a la red para restringir el acceso al panel desde direcciones IP específicas.

Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Policy:Kubernetes/KubeflowDashboardExposed

El panel de Kubeflow de un clúster de Kubernetes estaba expuesto a Internet

Gravedad predeterminada: media

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que el servicio de equilibrador de carga ha expuesto el panel de Kubeflow de su clúster a Internet. Un panel de Kubeflow expuesto hace que la interfaz de administración del entorno de Kubeflow sea accesible desde Internet y permite a los adversarios aprovechar cualquier brecha de autenticación y control de acceso que pueda existir.

Recomendaciones de corrección:

Debe asegurarse de que se apliquen una autenticación y una autorización sólidas en el panel de Kubeflow. También debe implementar un control de acceso a la red para restringir el acceso al panel desde direcciones IP específicas.

Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

PrivilegeEscalation:Kubernetes/PrivilegedContainer

Se ha lanzado un contenedor privilegiado con acceso a nivel raíz en su clúster de Kubernetes.

Gravedad predeterminada: media

- Característica: registros de auditoría de Kubernetes

Este resultado le informa de que se ha lanzado un contenedor privilegiado en su clúster de Kubernetes mediante una imagen que nunca antes se había utilizado para lanzar contenedores privilegiados en su clúster. Un contenedor privilegiado tiene acceso de nivel raíz al host. Los adversarios pueden lanzar contenedores privilegiados como una táctica de derivación de privilegios para acceder al host y, posteriormente, ponerlo en peligro.

Recomendaciones de corrección:

Si el lanzamiento de este contenedor es inesperado, es posible que las credenciales de identidad de usuario utilizadas para lanzarlo se hayan visto afectadas. Revoque el acceso del usuario y anule cualquier cambio que haya hecho un adversario en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

Se invocó de forma anómala una API de Kubernetes que se utiliza habitualmente para acceder a secretos.

Gravedad predeterminada: media

- Característica: registros de auditoría de Kubernetes

Este hallazgo indica que un usuario de Kubernetes de tu clúster ha invocado una operación de API anómala para recuperar secretos confidenciales del clúster. La API observada suele estar asociada a tácticas de acceso a las credenciales que pueden provocar una escalada de privilegios y un mayor acceso dentro del clúster. Si no se espera este comportamiento, puede indicar un error de configuración o que tus AWS credenciales están comprometidas.

El modelo de aprendizaje automático (ML) de detección de GuardDuty anomalías identificó la API observada como anómala. El modelo ML evalúa toda la actividad de las API de los usuarios dentro del clúster de EKS e identifica los eventos anómalos asociados a las técnicas utilizadas por usuarios no autorizados. El modelo de aprendizaje automático rastrea varios factores del funcionamiento de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el agente de usuario utilizado y el espacio de nombres que operó el usuario. Puedes encontrar los detalles de la solicitud de API que no son habituales en el panel de búsqueda de detalles de la GuardDuty consola.

Recomendaciones de corrección:

Examina los permisos concedidos al usuario de Kubernetes en tu clúster y asegúrate de que todos estos permisos son necesarios. Si los permisos se concedieron por error o de forma malintencionada, revoca el acceso del usuario y anula cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Si sus AWS credenciales están comprometidas, consulte. Corregir las credenciales potencialmente comprometidas AWS

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

Se creó RoleBinding o ClusterRoleBinding modificó un rol o un espacio de nombres confidencial demasiado permisivo en tu clúster de Kubernetes.

Gravedad predeterminada: media*

> **Note**
>
> La gravedad predeterminada de este resultado es media. Sin embargo, si una RoleBinding o ClusterRoleBinding incluye la tecla o, la ClusterRoles `admin` gravedad es alta. `cluster-admin`

- Característica: registros de auditoría de Kubernetes

Este hallazgo indica que un usuario de tu clúster de Kubernetes creó una `RoleBinding` o `ClusterRoleBinding` para vincular a un usuario a un rol con permisos de administrador o espacios de nombres confidenciales. Si no se espera este comportamiento, puede indicar un error de configuración o que tus credenciales están comprometidas. AWS

El modelo de aprendizaje automático (ML) de detección de GuardDuty anomalías identificó la API observada como anómala. El modelo ML evalúa toda la actividad de las API de los usuarios dentro del clúster de EKS. Este modelo de aprendizaje automático también identifica los eventos anómalos asociados a las técnicas utilizadas por un usuario no autorizado. El modelo de aprendizaje automático también rastrea varios factores del funcionamiento de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el agente de usuario utilizado y el espacio de nombres que utilizó el usuario. Puedes encontrar los detalles de la solicitud de API que no son habituales en el panel de búsqueda de detalles de la GuardDuty consola.

Recomendaciones de corrección:

Examina los permisos concedidos al usuario de Kubernetes. Estos permisos se definen en el rol y los sujetos involucrados en y. `RoleBinding` `ClusterRoleBinding` Si los permisos se concedieron

por error o de forma malintencionada, revoque el acceso de los usuarios y anule cualquier cambio realizado por un usuario no autorizado en su clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Si sus AWS credenciales están comprometidas, consulte. Corregir las credenciales potencialmente comprometidas AWS

Execution:Kubernetes/AnomalousBehavior.ExecInPod

Se ejecutó un comando dentro de un pod de forma anómala.

Gravedad predeterminada: media

- Característica: registros de auditoría de Kubernetes

Este hallazgo indica que se ejecutó un comando en un pod mediante la API exec de Kubernetes. La API exec de Kubernetes permite ejecutar comandos arbitrarios en un pod. Si este comportamiento no es el esperado para el usuario, el espacio de nombres o el pod, puede indicar un error de configuración o que tus credenciales están comprometidas. AWS

El modelo de aprendizaje automático (ML) con detección de GuardDuty anomalías identificó la API observada como anómala. El modelo ML evalúa toda la actividad de las API de los usuarios dentro del clúster de EKS. Este modelo de aprendizaje automático también identifica los eventos anómalos asociados a las técnicas utilizadas por un usuario no autorizado. El modelo de aprendizaje automático también rastrea varios factores del funcionamiento de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el agente de usuario utilizado y el espacio de nombres que utilizó el usuario. Puedes encontrar los detalles de la solicitud de API que no son habituales en el panel de búsqueda de detalles de la GuardDuty consola.

Recomendaciones de corrección:

Si la ejecución de este comando es inesperada, es posible que las credenciales de la identidad de usuario utilizada para ejecutar el comando estén comprometidas. Revoca el acceso de los usuarios y anula cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Si sus AWS credenciales están comprometidas, consulteCorregir las credenciales potencialmente comprometidas AWS.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

Se lanzó una carga de trabajo con un contenedor privilegiado de forma anómala.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este hallazgo le informa de que se lanzó una carga de trabajo con un contenedor privilegiado en su clúster de Amazon EKS. Un contenedor privilegiado tiene acceso de nivel raíz al host. Los usuarios no autorizados pueden lanzar contenedores privilegiados como una táctica de escalada de privilegios para obtener primero acceso al host y, después, ponerlo en peligro.

El modelo de aprendizaje automático (ML) con detección de GuardDuty anomalías identificó la creación o modificación del contenedor observada como anómala. El modelo ML evalúa toda la actividad de la API del usuario y de las imágenes del contenedor dentro del clúster de EKS. Este modelo de aprendizaje automático también identifica los eventos anómalos asociados a las técnicas utilizadas por un usuario no autorizado. El modelo de aprendizaje automático también rastrea varios factores del funcionamiento de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el agente de usuario utilizado, las imágenes del contenedor observadas en la cuenta y el espacio de nombres que utilizó el usuario. Puedes encontrar los detalles de la solicitud de API que no sean habituales en el panel de detalles de búsqueda de la GuardDuty consola.

Recomendaciones de corrección:

Si el lanzamiento de este contenedor es inesperado, es posible que las credenciales de la identidad de usuario utilizada para lanzar el contenedor estén comprometidas. Revoca el acceso de los usuarios y anula cualquier cambio realizado por un usuario no autorizado en tu clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Si sus AWS credenciales están comprometidas, consulteCorregir las credenciales potencialmente comprometidas AWS.

Si se espera el lanzamiento de este contenedor, se recomienda utilizar una regla de supresión con un criterio de filtrado basado en el

`resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` campo. En los criterios de filtro, el `imagePrefix` campo debe tener el mismo valor que el `imagePrefix` campo especificado en la búsqueda. Para obtener más información, consulte Reglas de supresión.

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed! ContainerWithSensitiveMount

Se desplegó una carga de trabajo de forma anómala, con una ruta de host confidencial integrada en la carga de trabajo.

Gravedad predeterminada: alta

- Característica: registros de auditoría de Kubernetes

Este hallazgo indica que se lanzó una carga de trabajo con un contenedor que incluía una ruta de host confidencial en la `volumeMounts` sección. Esto podría hacer que la ruta confidencial del host fuera accesible y grabable desde el interior del contenedor. Los usuarios no autorizados suelen utilizar esta técnica para acceder al sistema de archivos del host.

El modelo de aprendizaje automático (ML) de detección de GuardDuty anomalías identificó la creación o modificación del contenedor observada como anómala. El modelo ML evalúa toda la actividad de la API del usuario y de las imágenes del contenedor dentro del clúster de EKS. Este modelo de aprendizaje automático también identifica los eventos anómalos asociados a las técnicas utilizadas por un usuario no autorizado. El modelo de aprendizaje automático también rastrea varios factores del funcionamiento de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el agente de usuario utilizado, las imágenes del contenedor observadas en la cuenta y el espacio de nombres que utilizó el usuario. Puedes encontrar los detalles de la solicitud de API que no sean habituales en el panel de detalles de búsqueda de la GuardDuty consola.

Recomendaciones de corrección:

Si el lanzamiento de este contenedor es inesperado, es posible que las credenciales de la identidad de usuario utilizada para lanzar el contenedor estén comprometidas. Revoca el acceso de los usuarios y anula cualquier cambio realizado por un usuario no autorizado en tu clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Si sus AWS credenciales están comprometidas, consulteCorregir las credenciales potencialmente comprometidas AWS.

Si se espera el lanzamiento de este contenedor, se recomienda utilizar una regla de supresión con un criterio de filtrado basado en el `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` campo. En los criterios de filtro, el `imagePrefix` campo debe tener el mismo valor que el `imagePrefix` campo especificado en la búsqueda. Para obtener más información, consulte Reglas de supresión.

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Se lanzó una carga de trabajo de forma anómala.

Gravedad predeterminada: baja*

> **Note**
>
> La gravedad predeterminada es Baja. Sin embargo, si la carga de trabajo contiene un nombre de imagen potencialmente sospechoso, como una herramienta de prueba conocida, o un contenedor que ejecuta un comando potencialmente sospechoso en el momento del lanzamiento, como los comandos reverse shell, la gravedad de este tipo de hallazgo se considerará media.

- Característica: registros de auditoría de Kubernetes

Este hallazgo le informa de que una carga de trabajo de Kubernetes se creó o modificó de forma anómala, como una actividad de API, nuevas imágenes de contenedores o una configuración de carga de trabajo riesgosa, dentro de su clúster de Amazon EKS. Los usuarios no autorizados pueden lanzar contenedores como táctica para ejecutar código arbitrario con el fin de acceder primero al host y, después, ponerlo en peligro.

El modelo de aprendizaje automático (ML) con detección de GuardDuty anomalías identificó la creación o modificación del contenedor observada como anómala. El modelo ML evalúa toda la actividad de la API del usuario y de las imágenes del contenedor dentro del clúster de EKS. Este modelo de aprendizaje automático también identifica los eventos anómalos asociados a las técnicas

utilizadas por un usuario no autorizado. El modelo de aprendizaje automático también rastrea varios factores del funcionamiento de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el agente de usuario utilizado, las imágenes del contenedor observadas en la cuenta y el espacio de nombres que utilizó el usuario. Puedes encontrar los detalles de la solicitud de API que no sean habituales en el panel de detalles de búsqueda de la GuardDuty consola.

Recomendaciones de corrección:

Si el lanzamiento de este contenedor es inesperado, es posible que las credenciales de la identidad de usuario utilizada para lanzar el contenedor estén comprometidas. Revoca el acceso de los usuarios y anula cualquier cambio realizado por un usuario no autorizado en tu clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Si sus AWS credenciales están comprometidas, consulteCorregir las credenciales potencialmente comprometidas AWS.

Si se espera el lanzamiento de este contenedor, se recomienda utilizar una regla de supresión con un criterio de filtrado basado en el `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` campo. En los criterios de filtro, el `imagePrefix` campo debe tener el mismo valor que el `imagePrefix` campo especificado en la búsqueda. Para obtener más información, consulte Reglas de supresión.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Un rol muy permisivo o que ClusterRole se creó o modificó de forma anómala.

Gravedad predeterminada: baja

- Característica: registros de auditoría de Kubernetes

Este hallazgo le informa de que un usuario de Kubernetes en su clúster de Amazon EKS ejecutó una operación de API anómala para crear un `Role` o `ClusterRole` con permisos excesivos. Los actores pueden utilizar la creación de roles con permisos potentes para evitar el uso de roles integrados similares a los de los administradores y evitar ser detectados. El exceso de permisos puede provocar una escalada de privilegios, la ejecución remota de código y, potencialmente, el control de un espacio de nombres o un clúster. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales están comprometidas.

El modelo de aprendizaje automático (ML) de detección de GuardDuty anomalías identificó la API observada como anómala. El modelo ML evalúa toda la actividad de las API de los usuarios en su clúster de Amazon EKS e identifica los eventos anómalos asociados a las técnicas utilizadas por los usuarios no autorizados. El modelo de aprendizaje automático también rastrea varios factores del funcionamiento de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el agente de usuario utilizado, las imágenes del contenedor observadas en su cuenta y el espacio de nombres que utilizó el usuario. Puedes encontrar los detalles de la solicitud de API que no sean habituales en el panel de detalles de búsqueda de la GuardDuty consola.

Recomendaciones de corrección:

Examine los permisos definidos en `Role` o `ClusterRole` para asegurarse de que todos los permisos son necesarios y siga los principios de privilegios mínimos. Si los permisos se concedieron por error o de forma malintencionada, revoque el acceso de los usuarios y anule cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Si sus AWS credenciales están comprometidas, consulte. Corregir las credenciales potencialmente comprometidas AWS

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Un usuario comprobó su permiso de acceso de forma anómala.

Gravedad predeterminada: baja

- Característica: registros de auditoría de Kubernetes

Este hallazgo le informa de que un usuario de su clúster de Kubernetes ha comprobado correctamente si están permitidos o no los potentes permisos conocidos que pueden llevar a la escalada de privilegios y a la ejecución remota de código. Por ejemplo, un comando común que se utiliza para comprobar los permisos de un usuario es. `kubectl auth can-i` Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto comprometidas.

El modelo de aprendizaje automático (ML) con detección de GuardDuty anomalías identificó la API observada como anómala. El modelo ML evalúa toda la actividad de las API de los usuarios en su clúster de Amazon EKS e identifica los eventos anómalos asociados a las técnicas utilizadas por

los usuarios no autorizados. El modelo de aprendizaje automático también rastrea varios factores del funcionamiento de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, la verificación de los permisos y el espacio de nombres que utilizó el usuario. Puedes encontrar los detalles de la solicitud de API que no son habituales en el panel de búsqueda de detalles de la GuardDuty consola.

Recomendaciones de corrección:

Examina los permisos concedidos al usuario de Kubernetes para asegurarte de que todos los permisos son necesarios. Si los permisos se concedieron por error o de forma malintencionada, revoca el acceso del usuario y anula cualquier cambio realizado por un usuario no autorizado en tu clúster. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Si sus AWS credenciales están comprometidas, consulte. Corregir las credenciales potencialmente comprometidas AWS

Tipos de búsqueda de Lambda Protection

En esta sección se describen los tipos de búsqueda que son específicos de sus AWS Lambda recursos y que figuran como. `resourceType` `Lambda` Para conocer todos los resultados de Lambda, le recomendamos que examine el recurso en cuestión y determine si se comporta de la manera esperada. Si la actividad está autorizada, puede utilizar las reglas de supresión o las listas de amenazas e IP confiables para evitar las notificaciones de falsos positivos para ese recurso.

Si la actividad es inesperada, la mejor práctica de seguridad consiste en suponer que Lambda está potencialmente comprometida y seguir las recomendaciones de corrección.

Temas

- Backdoor:Lambda/C&CActivity.B
- CryptoCurrency:Lambda/BitcoinTool.B
- Trojan:Lambda/BlackholeTraffic
- Trojan:Lambda/DropPoint
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- UnauthorizedAccess:Lambda/TorClient
- UnauthorizedAccess:Lambda/TorRelay

Backdoor:Lambda/C&CActivity.B

Una función Lambda consulta una dirección IP asociada a un servidor de comando y control conocido.

Gravedad predeterminada: alta

- Funcionalidad: Supervisión de la actividad de la red Lambda

Este resultado le informa de que hay una instancia EC2 en el entorno de AWS que está consultando a un nombre de dominio asociado con un servidor de comando y control (C&C) conocido. La función Lambda asociada al hallazgo generado está potencialmente comprometida. Los servidores C&C son equipos que envían comandos a los miembros de un botnet.

Un botnet es una colección de dispositivos conectados a Internet (que pueden incluir PC, servidores, dispositivos móviles y dispositivos de Internet de las cosas) que están infectados y controlados por un tipo común de malware. A menudo, los botnets se utilizan para distribuir malware y recopilar información obtenida de forma indebida, como números de tarjetas de crédito. Dependiendo de la finalidad y la estructura del botnet, el servidor C&C también puede enviar comandos para comenzar un ataque de denegación de servicio distribuido (DDoS).

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir una función Lambda potencialmente comprometida.

CryptoCurrency:Lambda/BitcoinTool.B

Una instancia EC2 consulta una dirección IP asociada con una actividad relacionada con una criptomoneda.

Gravedad predeterminada: alta

- Funcionalidad: Supervisión de la actividad de la red Lambda

Este resultado le informa de que hay una instancia EC2 en el entorno de AWS que está consultando a una dirección IP que está asociada con actividad relacionada con bitcoin u otra criptomoneda. Los

actores de amenazas pueden intentar tomar el control de las funciones de Lambda para reutilizarlas maliciosamente para la minería no autorizada de criptomonedas.

Recomendaciones de corrección:

Si utiliza esta función Lambda para extraer o administrar criptomonedas, o si esta función está involucrada de algún otro modo en una actividad de cadena de bloques, es posible que se trate de una actividad esperada para su entorno. Si este es el caso en su entorno, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de . El segundo criterio de filtro debe ser el nombre de la función Lambda de la función implicada en la actividad de la cadena de bloques. Para obtener información sobre la creación de reglas de supresión, consulte Reglas de supresión.

Si esta actividad es inesperada, la función Lambda podría estar comprometida. Para obtener más información, consulte Corregir una función Lambda potencialmente comprometida.

Trojan:Lambda/BlackholeTraffic

Una instancia EC2 está intentando comunicarse con una dirección IP de un host remoto que es una dirección IP de agujero negro conocida.

Gravedad predeterminada: media

- Funcionalidad: Supervisión de la actividad de la red Lambda

Este hallazgo indica que una función Lambda incluida en la lista de su AWS entorno está intentando comunicarse con la dirección IP de un agujero negro (o sumidero). Los agujeros negros hacen referencia a lugares de la red donde el tráfico entrante o saliente se descarta silenciosamente sin informar al origen de que los datos no llegaron a su destinatario. Una dirección IP de agujero negro especifica una máquina host que no se está ejecutando o una dirección a la que no se le ha asignado ningún host. La función Lambda indicada está potencialmente comprometida.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir una función Lambda potencialmente comprometida.

Trojan:Lambda/DropPoint

Una instancia EC2 está intentando comunicarse con una dirección IP de un host remoto que se sabe que mantiene credenciales y otros datos robados capturados por malware.

Gravedad predeterminada: media

- Funcionalidad: Supervisión de la actividad de la red Lambda

Este resultado le informa de que una instancia EC2 de su entorno de AWS está intentando comunicarse con una dirección IP de un host remoto que se sabe que mantiene credenciales y otros datos robados capturados por malware.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir una función Lambda potencialmente comprometida.

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Una función Lambda realiza conexiones a una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: media

- Funcionalidad: Supervisión de la actividad de la red Lambda

Este resultado le informa de que una instancia EC2 del entorno de AWS está estableciendo comunicaciones salientes con una dirección IP incluida en una lista de amenazas que ha cargado. En , una lista de amenazas está formada por direcciones IP malintencionadas conocidas. genera resultados basados en las listas de amenazas cargadas. Puede ver los detalles de la lista de amenazas en los detalles de búsqueda de la consola GuardDuty.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir una función Lambda potencialmente comprometida.

UnauthorizedAccess:Lambda/TorClient

La instancia de EC2 está estableciendo conexiones con un guardia Tor o un nodo Authority.

Gravedad predeterminada: alta

- Funcionalidad: Supervisión de la actividad de la red Lambda

Este resultado le informa de que una instancia de EC2 del entorno de AWS está estableciendo conexiones con un guardia Tor o un nodo Authority. Tor es un software que permite las comunicaciones anónimas. Los guardias Tor y los nodos Authority actúan como gateways a una red Tor. Este tráfico puede indicar que esta función Lambda está potencialmente comprometida. Ahora actúa como cliente en una red Tor.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir una función Lambda potencialmente comprometida.

UnauthorizedAccess:Lambda/TorRelay

La instancia de EC2 está estableciendo conexiones a una red Tor como repetidor Tor.

Gravedad predeterminada: alta

- Funcionalidad: Supervisión de la actividad de la red Lambda

Este resultado le informa de que una instancia de EC2 de su entorno de AWS está estableciendo conexiones con una red Tor de una forma que sugiere que actúa como un repetidor Tor. Tor es un software que permite las comunicaciones anónimas. Los repetidores Tor aumentan el anonimato en la comunicación, ya que reenvía el tráfico potencialmente ilícito del cliente de un repetidor Tor a otro.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir una función Lambda potencialmente comprometida.

Tipos de búsqueda de protección contra malware

La protección contra malware GuardDuty proporciona una única detección de protección contra malware para todas las amenazas detectadas durante el escaneo de una instancia EC2 o una carga de trabajo de contenedor. El resultado incluye el número total de detecciones realizadas durante el análisis y, en función de la gravedad, proporciona detalles sobre las 32 amenazas principales que detecta. A diferencia de otros hallazgos de GuardDuty, los hallazgos de Malware Protection no se actualizan cuando se vuelve a escanear la misma instancia de EC2 o carga de trabajo del contenedor.

Se genera un nuevo resultado de protección contra malware por cada análisis que detecta malware. Los resultados de Malware Protection incluyen información sobre el análisis correspondiente que produjo el hallazgo, así como el hallazgo de GuardDuty que inició este análisis. Esto facilita la correlación del comportamiento sospechoso con el malware detectado.

> **Note**
>
> Cuando GuardDuty detecta actividad maliciosa en la carga de trabajo de un contenedor, Malware Protection no genera una detección de nivel EC2.

Los siguientes hallazgos son específicos de GuardDuty Malware Protection.

Temas

Execution:EC2/MaliciousFile

Se ha detectado un archivo malicioso en una instancia de EC2.

Gravedad predeterminada: varía en función de la amenaza detectada.

Este hallazgo indica que el análisis de GuardDuty Malware Protection ha detectado uno o más archivos maliciosos en la instancia de EC2 de la lista en su entorno. AWS Esta instancia EC2 podría estar comprometida. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada, puede que su instancia de EC2 esté comprometida. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Execution:ECS/MaliciousFile

Se ha detectado un archivo malicioso en un clúster de ECS.

Gravedad predeterminada: varía en función de la amenaza detectada.

Este hallazgo indica que el análisis de GuardDuty Malware Protection ha detectado uno o más archivos maliciosos en una carga de trabajo de contenedor que pertenece a un clúster de ECS. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada, el contenedor que pertenece al clúster de ECS podría estar en peligro. Para obtener más información, consulte Cómo corregir un clúster de ECS potencialmente comprometido.

Execution:Kubernetes/MaliciousFile

Se ha detectado un archivo malicioso en un clúster de Kubernetes.

Gravedad predeterminada: varía en función de la amenaza detectada.

Este hallazgo indica que el análisis de GuardDuty Malware Protection ha detectado uno o más archivos maliciosos en una carga de trabajo de contenedor que pertenece a un clúster de Kubernetes. Si se trata de un clúster gestionado por EKS, los detalles de los resultados proporcionarán información adicional sobre el recurso de EKS afectado. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los hallazgos.

Recomendaciones de corrección:

Si esta actividad es inesperada, la carga de trabajo de su contenedor podría verse comprometida. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Execution:Container/MaliciousFile

Se ha detectado un archivo malicioso en un contenedor independiente.

Gravedad predeterminada: varía en función de la amenaza detectada.

Este hallazgo indica que el análisis de GuardDuty Malware Protection ha detectado uno o más archivos maliciosos en una carga de trabajo de contenedor y no se ha identificado información sobre el clúster. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada, la carga de trabajo de su contenedor podría verse comprometida. Para obtener más información, consulte Corregir un contenedor independiente potencialmente comprometido.

Execution:EC2/SuspiciousFile

Se ha detectado un archivo sospechoso en una instancia EC2.

Gravedad predeterminada: varía en función de la amenaza detectada.

Este hallazgo indica que el análisis de GuardDuty Malware Protection ha detectado uno o más archivos sospechosos en una instancia EC2. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

`SuspiciousFile`las detecciones de tipos indican la presencia de programas potencialmente no deseados, como adware, spyware o herramientas de doble uso, en un recurso afectado. Estos programas podrían tener un impacto negativo en sus recursos o ser utilizados por los atacantes con fines malintencionados. Por ejemplo, los adversarios pueden utilizar las herramientas de red de forma legítima o malintencionada como herramientas de hackeo para intentar comprometer los recursos.

Cuando se detecte un archivo sospechoso, evalúe si espera verlo en su entorno. AWS Si el archivo es inesperado, siga las recomendaciones de corrección que se indican en la siguiente sección.

Recomendaciones de corrección:

Si esta actividad es inesperada, puede que su instancia de EC2 esté comprometida. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Execution:ECS/SuspiciousFile

Se ha detectado un archivo sospechoso en un clúster de ECS.

Gravedad predeterminada: varía en función de la amenaza detectada.

Este hallazgo indica que el análisis de GuardDuty Malware Protection ha detectado uno o más archivos sospechosos en un contenedor que pertenece a un clúster de ECS. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

`SuspiciousFile`las detecciones de tipos indican la presencia de programas potencialmente no deseados, como adware, spyware o herramientas de doble uso, en un recurso afectado. Estos programas podrían tener un impacto negativo en sus recursos o ser utilizados por los atacantes con fines malintencionados. Por ejemplo, los adversarios pueden utilizar las herramientas de red de forma legítima o malintencionada como herramientas de hackeo para intentar comprometer los recursos.

Cuando se detecte un archivo sospechoso, evalúe si espera verlo en su entorno. AWS Si el archivo es inesperado, siga las recomendaciones de corrección que se indican en la siguiente sección.

Recomendaciones de corrección:

Si esta actividad es inesperada, el contenedor que pertenece al clúster de ECS podría estar en peligro. Para obtener más información, consulte Cómo corregir un clúster de ECS potencialmente comprometido.

Execution:Kubernetes/SuspiciousFile

Se ha detectado un archivo sospechoso en un clúster de Kubernetes.

Gravedad predeterminada: varía en función de la amenaza detectada.

Este hallazgo indica que el análisis de GuardDuty Malware Protection ha detectado uno o más archivos sospechosos en un contenedor que pertenece a un clúster de Kubernetes. Si se trata de un clúster gestionado por EKS, los detalles de los resultados proporcionarán información adicional sobre el EKS afectado. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los hallazgos.

`SuspiciousFile`las detecciones de tipos indican la presencia de programas potencialmente no deseados, como adware, spyware o herramientas de doble uso, en un recurso afectado. Estos programas podrían tener un impacto negativo en sus recursos o ser utilizados por los atacantes con fines malintencionados. Por ejemplo, los adversarios pueden utilizar las herramientas de red de forma legítima o malintencionada como herramientas de hackeo para intentar comprometer los recursos.

Cuando se detecte un archivo sospechoso, evalúe si espera verlo en su entorno. AWS Si el archivo es inesperado, siga las recomendaciones de corrección que se indican en la siguiente sección.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la carga de trabajo del contenedor se vea comprometida. Para obtener más información, consulte Corrección de los resultados de la supervisión de registros de auditoría de EKS.

Execution:Container/SuspiciousFile

Se ha detectado un archivo sospechoso en un contenedor independiente.

Gravedad predeterminada: varía en función de la amenaza detectada.

Este hallazgo indica que el análisis de GuardDuty Malware Protection ha detectado uno o más archivos sospechosos en un contenedor sin información de clúster. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

`SuspiciousFile`las detecciones de tipos indican la presencia de programas potencialmente no deseados, como adware, spyware o herramientas de doble uso, en un recurso afectado. Estos programas podrían tener un impacto negativo en sus recursos o ser utilizados por los atacantes con fines malintencionados. Por ejemplo, los adversarios pueden utilizar las herramientas de red de forma legítima o malintencionada como herramientas de hackeo para intentar comprometer los recursos.

Cuando se detecte un archivo sospechoso, evalúe si espera verlo en su entorno. AWS Si el archivo es inesperado, siga las recomendaciones de corrección que se indican en la siguiente sección.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la carga de trabajo del contenedor se vea comprometida. Para obtener más información, consulte Corregir un contenedor independiente potencialmente comprometido.

Tipos de búsqueda GuardDuty RDS Protection

La protección GuardDuty RDS detecta un comportamiento de inicio de sesión anómalo en la instancia de la base de datos. Los siguientes resultados son específicos de los recursos del bucket de S3 y siempre tendrán un Tipo de recurso de . La gravedad y los detalles de los resultados variarán en función del tipo de resultado.

Temas

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Un usuario ha iniciado sesión correctamente en una base de datos de RDS de su cuenta de forma anómala.

Gravedad predeterminada: variable

> **Note**
>
> Según el comportamiento anómalo asociado a este hallazgo, la gravedad predeterminada puede ser baja, media y alta.
>
> - Bajo: si el nombre de usuario asociado a esta búsqueda inició sesión desde una dirección IP asociada a una red privada.
> - Medio: si el nombre de usuario asociado a esta búsqueda inició sesión desde una dirección IP pública.

- Alto: si hay un patrón constante de intentos fallidos de inicio de sesión desde direcciones IP públicas, lo que indica que las políticas de acceso son demasiado permisivas.

- Característica: monitoreo de la actividad de inicio de sesión con RDS

Este hallazgo le informa de que se ha observado un inicio de sesión correcto y anómalo en una base de datos de RDS de su entorno. AWS Esto puede indicar que un usuario anterior invisible inició sesión en una base de datos de RDS por primera vez. Un escenario común es el de un usuario interno que inicia sesión en una base de datos a la que acceden mediante programación las aplicaciones y no los usuarios individuales.

El modelo de aprendizaje automático (ML) de detección de anomalías (ML) de GuardDuty identificó este inicio de sesión exitoso como anómalo. El modelo ML evalúa todos los eventos de inicio de sesión en la base de datos Bases de datos compatibles de Amazon Aurora e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo ML rastrea varios factores de la actividad de inicio de sesión en el RDS, como el usuario que realizó la solicitud, la ubicación desde la que se realizó la solicitud y los detalles específicos de conexión a la base de datos que se utilizaron. Para obtener información sobre los eventos de inicio de sesión que son potencialmente inusuales, consulteAnomalías basadas en la actividad de inicio de sesión en RDS.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, se recomienda cambiar la contraseña del usuario de la base de datos asociada y revisar los registros de auditoría disponibles para ver si hay actividad realizada por el usuario anómalo. Los resultados de gravedad media y alta pueden indicar que existe una política de acceso demasiado permisiva a la base de datos y que las credenciales de los usuarios pueden haber quedado expuestas o comprometidas. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde las fuentes necesarias. Para obtener más información, consulte Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos.

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Se observaron uno o más intentos de inicio de sesión fallidos poco habituales en una base de datos de RDS de su cuenta.

Gravedad predeterminada: baja

- Característica: monitoreo de la actividad de inicio de sesión en RDS

Este hallazgo le informa de que se observaron uno o más errores de inicio de sesión anómalos en una base de datos de RDS de su entorno. AWS Un intento fallido de inicio de sesión desde direcciones IP públicas puede indicar que la base de datos de RDS de su cuenta ha sido objeto de un intento de ataque de fuerza bruta por parte de un agente potencialmente malintencionado.

El modelo de aprendizaje automático (ML) de detección de anomalías de GuardDuty identificó estos inicios de sesión fallidos como anómalos. El modelo ML evalúa todos los eventos de inicio de sesión en la base de datos Bases de datos compatibles de Amazon Aurora e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo ML rastrea varios factores de la actividad de inicio de sesión en el RDS, como el usuario que realizó la solicitud, la ubicación desde la que se realizó la solicitud y los detalles específicos de conexión a la base de datos que se utilizaron. Para obtener información sobre la actividad de inicio de sesión en RDS que puede ser inusual, consulte. Anomalías basadas en la actividad de inicio de sesión en RDS

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, puede indicar que la base de datos está expuesta públicamente o que existe una política de acceso demasiado permisiva a la base de datos. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde las fuentes necesarias. Para obtener más información, consulte Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos.

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Un usuario ha iniciado sesión correctamente en una base de datos de RDS de su cuenta desde una dirección IP pública de forma anómala tras un patrón constante de intentos de inicio de sesión fallidos e inusuales.

Gravedad predeterminada: alta

- Característica: monitorización de la actividad de inicio de sesión en RDS

Este hallazgo le informa de que se ha observado un inicio de sesión anómalo, indicativo de una fuerza bruta exitosa, en una base de datos de RDS de su entorno. AWS Antes de iniciar sesión correctamente de forma anómala, se observaba un patrón constante de intentos de inicio de sesión fallidos inusuales. Esto indica que es posible que el usuario y la contraseña asociados a la base de datos de RDS de su cuenta estén comprometidos y que una persona potencialmente malintencionada haya accedido a la base de datos de RDS.

El modelo de aprendizaje automático (ML) de detección de anomalías (ML) de GuardDuty identificó este inicio de sesión exitoso por fuerza bruta como anómalo. El modelo ML evalúa todos los eventos de inicio de sesión en la base de datos Bases de datos compatibles de Amazon Aurora e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo ML rastrea varios factores de la actividad de inicio de sesión en el RDS, como el usuario que realizó la solicitud, la ubicación desde la que se realizó la solicitud y los detalles específicos de conexión a la base de datos que se utilizaron. Para obtener información sobre la actividad de inicio de sesión en RDS que puede ser inusual, consulte. Anomalías basadas en la actividad de inicio de sesión en RDS

Recomendaciones de corrección:

Esta actividad indica que las credenciales de la base de datos pueden estar expuestas o comprometidas. Se recomienda cambiar la contraseña del usuario de la base de datos asociado y revisar los registros de auditoría disponibles para ver la actividad realizada por el usuario potencialmente comprometido. Un patrón constante de intentos inusuales de inicio de sesión fallidos indica una política de acceso demasiado permisiva a la base de datos o que la base de datos también puede haber estado expuesta al público. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde las fuentes necesarias. Para obtener más información, consulte Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos.

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Un usuario ha iniciado sesión correctamente en una base de datos de RDS de su cuenta desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Característica: monitoreo de la actividad de inicio de sesión en RDS

Este hallazgo le informa de que se ha producido una actividad de inicio de sesión correcta en el RDS desde una dirección IP asociada a una actividad maliciosa conocida en su AWS entorno. Esto indica que es posible que el usuario y la contraseña asociados a la base de datos de RDS de su cuenta estén comprometidos y que una persona potencialmente malintencionada haya accedido a la base de datos de RDS.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, puede indicar que las credenciales del usuario pueden estar expuestas o comprometidas. Se recomienda cambiar la contraseña del usuario de la base de datos asociado y revisar los registros de auditoría disponibles para ver si hay actividad realizada por el usuario comprometido. Esta actividad también puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde las fuentes necesarias. Para obtener más información, consulte Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos.

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Una dirección IP asociada a una actividad maliciosa conocida intentó iniciar sesión sin éxito en una base de datos de RDS de su cuenta.

Gravedad predeterminada: media

- Característica: monitorización de la actividad de inicio de sesión en RDS

Este hallazgo le informa de que una dirección IP asociada a una actividad maliciosa conocida intentó iniciar sesión en una base de datos de RDS de su AWS entorno, pero no proporcionó el nombre de usuario o la contraseña correctos. Esto indica que un agente potencialmente malintencionado podría estar intentando comprometer la base de datos de RDS de su cuenta.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde las fuentes necesarias. Para obtener más información, consulte Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos.

Discovery:RDS/MaliciousIPCaller

Una dirección IP asociada a una actividad maliciosa conocida ha explorado una base de datos de RDS de su cuenta; no se ha realizado ningún intento de autenticación.

Gravedad predeterminada: media

- Característica: monitoreo de la actividad de inicio de sesión en RDS

Este hallazgo le informa de que una dirección IP asociada a una actividad maliciosa conocida ha explorado una base de datos de RDS de su AWS entorno, aunque no se ha realizado ningún intento de inicio de sesión. Esto puede indicar que un agente potencialmente malintencionado está intentando buscar una infraestructura de acceso público.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde las fuentes necesarias. Para obtener más información, consulte Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos.

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Un usuario ha iniciado sesión correctamente en una base de datos de RDS de tu cuenta desde una dirección IP del nodo de salida de Tor.

Gravedad predeterminada: alta

- Característica: monitoreo de la actividad de inicio de sesión en RDS

Este hallazgo le informa de que un usuario ha iniciado sesión correctamente en una base de datos de RDS de su AWS entorno desde una dirección IP de un nodo de salida de Tor. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, puede indicar que las credenciales del usuario pueden haber quedado expuestas o comprometidas. Se recomienda cambiar la contraseña del usuario de la base de datos asociado y revisar los registros de auditoría disponibles para ver si hay actividad realizada por el usuario comprometido. Esta actividad también puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde las fuentes necesarias. Para obtener más información, consulte Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos.

CredentialAccess:RDS/TorIPCaller.FailedLogin

Una dirección IP de Tor intentó iniciar sesión sin éxito en una base de datos de RDS de tu cuenta.

Gravedad predeterminada: media

- Característica: monitoreo de la actividad de inicio de sesión en RDS

Este hallazgo le informa de que una dirección IP del nodo de salida de Tor intentó iniciar sesión en una base de datos de RDS de su AWS entorno, pero no proporcionó el nombre de usuario o la contraseña correctos. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde las fuentes necesarias. Para obtener más información, consulte Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos.

Discovery:RDS/TorIPCaller

Una dirección IP del nodo de salida de Tor ha explorado una base de datos de RDS de tu cuenta, pero no se ha realizado ningún intento de autenticación.

Gravedad predeterminada: media

- Característica: monitoreo de la actividad de inicio de sesión en RDS

Este hallazgo indica que una dirección IP del nodo de salida de Tor ha explorado una base de datos de RDS de su AWS entorno, aunque no se ha realizado ningún intento de inicio de sesión. Esto puede indicar que un agente potencialmente malintencionado está intentando buscar una infraestructura de acceso público. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde las fuentes necesarias. Para obtener más información, consulte Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos.

Tipos de búsqueda de Runtime Monitoring

Amazon GuardDuty genera los siguientes resultados de Runtime Monitoring para indicar posibles amenazas en función del comportamiento a nivel del sistema operativo de los hosts y contenedores

de Amazon EC2 en sus clústeres de Amazon EKS, las cargas de trabajo de Fargate y Amazon ECS y las instancias de Amazon EC2.

> **Note**
>
> Los tipos de resultados de la Supervisión en tiempo de ejecución se obtienen según los registros de tiempo de ejecución recopilados de los hosts. Los registros contienen campos, como las rutas de los archivos, que puede controlar un agente malicioso. Estos campos también se incluyen en los resultados para proporcionar un contexto de tiempo de ejecución GuardDuty . Al procesar los resultados de Runtime Monitoring fuera de la GuardDuty consola, debe desinfectar los campos de búsqueda. Por ejemplo, puede codificar en HTML los campos de resultado cuando los muestre en una página web.

Temas

- CryptoCurrency:Runtime/BitcoinTool.B
- Backdoor:Runtime/C&CActivity.B
- UnauthorizedAccess:Runtime/TorRelay
- UnauthorizedAccess:Runtime/TorClient
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/DropPoint
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Backdoor:Runtime/C&CActivity.B!DNS
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation

- UnauthorizedAccess:Runtime/MetadataDNSRebind
- Execution:Runtime/NewBinaryExecuted
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- DefenseEvasion:Runtime/ProcessInjection.Proc
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- DefenseEvasion:Runtime/FilelessExecution
- Impact:Runtime/CryptoMinerExecuted
- Execution:Runtime/NewLibraryLoaded
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Execution:Runtime/SuspiciousTool
- Execution:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/PtraceAntiDebugging
- Execution:Runtime/MaliciousFileExecuted

CryptoCurrency:Runtime/BitcoinTool.B

Una instancia o un contenedor de Amazon EC2 está consultando una dirección IP asociada con una actividad relacionada con una criptomoneda.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS está consultando una dirección IP que está asociada con una actividad relacionada

con criptomonedas. Los actores de las amenazas pueden intentar tomar el control de recursos de computación para reutilizarlos maliciosamente para la extracción no autorizada de criptomonedas.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si utiliza esta instancia o un contenedor de EC2 para extraer o administrar criptomonedas, o si cualquiera de estos está involucrado de otra manera en la actividad de cadena de bloques, el resultado CryptoCurrency:Runtime/BitcoinTool.B podría representar la actividad esperada para su entorno. Si este es el caso de su AWS entorno, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtro. El primer criterio de filtro debe utilizar el atributo Tipo de resultado con un valor de `CryptoCurrency:Runtime/BitcoinTool.B`. El segundo criterio de filtro debe ser el ID de instancia de la instancia o el ID de imagen de contenedor del contenedor implicado en una actividad relacionada con las criptomonedas o las cadenas de bloques. Para obtener más información, consulte Reglas de supresión.

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Backdoor:Runtime/C&CActivity.B

Una instancia o un contenedor de Amazon EC2 está consultando una IP que está asociada a un servidor de comando y control conocido.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que la instancia o el contenedor de EC2 que aparece en la lista dentro del entorno de AWS está consultando una IP asociada con un servidor de comando y control (C&C) conocido. La instancia o el contenedor que aparecen en la lista podrían estar potencialmente afectados. Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet.

Un botnet es una colección de dispositivos conectados a Internet (que pueden incluir PC, servidores, dispositivos móviles y dispositivos de Internet de las cosas) que están infectados y controlados por un tipo común de malware. A menudo, los botnets se utilizan para distribuir malware y recopilar información obtenida de forma indebida, como números de tarjetas de crédito. Dependiendo de la finalidad y la estructura del botnet, el servidor C&C también puede enviar comandos para comenzar un ataque de denegación de servicio distribuido (DDoS).

> **Note**
>
> Si la IP consultada está relacionada con log4j, los campos del resultado asociado incluirán los siguientes valores:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulte el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

UnauthorizedAccess:Runtime/TorRelay

La instancia o contenedor de Amazon EC2 está estableciendo conexiones a una red de Tor como relé de Tor.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este hallazgo indica que una instancia EC2 o un contenedor de tu AWS entorno se conecta a una red Tor de una manera que sugiere que actúa como un repetidor de Tor. Tor es un software que permite las comunicaciones anónimas. Tor incrementa el anonimato en la comunicación, ya que reenvía el tráfico potencialmente ilícito del cliente de un relé de Tor a otro.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

UnauthorizedAccess:Runtime/TorClient

La instancia o el contenedor de Amazon EC2 está estableciendo conexiones con un nodo Authority o Guard de Tor.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que una instancia de EC2 o un contenedor de su AWS entorno se está conectando a un nodo de Tor Guard o de Authority. Tor es un software que permite las comunicaciones anónimas. Los guardias Tor y los nodos Authority actúan como gateways a una red Tor. Este tráfico puede indicar que esta instancia o el contenedor de EC2 se han visto afectados y están actuando como clientes en una red de Tor. Este hallazgo puede indicar un acceso no autorizado a tus AWS recursos con la intención de ocultar la verdadera identidad del atacante.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Trojan:Runtime/BlackholeTraffic

Una instancia o un contenedor de Amazon EC2 intenta comunicarse con una dirección IP de un host remoto que es un agujero negro conocido.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este hallazgo indica que la instancia de EC2 que aparece en la lista o un contenedor de su AWS entorno podrían estar comprometidos porque están intentando comunicarse con la dirección IP de un agujero negro (o sumidero). Los agujeros negros hacen referencia a lugares de la red donde el tráfico entrante o saliente se descarta silenciosamente sin informar al origen de que los datos no llegaron a su destinatario esperado. Una dirección IP de agujero negro especifica una máquina host que no se está ejecutando o una dirección a la que no se le ha asignado ningún host.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulte el tipo de recurso en el panel de resultados de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Trojan:Runtime/DropPoint

Una instancia o un contenedor de Amazon EC2 está intentando comunicarse con una dirección IP de un host remoto que se sabe que conserva credenciales y otros datos robados capturados por malware.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que una instancia EC2 o un contenedor de su AWS entorno está intentando comunicarse con una dirección IP de un host remoto del que se sabe que guarda credenciales y otros datos robados capturados por software malicioso.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulte el tipo de recurso en el panel de información de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

CryptoCurrency:Runtime/BitcoinTool.B!DNS

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio asociado con una actividad de criptomoneda.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS está consultando un nombre de dominio que está asociado con actividades relacionadas con Bitcoin u otras criptomonedas. Los actores de las amenazas pueden intentar tomar el control de los recursos de computación para reutilizarlos maliciosamente para la extracción no autorizada de criptomonedas.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si utiliza esta instancia o contenedor de EC2 para extraer o administrar criptomonedas, o si cualquiera de estos está involucrado de otra manera en la actividad de cadena de bloques, el resultado CryptoCurrency:Runtime/BitcoinTool.B!DNS podría representar la actividad esperada para su entorno. Si este es el caso de su AWS entorno, le recomendamos que configure una

regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtrado. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `CryptoCurrency:Runtime/BitcoinTool.B!DNS`. El segundo criterio de filtro debe ser el ID de instancia de la instancia o el ID de imagen de contenedor del contenedor implicado en una actividad de criptomonedas o cadenas de bloques. Para obtener más información, consulte Reglas de supresión.

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Backdoor:Runtime/C&CActivity.B!DNS

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio que está asociado a un servidor de comando y control conocido.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que la instancia o el contenedor de EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio asociado con un servidor de comando y control (C&C) conocido. La instancia o el contenedor de EC2 de la lista podrían haberse visto afectados. Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet.

Un botnet es una colección de dispositivos conectados a Internet (que pueden incluir PC, servidores, dispositivos móviles y dispositivos de Internet de las cosas) que están infectados y controlados por un tipo común de malware. A menudo, los botnets se utilizan para distribuir malware y recopilar información obtenida de forma indebida, como números de tarjetas de crédito. Dependiendo de la finalidad y la estructura del botnet, el servidor C&C también puede enviar comandos para comenzar un ataque de denegación de servicio distribuido (DDoS).

> **Note**
>
> Si el nombre de dominio consultado está relacionado con log4j, los campos del resultado asociado incluirán los siguientes valores:
>
> - `service.additionalInfo.threatListName = Amazon`

- `service.additionalInfo.threatName = Log4j Related`

> **Note**
>
> Para comprobar cómo se GuardDuty genera este tipo de hallazgo, puedes realizar una solicitud de DNS desde tu instancia (si se usa `dig` para Linux o `nslookup` Windows) y compararla con un dominio de `pruebaguarddutyc2activityb.com`.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Trojan:Runtime/BlackholeTraffic!DNS

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio que se está redireccionando a una dirección IP de agujero negro.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS podría haberse visto afectado, ya que está consultando un nombre de dominio que se está redireccionando a una dirección IP de agujero negro. Los agujeros negros hacen referencia a lugares de la red donde el tráfico entrante o saliente se descarta silenciosamente sin informar al origen de que los datos no llegaron a su destinatario esperado.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Trojan:Runtime/DropPoint!DNS

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de un host remoto que se conoce que conservar credenciales y otros datos robados capturados por malware.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que una instancia EC2 o un contenedor de su AWS entorno está consultando el nombre de dominio de un host remoto del que se sabe que contiene credenciales y otros datos robados capturados por software malicioso.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulte el tipo de recurso en el panel de información de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Trojan:Runtime/DGADomainRequest.C!DNS

Una instancia o un contenedor de Amazon EC2 está consultando dominios generados mediante algoritmo. El malware suele utilizar dichos dominios y podría indicar que una instancia o un contenedor de EC2 se han visto afectados.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS está intentando consultar dominios de algoritmos de generación de dominios (DGA). Es posible que su recurso se haya visto afectado.

Los dominios DGA se utilizan para generar de forma periódica una gran cantidad de nombres de dominio que se pueden usar como puntos de encuentro con sus servidores de comando y control (C & C). Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet, que es una colección de dispositivos conectados a Internet que están infectados y son controlados por un tipo común de malware. El gran número de posibles puntos de encuentro dificulta un apagado eficaz de los botnets, ya que los equipos infectados intentan ponerse en contacto con algunos de estos nombres de dominio cada día para recibir actualizaciones o comandos.

> **Note**
>
> Este hallazgo se basa en dominios de DGA conocidos procedentes de fuentes de inteligencia sobre GuardDuty amenazas.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulte el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Trojan:Runtime/DriveBySourceTraffic!DNS

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de un host remoto que es una fuente conocida de ataques de descarga Drive-By.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS podría haberse visto afectada, ya que está consultando un nombre de dominio de

un host remoto que es un origen conocido de ataques de descargas Drive-By. Se trata de descargas no deseadas de software informático desde Internet que pueden iniciar la instalación automática de un virus, spyware o malware.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Trojan:Runtime/PhishingDomainRequest!DNS

Una instancia o un contenedor de Amazon EC2 está consultando dominios implicados en ataques de suplantación de identidad.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que hay una instancia o un contenedor de EC2 en el entorno de AWS que está intentando consultar un dominio implicado en ataques de suplantación de identidad. Los dominios de suplantación de identidad los configura alguien que se presenta como una institución legítima para inducir a las personas a proporcionar información confidencial, como información de identificación personal, datos bancarios y de tarjetas de crédito, y contraseñas. Es posible que su instancia o contenedor de EC2 esté intentando recuperar datos confidenciales almacenados en un sitio web de suplantación de identidad o que esté intentando configurar un sitio web de este tipo. Su instancia o contenedor de EC2 podrían haberse visto afectados.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Impact:Runtime/AbusedDomainRequest.Reputation

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de baja reputación que está asociado a dominios que se sabe que se han utilizado indebidamente.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que el contenedor o la instancia de EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación asociado a dominios o direcciones IP de los que se sabe que se ha utilizado indebidamente. Algunos ejemplos de dominios utilizados indebidamente son los nombres de dominio de nivel superior (TLD) y los nombres de dominio de segundo nivel (2LD), que proporcionan registros de subdominios gratuitos, así como proveedores de DNS dinámicos. Los actores de amenazas suelen utilizar estos servicios para registrar dominios de forma gratuita o a un bajo costo. Los dominios de baja reputación de esta categoría también pueden ser dominios caducados que se resuelven en la dirección IP de estacionamiento de un registrador y, por lo tanto, es posible que ya no estén activos. Una IP de estacionamiento es el lugar al que un registrador dirige el tráfico de dominios que no se han vinculado a ningún servicio. La instancia o el contenedor de Amazon EC2 que aparece en la lista pueden haberse visto afectados, ya que los actores de amenazas suelen utilizar estos registradores o servicios para la distribución de C&C y malware.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Impact:Runtime/BitcoinDomainRequest.Reputation

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de baja reputación que está asociado a la actividad relacionada con la criptomoneda.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que el contenedor o la instancia de EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio que está asociado a actividades relacionadas con Bitcoin u otras criptomonedas. Los actores de las amenazas pueden intentar tomar el control de recursos de computación para reutilizarlos maliciosamente para la extracción no autorizada de criptomonedas.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si utiliza esta instancia o el contenedor de EC2 para extraer o administrar criptomonedas, o si cualquiera de estos está involucrado de otra manera en la actividad de cadena de bloques, el resultado podría representar la actividad esperada para su entorno. Si este es el caso de su AWS entorno, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtro. El primer criterio de filtro debe utilizar el atributo Tipo de resultado con un valor de `Impact:Runtime/BitcoinDomainRequest.Reputation`. El segundo criterio de filtro debe ser el ID de instancia de la instancia o el ID de imagen de contenedor del contenedor implicado en una actividad relacionada con las criptomonedas o las cadenas de bloques. Para obtener más información, consulte Reglas de supresión.

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Impact:Runtime/MaliciousDomainRequest.Reputation

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de baja reputación que está asociado a dominios maliciosos conocidos.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que el contenedor o la instancia de EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación asociado a dominios o direcciones IP maliciosos conocidos. Por ejemplo, los dominios pueden estar asociados a una dirección IP conocida como oculta. Los dominios ocultos son aquellos que anteriormente estaban controlados por un agente de amenazas y las solicitudes que se les hagan pueden indicar que la instancia se ha visto afectada. Estos dominios también pueden estar correlacionados con campañas o algoritmos de generación de dominios maliciosos conocidos.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulte el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Impact:Runtime/SuspiciousDomainRequest.Reputation

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de baja reputación que resulta sospechoso por naturaleza debido a su antigüedad o a su baja popularidad.

Gravedad predeterminada: baja

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que el contenedor o la instancia de EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación que se sospecha que es malicioso. Se observaron características de este dominio que eran coherentes con las de dominios maliciosos observados anteriormente; sin embargo, nuestro modelo de reputación no pudo relacionarlo definitivamente con una amenaza conocida. Por lo general, estos dominios se han detectado recientemente o reciben poco tráfico.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

UnauthorizedAccess:Runtime/MetadataDNSRebind

Una instancia o un contenedor de Amazon EC2 hace búsquedas de DNS que se resuelven en el servicio de metadatos de instancia.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

> **Note**
>
> Actualmente, este tipo de búsqueda solo es compatible con la arquitectura AMD64.

Este hallazgo indica que una instancia de EC2 o un contenedor de su AWS entorno está consultando un dominio que se resuelve en la dirección IP de los metadatos de EC2 (169.254.169.254). Una consulta de DNS de este tipo puede indicar que la instancia es el objetivo de una técnica de reenlace de DNS. Esta técnica se puede utilizar para obtener metadatos de una instancia de EC2, que incluye las credenciales de IAM asociadas a la instancia.

El reenlace de DNS implica engañar a una aplicación que se ejecuta en la instancia de EC2 para que cargue datos devueltos desde una URL, de tal forma que el nombre de dominio de la URL se resuelve en la dirección IP de metadatos de EC2 (`169.254.169.254`). Esto hace que la aplicación obtenga acceso a los metadatos de EC2 y, posiblemente, los ponga a disposición del atacante.

Solo se puede obtener acceso a los metadatos de EC2 mediante el reenlace de DNS si la instancia de EC2 ejecuta una aplicación vulnerable que permite la inserción de URL o si un usuario obtiene acceso a la URL en un navegador web que se ejecuta en la instancia de EC2.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulte el tipo de recurso en el panel de resultados de la consola. GuardDuty

Recomendaciones de corrección:

En respuesta a este resultado, es importante evaluar si hay alguna aplicación vulnerable que se esté ejecutando en la instancia o en el contenedor de EC2 o si un usuario ha utilizado un navegador para acceder al dominio identificado en el resultado. Si la causa raíz es una aplicación vulnerable, corrija la vulnerabilidad. Si un usuario ha navegado por el dominio identificado, bloquee el dominio o impida que los usuarios puedan acceder a él. Si determina que el resultado está relacionado con cualquiera de los casos anteriores, debe revocar la sesión asociada a la instancia de EC2.

Algunos AWS clientes asignan intencionadamente la dirección IP de los metadatos a un nombre de dominio de sus servidores DNS autorizados. Si este es el caso en su entorno de , le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. El primer criterio de filtro debe utilizar el atributo Tipo de resultado con un valor de `UnauthorizedAccess:Runtime/MetaDataDNSRebind`. El segundo criterio de filtro debe ser el Dominio de la solicitud de DNS o el ID de imagen de contenedor del contenedor. El valor Dominio de la solicitud DNS debe coincidir con el dominio que ha asignado a la dirección IP de metadatos (`169.254.169.254`). Para obtener información sobre la creación de reglas de supresión, consulte Reglas de supresión.

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Execution:Runtime/NewBinaryExecuted

Se ha ejecutado un archivo binario recién creado o que se ha modificado recientemente en un contenedor.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que se ha ejecutado un archivo binario recién creado o que se ha modificado recientemente en un contenedor. Se recomienda mantener los contenedores inmutables durante el tiempo de ejecución y los archivos binarios, scripts o bibliotecas no deben crearse ni modificarse durante la vida útil del contenedor. Este comportamiento indica que un agente malintencionado ha accedido al contenedor, ha descargado y ejecutado software malicioso u otro tipo de software como parte del posible ataque. Si bien este tipo de actividad podría ser un indicio de una situación comprometida, también se trata de un patrón de uso común. Por lo tanto, GuardDuty utiliza mecanismos para identificar los casos sospechosos de esta actividad y genera este tipo de hallazgos solo para los casos sospechosos.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

PrivilegeEscalation:Runtime/DockerSocketAccessed

Un proceso dentro de un contenedor se comunica con el daemon de Docker mediante un socket de Docker.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

El socket de Docker es un socket de dominio Unix que el daemon de Docker (`dockerd`) utiliza para comunicarse con sus clientes. Un cliente puede llevar a cabo diversas acciones, como crear contenedores al comunicarse con el daemon de Docker a través del socket de Docker. Es sospechoso que un proceso de contenedor acceda al socket de Docker. Un proceso de contenedor puede escapar del contenedor y obtener acceso de host al comunicarse con el socket de Docket y crear un contenedor privilegiado.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

PrivilegeEscalation:Runtime/RuncContainerEscape

Se ha detectado un intento de acceso al host de un contenedor.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado indica que es posible que el archivo binario runC del host se haya sobrescrito. runC es el tiempo de ejecución de contenedores de bajo nivel que los tiempos de ejecución de contenedores de alto nivel, como Docker y Containerd, utilizan para generar y ejecutar contenedores. runC siempre se ejecuta con privilegios raíz porque necesita realizar una tarea de bajo nivel de creación de un contenedor. Una vulnerabilidad muy conocida en el pasado permitía a contenedores maliciosos anular el archivo binario RunC del anfitrión y obtener acceso raíz al host cuando se ejecutaba el binario RunC modificado.

Este resultado también puede indicar que un actor malicioso podría haber ejecutado un comando en uno de los dos tipos de contenedores siguientes:

- Un contenedor nuevo con una imagen controlada por un atacante.
- Un contenedor existente al que anteriormente podía acceder el atacante con permisos de escritura.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la consola. GuardDuty

- 1. Detalle del CVE-2019-5736

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

Se ha detectado un escape de un contenedor a través de runC en un clúster de Amazon EKS.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que se ha detectado un intento de modificar el archivo de agente de lanzamiento de un grupo de control (cgroup). Linux utiliza grupos de control (cgroups) para limitar, contabilizar y aislar el uso de recursos de un conjunto de procesos. Cada cgroup tiene un archivo de agente de lanzamiento (`release_agent`), un script que Linux ejecuta cuando termina cualquier proceso dentro del cgroup. El archivo de agente de lanzamiento debe ejecutarse siempre en el host. Un actor de amenazas dentro de un contenedor puede escapar al host mediante la escritura de comandos arbitrarios en el archivo de agente de lanzamiento que pertenece a un cgroup. Cuando termina un proceso dentro de ese cgroup, se ejecutan los comandos escritos por el actor.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la consola. GuardDuty

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.Proc

Se ha detectado una inyección de proceso mediante el sistema de archivos proc en un contenedor o en una instancia de Amazon EC2.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

La inyección de procesos es una técnica que los actores de amenazas utilizan para inyectar código en los procesos a fin de evadir las defensas y, potencialmente, aumentar sus privilegios. El sistema de archivos proc (procfs) es un sistema de archivos especial de Linux que presenta la memoria virtual del proceso como un archivo. La ruta de ese archivo es `/proc/PID/mem`, donde `PID` es el ID único del proceso. Un actor de amenazas puede escribir en este archivo para inyectar código en el proceso. Este resultado identifica los posibles intentos de escritura en este archivo.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su tipo de recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.Ptrace

Se ha detectado una inyección de proceso mediante una llamada al sistema ptrace en un contenedor o en una instancia de Amazon EC2.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

La inyección de procesos es una técnica que los actores de amenazas utilizan para inyectar código en los procesos a fin de evadir las defensas y, potencialmente, aumentar sus privilegios. Un proceso puede utilizar la llamada al sistema ptrace para inyectar código en otro proceso. Este resultado identifica un posible intento de inyectar código en un proceso mediante la llamada al sistema ptrace.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su tipo de recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

Se ha detectado una inyección de proceso mediante una escritura directa en la memoria virtual en un contenedor o en una instancia de Amazon EC2.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

La inyección de procesos es una técnica que los actores de amenazas utilizan para inyectar código en los procesos a fin de evadir las defensas y, potencialmente, aumentar sus privilegios. Un proceso puede utilizar una llamada al sistema como `process_vm_writev` para inyectar código directamente en la memoria virtual de otro proceso. Este resultado identifica un posible intento de inyectar código en un proceso mediante la llamada al sistema para escribir en la memoria virtual del proceso.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su tipo de recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Execution:Runtime/ReverseShell

Un proceso en un contenedor o en una instancia de Amazon EC2 ha creado un intérprete de comandos inverso.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Un intérprete de comandos inverso es una sesión de intérprete de comandos que se crea en una conexión que se ha iniciado del host de destino al host del actor. Esto es lo opuesto a un intérprete

de comandos normal que se inicia desde el host del actor hasta el host de destino. Los actores de amenazas crean un intérprete de comandos inverso para ejecutar comandos en el objetivo tras obtener el acceso inicial a este. Este resultado identifica un posible intento de crear un intérprete de comandos inverso.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su tipo de recurso se haya visto afectado.

DefenseEvasion:Runtime/FilelessExecution

Un proceso en un contenedor o en una instancia de Amazon EC2 ejecuta código desde la memoria.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa cuando se ejecuta un proceso mediante un archivo ejecutable en memoria en el disco. Se trata de una técnica de evasión de defensa habitual que impide escribir el ejecutable malicioso en el disco para evitar la detección basada en el análisis del sistema de archivos. Si bien el malware utiliza esta técnica, también tiene algunos casos de uso legítimos. Uno de los ejemplos es un compilador just-in-time (JIT) que escribe el código compilado en la memoria y lo ejecuta desde la memoria.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de resultados de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Impact:Runtime/CryptoMinerExecuted

Una instancia o un contenedor de Amazon EC2 ejecuta un archivo binario asociado con una actividad de extracción de criptomonedas.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que un contenedor o una instancia EC2 de su AWS entorno está ejecutando un archivo binario asociado a una actividad de minería de criptomonedas. Los actores de las amenazas pueden intentar tomar el control de recursos de computación para reutilizarlos maliciosamente para la extracción no autorizada de criptomonedas.

El agente de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulte el tipo de recurso en el panel de resultados de la GuardDuty consola.

Recomendaciones de corrección:

El agente de tiempo de ejecución supervisa los eventos desde varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los hallazgos de la GuardDuty consola y consulteCómo corregir los hallazgos de Runtime Monitoring.

Execution:Runtime/NewLibraryLoaded

Un proceso ha cargado una biblioteca recién creada o modificada recientemente dentro de un contenedor.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que se ha creado una biblioteca o que esta se ha modificado dentro de un contenedor durante el tiempo de ejecución y que un proceso que se ejecuta dentro del contenedor la ha cargado. Se recomienda mantener los contenedores inmutables durante el tiempo de ejecución y los archivos binarios, scripts o bibliotecas no deben crearse ni modificarse durante la vida útil del contenedor. La carga de una biblioteca recién creada o modificada en un contenedor puede indicar actividad sospechosa. Este comportamiento indica la posibilidad de que un actor malicioso haya accedido al contenedor, haya descargado y ejecutado malware u otro software como parte de una posible amenaza. Si bien este tipo de actividad podría ser un indicio de un compromiso, también es un patrón de uso común. Por lo tanto, GuardDuty utiliza mecanismos para

identificar los casos sospechosos de esta actividad y genera este tipo de hallazgos solo para los casos sospechosos.

El agente de tiempo de ejecución supervisa los eventos desde varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Un proceso dentro de un contenedor ha montado un sistema de archivos de host durante el tiempo de ejecución.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Varias técnicas de escape de contenedores implican montar un sistema de archivos de host dentro de un contenedor durante el tiempo de ejecución. Este resultado indica que un proceso dentro de un contenedor podría intentar montar un sistema de archivos de host, lo que podría indicar un intento de escape al host.

El agente de tiempo de ejecución supervisa los eventos desde varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

PrivilegeEscalation:Runtime/UserfaultfdUsage

Un proceso ha utilizado llamadas al sistema **`userfaultfd`** para gestionar los errores de página en el espacio de usuario.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Por lo general, los errores de página los gestiona el kernel en el espacio del kernel. Sin embargo, la llamada al sistema `userfaultfd` permite que un proceso gestione los errores de página en un sistema de archivos del espacio de usuario. Esta es una característica útil que permite la implementación de sistemas de archivos en el espacio de usuario. Por otro lado, también puede ser utilizada por un proceso potencialmente malicioso para interrumpir el funcionamiento del kernel desde el espacio de usuario. Interrumpir el kernel mediante una llamada al sistema `userfaultfd` es una técnica de explotación común para ampliar los intervalos de carrera cuando se explotan las condiciones de carrera del kernel. El uso de `userfaultfd` puede indicar una actividad sospechosa en la instancia de Amazon Elastic Compute Cloud (Amazon EC2).

El agente de tiempo de ejecución supervisa los eventos desde varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Execution:Runtime/SuspiciousTool

Un contenedor o una instancia de Amazon EC2 ejecuta un archivo binario o un script que se utiliza con frecuencia en situaciones de seguridad ofensivas, como la participación de pentests.

Gravedad predeterminada: variable

La gravedad de este hallazgo puede ser alta o baja, dependiendo de si la herramienta sospechosa detectada se considera de doble uso o si se trata exclusivamente de un uso ofensivo.

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que se ha ejecutado una herramienta sospechosa en una instancia o contenedor de EC2 de su AWS entorno. Esto incluye las herramientas utilizadas en las operaciones

de pentesting, también conocidas como herramientas de puerta trasera, escáneres de red y rastreadores de redes. Todas estas herramientas se pueden utilizar en contextos benignos, pero también suelen utilizarlas los actores de amenazas con malas intenciones. Observar las herramientas de seguridad ofensivas podría indicar que la instancia o el contenedor de EC2 asociados se han visto comprometidos.

GuardDuty examina la actividad y el contexto del tiempo de ejecución relacionados para generar este hallazgo solo cuando la actividad y el contexto asociados son potencialmente sospechosos.

El agente de tiempo de ejecución supervisa los eventos desde varios recursos. Para identificar el recurso afectado, consulta el tipo de recurso en los detalles de los hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Execution:Runtime/SuspiciousCommand

Se ha ejecutado un comando sospechoso en una instancia de Amazon EC2 o en un contenedor que indica que se ha puesto en peligro.

Gravedad predeterminada: variable

Según el impacto del patrón malicioso observado, la gravedad de este tipo de hallazgo puede ser baja, media o alta.

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que se ha ejecutado un comando sospechoso e indica que una instancia de Amazon EC2 o un contenedor de su AWS entorno se han visto comprometidos. Esto puede significar que un archivo se descargó de una fuente sospechosa y, a continuación, se ejecutó, o que un proceso en ejecución muestra un patrón malicioso conocido en su línea de comandos. Esto indica además que se está ejecutando malware en el sistema.

GuardDuty examina la actividad y el contexto relacionados con el tiempo de ejecución para generar este hallazgo solo cuando la actividad y el contexto asociados son potencialmente sospechosos.

El agente de tiempo de ejecución supervisa los eventos desde varios recursos. Para identificar el recurso afectado, consulta el tipo de recurso en los detalles de los hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

DefenseEvasion:Runtime/SuspiciousCommand

Se ha ejecutado un comando en la instancia o contenedor de Amazon EC2 que aparece en la lista e intenta modificar o deshabilitar un mecanismo de defensa de Linux, como un firewall o los servicios esenciales del sistema.

Gravedad predeterminada: variable

Según el mecanismo de defensa que se haya modificado o desactivado, la gravedad de este tipo de hallazgo puede ser alta, media o baja.

- Característica: supervisión en tiempo de ejecución

Este hallazgo indica que se ha ejecutado un comando que intenta ocultar un ataque a los servicios de seguridad del sistema local. Esto incluye acciones como deshabilitar el firewall de Unix, modificar las tablas de IP locales, eliminar crontab entradas, deshabilitar un servicio local o hacerse cargo de la función. `LDPreload` Cualquier modificación es altamente sospechosa y puede ser indicativa de que se ha producido algún tipo de compromiso. Por lo tanto, estos mecanismos detectan o evitan que el sistema siga comprometiéndose.

GuardDuty examina la actividad y el contexto relacionados con el tiempo de ejecución, de modo que solo genera este hallazgo cuando la actividad y el contexto asociados son potencialmente sospechosos.

El agente de tiempo de ejecución supervisa los eventos desde varios recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en los detalles de los hallazgos en la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

DefenseEvasion:Runtime/PtraceAntiDebugging

Un proceso de un contenedor o de una instancia de Amazon EC2 ha ejecutado una medida antidepuración mediante la llamada al sistema ptrace.

Gravedad predeterminada: baja

- Característica: supervisión en tiempo de ejecución

Este hallazgo muestra que un proceso que se ejecuta en una instancia de Amazon EC2 o en un contenedor de su AWS entorno ha utilizado la llamada al sistema ptrace con la opción. `PTRACE_TRACEME` Esta actividad provocaría que un depurador adjunto se separara del proceso en ejecución. Si no hay ningún depurador adjunto, no tiene ningún efecto. Sin embargo, la actividad en sí misma suscita sospechas. Esto podría indicar que se está ejecutando malware en el sistema. El malware utiliza con frecuencia técnicas antidepuración para evadir el análisis, y estas técnicas se pueden detectar en tiempo de ejecución.

GuardDuty examina la actividad y el contexto relacionados con el tiempo de ejecución, de modo que solo genera esta información cuando la actividad y el contexto asociados son potencialmente sospechosos.

El agente de tiempo de ejecución supervisa los eventos desde varios recursos. Para identificar el recurso afectado, consulta el tipo de recurso en los detalles de los hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

Execution:Runtime/MaliciousFileExecuted

Se ha ejecutado un archivo ejecutable malicioso conocido en una instancia de Amazon EC2 o en un contenedor.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que se ha ejecutado un ejecutable malicioso conocido en una instancia de Amazon EC2 o en un contenedor de su AWS entorno. Este es un fuerte indicador de que la instancia o el contenedor se han visto potencialmente comprometidos y de que se ha ejecutado malware.

El malware suele utilizar técnicas antidepuración para evadir el análisis, y estas técnicas se pueden detectar en tiempo de ejecución.

GuardDuty examina la actividad y el contexto relacionados con el tiempo de ejecución, de modo que solo genera esta información cuando la actividad y el contexto asociados son potencialmente sospechosos.

El agente de tiempo de ejecución supervisa los eventos desde varios recursos. Para identificar el recurso afectado, consulta el tipo de recurso en los detalles de los hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte Cómo corregir los hallazgos de Runtime Monitoring.

GuardDuty Tipos de búsqueda S3

Los siguientes hallazgos son específicos de los recursos de Amazon S3 y tendrán un tipo de recurso igual a `S3Bucket` si la fuente de datos son eventos de CloudTrail datos de S3 o `AccessKey` si la fuente de datos son eventos CloudTrail de administración. La gravedad y los detalles de los resultados variarán en función del tipo de resultado y el permiso asociado con el bucket.

Los resultados que se muestran aquí incluyen los orígenes de datos y los modelos utilizados para generar ese tipo de resultado. Para obtener más información sobre orígenes de datos y modelos, consulte Orígenes de datos fundamentales.

> **Important**
>
> Los resultados con una fuente de CloudTrail datos de eventos de datos para S3 solo se generan si tiene habilitada la protección de S3 GuardDuty. La protección de S3 se habilita

de forma predeterminada en todas las cuentas creadas después del 31 de julio de 2020. Para obtener información acerca de cómo activar o desactivar la protección de S3, consulte Protección de Amazon S3 en Amazon GuardDuty

Para cualquier resultado del tipo `S3Bucket`, se recomienda examinar los permisos del bucket en cuestión y los permisos de los usuarios implicados en el resultado. Si la actividad es inesperada, consulte las recomendaciones de corrección que se detallan en Corregir un bucket de S3 potencialmente comprometido.

Temas

- Discovery:S3/AnomalousBehavior
- Discovery:S3/MaliciousIPCaller
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- Exfiltration:S3/AnomalousBehavior
- Exfiltration:S3/MaliciousIPCaller
- Impact:S3/AnomalousBehavior.Delete
- Impact:S3/AnomalousBehavior.Permission
- Impact:S3/AnomalousBehavior.Write
- Impact:S3/MaliciousIPCaller
- PenTest:S3/KaliLinux
- PenTest:S3/ParrotLinux
- PenTest:S3/PentooLinux
- Policy:S3/AccountBlockPublicAccessDisabled
- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- UnauthorizedAccess:S3/TorIPCaller

Discovery:S3/AnomalousBehavior

Se ha invocado de forma anómala una API que se utiliza habitualmente para descubrir objetos de S3.

Gravedad predeterminada: baja

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que una entidad de IAM ha invocado una API de S3 para detectar los buckets de S3 en su entorno, como, por ejemplo, `ListObjects`. Este tipo de actividad está asociada a la fase de descubrimiento de un ataque, en la que un atacante recopila información para determinar si su entorno de AWS es susceptible de un ataque más amplio. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, una entidad de IAM sin historial previo invoca una API de S3 o una entidad de IAM invoca una API de S3 desde una ubicación inusual.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Hace un seguimiento a varios factores de las solicitudes de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud, la API específica que se solicitó, el bucket que se solicitó y la cantidad de llamadas que se hicieron a la API. Para obtener más información acerca de los factores de una solicitud de API que son inusuales para la identidad de usuario que ha invocado la solicitud, consulte Detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Discovery:S3/MaliciousIPCaller

Se ha invocado una API de S3 que se suele utilizar para detectar recursos en un entorno de AWS desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que se ha invocado una operación de API de S3 desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a la fase de descubrimiento de un ataque, cuando un adversario recopila información sobre su entorno de AWS. Entre los ejemplos se incluyen `GetObjectAcl` y `ListObjects`.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Discovery:S3/MaliciousIPCaller.Custom

Se ha invocado una API de S3 desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que se ha invocado una API de S3, como `GetObjectAcl` o `ListObjects`, desde una dirección IP que aparece en una lista de amenazas que ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. Este tipo de actividad está asociada a la fase de detección de un ataque, en la que un atacante recopila información para determinar si su entorno de AWS es susceptible de un ataque más amplio.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Discovery:S3/TorIPCaller

Se ha invocado una API de S3 desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que se ha invocado una API de S3, como `GetObjectAcl` o `ListObjects`, desde una dirección IP de nodo de salida de Tor. Este tipo de actividad está asociada a la fase de detección de un ataque, en la que un atacante recopila información para determinar si su entorno de AWS es susceptible de un ataque más amplio. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Exfiltration:S3/AnomalousBehavior

Una entidad de IAM ha invocado una API de S3 de forma sospechosa.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado indica que una entidad de IAM está haciendo llamadas a la API que implican un bucket de S3 y que esta actividad difiere de la referencia establecida por esa entidad. La llamada a la API utilizada en esta actividad está asociada a la fase de exfiltración de un ataque, en la que un atacante intenta recopilar datos. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, una entidad de IAM sin historial previo invoca una API de S3 o una entidad de IAM invoca una API de S3 desde una ubicación inusual.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Hace un seguimiento a varios factores de las solicitudes de API, como el usuario que hizo la solicitud, la ubicación desde

la que se hizo la solicitud, la API específica que se solicitó, el bucket que se solicitó y la cantidad de llamadas que se hicieron a la API. Para obtener más información acerca de los factores de una solicitud de API que son inusuales para la identidad de usuario que ha invocado la solicitud, consulte Detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Exfiltration:S3/MaliciousIPCaller

Se ha invocado una API de S3 que se suele utilizar para recopilar datos de un entorno de AWS desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que se ha invocado una operación de API de S3 desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a tácticas de exfiltración, en las que un adversario intenta recopilar datos de su red. Entre los ejemplos se incluyen `GetObject` y `CopyObject`.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Impact:S3/AnomalousBehavior.Delete

Una entidad de IAM ha invocado una API de S3 que intenta eliminar datos de forma sospechosa.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado indica que una entidad de IAM en su entorno de AWS está haciendo llamadas a la API que implican un bucket de S3 y que esta actividad difiere de la referencia establecida por esa entidad. La llamada a la API utilizada en esta actividad está asociada a un ataque que intenta eliminar datos. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, una entidad de IAM sin historial previo invoca una API de S3 o una entidad de IAM invoca una API de S3 desde una ubicación inusual.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Hace un seguimiento a varios factores de las solicitudes de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud, la API específica que se solicitó, el bucket que se solicitó y la cantidad de llamadas que se hicieron a la API. Para obtener más información acerca de los factores de una solicitud de API que son inusuales para la identidad de usuario que ha invocado la solicitud, consulte Detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Se recomienda llevar a cabo una auditoría del contenido del bucket de S3 para determinar si se puede o se debe restaurar la versión anterior del objeto.

Impact:S3/AnomalousBehavior.Permission

Se ha invocado de forma anómala una API que se utiliza habitualmente para establecer los permisos de la lista de control de acceso (ACL).

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que una entidad de IAM de su entorno de AWS ha cambiado una política de bucket o una ACL en los buckets de S3 de la lista. Este cambio puede exponer públicamente sus buckets de S3 a todos los usuarios de AWS autenticados.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Hace un seguimiento a varios factores de las solicitudes de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud, la API específica que se solicitó, el bucket que se solicitó y la cantidad de llamadas que se hicieron a la API. Para obtener más información acerca de los factores de una solicitud de API que son inusuales para la identidad de usuario que ha invocado la solicitud, consulte Detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Se recomienda llevar a cabo una auditoría del contenido del bucket de S3 para asegurarse de que no se haya permitido el acceso público a ningún objeto de forma inesperada.

Impact:S3/AnomalousBehavior.Write

Una entidad de IAM ha invocado una API de S3 que intenta escribir datos de forma sospechosa.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado indica que una entidad de IAM en su entorno de AWS está haciendo llamadas a la API que implican un bucket de S3 y que esta actividad difiere de la referencia establecida por esa entidad. La llamada a la API utilizada en esta actividad está asociada a un ataque que intenta escribir datos. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, una entidad de IAM sin historial previo invoca una API de S3 o una entidad de IAM invoca una API de S3 desde una ubicación inusual.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Hace un seguimiento a varios factores de las solicitudes de API, como el usuario que hizo la solicitud, la ubicación desde

la que se hizo la solicitud, la API específica que se solicitó, el bucket que se solicitó y la cantidad de llamadas que se hicieron a la API. Para obtener más información acerca de los factores de una solicitud de API que son inusuales para la identidad de usuario que ha invocado la solicitud, consulte Detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Se recomienda llevar a cabo una auditoría del contenido del bucket de S3 para asegurarse de que esta llamada a la API no haya escrito datos maliciosos o no autorizados.

Impact:S3/MaliciousIPCaller

Se ha invocado una API de S3 que se utiliza habitualmente para manipular datos o procesos de un entorno de AWS desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que se ha invocado una operación de API de S3 desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a tácticas de impacto, en las que un adversario intenta manipular, interrumpir o destruir datos de su entorno de AWS. Entre los ejemplos se incluyen `PutObject` y `PutObjectAcl`.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

PenTest:S3/KaliLinux

Se ha invocado una API de S3 desde una máquina de Kali Linux.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que una máquina que ejecuta Kali Linux está haciendo llamadas a la API de S3 con credenciales que pertenecen a su cuenta de AWS. Sus credenciales podrían estar comprometidas. Kali Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para encontrar puntos débiles en la configuración de EC2 y obtener acceso no autorizado al entorno de AWS.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

PenTest:S3/ParrotLinux

Se ha invocado una API de S3 desde una máquina de Parrot Security Linux.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que una máquina que ejecuta Parrot Security Linux está haciendo llamadas a la API de S3 con credenciales que pertenecen a su cuenta de AWS. Sus credenciales podrían estar comprometidas. Parrot Security Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para encontrar puntos débiles en la configuración de EC2 y obtener acceso no autorizado al entorno de AWS.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

PenTest:S3/PentooLinux

Se ha invocado una API de S3 desde una máquina de Pentoo Linux.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que una máquina que ejecuta Pentoo Linux está haciendo llamadas a la API de S3 con credenciales que pertenecen a su cuenta de AWS. Sus credenciales podrían estar comprometidas. Pentoo Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para encontrar puntos débiles en la configuración de EC2 y obtener acceso no autorizado al entorno de AWS.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Policy:S3/AccountBlockPublicAccessDisabled

Una entidad de IAM ha invocado una API utilizada para desactivar el bloqueo de acceso público de S3 en una cuenta.

Gravedad predeterminada: baja

- Fuente de datos: eventos CloudTrail de gestión

Este resultado le informa de que el bloqueo de acceso público de Amazon S3 estaba desactivado en la cuenta. Cuando se activa la configuración de Bloqueo de acceso público de S3, se utiliza para filtrar las políticas o las listas de control de acceso (ACL) en los buckets como medida de seguridad para prevenir la exposición pública involuntaria de datos.

Normalmente, el Bloqueo de acceso público de S3 está desactivado en una cuenta para permitir el acceso público a un bucket o a los objetos que este contiene. Cuando Bloqueo de acceso público

de S3 está desactivado para una cuenta, el acceso a sus buckets se controla mediante las políticas, las ACL o la configuración de Bloqueo de acceso público por bucket que se aplique a sus buckets individuales. Esto no necesariamente significa que los buckets se compartan públicamente, pero sí es importante auditar los permisos que se aplican a los buckets para confirmar que proporcionan el nivel de acceso adecuado.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Policy:S3/BucketAnonymousAccessGranted

Una entidad principal de IAM ha concedido acceso a Internet a un bucket de S3 al cambiar las políticas o las ACL del bucket.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de gestión

Este resultado le informa de que el bucket de S3 que aparece en la lista se ha hecho públicamente accesible en Internet porque una entidad de IAM ha cambiado una política de bucket o una ACL de ese bucket. Tras detectar un cambio en la política o en la ACL, utiliza el razonamiento automatizado desarrollado por Zelkova para determinar si el bucket es de acceso público.

> **Note**
>
> Si las ACL o las políticas de un bucket están configuradas para denegar explícitamente o denegar todo, es posible que este resultado no refleje el estado actual del bucket. Este resultado no reflejará ninguna configuración de Bloqueo de acceso público de S3 que pudiera haberse habilitado para su bucket de S3. En esos casos, el valor `effectivePermission` del resultado se marcará como `UNKNOWN`.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Policy:S3/BucketBlockPublicAccessDisabled

Una entidad de IAM ha invocado una API utilizada para desactivar el bloqueo de acceso público de S3 en un bucket.

Gravedad predeterminada: baja

- Fuente de datos: eventos CloudTrail de gestión

Este resultado le informa de que el bloqueo de acceso público se ha deshabilitado para el bucket de S3 que aparece en la lista. Cuando se activa, la configuración de Bloqueo de acceso público de S3 se utiliza para filtrar las políticas o las listas de control de acceso (ACL) aplicadas a los buckets como medida de seguridad para prevenir la exposición pública involuntaria de datos.

Normalmente, el Bloqueo de acceso público de S3 está desactivado en un bucket para permitir el acceso público a este o a los objetos que contiene. Cuando el Bloqueo de acceso público de S3 se deshabilita en un bucket, las políticas o las ACL que se han aplicado al bucket controlan el acceso a este. Esto no significa que el bucket se comparta públicamente, pero sí es importante auditar las políticas y ACL que se aplican al bucket para confirmar que se apliquen los permisos adecuados.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Policy:S3/BucketPublicAccessGranted

Una entidad principal de IAM ha concedido acceso público a un bucket de S3 a todos los usuarios de AWS al cambiar las políticas o las ACL del bucket.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de gestión

Este resultado le informa de que el bucket de S3 que aparece en la lista se ha expuesto públicamente a todos los usuarios de AWS autenticados porque una entidad de IAM ha cambiado una política de bucket o una ACL de ese bucket de S3. Tras detectar un cambio en la política o en la ACL, utiliza el razonamiento automatizado desarrollado por Zelkova para determinar si el bucket es de acceso público.

> **Note**
>
> Si las ACL o las políticas de un bucket están configuradas para denegar explícitamente o denegar todo, es posible que este resultado no refleje el estado actual del bucket. Este resultado no reflejará ninguna configuración de Bloqueo de acceso público de S3 que pudiera haberse habilitado para su bucket de S3. En esos casos, el valor `effectivePermission` del resultado se marcará como `UNKNOWN`.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Stealth:S3/ServerAccessLoggingDisabled

El registro de acceso al servidor de S3 se ha deshabilitado para un bucket.

Gravedad predeterminada: baja

- Fuente de datos: eventos CloudTrail de gestión

Este resultado le informa de que el registro de acceso al servidor de S3 está deshabilitado para un bucket dentro de su entorno de AWS. Si está deshabilitada, no se crea ningún registro de solicitudes web para los intentos de acceso al depósito de S3 identificado; sin embargo, se siguen rastreando las llamadas a la API de administración de S3 al depósito DeleteBucket, por ejemplo. Si el registro de eventos de datos de S3 está habilitado CloudTrail para este depósito, se seguirá rastreando las solicitudes web de los objetos incluidos en el depósito. La desactivación del registro es una

técnica que suelen utilizar los usuarios no autorizados para evitar que los detecten. Para obtener más información sobre los registros de S3, consulte Registro de acceso al servidor de S3 y Opciones de registro para S3.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

Se ha invocado una API de S3 desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que se ha invocado una operación de la API de S3, como `PutObject` o `PutObjectAcl`, desde una dirección IP que aparece en una lista de amenazas que ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

UnauthorizedAccess:S3/TorIPCaller

Se ha invocado una API de S3 desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que se ha invocado una operación de la API de S3, como `PutObject` o `PutObjectAcl`, desde una dirección IP de nodo de salida de Tor. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Este resultado puede indicar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Tipos de resultados retirados

Un resultado es una notificación que contiene detalles sobre un problema potencial de seguridad descubierto por . Para obtener más información acerca de cambios importantes en los tipos de resultado de GuardDuty, incluidos los retirados o añadidos recientemente, consulte Historial de documentos de Amazon GuardDuty.

Los siguientes tipos de búsqueda se retiran y GuardDuty ya no los genera.

> **Important**
>
> NO PUEDE reactivar tipos de resultados de retirados.

Temas

- Exfiltration:S3/ObjectRead.Unusual
- Impact:S3/PermissionsModification.Unusual
- Impact:S3/ObjectDelete.Unusual
- Discovery:S3/BucketEnumeration.Unusual
- Persistence:IAMUser/NetworkPermissions
- Persistence:IAMUser/ResourcePermissions
- Persistence:IAMUser/UserPermissions
- PrivilegeEscalation:IAMUser/AdministrativePermissions

- Recon:IAMUser/NetworkPermissions
- Recon:IAMUser/ResourcePermissions
- Recon:IAMUser/UserPermissions
- ResourceConsumption:IAMUser/ComputeResources
- Stealth:IAMUser/LoggingConfigurationModified
- UnauthorizedAccess:IAMUser/ConsoleLogin
- UnauthorizedAccess:EC2/TorIPCaller
- Backdoor:EC2/XORDDOS
- Behavior:IAMUser/InstanceLaunchUnusual
- CryptoCurrency:EC2/BitcoinTool.A
- UnauthorizedAccess:IAMUser/UnusualASNCaller

Exfiltration:S3/ObjectRead.Unusual

Una entidad de IAM invocó una API de S3 de forma sospechosa.

Gravedad predeterminada: media

> **Note**
>
> La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia AWS, la gravedad del resultado es alta.

- Fuente de datos: eventos de datos de CloudTrail para S3

Este hallazgo le informa de que una entidad de IAM de su AWS entorno está realizando llamadas a la API que involucran un segmento de S3 y que difieren de la línea base establecida por esa entidad. La llamada a la API utilizada en esta actividad está asociada a la fase de exfiltración de un ataque, en la que un atacante intenta recopilar datos. Esta actividad es sospechosa porque la forma en que la entidad de IAM invocó la API era inusual. Por ejemplo, esta entidad de IAM no tenía antecedentes de invocación de este tipo de API o la API se invocó desde una ubicación inusual.

Recomendaciones de corrección:

Si esta actividad es inesperada para el director asociado, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Impact:S3/PermissionsModification.Unusual

Una entidad de IAM invocó una API para modificar los permisos en uno o más recursos de S3.

Gravedad predeterminada: media

> **Note**
>
> La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia AWS, la gravedad del resultado es alta.

Este hallazgo le informa de que una entidad de IAM está realizando llamadas a la API diseñadas para modificar los permisos en uno o más depósitos u objetos de su entorno. AWS Es posible que un atacante lleve a cabo esta acción para permitir que la información se comparta fuera de la cuenta. Esta actividad es sospechosa porque la forma en que la entidad de IAM invocó la API era inusual. Por ejemplo, esta entidad de IAM no tenía antecedentes de invocación de este tipo de API o la API se invocó desde una ubicación inusual.

Recomendaciones de corrección:

Si esta actividad es inesperada para el director asociado, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Impact:S3/ObjectDelete.Unusual

Una entidad de IAM invocó una API que se utiliza para eliminar datos en un bucket de S3.

Gravedad predeterminada: media

> **Note**
>
> La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia AWS, la gravedad del resultado es alta.

Este hallazgo le informa de que una entidad de IAM específica de su AWS entorno está realizando llamadas a la API diseñadas para eliminar los datos del depósito de S3 de la lista mediante la eliminación del propio depósito. Esta actividad es sospechosa porque la forma en que la entidad de IAM invocó la API no era habitual. Por ejemplo, esta entidad de IAM no tenía antecedentes de invocación de este tipo de API o la API se invocó desde una ubicación inusual.

Recomendaciones de corrección:

Si esta actividad es inesperada para el director asociado, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Discovery:S3/BucketEnumeration.Unusual

Una entidad de IAM ha invocado una API de S3 que se utiliza para detectar los buckets de S3 de la red.

Gravedad predeterminada: media

> **Note**
>
> La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia AWS, la gravedad del resultado es alta.

Este hallazgo le informa de que una entidad de IAM ha invocado una API de S3 para detectar los buckets de S3 en su entorno, por ejemplo. `ListBuckets` Este tipo de actividad está asociada a la

fase de descubrimiento de un ataque, en la que un atacante recopila información para determinar si su AWS entorno es susceptible a un ataque más amplio. Esta actividad es sospechosa porque la forma en que la entidad de IAM invocó la API no era habitual. Por ejemplo, esta entidad de IAM no tenía antecedentes de invocación de este tipo de API o la API se invocó desde una ubicación inusual.

Recomendaciones de corrección:

Si esta actividad es inesperada para el director asociado, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte Corregir un bucket de S3 potencialmente comprometido.

Persistence:IAMUser/NetworkPermissions

Un usuario de IAM invocó una API que se suele usar para cambiar los permisos de acceso de red de los grupos de seguridad, las rutas y las listas de control de acceso de las cuentas de AWS.

Gravedad predeterminada: media

> **Note**
>
> La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia AWS, la gravedad del resultado es alta.

Este resultado le indica que una entidad principal concreta del entorno de AWS está mostrando un comportamiento diferente de la línea de referencia establecida. Esta entidad de seguridad nunca antes había invocado esta API.

Este hallazgo se produce cuando los ajustes de configuración de la red se modifican en circunstancias sospechosas, como cuando un director invoca la `CreateSecurityGroup` API sin antecedentes de haberlo hecho. A menudo los atacantes intentan cambiar los grupos de seguridad, permitiendo que un volumen determinado de tráfico entre en varios puertos a fin de mejorar su capacidad para obtener acceso al bot que pueden haber plantado en su instancia EC2.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Persistence:IAMUser/ResourcePermissions

Una entidad de seguridad ha invocado una API que suele usarse para cambiar las políticas de acceso de seguridad de varios recursos de una cuenta de AWS.

Gravedad predeterminada: media

> **Note**
>
> La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia AWS, la gravedad del resultado es alta.

Este resultado le indica que una entidad principal concreta del entorno de AWS está mostrando un comportamiento diferente de la línea de referencia establecida. Esta entidad de seguridad nunca antes había invocado esta API.

Este hallazgo se activa cuando se detecta un cambio en las políticas o los permisos asociados a AWS los recursos, por ejemplo, cuando un director de su AWS entorno invoca la `PutBucketPolicy` API sin un historial previo de haberlo hecho. Algunos servicios, como Amazon S3, pueden tener permisos asociados a un recurso que permitan que una o varias entidades de seguridad puedan obtener acceso a dicho recurso. Con las credenciales robadas los atacantes pueden cambiar las políticas asociadas a un recurso y concederse a sí mismos acceso en adelante a dicho recurso.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Persistence:IAMUser/UserPermissions

Una entidad de seguridad ha invocado una API que suele utilizarse para añadir, modificar o eliminar usuarios, grupos o políticas de IAM en una cuenta de AWS.

Gravedad predeterminada: media

> **Note**
>
> La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia AWS, la gravedad del resultado es alta.

Este resultado le indica que una entidad principal concreta del entorno de AWS está mostrando un comportamiento diferente de la línea de referencia establecida. Esta entidad de seguridad nunca antes había invocado esta API.

Este hallazgo se debe a cambios sospechosos en los permisos relacionados con los usuarios de su AWS entorno, por ejemplo, cuando un director de su AWS entorno invoca la `AttachUserPolicy` API sin tener antecedentes de hacerlo. Los atacantes pueden utilizar credenciales robadas para crear nuevos usuarios, añadir políticas de acceso a los usuarios existentes o crear claves de acceso para maximizar su acceso a una cuenta, incluso si su punto de acceso original está cerrado. Por ejemplo, el propietario de la cuenta podría darse cuenta del robo de un usuario o una contraseña de IAM en concreto y eliminarlos de la cuenta. Sin embargo, es posible que no eliminen a otros usuarios que hayan sido creados por un administrador creado de forma fraudulenta, lo que dejaría su AWS cuenta accesible al atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

PrivilegeEscalation:IAMUser/AdministrativePermissions

Una entidad principal ha intentado asignarse una política excesivamente permisiva.

Gravedad predeterminada: baja

> **Note**
>
> La gravedad de este resultado es baja si no se consigue completar el intento de escalado de privilegios o media si el intento se realiza con éxito.

Este resultado le informa de que una entidad de seguridad concreta del entorno de AWS está registrando un comportamiento que puede indicar un ataque de escalado de privilegios. Este resultado se activa cuando un usuario o un rol intentan asignarse una política excesivamente permisiva. Si el usuario o el rol en cuestión no debe tener privilegios administrativos, puede que las credenciales del usuario estén en riesgo o que los permisos del rol no se hayan configurado correctamente.

Los atacantes utilizarán credenciales robadas para crear nuevos usuarios, añadir políticas de acceso a los usuarios existentes o crear claves de acceso para maximizar su acceso a una cuenta, incluso si su punto de acceso original está cerrado. El propietario de la cuenta podría percatarse de que le han robado una contraseña o un determinado usuario de IAM y eliminarlos de la cuenta. Sin embargo, es posible que no eliminara otros usuarios creados por la entidad de seguridad que se generó de forma fraudulenta, por lo que la cuenta de AWS seguiría siendo accesible para el atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Recon:IAMUser/NetworkPermissions

Una entidad de seguridad ha invocado una API que suele usarse para cambiar los permisos de acceso de red de los grupos de seguridad, las rutas y las listas de control de acceso de las cuentas de AWS.

Gravedad predeterminada: media

> **Note**
>
> La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia AWS, la gravedad del resultado es alta.

Este resultado le indica que una entidad principal concreta del entorno de AWS está mostrando un comportamiento diferente de la línea de referencia establecida. Esta entidad de seguridad nunca antes había invocado esta API.

Este resultado se activa cuando se sondean los permisos de acceso a recursos de su cuenta de AWS en circunstancias sospechosas. Por ejemplo, si una entidad de seguridad invoca la API StopLogging cuando nunca antes lo había hecho. Un atacante puede utilizar las credenciales robadas para realizar este reconocimiento de sus recursos de AWS y encontrar de esta manera información valiosa o determinar cuáles son las capacidades de las credenciales que han caído en sus manos.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Recon:IAMUser/ResourcePermissions

Una entidad de seguridad ha invocado una API que suele usarse para cambiar las políticas de acceso de seguridad de varios recursos de una cuenta de AWS.

Gravedad predeterminada: media

> **Note**
>
> La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia AWS, la gravedad del resultado es alta.

Este resultado le indica que una entidad principal concreta del entorno de AWS está mostrando un comportamiento diferente de la línea de referencia establecida. Esta entidad de seguridad nunca antes había invocado esta API.

Este resultado se activa cuando se sondean los permisos de acceso a recursos de su cuenta de AWS en circunstancias sospechosas. Por ejemplo, si una entidad de seguridad invoca la API StopLogging cuando nunca antes lo había hecho. Un atacante puede utilizar las credenciales robadas para realizar este reconocimiento de sus recursos de AWS y encontrar de esta manera información valiosa o determinar cuáles son las capacidades de las credenciales que han caído en sus manos.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Recon:IAMUser/UserPermissions

Una entidad de seguridad ha invocado una API que suele utilizarse para añadir, modificar o eliminar usuarios, grupos o políticas de IAM en una cuenta de AWS.

Gravedad predeterminada: media

> **Note**
>
> La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia AWS, la gravedad del resultado es alta.

Este resultado se activa cuando se sondean los permisos de usuario de su entorno de AWS en circunstancias sospechosas. Por ejemplo, si una entidad de seguridad invoca la API StopLogging cuando nunca antes lo había hecho. Un atacante puede utilizar las credenciales robadas para realizar este reconocimiento de sus recursos de AWS y encontrar de esta manera información valiosa o determinar cuáles son las capacidades de las credenciales que han caído en sus manos.

Este resultado le indica que una entidad principal concreta del entorno de AWS está mostrando un comportamiento diferente de la línea de referencia establecida. Esta entidad principal no tiene historial previo de invocación de esta API de esta manera.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

ResourceConsumption:IAMUser/ComputeResources

Una entidad principal ha invocado una API que suele utilizarse para lanzar recursos de computación como instancias EC2.

Gravedad predeterminada: media

> **Note**
>
> La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia AWS, la gravedad del resultado es alta.

Este resultado se activa cuando se lanzan instancias EC2 de su entorno de AWS en circunstancias sospechosas. Este hallazgo indica que un director específico de su AWS entorno presenta un comportamiento diferente del punto de referencia establecido; por ejemplo, si un director (Usuario raíz de la cuenta de AWSun rol de IAM o un usuario de IAM) ha invocado la `RunInstances` API sin antecedentes de haberlo hecho. Esto podría ser señal de que un atacante está utilizando credenciales robadas para robar tiempo de computación (posiblemente minería de criptomoneda o violación de contraseñas). También puede ser señal de que un atacante está utilizando una instancia EC2 de su entorno de AWS y sus credenciales para mantener el acceso a su cuenta.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Stealth:IAMUser/LoggingConfigurationModified

Una entidad principal ha invocado una API que suele utilizarse para parar el registro en CloudTrail, suprimir registros existentes y eliminar de cualquier otra forma los rastros de la actividad de una cuenta de AWS.

Gravedad predeterminada: media

> **Note**
>
> La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia AWS, la gravedad del resultado es alta.

Este resultado se activa cuando se modifica la configuración de registro de su cuenta de AWS en circunstancias sospechosas. Este hallazgo le informa de que un director específico de su AWS entorno presenta un comportamiento diferente del punto de referencia establecido; por ejemplo, si un director (Usuario raíz de la cuenta de AWSun rol de IAM o un usuario de IAM) ha invocado la `StopLogging` API sin un historial previo de haberlo hecho. Esto puede ser señal de que un atacante está intentando cubrir sus huellas eliminando cualquier rastro de su actividad.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

UnauthorizedAccess:IAMUser/ConsoleLogin

Se observó que una entidad de seguridad de su cuenta de AWS ha iniciado sesión de forma inusual en la consola.

Gravedad predeterminada: media

> **Note**
>
> La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con credenciales temporales de AWS creadas en una instancia AWS, la gravedad del resultado es alta.

Este resultado se activa cuando se detecta un inicio de sesión en la consola en circunstancias sospechosas. Por ejemplo, si una entidad de seguridad ha invocado anteriormente la API ConsoleLogin desde una ubicación o un cliente específicos cuando nunca antes lo había hecho. Esto podría ser señal de que se están usando credenciales robadas para obtener acceso a su cuenta de AWS o que un usuario válido está obteniendo acceso a la cuenta de forma no válida o menos segura (por ejemplo, no obtiene acceso mediante una VPN aprobada).

Este resultado le informa de que una entidad de seguridad concreta del entorno de AWS está registrando un comportamiento diferente a la línea de referencia establecida. Esta entidad de seguridad nunca antes había iniciado sesión con esta aplicación cliente desde esta ubicación específica.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

UnauthorizedAccess:EC2/TorIPCaller

La instancia EC2 recibe conexiones entrantes de un nodo de salida Tor.

Gravedad predeterminada: media

Este resultado le informa de que una instancia EC2 del entorno de AWS está recibiendo conexiones entrantes de un nodo de salida Tor. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, puede que su instancia de EC2 esté comprometida. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Backdoor:EC2/XORDDOS

Una instancia EC2 está intentando comunicarse con una dirección IP relacionada con malware XorDDos.

Gravedad predeterminada: alta

Este resultado le informa de que hay una instancia EC2 en el entorno de AWS que intenta comunicarse con una dirección IP relacionada con malware XorDDos. Esta instancia EC2 podría estar comprometida. XOR DDoS es malware troyano que secuestra sistemas Linux. En un intento de obtener acceso al sistema, lanza un ataque de fuerza bruta para descubrir la contraseña de los servicios de Secure Shell (SSH) en Linux. Después de haber adquirido las credenciales de SSH y haber realizado correctamente el inicio de sesión, utiliza privilegios raíz para ejecutar un script que descarga e instala XOR DDoS. A continuación, este malware se utiliza como parte de un botnet para lanzar ataques de denegación de servicio distribuido (DDoS) contra otros destinos.

Recomendaciones de corrección:

Si esta actividad es inesperada, puede que su instancia de EC2 esté comprometida. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

Behavior:IAMUser/InstanceLaunchUnusual

Un usuario de IAM lanzó una instancia EC2 de un tipo inusual.

Gravedad predeterminada: alta

Este resultado le informa de que un usuario concreto de IAM del entorno de AWS exhibe un comportamiento distinto de la referencia establecida. Este usuario de IAM no tiene historial previo de lanzamientos de una instancia EC2 de este tipo. Sus credenciales podrían estar comprometidas.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

CryptoCurrency:EC2/BitcoinTool.A

La instancia EC2 se está comunicando con grupos de minería de Bitcoin.

Gravedad predeterminada: alta

Este resultado le informa de que una instancia EC2 del entorno de AWS se está comunicando con grupos de minería de Bitcoin. En el campo de la minería de criptomonedas, un grupo de minería es la agrupación de recursos por parte de mineros que comparten potencia de procesamiento a través de una red para dividir la compensación en función de la cantidad de trabajo con la que han contribuido para resolver un bloque. A menos que utilice esta instancia EC2 para la minería de Bitcoin, dicha instancia podría estar comprometida.

Recomendaciones de corrección:

Si esta actividad es inesperada, puede que su instancia de EC2 esté comprometida. Para obtener más información, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

UnauthorizedAccess:IAMUser/UnusualASNCaller

Se ha invocado una API desde una dirección IP de una red inusual.

Gravedad predeterminada: alta

Este resultado le informa de que se ha invocado cierta actividad desde una dirección IP de una red inusual. Esta red no se ha observado nunca en todo el historial de uso de AWS del usuario descrito.

Esta actividad puede incluir un inicio de sesión en la consola, un intento de lanzar una instancia EC2, la creación de un nuevo usuario de IAM, la modificación de sus privilegios de AWS, etc. Esto puede indicar un acceso no autorizado a los recursos de AWS.

Recomendaciones de corrección:

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte . Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.

Resultados por tipo de recurso

Las siguientes páginas se clasifican por tipo de recurso asociado a un GuardDuty hallazgo:

- Tipos de resultados de EC2
- Tipos de búsqueda de Runtime Monitoring
- Tipos de resultados de IAM
- Tipos de resultados de registros de auditoría de Kubernetes
- Tipos de búsqueda de Lambda Protection
- Tipos de búsqueda de protección contra malware
- Tipos de búsqueda de RDS Protection
- Tipos de resultados de S3

Tabla de resultados

En la siguiente tabla, se muestran todos los tipos de resultados activos ordenados por el origen de datos o la característica fundamental, según corresponda. Algunos de los siguientes tipos de resultados pueden tener una gravedad variable, la cual se indica con un asterisco (*). Para obtener información sobre la gravedad variable de un tipo de resultado, consulte la descripción detallada de este.

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Discovery:S3/AnomalousBehavior	Amazon S3	CloudTrail eventos de datos para S3	Baja

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Discovery:S3/MaliciousIPCaller	Amazon S3	CloudTrail eventos de datos para S3	Alta
Discovery:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail eventos de datos para S3	Alta
Discovery:S3/TorIPCaller	Amazon S3	CloudTrail eventos de datos para S3	Medio
Exfiltration:S3/AnomalousBehavior	Amazon S3	CloudTrail eventos de datos para S3	Alta
Exfiltration:S3/MaliciousIPCaller	Amazon S3	CloudTrail eventos de datos para S3	Alta
Impact:S3/AnomalousBehavior.Delete	Amazon S3	CloudTrail eventos de datos para S3	Alta
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail eventos de datos para S3	Alta
Impact:S3/AnomalousBehavior.Write	Amazon S3	CloudTrail eventos de datos para S3	Medio

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Impact:S3/MaliciousIPCaller	Amazon S3	CloudTrail eventos de datos para S3	Alta
PenTest:S3/KaliLinux	Amazon S3	CloudTrail eventos de datos para S3	Medio
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail eventos de datos para S3	Medio
PenTest:S3/PentooLinux	Amazon S3	CloudTrail eventos de datos para S3	Medio
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail eventos de datos para S3	Alta
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail eventos de datos para S3	Alta
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestión	Medio
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestión	Medio

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestión	Baja
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestión	Alta
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestión	Alta
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestión	Medio
PenTest:IAMUser/KaliLinux	IAM	CloudTrail evento de gestión	Medio
PenTest:IAMUser/ParrotLinux	IAM	CloudTrail evento de gestión	Medio
PenTest:IAMUser/PentooLinux	IAM	CloudTrail evento de gestión	Medio

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestión	Medio
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail evento de gestión	Baja
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	CloudTrail evento de gestión	Alta*
Policy:S3/AccountBlockPublicAccessDisabled	Amazon S3	CloudTrail evento de gestión	Baja
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	CloudTrail evento de gestión	Alta
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	CloudTrail evento de gestión	Baja

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Policy:S3/BucketPublicAccessGranted	Amazon S3	CloudTrail evento de gestión	Alta
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestión	Medio
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail evento de gestión	Medio
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail evento de gestión	Medio
Recon:IAMUser/TorIPCaller	IAM	CloudTrail evento de gestión	Medio
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail evento de gestión	Baja
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail evento de gestión	Baja

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail evento de gestión	Medio
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail evento de gestión	Medio
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail evento de gestión	Medio
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail evento de gestión	Medio
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail eventos de gestión o eventos CloudTrail de datos para S3	Baja

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail eventos de gestión o eventos CloudTrail de datos para S3	Alta
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	Registros de DNS	Alta
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	Registros de DNS	Alta
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	Registros de DNS	Medio
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	Registros de DNS	Alta
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	Registros de DNS	Alta

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	Registros de DNS	Baja
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	Registros de DNS	Medio
Trojan:EC2/DGADomainRequest.B	Amazon EC2	Registros de DNS	Alta
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	Registros de DNS	Alta
Trojan:EC2/DNSDataExfiltration	Amazon EC2	Registros de DNS	Alta
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	Registros de DNS	Alta
Trojan:EC2/DropPoint!DNS	Amazon EC2	Registros de DNS	Medio
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	Registros de DNS	Alta

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	Registros de DNS	Alta
Execution:Container/MaliciousFile	Contenedor	Volúmenes de EBS	Varía en función de la amenaza detectada
Execution:Container/SuspiciousFile	Contenedor	Volúmenes de EBS	Varía en función de la amenaza detectada
Execution:EC2/MaliciousFile	EC2	Volúmenes de EBS	Varía en función de la amenaza detectada
Execution:EC2/SuspiciousFile	EC2	Volúmenes de EBS	Varía en función de la amenaza detectada
Execution:ECS/MaliciousFile	ECS	Volúmenes de EBS	Varía en función de la amenaza detectada
Execution:ECS/SuspiciousFile	ECS	Volúmenes de EBS	Varía en función de la amenaza detectada
Execution:Kubernetes/MaliciousFile	Kubernetes	Volúmenes de EBS	Varía en función de la amenaza detectada

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Execution:Kubernetes/SuspiciousFile	Kubernetes	Volúmenes de EBS	Varía en función de la amenaza detectada
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	Registros de auditoría de Kubernetes	Medio
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	Registros de auditoría de Kubernetes	Alta
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Registros de auditoría de Kubernetes	Alta
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Registros de auditoría de Kubernetes	Alta

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	Registros de auditoría de Kubernetes	Alta
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	Registros de auditoría de Kubernetes	Alta
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Registros de auditoría de Kubernetes	Alta
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Registros de auditoría de Kubernetes	Alta
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	Registros de auditoría de Kubernetes	Alta
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	Registros de auditoría de Kubernetes	Baja

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	Registros de auditoría de Kubernetes	Medio
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Registros de auditoría de Kubernetes	Medio
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Registros de auditoría de Kubernetes	Medio
Discovery:Kubernetes/TorIPCaller	Kubernetes	Registros de auditoría de Kubernetes	Medio
Execution:Kubernetes/ExecInKubeSystemPod	Kubernetes	Registros de auditoría de Kubernetes	Medio
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	Registros de auditoría de Kubernetes	Medio

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	Registros de auditoría de Kubernetes	Baja
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	Registros de auditoría de Kubernetes	Alta
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Registros de auditoría de Kubernetes	Alta
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Registros de auditoría de Kubernetes	Alta
Impact:Kubernetes/TorIPCaller	Kubernetes	Registros de auditoría de Kubernetes	Alta
Persistence:Kubernetes/ContainerWithSensitiveMount	Kubernetes	Registros de auditoría de Kubernetes	Medio

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	Registros de auditoría de Kubernetes	Medio
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Registros de auditoría de Kubernetes	Medio
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Registros de auditoría de Kubernetes	Alta
Persistence:Kubernetes/TorIPCaller	Kubernetes	Registros de auditoría de Kubernetes	Medio
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	Registros de auditoría de Kubernetes	Alta
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	Registros de auditoría de Kubernetes	Alta

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	Registros de auditoría de Kubernetes	Medio
Policy:Kubernetes/ExposedDashboard	Kubernetes	Registros de auditoría de Kubernetes	Medio
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	Registros de auditoría de Kubernetes	Mediana
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	Registros de auditoría de Kubernetes	Baja

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	Registros de auditoría de Kubernetes	Alta
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	Registros de auditoría de Kubernetes	Alta
PrivilegeEscalation:Kubernetes/PrivilegedContainer	Kubernetes	Registros de auditoría de Kubernetes	Medio
Backdoor:Lambda/C&CActivity.B	Lambda	Supervisión de la actividad de red de Lambda	Alta
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Supervisión de la actividad de red de Lambda	Alta

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Trojan:Lambda/BlackholeTraffic	Lambda	Supervisión de la actividad de red de Lambda	Medio
Trojan:Lambda/DropPoint	Lambda	Supervisión de la actividad de red de Lambda	Medio
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Supervisión de la actividad de red de Lambda	Medio
UnauthorizedAccess:Lambda/TorClient	Lambda	Supervisión de la actividad de red de Lambda	Alta
UnauthorizedAccess:Lambda/TorRelay	Lambda	Supervisión de la actividad de red de Lambda	Alta
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	Bases de datos compatibles de Amazon Aurora	Supervisión de la actividad de inicio de sesión de RDS	Baja

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	Bases de datos compatibles de Amazon Aurora	Supervisión de la actividad de inicio de sesión de RDS	Alta
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	Bases de datos compatibles de Amazon Aurora	Supervisión de la actividad de inicio de sesión de RDS	Variable*
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	Bases de datos compatibles de Amazon Aurora	Supervisión de la actividad de inicio de sesión de RDS	Medio
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	Bases de datos compatibles de Amazon Aurora	Supervisión de la actividad de inicio de sesión de RDS	Alta
CredentialAccess:RDS/TorIPCaller.FailedLogin	Bases de datos compatibles de Amazon Aurora	Supervisión de la actividad de inicio de sesión de RDS	Medio
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	Bases de datos compatibles de Amazon Aurora	Supervisión de la actividad de inicio de sesión de RDS	Alta

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Discovery:RDS/MaliciousIPCaller	Bases de datos compatibles de Amazon Aurora	Supervisión de la actividad de inicio de sesión de RDS	Medio
Discovery:RDS/TorIPCaller	Bases de datos compatibles de Amazon Aurora	Supervisión de la actividad de inicio de sesión de RDS	Medio
Backdoor:Runtime/C&CActivity.B	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alta
Backdoor:Runtime/C&CActivity.B!DNS	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Alta
CryptoCurrency:Runtime/BitcoinTool.B	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Alta
CryptoCurrency:Runtime/BitcoinTool.B!DNS	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Alta
DefenseEvasion:Runtime/FilelessExecution	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Medio

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
DefenseEvasion:Runtime/ProcessInjection.Proc	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Alta
DefenseEvasion:Runtime/ProcessInjection.Ptrace	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Medio
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Alta
DefenseEvasion:Runtime/PtraceAntiDebugging	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Baja
DefenseEvasion:Runtime/SuspiciousCommand	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Alta
Execution:Runtime/MaliciousFileExecuted	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Alta
Execution:Runtime/NewBinaryExecuted	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Medio

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Execution:Runtime/NewLibraryLoaded	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Medio
Execution:Runtime/SuspiciousCommand	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Variable
Execution:Runtime/SuspiciousTool	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Variable
Execution:Runtime/ReverseShell	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Alta
Impact:Runtime/AbusedDomainRequest.Reputation	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Medio
Impact:Runtime/BitcoinDomainRequest.Reputation	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Alta
Impact:Runtime/CryptoMinerExecuted	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Alta

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Impact:Runtime/MaliciousDomainRequest.Reputation	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Medio
Impact:Runtime/SuspiciousDomainRequest.Reputation	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Baja
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Alta
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	Instancia, clúster EKS, clúster ECS o contenedor	Supervisión en tiempo de ejecución	Medio
PrivilegeEscalation:Runtime/DockerSocketAccessed	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
PrivilegeEscalation:Runtime/RuncContainerEscape	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alta
PrivilegeEscalation:Runtime/UserfaultfdUsage	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
Trojan:Runtime/BlackholeTraffic	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
Trojan:Runtime/BlackholeTraffic!DNS	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
Trojan:Runtime/DropPoint	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
Trojan:Runtime/DGADomainRequest.C!DNS	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alta

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Trojan:Runtime/DriveBySourceTraffic!DNS	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alta
Trojan:Runtime/DropPoint!DNS	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Medio
Trojan:Runtime/PhishingDomainRequest!DNS	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alta
UnauthorizedAccess:Runtime/MetadataDNSRebind	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alta
UnauthorizedAccess:Runtime/TorClient	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alta
UnauthorizedAccess:Runtime/TorRelay	Instancia, clúster de EKS, clúster de ECS o contenedor	Supervisión en tiempo de ejecución	Alta
Backdoor:EC2/C&CActivity.B	EC2	Logs de flujo de VPC	Alta

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Backdoor:EC2/DenialOfService.Dns	EC2	Logs de flujo de VPC	Alta
Backdoor:EC2/DenialOfService.Tcp	EC2	Logs de flujo de VPC	Alta
Backdoor:EC2/DenialOfService.Udp	EC2	Logs de flujo de VPC	Alta
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	EC2	Logs de flujo de VPC	Alta
Backdoor:EC2/DenialOfService.UnusualProtocol	EC2	Logs de flujo de VPC	Alta
Backdoor:EC2/Spambot	EC2	Logs de flujo de VPC	Medio
Behavior:EC2/NetworkPortUnusual	EC2	Logs de flujo de VPC	Medio
Behavior:EC2/TrafficVolumeUnusual	EC2	Logs de flujo de VPC	Medio
CryptoCurrency:EC2/BitcoinTool.B	EC2	Logs de flujo de VPC	Alta

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
DefenseEvasion:EC2/UnusualDNSResolver	EC2	Logs de flujo de VPC	Medio
DefenseEvasion:EC2/UnusualDoHActivity	EC2	Logs de flujo de VPC	Medio
DefenseEvasion:EC2/UnusualDoTActivity	EC2	Logs de flujo de VPC	Medio
Impact:EC2/PortSweep	EC2	Logs de flujo de VPC	Alta
Impact:EC2/WinRMBruteForce	EC2	Logs de flujo de VPC	Baja
Recon:EC2/PortProbeEMRUnprotectedPort	EC2	Logs de flujo de VPC	Alta
Recon:EC2/PortProbeUnprotectedPort	EC2	Logs de flujo de VPC	Baja
Recon:EC2/Portscan	EC2	Logs de flujo de VPC	Medio

Tipo de resultado	Tipo de recurso	Origen de datos o característica fundamental	Gravedad del resultado
Trojan:EC2/BlackholeTraffic	EC2	Logs de flujo de VPC	Medio
Trojan:EC2/DropPoint	EC2	Logs de flujo de VPC	Medio
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	EC2	Logs de flujo de VPC	Medio
UnauthorizedAccess:EC2/RDPBruteForce	EC2	Logs de flujo de VPC	Baja
UnauthorizedAccess:EC2/SSHBruteForce	EC2	Logs de flujo de VPC	Baja
UnauthorizedAccess:EC2/TorClient	EC2	Logs de flujo de VPC	Alta
UnauthorizedAccess:EC2/TorRelay	EC2	Logs de flujo de VPC	Alta

Gestión de los GuardDuty hallazgos de Amazon

GuardDuty ofrece varias funciones importantes que le ayudarán a clasificar, almacenar y gestionar sus hallazgos. Estas características le ayudarán a adaptar los resultados a su entorno específico, reducir el ruido de los resultados de bajo valor y centrarse en amenazas para su entorno único de AWS . Revisa los temas de esta página para entender cómo puedes usar estas funciones para aumentar el valor GuardDuty de los hallazgos.

Temas:

Creación de respuestas personalizadas a GuardDuty los hallazgos con Amazon CloudWatch Events

Configura notificaciones automáticas para GuardDuty los hallazgos a través de los CloudWatch eventos de Amazon. También puedes automatizar otras tareas a través de CloudWatch Events para ayudarte a responder a los hallazgos.

Descripción de CloudWatch los registros y los motivos por los que se omiten recursos durante el análisis de Malware Protection

Descubra cómo puede auditar los CloudWatch registros para protegerse contra el GuardDuty malware y cuáles son los motivos por los que la instancia de Amazon EC2 o los volúmenes de Amazon EBS afectados pueden haberse omitido durante el proceso de escaneo.

Denunciar falsos positivos en GuardDuty Malware Protection

Obtenga información sobre la experiencia de los falsos positivos en GuardDuty Malware Protection y cómo puede denunciar las detecciones de amenazas por falsos positivos.

Panel Resumen

El panel de resumen proporciona una vista agregada de los GuardDuty hallazgos generados Cuenta de AWS en su región actual. En la actualidad, el panel admite un volumen de hasta 5000 resultados. Sin embargo, puede ver los detalles de todos los hallazgos en la página de hallazgos de la GuardDuty consola GetFindingso bien ListFindings.

> **Note**
>
> El resumen de los hallazgos solo está disponible en la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

Las siguientes secciones lo ayudarán a acceder al panel y a comprender sus componentes.

Contenido

Acceso al panel Resumen

En la GuardDuty consola, el panel de resumen muestra una vista consolidada de los últimos 5000 GuardDuty hallazgos generados en la región actual.

Acceso al panel Resumen

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, elija Resumen. Al abrir la consola, se GuardDuty muestra el panel de resumen.
3. De forma predeterminada, el resumen se muestra para el mismo día (Hoy). La GuardDuty consola ofrece una opción para ver el resumen de los últimos 2 días, los últimos 7 días y los últimos 30 días. Para cambiar el intervalo de tiempo predeterminado, elija una de las opciones del menú desplegable que está sobre el panel Información general.
4. Filtración de los datos

   - Los widgets Cuentas con la mayoría de los resultados, Recursos con la mayoría de los resultados y Resultados menos frecuentes lo ayudan a filtrar los datos en función del nivel de gravedad de los resultados.
   - El widget Recursos con la mayoría de los resultados también lo ayuda a filtrar los datos en función del tipo de recurso potencialmente afectado.

     Una cuenta de miembro puede ver los detalles del recurso potencialmente afectado que pertenece a su propia cuenta. Si es GuardDuty administrador de una cuenta y desea ver los detalles del recurso potencialmente afectado, abra la GuardDuty consola con las credenciales de la cuenta de miembro asociada.
5. Cobertura del plan de protección

   La cobertura del plan de protección proporciona el recuento de las cuentas de los miembros que se han activado GuardDuty en su organización. Las estadísticas solo son visibles para el GuardDuty administrador delegado.

Descripción del panel Resumen

En el panel Resumen se muestran los datos agregados en las siguientes secciones. Antes de proceder a ver y comprender el resumen, asegúrese de elegir la Región de AWS que desee en el selector de región situado en la parte superior de la consola. Además, asegúrese de elegir el

intervalo de tiempo deseado en el menú desplegable situado encima del panel Información general. Si no se generaron resultados para los parámetros elegidos, no habrá datos disponibles en ninguno de los widgets.

De un volumen de hasta 5000 GuardDuty hallazgos, el panel de resumen, con las cuentas con la mayoría de los hallazgos, los recursos con el mayor número de hallazgos y los hallazgos menos frecuentes, muestra los datos basados en los 5 resultados principales. Para un análisis más profundo, consulta la página de resultados de la GuardDuty consola.

Información general

En esta sección se proporcionan los siguientes datos:

- Resultados totales: indica el número total de resultados generados en su cuenta en la región actual.
- Hallazgos de gravedad alta: indica el número de GuardDuty hallazgos que tienen un nivel de gravedad alto en la región actual.
- Recursos con resultados: indica el número de recursos que están asociados a un resultado y que están potencialmente en peligro.
- Cuentas con resultados: indica el número de cuentas en las que se generó al menos un resultado. Si es una cuenta independiente, el valor de este campo es 1.

En el caso de los intervalos de tiempo 7 últimos días y 30 últimos días, en el panel Información general se puede mostrar la diferencia porcentual entre los resultados generados semana tras semana (WoW) o mes tras mes (MoM), respectivamente. Si no se generó ningún resultado la semana o el mes anterior y no hay datos para comparar, es posible que la diferencia porcentual no esté disponible.

Si eres GuardDuty administrador de una cuenta, todos estos campos proporcionan los datos resumidos de todas las cuentas de los miembros de tu organización.

Resultados por gravedad

En esta sección se muestra un gráfico de barras con el número total de resultados en el intervalo de tiempo elegido. Puede ver el número de resultados de gravedad baja, media o alta generados en una fecha específica dentro del intervalo de tiempo elegido.

Tipos de resultados más comunes

En esta sección, se muestra en un gráfico circular los cinco tipos de hallazgos más comunes, observados a partir de un volumen de hasta los últimos 5000 GuardDuty hallazgos generados en la región actual. En este gráfico circular se muestran los siguientes datos cuando se pasa el ratón por encima de cada sector:

- Recuento de resultados: indica el número de veces que se ha generado este resultado en el intervalo de tiempo elegido.
- Gravedad: indica el nivel de gravedad del resultado, por ejemplo, media y alta.
- Porcentaje: indica la proporción de este tipo de resultado en el gráfico circular.
- Generado más recientemente: indica cuánto tiempo ha pasado desde que se generó este tipo de resultado por última vez.

Cuentas con la mayoría de los resultados

En esta sección se proporcionan los siguientes datos:

- Cuenta: indica el Cuenta de AWS identificador en el que se generó el hallazgo.
- Recuento de resultados: indica el número de veces que se generó un resultado para este ID de cuenta.
- Generado más recientemente: indica cuánto tiempo ha pasado desde que se generó un tipo de resultado por última vez para este ID de cuenta.
- Gravedad alta: de forma predeterminada, los datos se muestran para los tipos de resultados de gravedad alta. Las opciones posibles para este campo son Gravedad alta, Gravedad media y Todas las gravedades.

Recursos con resultados

En esta sección se proporcionan los siguientes datos:

- Recurso: indica el tipo de recurso potencialmente afectado y, si este recurso pertenece a su cuenta, puede acceder al enlace rápido para ver los detalles del recurso. Si es GuardDuty administrador de una cuenta, puede ver los detalles del recurso potencialmente afectado accediendo a la GuardDuty consola con las credenciales de la cuenta de miembro a la que pertenece este recurso.

- Cuenta: indica el Cuenta de AWS ID al que pertenece este recurso.
- Recuento de resultados: indica el número de veces que este recurso se asoció a un resultado.
- Generado más recientemente: indica cuánto tiempo ha pasado desde que se generó por última vez un tipo de resultado asociado a este recurso.
- Todos los tipos de recursos: de forma predeterminada, los datos se muestran para todos los tipos de recursos. Al usar el menú desplegable, puede ver los datos de un tipo de recurso específico, como Instance AccessKey, Lambda y otros.
- Gravedad alta: de forma predeterminada, los datos se muestran para los tipos de resultados de gravedad alta. Al usar el menú desplegable, puede ver los datos de otros niveles de gravedad. Las opciones posibles son Gravedad alta, Gravedad media y Todas las gravedades.

Resultados menos frecuentes

En esta sección se proporcionan los detalles de los tipos de búsqueda que no se generan con frecuencia en su AWS entorno. Esta información puede ayudarlo a investigar un patrón de amenazas emergentes en su entorno y a tomar medidas al respecto. En la tabla se muestran los siguientes datos:

- Tipo de resultado: indica el nombre del tipo de resultado.
- Recuento de resultados: indica el número de veces que se generó este tipo de resultado en el intervalo de tiempo elegido.
- Generado más recientemente: indica cuánto tiempo ha pasado desde que se generó este tipo de resultado por última vez.
- Gravedad alta: de forma predeterminada, los datos se muestran para los tipos de resultados de gravedad alta. Las opciones posibles para este campo son Gravedad alta, Gravedad media y Todas las gravedades.

Cobertura del plan de protección

En esta sección se indica el número de cuentas de miembros activas que pertenecen a su organización y que han habilitado una o más funciones y funciones adicionales (según proceda) en la configuración actual Región de AWS.

Solo un GuardDuty administrador delegado puede ver las estadísticas de las cuentas de los miembros de su organización. Si una función no está configurada, elija Configurar en la columna Acciones.

Al crear una nueva AWS organización, es posible que se tarden hasta 24 horas en generar las estadísticas de toda la organización.

Envío de comentarios sobre el panel Resumen

GuardDuty te anima a que envíes comentarios sobre la usabilidad, las funciones y el rendimiento del panel de resumen. Esto nos ayudará a mejorar el panel.

Envío de comentarios sobre el panel Resumen

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, elija Resumen. Al abrir la GuardDuty consola, se muestra el panel de resumen.
3. Elija Comentarios en la esquina superior derecha del panel. Se abrirá un formulario. Después de enviar los comentarios, seleccione Enviar.

Filtrado de hallazgos

Un filtro de resultado le permite ver los resultados que coinciden con los criterios que especifique y filtrar los resultados que no coincidan. Puedes crear fácilmente filtros de búsqueda con la GuardDuty consola de Amazon o puedes crearlos con la CreateFilterAPI mediante JSON. Consulte las siguientes secciones para entender cómo crear un filtro en la consola. Para utilizar estos filtros con el objetivo de archivar automáticamente los resultados entrantes, consulte Reglas de supresión.

Crear filtros en la GuardDuty consola

Los filtros de búsqueda se pueden crear y probar a través de la GuardDuty consola. Puede guardar los filtros creados a través de la consola para utilizarlos en reglas de supresión o futuras operaciones de filtro. Un filtro se compone de al menos un criterio de filtro, que consiste en un atributo de filtro emparejado con al menos un valor.

Cuando cree filtros, tenga en cuenta lo siguiente:

- Los filtros no aceptan comodines.
- Puede especificar un mínimo de un atributo y un máximo de 50 atributos como criterios para un determinado filtro.
- Cuando se utiliza la condición igual que o no es igual que para filtrar por un valor de atributo, como ID de cuenta, se puede especificar un máximo de 50 valores.

- Cada atributo de los criterios de filtro se evalúa como un operador AND. Se evalúan varios valores para el mismo atributo como AND/OR.

Filtrado de resultados (consola)

1. Selecciona Añadir criterios de filtro sobre la lista de GuardDuty resultados que se muestra.
2. En la lista de atributos ampliada, seleccione los atributos que desea especificar como criterios del filtro, como ID de cuenta o Tipo de acción.

   > **Note**
   >
   > Para obtener una lista de atributos que puede utilizar para crear criterios de filtro, consulte la tabla de atributos de filtro que se muestra en esta página.

3. En el campo de texto que se muestra, especifique un valor para cada atributo seleccionado y, a continuación, seleccione Aplicar.

   > **Note**
   >
   > Después de aplicar un filtro, para convertirlo a fin de excluir los resultados que coincidan con él, elija el punto negro que aparece a la izquierda del nombre del filtro. Lo que sucede en realidad es que se crea un filtro "distinto de" para el atributo seleccionado.

4. Para guardar los atributos especificados y sus valores (criterios de filtro) como un filtro, seleccione Save (Guardar). Introduzca el nombre y la descripción del filtro y, a continuación, elija Listo.

Filtro de atributos

Al crear filtros u ordenar los resultados mediante las operaciones de la API, debe especificar los criterios de filtro en JSON. Estos criterios de filtro se correlacionan con el JSON de los detalles de un resultado. La siguiente tabla contiene una lista de los nombres que se muestran en la consola para los atributos del filtro y sus nombres de campo JSON equivalentes.

Nombre de campo de la consola	Nombre del campo JSON
ID de cuenta	accountId

Nombre de campo de la consola	Nombre del campo JSON
ID del resultado	id
Región	region
Gravedad	severity Si se utiliza `severity` con la API, la AWS CLI o AWS CloudFormation, tendrá un valor numérico. Para más información, consulte findingCriteria.
Tipo de búsqueda	type
Actualizado a las	updatedAt
ID de clave de acceso)	recurso. accessKeyDetails. accessKeyId
ID principal	recurso. accessKeyDetails. ID principal
Nombre de usuario	recurso. accessKeyDetails.nombre de usuario
Tipo de usuario	recurso. accessKeyDetails.Tipo de usuario
ID del perfil de instancia de IAM	Detalles del recurso. Instance. iamInstanceProfile.id
ID de instancia	resource.instanceDetails.instanceId
ID de imagen de la instancia	resource.instanceDetails.imageId
Clave de etiqueta de instancia	resource.instanceDetails.tags.key
Valor de etiqueta de instancia	resource.instanceDetails.tags.value
Dirección IPv6	resource.instanceDetails.networkInterfaces.ipv6Addresses
Dirección IPv4 privada	resource.instanceDetails.NetworkInterfaces. privateIpAddresses. privateIpAddress

Nombre de campo de la consola	Nombre del campo JSON
Nombre DNS público	Resource.InstanceDetails.Interfaces de red. publicDnsName
IP pública	resource.instanceDetails.networkInterfaces.publicIp
ID de grupo de seguridad	resource.instanceDetails.networkInterfaces.securityGroups.groupId
Nombre del grupo de seguridad	resource.instanceDetails.networkInterfaces.securityGroups.groupName
ID de subred	resource.instanceDetails.networkInterfaces.subnetId
VPC ID	resource.instanceDetails.networkInterfaces.vpcId
ARN de Outpost	resource.instanceDetails.outpostARN
Tipo de recurso	resource.resourceType
Permisos de bucket	resource.s3BucketDetails. Acceso público. Permiso efectivo
Nombre del bucket	recurso.s3 BucketDetails .name
Clave de la etiqueta del bucket	recurso.s3 BucketDetails .tags.key
valor de la etiqueta del bucket	recurso.s3 BucketDetails .tags.value
Tipo de bucket	recursos.s3 BucketDetails .type
Tipo de acción	service.action.actionType
API llamada	servicio.acción. awsApiCallAcción.api
Tipo de intermediario de la API	servicio.acción. awsApiCallAction.CallerType

Nombre de campo de la consola	Nombre del campo JSON
Código de error de la API	servicio.acción. awsApiCallAcción. Código de error
Ciudad del intermediario de la API	servicio.acción. awsApiCallAcción. remoteIpDetails.city.CityName
País del intermediario de la API	service.action. awsApiCallAcción. remoteIpDetails.país.Nombre del país
Dirección IPv4 del intermediario de la API	servicio.acción. awsApiCallAcción. remoteIpDetails.Dirección IP V4
ID de ASN del intermediario de la API	servicio.acción. awsApiCallAcción. remoteIpDetails.organization.asn
Nombre ASN del intermediario de la API	servicio.acción. awsApiCallAcción. remoteIpDetails.Organización. Asnorg
Nombre del servicio del intermediario de la API	servicio.acción. awsApiCallAction.serviceName
Dominio de la solicitud DNS	servicio.acción. dnsRequestAction.dominio
Sufijo de dominio de solicitud de DNS	service.action. dnsRequestAction. domainWithSuffix
Conexión de red bloqueada	servicio.acción. networkConnectionAction.bloqueado
Dirección de la conexión de red	servicio.acción. networkConnectionAction. Dirección de conexión
Puerto local de la conexión de red	servicio.acción. networkConnectionAction. localPortDetails.port
Protocolo de conexión de red	servicio.acción. networkConnectionAction.protocolo

Nombre de campo de la consola	Nombre del campo JSON
Ciudad de la conexión de red	servicio.acción. networkConnectionAction. remoteIpDetails.city.cityname
País de la conexión de red	service.action. networkConnectionAction. remoteIpDetails. País. Nombre del país
Dirección IPv4 remota de la conexión de red	servicio.acción. networkConnectionAction. remoteIpDetails.Dirección IP V4
ID de ASN de la IP remota de la conexión de red	servicio.acción. networkConnectionAction. remoteIpDetails.organization.asn
Nombre ASN de la IP remota de la conexión de red	servicio.acción. networkConnectionAction. remoteIpDetails. Organización. Asnorg
Puerto remoto de la conexión de red	servicio.acción. networkConnectionAction. remotePortDetails.port
Cuenta remota afiliada	servicio.acción. awsApiCallAcción. remoteAcc ountDetails... afiliado.
Dirección IPv4 de la persona que llama a la API de Kubernetes	servicio.acción. kubernetesApiCallAcción. remoteIpDetails.Dirección IP V4
Espacio de nombres de Kubernetes	servicio.acción. kubernetesApiCallAction.nam espace
ID de ASN que llama a la API de Kubernetes	service.action. kubernetesApiCallAcción. remoteIpDetails.organization.asn
URI de solicitud de llamada a la API de Kubernetes	servicio.acción. kubernetesApiCallAcción.URI de solicitud
Código de estado de la API de Kubernetes	service.action. kubernetesApiCallAcción. Código de estado
Dirección IPv4 local de conexión de red	servicio.acción. networkConnectionAction. localIpDetails.Dirección IP V4

Nombre de campo de la consola	Nombre del campo JSON
Protocolo	servicio.acción. networkConnectionAction.protocolo
Nombre del servicio de llamada a la API	servicio.acción. awsApiCallAction.serviceName
ID de cuenta de la persona que llama a la API	servicio.acción. awsApiCallAcción. remoteAccountDetails. ID de cuenta
Nombre de la lista de amenazas	Servicio. Información adicional. threatListName
Rol de recurso	service.resourceRole
Nombre del clúster de EKS	recurso. eksClusterDetails.nombre
Nombre de la carga de trabajo de Kubernetes	resource.Detalles de Kubernetes. kubernetesWorkloadDetails.nombre
Nombre de espacio de la carga de trabajo de Kubernetes	resource.Detalles de Kubernetes. kubernetesWorkloadDetails.espacio de nombres
Nombre de usuario de Kubernetes	Resource.Detalles de Kubernetes. kubernetesUserDetails.nombre de usuario
Imagen del contenedor de Kubernetes	recurso. Detalles de Kubernetes. kubernetesWorkloadDetails.contenedores.imagen
Prefijo de la imagen del contenedor de Kubernetes	Resource.Detalles de Kubernetes. kubernetesWorkloadDetails.containers.prefijo de imagen
ID de análisis	servicio. ebsVolumeScanDetalles. Scanid
Nombre de la amenaza	servicio. ebsVolumeScanDetalles. Detecciones de escaneo. threatDetectedByNombre.ThreatNames.name
Gravedad de la amenaza	servicio. ebsVolumeScanDetalles. Detecciones de escaneo. threatDetectedByNombre.ThreatNames.Severity

Nombre de campo de la consola	Nombre del campo JSON
SHA de archivo	servicio. ebsVolumeScanDetalles. Detecciones de escaneo. threatDetectedByNombre.threatnames.filepaths.hash
Nombre del clúster de ECS	recurso. ecsClusterDetails.nombre
Imagen del contenedor de ECS	recurso. ecsClusterDetails.taskdetails.containers.image
ARN de definición de tarea de ECS	recurso. ecsClusterDetails.taskdetails.definitionARN
Imagen de contenedor independiente	resource.containerDetails.image
ID de instancia de base de datos	recurso. rdsDbInstanceDetalles. dbInstanceIdentifier
ID de clúster de base de datos	recurso. rdsDbInstanceDetalles. dbClusterIdentifier
Motor de base de datos	recurso. rdsDbInstanceDetalles. Motor
Usuario de base de datos	recurso. rdsDbUserDetalles. Usuario
Clave de etiqueta de instancia de base de datos	recurso. rdsDbInstanceDetails.tags.key
Valor de etiqueta de instancia de base de datos	recurso. rdsDbInstanceDetalles.Etiquetas.Valor
SHA-256 ejecutable	service.runtimeDetails.process.executableSha256
Process name (Nombre del proceso)	service.runtimeDetails.process.name
Ruta de ejecución	service.runtimeDetails.process.executablePath
Nombre de la función Lambda	resource.lambdaDetails.functionName
ARN de la función Lambda	resource.lambdaDetails.functionArn

Nombre de campo de la consola	Nombre del campo JSON
Clave de etiqueta de la función de Lambda	resource.lambdaDetails.tags.key
Valor de etiqueta de la función de Lambda	resource.lambdaDetails.tags.value
Dominio de la solicitud DNS	servicio.acción. dnsRequestAction. domainWithSuffix

Reglas de supresión

Una regla de supresión es un conjunto de criterios, que consta de un atributo de filtro emparejado con un valor, utilizado para filtrar resultados mediante el archivado automático de resultados nuevos que coinciden con los criterios especificados. Las reglas de supresión se pueden utilizar para filtrar los resultados de bajo valor, los resultados positivos falsos o las amenazas sobre las que no se pretende actuar, a fin de facilitar el reconocimiento de las amenazas de seguridad que tienen el mayor impacto en su entorno.

Después de crear una regla de supresión, los nuevos resultados que coincidan con los criterios definidos en la regla se archivan automáticamente siempre que la regla de supresión esté en su lugar. Puede utilizar un filtro existente para crear una regla de supresión o crear una regla de supresión a partir de una nuevo filtro que defina. Puede configurar reglas de supresión para suprimir tipos de hallazgos completos o definir criterios de filtro más detallados para suprimir sólo instancias específicas de un tipo de hallazgo determinado. Las reglas de supresión se pueden editar en cualquier momento.

Los hallazgos suprimidos no se envían a AWS Security Hub Amazon Simple Storage Service, Amazon Detective o Amazon EventBridge, lo que reduce el ruido de las búsquedas si se consumen GuardDuty los hallazgos a través de Security Hub, un SIEM de terceros u otras aplicaciones de alerta y emisión de tickets. Si la has activadoGuardDuty Protección contra malware, los GuardDuty resultados suprimidos no iniciarán un análisis de software malicioso.

GuardDuty sigue generando hallazgos incluso cuando se ajustan a tus reglas de supresión; sin embargo, esos hallazgos se marcan automáticamente como archivados. El hallazgo archivado se almacena GuardDuty durante 90 días y se puede ver en cualquier momento durante ese período. Para ver los hallazgos suprimidos en la GuardDuty consola, selecciona Archivado en la tabla de hallazgos o a través de la GuardDuty API utilizando la ListFindingsAPI con un `findingCriteria` criterio de `service.archived` igual a verdadero.

> **Note**
>
> En un entorno con varias cuentas, solo el GuardDuty administrador puede crear reglas de supresión.

Casos de uso comunes para reglas de supresión y ejemplos

Los siguientes tipos de resultados tienen casos de uso habituales para aplicar reglas de supresión. Seleccione el nombre del resultado para obtener más información sobre él o consulte la información para crear una regla de supresión para ese tipo de resultado desde la consola.

> **Important**
>
> GuardDuty recomienda crear reglas de supresión de forma reactiva y solo para los casos en los que se hayan identificado falsos positivos de forma repetida.

- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS: utilice una regla de supresión para archivar automáticamente resultados generados cuando se configuran las redes de la VPC para dirigir el tráfico de Internet a fin de que salga desde una puerta de enlace en las instalaciones en lugar de una puerta de enlace de Internet de VPC.

  Este resultado se genera cuando la red está configurada para dirigir el tráfico de Internet de tal forma que salga por una puerta de enlace en las instalaciones y no por una puerta de enlace de Internet (IGW) de la VPC. Las configuraciones comunes, como el uso de AWS Outposts o de conexiones de VPN de la VPC, pueden generar tráfico dirigido de esta manera. Si se trata de un comportamiento esperado, se recomienda utilizar reglas de supresión en y crear una regla que conste de dos criterios de filtro. El primer criterio es Tipo de resultado, que debería ser `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. El segundo criterio de filtro es la Dirección IPv4 de la persona que llama a la API con el rango de direcciones IP o CIDR de su puerta de enlace de Internet en las instalaciones. En el siguiente ejemplo, se representa el filtro que utilizaría para suprimir este tipo de resultado en función de la dirección IP de la persona que llama a la API.

```
Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
 API caller IPv4 address: 198.51.100.6
```

> **Note**
>
> Para incluir varias IP de personas que llaman a la API, puede agregar un nuevo filtro de direcciones IPv4 de las personas que llaman a la API para cada una de ellas.

- Recon:EC2/Portscan: utilice una regla de supresión para archivar automáticamente los resultados cuando utilice una aplicación de evaluación de vulnerabilidades.

  La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `Recon:EC2/Portscan`. El segundo criterio de filtro debe coincidir con la instancia o instancias que alojan estas herramientas de evaluación de vulnerabilidades. Puede utilizar el atributo ID de imagen de instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. En el siguiente ejemplo, se representa el filtro que utilizaría para suprimir este tipo de resultado en función de las instancias con una determinada AMI.

  ```
  Finding type: Recon:EC2/Portscan Instance image ID: ami-999999999
  ```

- UnauthorizedAccess:EC2/SSHBruteForce: utilice una regla de supresión para archivar automáticamente los resultados cuando tengan como objetivo las instancias de bastión.

  Si el objetivo del intento de fuerza bruta es un bastión anfitrión, esto puede representar el comportamiento esperado en su entorno. AWS Si este es el caso, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `UnauthorizedAccess:EC2/SSHBruteForce`. El segundo criterio de filtro debe coincidir con la instancia o instancias que sirven como host de bastión. Puede utilizar el atributo ID de imagen de la instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. En el siguiente ejemplo, se representa el filtro que utilizaría para suprimir este tipo de resultado en función de las instancias con un determinado valor de etiqueta de instancia.

  ```
  Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
  ```

- Recon:EC2/PortProbeUnprotectedPort: utilice una regla de supresión para archivar automáticamente los resultados cuando tengan como objetivo las instancias que se hayan visto expuestas de manera intencional.

Puede haber casos en los que las instancias se exponen de forma intencionada, por ejemplo, si están alojando servidores web. Si este es el caso de su AWS entorno, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `Recon:EC2/PortProbeUnprotectedPort`. El segundo criterio de filtro debe coincidir con la instancia o instancias que sirven como host de bastión. Puede utilizar el atributo ID de imagen de instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. En el siguiente ejemplo, se representa el filtro que utilizaría para suprimir este tipo de resultado en función de las instancias con una determinada clave de etiqueta de instancia en la consola.

```
Finding type: Recon:EC2/PortProbeUnprotectedPort Instance tag key: prod
```

Reglas de supresión recomendadas para los resultados de la supervisión en tiempo de ejecución de EKS

- PrivilegeEscalation:Runtime/DockerSocketAccessed se genera cuando un proceso dentro de un contenedor se comunica con el socket de Docker. Es posible que haya contenedores de su entorno que necesiten acceso al socket de Docker por motivos legítimos. El acceso desde dichos contenedores generará resultados PrivilegeEscalation:Runtime/DockerSocketAccessed. Si este es el caso de su AWS entorno, le recomendamos que configure una regla de supresión para este tipo de hallazgo. Los primeros criterios deben utilizar el campo Tipo de resultado con un valor equivalente a `PrivilegeEscalation:Runtime/DockerSocketAccessed`. El segundo criterio de filtro es el campo Ruta ejecutable con un valor igual al `executablePath` del proceso en el resultado generado. De manera alternativa, el segundo criterio de filtro puede utilizar el campo SHA-256 ejecutable con un valor igual al `executableSha256` del proceso en el resultado generado.
- Los clústeres de Kubernetes ejecutan sus propios servidores DNS como pods; por ejemplo, `coredns`. Por lo tanto, para cada búsqueda de DNS desde un pod, GuardDuty captura dos eventos de DNS: uno del pod y otro del pod del servidor. Esto puede generar duplicados para los siguientes resultados de DNS:
  - Backdoor:Runtime/C&CActivity.B!DNS
  - CryptoCurrency:Runtime/BitcoinTool.B!DNS
  - Impact:Runtime/AbusedDomainRequest.Reputation

- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS

Los resultados duplicados incluirán los detalles del pod, el contenedor y el proceso que corresponden al pod de su servidor DNS. Puede configurar una regla de supresión para suprimir estos resultados duplicados utilizando estos campos. El primer criterio de filtro debe utilizar el campo Tipo de resultado con un valor igual a un tipo de resultado de DNS de la lista de resultados proporcionada anteriormente en esta sección. El segundo criterio de filtro puede ser Ruta ejecutable con un valor igual al `executablePath` del servidor DNS o SHA-256 ejecutable con un valor igual al `executableSHA256` del servidor DNS en el resultado generado. Como tercer criterio de filtro opcional, puede utilizar el campo Imagen del contenedor de Kubernetes con un valor igual al de la imagen del contenedor del pod del servidor DNS en el resultado generado.

Para crear reglas de supresión en GuardDuty

Elija el método de acceso que prefiera para crear o gestionar las reglas de supresión GuardDuty.

Console

Puede visualizar, crear y gestionar las reglas de supresión mediante la GuardDuty consola. Las reglas de supresión se generan de la misma manera que los filtros y los filtros guardados existentes se pueden utilizar como reglas de supresión. Para obtener más información acerca de la creación de filtros, consulte Filtrado de hallazgos.

Para crear una regla de supresión mediante la consola:

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En la página Resultados, seleccione Suprimir resultados para abrir el panel de reglas de supresión.

3. Para abrir el menú de criterios de filtro, introduzca los **`filter criteria`** en el campo Agregar criterios de filtro. Puede elegir un criterio de la lista. Introduzca un valor válido para el criterio elegido.

   > **Note**
   >
   > Para determinar el valor válido, consulte la tabla de resultados y elija un resultado que desee suprimir. Revise sus detalles en el panel de resultados.

   Puede agregar varios criterios de filtro y asegurarse de que solo aparezcan en la tabla los resultados que desee suprimir.
4. Escriba un Nombre y una Descripción para la regla de supresión. Los caracteres válidos incluyen los caracteres alfanuméricos, el punto (.), el guion (-), el guion bajo (_) y espacios.
5. Seleccione Guardar.

También puede crear una regla de supresión a partir de un filtro guardado existente. Para obtener más información acerca de la creación de filtros, consulte Filtrado de hallazgos.

Para crear una regla de supresión a partir de un filtro guardado:

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En la página Resultados, seleccione Suprimir resultados para abrir el panel de reglas de supresión.
3. En el menú desplegable Reglas guardadas, seleccione un filtro guardado.
4. También puede agregar nuevos criterios de filtro. Puede omitir este paso si no necesita criterios de filtro adicionales.

   Para abrir el menú de criterios de filtro, introduzca los **`filter criteria`** en el campo Agregar criterios de filtro. Puede elegir un criterio de la lista. Introduzca un valor válido para el criterio elegido.

   > **Note**
   >
   > Para determinar el valor válido, consulte la tabla de resultados y elija un resultado que desee suprimir. Revise sus detalles en el panel de resultados.

5. Escriba un Nombre y una Descripción para la regla de supresión. Los caracteres válidos incluyen los caracteres alfanuméricos, el punto (.), el guion (-), el guion bajo (_) y espacios.
6. Seleccione Guardar.

Para eliminar una regla de supresión:

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En la página Resultados, seleccione Suprimir resultados para abrir el panel de reglas de supresión.
3. En el menú desplegable Reglas guardadas, seleccione un filtro guardado.
4. Elija Delete rule (Eliminar regla).

API/CLI

Para crear una regla de supresión mediante una API:

1. También puede crear reglas de supresión a través de la API CreateFilter. Para ello, especifique los criterios de filtro en un archivo JSON según el formato del ejemplo que se detalla a continuación. El siguiente ejemplo suprimirá cualquier resultado de baja gravedad no archivado que contenga una solicitud de DNS al dominio test.example.com. Para los resultados de gravedad media, la lista de entrada será `["4", "5", "7"]`. Para los resultados de gravedad alta, la lista de entrada será `["6", "7", "8"]`. También puede filtrar en función de cualquier valor de la lista.

```
{
    "Criterion": {
        "service.archived": {
            "Eq": [
                "false"
            ]
        },
        "service.action.dnsRequestAction.domain": {
            "Eq": [
                "test.example.com"
            ]
        },
        "severity": {
            "Eq": [
```

```
                "1",
                "2",
                "3"
            ]
        }
    }
}
```

Para obtener una lista de los nombres de campo JSON y su equivalente de consola, consulte Filtro de atributos.

Para probar sus criterios de filtro, utilice el mismo criterio de JSON en la API ListFindings y confirme que se hayan seleccionado los resultados correctos. Para probar tus criterios de filtro, AWS CLI sigue el ejemplo con tu propio DetectoriD y un archivo.json.

Para encontrar los de `detectorId` tu cuenta y región actuales, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
finding-criteria file://criteria.json
```

2. Cargue el filtro para utilizarlo como regla de supresión con la API CreateFilter o mediante la CLI de AWS según el ejemplo siguiente con su propio ID de detector, un nombre para la regla de supresión y un archivo .json.

   Para encontrar la correspondiente `detectorId` a tu cuenta y a la región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty create-filter --action ARCHIVE --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria
 file://criteria.json
```

Puede ver una lista de sus filtros mediante programación con la API ListFilter. Para ver los detalles de un filtro individual, proporcione el nombre del filtro a la API GetFilter. Actualice los filtros mediante la API UpdateFilter o elimínelos con ayuda de la API DeleteFilter.

Uso de listas de IP de confianza y listas de amenazas

Amazon GuardDuty supervisa la seguridad de su AWS entorno mediante el análisis y el procesamiento de los registros de flujo de VPC, los registros de AWS CloudTrail eventos y los registros de DNS. Puede personalizar este alcance de monitoreo configurándolo GuardDuty para detener las alertas de IP confiables de sus propias listas de IP confiables y alertar sobre IP maliciosas conocidas de sus propias listas de amenazas.

Las listas de IP de confianza y de amenazas se aplican únicamente al tráfico destinado a direcciones IP direccionables públicamente. Los efectos de una lista se aplican a todos los registros de flujo de la VPC y a CloudTrail las conclusiones, pero no a las conclusiones del DNS.

GuardDuty se puede configurar para usar los siguientes tipos de listas.

Lista de IP de confianza

Las listas de IP de confianza se componen de direcciones IP en las que ha confiado para una comunicación segura con su AWS infraestructura y sus aplicaciones. GuardDuty no genera un registro de flujo de VPC ni encuentra CloudTrail direcciones IP en listas de IP confiables. Puede incluir un máximo de 2000 direcciones IP y rangos de CIDR en una única lista de IP de confianza. Solo puede tener una lista de IP de confianza cargada a la vez por cuenta y región de AWS .

Lista de IP de amenazas

Las listas de amenazas están formadas por direcciones IP malintencionadas conocidas. La inteligencia sobre amenazas de terceros puede ofrecer esta lista, que también se puede crear específicamente para su organización. Además de generar hallazgos debido a una actividad potencialmente sospechosa, GuardDuty también genera hallazgos basados en estas listas de amenazas. Puede incluir un máximo de 250 000 direcciones IP y rangos de CIDR en una sola lista de amenazas. GuardDuty solo genera resultados en función de una actividad que incluya direcciones IP y rangos de CIDR en sus listas de amenazas; los hallazgos no se generan en función de los nombres de dominio. En un momento dado, puede cargar hasta seis listas de amenazas Cuenta de AWS por región.

> **Note**
>
> Si incluye la misma IP en una lista de IP de confianza y una lista de amenazas, la lista de IP de confianza la procesará primero y no generará ningún resultado.

En entornos con varias cuentas, solo los usuarios de cuentas de GuardDuty administrador pueden añadir y gestionar listas de IP fiables y listas de amenazas. Las listas de direcciones IP fiables y las listas de amenazas que carga la cuenta de administrador están sujetas a la GuardDuty funcionalidad de las cuentas de los miembros. En otras palabras, en las cuentas de los miembros GuardDuty genera resultados basados en actividades que involucran direcciones IP maliciosas conocidas de las listas de amenazas de la cuenta de administrador, y no genera hallazgos basados en actividades que involucran direcciones IP de las listas de IP confiables de la cuenta de administrador. Para obtener más información, consulte Administrar varias cuentas en Amazon GuardDuty.

Formatos de las listas

GuardDuty acepta listas en los siguientes formatos.

El tamaño máximo de cada archivo que aloja la lista de IP de confianza o la lista de IP de amenazas es de 35 MB. En las listas de IP de confianza y las listas de IP de amenazas, las direcciones IP y los rangos de CIDR deben aparecer de uno en uno en cada línea. Solo se aceptan direcciones IPv4.

- Texto sin formato (TXT)

  Este formato admite direcciones IP individuales y de bloque de CIDR. En la siguiente lista de ejemplo se utiliza texto sin formato (TXT).

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

- Structured Threat Information Expression (STIX)

  Este formato admite direcciones IP individuales y de bloque de CIDR. En la siguiente lista de ejemplo se utiliza el formato STIX.

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:ttp="http://stix.mitre.org/TTP-1"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
```

```
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
stix_core.xsd
    http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
campaign.xsd
    http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
indicator.xsd
    http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
    http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
default_vocabularies/1.2.0/stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
objects/Address/2.1/Address_Object.xsd"
    id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
    version="1.2">
    <stix:Observables cybox_major_version="1" cybox_minor_version="1">
        <cybox:Observable id="example:observable-80b26f43-
dc41-43ff-861d-19aff31e0236">
            <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">

 <AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
            <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable
 id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
            <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
```

```
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
    </stix:Observables>
</stix:STIX_Package>
```

- CSV de Open Threat Exchange (OTX)TM

  Este formato admite direcciones IP individuales y de bloque de CIDR. En la siguiente lista de ejemplo se utiliza el formato de CSV de `OTX`TM.

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

- FireEyeTM iSight Threat Intelligence (CSV)

  Este formato admite direcciones IP individuales y de bloque de CIDR. En la siguiente lista de ejemplo se utiliza un formato de CSV de `FireEye`TM.

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp,
 subject, recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier,
 md5, sha1, sha256, description, fileType, packer, userAgent, registry,
 fileCompilationDateTime, filePath, asn, cidr, domain, domainTimeOfLookup,
 networkIdentifier, ip, port, protocol, registrantEmail, registrantName, networkType,
 url, malwareFamily, malwareFamilyId, actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400

01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 198.51.100.1, , , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
```

```
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400
```

- CSV de Proofpoint™ ET Intelligence Feed

  Este formato admite solo direcciones IP individuales. En la siguiente lista de ejemplo se utiliza el formato de CSV de `Proofpoint`. El parámetro `ports` es opcional. Si omite el puerto, asegúrese de dejar una coma (,) al final.

```
ip, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

- AlienVaultFuente de reputación de ™

  Este formato admite solo direcciones IP individuales. En la siguiente lista de ejemplo se utiliza el formato `AlienVault`.

```
198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
```

Permisos necesarios para cargar listas de IP de confianza y listas de amenazas

Varias identidades de IAM requieren permisos especiales para funcionar con listas de IP confiables y listas de amenazas. GuardDuty Una identidad con la política administrada AmazonGuardDutyFullAccess adjunta solo puede cambiar de nombre y desactivar las listas de IP de confianza y las listas de amenazas cargadas.

Para conceder a diferentes identidades acceso completo para trabajar con listas de IP de confianza y listas de amenazas (además de cambiar de nombre y desactivar estas listas, esto incluye la adición, activación, eliminación y actualización de la ubicación o el nombre de las listas), asegúrese de que las siguientes acciones estén presentes en la política de permisos adjunta a un usuario, grupo o rol:

```
{
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
```

```
        "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::555555555555:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

> **Important**
>
> Estas acciones no se incluyen en la política administrada `AmazonGuardDutyFullAccess`.

Uso del cifrado del servidor para listas de IP de confianza y listas de amenazas

GuardDuty admite los siguientes tipos de cifrado para las listas: SSE-AES256 y SSE-KMS. No se admite SSE-C. Para obtener más información sobre los tipos de cifrado para S3, consulte Protección de los datos con el cifrado del servidor.

Si su lista está cifrada mediante el cifrado SSE-KMS del lado del servidor, debe conceder al rol GuardDuty AWSServiceRoleForAmazonGuardDutyvinculado al servicio permiso para descifrar el archivo a fin de activar la lista. Agregue la siguiente declaración a la política de claves de KMS y sustituya el ID de cuenta por el suyo:

```
{
    "Sid": "AllowGuardDutyServiceRole",
    "Effect": "Allow",
    "Principal": {
    "AWS": "arn:aws:iam::123456789123:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty"
    },
    "Action": "kms:Decrypt*",
    "Resource": "*"
}
```

Adición y activación de una lista de IP de confianza o una lista de IP de amenazas

Elija uno de los siguientes métodos de acceso para agregar y activar una lista de IP de confianza o una lista de IP de amenazas.

Console

(Opcional) Paso 1: obtención de la URL de ubicación de la lista

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación, elija Buckets.
3. Elija el nombre del bucket de Amazon S3 que contiene la lista específica que desea agregar.
4. Elija el nombre del objeto (lista) para consultar sus detalles.
5. En la pestaña Propiedades, copie el URI de S3 de este objeto.

Paso 2: agregación de una lista de IP de confianza o una lista de amenazas

> **Important**
>
> De forma predeterminada, solo puede tener una lista de IP de confianza a la vez. Del mismo modo, puede tener hasta seis listas de amenazas.

1. Abra la consola en https://console.aws.amazon.com/guardduty/. GuardDuty
2. En el panel de navegación, elija Listas.
3. En la página List management, seleccione Add a trusted IP list o Add a threat list.
4. En función de su selección, aparecerá un cuadro de diálogo. Siga estos pasos:
   a. En Nombre de la lista, ingrese un nombre para la lista.

      Restricciones de nomenclatura de listas: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guiones (-) y guiones bajos (_).
   b. En Ubicación, indique la ubicación en la que ha cargado la lista. Si aún no la tiene, consulte Step 1: Fetching location URL of your list.

      Formato de la URL de ubicación

      - https://s3.amazonaws.com/bucket.name/file.txt
      - https://s3-aws-region.amazonaws.com/bucket.name/file.txt
      - http://bucket.s3.amazonaws.com/file.txt
      - http://bucket.s3-aws-region.amazonaws.com/file.txt

- s3://bucket.name/file.txt

c. Active la casilla I agree.

d. Elija Add list. De forma predeterminada, el estado de la lista agregada es Inactivo. Para que la lista sea efectiva, debe activarla.

Paso 3: activar una lista de IP de confianza o una lista de amenazas

1. Abra la consola en https://console.aws.amazon.com/guardduty/ GuardDuty .
2. En el panel de navegación, elija Listas.
3. En la página Administración de listas, seleccione la lista que desee activar.
4. Elija Acciones y, a continuación, elija Activar. La lista puede tardar hasta 15 minutos en ser efectiva.

API/CLI

En el caso de las listas de IP de confianza

- Ejecute CreateIPSet. Asegúrese de proporcionar el valor de `detectorId` de la cuenta de miembro para la que desea crear esta lista de IP de confianza.

  Restricciones de nomenclatura de listas: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guiones (-) y guiones bajos (_).

  - Como alternativa, puede ejecutar el siguiente comando de la AWS Command Line Interface y asegurarse de sustituir `detector-id` por el ID de detector de la cuenta de miembro para la que actualizará la lista de IP de confianza.

```
aws guardduty create-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --format Plaintext --location https://
s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/DOC-EXAMPLE-SOURCE-FILE.format --
activate
```

En el caso de las listas de amenazas

- Ejecute CreateThreatIntelSet. Asegúrese de proporcionar el valor de `detectorId` de la cuenta de miembro para la que desea crear esta lista de amenazas.

- Como alternativa, puede ejecutar el siguiente comando de la AWS Command Line Interface . Asegúrese de proporcionar el valor de `detectorId` de la cuenta de miembro para la que desea crear una lista de amenazas.

```
aws guardduty create-threat-intel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --
format Plaintext --location https://s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/
DOC-EXAMPLE-SOURCE-FILE.format --activate
```

> **Note**
>
> Después de activar o actualizar cualquier lista de IP, la sincronización de la lista GuardDuty puede tardar hasta 15 minutos.

Actualización de las listas de IP de confianza y listas de amenazas

Puede actualizar el nombre de una lista o las direcciones IP agregadas a una lista que ya se haya agregado y activado. Si actualiza una lista, debe volver a activarla GuardDuty para poder utilizar la última versión de la lista.

Elija uno de los métodos de acceso para actualizar una lista de IP de confianza o de amenazas.

Console

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, elija Listas.
3. En la página Administración de listas, seleccione el conjunto de IP de confianza o una lista de amenazas que desee actualizar.
4. Seleccione Acciones y, a continuación, Editar.
5. En el cuadro de diálogo Actualizar lista, actualice la información según sea necesario.

   Restricciones de nomenclatura de listas: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guiones (-) y guiones bajos (_).
6. Marque la casilla Estoy de acuerdo y, a continuación, elija Actualizar lista. El valor de la columna Estado cambiará a Inactivo.

7. Reactivación de la lista actualizada

   a. En la página Administración de listas, seleccione la lista que desee volver a activar.

   b. Elija Acciones y, a continuación, elija Activar.

API/CLI

1. Ejecute UpdateIPSet para actualizar una lista de IP de confianza.
   - Como alternativa, puede ejecutar el siguiente comando de la AWS CLI para actualizar una lista de IP de confianza; asegúrese de sustituir `detector-id` por el ID de detector de la cuenta de miembro para la que actualizará la lista de IP de confianza.

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
activate
```

2. Ejecute UpdateThreatIntelSet para actualizar una lista de amenazas.
   - Como alternativa, puede ejecutar el siguiente comando de la AWS CLI para actualizar una lista de amenazas; asegúrese de sustituir `detector-id` por el ID de detector de la cuenta de miembro para la que actualizará la lista de amenazas.

```
aws guardduty update-threatintel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --activate
```

Desactivación o eliminación de una lista de IP de confianza o una lista de amenazas

Elija uno de los métodos de acceso para eliminar (mediante la consola) o desactivar (mediante la API o CLI) una lista de IP de confianza o una lista de amenazas.

Console

1. Abra la consola en https://console.aws.amazon.com/guardduty/ GuardDuty .
2. En el panel de navegación, elija Listas.
3. En la página Administración de listas, seleccione la lista que desee eliminar.
4. Elija Acciones y, a continuación, elija Eliminar.

5. Confirme la acción y elija Eliminar. La lista específica ya no estará disponible en la tabla.

API/CLI

1. En el caso de una lista de IP de confianza

   Ejecute UpdateIPSet para actualizar una lista de IP de confianza.

   - Como alternativa, puede ejecutar el siguiente comando de la AWS CLI para actualizar una lista de IP de confianza; asegúrese de sustituir `detector-id` por el ID de detector de la cuenta de miembro para la que actualizará la lista de IP de confianza.

     Para encontrar la correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

     ```
     aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
      --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
     no-activate
     ```

2. En el caso de una lista de amenazas

   Ejecute UpdateThreatIntelSet para actualizar una lista de amenazas.

   - Como alternativa, puede ejecutar el siguiente comando de la AWS CLI para actualizar una lista de IP de confianza; asegúrese de sustituir `detector-id` por el ID de detector de la cuenta de miembro para la que actualizará la lista de amenazas.

     ```
     aws guardduty update-threatintel-set --detector-
     id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
     intel-set-id d4b94fc952d6912b8f3060768example --no-activate
     ```

Exportación de resultados

GuardDuty conserva los hallazgos generados durante un período de 90 días. GuardDuty exporta los resultados activos a Amazon EventBridge (EventBridge). Si lo desea, puede exportar los resultados generados a un bucket de Amazon Simple Storage Service (Amazon S3). Esto le ayudará a realizar un seguimiento de los datos históricos de las actividades potencialmente sospechosas en su cuenta y a evaluar si las medidas correctivas recomendadas se han aplicado correctamente.

Todos los nuevos hallazgos activos que se GuardDuty generen se exportan automáticamente unos 5 minutos después de generarse el hallazgo. Puede establecer la frecuencia con la que se exportan las actualizaciones de los hallazgos activos EventBridge. La frecuencia que seleccione se aplica a la exportación de nuevas apariciones de hallazgos existentes a EventBridge su bucket de S3 (cuando está configurado) y a Detective (cuando está integrado). Para obtener información sobre cómo GuardDuty se agregan varias apariciones de hallazgos existentes, consulteGuardDuty encontrar agregación.

Cuando configura los ajustes para exportar los hallazgos a un bucket de Amazon S3, GuardDuty utiliza AWS Key Management Service (AWS KMS) para cifrar los datos de los hallazgos en su bucket de S3. Esto requiere que añada permisos a su bucket de S3 y a la AWS KMS clave para GuardDuty poder utilizarlos para exportar los resultados a su cuenta.

Contenido

Consideraciones

Antes de continuar con los requisitos previos y los pasos para exportar los resultados, tenga en cuenta los siguientes conceptos clave:

- La configuración de exportación es regional: debe configurar las opciones de exportación en cada región en la que las utilice GuardDuty.
- Exportación de los resultados a buckets de Amazon S3 en diferentes regiones Regiones de AWS (entre regiones): GuardDuty admite la siguiente configuración de exportación:
  - El bucket u objeto de Amazon S3 y la AWS KMS clave deben pertenecer al mismo sitio Región de AWS.
  - En el caso de los hallazgos generados en una región comercial, puede optar por exportarlos a un bucket de S3 en cualquier región comercial. Sin embargo, no puede exportar estos resultados a un depósito de S3 en una región que haya optado por participar.

  - En el caso de los hallazgos generados en una región de suscripción voluntaria, puede optar por exportarlos a la misma región en la que se generaron o a cualquier región comercial. Sin embargo, no puedes exportar los resultados de una región de suscripción a otra región de suscripción.
- Permisos para exportar los hallazgos: para configurar los ajustes de exportación de los hallazgos activos, su bucket de S3 debe tener permisos que permitan GuardDuty cargar objetos. También debe tener una AWS KMS clave que GuardDuty pueda utilizar para cifrar los hallazgos.
- Los hallazgos archivados no se exportan: el comportamiento predeterminado es que los hallazgos archivados, incluidas las nuevas instancias de hallazgos suprimidos, no se exportan.

  Para exportar un hallazgo archivado, debe desarchivarlo. Esto cambiará su estado a Activo. Según la frecuencia de exportación, el hallazgo se exportará al depósito S3 configurado.
- GuardDuty la cuenta de administrador puede exportar las conclusiones generadas en las cuentas de los miembros asociadas: al configurar la exportación en una cuenta de administrador, todas las conclusiones de las cuentas de miembros asociadas que se generen en la misma región también se exportan a la misma ubicación que configuró para la cuenta de administrador. Para obtener más información, consulte Comprender la relación entre la cuenta de GuardDuty administrador y las cuentas de los miembros.

Paso 1: Permisos necesarios para exportar los resultados

Al configurar los ajustes para la exportación de los resultados, selecciona un depósito de Amazon S3 donde puede almacenar los hallazgos y una AWS KMS clave para usarla para el cifrado de datos. Además de los permisos para GuardDuty las acciones, también debe tener permisos para las siguientes acciones a fin de configurar correctamente los ajustes de exportación de los hallazgos:

- s3: GetBucketLocation
- s3: PutObject

Paso 2: Adjuntar la política a su clave KMS

GuardDuty cifra los datos de los hallazgos de su depósito mediante. AWS Key Management Service Para configurar correctamente los ajustes, primero debe dar GuardDuty permiso para usar una clave KMS. Para conceder los permisos, adjunte la política a su clave de KMS.

Cuando usas una clave KMS de otra cuenta, debes aplicar la política de claves iniciando sesión en el Cuenta de AWS propietario de la clave. Cuando configure los ajustes para exportar los resultados, también necesitará el ARN clave de la cuenta propietaria de la clave.

Para modificar la política de claves de KMS GuardDuty para cifrar los hallazgos exportados

1. Abra la AWS KMS consola en https://console.aws.amazon.com/kms.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. Seleccione una clave de KMS existente o siga los pasos para crear una nueva clave en la Guía para AWS Key Management Service desarrolladores, que utilizará para cifrar los resultados exportados.

   > **Note**
   >
   > La clave Región de AWS de KMS y el bucket de Amazon S3 deben ser iguales.

   Puede usar el mismo bucket de S3 y el mismo key pair de claves de KMS para exportar los resultados de cualquier región aplicable. Para obtener más información, consulte Consideraciones para exportar los resultados de todas las regiones.
4. En la sección Key policy (Política de claves), elija Edit (Editar).

   Si aparece la vista Cambiar a política, selecciónela para que aparezca la política clave y, a continuación, seleccione Editar.
5. Copie el siguiente bloque de políticas en su política de claves de KMS para conceder GuardDuty permiso para usar su clave.

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "KMS key ARN",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012",
```

```
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
    }
}
```

6. Edite la política sustituyendo los siguientes valores que están formateados en *rojo* en el ejemplo de política:

   1. Sustituya el *ARN de la clave de KMS* por el nombre de recurso de Amazon (ARN) de la clave de KMS. Para localizar el ARN clave, consulta Cómo encontrar el ID y el ARN de la clave en la Guía para desarrolladores.AWS Key Management Service
   2. Sustituya *123456789012* por el Cuenta de AWS identificador propietario de la cuenta que exporta los resultados. GuardDuty
   3. Sustituya la *región 2* por la que Región de AWS se generan las conclusiones. GuardDuty
   4. Sustituya el *SourceDetectorID* por el `detectorID` de la GuardDuty cuenta de la región específica en la que se generaron los hallazgos.

      Para encontrar el `detectorId` de tu cuenta y la región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

   > **Note**
   >
   > Si lo utilizas GuardDuty en una región en la que puedes suscribirte, sustituye el valor del «Servicio» por el punto final regional de esa región. Por ejemplo, si lo utilizas GuardDuty en la región de Oriente Medio (Bahréin) (me-south-1), sustitúyelo por. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` Para obtener información sobre los puntos de conexión de cada región que se haya suscrito, consulta GuardDuty los puntos de conexión y las cuotas.

7. Si has añadido la declaración de política antes de la declaración final, añade una coma antes de añadir esta declaración. Asegúrese de que la sintaxis JSON de su política de claves de KMS sea válida.

   Seleccione Guardar.

8. (Opcional) copia la clave ARN en un bloc de notas para usarla en los pasos posteriores.

Paso 3: Adjuntar la política al bucket de Amazon S3

Añada permisos al depósito de Amazon S3 al que exportará los resultados para GuardDuty poder cargar objetos en este depósito de S3. Independientemente de si utiliza un bucket de Amazon S3 que pertenezca a su cuenta o a una diferente Cuenta de AWS, debe añadir estos permisos.

Si en algún momento decide exportar las conclusiones a un bucket de S3 diferente, para seguir exportando las conclusiones, debe añadir permisos a ese bucket de S3 y volver a configurar los ajustes de exportación de las conclusiones.

Si aún no tiene un depósito de Amazon S3 al que desee exportar estos resultados, consulte Creación de un depósito en la Guía del usuario de Amazon S3.

Para adjuntar permisos a su política de buckets de S3

1. Siga los pasos descritos en Para crear o editar una política de bucket en la Guía del usuario de Amazon S3, hasta que aparezca la página Editar política de bucket.
2. La política de ejemplo muestra cómo conceder GuardDuty permisos para exportar los resultados a su bucket de Amazon S3. Si cambias la ruta después de configurar los resultados de exportación, debes modificar la política para conceder el permiso a la nueva ubicación.

   Copia el siguiente ejemplo de política y pégalo en el editor de políticas de Bucket.

   Si agregó la declaración de política antes de la declaración final, agregue una coma antes de agregar esta declaración. Asegúrese de que la sintaxis JSON de su política de claves de KMS sea válida.

   Política de ejemplo de bucket de S3

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGuardDutygetBucketLocation",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "Amazon S3 bucket ARN",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
"arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "AllowGuardDutyPutObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
"arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "DenyUnencryptedUploadsThis is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "DenyIncorrectHeaderThis is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
```

```
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id": "KMS key ARN"
                }
            }
        },
        {
            "Sid": "DenyNon-HTTPS",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

3. Edite la política sustituyendo los siguientes valores que están formateados en *rojo* en el ejemplo de política:

   1. Sustituya el *ARN del bucket de Amazon S3* por el nombre de recurso de Amazon (ARN) del bucket de Amazon S3. Puedes encontrar el ARN del bucket en la página de edición de la política del bucket en la consola https://console.aws.amazon.com/s3/.
   2. Sustituya *123456789012* por el Cuenta de AWS ID propietario de la cuenta que exporta los GuardDuty resultados.
   3. Sustituya la *región 2* por la que Región de AWS se generan las conclusiones. GuardDuty
   4. Sustituya el *SourceDetectorID* por el `detectorID` de la GuardDuty cuenta de la región específica en la que se generaron los hallazgos.

      Para encontrar el `detectorId` de tu cuenta y la región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.
   5. Sustituya la parte *[prefijo opcional]* del valor del marcador de posición *ARN/[prefijo opcional] del depósito S3* por una ubicación de carpeta opcional a la

que desee exportar los resultados. Para obtener más información sobre el uso de prefijos, consulte Organizar objetos mediante prefijos en la Guía del usuario de Amazon S3.

Si proporciona una ubicación de carpeta opcional que aún no existe, la GuardDuty creará solo si la cuenta asociada al bucket de S3 es la misma que la cuenta que exporta los resultados. Al exportar los resultados a un depósito de S3 que pertenece a otra cuenta, la ubicación de la carpeta debe existir ya.

6. Sustituya el *ARN de la clave de KMS* por el nombre de recurso de Amazon (ARN) de la clave de KMS asociada al cifrado de los hallazgos exportados al bucket de S3. Para localizar el ARN clave, consulta Cómo encontrar el ID y el ARN de la clave en la Guía para desarrolladores.AWS Key Management Service

> **Note**
>
> Si lo utilizas GuardDuty en una región en la que se ha optado por participar, sustituye el valor del «Servicio» por el punto final regional de esa región. Por ejemplo, si lo utilizas GuardDuty en la región de Oriente Medio (Bahréin) (me-south-1), sustitúyelo por. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` Para obtener información sobre los puntos de conexión de cada región que se haya suscrito, consulta GuardDuty los puntos de conexión y las cuotas.

4. Seleccione Guardar.

Paso 4: Exportar los resultados a un bucket de S3 (consola)

GuardDuty le permite exportar los resultados a un depósito existente en otro Cuenta de AWS.

Al crear un nuevo depósito de S3 o al elegir uno existente en su cuenta, puede añadir un prefijo opcional. Al configurar las conclusiones de la exportación, GuardDuty crea una nueva carpeta en el depósito de S3 para guardar las conclusiones. El prefijo se añadirá a la estructura de carpetas predeterminada que se GuardDuty creó. Por ejemplo, el formato del prefijo opcional. `/AWSLogs/123456789012/GuardDuty/Region`

> **Important**
>
> La clave de KMS y el bucket de S3 deben estar en la misma región.

Antes de completar estos pasos, asegúrese de haber adjuntado las políticas respectivas a la clave de KMS y al bucket de S3 existente.

Para configurar los resultados de la exportación

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, seleccione Configuración.
3. En la página de configuración, en las opciones de exportación de Findings, para S3 bucket, seleccione Configurar ahora (o Editar, según sea necesario).
4. Para el ARN del bucket S3, introduzca el. **`bucket ARN`** Para encontrar el ARN del bucket, consulte Visualización de las propiedades de un bucket de S3 en la Guía del usuario de Amazon S3. En la pestaña Permisos de la página de propiedades del bucket asociado en la consola https://console.aws.amazon.com/guardduty/.
5. Para el ARN de la clave KMS, introduzca el. **`key ARN`** Para localizar el ARN clave, consulta Cómo encontrar el ID y el ARN de la clave en la Guía para desarrolladores.AWS Key Management Service
6. Adjunte políticas

   - Realice los pasos para adjuntar la política de bucket de S3. Para obtener más información, consulte Paso 3: Adjuntar la política al bucket de Amazon S3.

   - Realice los pasos para adjuntar la política de claves de KMS. Para obtener más información, consulte Paso 2: Adjuntar la política a su clave KMS.
7. Seleccione Save (Guardar).

Paso 5: Establecer la frecuencia para exportar los hallazgos activos actualizados

Configure la frecuencia de exportación de los hallazgos activos actualizados según corresponda a su entorno. De forma predeterminada, los resultados actualizados se exportan cada 6 horas. Esto

significa que cualquier dato que se actualice después de la exportación más reciente se incluirá en la siguiente exportación. Si los hallazgos actualizados se exportan cada 6 horas y la exportación se produce a las 12:00, cualquier hallazgo que actualice después de las 12:00 se exportará a las 18:00.

Establecimiento de la frecuencia

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. Elija Configuración.
3. En la sección Opciones de exportación de resultados, seleccione Frecuencia de los resultados actualizados. Esto establece la frecuencia de exportación de los hallazgos activos actualizados tanto EventBridge a Amazon S3 como a Amazon S3. Puede elegir entre las siguientes opciones:
   - Actualice EventBridge y S3 cada 15 minutos
   - Actualice EventBridge y S3 cada 1 hora
   - Update CWE and S3 every 6 hours (default) (Actualizar CWE y S3 cada 6 horas (predeterminado))
4. Elija Guardar cambios.

Creación de respuestas personalizadas a GuardDuty los hallazgos con Amazon CloudWatch Events

GuardDuty crea un evento para Amazon CloudWatch Events cuando se produce algún cambio en los resultados. Al buscar cambios que crearán un CloudWatch evento, se incluyen los hallazgos recién generados o los hallazgos agregados recientemente. Los eventos se emiten en la medida de lo posible.

A cada GuardDuty hallazgo se le asigna un identificador de hallazgo. GuardDuty crea un CloudWatch evento para cada hallazgo con un identificador de hallazgo único. Todas las ocurrencias posteriores de un resultado existente se agregarán al resultado original. Para obtener más información, consulte GuardDuty encontrar agregación.

> **Note**
>
> Si su cuenta es un administrador GuardDuty delegado, los CloudWatch eventos se publican en su cuenta y en la cuenta del miembro en la que se generó el hallazgo.

Al usar CloudWatch eventos con GuardDuty, puedes automatizar las tareas para ayudarte a responder a los problemas de seguridad revelados por GuardDuty los hallazgos.

Para recibir notificaciones sobre GuardDuty los hallazgos basados en CloudWatch eventos, debes crear una regla de CloudWatch eventos y un objetivo para ellos GuardDuty. Esta regla permite CloudWatch enviar notificaciones de los hallazgos que se GuardDuty generen al objetivo especificado en la regla. Para obtener más información, consulte Creación de una regla y un objetivo de CloudWatch eventos para GuardDuty (CLI).

Temas

CloudWatch Frecuencia de notificación de eventos para GuardDuty

Notificaciones de resultados recién generados con un identificador de resultado único

GuardDuty envía una notificación basada en el CloudWatch evento en un plazo de 5 minutos a partir del hallazgo. Este evento (y esta notificación) también contiene todos los casos posteriores de este resultado que se producen en los primeros 5 minutos desde que se generó este resultado con un ID único.

> **Note**
>
> La frecuencia de las notificaciones sobre resultados recién generados es de 5 minutos de manera predeterminada. Esta frecuencia no se puede actualizar.

Notificaciones de casos de resultados subsiguientes

De forma predeterminada, para cada hallazgo con un identificador de hallazgo único, GuardDuty se agregan todas las apariciones posteriores de un tipo de hallazgo concreto que se produzcan dentro de los intervalos de 6 horas en un solo evento. GuardDuty a continuación, envía una notificación sobre las siguientes incidencias en función de este evento. De forma predeterminada,

cada 6 horas GuardDuty envía notificaciones basadas en CloudWatch eventos cada 6 horas para las siguientes apariciones de los hallazgos existentes.

Solo una cuenta de administrador puede personalizar la frecuencia predeterminada de las notificaciones que se envían acerca de la posterior aparición de CloudWatch eventos. Los usuarios de las cuentas de miembro no pueden personalizar esta frecuencia. El valor de frecuencia establecido por la cuenta de administrador en su propia cuenta depende de la GuardDuty funcionalidad de todas las cuentas de sus miembros. Si un usuario de una cuenta de administrador establece este valor de frecuencia en 1 hora, todas las cuentas de los miembros también tendrán una frecuencia de 1 hora para recibir notificaciones sobre los siguientes hallazgos. Para obtener más información, consulte Administrar varias cuentas en Amazon GuardDuty.

> **Note**
>
> Como cuenta de administrador, puede personalizar la frecuencia predeterminada de las notificaciones sobre los siguientes casos de búsqueda. Los valores posibles son 15 minutos, una hora o seis horas, que es el valor predeterminado. Para obtener información acerca de la configuración de la frecuencia de estas notificaciones, consulte Paso 5: Establecer la frecuencia para exportar los hallazgos activos actualizados.

Supervisión de los GuardDuty hallazgos archivados con Events CloudWatch

En el caso de las conclusiones archivadas manualmente, las apariciones iniciales y todas las posteriores (generadas una vez finalizado el archivado) se envían a CloudWatch Events según la frecuencia descrita anteriormente.

En el caso de las conclusiones archivadas automáticamente, las apariciones iniciales y todas las posteriores de estas conclusiones (generadas una vez finalizado el archivado) no se envían a Eventos. CloudWatch

CloudWatch formato de evento para GuardDuty

El CloudWatch evento para GuardDuty tiene el siguiente formato.

```
{
 "version": "0",
```

```
 "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
 "detail-type": "GuardDuty Finding",
 "source": "aws.guardduty",
 "account": "111122223333",
 "time": "1970-01-01T00:00:00Z",
 "region": "us-east-1",
 "resources": [],
 "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
}
```

> **Note**
>
> El valor de detalle devuelve los detalles en formato JSON de un solo resultado como objeto, en lugar de devolver el valor “resultados”, que puede respaldar varios resultados dentro de una matriz.

Para obtener una lista completa de todos los parámetros incluidos en la `GUARDDUTY_FINDING_JSON_OBJECT`, consulte GetFindings. El parámetro `id` que aparece en la `GUARDDUTY_FINDING_JSON_OBJECT` es el ID de resultado descrito anteriormente.

Crear una regla de CloudWatch eventos para notificarle los GuardDuty hallazgos (consola)

Puedes usar CloudWatch Events with GuardDuty para configurar alertas de búsqueda automatizadas enviando los eventos de GuardDuty búsqueda a un centro de mensajería para aumentar la visibilidad de GuardDuty los hallazgos. En este tema, se muestra cómo enviar alertas de hallazgos a correo electrónico, Slack o Amazon Chime. Para ello, configura un tema de SNS y, a continuación, lo conecta a CloudWatch una regla de eventos.

Configuración de un tema y un punto de conexión de Amazon SNS

Para empezar, antes debe configurar un tema en Amazon Simple Notification Service y agregar un punto de conexión. Para más información, consulte Introducción en la Guía para desarrolladores de Amazon Simple Notification Service.

Este procedimiento establece dónde desea enviar GuardDuty los datos de búsqueda. El tema de SNS se puede agregar a una regla de CloudWatch eventos durante o después de la creación de la regla de eventos.

Email setup

Creación de un tema de SNS

1. Inicie sesión en la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. Seleccione Temas en el panel de navegación y después Crear un tema.
3. En la sección Crear tema, elija Estándar. A continuación, introduzca un nombre para el tema, como **`GuardDuty_to_Email`**. Lo demás datos son opcionales.
4. Elija Create Topic (Crear tema). Se abrirán los detalles del nuevo tema.
5. En la sección «Suscripciones», elija Crear suscripción.
6. a. En el menú Protocolo, seleccione Correo electrónico.
   b. En el campo Punto de enlace, agregue la dirección de correo electrónico en la que desea recibir las notificaciones.

   > **Note**
   >
   > Una vez creada la suscripción, tendrá que confirmarla a través del cliente de correo electrónico.

   c. Elija Crear suscripción
7. Busque el mensaje de suscripción en la bandeja de entrada y elija Confirmar suscripción.

Slack setup

Creación de un tema de SNS

1. Inicie sesión en la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. Seleccione Temas en el panel de navegación y después Crear un tema.
3. En la sección Crear tema, elija Estándar. A continuación, introduzca un nombre para el tema, como **`GuardDuty_to_Slack`**. Lo demás datos son opcionales. Elija Crear tema para finalizar.

Configuración de un cliente de AWS Chatbot

1. Vaya a la consola de AWS Chatbot
2. En el panel Clientes configurados, seleccione Configurar un nuevo cliente.
3. Elija Slack y confirme mediante “Configurar”.

> **Note**
>
> Al elegir Slack, debe confirmar los permisos de AWS Chatbot para acceder a su canal. Para ello, seleccione “Permitir”.

4. Seleccione Configurar un nuevo canal para abrir el panel de detalles de configuración.
   a. Escriba un nombre para el canal.
   b. Para el canal de Slack, elija el canal que quiera utilizar. Para utilizar un canal privado de Slack con AWS Chatbot, elija Canal privado.
   c. En Slack, copie el ID de canal del canal privado. Para ello, haga clic con el botón derecho en el nombre del canal y seleccione Copiar enlace.
   d. En la consola de administración de AWS, en la ventana de AWS Chatbot, pegue el ID que copió de Slack en el campo ID de canal privado.
   e. En Permisos, elija crear un rol de IAM mediante una plantilla, en caso de que aún no tenga uno.
   f. En plantillas de Política, elija Permisos de notificación. Esta es la plantilla de política de IAM para AWS Chatbot. Proporciona los permisos de lectura y lista necesarios para CloudWatch alarmas, eventos y registros, así como para temas de Amazon SNS.
   g. Elija la región en la que ha creado anteriormente su tema de SNS y, a continuación, seleccione el tema de Amazon SNS que ha creado para enviar notificaciones al canal de Slack.
5. Seleccione Configure (Configurar).

Chime setup

Creación de un tema de SNS

1. Inicie sesión en la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.

2. Seleccione Temas en el panel de navegación y después Crear un tema.
3. En la sección Crear tema, elija Estándar. A continuación, introduzca un nombre para el tema, como **`GuardDuty_to_Chime`**. Lo demás datos son opcionales. Elija Crear tema para finalizar.

Configuración de un cliente de AWS Chatbot

1. Vaya a la consola de AWS Chatbot
2. En el panel Clientes configurados, seleccione Configurar un nuevo cliente.
3. Elija Chime y confirme mediante “Configurar”.
4. En el panel Detalles de configuración, introduzca un nombre para el canal.
5. En Chime, abra la sala de chat deseada
   a. Elija el icono de engranaje en la esquina superior derecha y elija Manage webhooks and bots (Administrar webhooks y bots).
   b. Seleccione Copiar URL para copiar la URL del webhook a su portapapeles.
6. En la consola de administración de AWS, en la ventana de AWS Chatbot, pegue la URL que copió en el campo URL de webhook.
7. En Permisos, elija crear un rol de IAM mediante una plantilla, en caso de que aún no tenga uno.
8. En plantillas de Política, elija Permisos de notificación. Esta es la plantilla de política de IAM para AWS Chatbot. Proporciona los permisos de lectura y lista necesarios para CloudWatch alarmas, eventos y registros, así como para temas de Amazon SNS.
9. Elija la región en la que ha creado anteriormente su tema de SNS y, a continuación, seleccione el tema de Amazon SNS que ha creado para enviar notificaciones a la sala de Chime.
10. Seleccione Configure (Configurar).

Configure un CloudWatch evento para obtener información GuardDuty

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. Seleccione Reglas en el panel de navegación y después Crear una regla.
3. En el menú Nombre del servicio, elija GuardDuty.

4. En el menú Tipo de evento, seleccione GuardDutyBuscar.
5. En Vista previa del patrón de eventos, elija Editar.
6. Pegue el siguiente código JSON en Vista previa del patrón de eventos y elija Guardar.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
      4,
      4.0,
      4.1,
      4.2,
      4.3,
      4.4,
      4.5,
      4.6,
      4.7,
      4.8,
      4.9,
      5,
      5.0,
      5.1,
      5.2,
      5.3,
      5.4,
      5.5,
      5.6,
      5.7,
      5.8,
      5.9,
      6,
      6.0,
      6.1,
      6.2,
      6.3,
      6.4,
      6.5,
      6.6,
```

```
      6.7,
      6.8,
      6.9,
      7,
      7.0,
      7.1,
      7.2,
      7.3,
      7.4,
      7.5,
      7.6,
      7.7,
      7.8,
      7.9,
      8,
      8.0,
      8.1,
      8.2,
      8.3,
      8.4,
      8.5,
      8.6,
      8.7,
      8.8,
      8.9
    ]
  }
}
```

> **Note**
>
> El código anterior alertará de cualquier hallazgo de gravedad media o alta.

7. En la sección Destinos, haga clic en Agregar destino.
8. En el menú Seleccionar destinos, elija Tema de SNS.
9. En Seleccionar un tema, elija el nombre del tema de SNS que creó en el paso 1.
10. Configure la entrada para el evento.

    - Si está configurando las notificaciones para Chime o Slack, vaya al paso 11, el tipo de entrada predeterminado es Evento coincidente.

- Si está configurando notificaciones de correo electrónico a través de SNS, siga los pasos que se indican a continuación para personalizar el mensaje que se envía a la bandeja de entrada:

a. Expanda Configurar entrada y elija Transformador de entrada.

b. Copie el código siguiente y péguelo en el campo Ruta de entrada .

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

c. Copie el código siguiente y péguelo en el campo Plantilla de entrada para dar formato al correo electrónico.

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type
 <Finding_Type> in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"
```

11. Haga clic en Configurar los detalles.
12. En la página Configurar los detalles de la regla, escriba los valores que correspondan en los campos Nombre y Descripción de la regla y elija Crear una regla.

Creación de una regla y un objetivo de CloudWatch eventos para GuardDuty (CLI)

El siguiente procedimiento muestra cómo utilizar los AWS CLI comandos para crear una regla de CloudWatch eventos y un destino para ellos GuardDuty. En concreto, el procedimiento muestra cómo

crear una regla que permita CloudWatch enviar eventos para todos los hallazgos que GuardDuty genere y añadir una AWS Lambda función como destino de la regla.

> **Note**
>
> Además de las funciones de Lambda, GuardDuty son CloudWatch compatibles con los siguientes tipos de objetivos: instancias de Amazon EC2, transmisiones de Amazon Kinesis, tareas de Amazon ECS, máquinas de estadoAWS Step Functions, comandos y objetivos integradosrun.

También puede crear una regla de CloudWatch eventos y un objetivo para ellos GuardDuty a través de la CloudWatch consola de eventos. Para obtener más información y pasos detallados, consulte Crear una regla de CloudWatch eventos que se active en un evento. En la sección Event Source (Origen de evento), seleccione **`GuardDuty`** para Service name (Nombre de servicio) y **`GuardDuty Finding`** para Event Type (Tipo de evento).

Creación de una regla y un destino

1. Para crear una regla que permita CloudWatch enviar eventos para todos los hallazgos que se GuardDuty generen, ejecute el siguiente comando CloudWatch CLI.

   ```
   AWS events put-rule --name Test --event-pattern "{\"source\":
   [\"aws.guardduty\"]}"
   ```

   > **Important**
   >
   > Puede personalizar aún más la regla para que indique que solo se CloudWatch envíen eventos para un subconjunto de los hallazgos GuardDuty generados. Este subconjunto se basa en los atributos de resultado o atributos especificados en la regla. Por ejemplo, utilice el siguiente comando CLI para crear una regla que CloudWatch permita enviar solo eventos para los GuardDuty hallazgos con una gravedad de 5 u 8:
   > `AWS events put-rule --name Test --event-pattern "{\"source\": [\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"], \"detail\":{\"severity\":[5,8]}}"`
   > Para ello, puede utilizar cualquiera de los valores de propiedad que estén disponibles en el JSON para GuardDuty los hallazgos.

2. Para adjuntar una función Lambda como destino para la regla que creó en el paso 1, ejecute el siguiente comando CloudWatch CLI.

   ```
   AWS events put-targets --rule Test --targets
   Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
   ```

   > **Note**
   >
   > Asegúrese de reemplazar <your_function>el comando anterior por su función Lambda real para los GuardDuty eventos.

3. Para agregar los permisos necesarios para invocar el destino, ejecute el siguiente comando de la CLI de Lambda.

   ```
   AWS lambda add-permission --function-name <your_function> --statement-
   id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
   ```

   > **Note**
   >
   > Asegúrese de reemplazar <your_function>el comando anterior por su función Lambda real para los GuardDuty eventos.

   > **Note**
   >
   > En el procedimiento anterior, utilizamos una función Lambda como objetivo de la regla que activa CloudWatch los eventos. También puede configurar otros AWS recursos como objetivos para activar CloudWatch eventos. Para obtener más información, consulte PutTargets.

CloudWatch Eventos para entornos GuardDuty con varias cuentas

Como GuardDuty administrador, las reglas de CloudWatch eventos de su cuenta se activarán en función de las conclusiones aplicables de sus cuentas de miembros. Esto significa que si configuras una notificación de localización a través de CloudWatch Eventos en tu cuenta de administrador, tal y como se detalla en la sección anterior, se te notificarán los hallazgos de gravedad alta y media generados por tus cuentas de miembro, además de por las tuyas propias.

Puedes identificar la cuenta de miembro en la que se originó el GuardDuty hallazgo con el `accountId` campo de detalles JSON del hallazgo.

Para empezar a escribir una regla de evento personalizada para una cuenta de miembro específica de su entorno en la consola, cree una nueva regla y pegue la siguiente plantilla en la vista previa del patrón de eventos mediante la agregación del ID de cuenta de la cuenta de miembro que desee que desencadene el evento.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

> **Note**
>
> Este ejemplo desencadenará cualquier resultado correspondiente al ID de cuenta que aparece en la lista. Se pueden agregar varios ID, separados por una coma según la sintaxis JSON.

Descripción de CloudWatch los registros y los motivos por los que se omiten recursos durante el análisis de Malware Protection

GuardDuty Malware Protection publica los eventos en su grupo de CloudWatch registro de Amazon / aws/guardduty/ malware-scan-events. Para cada uno de los eventos relacionados con el análisis de malware, puede supervisar el estado y el resultado del análisis de los recursos afectados. Es posible que algunos recursos de Amazon EC2 y volúmenes de Amazon EBS se hayan omitido durante el análisis de Protección contra malware.

GuardDuty Registros de auditoría en Malware CloudWatch Protection

El grupo de registros malware-scan-events CloudWatch /aws/guardduty/admite tres tipos de eventos de análisis.

Nombre del evento de análisis de Protección contra malware	Explicación
`EC2_SCAN_STARTED`	Se crea cuando un equipo de protección contra GuardDuty malware inicia el proceso de análisis de malware, por ejemplo, cuando se prepara para tomar una instantánea de un volumen de EBS.
`EC2_SCAN_COMPLETED`	Se crea cuando se completa el análisis de GuardDuty Malware Protection en al menos uno de los volúmenes de EBS del recurso afectado. Este evento también incluye el valor de `snapshotId` que pertenece al volumen de EBS analizado. Una vez finalizado el análisis, el resultado será `CLEAN`, `THREATS_FOUND` o `NOT_SCANNED` .
`EC2_SCAN_SKIPPED`	Se crea cuando el análisis de GuardDuty Malware Protection omite todos los volúmenes de EBS del recurso afectado. Para identificar el motivo de la omisión, seleccione el evento correspondiente y consulte los detalles. Para obtener más información sobre los motivos de la omisión, consulte Motivos para omitir un recurso durante el análisis de malware a continuación.

> **Note**
>
> Si utilizas unaAWS Organizations, los eventos de CloudWatch registro de las cuentas de los miembros de Organizations se publican tanto en la cuenta del administrador como en el grupo de registro de la cuenta de miembro.

Elige el método de acceso que prefieras para ver y consultar CloudWatch los eventos.

Console

1. Inicie sesión en la CloudWatch consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, en Registros, seleccione Grupos de registros. Elija el grupo de malware-scan-events registros /aws/guardduty/ para ver los eventos de análisis de Malware Protection. GuardDuty

   Para ejecutar una consulta, elija Información de registros.

   Para obtener información sobre cómo ejecutar una consulta, consulte Análisis de datos de registro con CloudWatch Logs Insights en la Guía del CloudWatch usuario de Amazon.
3. Elija ID de análisis para supervisar los detalles del recurso afectado y los resultados de malware. Por ejemplo, puede ejecutar la siguiente consulta para filtrar los eventos del CloudWatch registro mediante`scanId`. Asegúrese de utilizar su propio valor de *`scan-id`* válido.

   ```
   fields @timestamp, @message, scanRequestDetails.scanId as scanId
   | filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
   | sort @timestamp asc
   ```

API/CLI

- Para trabajar con grupos de registros, consulte Buscar entradas de registro utilizando AWS CLI la Guía del CloudWatch usuario de Amazon.

  Elija el grupo de malware-scan-events registros /aws/guardduty/ para ver los eventos de escaneo de Malware Protection. GuardDuty

- Para ver y filtrar los eventos de registro, consulte GetLogEventsy FilterLogEvents, respectivamente, en la referencia de la CloudWatch API de Amazon.

GuardDuty Protección contra malware: retención de registros

El período de retención de registros predeterminado para el grupo de registros /aws/guardduty/ es de 90 días, tras los cuales los eventos del malware-scan-events registro se eliminan automáticamente. Para cambiar la política de retención de registros de su grupo de registros, consulte Cambiar la retención de datos de CloudWatch registro en los registros o. CloudWatch PutRetentionPolicy

Motivos para omitir un recurso durante el análisis de malware

En los eventos relacionados con el análisis de malware, es posible que se hayan omitido algunos recursos de EC2 y volúmenes de EBS durante el proceso de análisis. En la siguiente tabla se enumeran los motivos por los que GuardDuty Malware Protection puede no analizar los recursos. Si procede, siga los pasos propuestos para resolver estos problemas y analice estos recursos la próxima vez que GuardDuty Malware Protection inicie un análisis de malware. Los demás problemas se utilizan para informarle sobre el curso de los eventos y no son procesables.

Razones de omisión	Explicación	Pasos propuestos	
`RESOURCE_NOT_FOUND`	El valor de `resourceArn` proporcionado para iniciar el análisis de malware bajo demanda no se encontró en su entorno de AWS.	Valide el valor de `resourceArn` de la carga de trabajo de su instancia o contenedor de Amazon EC2 e inténtelo de nuevo.	
`ACCOUNT_INELIGIBLE`	El ID de AWS cuenta desde el que intentó iniciar un análisis de malware bajo demanda no está activado. GuardDuty	Comprueba que GuardDuty esté activado para esta AWS cuenta. Cuando GuardDuty habilitas una nuevaRegión de	

Razones de omisión	Explicación	Pasos propuestos	
		AWS, la sincroniz ación puede tardar hasta 20 minutos.	
`UNSUPPORT ED_KEY_EN CRYPTION`	GuardDuty La protección contra malware admite volúmenes cifrados o no cifrados con una clave gestionad a por el cliente. No admite el análisis de volúmenes de EBS cifrados con el cifrado de Amazon EBS. En la actualidad, existe una diferenci a regional en la que este motivo de omisión no es aplicable. Para obtener más informaci ón al respectoR egiones de AWS, consulteDisponibi lidad de caracterí sticas específicas por región.	Sustituya la clave de cifrado por una clave administrada por el cliente. Para obtener más informaci ón sobre los tipos de cifrado GuardDuty compatibles, consulteVolúmenes de Amazon EBS compatibles para el análisis de malware.	

Razones de omisión	Explicación	Pasos propuestos	
`EXCLUDED_BY_SCAN_SETTINGS`	La instancia de EC2 o el volumen de EBS se excluyó durante el análisis de malware. Hay dos posibilidades: la etiqueta se agregó a la lista de inclusión, pero el recurso no está asociado a esta etiqueta, la etiqueta se agregó a la lista de exclusión y el recurso está asociado a esta etiqueta o la etiqueta `GuardDutyExcluded` está establecida en `true` para este recurso.	Actualice las opciones de análisis o las etiquetas asociadas a su recurso de Amazon EC2. Para obtener más información, consulte Opciones de análisis con etiquetas definidas por el usuario.	
`UNSUPPORTED_VOLUME_SIZE`	El volumen es mayor que 1024 GB.	No se puede procesar.	
`NO_VOLUMES_ATTACHED`	GuardDuty Malware Protection encontró la instancia en su cuenta, pero no se adjuntó ningún volumen de EBS a esta instancia para continuar con el escaneo.	No se puede procesar.	
`UNABLE_TO_SCAN`	Se trata de un error de servicio interno.	No se puede procesar.	

Razones de omisión	Explicación	Pasos propuestos	
SNAPSHOT_NOT_FOUND	No se encontraron las instantáneas creadas a partir de los volúmenes de EBS y compartidas con la cuenta de servicio y GuardDuty Malware Protection no pudo continuar con el escaneo.	Asegúrese CloudTrail de que las instantáneas no se hayan eliminado de forma intencionada.	
SNAPSHOT_QUOTA_REACHED	Ha alcanzado el volumen máximo permitido de instantáneas para cada región. Esto impide no solo retener, sino también crear nuevas instantáneas.	Puede eliminar las instantáneas antiguas o solicitar un aumento de cuota. Puede ver el límite predeterminado de instantáneas por región y consultar cómo solicitar un aumento de cuota en el apartado Service quotas en la Guía de referencia general de AWS.	
MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED	Se adjuntaron más de 11 volúmenes de EBS a una instancia EC2. GuardDuty Malware Protection escaneó los primeros 11 volúmenes de EBS y los obtuvo ordenándolos alfabéticamente. `deviceName`	No se puede procesar.	

Razones de omisión	Explicación	Pasos propuestos	
`UNSUPPORTED_PRODUCT_CODE_TYPE`	GuardDuty no admite el escaneo de instancias con como. `productCode marketplace` Para obtener más información, consulte AMI de pago en la Guía del usuario de instancias de Linux de Amazon EC2. Para obtener más información sobre `productCode` , consulte ProductCode en la Referencia de la API de Amazon EC2.	No se puede procesar.	

Denunciar falsos positivos en GuardDuty Malware Protection

Los escaneos de GuardDuty Malware Protection pueden identificar un archivo inofensivo en la carga de trabajo de su instancia o contenedor de Amazon EC2 como malicioso o dañino. Para mejorar su experiencia con Malware Protection y el servicio GuardDuty, puede informar de resultados falsos positivos si cree que un archivo identificado como malicioso o dañino durante un análisis no contiene realmente malware.

Envío de un archivo con un falso positivo

1. Abra la consola de en https://console.aws.amazon.com/guardduty.
2. Cuando identifique lo que parece ser un resultado falso positivo, póngase en contacto con nosotros AWS Support para iniciar el proceso de envío de un archivo con un falso positivo.
3. Elija Escaneos de malware.
4. Elija un escaneo para ver su identificador de búsqueda.

5. Proporcione el identificador de búsqueda. También debe proporcionar el hash SHA-256 del archivo. Esto es necesario para garantizar que GuardDuty Malware Protection haya recibido el archivo correcto.
6. El AWS Support equipo le proporcionará una URL de Amazon Simple Storage Service (S3) que podrá utilizar para cargar el archivo y el hash SHA-256. Informe al AWS Support equipo una vez que haya cargado correctamente el archivo.

> **Warning**
>
> No proporciones directamente el archivo o el hash SHA-256 a. AWS Support Solo debe cargar el archivo y el hash a Amazon S3 a través de la URL proporcionada. Si no carga el archivo y el hash en un plazo de siete días a partir de la recepción de la URL, esta dejará de ser válida. Si la URL deja de ser válida, tendrás que comunicarte con nosotros AWS Support para recibir una nueva URL.

GuardDuty conserva su archivo durante no más de 30 días. Los miembros del equipo de GuardDuty analizarán su envío y tomarán las medidas adecuadas para mejorar su experiencia con Malware Protection y el servicio GuardDuty.

Corregir los problemas de seguridad descubiertos por GuardDuty

Amazon GuardDuty genera resultados que indican posibles problemas de seguridad. En esta versión de GuardDuty, los posibles problemas de seguridad indican que la carga de trabajo de la instancia EC2 o del contenedor está en peligro, o bien un conjunto de credenciales comprometidas en su AWS entorno. En las siguientes secciones, se describen los pasos de corrección recomendados para estos escenarios. Si hay escenarios de corrección alternativos, se describirán en la entrada para ese tipo de resultado específico. Para acceder a toda la información sobre un tipo de resultado, selecciónelo en la Tabla de tipos de resultados activos.

Contenido

Corregir una instancia de Amazon EC2 potencialmente comprometida

Siga estos pasos recomendados para corregir una instancia EC2 potencialmente comprometida en su entorno: AWS

1. Identifique la instancia de Amazon EC2 potencialmente comprometida

   Examine la instancia posiblemente comprometida en busca de malware y elimínelo. Puede utilizar Análisis de malware bajo demanda para identificar el malware en la instancia de EC2

potencialmente afectada o comprobar AWS Marketplace para ver si hay productos asociados útiles para identificar y eliminar el malware.

2. Aísle la instancia de Amazon EC2 potencialmente comprometida

   Si es posible, siga los siguientes pasos para aislar la instancia potencialmente comprometida:

   1. Cree un grupo de seguridad dedicado a Isolation.
   2. Cree una regla única `0.0.0.0/0 (0-65535)` para todo el tráfico de las reglas de salida.

      Cuando se aplique esta regla, convertirá todo el tráfico saliente existente (y el nuevo) en tráfico no rastreado, lo que bloqueará cualquier sesión saliente establecida. Para obtener más información, consulte Conexiones sin seguimiento.
   3. Elimine todas las asociaciones de grupos de seguridad actuales de la instancia potencialmente comprometida.
   4. Asocie el grupo de seguridad Isolation a esta instancia.

      Tras la asociación, elimine la regla `0.0.0.0/0 (0-65535)` para todo el tráfico de las reglas de salida del grupo de seguridad Isolation.

3. Identifique el origen de la actividad sospechosa

   Si se detecta malware, con base en el tipo de resultado de su cuenta, identifique y detenga la actividad potencialmente no autorizada en su instancia de EC2. Esto puede requerir acciones como cerrar cualquier puerto abierto, cambiar las políticas de acceso y actualizar las aplicaciones para corregir las vulnerabilidades.

   Si no puede identificar ni detener la actividad no autorizada en su instancia de EC2 potencialmente comprometida, le recomendamos que cierre la instancia de EC2 comprometida y la sustituya por una nueva, según sea necesario. A continuación se enumeran recursos adicionales para proteger instancias EC2:

   - Secciones “Seguridad” y “Redes” en Prácticas recomendadas de Amazon EC2
   - Grupos de seguridad de Amazon EC2 para instancias de Linux y Grupos de seguridad de Amazon EC2 para instancias de Windows
   - Seguridad en Amazon EC2
   - Sugerencias para proteger la instancia EC2.
   - AWS prácticas recomendadas de seguridad
   - Incidentes en el dominio de infraestructura en AWS

4. Examinar AWS re:Post

   Visite AWS re:Post https://forums.aws.amazon.com/index.jspa para obtener más ayuda.

5. Envíe una solicitud de asistencia técnica

   Si es suscriptor de un paquete Premium Support, puede enviar una solicitud de asistencia técnica.

Corregir un bucket de S3 potencialmente comprometido

Siga estos pasos recomendados para corregir un bucket de Amazon S3 de su AWS entorno que podría estar en peligro:

1. Identifique el recurso de S3 potencialmente comprometido.

   Si se GuardDuty busca S3, se mostrará el bucket de S3 asociado, su nombre de recurso de Amazon (ARN) y su propietario en los detalles de búsqueda.

2. Identifique el origen de la actividad sospechosa y la llamada a la API que se utilizó.

   La llamada a la API utilizada se mostrará como `API` en los detalles de resultado. El origen será una entidad principal de IAM (ya sea un rol de IAM, un usuario o una cuenta) y los detalles de identificación figurarán en el resultado. Según el tipo de origen, estará disponible la dirección IP remota o la información del dominio de origen, lo que puede ayudarle a evaluar si el origen fue autorizado. Si el hallazgo involucró credenciales de una instancia de Amazon EC2, también se incluirán los detalles de ese recurso.

3. Determine si el origen de la llamada tenía autorización para acceder al recurso identificado.

   Por ejemplo, considere lo siguiente:

   - Si estuvo implicado un usuario de IAM, ¿es posible que sus credenciales se hayan visto comprometidas? Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.
   - Si se ha invocado una API desde una entidad principal que no tiene antecedentes de haber invocado este tipo de API, ¿este origen necesita permisos de acceso para esta operación? ¿Se pueden restringir aún más los permisos del bucket?
   - Si el acceso se vio desde nombre de usuario `ANONYMOUS_PRINCIPAL` con el tipo de usuario de la `AWSAccount`, esto indica que el bucket es público y se ha accedido a él. ¿Este bucket debería ser público? Si no es así, consulte las siguientes recomendaciones de seguridad para encontrar soluciones alternativas al uso compartido de los recursos de S3.

- Si el acceso se hizo mediante una llamada a `PreflightRequest` correcta desde el nombre de usuario `ANONYMOUS_PRINCIPAL` y el tipo de usuario de la `AWSAccount`, esto indica que el bucket tiene una política de intercambio de recursos entre orígenes (CORS) establecida. ¿Este bucket debería tener una política CORS? Si no es así, asegúrese de que el bucket no sea inadvertidamente público y revise las recomendaciones de seguridad que aparecen a continuación en busca de soluciones alternativas al uso compartido de los recursos de S3. Para más información sobre CORS, consulte Uso compartido de recursos entre orígenes (CORS) en la Guía del usuario de S3.

4. Determine si el bucket de S3 contiene datos confidenciales.

   Utilice Amazon Macie para determinar si el bucket de S3 contiene información confidencial, como información de identificación personal (PII), datos financieros o credenciales. Si la detección automática de datos confidenciales está habilitada para su cuenta de Macie, revise los detalles del bucket de S3 para comprender mejor su contenido. Si esta característica está deshabilitada en su cuenta de Macie, se recomienda que la active para agilizar la evaluación. Como alternativa, puede crear y ejecutar un trabajo de detección de datos confidenciales para inspeccionar los objetos del bucket de S3 en busca de datos confidenciales. Para más información, consulte Discovering sensitive data with Macie.

Si se autorizó el acceso, puede ignorar el resultado. La consola https://console.aws.amazon.com/guardduty/ le permite configurar reglas para suprimir por completo los resultados individuales y evitar que vuelvan a aparecer. Para obtener más información, consulte Reglas de supresión.

Si determina que una persona no autorizada ha expuesto sus datos de S3 o ha accedido a ellos, revise las siguientes recomendaciones de seguridad de S3 para reforzar los permisos y restringir el acceso. Las soluciones de corrección adecuadas dependerán de las necesidades de su entorno específico.

Recomendaciones basadas en las necesidades específicas de acceso al bucket de S3

La siguiente lista proporciona recomendaciones basadas en las necesidades específicas de acceso a los buckets de Amazon S3:

- Para limitar el acceso público al uso de datos de S3 de forma centralizada, S3 bloquea el acceso público. La configuración de bloqueo de acceso público se puede habilitar para los puntos de acceso, los depósitos y AWS las cuentas mediante cuatro configuraciones diferentes para

controlar la granularidad del acceso. Para obtener más información, consulte Configuración del Bloqueo de acceso público de S3.

- AWS Las políticas de acceso se pueden usar para controlar cómo los usuarios de IAM pueden acceder a sus recursos o cómo pueden acceder a sus depósitos. Para obtener más información, consulte Uso de políticas de bucket y de usuario.

  Además, puede utilizar puntos de conexión de la nube privada virtual (VPC) con políticas de bucket de S3 para restringir el acceso a puntos de conexión de VPC específicos. Para obtener más información, consulte Example Bucket Policies for VPC Endpoints for Amazon S3
- Para permitir temporalmente el acceso a sus objetos de S3 a entidades de confianza ajenas a su cuenta, puede crear una URL prefirmada a través de S3. Este acceso se crea con las credenciales de su cuenta y, según las credenciales utilizadas, puede durar de 6 horas a 7 días. Para más información, consulte Generación de URL prefirmadas con S3.
- Para los casos de uso que requieren el uso compartido de objetos de S3 entre distintos orígenes, puede utilizar los puntos de acceso de S3 para crear conjuntos de permisos que restrinjan el acceso únicamente a los que están dentro de su red privada. Para obtener más información, consulte Administración del acceso a datos con puntos de acceso de Amazon S3.
- Para conceder acceso seguro a sus recursos de S3 a otras AWS cuentas, puede utilizar una lista de control de acceso (ACL). Para obtener más información, consulte Gestión del acceso a S3 con ACL.

Para obtener más información sobre las opciones de seguridad de S3, consulte las prácticas recomendadas de seguridad de S3.

Cómo corregir un clúster de ECS potencialmente comprometido

Siga estos pasos recomendados para corregir un clúster de Amazon ECS potencialmente comprometido en su AWS entorno:

1. Identifique el clúster de ECS potencialmente comprometido.

   El hallazgo de ECS sobre la protección contra GuardDuty malware proporciona los detalles del clúster de ECS en el panel de detalles del hallazgo.
2. Evalúe el origen del malware

Evalúe si el malware detectado estaba en la imagen del contenedor. Si había malware en la imagen, identifique todas las demás tareas que se estén ejecutando con esta imagen. Para obtener información sobre la ejecución de tareas, consulte ListTasks.

3. Aísle las tareas potencialmente afectadas

   Para aislar las tareas afectadas, deniegue todo el tráfico de entrada y salida a la tarea. Una norma de denegación total de tráfico puede ayudarle a detener un ataque que ya está en marcha, ya que interrumpe todas las conexiones con la tarea.

Si se autorizó el acceso, puede ignorar el resultado. La consola https://console.aws.amazon.com/guardduty/ le permite configurar reglas para suprimir por completo los resultados individuales y evitar que vuelvan a aparecer. Para obtener más información, consulte Reglas de supresión.

Corregir las credenciales potencialmente comprometidas AWS

Siga estos pasos recomendados para corregir las credenciales potencialmente comprometidas en su AWS entorno:

1. Identifique la entidad de IAM potencialmente comprometida y la llamada a la API utilizada.

   La llamada a la API utilizada se mostrará como `API` en los detalles de resultado. La entidad de IAM (ya sea un rol o un usuario de IAM) y su información de identificación aparecerán en la sección Recursos de la sección de detalles de la búsqueda. El tipo de entidad de IAM implicada puede determinarse mediante el campo Tipo de usuario, el nombre de la entidad de IAM estará en el campo Nombre de usuario. El tipo de entidad de IAM implicada en el resultado también puede determinarse mediante el ID de clave de acceso utilizado.

   Para las claves que empiecen con `AKIA`:

   Este tipo de clave es una credencial administrada por el cliente a largo plazo asociada con un usuario de IAM o Usuario raíz de la cuenta de AWS. Para obtener información sobre la administración de claves de acceso para usuarios de IAM, consulte Administración de las claves de acceso de los usuarios de IAM.

   Para las claves que empiecen con `ASIA`:

   Este tipo de clave es una credencial temporal a corto plazo generada por AWS Security Token Service. Estas claves solo existen durante un período breve y no se pueden ver ni administrar en la Consola AWS de administración. Los roles de IAM siempre utilizarán AWS

STS credenciales, pero también se pueden generar para los usuarios de IAM. Para obtener más información, AWS STS consulte IAM: credenciales de seguridad temporales.

Si se utilizó un rol, el campo Nombre de usuario indicará el nombre del rol utilizado. Para determinar cómo se solicitó la clave, AWS CloudTrail examine el `sessionIssuer` elemento de la entrada del CloudTrail registro. Para obtener más información, consulte IAM e información en. AWS STS CloudTrail

2. Revise los permisos de la entidad de IAM.

   Abra la consola de IAM. Según el tipo de entidad utilizada, seleccione la pestaña Usuarios o Funciones y localice la entidad afectada escribiendo el nombre identificado en el campo de búsqueda. Utilice las pestañas Permisos y Acceso a Advisor para revisar los permisos efectivos para esa entidad.

3. Determine si las credenciales de entidad de IAM se utilizaron legítimamente.

   Póngase en contacto con el usuario de las credenciales para determinar si la actividad fue intencionada.

   Por ejemplo, averigüe si el usuario hizo lo siguiente:

   - Invocó la operación de API que figuraba en el GuardDuty hallazgo
   - Invocó la operación de la API en el momento que se muestra en el resultado de GuardDuty
   - Invocó la operación de la API desde la dirección IP que se muestra en el resultado de GuardDuty

Si esta actividad es un uso legítimo de las AWS credenciales, puede ignorar la GuardDuty conclusión. La consola https://console.aws.amazon.com/guardduty/ le permite configurar reglas para suprimir por completo los resultados individuales y evitar que vuelvan a aparecer. Para obtener más información, consulte Reglas de supresión.

Si no puedes confirmar si esta actividad es un uso legítimo, podría deberse a que la clave de acceso concreta (las credenciales de inicio de sesión del usuario de IAM) o, posiblemente, la totalidad de esta clave. Cuenta de AWSSi sospechas que tus credenciales se han visto comprometidas, consulta la información del artículo Mi sistema Cuenta de AWS puede estar comprometido para solucionar este problema.

Corregir un contenedor independiente potencialmente comprometido

1. Aísle el contenedor potencialmente comprometido

   Los siguientes pasos le ayudarán a identificar e identificar la carga de trabajo del contenedor potencialmente malintencionada:

   - Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
   - En la página de hallazgos, elija el hallazgo correspondiente para ver el panel de hallazgos.
   - En el panel de resultados, en la sección Recurso afectado, puede ver el ID y el Nombre del contenedor.

   Aísle este contenedor de otras cargas de trabajo de contenedores.
2. Pause el contenedor

   Suspenda todos los procesos de su contenedor.

   Para obtener información sobre cómo congelar un contenedor, consulte Pausar un contenedor.

   Detenga el contenedor

   Si el paso anterior no funciona y el contenedor no se detiene, pare el funcionamiento del contenedor. Si ha activado la Retención de instantáneas función, GuardDuty conservará las instantáneas de los volúmenes de EBS que contengan software malicioso.

   Para obtener información sobre cómo detener el contenedor, consulte Detener un contenedor.
3. Evalúe la presencia de malware

   Evalúe si el malware estaba en la imagen del contenedor.

Si se autorizó el acceso, puede ignorar el resultado. La consola https://console.aws.amazon.com/guardduty/ le permite configurar reglas para suprimir por completo los resultados individuales y evitar que vuelvan a aparecer. La GuardDuty consola le permite configurar reglas para suprimir por completo los hallazgos individuales y evitar que aparezcan. Para obtener más información, consulte Reglas de supresión.

Corrección de los resultados de la supervisión de registros de auditoría de EKS

Amazon GuardDuty genera resultados que indican posibles problemas de seguridad de Kubernetes cuando la monitorización de registros de auditoría de EKS está habilitada para su cuenta. Para obtener más información, consulte Supervisión de registros de auditoría de EKS. En las siguientes secciones, se describen los pasos de corrección recomendados para estos escenarios. Las acciones de corrección específicas se describen en la entrada de ese tipo de resultado en concreto. Para acceder a toda la información sobre un tipo de resultado, selecciónelo en la Tabla de tipos de resultados activos.

Si alguno de los tipos de resultados de la supervisión de registros de auditoría de EKS se generó de forma expectante, puede considerar la posibilidad de agregar Reglas de supresión para evitar futuras alertas.

Los distintos tipos de ataques y problemas de configuración pueden provocar GuardDuty conclusiones sobre Kubernetes. Esta guía le ayuda a identificar las causas fundamentales de los GuardDuty hallazgos relacionados con su clúster y describe las pautas de corrección adecuadas. Las siguientes son las principales causas que conducen a los hallazgos de GuardDuty Kubernetes:

- Posibles problemas de configuración
- Corregir a los usuarios de Kubernetes potencialmente comprometidos
- Corregir los pods de Kubernetes potencialmente comprometidos
- Corregir los nodos de Kubernetes potencialmente comprometidos
- Corregir las imágenes de contenedores potencialmente comprometidas

> **Note**
>
> Antes de la versión 1.14 de Kubernetes, el `system:unauthenticated` grupo estaba asociado a Kubernetes y de forma predeterminada. `system:discovery` `system:basic-user` ClusterRoles Esto puede permitir el acceso no deseado de usuarios anónimos. Las actualizaciones del clúster no revocan estos permisos, lo que significa que, incluso si ha actualizado el clúster a la versión 1.14 o posterior, es posible que estos permisos sigan vigentes. Se recomienda que desasocie estos permisos del grupo `system:unauthenticated`.

Para obtener más información sobre la eliminación de estos permisos, consulte Prácticas recomendadas de seguridad para Amazon EKS en la Guía del usuario de Amazon EKS.

Posibles problemas de configuración

Si un resultado indica un problema de configuración, consulte la sección de corrección de ese resultado para obtener directrices sobre cómo resolver ese problema concreto. Para obtener más información, consulte los siguientes tipos de resultados que indican problemas de configuración:

- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/KubeflowDashboardExposed
- Cualquier hallazgo que termine en SuccessfulAnonymousAccess

Corregir a los usuarios de Kubernetes potencialmente comprometidos

Un GuardDuty hallazgo puede indicar que un usuario de Kubernetes está en peligro cuando un usuario identificado en el hallazgo ha realizado una acción de API inesperada. Puede identificar el usuario en la sección Detalles del usuario de Kubernetes de los detalles de un resultado en la consola o en `resources.eksClusterDetails.kubernetesDetails.kubernetesUserDetails` del JSON de resultados. Estos detalles del usuario incluyen `user name`, `uid` y los grupos de Kubernetes a los que pertenece el usuario.

Si el usuario accedía a la carga de trabajo mediante una entidad de IAM, puede utilizar la sección `Access Key details` para identificar los detalles de un usuario o rol de IAM. Consulte los siguientes tipos de usuarios y sus directrices de corrección.

> **Note**
>
> Puede utilizar Amazon Detective para investigar más el rol de IAM o el usuario identificado en el resultado. Mientras ves los detalles de la búsqueda en la GuardDuty consola, selecciona Investigar en Detective. A continuación, seleccione el AWS usuario o el rol de los elementos de la lista para investigarlo en Detective.

Administrador de Kubernetes integrado: usuario predeterminado asignado por Amazon EKS a la identidad de IAM que creó el clúster. Este tipo de usuario se identifica mediante el nombre de usuario `kubernetes-admin`.

Revocación del acceso de un administrador de Kubernetes integrado:

- Identifique el valor de `userType` en la sección `Access Key details`.
  - Si `userType` es Rol y el rol pertenece a un rol de instancia de EC2:
    - Identifique esa instancia y, a continuación, siga las instrucciones que se indican en Corregir una instancia de Amazon EC2 potencialmente comprometida.
  - Si `userType` es Usuario o es un rol que ha asumido un usuario:
    1. Rote la clave de acceso de ese usuario.
    2. Rote los secretos a los que haya accedido el usuario.
    3. Revisa la información de Mi AWS cuenta, que puede estar comprometida, para obtener más información.

Usuario autenticado de OIDC: usuario al que se ha concedido acceso a través de un proveedor de OIDC. Normalmente, un usuario de OIDC tiene una dirección de correo electrónico como nombre de usuario. Puede comprobar si el clúster usa OIDC con el siguiente comando: `aws eks list-identity-provider-configs --cluster-name` *`your-cluster-name`*

Revocación del acceso de un usuario autenticado de OIDC:

1. Rote las credenciales de ese usuario en el proveedor de OIDC.
2. Rote los secretos a los que haya accedido el usuario.

AWSUsuario ConfigMap definido por autenticación: usuario de IAM al que se le concedió acceso mediante una autenticación. AWSConfigMap Para obtener más información, consulte Administración de usuarios o roles de IAM para su clúster en la Guía del usuario de EKS. Puede revisar sus permisos con el siguiente comando: `kubectl edit configmaps aws-auth --namespace kube-system`

Para revocar el acceso de un usuario: AWS ConfigMap

1. Utilice el siguiente comando para abrir el ConfigMap.

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifique la entrada de rol o usuario en la sección MapRoles o MapUsers con el mismo nombre de usuario que el indicado en la sección de detalles de usuario de Kubernetes que encontró. GuardDuty Consulte el siguiente ejemplo, en el que se ha identificado al usuario administrador en un resultado.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      user name: system:node:EC2_PrivateDNSName
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::123456789012:user/admin
      username: admin
      groups:
        - system:masters
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

3. Elimine ese usuario de. ConfigMap Consulte el siguiente ejemplo, en el que se ha eliminado el usuario administrador.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

4. Si `userType` es Usuario o es un rol que ha asumido un usuario:
   a. Rote la clave de acceso de ese usuario.
   b. Rote los secretos a los que haya accedido el usuario.
   c. Revise la información de Mi AWS cuenta puede estar comprometida para obtener más detalles.

Si el resultado no tiene una sección `resource.accessKeyDetails`, el usuario es una cuenta de servicio de Kubernetes.

Cuenta de servicio: la cuenta de servicio proporciona una identidad para los pods y se puede identificar mediante un nombre de usuario con el siguiente formato: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Para revocar el acceso a una cuenta de servicio:

1. Cambie las credenciales de la cuenta de servicio.
2. Consulte las directrices sobre el peligro de los pods en la siguiente sección.

Corregir los pods de Kubernetes potencialmente comprometidos

Cuando se GuardDuty especifican los detalles de un pod o recurso de carga de trabajo dentro de la `resource.kubernetesDetails.kubernetesWorkloadDetails` sección, ese pod o recurso de carga de trabajo se ha visto potencialmente comprometido. Un GuardDuty hallazgo puede indicar que un solo pod se ha visto comprometido o que varios pods se han visto comprometidos a través de un recurso de nivel superior. Consulte los siguientes escenarios de peligro para obtener directrices sobre cómo identificar el pod o los pods que se han puesto en peligro.

Pods individuales en peligro

Si el campo `type` de la sección `resource.kubernetesDetails.kubernetesWorkloadDetails` es pods, el resultado identifica un solo pod. El campo `name` es el nombre de los pods y el campo `namespace` es su espacio de nombres.

Para obtener información sobre cómo identificar el nodo trabajador que ejecuta los pods, consulte Identificar los pods y el nodo trabajador infractores.

Pods en peligro a través de un recurso de carga de trabajo

Si el campo `type` de la sección `resource.kubernetesDetails.kubernetesWorkloadDetails` identifica un recurso de carga de trabajo, como `Deployment`, es probable que todos los pods de ese recurso de carga de trabajo estén en peligro.

Para obtener información sobre cómo identificar todos los pods del recurso de carga de trabajo y los nodos en los que se ejecutan, consulte Identificar los pods y los nodos de trabajo infractores mediante el nombre de la carga de trabajo.

Pods en peligro a través de una cuenta de servicio

Si un GuardDuty hallazgo identifica una cuenta de servicio en la `resource.kubernetesDetails.kubernetesUserDetails` sección, es probable que los pods que utilizan la cuenta de servicio identificada estén comprometidos. El nombre de usuario indicado en un resultado es una cuenta de servicio si tiene el siguiente formato: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Para obtener información sobre cómo identificar todos los pods que utilizan la cuenta de servicio y los nodos en los que se ejecutan, consulte Identificar los pods y los nodos de trabajo infractores mediante el nombre de la cuenta de servicio.

Una vez que haya identificado todos los pods comprometidos y los nodos en los que se ejecutan, consulte la guía de prácticas recomendadas de Amazon EKS para aislar el pod, rotar sus credenciales y recopilar datos para su análisis forense.

Para corregir un pod potencialmente comprometido:

1. Identifique la vulnerabilidad que puso en peligro a los pods.
2. Implemente la corrección para esa vulnerabilidad e inicie nuevos pods de reemplazo.
3. Elimine los pods vulnerables.

   Para obtener más información, consulte Reimplementar un pod o un recurso de carga de trabajo comprometido.

Si al nodo trabajador se le ha asignado una función de IAM que permite a los pods acceder a otros AWS recursos, elimina esas funciones de la instancia para evitar que el ataque cause más daños.

Del mismo modo, si al pod se le ha asignado un rol de IAM, evalúe si puede eliminar de forma segura las políticas de IAM del rol sin que ello afecte a otras cargas de trabajo.

Corregir las imágenes de contenedores potencialmente comprometidas

Cuando un GuardDuty hallazgo indica que un módulo está en peligro, la imagen utilizada para lanzarlo podría ser maliciosa o estar comprometida. GuardDuty los hallazgos identifican la imagen del contenedor en el `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` campo. Para determinar si la imagen es malintencionada, analícela en busca de malware.

Para corregir una imagen de contenedor potencialmente comprometida:

1. Deje de usar la imagen inmediatamente y elimínela del repositorio de imágenes.
2. Identifique todos los pods con la imagen potencialmente comprometida.

   Para obtener más información, consulte Identificar los módulos con nodos de trabajo e imágenes de contenedores potencialmente vulnerables o comprometidos.
3. Aísle los módulos potencialmente comprometidos, altere las credenciales y recopile datos para su análisis. Para obtener más información, consulte la guía de prácticas recomendadas de Amazon EKS.
4. Elimine todos los pods utilizando la imagen potencialmente comprometida.

Corregir los nodos de Kubernetes potencialmente comprometidos

Un GuardDuty hallazgo puede indicar que un nodo está en peligro si el usuario identificado en el hallazgo representa la identidad de un nodo o si el hallazgo indica el uso de un contenedor privilegiado.

La identidad del usuario es un nodo de trabajo si el campo username tiene el siguiente formato: `system:node:node name`. Por ejemplo, `system:node:ip-192-168-3-201.ec2.internal`. Esto indica que el adversario ha obtenido acceso al nodo y está utilizando las credenciales del nodo para comunicarse con el punto de conexión de la API de Kubernetes.

Un resultado indica el uso de un contenedor privilegiado si uno o varios de los contenedores enumerados en el resultado tienen el campo de resultado `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.` establecido en `True`.

Para corregir un nodo potencialmente comprometido:

1. Aísle el módulo, modifique sus credenciales y recopile datos para su análisis forense.

   Para obtener más información, consulte la guía de prácticas recomendadas de Amazon EKS.
2. Identifique las cuentas de servicio que utilizan todos los pods que se ejecutan en el nodo potencialmente comprometido. Revise sus permisos y rote las cuentas de servicio si es necesario.
3. Termine el nodo potencialmente comprometido.

Cómo corregir los hallazgos de Runtime Monitoring

Cuando habilitas Runtime Monitoring para tu cuenta, Amazon GuardDuty puede generar datos Tipos de búsqueda de Runtime Monitoring que indiquen posibles problemas de seguridad en tu AWS entorno. Los posibles problemas de seguridad indican una instancia de Amazon EC2, una carga de trabajo de contenedor, un clúster de Amazon EKS o un conjunto de credenciales comprometidas en su AWS entorno. El agente de seguridad supervisa los eventos de tiempo de ejecución procedentes de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulte el tipo de recurso en los detalles de búsqueda generados en la GuardDuty consola. En la siguiente sección se describen los pasos de corrección recomendados para cada tipo de recurso.

Instance

Si el tipo de recurso en los detalles del resultado es Instancia, indica que una instancia de EC2 o un nodo de EKS están potencialmente en peligro.

- Para corregir un nodo de EKS en peligro, consulte Corregir los nodos de Kubernetes potencialmente comprometidos.
- Para corregir una instancia de EC2 en peligro, consulte Corregir una instancia de Amazon EC2 potencialmente comprometida.

EKSCluster

Si el tipo de recurso en los detalles del resultado es EKSCluster, indica que un pod o un contenedor de un clúster de EKS están potencialmente en peligro.

- Para corregir un pod en peligro, consulte Corregir los pods de Kubernetes potencialmente comprometidos.

- Para corregir una imagen de contenedor en peligro, consulte Corregir las imágenes de contenedores potencialmente comprometidas.

ECSCluster

Si el tipo de recurso en los detalles de la búsqueda es ECSCluster, indica que una tarea de ECS o un contenedor dentro de una tarea de ECS está potencialmente comprometido.

1. Identifique el clúster de ECS afectado

   El hallazgo GuardDuty de Runtime Monitoring proporciona los detalles del clúster de ECS en el panel de detalles del hallazgo o en la `resource.ecsClusterDetails` sección del JSON de búsqueda.

2. Identifique la tarea de ECS afectada

   El hallazgo GuardDuty de Runtime Monitoring proporciona los detalles de la tarea de ECS en el panel de detalles del hallazgo o en la `resource.ecsClusterDetails.taskDetails` sección del JSON de búsqueda.

3. Aísle la tarea afectada

   Aísle la tarea afectada negando todo el tráfico de entrada y salida a la tarea. Una regla que prohíba todo el tráfico puede ayudar a detener un ataque que ya está en marcha, ya que interrumpe todas las conexiones con la tarea.

4. Corrija la tarea comprometida

   a. Identifique la vulnerabilidad que puso en peligro la tarea.

   b. Implemente la solución para esa vulnerabilidad y comience de nuevo la tarea de reemplazo.

   c. Detenga la tarea vulnerable.

Container

Si el tipo de recurso en los detalles del resultado es Contenedor, indica que un contenedor independiente está potencialmente en peligro.

- Para corregirlo, consulte Corregir un contenedor independiente potencialmente comprometido.
- Si el resultado se genera en varios contenedores con la misma imagen de contenedor, consulte Corregir las imágenes de contenedores potencialmente comprometidas.

- Si el contenedor ha accedido al host de EC2 subyacente, es posible que las credenciales de la instancia asociadas se hayan puesto en peligro. Para obtener más información, consulte Corregir las credenciales potencialmente comprometidas AWS.
- Si un agente potencialmente malintencionado ha accedido al nodo de EKS subyacente o a una instancia de EC2, consulte la corrección recomendada en las pestañas EKSCluster e Instancia.

Corrección de imágenes de contenedor en peligro

Cuando un GuardDuty hallazgo indica que una tarea está en peligro, la imagen utilizada para iniciarla podría ser maliciosa o estar comprometida. GuardDuty los resultados identifican la imagen del contenedor en el `resource.ecsClusterDetails.taskDetails.containers.image` campo. Para determinar si la imagen es maliciosa o no, escaneándola en busca de malware.

Para corregir la imagen de un contenedor comprometida

1. Deje de usar la imagen inmediatamente y elimínela del repositorio de imágenes.
2. Identifique todas las tareas que utilizan esta imagen.
3. Detenga todas las tareas que utilizan la imagen comprometida. Actualice sus definiciones de tareas para que dejen de usar la imagen comprometida.

Corregir una base de datos potencialmente comprometida

GuardDuty genera datos Tipos de búsqueda de RDS Protection que indican un comportamiento de inicio de sesión potencialmente sospechoso y anómalo en su cuenta Bases de datos compatibles después de activarlo. GuardDuty Protección RDS Mediante la actividad de inicio de sesión de RDS, GuardDuty analiza y perfila las amenazas identificando patrones inusuales en los intentos de inicio de sesión.

> **Note**
>
> Para acceder a toda la información sobre un tipo de resultado, selecciónelo en la Tabla de resultados.

Siga estos pasos recomendados para corregir una base de datos de Amazon Aurora potencialmente comprometida en su AWS entorno.

Temas

Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos

Los siguientes pasos recomendados pueden ayudarlo a corregir una base de datos de Aurora potencialmente en peligro que presenta un comportamiento atípico en relación con los eventos de inicio de sesión correctos.

1. Identifique la base de datos y el usuario afectados.

   El GuardDuty resultado generado proporciona el nombre de la base de datos afectada y los detalles de usuario correspondientes. Para obtener más información, consulte Detalles de los resultados.
2. Confirme si este comportamiento es esperado o inesperado.

   En la siguiente lista se especifican los posibles escenarios que pueden haber provocado GuardDuty la generación de un hallazgo:
   - Un usuario que inicia sesión en su base de datos después de un largo periodo de tiempo.
   - Un usuario que inicia sesión en su base de datos de forma ocasional (por ejemplo, un analista financiero que inicia sesión cada trimestre).
   - Un agente potencialmente sospechoso que participa en un intento de inicio de sesión correcto podría poner en peligro la base de datos.
3. Comience este paso si el comportamiento es inesperado.

   1. Restrinja el acceso a la base de datos.

      Restrinja el acceso a la base de datos para las cuentas sospechosas y el origen de esta actividad de inicio de sesión. Para obtener más información, consulte Corrección de credenciales potencialmente en peligro y Restricción del acceso a la red.

2. Evalúe el impacto y determine a qué información se accedió.
   - Si están disponibles, revise los registros de auditoría para identificar los datos a los que se puede haber accedido. Para obtener más información, consulte Supervisión de eventos, registros y flujos en un clúster de bases de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora.
   - Determine si se accedió a información confidencial o protegida o si se modificó.

Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos

Los siguientes pasos recomendados pueden ayudarlo a corregir una base de datos de Aurora potencialmente en peligro que presenta un comportamiento atípico en relación con los eventos de inicio de sesión fallidos.

1. Identifique la base de datos y el usuario afectados.

   El GuardDuty resultado generado proporciona el nombre de la base de datos afectada y los detalles de usuario correspondientes. Para obtener más información, consulte Detalles de los resultados.
2. Identifique el origen de los intentos de inicio de sesión fallidos.

   La GuardDuty búsqueda generada proporciona la dirección IP y la organización de la ASN (si se trata de una conexión pública) en la sección Actor del panel de búsqueda.

   Un sistema autónomo (AS) es un grupo de uno o varios prefijos de IP (listas de direcciones IP accesibles en una red) administrado por uno o más operadores de red que mantienen una política de enrutamiento única y claramente definida. Los operadores de red necesitan números de sistemas autónomos (ASN) para controlar el enrutamiento en sus redes e intercambiar información de enrutamiento con otros proveedores de servicios de internet (ISP).
3. Confirme que este comportamiento es inesperado.

   Examine si esta actividad representa un intento de obtener acceso adicional no autorizado a la base de datos de la siguiente manera:
   - Si el origen es interno, compruebe si una aplicación está mal configurada y si está intentando conectarse repetidamente.

- Si se trata de un agente externo, compruebe si la base de datos correspondiente es pública o está mal configurada y, por lo tanto, permite que posibles actores malintencionados utilicen nombres de usuario comunes por fuerza bruta.

4. Comience este paso si el comportamiento es inesperado.

    1. Restrinja el acceso a la base de datos.

        Restrinja el acceso a la base de datos para las cuentas sospechosas y el origen de esta actividad de inicio de sesión. Para obtener más información, consulte Corrección de credenciales potencialmente en peligro y Restricción del acceso a la red.

    2. Analice la causa raíz y determine los pasos que podrían haber llevado a esta actividad.

        Configure una alerta para recibir una notificación cuando una actividad modifique una política de red y cree un estado no seguro. Para obtener más información, consulte Firewall policies in AWS Network Firewall en la Guía para desarrolladores deAWS Network Firewall .

Corrección de credenciales potencialmente en peligro

Un GuardDuty hallazgo puede indicar que las credenciales de usuario de una base de datos afectada se han visto comprometidas cuando el usuario identificado en el hallazgo ha realizado una operación inesperada en la base de datos. Puede identificar el usuario en la sección Detalles del usuario de base de datos de RDS del panel de resultados de la consola o en `resource.rdsDbUserDetails` del JSON de resultados. Estos detalles del usuario incluyen el nombre de usuario, la aplicación utilizada, la base de datos a la que se ha accedido, la versión de SSL y el método de autenticación.

- Para revocar el acceso o rotar las contraseñas de usuarios específicos que participan en el resultado, consulte Seguridad con Amazon Aurora MySQL o Seguridad con Amazon Aurora PostgreSQL en la Guía del usuario de Amazon Aurora.
- Úselo AWS Secrets Manager para almacenar de forma segura y rotar automáticamente los secretos de las bases de datos de Amazon Relational Database Service (RDS). Para obtener más información, consulte Tutoriales deAWS Secrets Manager en la Guía del usuario deAWS Secrets Manager .
- Utilice la autenticación de bases de datos de IAM para administrar el acceso de los usuarios a las bases de datos sin necesidad de contraseñas. Para obtener más información, consulte Autenticación de bases de datos de IAM en la Guía del usuario de Amazon Aurora.

Para obtener más información, consulte Prácticas recomendadas de seguridad para Amazon Relational Database Service en la Guía del usuario de Amazon RDS.

Restricción del acceso a la red

Un GuardDuty hallazgo puede indicar que se puede acceder a una base de datos más allá de las aplicaciones o de la Nube Privada Virtual (VPC). Si la dirección IP remota del resultado es un origen de conexión inesperado, audite los grupos de seguridad. Encontrará una lista de los grupos de seguridad adjuntos a la base de datos en Grupos de seguridad, en la consola https://console.aws.amazon.com/rds/ o en `resource.rdsDbInstanceDetails.dbSecurityGroups` del JSON de resultados. Para obtener más información sobre la configuración de los grupos de seguridad, consulte Control de acceso con grupos de seguridad en la Guía del usuario de Amazon RDS.

Si utiliza un firewall, restrinja el acceso a la red a la base de datos; para ello, reconfigure las listas de control de acceso a la red (NACL). Para obtener más información, consulte Firewall in AWS Network Firewall en la Guía para desarrolladores deAWS Network Firewall .

Corregir una función Lambda potencialmente comprometida

Si se GuardDuty genera un resultado de Lambda Protection y la actividad es inesperada, la función Lambda puede verse comprometida. Recomendamos seguir estos pasos para corregir una función de Lambda en peligro.

Corrección de los resultados de la protección de Lambda

1. Identifique la versión de la función Lambda potencialmente comprometida.

   Una GuardDuty búsqueda de Lambda Protection proporciona el nombre, el nombre del recurso de Amazon (ARN), la versión de la función y el ID de revisión asociados a la función de Lambda que aparecen en los detalles de la búsqueda.
2. Identifique el origen de la actividad potencialmente sospechosa.

   a. Revise el código asociado a la versión de la función de Lambda implicada en el resultado.

   b. Revise las bibliotecas y capas importadas de la versión de la función de Lambda implicada en el resultado.

c. Si ha activado AWS Lambda las funciones de digitalización en Amazon Inspector, revise las conclusiones de Amazon Inspector asociadas a la función Lambda implicada en la búsqueda.

d. Revise los AWS CloudTrail registros para identificar el factor principal que provocó la actualización de la función y asegúrese de que la actividad estaba autorizada o prevista.

3. Corrija la función Lambda potencialmente comprometida.

a. Deshabilite los desencadenadores de ejecución de la función de Lambda implicada en el resultado. Para obtener más información, consulte. DeleteFunctionEventInvokeConfig

b. Revise el código de Lambda y actualice las importaciones de bibliotecas y las capas de la función de Lambda para eliminar las bibliotecas y las capas potencialmente sospechosas.

c. Mitigue los resultados de Amazon Inspector relacionados con la función de Lambda implicada en el resultado.

Administrar varias cuentas en Amazon GuardDuty

Cuando su AWS entorno tiene varias cuentas, puede administrarlas designando una AWS cuenta como su cuenta de administrador. A continuación, puede asociar otras AWS cuentas a esta cuenta de administrador como cuentas de miembros. Esta cuenta de GuardDuty administrador designada puede configurar los planes de protección. GuardDuty Hay dos formas de asociar cuentas a una cuenta de administrador: crear una organización utilizando una cuenta de administrador AWS Organizations y una o más cuentas de miembros que pertenezcan a esta organización, o enviar una invitación a una AWS cuenta a través de ella GuardDuty.

GuardDuty recomienda utilizar AWS Organizations este método. Para obtener más información sobre la configuración de una organización, consulte Creación de una organización en la Guía del usuario de AWS Organizations .

Administrar varias cuentas con AWS Organizations

Si la cuenta que desea especificar como cuenta de GuardDuty administrador forma parte de una organización AWS Organizations, puede especificar esa cuenta como administrador delegado de la organización. GuardDuty La cuenta que está registrada como administrador delegado se convierte automáticamente en la cuenta de GuardDuty administrador.

Puede usar esta cuenta de administrador para habilitar y administrar GuardDuty cualquier cuenta Cuenta de AWS de la organización al agregar esa cuenta como cuenta de miembro.

Si ya tiene una cuenta de GuardDuty administrador con cuentas de miembro asociadas mediante invitación, puede registrar esa cuenta como administrador GuardDuty delegado de la organización. Cuando lo haga, todas las cuentas de miembro asociadas actualmente seguirán siendo miembros, lo que le permitirá aprovechar al máximo la funcionalidad adicional de administrar sus GuardDuty cuentas con AWS Organizations ella.

Para obtener más información sobre cómo admitir la entrada de varias cuentas GuardDuty a través de una organización, consulteAdministrar GuardDuty cuentas con AWS Organizations.

Administración de varias cuentas a través de invitaciones

Si las cuentas que desea asociar no forman parte de su organización, puede especificar una cuenta de administrador GuardDuty y, a continuación, utilizarla para invitar a otras personas Cuentas de

AWS a convertirse en cuentas de miembros. Cuando la cuenta invitada acepta la invitación, se convierte en una cuenta de GuardDuty miembro asociada a la cuenta de administrador.

Para obtener más información sobre cómo admitir varias cuentas mediante invitación, GuardDuty consulteAdministrar GuardDuty cuentas por invitación.

Comprender la relación entre la cuenta de GuardDuty administrador y las cuentas de los miembros

Cuando se utiliza GuardDuty en un entorno de varias cuentas, la cuenta de administrador puede gestionar ciertos aspectos de las cuentas de los miembros GuardDuty en nombre de las cuentas de los miembros. Las principales funciones que puede tener la cuenta de administrador son las siguientes:

- Agregar y quitar cuentas miembro asociadas. El proceso por el que se realiza esta acción es distinto en función de si las cuentas se han asociado a través de una organización o de una invitación.
- Gestione el estado de las cuentas GuardDuty de los miembros asociadas, incluidas la activación y la suspensión. GuardDuty

  > **Note**
  >
  > Las cuentas de administrador delegado se gestionan mediante la AWS Organizations activación automática de GuardDuty las cuentas añadidas como miembros.

- Personalice los hallazgos dentro de la GuardDuty red mediante la creación y administración de reglas de supresión, listas de IP confiables y listas de amenazas. Las cuentas miembro pierden el acceso a estas características en los entornos con varias cuentas.

En la siguiente tabla se detalla la relación entre la cuenta de GuardDuty administrador y las cuentas de los miembros.

En esta tabla:

- Propia: una cuenta solo puede realizar la acción indicada para su propia cuenta.
- Cualquiera: una cuenta puede realizar la acción indicada para cualquier cuenta asociada.

- Todas: una cuenta puede realizar la acción indicada y se aplica a todas las cuentas asociadas. Por lo general, la cuenta que realiza esta acción es una cuenta de GuardDuty administrador designada

Las celdas de la tabla con guiones (—) indican que la cuenta no puede realizar la acción indicada.

Action	A través de AWS Organizations		Por invitación	
	Cuenta de GuardDuty administrador delegado	Cuenta de miembro asociada	Cuenta de GuardDuty administrador delegado	Cuenta de miembro asociada
Enable GuardDuty	Any	–	Self	Self
Enable GuardDuty automatically for the entire organization (`ALL`, `NUEVO`, `NONE`)	All	–	–	–
View all Organizations member accounts regardless of GuardDuty status	Any	–	–	–
Generate sample findings	Self	Self	Self	Self
View all GuardDuty findings	Any	Self	Any	Self

Archive GuardDuty findings	Any	–	Any	–
Apply suppressi on rules	All	–	All	–
Create trusted IP list or threat lists	All	–	All	–
Update trusted IP list or threat lists	All	–	All	–
Delete trusted IP list or threat lists	All	–	All	–
Set EventBrid ge notification frequency	All	–	All	Self
Set Amazon S3 location for exporting findings	All	–	All	Self
Enable one or more optional protection plans for the entire organization (`ALL`, `NUEVO`, `NONE`)	All	–	–	–

Enable any GuardDuty protection plan for individual accounts	Any	–	Any	Self
Disassociate a member account	Any	–	Any	–
Disassociate from an administrator account account	–	Self[#]	–	Self
Delete a disassociated member account	Any	–	Any	–
Suspend GuardDuty	Any[*]	–	Any[*]	–
Disable GuardDuty	Any[*]	–	Any[*]	–

- # Indica que la cuenta solo puede realizar esta acción si la cuenta de GuardDuty administrador delegado no ha configurado la preferencia de activación automática para los miembros de `ALL` la organización.
- * Indica que esta acción debe realizarse en todas las cuentas asociadas antes de realizarla en esta cuenta. Tras desasociar estas cuentas, debe eliminarlas. Para obtener más información sobre la realización de estas tareas en su organización, consulteMantener su organización dentro GuardDuty.

Administrar GuardDuty cuentas con AWS Organizations

Si la utiliza GuardDuty con una AWS organización, la cuenta de administración de esa organización puede designar cualquier cuenta de la organización como cuenta de GuardDuty administrador delegado. Para esta cuenta de administrador, GuardDuty se habilita automáticamente solo en la

cuenta designada Región de AWS. Esta cuenta también tiene permiso para habilitar y administrar GuardDuty todas las cuentas de la organización dentro de esa región. La cuenta de administrador puede ver los miembros de esta AWS organización y añadirlos a ella.

Si ya ha configurado una cuenta de GuardDuty administrador con cuentas de miembro asociadas mediante invitación y las cuentas de miembros forman parte de la misma organización, su tipo cambia de By Invitation a Via Organizations cuando configura una cuenta de GuardDuty administrador delegado para su organización. Si una cuenta de GuardDuty administrador delegado ha agregado previamente miembros por invitación que no forman parte de la misma organización, su tipo sigue siendo por invitación. En ambos casos, las cuentas agregadas anteriormente son cuentas de miembros que están asociadas a la cuenta de GuardDuty administrador delegado de la organización.

Puede seguir añadiendo cuentas como miembros aunque no pertenezcan a su organización. Para obtener más información, consulte Agregación y administración de cuentas por invitación o Designar una cuenta de GuardDuty administrador delegado y administrar los miembros mediante la consola GuardDuty .

Contenido

Consideraciones y recomendaciones a la hora de designar una cuenta de administrador delegado GuardDuty

Las siguientes consideraciones y recomendaciones pueden ayudarle a entender cómo funciona una cuenta de GuardDuty administrador delegado en: GuardDuty

Una cuenta de GuardDuty administrador delegado puede gestionar un máximo de 50 000 miembros.

Hay un límite de 50 000 cuentas de miembros por cuenta de GuardDuty administrador delegado. Esto incluye las cuentas de miembros que se agreguen a través de su organización AWS Organizations o las que hayan aceptado la invitación de la cuenta de GuardDuty administrador para unirse a su organización. Sin embargo, puede haber más de 50 000 cuentas en su AWS organización.

Si superas el límite de 50 000 cuentas de CloudWatch miembros, recibirás una notificación y un correo electrónico a la cuenta de GuardDuty administrador delegado designada. AWS Health Dashboard

Una cuenta de GuardDuty administrador delegado es regional.

A diferencia AWS Organizations de, GuardDuty es un servicio regional. Las cuentas de GuardDuty administrador delegado y sus cuentas de miembros deben añadirse AWS Organizations en cada región deseada en la que se haya GuardDuty activado. Si la cuenta de administración de la organización designa una cuenta de GuardDuty administrador delegado solo en EE. UU. Este (Norte de Virginia), la cuenta de GuardDuty administrador delegado solo administrará las cuentas de los miembros que se agreguen a la organización en esa región. Para obtener más información sobre la paridad de funciones en las regiones en las que GuardDuty está disponible, consulte. Regiones y puntos de conexión

Casos especiales para las regiones que se suscriben

- Cuando una cuenta de GuardDuty administrador delegado opta por no participar en una región de suscripción, incluso si su organización tiene la configuración de activación GuardDuty automática configurada solo para cuentas de miembros nuevos (`NEW`) o para todas las cuentas de miembros (`ALL`), GuardDuty no se puede habilitar para ninguna cuenta de miembro de la organización que esté deshabilitada actualmente. GuardDuty Para obtener información sobre la configuración de las cuentas de sus miembros, abra Cuentas en el panel de navegación de la GuardDuty consola o utilice la API. ListMembers
- Cuando trabaje con la configuración de GuardDuty activación automática establecida en`NEW`, asegúrese de que se cumpla la siguiente secuencia:

  1. Las cuentas de los miembros se registran en una región de suscripción.
  2. Agregue las cuentas de los miembros a su organización en. AWS Organizations

  Si cambias el orden de estos pasos, la configuración de GuardDuty activación automática con no **`NEW`** funcionará en la región de suscripción específica porque la cuenta de miembro ya no es nueva en la organización. GuardDuty ofrece dos soluciones alternativas:

- Establezca la configuración de GuardDuty activación automática enALL, que incluye las cuentas de los miembros nuevas y existentes. En este caso, el orden de estos pasos no es relevante.
- Si la cuenta de un miembro ya forma parte de su organización, gestione la GuardDuty configuración de esta cuenta de forma individual en la región de suscripción específica mediante la GuardDuty consola o la API.

Se recomienda que una AWS organización tenga la misma cuenta de GuardDuty administrador delegado en todas las. Regiones de AWS

Le recomendamos que designe la misma cuenta de GuardDuty administrador delegado para su organización en todos los lugares en los que la Regiones de AWS haya activado. GuardDuty Si designa una cuenta como cuenta de GuardDuty administrador delegado en una región, se recomienda que utilice la misma cuenta que cuenta de GuardDuty administrador delegado en todas las demás regiones.

Puede designar una nueva cuenta de GuardDuty administrador delegado en cualquier momento. Para obtener más información sobre cómo eliminar la cuenta de GuardDuty administrador delegado existente, consulte. Cambiar la cuenta de GuardDuty administrador delegado

No se recomienda configurar la cuenta de administración de la organización como cuenta de GuardDuty administrador delegado.

La cuenta de administración de su organización puede ser la cuenta de GuardDuty administrador delegado. Sin embargo, las prácticas recomendadas de seguridad de AWS siguen el principio de privilegios mínimos y no recomiendan esta configuración.

El cambio de una cuenta de GuardDuty administrador delegado no desactiva las cuentas de GuardDuty los miembros.

Si elimina una cuenta de GuardDuty administrador delegado, GuardDuty elimina todas las cuentas de miembro asociadas a esta cuenta de administrador delegado GuardDuty . GuardDuty sigue habilitada para todas estas cuentas de miembros.

Permisos necesarios para designar una cuenta de GuardDuty administrador delegado

Al delegar una cuenta de GuardDuty administrador delegado, debes tener permisos para habilitarla, así GuardDuty como determinadas AWS Organizations acciones de la API. Puede agregar la siguiente instrucción al final de una política de IAM para otorgar estos permisos:

```
{
    "Sid": "PermissionsForGuardDutyAdmin",
    "Effect": "Allow",
    "Action": [
        "guardduty:EnableOrganizationAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
```

Además, si deseas designar tu cuenta de AWS Organizations administración como cuenta de GuardDuty administrador GuardDuty delegado, esa entidad necesitará `CreateServiceLinkedRole` permisos para inicializarse. GuardDuty Para ello, añada la siguiente declaración a la política de IAM y sustituya *111122223333* por el Cuenta de AWS ID de la cuenta de administración de su organización:

```
{
 "Sid": "PermissionsToEnableGuardDuty"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty",
 "Condition": {
  "StringLike": {
   "iam:AWSServiceName": "guardduty.amazonaws.com"
  }
 }
}
```

Designar una cuenta de GuardDuty administrador delegado y administrar los miembros mediante la consola GuardDuty

Contenido

Paso 1: Designe una cuenta de GuardDuty administrador delegado para su organización

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Para iniciar sesión, utilice las credenciales de la cuenta de administración de su organización de AWS Organizations .
2. Si ya ha activado GuardDuty la cuenta de administración, omita este paso y siga el siguiente.

   Si GuardDuty aún no la has activado, selecciona Comenzar y, a continuación, designa una cuenta de GuardDuty administrador delegado en la GuardDuty página de bienvenida.

   > **Note**
   >
   > La cuenta de administración debe tener la función GuardDuty vinculada al servicio (SLR) para que la cuenta de GuardDuty administrador delegado pueda habilitarla y administrarla en esa cuenta. GuardDuty Una vez que habilita GuardDuty la cuenta de administración en una región, esta SLR se crea automáticamente.
3. Realice este paso una vez que haya activado GuardDuty la cuenta de administración. En el panel de navegación de la GuardDuty consola, selecciona Configuración. En la página de configuración, introduzca el Cuenta de AWS ID de 12 dígitos de la cuenta que desee designar como cuenta de GuardDuty administrador delegado de la organización.

   Asegúrese de activar la cuenta GuardDuty de GuardDuty administrador delegado recién designada; de lo contrario, no podrá realizar ninguna acción.
4. Elija Delegar.

5. (Recomendado) Repita el paso anterior para designar la cuenta de GuardDuty administrador delegado en cada una de las cuentas en las que la Región de AWS haya GuardDuty activado.

Paso 2: Configurar las preferencias de activación automática para su organización

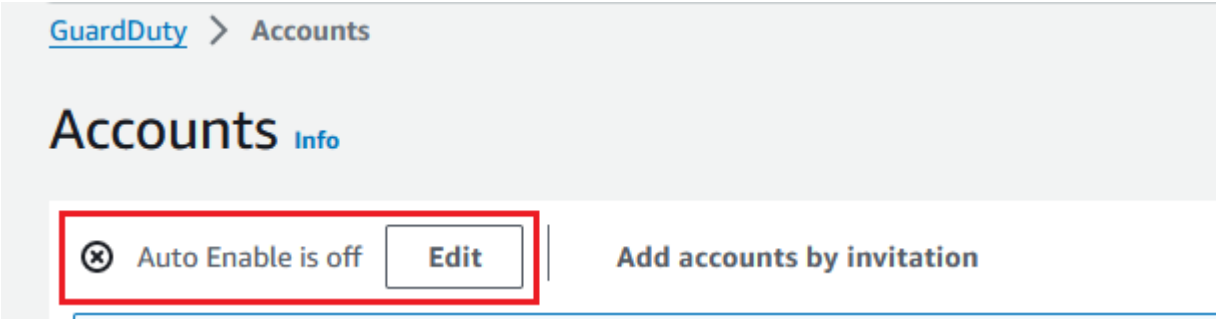
1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Para iniciar sesión, utilice las credenciales de la cuenta de GuardDuty administrador.

2. En el panel de navegación, elija Accounts (Cuentas).

   La página Cuentas proporciona opciones de configuración para que la cuenta de GuardDuty administrador se active automáticamente GuardDuty y los planes de protección opcionales en nombre de las cuentas de los miembros que pertenecen a la organización.

3. Para actualizar la configuración de activación automática existente, selecciona Editar.



   Este soporte está disponible para configurar todos GuardDuty los planes de protección opcionales compatibles con usted. Región de AWS Puede seleccionar una de las siguientes opciones de configuración GuardDuty en nombre de sus cuentas de miembro:

   - Habilitar para todas las cuentas (**ALL**): seleccione esta opción para habilitar la opción correspondiente para todas las cuentas de una organización. Esto incluye las cuentas nuevas que se unen a la organización y las cuentas que pueden haber sido suspendidas o eliminadas de la organización. Esto también incluye la cuenta de GuardDuty administrador delegado.

     > **Note**
     >
     > La actualización de la configuración de todas las cuentas de los miembros puede tardar hasta 24 horas.

- Habilitación automática para cuentas nuevas (**`NEW`**): seleccione esta opción para habilitar GuardDuty automáticamente los planes de protección opcionales solo para las cuentas de los nuevos miembros cuando se unan a su organización.
- No activar (**`NONE`**): seleccione esta opción para evitar que se active la opción correspondiente para las nuevas cuentas de su organización. En este caso, la cuenta de GuardDuty administrador administrará cada cuenta de forma individual.

  Cuando actualizas la configuración de activación automática desde `ALL` o `NEW` hasta`NONE`, esta acción no deshabilita la opción correspondiente para tus cuentas existentes. Esta configuración se aplicará a las nuevas cuentas que se unan a la organización. Después de actualizar la configuración de activación automática, ninguna cuenta nueva tendrá habilitada la opción correspondiente.

> **Note**
>
> Cuando una cuenta de GuardDuty administrador delegado opta por no participar en una región de suscripción, incluso si su organización tiene la configuración de activación GuardDuty automática configurada solo para cuentas de miembros nuevos (`NEW`) o para todas las cuentas de miembros (`ALL`), GuardDuty no se puede habilitar para ninguna cuenta de miembro de la organización que esté deshabilitada actualmente. GuardDuty Para obtener información sobre la configuración de las cuentas de sus miembros, abra Cuentas en el panel de navegación de la GuardDuty consola o utilice la API. ListMembers

4. Elija Guardar cambios.
5. (Opcional) Si quiere usar las mismas preferencias en cada región, actualice las preferencias en cada una de las regiones compatibles por separado.

   Es posible que algunos de los planes de protección opcionales no estén disponibles en todos los Regiones de AWS lugares donde GuardDuty están disponibles. Para obtener más información, consulte Regiones y puntos de conexión.

Paso 3: agregación de cuentas como miembros de su organización

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

Para iniciar sesión, utilice las credenciales de la cuenta de GuardDuty administrador delegado.

2. En el panel de navegación, elija Accounts (Cuentas).

   La tabla de cuentas muestra todas las cuentas que se agregan A través de organizaciones (AWS Organizations) o Por invitación. Si una cuenta de miembro no está asociada a la cuenta de GuardDuty administrador de la organización, el estado de esta cuenta de miembro es No es miembro.

3. Seleccione uno o varios ID de cuenta que desee agregar como miembros. Estos ID de cuenta deben tener el Tipo como A través de organizaciones.

   Las cuentas que se agregan por invitación no forman parte de su organización. Puede administrador dichas cuentas de forma individual. Para obtener más información, consulte Administración de cuentas por invitación.

4. Seleccione el menú desplegable Acciones y, a continuación, elija Agregar miembro. Después de añadir esta cuenta como miembro, se aplicará la GuardDuty configuración de activación automática. En función de los ajustes establecidosthe section called “Paso 1: Designe una cuenta de GuardDuty administrador delegado para su organización”, la GuardDuty configuración de estas cuentas puede cambiar.

5. Puede seleccionar la flecha hacia abajo de la columna Estado para ordenar las cuentas según el estado No es miembro y, a continuación, elegir las cuentas que no GuardDuty estén habilitadas en la región actual.

   Si aún no se ha agregado como miembro ninguna de las cuentas que figuran en la tabla de cuentas, puedes habilitarlas GuardDuty en la región actual para todas las cuentas de la organización. Elija Habilitar en el encabezado de la parte superior de la página. Esta acción activa automáticamente la GuardDuty configuración de activación automática, de modo que GuardDuty se habilita para cualquier cuenta nueva que se una a la organización.

6. Elija Confirmar para agregar las cuentas como miembros. Esta acción también se activa GuardDuty para todas las cuentas seleccionadas. El Estado de las cuentas invitadas cambiará a Habilitado.

7. (Recomendado) Repita estos pasos en cada una de ellas Región de AWS. Esto garantiza que la cuenta de GuardDuty administrador delegado pueda gestionar las búsquedas y otras configuraciones de las cuentas de los miembros en todas las regiones en las que haya GuardDuty activado la cuenta.

La función de activación automática se habilita GuardDuty para todos los futuros miembros de su organización. Esto permite que su cuenta de GuardDuty administrador delegado administre los nuevos miembros que se creen o se agreguen a la organización. Cuando el número de cuentas de miembros alcanza el límite de 50 000, la función de activación automática se desactiva automáticamente. Si eliminas una cuenta de miembro y el número total de miembros se reduce a menos de 50 000, la función de activación automática se vuelve a activar.

Paso 4 (opcional): configurar los planes de protección para cuentas individuales

Puede configurar planes de protección para cuentas individuales a través de la página Cuentas.

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Utilice las credenciales de la cuenta GuardDuty de administrador delegado.
2. En el panel de navegación, elija Accounts (Cuentas).
3. Seleccione una o más cuentas donde desee configurar un plan de protección. Repita los pasos siguientes para cada plan de protección que desee configurar:

   a. Seleccione Editar planes de protección.

   b. En la lista de planes de protección, elija aquel que desee configurar.

   c. Elija una de las acciones que desee llevar a cabo para este plan de protección y, a continuación, seleccione Confirmar.

   d. Para la cuenta seleccionada, la columna correspondiente al plan de protección configurado mostrará la configuración actualizada como Habilitado o No habilitado.

Designar una cuenta de GuardDuty administrador GuardDuty delegado y gestionar los miembros mediante la API

Contenido

Paso 1: Designe una cuenta de GuardDuty administrador delegado para su organización AWS

1. Ejecute enableOrganizationAdminAccountcon las credenciales de la cuenta Cuenta de AWS de administración de la organización.

   - Alternativamente, puede usarlo AWS Command Line Interface para hacer esto. El siguiente AWS CLI comando designa una cuenta de GuardDuty administrador delegado únicamente para su región actual. Ejecuta el siguiente AWS CLI comando y asegúrate de sustituir *1111* por el Cuenta de AWS ID de la cuenta que deseas designar como cuenta de administrador delegado GuardDuty :

     ```
     aws guardduty enable-organization-admin-account --admin-account-id 111111111111
     ```

     Para designar la cuenta de GuardDuty administrador delegado para otras regiones, especifique la región en el comando. AWS CLI El siguiente ejemplo muestra cómo habilitar una cuenta de GuardDuty administrador delegado en el oeste de EE. UU. (Oregón). Asegúrese de sustituir *us-west-2* por la región a la que desee asignar la cuenta de administrador GuardDuty delegado GuardDuty .

     ```
     aws guardduty enable-organization-admin-account --admin-account-id 111111111111
      --region us-west-2
     ```

     Para obtener información sobre la ubicación Regiones de AWS GuardDuty disponible, consulte. Regiones y puntos de conexión

   Si no GuardDuty está habilitada para su cuenta de GuardDuty administrador delegado, no podrá realizar ninguna acción. Si aún no lo ha hecho, asegúrese de habilitarla GuardDuty para la cuenta de GuardDuty administrador delegado recién designada.

2. (Recomendado) repita el paso anterior para designar la cuenta de GuardDuty administrador delegado en cada una de las cuentas en las que la Región de AWS haya GuardDuty activado.

Paso 2: configuración de las preferencias de habilitación automática para la organización

1. 1. Ejecute con UpdateOrganizationConfigurationlas credenciales de la cuenta de GuardDuty administrador delegado para configurar GuardDuty automáticamente los planes de protección opcionales en esa región para su organización

   Para encontrar los `detectorId` de su cuenta y región actuales, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

   > **Note**
   >
   > Para obtener información sobre las distintas configuraciones de activación automática, consulte autoEnableOrganizationMiembros.

   2. Para configurar las preferencias de habilitación automática para cualquiera de los planes de protección opcionales admitidos en su región, siga los pasos que se indican en las secciones de la documentación correspondientes a cada plan de protección.
   3. Puede validar las preferencias de su organización en la región actual. Ejecute describeOrganizationConfiguration. Asegúrese de especificar el ID de detector de la cuenta de GuardDuty administrador delegado.

   > **Note**
   >
   > La actualización de la configuración de todas las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

- 1. Como alternativa, ejecute el siguiente AWS CLI comando para configurar las preferencias y habilitar o deshabilitar automáticamente GuardDuty en esa región las nuevas cuentas (`NEW`) que se unan a la organización, todas las cuentas (`ALL`) o ninguna de las cuentas (`NONE`) de la organización. Para obtener más información, consulte autoEnableOrganizationMiembros. Según sus preferencias, es posible que deba sustituir `NEW` por `ALL` o `NONE`. Si configura el plan de protección con`ALL`, el plan de protección también se habilitará para la cuenta de GuardDuty administrador delegado. Asegúrese de especificar el ID del detector de la cuenta de GuardDuty administrador delegado que gestiona la configuración de la organización.

Para encontrar el de `detectorId` su cuenta y su región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
```

2. Puede validar las preferencias de su organización en la región actual. Ejecute el siguiente AWS CLI comando utilizando el ID de detector de la cuenta de GuardDuty administrador delegado.

```
aws guardduty describe-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0
```

2. (Se recomienda) repita los pasos anteriores en cada región utilizando el ID de detector de la cuenta de GuardDuty administrador delegado.

> **Note**
>
> Cuando una cuenta de GuardDuty administrador delegado opta por no participar en una región de suscripción, incluso si su organización tiene la configuración de activación GuardDuty automática configurada solo para cuentas de miembros nuevos (`NEW`) o para todas las cuentas de miembros (`ALL`), GuardDuty no se puede habilitar para ninguna cuenta de miembro de la organización que esté deshabilitada actualmente. GuardDuty Para obtener información sobre la configuración de las cuentas de sus miembros, abra Cuentas en el panel de navegación de la GuardDuty consola o utilice la API. ListMembers

Paso 3: agregación de cuentas como miembros de su organización

- Ejecute con CreateMembersla las credenciales de la cuenta de GuardDuty administrador delegado designada en el paso anterior.

  Debe especificar el ID de detector regional de la cuenta de GuardDuty administrador delegado y los detalles de la cuenta (Cuenta de AWS ID y direcciones de correo electrónico correspondientes) de las cuentas que desee añadir como GuardDuty miembros. Puede crear uno o varios miembros con esta operación de API.

Cuando trabajes CreateMembers en tu organización, las preferencias de activación automática para los nuevos miembros se aplicarán a medida que las nuevas cuentas de miembros se unan a tu organización. Si trabajas CreateMembers con una cuenta de miembro existente, la configuración de la organización también se aplicará a los miembros existentes. Esto podría cambiar la configuración actual de las cuentas de los miembros existentes.

Ejecuta ListAccountsla referencia de la AWS Organizations API para ver todas las cuentas de la AWS organización.

> **Important**
>
> Cuando añadas una cuenta como GuardDuty miembro, se GuardDuty habilitará automáticamente en esa región. Hay una excepción a la cuenta de administración de la organización. Antes de que la cuenta de administración se añada como GuardDuty miembro, debe estar GuardDuty habilitada.

- Como alternativa, puede utilizar AWS Command Line Interface. Ejecute el siguiente comando de la AWS CLI y asegúrese de utilizar su propio ID de detector válido, su ID de Cuenta de AWS y la dirección de correo electrónico asociada al ID de la cuenta.

  Para encontrar la correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  account-details AccountId=111122223333,Email=guardduty-member-name@amazon.com
  ```

  Para ver una lista de todos los miembros de la organización, ejecuta el siguiente AWS CLI comando:

  ```
  aws organizations list-accounts
  ```

Después de añadir esta cuenta como miembro, se aplicará la GuardDuty configuración de activación automática.

Mantener su organización dentro GuardDuty

Como cuenta de GuardDuty administrador delegado, usted es responsable de mantener la configuración GuardDuty y sus planes de protección opcionales para todas las cuentas de su organización, en cada una de ellas compatibles. Región de AWS En las siguientes secciones se proporcionan las opciones para mantener el estado de configuración de cualquiera de sus planes de protección opcionales GuardDuty o de cualquiera de sus planes de protección opcionales:

Para mantener el estado de configuración de toda la organización en cada región

- Configure las preferencias de activación automática para toda la organización mediante la GuardDuty consola: puede habilitarla GuardDuty automáticamente para todos (`ALL`) los miembros de la organización o para los nuevos (`NEW`) miembros que se unan a la organización, o puede optar por no (`NONE`) habilitarla automáticamente para ninguno de los miembros de la organización.

  También puede configurar los mismos ajustes o ajustes diferentes para cualquiera de los planes de protección incluidos. GuardDuty

  La actualización de la configuración de todas las cuentas de los miembros de la organización puede tardar hasta 24 horas.
- Actualice las preferencias de activación automática mediante la API: ejecute UpdateOrganizationConfigurationpara configurar GuardDuty automáticamente sus planes de protección opcionales para la organización. Cuando vayas CreateMembersa añadir nuevas cuentas de miembros a tu organización, los ajustes configurados se aplicarán automáticamente. Si trabajas CreateMembers con una cuenta de miembro existente, la configuración de la organización también se aplicará a los miembros existentes. Esto podría cambiar la configuración actual de las cuentas de los miembros existentes.

  Para ver todas las cuentas de tu organización, consulta la ListAccountsreferencia de la AWS Organizations API.

Para mantener el estado de configuración de las cuentas de los miembros de forma individual en cada región

- Para ver todas las cuentas de su organización, consulte ListAccountsla referencia de la AWS Organizations API.
- Si desea que algunas cuentas de miembros tengan un estado de configuración diferente, ejecútelas UpdateMemberDetectorspara cada cuenta de miembro de forma individual.

Puede utilizar la GuardDuty consola para realizar la misma tarea accediendo a la página de cuentas de la GuardDuty consola.

Para obtener información sobre cómo habilitar los planes de protección para cuentas individuales mediante la consola o la API, consulte la página de configuración del plan de protección correspondiente.

Cambiar la cuenta de GuardDuty administrador delegado

Puede cambiar la cuenta de GuardDuty administrador delegado de su organización en cada región y, a continuación, delegar un nuevo administrador en cada región. Para mantener una política de seguridad para las cuentas de los miembros de su organización en una región, debe tener una cuenta de GuardDuty administrador delegado en esa región.

Eliminar la cuenta de administrador delegado GuardDuty existente

Paso 1: Eliminar la cuenta de GuardDuty administrador delegado existente en cada región

1. Como cuenta de GuardDuty administrador delegado existente, enumere todas las cuentas de miembros asociadas a su cuenta de administrador. Corre ListMemberscon`OnlyAssociated=false`.
2. Si la preferencia de activación automática de alguno de los planes de protección opcionales GuardDuty o alguno de ellos está establecida en`ALL`, ejecute UpdateOrganizationConfigurationpara actualizar la configuración de la organización a uno `NEW` de los dos. `NONE` Esta acción evitará que se produzca un error al desasociar todas las cuentas de los miembros en el siguiente paso.
3. Ejecute DisassociateMemberspara desasociar todas las cuentas de miembro asociadas a la cuenta de administrador.
4. Ejecute DeleteMemberspara eliminar las asociaciones entre la cuenta de administrador y las cuentas de los miembros.
5. Como cuenta de administración de la organización, ejecute DisableOrganizationAdminAccountpara eliminar la cuenta de GuardDuty administrador delegado existente.
6. Repita estos pasos en cada uno de los Región de AWS lugares en los que tenga esta cuenta de GuardDuty administrador delegado.

Paso 2: Para anular el registro de una cuenta de GuardDuty administrador delegado existente en AWS Organizations (acción global única)

- Ejecuta DeregisterDelegatedAdministratorla referencia de la AWS Organizations API para anular el registro de la cuenta de administrador delegado GuardDuty existente en. AWS Organizations

  Como alternativa, puede ejecutar el siguiente comando: AWS CLI

  ```
  aws organizations deregister-delegated-administrator --account-id 111122223333 --
  service-principal guardduty.amazonaws.com
  ```

  Asegúrese de reemplazar *111122223333* por la cuenta de administrador delegado GuardDuty existente.

  Tras anular el registro de la antigua cuenta de GuardDuty administrador delegado, puede añadirla como cuenta de miembro a la nueva cuenta de administrador delegado. GuardDuty

Designar una nueva cuenta de administrador delegado GuardDuty en cada región

1. Designe una nueva cuenta de GuardDuty administrador delegado en cada región mediante uno de los siguientes métodos de acceso:
   - Uso de GuardDuty la consola —Paso 1: Designe una cuenta de GuardDuty administrador delegado para su organización.
   - Uso de GuardDuty la API —Paso 1: Designe una cuenta de GuardDuty administrador delegado para su organización AWS.
2. Ejecute DescribeOrganizationConfigurationpara ver la configuración de activación automática actual de su organización.

   > **Important**
   >
   > Antes de añadir miembros a la nueva cuenta de GuardDuty administrador delegado, debe comprobar la configuración de activación automática de su organización. Esta configuración es específica de la nueva cuenta de GuardDuty administrador delegado y de la región seleccionada, y no está relacionada con ellas. AWS Organizations Al añadir una cuenta de miembro de la organización (nueva o existente) a la nueva cuenta de GuardDuty administrador delegado, la configuración de activación automática de la

nueva cuenta de GuardDuty administrador delegado se aplicará en el momento de la activación GuardDuty o en cualquiera de sus planes de protección opcionales.

Para cambiar la configuración de esta organización para la nueva cuenta de GuardDuty administrador delegado, utilice uno de los siguientes métodos de acceso:

- Uso de GuardDuty la consola —Paso 2: Configurar las preferencias de activación automática para su organización.
- Uso de GuardDuty la API —Paso 2: configuración de las preferencias de habilitación automática para la organización.

Administrar GuardDuty cuentas por invitación

Para administrar cuentas que estén fuera de la organización, puede utilizar el método de invitación heredado. Con este método, su cuenta se designa como cuenta de administrador cuando otra cuenta acepta su invitación para convertirse en cuenta de miembro.

Si su cuenta no es una cuenta de administrador, puede aceptar una invitación de otra cuenta. Al aceptar, su cuenta se convierte en cuenta miembro. Una AWS cuenta no puede ser una cuenta de GuardDuty administrador y una cuenta de miembro al mismo tiempo.

Cuando aceptas una invitación de una cuenta, no puedes aceptar una invitación de otra cuenta. Para aceptar una invitación de otra cuenta, primero tendrás que desvincular tu cuenta de la cuenta de administrador existente. Como alternativa, la cuenta de administrador también puede desasociar tu cuenta y eliminarla de su organización.

Las cuentas asociadas por invitación tienen la misma account-to-member relación de administrador general que las cuentas asociadas por AWS Organizations, tal y como se describe enComprender la relación entre la cuenta de GuardDuty administrador y las cuentas de los miembros. Sin embargo, los usuarios de las cuentas de administrador de invitaciones no pueden habilitar GuardDuty en nombre de las cuentas de los miembros asociadas ni ver otras cuentas que no sean miembros de su AWS Organizations organización.

Important

La transferencia de datos entre regiones puede producirse cuando se GuardDuty crean cuentas de miembros con este método. Para verificar las direcciones de correo electrónico

de las cuentas de los miembros, GuardDuty utiliza un servicio de verificación de correo electrónico que funciona solo en la región de EE. UU. Este (Virginia del Norte).

Agregación y administración de cuentas por invitación

Elija uno de los métodos de acceso para añadir e invitar a las cuentas a convertirse en cuentas de GuardDuty miembros como cuentas de GuardDuty administrador.

Console

Paso 1: agregación de una cuenta

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, elija Accounts (Cuentas).
3. Seleccione Agregar cuentas mediante invitación en el panel superior.
4. En la página Añadir cuentas de miembros, en Introducir los detalles de la cuenta, introduzca el Cuenta de AWS ID y la dirección de correo electrónico asociados a la cuenta que desee añadir.
5. Para agregar otra fila para introducir los detalles de la cuenta de uno en uno, elija Agregar otra cuenta. También puede seleccionar Cargar un archivo .csv con los detalles de la cuenta para agregar cuentas en bloque.

   Important

   La primera línea del archivo .csv debe contener el encabezado, tal como se muestra en el ejemplo siguiente: `Account ID,Email`. Cada línea subsiguiente debe contener un único Cuenta de AWS identificador válido y su dirección de correo electrónico asociada. El formato de una fila es válido si contiene solo un Cuenta de AWS identificador y la dirección de correo electrónico asociada separados por una coma.

   ```
   Account ID,Email
   555555555555,user@example.com
   ```

6. Después de agregar todos los detalles de las cuentas, seleccione Siguiente. Puede ver las cuentas recién agregadas en la tabla Cuentas. El Estado de estas cuentas será Invitación

no enviada. Para obtener información sobre cómo enviar una invitación a una o más cuentas agregadas, consulte Step 2 - Invite an account.

Paso 2: invitación a una cuenta

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, elija Accounts (Cuentas).
3. Selecciona una o más cuentas a las que quieras invitar a Amazon GuardDuty.
4. Seleccione el menú desplegable Acciones y, a continuación, elija Invitar.
5. En el cuadro de GuardDuty diálogo Invitación a, introduce un mensaje de invitación (opcional).

   Si la cuenta invitada no tiene acceso al correo electrónico, seleccione la casilla Enviar también una notificación de correo electrónico al usuario raíz de la Cuenta de AWS del invitado y generar una alerta en la AWS Health Dashboard del invitado.
6. Seleccione Send invitation (Enviar invitación). Si los invitados tienen acceso a la dirección de correo electrónico especificada, pueden ver la invitación abriendo la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
7. Cuando el invitado acepta la invitación, el valor de la columna Estado cambia a Invitado. Para obtener más información sobre la aceptación de una invitación, consulte Step 3 - Accept an invitation.

Paso 3: aceptación de una invitación

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   > **Important**
   >
   > Debe habilitarla GuardDuty antes de poder ver o aceptar una invitación de membresía.

2. Haz lo siguiente solo si GuardDuty aún no la has activado; de lo contrario, puedes saltarte este paso y continuar con el siguiente.

   Si aún no lo has activado GuardDuty, selecciona Get Started en la GuardDuty página de Amazon.

En la GuardDuty página de bienvenida, selecciona Activar GuardDuty.

3. Después de activar GuardDuty tu cuenta, sigue los siguientes pasos para aceptar la invitación de membresía:

   a. En el panel de navegación, seleccione Configuración.

   b. Elija Cuentas.

   c. En Cuentas, asegúrese de verificar el propietario de la cuenta desde la que acepta la invitación. Active Aceptar para aceptar la invitación para hacerse miembro.

4. Tras aceptar la invitación, su cuenta pasará a ser una cuenta de GuardDuty miembro. La cuenta cuyo propietario envió la invitación pasa a ser la cuenta de GuardDuty administrador. La cuenta de administrador sabrá que ha aceptado la invitación. Se actualizará la tabla de GuardDuty cuentas de su cuenta. El valor de la columna Estado correspondiente al ID de su cuenta de miembro cambiará a Activado. El propietario de la cuenta de administrador ahora puede ver GuardDuty y administrar las configuraciones del plan de protección en nombre de su cuenta. La cuenta de administrador también puede ver y gestionar las GuardDuty conclusiones generadas para su cuenta de miembro.

API/CLI

Puede designar una cuenta de GuardDuty administrador y crear o añadir cuentas de GuardDuty miembros mediante invitación a través de las operaciones de la API. Ejecute las siguientes operaciones de GuardDuty API para designar la cuenta de administrador y las cuentas de los miembros GuardDuty.

Complete el siguiente procedimiento con las credenciales de la cuenta Cuenta de AWS que desee designar como cuenta de GuardDuty administrador.

Creación o agregación de cuentas de miembro

1. Ejecute la operación de CreateMembersAPI con las credenciales de la AWS cuenta que se ha GuardDuty activado. Esta es la cuenta que quieres que sea la GuardDuty cuenta de administrador.

   Debe especificar el ID de detección de la AWS cuenta actual y el ID de cuenta y la dirección de correo electrónico de las cuentas de las que quiere convertirse en GuardDuty miembro. Puede crear uno o varios miembros con esta operación de API.

También puede usar las herramientas de línea de AWS comandos para designar una cuenta de administrador ejecutando el siguiente comando CLI. No olvide utilizar su propio ID de detector, ID de cuenta y correo electrónico.

Para encontrar la correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-details AccountId=111122223333,Email=guardduty-member@organization.com
```

2. Ejecute InviteMemberscon las credenciales de la AWS cuenta que se ha GuardDuty activado. Esta es la cuenta que desea que sea la GuardDuty cuenta de administrador.

   Debe especificar el identificador del detector de la AWS cuenta actual y los identificadores de las cuentas de las que quiere convertirse en GuardDuty miembro. Con esta operación de la API, puede invitar a uno o varios miembros.

   > **Note**
   >
   > También puede especificar un mensaje de invitación opcional mediante el parámetro de solicitud `message`.

   También puede utilizarla AWS Command Line Interface para designar las cuentas de los miembros ejecutando el siguiente comando. No olvide utilizar su propio ID de detector y unos ID válidos para las cuentas a las que desea invitar.

   Para encontrar la correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

   ```
   aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-ids 111122223333
   ```

Aceptación de invitaciones

Complete el siguiente procedimiento con las credenciales de cada AWS cuenta que desee designar como cuenta de GuardDuty miembro.

1. Ejecute la operación de CreateDetectorAPI para cada AWS cuenta que haya sido invitada a convertirse en cuenta de GuardDuty miembro y para la que desee aceptar una invitación.

   Debe especificar si el recurso detector se va a habilitar mediante el GuardDuty servicio. Se debe crear y habilitar un detector GuardDuty para que entre en funcionamiento. Primero debe activarlo GuardDuty antes de aceptar una invitación.

   También puede hacerlo mediante las herramientas de línea de AWS comandos mediante el siguiente comando CLI.

   ```
   aws guardduty create-detector --enable
   ```

2. Ejecute la operación de AcceptAdministratorInvitationAPI para cada AWS cuenta en la que desee aceptar la invitación de membresía, utilizando las credenciales de esa cuenta.

   Debe especificar el ID de detección de esta AWS cuenta para la cuenta del miembro, el ID de cuenta de la cuenta de administrador que envió la invitación y el ID de invitación de la invitación que está aceptando. Puede consultar el ID de cuenta de la cuenta de administrador en el correo electrónico de invitación o con la operación ListInvitations de la API.

   También puede aceptar una invitación mediante las herramientas de línea de AWS comandos ejecutando el siguiente comando CLI. No olvide utilizar un ID de detector, un ID de cuenta de administrador y un ID de invitación que sean válidos.

   Para encontrar la correspondiente `detectorId` a su cuenta y región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

   ```
   aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --administrator-id 444455556666 --invitation-
   id 84b097800250d17d1872b34c4daadcf5
   ```

Consolidar las cuentas de GuardDuty administrador en una sola cuenta de administrador delegado GuardDuty de la organización

GuardDuty recomienda utilizar la asociación AWS Organizations para gestionar las cuentas de los miembros en una cuenta de administrador delegado. GuardDuty Puede utilizar el proceso de ejemplo que se describe a continuación para consolidar la cuenta de administrador y el miembro asociado

por invitación en una organización en una única cuenta de GuardDuty administrador GuardDuty delegado.

> **Note**
>
> Las cuentas que ya están siendo administradas por una cuenta de GuardDuty administrador delegado o las cuentas de miembros activos que están asociadas a una cuenta de GuardDuty administrador delegado no se pueden agregar a una cuenta de administrador delegado GuardDuty diferente. Cada organización solo puede tener una cuenta de GuardDuty administrador delegado por región y cada cuenta de miembro solo puede tener una cuenta de administrador delegado. GuardDuty

Elija uno de los métodos de acceso para consolidar las cuentas de GuardDuty administrador en una única cuenta de administrador delegado. GuardDuty

Console

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Para iniciar sesión, utilice las credenciales de la cuenta de administración de la organización.
2. Todas las cuentas que desee gestionar GuardDuty deben formar parte de su organización. Para obtener información sobre cómo agregar una cuenta a su organización, consulte Invitar a un usuario Cuenta de AWS a unirse a su organización.
3. Asegúrese de que todas las cuentas de los miembros estén asociadas a la cuenta que desee designar como cuenta única de GuardDuty administrador delegado. Desasocie cualquier cuenta de miembro que aún esté asociada a las cuentas de administrador preexistentes.

   Los siguientes pasos le ayudarán a desasociar las cuentas de miembro de la cuenta de administrador preexistente:

   a. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
   b. Para iniciar sesión, utilice las credenciales de la cuenta de administrador preexistente.
   c. En el panel de navegación, elija Accounts (Cuentas).
   d. En la página Cuentas, seleccione una o más cuentas que quiera desasociar de la cuenta de administrador.
   e. Seleccione Acciones y, a continuación, seleccione Desasociar cuenta.

f. Seleccione Confirmar para finalizar el paso.

4. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Para iniciar sesión, utilice las credenciales de la cuenta de administración.

5. En el panel de navegación, seleccione Configuración. En la página de configuración, designe la cuenta de GuardDuty administrador delegado de la organización.
6. Inicie sesión en la cuenta de GuardDuty administrador delegado designada.
7. Agregue miembros de la organización. Para obtener más información, consulte Administrar GuardDuty cuentas con AWS Organizations.

API/CLI

1. Todas las cuentas que desee gestionar GuardDuty deben formar parte de su organización. Para obtener información sobre cómo agregar una cuenta a su organización, consulte Invitar a un usuario Cuenta de AWS a unirse a su organización.
2. Asegúrese de que todas las cuentas de los miembros estén asociadas a la cuenta que desee designar como cuenta única de GuardDuty administrador delegado.

   a. Ejecute DisassociateMemberspara desasociar cualquier cuenta de miembro que aún esté asociada a las cuentas de administrador preexistentes.

   b. Como alternativa, puedes ejecutar el siguiente comando y reemplazar *777777777777* por el ID de detección de la cuenta de administrador preexistente de la que deseas desasociar la cuenta de miembro. AWS Command Line Interface Sustituya *666666666666* por el ID de Cuenta de AWS de la cuenta de miembro que desee desasociar.

   ```
   aws guardduty disassociate-members --detector-id 777777777777 --account-
   ids 666666666666
   ```

3. Ejecute EnableOrganizationAdminAccountpara delegar an Cuenta de AWS como cuenta de administrador delegado. GuardDuty

   Como alternativa, puede ejecutar el siguiente comando AWS Command Line Interface para delegar una cuenta de GuardDuty administrador delegado:

   ```
   aws guardduty enable-organization-admin-account --admin-account-id 777777777777
   ```

4. Agregue miembros de la organización. Para obtener más información, consulte Create or add member member accounts using API.

> **Important**
>
> Para maximizar la eficacia de un servicio regional GuardDuty, le recomendamos que designe su cuenta de GuardDuty administrador delegado y añada todas las cuentas de los miembros de cada región.

Habilite GuardDuty varias cuentas simultáneamente

Utilice el siguiente método para GuardDuty activarla en varias cuentas al mismo tiempo.

Utilice scripts de Python para habilitar GuardDuty varias cuentas simultáneamente

Puede automatizar la activación o desactivación de GuardDuty varias cuentas mediante los scripts del repositorio de ejemplos de scripts GuardDuty multicuenta de Amazon. Utilice el proceso de esta sección GuardDuty para habilitar una lista de cuentas de miembros que utilizan Amazon EC2. Para obtener información sobre el uso del script de desactivación o la configuración del script de forma local, consulte las instrucciones del enlace compartido.

El `enableguardduty.py` script habilita GuardDuty, envía invitaciones desde la cuenta de administrador y acepta invitaciones en todas las cuentas de los miembros. El resultado es una GuardDuty cuenta de administrador que contiene todos los datos de seguridad de todas las cuentas de los miembros. Como GuardDuty está aislada por región, los resultados de cada cuenta de miembro se acumulan en la región correspondiente de la cuenta de administrador. Por ejemplo, la región us-east-1 de su cuenta de GuardDuty administrador contiene los resultados de seguridad de todos los hallazgos de us-east-1 de todas las cuentas de miembros asociadas.

Estos scripts dependen de un rol de IAM compartido que tiene la política administrada: AWS política gestionada: AmazonGuardDutyFullAccess. Esta política proporciona a las entidades acceso a la cuenta de administrador GuardDuty y a cada una de las cuentas que desee activar, y debe estar presente en ella GuardDuty.

El siguiente proceso se activa GuardDuty en todas las regiones disponibles de forma predeterminada. Solo puede habilitarlo GuardDuty en regiones específicas utilizando el `--enabled_regions` argumento opcional y proporcionando una lista de regiones separadas por

comas. Si lo desea, también puede personalizar el mensaje de invitación que se envía a las cuentas miembro abriendo `enableguardduty.py` y editando la cadena `gd_invite_message`.

1. Cree un rol de IAM en la cuenta de GuardDuty administrador y adjunte la AWS política gestionada: AmazonGuardDutyFullAccess política que desee habilitar. GuardDuty
2. Cree un rol de IAM en cada cuenta de miembro que desee que administre su cuenta de GuardDuty administrador. Este rol debe tener el mismo nombre que el rol creado en el paso 1, debe permitir que la cuenta de administrador sea una entidad de confianza y debe tener la misma política de AmazonGuardDutyFullAccess administración descrita anteriormente.
3. Lance una nueva instancia de Amazon Linux con un rol asociado que tenga la siguiente relación de confianza para permitir que la instancia adopte un rol de servicio.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Inicie sesión en la nueva instancia y ejecute los siguientes comandos para configurarla.

```
sudo yum install git python
sudo yum install python-pip
pip install boto3
aws configure
git clone https://github.com/aws-samples/amazon-guardduty-multiaccount-scripts.git
cd amazon-guardduty-multiaccount-scripts
sudo chmod +x disableguardduty.py enableguardduty.py
```

5. Cree un archivo CSV que contenga una lista con los ID y los correos electrónicos de las cuentas miembro en las que agregó un rol en el paso 2. En cada línea debe aparecer una sola cuenta; el ID y la dirección de correo electrónico deben estar separados por una coma como en el siguiente ejemplo.

```
111122223333,guardduty-member@organization.com
```

> **Note**
>
> El archivo CSV debe estar en la misma ubicación que el script `enableguardduty.py`. Puede copiar un archivo CSV existente de Amazon S3 en el directorio actual con el siguiente método.
>
> ```
> aws s3 cp s3://my-bucket/my_key_name example.csv
> ```

6. Ejecute el script de Python. Asegúrese de proporcionar su ID de cuenta de GuardDuty administrador, el nombre del rol creado en los primeros pasos y el nombre del archivo CSV como argumentos.

```
python enableguardduty.py --master_account 444455556666 --assume_role
 roleName accountID.csv
```

Estimación de costos GuardDuty

Puede utilizar las operaciones de la GuardDuty consola o de la API para estimar los costes de uso promedio diarios. GuardDuty Durante el periodo de prueba gratuito de 30 días, la estimación de costos proyecta cuáles serán los costos estimados después del periodo de prueba. Si opera en un entorno de varias cuentas, su cuenta de GuardDuty administrador puede supervisar las métricas de costes de todas las cuentas de los miembros.

Puede ver la estimación de costos en función de las siguientes métricas:

- ID de cuenta: indica el costo estimado de su cuenta o de sus cuentas de miembro si opera como una cuenta de GuardDuty administrador.
- Fuente de datos: muestra el costo estimado de la fuente de datos especificada para los siguientes tipos de fuentes de GuardDuty datos: registros de flujo de VPC, registros de CloudTrail administración, eventos de CloudTrail datos o registros de DNS.
- Características: muestra el costo estimado en la fuente de datos especificada para las siguientes GuardDuty funciones: eventos de datos para S3, monitoreo de registros de auditoría de EKS, CloudTrail datos de volumen de EBS, actividad de inicio de sesión en RDS, monitoreo de tiempo de ejecución de EKS, monitoreo de tiempo de ejecución de Fargate, monitoreo de tiempo de ejecución de EC2 o monitoreo de actividad de red Lambda.
- Buckets de S3: indica el costo estimado de los eventos de datos de S3 en un bucket específico o en los buckets más caros de las cuentas de su entorno.

> **Note**
>
> Las estadísticas de los buckets de S3 solo están disponibles si la protección de S3 está habilitada para la cuenta. Para obtener más información, consulte Protección de Amazon S3 en Amazon GuardDuty.

Comprenda cómo se calculan los costos de uso GuardDuty

Las estimaciones que se muestran en la GuardDuty consola pueden diferir ligeramente de las de AWS Billing and Cost Management la consola. En la siguiente lista se explica cómo se GuardDuty calculan los costes de uso:

- La estimación GuardDuty de uso es solo para la región actual.

- Durante la prueba gratuita de 30 días, el GuardDuty uso estimado se basa en los últimos 7 a 30 días de uso.

> **Note**
>
> Si la duración del uso de una función GuardDuty o una de las funciones GuardDuty es inferior a 7 días, el importe de uso se muestra como 0,00 en la ***divisa***.

- La estimación del costo de uso de la versión de prueba incluye la estimación de las características y los orígenes de datos básicos que se encuentran actualmente en el periodo de prueba. Cada función y fuente de datos GuardDuty tiene su propio período de prueba, pero puede coincidir con el período de prueba GuardDuty o con otra función que se haya activado al mismo tiempo.
- La estimación GuardDuty de uso incluye descuentos en los precios por GuardDuty volumen por región, tal y como se detalla en la página de GuardDuty precios de Amazon, pero solo para las cuentas individuales que cumplan con los niveles de precios por volumen. Los descuentos en los precios por volumen no se incluyen en las estimaciones del uso total combinado entre las cuentas de una organización. Para obtener información sobre los precios con descuentos por volumen de uso combinado, consulte Facturación de AWS : descuentos por volumen.

Supervisión del tiempo de ejecución: cómo afectan los registros de flujo de VPC de las instancias EC2 al costo de uso

Si administra el agente de seguridad (de forma manual o a través de él GuardDuty) en EKS Runtime Monitoring o Runtime Monitoring for EC2, y si actualmente GuardDuty está desplegado en una instancia de Amazon EC2 y recibe Tipos de eventos de tiempo de ejecución recopilados el de esta instancia GuardDuty , no se le Cuenta de AWS cobrará por el análisis de los registros de flujo de VPC de esta instancia de Amazon EC2. Esto ayuda a GuardDuty evitar el doble de los gastos de uso de la cuenta.

¿Cómo GuardDuty calcula el costo de uso de CloudTrail los eventos

Cuando lo habilitas GuardDuty, comienza a consumir automáticamente los registros de AWS CloudTrail eventos registrados para tu cuenta en la seleccionada Región de AWS. GuardDuty replica los registros de eventos del servicio global y, a continuación, los procesa de forma independiente en cada región en la que lo haya GuardDuty activado. Esto ayuda a GuardDuty mantener los perfiles de usuario y rol en cada región para identificar anomalías.

Su CloudTrail configuración no afecta al coste de GuardDuty uso ni a la forma en que GuardDuty procesa los registros de eventos. El coste GuardDuty de uso se ve afectado por el uso de AWS las API en las que se inicia sesión CloudTrail. Para obtener más información, consulte AWS CloudTrail registros de eventos.

Revisar las estadísticas GuardDuty de uso

Elige el método de acceso que prefieras para revisar las estadísticas de uso de tu GuardDuty cuenta. Si eres GuardDuty administrador de una cuenta, los siguientes métodos te ayudarán a revisar las estadísticas de uso de todos los miembros.

Console

1. Abre la GuardDuty consola en https://console.aws.amazon.com/guardduty/.

   Asegúrese de utilizar la cuenta de GuardDuty administrador.
2. En el panel de navegación, elija Uso.
3. En la página de uso, una cuenta de GuardDuty administrador con cuentas de miembros puede ver el coste organizativo estimado de los últimos 30 días. Se trata de un coste de uso total estimado para su organización.
4. GuardDuty Las cuentas de administrador con miembros pueden ver el desglose de los costos de uso por fuente de datos o por cuentas. Las cuentas individuales o independientes pueden ver el desglose por fuente de datos.

   Si tiene cuentas de miembro, puede ver las estadísticas de una cuenta individual seleccionándola en la tabla de cuentas.

API/CLI

Ejecute la operación de la GetUsageStatisticsAPI con las credenciales de la cuenta de GuardDuty administrador. Proporcione la siguiente información para ejecutar el comando:

- (Obligatorio) proporciona el ID del GuardDuty detector regional de la cuenta de la que quieres recuperar las estadísticas.
- (Obligatorio) Proporcione uno de los tipos de estadísticas que desee recuperar: `SUM_BY_ACCOUNT | SUM_BY_DATA_SOURCE | SUM_BY_RESOURCE | SUM_BY_FEATURE | TOP_ACCOUNTS_BY_FEATURE`.

Actualmente, `TOP_ACCOUNTS_BY_FEATURE` no admite la recuperación de las estadísticas de uso. `RDS_LOGIN_EVENTS`

- (Obligatorio) proporciona una o más fuentes de datos o funciones para consultar tus estadísticas de uso.
- (Opcional) Proporcione una lista de los ID de cuentas de los que desea recuperar las estadísticas de uso.

También puede utilizar la AWS Command Line Interface. El siguiente comando es un ejemplo de cómo recuperar las estadísticas de uso de todas las fuentes de datos y funciones, calculadas por cuentas. Asegúrese de sustituir `detector-id` por su propio ID de detector válido. En el caso de las cuentas independientes, este comando devuelve el costo del uso de los últimos 30 días únicamente para su cuenta. Si es GuardDuty administrador de una cuenta con cuentas de miembros, verá los costos listados por cuenta para todos los miembros.

Para encontrar los `detectorId` de su cuenta y su región actual, consulte la página de configuración de la consola https://console.aws.amazon.com/guardduty/.

Sustitúyala `SUM_BY_ACCOUNT` por el tipo con el que quieras calcular las estadísticas de uso.

Para monitorear el costo únicamente de las fuentes de datos

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"DataSources":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_LOGS", "KUBERNETES_AUDIT_LOGS",
 "EC2_MALWARE_SCAN"]}'
```

Para monitorear el costo de las funciones

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"Features":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_DATA_EVENTS", "EKS_AUDIT_LOGS",
 "EBS_MALWARE_PROTECTION", "RDS_LOGIN_EVENTS", "LAMBDA_NETWORK_LOGS",
 "EKS_RUNTIME_MONITORING", "FARGATE_RUNTIME_MONITORING", "EC2_RUNTIME_MONITORING"]}'
```

Seguridad en Amazon GuardDuty

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

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Terceros clientes prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los Programas de conformidad de AWS. Para conocer los programas de conformidad que se aplican a CloudWatch, 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 los reglamentos vigentes.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza . Muestra cómo configurar para satisfacer sus objetivos de seguridad y conformidad. También puede aprender a utilizar otros servicios de AWS que lo ayuden a monitorear y proteger los recursos de IAM.

Contenido

Protección de datos en Amazon GuardDuty

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

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

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final 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. Esto incluye cuando trabaja GuardDuty o Servicios de AWS utiliza la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o

diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

Todos los datos de los GuardDuty clientes se cifran en reposo mediante soluciones AWS de cifrado.

GuardDuty los datos, como los hallazgos, se cifran en reposo mediante AWS Key Management Service (AWS KMS) utilizando AWS claves gestionadas por el cliente.

Cifrado en tránsito

GuardDuty analiza los datos de registro de otros servicios. Cifra todos los datos en tránsito de estos servicios con HTTPS y KMS. Una vez que GuardDuty extrae la información que necesita de los registros, estos se descartan. Para obtener más información sobre cómo se GuardDuty utiliza la información de otros servicios, consulte las fuentes de GuardDuty datos.

GuardDuty los datos se cifran en tránsito entre los servicios.

Optar por no utilizar sus datos para mejorar el servicio

Puede optar por no utilizar sus datos para desarrollar GuardDuty y mejorar otros servicios de AWS seguridad mediante la política de AWS Organizations exclusión. Puede optar por excluirse incluso si actualmente GuardDuty no recopila ningún dato de este tipo. Para más información sobre cómo excluirse, consulte Políticas de exclusión de servicios de IA en la Guía del usuario de AWS Organizations .

> **Note**
>
> Para poder utilizar la política de exclusión voluntaria, sus AWS cuentas deben estar gestionadas de forma centralizada por AWS Organizations. Si aún no ha creado una organización para sus AWS cuentas, consulte Creación y administración de una organización en la Guía del AWS Organizations usuario.

La exclusión tiene los siguientes efectos:

- GuardDuty eliminará los datos que recopiló y almacenó con fines de mejora del servicio antes de su exclusión voluntaria (si la hubiera).

- Una vez que opte por no participar, ya no GuardDuty recopilará ni almacenará estos datos con fines de mejora del servicio.

En los siguientes temas se explica cómo cada una de las funciones incluidas en GuardDuty ella puede gestionar sus datos con el fin de mejorar el servicio.

Contenido

GuardDuty Supervisión del tiempo de ejecución

GuardDuty Runtime Monitoring ofrece detección de amenazas en tiempo de ejecución para los clústeres de Amazon Elastic Kubernetes Service (Amazon EKS) AWS Fargate (Fargate) , solo para Amazon Elastic Container Service (Amazon ECS) y para las instancias de Amazon Elastic Compute Cloud (Amazon EC2) de su entorno. AWS Después de activar Runtime Monitoring e implementar el agente de GuardDuty seguridad para su recurso, GuardDuty comienza a monitorear y analizar los eventos de tiempo de ejecución asociados a su recurso. Estos tipos de eventos de tiempo de ejecución incluyen eventos de proceso, eventos de contenedor, eventos de DNS y más. Para obtener más información, consulte Tipos de eventos de tiempo de ejecución recopilados que utilizan GuardDuty .

Aunque GuardDuty ahora recopila argumentos de línea de comandos que puede dirigir a sus cargas de trabajo, actualmente no los usa para mejorar el servicio (puede que lo haga en el futuro). Hemos empezado a recopilar argumentos basados en la línea de comandos para anticiparnos a las nuevas reglas de detección de amenazas y a los resultados que se publicarán próximamente. Su confianza, la privacidad y la seguridad de su contenido son nuestra máxima prioridad y garantizamos que nuestro uso cumpla con nuestros compromisos con usted. Para obtener más información, consulte Preguntas frecuentes sobre privacidad de datos.

GuardDuty Protección contra el malware

GuardDuty Malware Protection analiza y detecta el malware contenido en los volúmenes de EBS adjuntos a sus cargas de trabajo de instancias y contenedores de Amazon EC2 potencialmente comprometidas. Cuando GuardDuty Malware Protection identifica un archivo de volumen de EBS como malicioso o dañino, GuardDuty Malware Protection recopila y almacena este archivo para desarrollar y mejorar las detecciones de malware y el servicio. GuardDuty Este archivo también

se puede utilizar para desarrollar y mejorar otros servicios de AWS seguridad. Su confianza, la privacidad y la seguridad de su contenido son nuestra máxima prioridad y garantizamos que nuestro uso cumpla con nuestros compromisos con usted. Para obtener más información, consulte Preguntas frecuentes sobre privacidad de datos.

Registrar llamadas a GuardDuty la API de Amazon con AWS CloudTrail

Amazon GuardDuty está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en GuardDuty. CloudTrail captura todas las llamadas a las API GuardDuty como eventos, incluidas las llamadas desde la GuardDuty consola y las llamadas en código a las GuardDuty API. Si crea un registro, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon Simple Storage Service (Amazon S3), incluidos los eventos de. GuardDuty Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por usted CloudTrail, puede determinar el destinatario de la solicitud GuardDuty, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información sobre CloudTrail cómo configurarla y habilitarla, consulte la Guía del AWS CloudTrail usuario.

GuardDuty información en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad de eventos admitida GuardDuty, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de los eventos de tu AWS cuenta, incluidos los eventos de tu cuenta GuardDuty, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones. 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. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte:

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

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 hizo con las credenciales de inicio de sesión del usuario raíz o del usuario de IAM
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte Elemento userIdentity de CloudTrail .

GuardDuty controle los eventos del plano en CloudTrail

De forma predeterminada, CloudTrail registra todas las operaciones de la GuardDuty API proporcionadas en la referencia de la GuardDuty API de Amazon como eventos en CloudTrail archivos.

GuardDuty eventos de datos en CloudTrail

GuardDuty Supervisión del tiempo de ejecuciónutiliza un agente de GuardDuty seguridad desplegado en sus clústeres de Amazon Elastic Kubernetes Service (Amazon EKS), AWS Fargate instancias de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) y tareas `aws-guardduty-agent` (solo Amazon Elastic Container Service (Amazon ECS)) para recopilar complementos Tipos de eventos de tiempo de ejecución recopilados () AWS que recopilan sus cargas de trabajo y luego las envían para detectar y analizar amenazas. GuardDuty

Registro y supervisión de eventos de datos

Si lo desea, puede configurar los AWS CloudTrail registros para ver los eventos de datos de su agente de seguridad. GuardDuty

Para crearlos y configurarlos CloudTrail, consulte los eventos de datos en la Guía del AWS CloudTrail usuario y siga las instrucciones para registrar los eventos de datos con los selectores

de eventos avanzados del AWS Management Console. Al registrar el registro de seguimiento, asegúrese de hacer los siguientes cambios:

- Para el tipo de evento de datos, elija GuardDuty detector.
- En Plantilla de selector de registros, elija Registrar todos los eventos.
- Amplíe la Vista JSON para la configuración. Debería ser similar al siguiente JSON:

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

Tras activar el selector de la ruta, diríjase a la consola de Amazon S3 en https://console.aws.amazon.com/s3/. Puede descargar los eventos de datos del bucket de S3 que eligió al momento de configurar los CloudTrail registros.

Ejemplo: entradas de archivos de GuardDuty registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que muestra el evento del plano de datos.


```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
            "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-
instance/i-123412341234example",
            "accountId": "111122223333",
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "111122223333:aws:ec2-instance",
                    "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
                    "accountId": "111122223333",
                    "userName": "aws:ec2-instance"
                },
                "attributes": {
                    "creationDate": "2023-03-05T04:00:21Z",
                    "mfaAuthenticated": "false"
                },
                "ec2RoleDelivery": "2.0"
            }
        },
        "eventTime": "2023-03-05T06:03:49Z",
        "eventSource": "guardduty.amazonaws.com",
        "eventName": "SendSecurityTelemetry",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "54.240.230.177",
        "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
        "requestParameters": null,
        "responseElements": null,
        "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
        "readOnly": false,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::GuardDuty::Detector",
            "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
```

```
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data",
        "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
        }
    }
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `CreateIPThreatIntelSet` acción (evento del plano de control).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-06-14T22:54:20Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2018-06-14T22:57:56Z",
    "eventSource": "guardduty.amazonaws.com",
    "eventName": "CreateThreatIntelSet",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.240.230.177",
    "userAgent": "console.amazonaws.com",
```

```
    "requestParameters": {
        "detectorId": "12abc34d567e8fa901bc2d34e56789f0",
        "name": "Example",
        "format": "TXT",
        "activate": false,
        "location": "https://s3.amazonaws.com/bucket.name/file.txt"
    },
    "responseElements": {
        "threatIntelSetId": "1ab200428351c99d859bf61992460d24"
    },
    "requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",
    "eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```


A partir de la información de este evento, puede determinar que la solicitud se realizó para crear una lista de amenazas `Example` en GuardDuty. También puede ver que la solicitud la hizo una usuaria llamada Alice el 14 de junio de 2018.

Identity and Access Management para Amazon GuardDuty

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 autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. GuardDuty IAM es un Servicio de AWS que se puede utilizar sin cargo adicional.

Temas

- AWS políticas gestionadas para Amazon GuardDuty

Público

La forma en que utilice AWS Identity and Access Management (IAM) difiere en función del trabajo que realice en GuardDuty.

Usuario del servicio: si utiliza el GuardDuty servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más GuardDuty funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ser útil para solicitar los permisos correctos a su administrador. Si no puede acceder a una característica en GuardDuty, consulte Solución de problemas de GuardDuty identidad y acceso a Amazon.

Administrador de servicios: si estás a cargo de GuardDuty los recursos de tu empresa, probablemente tengas acceso total a ellos GuardDuty. Su trabajo consiste en determinar a qué GuardDuty funciones y recursos 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 la IAM GuardDuty, consulteCómo GuardDuty funciona Amazon con IAM.

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

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. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como 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 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 use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para más información, consulte Autenticación multifactor en la Guía del Usuario de AWS IAM Identity Center 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 recursos y Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el 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 de usuario de IAM.

Identidad federada

Como práctica recomendada, solicite que los usuarios humanos, incluidos los que requieren acceso de administrador, utilicen la federación con un proveedor de identidades para acceder a Servicios de AWS utilizando credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidad web, el AWS Directory Service, el directorio del Identity Center, o cualquier usuario que acceda a Servicios de AWS utilizando credenciales proporcionadas a través de una fuente de

identidad. Cuando identidades federadas acceden a Cuentas de AWS, asumen roles y los roles proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el IAM Identity Center o puede conectarse y sincronizar con un conjunto de usuarios, así como grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones y Cuentas de AWS. Para más información, consulte ¿Qué es IAM Identity Center? en la Guía del Usuario de AWS IAM Identity Center.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad de la Cuenta de 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 la 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 Console cambiando de roles. Puede asumir un rol llamando a una operación de la AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, 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 permisos para este. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos que están definidos en este. 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 Centro de identidades de IAM, debe configurar un conjunto de permisos. El Centro de identidades de IAM correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder sus 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 adjuntar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, 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.
  - Sesiones de acceso directo (FAS): cuando utiliza un usuario o rol de IAM para realizar acciones en AWS, se considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS usa los permisos de la entidad principal que llama un Servicio de AWS, junto con la solicitud de Servicio de AWS, para realizar solicitudes a los servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros recursos o Servicios de AWS para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre las políticas al momento de realizar solicitudes de FAS, consulte Reenviar las 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 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 servicio: un rol vinculado a servicio 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 la 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 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 EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia adjuntado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias 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 asocian 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 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 bajo qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede agregar las políticas de IAM a los 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 AWS Management Console, la 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 de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y bajo 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 adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas por AWS y las políticas administradas por el cliente. Para 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 adjuntan a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se adjunta 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 en función de 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 otorgan.

- 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 identidad. 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 especifique 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 empresa o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias Cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada Usuario raíz de la cuenta de AWS. Para más información sobre Organizations 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 acerca de cómo AWS decide si permitir o no una

solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del Usuario de IAM.

Cómo GuardDuty funciona Amazon con IAM

Antes de utilizar IAM para gestionar el acceso GuardDuty, infórmate sobre las funciones de IAM disponibles. GuardDuty

Funciones de IAM que puedes usar con Amazon GuardDuty

Características de IAM	GuardDuty soporte
Políticas basadas en identidad	Sí
Políticas basadas en recursos	No
Acciones de política	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	Sí
Roles vinculados a servicios	Sí

Para obtener una visión general de cómo GuardDuty funcionan otros AWS servicios con la mayoría de las funciones de IAM, consulte AWSlos servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para GuardDuty

Compatibilidad con las políticas basadas en identidad	Sí

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

Con las políticas basadas en identidad de IAM, puede especificar las acciones y recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política en función de identidad porque se aplica al usuario o rol al que está asociado. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del Usuario de IAM.

Ejemplos de políticas basadas en la identidad para GuardDuty

Para ver ejemplos de políticas GuardDuty basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para Amazon GuardDuty

Políticas basadas en recursos incluidas GuardDuty

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se adjuntan a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se adjunta 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.

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando la entidad principal y el recurso se encuentran en Cuentas de AWS diferentes, un administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, asocie la entidad a una política en función de identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política en función de identidad adicional. Para más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del Usuario de IAM.

Acciones políticas para GuardDuty

Admite acciones de política	Sí

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 bajo 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.

Para ver una lista de GuardDuty acciones, consulta Acciones definidas por Amazon GuardDuty en la Referencia de autorización de servicio.

Las acciones políticas GuardDuty utilizan el siguiente prefijo antes de la acción:

```
guardduty
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "guardduty:action1",
```

```
      "guardduty:action2"
        ]
```

Para ver ejemplos de políticas GuardDuty basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para Amazon GuardDuty

Recursos de políticas para GuardDuty

Admite recursos de políticas	Sí

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 bajo 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 ver una lista de los tipos de GuardDuty recursos y sus ARN, consulte Recursos definidos por Amazon GuardDuty en la Referencia de autorización de servicio. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por Amazon. GuardDuty

Para ver ejemplos de políticas GuardDuty basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para Amazon GuardDuty

Claves de condición de la política para GuardDuty

Admite claves de condición de política específicas del servicio	Sí

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 bajo 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 `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación lógica `OR`. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También 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.

Para ver una lista de claves de GuardDuty estado, consulta Claves de estado de Amazon GuardDuty en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por Amazon GuardDuty.

Para ver ejemplos de políticas GuardDuty basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para Amazon GuardDuty

Listas de control de acceso (ACL) en GuardDuty

Admite las ACL	No

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

Control de acceso basado en atributos (ABAC) con GuardDuty

Admite ABAC (etiquetas en las políticas)	Parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a muchos recursos de AWS. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del Usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del Usuario de IAM.

Uso de credenciales temporales con GuardDuty

Compatible con el uso de credenciales temporales	Sí

Algunos Servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre qué Servicios de AWS funcionan con credenciales temporales, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en la AWS Management Console con cualquier método, excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accede a AWS utilizando el enlace de inicio de sesión único (SSO) de la empresa, ese proceso crea automáticamente credenciales temporales. También crea automáticamente credenciales temporales cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobrel cambio de roles, consulte Cambio a un rol (consola) en la Guía del Usuario de IAM.

Puede crear credenciales temporales de forma manual mediante la AWS CLI o la API de AWS. A continuación, puede usar esas credenciales temporales para acceder a AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de usar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para GuardDuty

Admite Forward access sessions (FAS)	Sí

Cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS usa los permisos de la entidad principal que llama un Servicio de AWS, junto con la solicitud de Servicio de AWS, para realizar solicitudes a los servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros recursos o Servicios de AWS para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre las políticas al momento de realizar solicitudes de FAS, consulte Reenviar las sesiones de acceso.

Roles de servicio para GuardDuty

Compatible con roles de servicio	Sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del Usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la GuardDuty funcionalidad. Edite las funciones de servicio solo cuando se GuardDuty proporcionen instrucciones para hacerlo.

Funciones vinculadas al servicio para GuardDuty

Compatible con roles vinculados a servicios	Sí

Un rol vinculado a un servicio 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 la 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.

Para obtener más información sobre la creación o la administración de funciones GuardDuty vinculadas a servicios, consulte. Uso de roles vinculados a servicios para Amazon GuardDuty

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a servicios. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios en cuestión.

Ejemplos de políticas basadas en identidad para Amazon GuardDuty

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de GuardDuty. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API de AWS. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede agregar las políticas de IAM a los roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del Usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por GuardDuty, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon GuardDuty en la Referencia de autorización de servicio.

Temas

Prácticas recomendadas relativas a políticas

Las políticas basadas en la identidad determinan si alguien puede crear GuardDuty recursos de su cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidad:

- Comience con las políticas administradas por 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 por AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en la Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS 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 de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se 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.
- Use 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 más información, consulte Elementos de la política JSON de IAM: condición en la Guía del usuario de IAM.

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

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

Mediante la consola de GuardDuty

Para acceder a la GuardDuty consola de Amazon, debes tener un conjunto mínimo de permisos. Estos permisos deben permitirte enumerar y ver detalles sobre los GuardDuty recursos de tu cuentaCuenta de AWS. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la GuardDuty consola, adjunte también la política `ReadOnly` AWS gestionada GuardDuty `ConsoleAccess` o la política gestionada a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM.

Permisos requeridos para habilitar GuardDuty

Para conceder los permisos que deben tener varias identidades de IAM (usuarios, grupos y roles), adjunte la AWS política gestionada: AmazonGuardDutyFullAccess política requerida para GuardDuty habilitarlos.

Permitir a los usuarios consultar sus propios permisos

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

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

```
        }
    ]
}
```

Política de IAM personalizada para conceder acceso de solo lectura a GuardDuty

Para conceder acceso de solo lectura, GuardDuty puede utilizar la política gestionada. `AmazonGuardDutyReadOnlyAccess`

Para crear una política personalizada que conceda a un rol, usuario o grupo de IAM acceso de solo lectura GuardDuty, puedes usar la siguiente declaración:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ListMembers",
                "guardduty:GetMembers",
                "guardduty:ListInvitations",
                "guardduty:ListDetectors",
                "guardduty:GetDetector",
                "guardduty:ListFindings",
                "guardduty:GetFindings",
                "guardduty:ListIPSets",
                "guardduty:GetIPSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:GetThreatIntelSet",
                "guardduty:GetMasterAccount",
                "guardduty:GetInvitationsCount",
                "guardduty:GetFindingsStatistics",
                "guardduty:DescribeMalwareScans",
                "guardduty:UpdateMalwareScanSettings",
                "guardduty:GetMalwareScanSettings"
            ],
            "Resource": "*"
        }
    ]
}
```

Denegar el acceso a los resultados GuardDuty

Puede usar la siguiente política para denegar el acceso a los GuardDuty hallazgos a un rol, usuario o grupo de IAM. Los usuarios no pueden ver los resultados ni sus detalles, pero pueden acceder a todas las demás GuardDuty operaciones:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateDetector",
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "guardduty:CreateIPSet",
                "guardduty:DeleteIPSet",
                "guardduty:UpdateIPSet",
                "guardduty:GetIPSet",
                "guardduty:ListIPSets",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:UpdateThreatIntelSet",
                "guardduty:GetThreatIntelSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:ArchiveFindings",
                "guardduty:UnarchiveFindings",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateMembers",
                "guardduty:InviteMembers",
                "guardduty:GetMembers",
                "guardduty:DeleteMembers",
                "guardduty:DisassociateMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:ListMembers",
                "guardduty:GetMasterAccount",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:AcceptAdministratorInvitation",
                "guardduty:ListInvitations",
                "guardduty:GetInvitationsCount",
```

```
                "guardduty:DeclineInvitations",
                "guardduty:DeleteInvitations"
            ],
            "Resource": "*"
        },
         {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

Utilizar una política de IAM personalizada para limitar el acceso a los recursos GuardDuty

Para definir el acceso de un usuario en GuardDuty función del ID del detector, puedes utilizar todas las acciones de la GuardDuty API en tus políticas de IAM personalizadas, excepto las siguientes operaciones:

- `guardduty:CreateDetector`
- `guardduty:DeclineInvitations`
- `guardduty:DeleteInvitations`
- `guardduty:GetInvitationsCount`

- `guardduty:ListDetectors`
- `guardduty:ListInvitations`

Utilice las siguientes operaciones en una política de IAM para definir el acceso de un usuario en GuardDuty función del ID y el ID del IPset: ThreatIntelSet

- `guardduty:DeleteIPSet`
- `guardduty:DeleteThreatIntelSet`
- `guardduty:GetIPSet`
- `guardduty:GetThreatIntelSet`
- `guardduty:UpdateIPSet`
- `guardduty:UpdateThreatIntelSet`

En los siguientes ejemplos se muestra cómo crear políticas con algunas de las operaciones anteriores:

- Esta política permite a un usuario ejecutar la operación `guardduty:UpdateDetector`, con el ID de detector 1234567 en la región us-east-1:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateDetector",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
        }
    ]
}
```

- Esta política permite a un usuario ejecutar la operación `guardduty:UpdateIPSet`, con el ID de detector 1234567 y el ID de IPSet 000000 en la región us-east-1:

> **Note**
>
> Asegúrese de que el usuario tenga los permisos necesarios para acceder a las listas de direcciones IP confiables y a las listas de amenazas. GuardDuty Para obtener más información, consulte Permisos necesarios para cargar listas de IP de confianza y listas de amenazas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/000000"
        }
    ]
}
```

- Esta política permite a un usuario ejecutar la operación `guardduty:UpdateIPSet`, con cualquier ID de detector y el ID de IPSet 000000 en la región us-east-1:

> **Note**
>
> Asegúrese de que el usuario tenga los permisos necesarios para acceder a las listas de direcciones IP confiables y a las listas de amenazas GuardDuty. Para obtener más información, consulte Permisos necesarios para cargar listas de IP de confianza y listas de amenazas.

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

```
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
        }
    ]
}
```

- Esta política permite a un usuario ejecutar la operación `guardduty:UpdateIPSet`, con su ID de detector y cualquier ID de IPSet en la región us-east-1:

> **Note**
>
> Asegúrese de que el usuario tenga los permisos necesarios para acceder a las listas de direcciones IP confiables y a las listas de amenazas GuardDuty. Para obtener más información, consulte Permisos necesarios para cargar listas de IP de confianza y listas de amenazas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/*"
        }
    ]
}
```

Uso de roles vinculados a servicios para Amazon GuardDuty

Amazon GuardDuty usa roles AWS Identity and Access Management vinculados a servicios (IAM). Un rol vinculado a un servicio (SLR) es un tipo único de rol de IAM al que se vincula directamente. GuardDuty Los roles vinculados al servicio están predefinidos GuardDuty e incluyen todos los permisos necesarios para llamar a otros servicios GuardDuty en su nombre. AWS

Con el rol vinculado al servicio, puedes configurarlo manualmente GuardDuty sin tener que añadir los permisos necesarios. GuardDuty define los permisos de su función vinculada al servicio y, a menos que los permisos se definan de otra manera, solo GuardDuty puede asumir la función. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se puede adjuntar a ninguna otra entidad de IAM.

GuardDuty admite el uso de funciones vinculadas al servicio en todas las regiones en las que esté disponible. GuardDuty Para obtener más información, consulte Regiones y puntos de conexión.

Puede eliminar el rol GuardDuty vinculado al servicio solo después de haberlo desactivado por primera vez GuardDuty en todas las regiones en las que esté habilitado. Esto protege sus GuardDuty recursos porque no puede eliminar el permiso de acceso a ellos sin darse cuenta.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM y busque los servicios que tienen Sí en la columna Rol vinculado a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de rol vinculados al servicio para GuardDuty

GuardDuty usa el rol vinculado al servicio (SLR) denominado. `AWSServiceRoleForAmazonGuardDuty` La SLR permite realizar GuardDuty las siguientes tareas. También permite GuardDuty incluir los metadatos recuperados pertenecientes a la instancia EC2 en los hallazgos que se GuardDuty puedan generar sobre la potencial amenaza. El rol vinculado a servicios `AWSServiceRoleForAmazonGuardDuty` confía en el servicio `guardduty.amazonaws.com` para asumir el rol.

Las políticas de permisos ayudan a GuardDuty realizar las siguientes tareas:

- Utilice las acciones de Amazon EC2 para administrar y recuperar información sobre sus instancias, de EC2, imágenes y componentes de red, como VPC, subredes, puertas de enlace de tránsito y grupos de seguridad.
- Utilice AWS Systems Manager acciones para gestionar las asociaciones de SSM en las instancias de Amazon EC2 al GuardDuty habilitar Runtime Monitoring con un agente automatizado para Amazon EC2. Cuando la configuración GuardDuty automática de agentes está deshabilitada, solo GuardDuty tiene en cuenta las instancias de EC2 que tienen una etiqueta de inclusión (:). `GuardDutyManaged true`
- Use AWS Organizations acciones para describir las cuentas asociadas y el identificador de la organización.

- Utilizar las acciones de Amazon S3 para recuperar información sobre buckets y objetos de S3.
- Utilice AWS Lambda acciones para recuperar información sobre las funciones y etiquetas de Lambda.
- Utilice las acciones de Amazon EKS para administrar y recuperar información sobre los clústeres de EKS y administrar los complementos de Amazon EKS en los clústeres de EKS. Las acciones de EKS también recuperan la información sobre las etiquetas asociadas a GuardDuty ellas.
- Utilice IAM para crear los Permisos de roles vinculados a servicios para Protección contra malware después de habilitar Protección contra malware.
- Utilice las acciones de Amazon ECS para gestionar y recuperar información sobre los clústeres de Amazon ECS y gestione la configuración de la cuenta de Amazon ECS con`guarddutyActivate`. Las acciones relacionadas con Amazon ECS también recuperan la información sobre las etiquetas asociadas a ellas GuardDuty.

El rol se configura con la siguiente política administrada por AWS, que se denomina `AmazonGuardDutyServiceRolePolicy`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GuardDutyGetDescribeListPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeTransitGatewayAttachments",
                "organizations:ListAccounts",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketTagging",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAllMyBuckets",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
```

```
                "s3:GetBucketPolicyStatus",
                "lambda:GetFunctionConfiguration",
                "lambda:ListTags",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeSecurityGroups",
                "ecs:ListClusters",
                "ecs:DescribeClusters"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GuardDutyCreateSLRPolicy",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                },
                "StringLike": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.*.guardduty-data",
                        "com.amazonaws.*.guardduty-data-fips"
                    ]
                }
            }
        },
        {
            "Sid": "GuardDutyModifyDeleteVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:ModifyVpcEndpoint",
                "ec2:DeleteVpcEndpoints"
            ],
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpoint",
                "ec2:ModifyVpcEndpoint"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*",
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:subnet/*"
            ]
        },
        {
             "Sid": "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
             "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateVpcEndpoint"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutySecurityGroupManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
```

```
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/GuardDutyManaged": "*"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupForVpcPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        },
        {
            "Sid": "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSecurityGroup"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateEksAddonPolicy",
            "Effect": "Allow",
```

```
            "Action": "eks:CreateAddon",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEksAddonManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "eks:DeleteAddon",
                "eks:UpdateAddon",
                "eks:DescribeAddon"
            ],
            "Resource": "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
        },
        {
            "Sid": "GuardDutyEksClusterTagResourcePolicy",
            "Effect": "Allow",
            "Action": "eks:TagResource",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEcsPutAccountSettingsDefaultPolicy",
            "Effect": "Allow",
            "Action": "ecs:PutAccountSettingDefault",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:account-setting": [
                        "guardDutyActivate"
                    ]
                 }
            }
        },
        {
            "Sid": "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
```

```
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:DeleteAssociation",
                "ssm:UpdateAssociation",
                "ssm:CreateAssociation",
                "ssm:StartAssociationsOnce"
            ],
            "Resource": "arn:aws:ssm:*:*:association/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmAddTagsToResourcePermission",
            "Effect": "Allow",
            "Action": [
                "ssm:AddTagsToResource"
            ],
            "Resource": "arn:aws:ssm:*:*:association/*",
            "Condition":{
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                },
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmCreateUpdateAssociationInstanceDocumentPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateAssociation",
                "ssm:UpdateAssociation"
            ],
            "Resource": "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
        },
        {
```

```
            "Sid": "SsmSendCommandPermission",
            "Effect": "Allow",
            "Action": "ssm:SendCommand",
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
            ]
        },
        {
            "Sid": "SsmGetCommandStatus",
            "Effect": "Allow",
            "Action": "ssm:GetCommandInvocation",
            "Resource": "*"
        }
   ]
}
```

A continuación se presenta la política de confianza que se asocia al rol vinculado a servicio `AWSServiceRoleForAmazonGuardDuty`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Crear un rol vinculado a un servicio para GuardDuty

El rol `AWSServiceRoleForAmazonGuardDuty` vinculado al servicio se crea automáticamente cuando lo habilitas GuardDuty por primera vez o lo habilitas GuardDuty en una región compatible en la que antes no lo tenías habilitado. También puede crear el rol vinculado al servicio manualmente mediante la consola de IAM, la API de IAM o la misma AWS CLI.

> **Important**
>
> El rol vinculado al servicio que se crea para la cuenta de administrador GuardDuty delegado no se aplica a las cuentas de los miembros. GuardDuty

Debe configurar permisos para permitir a una entidad principal de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para que el rol `AWSServiceRoleForAmazonGuardDuty` vinculado al servicio se cree correctamente, el director de IAM GuardDuty con el que utilices debe tener los permisos necesarios. Para conceder los permisos necesarios, asocie la siguiente política a un usuario, un grupo o un rol de :

> **Note**
>
> Sustituya el ejemplo de *`ID de cuenta`* del siguiente ejemplo por el ID de cuenta real AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

Para obtener más información acerca de cómo crear un rol manualmente, consulte Crear un rol vinculado a un servicio en la Guía del usuario de IAM.

Edición de un rol vinculado a un servicio para GuardDuty

GuardDuty no permite editar el rol vinculado al `AWSServiceRoleForAmazonGuardDuty` servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol utilizando 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 GuardDuty

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no conservará una entidad no utilizada que no se monitoree ni se mantenga de forma activa.

> **Important**
>
> Si ha habilitado Protección contra malware, la eliminación de `AWSServiceRoleForAmazonGuardDuty` no elimina `AWSServiceRoleForAmazonGuardDutyMalwareProtection` automáticamente. Si desea eliminar `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, consulte Eliminación de un rol vinculado a servicios para Protección contra malware.

Primero debe deshabilitarlo GuardDuty en todas las regiones en las que esté habilitado para eliminar el. `AWSServiceRoleForAmazonGuardDuty` Si el GuardDuty servicio no está deshabilitado al intentar eliminar el rol vinculado al servicio, se producirá un error en la eliminación. Para obtener más información, consulte Suspender o deshabilitar GuardDuty.

Cuando lo inhabilitas GuardDuty, `AWSServiceRoleForAmazonGuardDuty` no se elimina automáticamente. Si lo GuardDuty vuelves a activar, empezará a usar lo existente`AWSServiceRoleForAmazonGuardDuty`.

Cómo eliminar manualmente el rol vinculado a servicios mediante IAM

Usa la consola de IAM AWS CLI, la o la API de IAM para eliminar la función vinculada al `AWSServiceRoleForAmazonGuardDuty` servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Compatible Regiones de AWS

Amazon GuardDuty admite el uso de la función `AWSServiceRoleForAmazonGuardDuty` vinculada al servicio en todos los Regiones de AWS lugares disponibles GuardDuty . Para ver una lista de las regiones en las GuardDuty que está disponible actualmente, consulta los GuardDuty puntos de conexión y las cuotas de Amazon en. Referencia general de Amazon Web Services

Permisos de roles vinculados a servicios para Protección contra malware

Protección contra malware usa el rol vinculado a servicios (SLR) denominado `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Esta cámara réflex permite a Malware Protection realizar escaneos sin agentes para detectar malware en su cuenta. GuardDuty Permite GuardDuty crear una instantánea del volumen de EBS en su cuenta y compartirla con la cuenta de servicio. GuardDuty Tras GuardDuty evaluar la instantánea, incluye los metadatos de la carga de trabajo del contenedor y de la instancia de EC2 recuperados en las conclusiones sobre protección contra malware. El rol vinculado a servicios `AWSServiceRoleForAmazonGuardDutyMalwareProtection` confía en el servicio `malware-protection.guardduty.amazonaws.com` para asumir el rol.

Las políticas de permisos para este rol ayudan a Malware Protection a realizar las siguientes tareas:

- Utilice las acciones de Amazon Elastic Compute Cloud (Amazon EC2) para recuperar información sobre sus instancias, volúmenes e instantáneas de Amazon EC2. Protección contra malware también proporciona permiso para acceder a los metadatos de los clústeres de Amazon EKS y Amazon ECS.
- Crear instantáneas para los volúmenes de EBS cuya etiqueta `GuardDutyExcluded` no esté configurada como `true`. De forma predeterminada, las instantáneas se crean con una etiqueta `GuardDutyScanId`. No elimine esta etiqueta; si lo hace, Protección contra malware no tendrá acceso a las instantáneas.

> **Important**
>
> Si lo configura`true`, el GuardDuty servicio no podrá acceder a estas instantáneas en el futuro. `GuardDutyExcluded` Esto se debe a que las demás instrucciones de esta función vinculada al servicio GuardDuty impiden realizar ninguna acción en las instantáneas para las que se ha establecido esa función. `GuardDutyExcluded` `true`

- Permitir compartir y eliminar instantáneas solo si la etiqueta `GuardDutyScanId` existe y la etiqueta `GuardDutyExcluded` no está establecida en `true`.

> **Note**
>
> No permita que Protección contra malware haga públicas las instantáneas.

- Acceda a las claves administradas por el cliente, excepto a las que tengan una `GuardDutyExcluded` etiqueta configurada como`true`, `CreateGrant` para crear un volumen de EBS cifrado y acceder a él desde la instantánea cifrada que se comparte con la cuenta de servicio. GuardDuty Para obtener una lista de las cuentas de GuardDuty servicio de cada región, consulte[GuardDuty cuentas de servicio por Región de AWS](#).
- Acceda a los CloudWatch registros de los clientes para crear el grupo de registros de Malware Protection y coloque los registros de eventos de análisis de malware en el grupo de `/aws/guardduty/malware-scan-events` registros.
- Permitir que el cliente decida si quiere conservar en su cuenta las instantáneas en las que se detectó el malware. Si el análisis detecta malware, la función vinculada al servicio permite añadir dos etiquetas GuardDuty a las instantáneas: y. `GuardDutyFindingDetected` `GuardDutyExcluded`

> **Note**
>
> La etiqueta `GuardDutyFindingDetected` especifica que las instantáneas contienen malware.

- Determine si un volumen está cifrado con una clave gestionada por EBS. GuardDuty realiza la `DescribeKey` acción para determinar la clave `key Id` gestionada por EBS en su cuenta.
- Obtenga la instantánea de los volúmenes de EBS cifrados con Clave administrada de AWS, de su propiedad Cuenta de AWS y cópiela en la. [GuardDuty cuenta de servicio](#) Para ello, utilizamos

los permisos `GetSnapshotBlock` y. `ListSnapshotBlocks` GuardDuty luego escaneará la instantánea en la cuenta de servicio. En la actualidad, es Clave administrada de AWS posible que el soporte de protección contra malware para escanear volúmenes de EBS cifrados con los que esté cifrado no esté disponible en todos los Regiones de AWS. Para obtener más información, consulte Disponibilidad de características específicas por región.

- Permita que Amazon EC2 llame AWS KMS en nombre de Malware Protection para realizar varias acciones criptográficas en las claves administradas por el cliente. Acciones como `kms:ReEncryptTo` y `kms:ReEncryptFrom` son obligatorias para compartir las instantáneas cifradas con las claves administradas por el cliente. Solo se puede acceder a las claves para las que la etiqueta `GuardDutyExcluded` no esté establecida en `true`.

El rol se configura con la siguiente política administrada por AWS, que se denomina `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "DescribeAndListPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ecs:ListClusters",
                "ecs:ListContainerInstances",
                "ecs:ListTasks",
                "ecs:DescribeTasks",
                "eks:DescribeCluster"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateSnapshotVolumeConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:volume/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
```

```
            }
        },
        {
            "Sid": "CreateSnapshotConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyScanId"
                }
            }
        },
        {
            "Sid": "CreateTagsPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:*/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSnapshot"
                }
            }
        },
        {
            "Sid": "AddTagsToSnapshotPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyExcluded",
                        "GuardDutyFindingDetected"
                    ]
                }
            }
        },
        {
            "Sid": "DeleteAndShareSnapshotPermission",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:DeleteSnapshot",
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "PreventPublicAccessToSnapshotPermission",
            "Effect": "Deny",
            "Action": [
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:Add/group": "all"
                }
            }
        },
        {
            "Sid": "CreateGrantPermission",
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:ebs:id": "snap-*"
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
                        "CreateGrant",
                        "GenerateDataKeyWithoutPlaintext",
```

```
                    "ReEncryptFrom",
                    "ReEncryptTo",
                    "RetireGrant",
                    "DescribeKey"
                ]
            },
            "Bool": {
                "kms:GrantIsForAWSResource": "true"
            }
        }
    },
    {
        "Sid": "ShareSnapshotKMSPermission",
        "Effect": "Allow",
        "Action": [
            "kms:ReEncryptTo",
            "kms:ReEncryptFrom"
        ],
        "Resource": "arn:aws:kms:*:*:key/*",
        "Condition": {
            "StringLike": {
                "kms:ViaService": "ec2.*.amazonaws.com"
            },
            "Null": {
                "aws:ResourceTag/GuardDutyExcluded": "true"
            }
        }
    },
    {
        "Sid": "DescribeKeyPermission",
        "Effect": "Allow",
        "Action": "kms:DescribeKey",
        "Resource": "arn:aws:kms:*:*:key/*"
    },
    {
        "Sid": "GuardDutyLogGroupPermission",
        "Effect": "Allow",
        "Action": [
            "logs:DescribeLogGroups",
            "logs:CreateLogGroup",
            "logs:PutRetentionPolicy"
        ],
        "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
    },
```

```
        {
            "Sid": "GuardDutyLogStreamPermission",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
        },
        {
            "Sid": "EBSDirectAPIPermissions",
            "Effect": "Allow",
            "Action": [
                "ebs:GetSnapshotBlock",
                "ebs:ListSnapshotBlocks"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        }
    ]
}
```

La siguiente política de confianza se ha adjuntado al rol vinculado a servicios `AWSServiceRoleForAmazonGuardDutyMalwareProtection`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
```

```
  ]
}
```

Creación de un rol vinculado a servicios para Protección contra malware

El rol vinculado a servicios `AWSServiceRoleForAmazonGuardDutyMalwareProtection` se crea automáticamente cuando se habilita Protección contra malware por primera vez o al habilitar Protección contra malware en una región compatible en la que no estaba habilitado. También puede crear el rol vinculado a servicios `AWSServiceRoleForAmazonGuardDutyMalwareProtection` manualmente con la consola de IAM, la CLI de IAM o la API de IAM.

> **Note**
>
> De forma predeterminada, si eres nuevo en Amazon GuardDuty, la protección contra malware se activa automáticamente.

> **Important**
>
> El rol vinculado al servicio que se crea para la cuenta de GuardDuty administrador delegado no se aplica a las cuentas de los miembros. GuardDuty

Debe configurar permisos para permitir a una entidad principal de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para que el rol `AWSServiceRoleForAmazonGuardDutyMalwareProtection` vinculado al servicio se cree correctamente, la identidad de IAM que utilices GuardDuty debe tener los permisos necesarios. Para conceder los permisos necesarios, asocie la siguiente política a un usuario, un grupo o un rol de :

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
```

```
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

Para obtener más información sobre cómo crear un rol manualmente, consulte Crear un rol vinculado a servicios en la Guía del usuario de IAM.

Edición de un rol vinculado a servicios para Protección contra malware

Protección contra malware no le permite editar el rol vinculado a servicios `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol utilizando IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a servicios para Protección contra malware

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no conservará una entidad no utilizada que no se monitoree ni se mantenga de forma activa.

> **Important**
>
> Para poder eliminar `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, primero debe deshabilitar Protección contra malware en todas las regiones en las que esté habilitada.
> Si Protección contra malware está habilitada cuando intenta eliminar el rol vinculado a servicios, el rol no se eliminará. Para obtener más información, consulte Para activar o desactivar el GuardDuty análisis de malware iniciado.

Si selecciona Deshabilitar para detener el servicio Protección contra malware, `AWSServiceRoleForAmazonGuardDutyMalwareProtection` no se elimina automáticamente. Si, a continuación, selecciona Activar para volver a iniciar el servicio de protección contra malware, GuardDuty empezará a utilizar el existente. `AWSServiceRoleForAmazonGuardDutyMalwareProtection`

Cómo eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la AWS CLI o la API de IAM para eliminar el rol vinculado al `AWSServiceRoleForAmazonGuardDutyMalwareProtection` servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Soportado Regiones de AWS

Amazon GuardDuty admite el uso de la función `AWSServiceRoleForAmazonGuardDutyMalwareProtection` vinculada al servicio en todos los Regiones de AWS lugares donde esté disponible Malware Protection.

Para ver una lista de las regiones en las GuardDuty que está disponible actualmente, consulta los GuardDuty puntos de conexión y las cuotas de Amazon en. Referencia general de Amazon Web Services

> **Note**
>
> La protección contra malware no está disponible actualmente en AWS GovCloud (EE. UU. este) ni (EE. UU., AWS GovCloud oeste).

Solución de problemas de GuardDuty identidad y acceso a Amazon

Usa la siguiente información para ayudarte a diagnosticar y solucionar los problemas más comunes que puedes encontrar al trabajar con un GuardDuty IAM.

Temas

- No estoy autorizado a realizar ninguna acción en GuardDuty
- No estoy autorizado a realizar iam:PassRole.
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis GuardDuty recursos.

No estoy autorizado a realizar ninguna acción en GuardDuty

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `guardduty:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 guardduty:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `guardduty:`*`GetWidget`*.

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.

No estoy autorizado a realizar iam:PassRole.

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

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

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en GuardDuty. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis GuardDuty recursos.

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 saber si GuardDuty es compatible con estas funciones, consulteCómo GuardDuty funciona Amazon con IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte 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 acerca de 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 una 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.

AWS políticas gestionadas para Amazon GuardDuty

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas tú mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios añaden permisos adicionales a una política AWS gestionada para admitir nuevas funciones. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Lo más probable es que los servicios actualicen una política AWS administrada cuando se lanza una nueva función o cuando hay nuevas operaciones disponibles. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política ReadOnlyAccess AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripción de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

AWS política gestionada: AmazonGuardDutyFullAccess

Puede adjuntar la política de `AmazonGuardDutyFullAccess` a las identidades de IAM.

Esta política otorga permisos administrativos que permiten al usuario el acceso total a todas GuardDuty las acciones.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `GuardDuty`— Permite a los usuarios el acceso total a todas GuardDuty las acciones.
- `IAM`— Permite a los usuarios crear el rol GuardDuty vinculado al servicio. Esto permite al GuardDuty administrador habilitar las cuentas de GuardDuty los miembros.
- `Organizations`— Permite a los usuarios designar un administrador delegado y gestionar los miembros de una GuardDuty organización.

El permiso para llevar a cabo una acción `iam:GetRole` en `AWSServiceRoleForAmazonGuardDutyMalwareProtection` establece si el rol vinculado a servicios (SLR) de Protección contra malware existe en una cuenta.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonGuardDutyFullAccessSid1",
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleSid1",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "guardduty.amazonaws.com",
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
```

```
            "Sid": "ActionsForOrganizationsSid1",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IamGetRoleSid1",
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

AWS política gestionada: AmazonGuardDutyReadOnlyAccess

Puede adjuntar la política de `AmazonGuardDutyReadOnlyAccess` a las identidades de IAM.

Esta política otorga permisos de solo lectura que permiten al usuario ver las GuardDuty conclusiones y los detalles de su GuardDuty organización.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `GuardDuty`— Permite a los usuarios ver los GuardDuty resultados y realizar operaciones de API que comiencen con `GetList`, o. `Describe`
- `Organizations`— Permite a los usuarios recuperar información sobre GuardDuty la configuración de la organización, incluidos los detalles de la cuenta de administrador delegado.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:Describe*",
                "guardduty:Get*",
                "guardduty:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS política gestionada: AmazonGuardDutyServiceRolePolicy

No puede asociar `AmazonGuardDutyServiceRolePolicy` a sus entidades IAM. Esta política AWS gestionada está asociada a un rol vinculado al servicio que permite GuardDuty realizar acciones en su nombre. Para obtener más información, consulte Permisos de rol vinculados al servicio para GuardDuty.

GuardDuty actualizaciones de las políticas gestionadas AWS

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas GuardDuty desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del GuardDuty documento.

Cambio	Descripción	Fecha
AmazonGuardDutyServiceRolePolicy: actualización de una política existente.	Utilice AWS Systems Manager acciones para gestionar las asociaciones de SSM en las instancias de Amazon EC2 al GuardDuty habilitar Runtime Monitoring con un agente automatizado para Amazon EC2. Cuando la configuración GuardDuty automática de agentes está deshabilitada, solo GuardDuty tiene en cuenta las instancias EC2 que tienen una etiqueta de inclusión (:). `GuardDuty Managed true`	26 de marzo de 2024
AmazonGuardDutyServiceRolePolicy: actualización de una política existente.	GuardDuty ha añadido un nuevo permiso `organization:DescribeOrganization` para recuperar el ID de organización de la cuenta de Amazon VPC compartida y configurar la política de puntos finales de Amazon VPC con el ID de la organización.	9 de febrero de 2024
AmazonGuardDutyMalwareProtectionServiceRolePolítica: se actualiza a una política existente.	Malware Protection ha añadido dos permisos: `GetSnapshotBlock` el de `ListSnapshotBlocks` obtener una instantánea de un volumen de EBS (cifrada mediante Clave administrada de AWS) Cuenta de AWS y copiarla a la cuenta de	25 de enero de 2024

Cambio	Descripción	Fecha
	GuardDuty servicio antes de iniciar el análisis de software malicioso.	
AmazonGuardDutyServiceRolePolicy: actualización de una política actual	Se han añadido nuevos permisos que permiten GuardDuty añadir la configuración de la cuenta de `guarddutyActivate` Amazon ECS y realizar, enumerar y describir operaciones en los clústeres de Amazon ECS.	26 de noviembre de 2023
AmazonGuardDutyReadOnlyAccess: actualización de una política actual	GuardDuty agregó una nueva política `organizations` para`ListAccounts` .	16 de noviembre de 2023
AmazonGuardDutyFullAccess: actualización de una política actual	GuardDuty agregó una nueva política `organizations` para`ListAccounts` .	16 de noviembre de 2023
AmazonGuardDutyServiceRolePolicy: actualización de una política actual	GuardDuty agregó nuevos permisos para admitir la próxima función de monitoreo de tiempo de ejecución de GuardDuty EKS.	8 de marzo de 2023

Cambio	Descripción	Fecha
AmazonGuardDutyServiceRolePolicy: actualización de una política actual	GuardDuty ha añadido nuevos permisos que permiten crear un rol vinculado GuardDuty al servicio para la protección contra malware. Esto ayudará a GuardDuty agilizar el proceso de activación de la protección contra el malware. GuardDuty ahora puede realizar la siguiente acción de IAM: `{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }`	21 de febrero de 2023
AmazonGuardDutyFullAccess: actualización de una política actual	GuardDuty ARN actualizado para `iam:GetRole . *AWSServiceRoleForAmazonGuardDutyMalwareProtection`	26 de julio de 2022

Cambio	Descripción	Fecha
AmazonGuardDutyFullAccess: actualización de una política actual	GuardDuty se agregó uno nuevo `AWSServiceName` para permitir la creación de un rol vinculado al servicio mediante `iam:CreateServiceLinkedRole` el servicio de protección GuardDuty contra malware. GuardDuty ahora puede realizar la `iam:GetRole` acción para obtener información. `AWSServiceRole`	26 de julio de 2022

Cambio	Descripción	Fecha
AmazonGuardDutyServiceRolePolicy: actualización de una política actual	GuardDuty se han añadido nuevos permisos que permiten GuardDuty utilizar las acciones de red de Amazon EC2 para mejorar los resultados. GuardDuty ahora puede realizar las siguientes acciones de EC2 para obtener información sobre cómo se comunican sus instancias de EC2. Esta información se utiliza para mejorar la precisión de los resultados. • `ec2:DescribeVpcEndpoints` • `ec2:DescribeSubnets` • `ec2:DescribeVpcPeeringConnections` • `ec2:DescribeTransitGatewayAttachments`	3 de agosto de 2021
GuardDuty comenzó a rastrear los cambios	GuardDuty comenzó a rastrear los cambios de sus políticas AWS gestionadas.	3 de agosto de 2021

Validación de conformidad para Amazon GuardDuty

Para saber si un Servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte Servicios de AWS en el ámbito del programa de conformidad y escoja el

programa de conformidad que le interese. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad de conformidad al utilizar Servicios de AWS se determina en función de la sensibilidad de los datos, los destinos de cumplimiento de su empresa y la legislación y los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- Guías de inicio rápido de seguridad y conformidad: estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones compatibles con HIPAA.

  > **Note**
  >
  > No todos los Servicios de AWS son compatibles con HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- AWS Customer Compliance Guides: comprenda el modelo de responsabilidad compartida desde el punto de vista de la conformidad. En las guías se resumen las prácticas recomendadas para garantizar la seguridad de los Servicios de AWS y se orientan los controles de seguridad en varios marcos (incluidos el National Institute of Standards and Technology o NIST, el Payment Card Industry Security Standards Council o PCI y la International Organization for Standardization o ISO).
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este Servicio de AWS proporciona una visión completa de su estado de seguridad en AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la

seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la referencia de controles de Security Hub.

- AWS Audit Manager: este Servicio de AWS le ayuda a auditar continuamente el uso de AWS con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

Resiliencia de Amazon GuardDuty

La infraestructura global de AWS está conformada por regiones y zonas de disponibilidad de 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 zonas de disponibilidad y las regiones de AWS, consulte Infraestructura global de AWS.

Seguridad de la infraestructura en Amazon Amazon GuardDuty

Como se trata de un servicio administrado, Amazon Athena se encuentra protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas en AWS para acceder 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 de seguridad de IAM. También puede utilizar AWS

Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

AWSintegraciones de servicios con GuardDuty

GuardDuty se puede integrar en otros servicios de seguridad. AWS Estos servicios pueden ingerir datos de GuardDuty para que pueda ver los hallazgos de nuevas formas. Consulte las siguientes opciones de integración para obtener más información sobre cómo funciona cada servicio con .

Integración de GuardDuty con AWS Security Hub

AWS Security Hubrecopila datos de seguridad de todas sus AWS cuentas de, de sus servicios y de los productos de terceros compatibles para evaluar el estado de seguridad de su entorno de acuerdo con los estándares y las mejores prácticas del sector. Además de evaluar su postura de seguridad, Security Hub crea una ubicación central para encontrar información sobre todos sus AWS servicios integrados y productos de AWS socios. Al habilitar Security Hub con GuardDuty, Security Hub podrá ingerir automáticamente los datos de hallazgos de GuardDuty.

Para obtener más información sobre el uso de Security Hub con GuardDuty, consulte. Integración con AWS Security Hub

Integración de GuardDuty con Amazon Detective

Amazon Detective utiliza los datos de registro de todas sus AWS cuentas para crear visualizaciones de datos para sus recursos y direcciones IP que interactúan con su entorno. Las visualizaciones de Detective le ayudan a investigar los problemas de seguridad de forma rápida y sencilla. Una vez que ambos servicios estén activados, puede pasar de GuardDuty a buscar información en la consola de Detective.

Para obtener información más detallada acerca de cómo utilizar el agente con , consulte .

Integración con AWS Security Hub

AWS Security Hub le proporciona una visión completa de su estado de seguridad en AWS y lo ayuda a comprobar su entorno con las prácticas recomendadas y los estándares del sector de seguridad. Security Hub recopila datos de seguridad de todas AWS las cuentas, servicios y productos de socios externos compatibles y le ayuda a analizar sus tendencias de seguridad e identificar los problemas de seguridad más prioritarios.

La GuardDuty integración de Amazon con Security Hub le permite enviar los resultados desde GuardDuty Security Hub. Security Hub puede incluir esos resultados en su análisis de la posición de seguridad.

Contenido

Cómo GuardDuty envía Amazon los resultados a AWS Security Hub

En AWS Security Hub, los problemas de seguridad se rastrean como hallazgos. Algunos hallazgos provienen de problemas detectados por otros AWS servicios o por socios externos. Security Hub también cuenta con un conjunto de reglas que utiliza para detectar problemas de seguridad y generar resultados.

Security Hub proporciona herramientas para administrar los resultados de todas estas fuentes. Puede ver y filtrar listas de resultados y ver los detalles de una búsqueda. Para obtener más información, consulte Visualización de resultados en la Guía del usuario de AWS Security Hub . También puede realizar un seguimiento del estado de una investigación de un resultado. Para obtener más información, consulte Adopción de medidas en función de los resultados en la Guía del usuario de AWS Security Hub .

Todos los resultados de Security Hub utilizan un formato JSON estándar denominado AWS Security Finding Format (ASFF). El ASFF incluye detalles sobre el origen del problema, los recursos afectados y el estado actual del resultado. Consulte Formato de resultado de seguridad de AWS (ASFF) en la Guía del usuario de AWS Security Hub .

Amazon GuardDuty es uno de los AWS servicios que envía los resultados a Security Hub.

Tipos de hallazgos que se GuardDuty envían a Security Hub

Una vez que habilita GuardDuty un Security Hub en la misma cuenta dentro de la misma Región de AWS, GuardDuty comienza a enviar todos los hallazgos generados a Security Hub. Estas conclusiones se envían a Security Hub mediante el formato AWS de búsqueda de seguridad (ASFF). En ASFF, el campo `Types` proporciona el tipo de resultado.

Latencia para enviar nuevos hallazgos

Cuando GuardDuty crea un nuevo hallazgo, normalmente se envía a Security Hub en un plazo de cinco minutos.

Reintento cuando Security Hub no está disponible

Si Security Hub no está disponible, GuardDuty vuelve a intentar enviar las conclusiones hasta que las reciba.

Actualización de los resultados existentes en Security Hub

Después de enviar un hallazgo a Security Hub, GuardDuty envía actualizaciones para reflejar las observaciones adicionales de la actividad de búsqueda a Security Hub. Las nuevas observaciones de estos hallazgos se envían a Security Hub en función de la Paso 5: Exportar la frecuencia de actualización configuración de su Cuenta de AWS.

Cuando archiva o desarchiva un hallazgo, GuardDuty no lo envía a Security Hub. Los resultados desarchivados manualmente que se activen posteriormente no GuardDuty se envían a Security Hub.

Visualización de GuardDuty los resultados en AWS Security Hub

Para ver tus GuardDuty hallazgos en Security Hub, selecciona Ver hallazgos en Amazon en la página GuardDuty de resumen. Como alternativa, puede seleccionar Hallazgos en el panel de navegación y filtrar los hallazgos para que se muestren solo GuardDuty los hallazgos seleccionando el campo Nombre del producto: con un valor de`GuardDuty`.

Interpretar los nombres de los GuardDuty buscados en AWS Security Hub

GuardDuty envía los resultados a Security Hub mediante el formato AWS de búsqueda de seguridad (ASFF). En ASFF, el campo `Types` proporciona el tipo de resultado. Los tipos de ASFF utilizan un esquema de nomenclatura diferente al de GuardDuty los tipos. En la siguiente tabla se detallan todos los tipos de GuardDuty hallazgos con su homólogo de ASFF tal y como aparecen en Security Hub.

> **Note**
>
> Para algunos tipos de GuardDuty búsqueda, Security Hub asigna diferentes nombres de búsqueda de ASFF en función de si la función de recurso del detalle de búsqueda era ACTOR o TARGET. Para más información, consulte Detalles de los resultados.

GuardDuty tipo de búsqueda	Tipo de resultado de ASFF
Backdoor:EC2/C&CActivity.B	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS
Backdoor:EC2/DenialOfService.Dns	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns
Backdoor:EC2/DenialOfService.Tcp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp
Backdoor:EC2/DenialOfService.Udp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol
Backdoor:EC2/Spambot	TTPs/Command and Control/Backdoor:EC2-Spambot
Behavior:EC2/NetworkPortUnusual	Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual

GuardDuty tipo de búsqueda	Tipo de resultado de ASFF
Backdoor:Lambda/C&CActivity.B	TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B
Backdoor:Runtime/C&CActivity.B	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B
Backdoor:Runtime/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS
CredentialAccess:IAMUser/AnomalousBehavior	TTPs/Credential Access/IAMUser-AnomalousBehavior
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulLogin
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/RDS-TorIPCaller.FailedLogin
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-TorIPCaller.SuccessfulLogin
CryptoCurrency:EC2/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B

GuardDuty tipo de búsqueda	Tipo de resultado de ASFF
CryptoCurrency:EC2/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS
DefenseEvasion:EC2/UnusualDNSResolver	TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver
DefenseEvasion:EC2/UnusualDoHActivity	TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity
DefenseEvasion:EC2/UnusualDoTActivity	TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity
DefenseEvasiontipo de búsqueda ----SEP----:IAMuser/ AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand
Descubrimiento: soy usuario/ Anomalous Behavior	TTPs/Discovery/IAMUser-AnomalousBehavior

GuardDuty tipo de búsqueda	Tipo de resultado de ASFF
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
Discovery:S3/AnomalousBehavior	TTPs/Discovery:S3-AnomalousBehavior
Discovery:S3/BucketEnumeration.Unusual	TTPs/Discovery:S3-BucketEnumeration.Unusual
Discovery:S3/MaliciousIPCaller.Custom	TTPs/Discovery:S3-MaliciousIPCaller.Custom
Discovery:S3/TorIPCaller	TTPs/Discovery:S3-TorIPCaller
Discovery:S3/MaliciousIPCaller	TTPs/Discovery:S3-MaliciousIPCaller
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile

GuardDuty tipo de búsqueda	Tipo de resultado de ASFF
Execution:Container/MaliciousFile	TTPs/Execution/Execution:Container-MaliciousFile
Execution:EC2/SuspiciousFile	TTPs/Execution/Execution:EC2-SuspiciousFile
Execution:ECS/SuspiciousFile	TTPs/Execution/Execution:ECS-SuspiciousFile
Execution:Kubernetes/SuspiciousFile	TTPs/Execution/Execution:Kubernetes-SuspiciousFile
Execution:Container/SuspiciousFile	TTPs/Execution/Execution:Container-SuspiciousFile
Execution:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted
Execution:Runtime/NewBinaryExecuted	TTPs/Execution/Execution:Runtime-NewBinaryExecuted
Execution:Runtime/NewLibraryLoaded	TTPs/Execution/Execution:Runtime-NewLibraryLoaded
Execution:Runtime/ReverseShell	TTPs/Execution/Execution:Runtime-ReverseShell
Execution:Runtime/SuspiciousCommand	TTPs/Execution/Execution:Runtime-SuspiciousCommand
Execution:Runtime/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual
Exfiltration:S3/MaliciousIPCaller	TTPs/Exfiltration:S3-MaliciousIPCaller

GuardDuty tipo de búsqueda	Tipo de resultado de ASFF
Impact:EC2/AbusedDomainRequest.Reputation	TTPs/Impact:EC2-AbusedDomainRequest.Reputation
Impact:EC2/BitcoinDomainRequest.Reputation	TTPs/Impact:EC2-BitcoinDomainRequest.Reputation
Impact:EC2/MaliciousDomainRequest.Reputation	TTPs/Impact:EC2-MaliciousDomainRequest.Reputation
Impact:EC2/PortSweep	TTPs/Impact/Impact:EC2-PortSweep
Impact:EC2/SuspiciousDomainRequest.Reputation	TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation
Impact:EC2/WinRMBruteForce	TTPs/Impact/Impact:EC2-WinRMBruteForce
Impacto: soy usuario/ AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior
Impact:Runtime/AbusedDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation
Impact:Runtime/BitcoinDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation
Impact:Runtime/CryptoMinerExecuted	TTPs/Impact/Impact:Runtime-CryptoMinerExecuted
Impact:Runtime/MaliciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation
Impact:Runtime/SuspiciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputatio
Impact:S3/AnomalousBehavior.Delete	TTPs/Impact:S3-AnomalousBehavior.Delete
Impact:S3/AnomalousBehavior.Permission	TTPs/Impact:S3-AnomalousBehavior.Permission

GuardDuty tipo de búsqueda	Tipo de resultado de ASFF
Impact:S3/AnomalousBehavior.Write	TTPs/Impact:S3-AnomalousBehavior.Write
Impact:S3/ObjectDelete.Unusual	TTPs/Impact:S3-ObjectDelete.Unusual
Impact:S3/PermissionsModification.Unusual	TTPs/Impact:S3-PermissionsModification.Unusual
Impact:S3/MaliciousIPCaller	TTPs/Impact:S3-MaliciousIPCaller
InitialAccessImpacto: iamuser/ ----SEP----:iamuser/ AnomalousBehavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
PenTest:IAMUser/KaliLinux	TTPs/PenTest:IAMUser/KaliLinux
PenTest:IAMUser/ParrotLinux	TTPs/PenTest:IAMUser/ParrotLinux
PenTest:IAMUser/PentooLinux	TTPs/PenTest:IAMUser/PentooLinux
PenTest:S3/KaliLinux	TTPs/PenTest:S3-KaliLinux
PenTest:S3/ParrotLinux	TTPs/PenTest:S3-ParrotLinux
PenTest:S3/PentooLinux	TTPs/PenTest:S3-PentooLinux
Persistencia: IamUser/ AnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions
Persistence:IAMUser/UserPermissions	TTPs/Persistence/Persistence:IAMUser-UserPermissions
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage

GuardDuty tipo de búsqueda	Tipo de resultado de ASFF
Policy:S3/AccountBlockPublicAccessDisabled	TTPs/Policy:S3-AccountBlockPublicAccessDisabled
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccessGranted
Policy:S3/BucketBlockPublicAccessDisabled	Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled
Policy:S3/BucketPublicAccessGranted	TTPs/Policy:S3-BucketPublicAccessGranted
PrivilegeEscalationPersistencia: iamuser/ ----sep----:iamuser/ AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleBindingCreated
PriviledgeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleCreated
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified
PrivilegeEscalation:Runtime/DockerSocketAccessed	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed
PrivilegeEscalation:Runtime/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape
PrivilegeEscalation:Runtime/UserfaultfdUsage	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage

GuardDuty tipo de búsqueda	Tipo de resultado de ASFF
Recon:EC2/PortProbeEMRUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort
Recon:EC2/PortProbeUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort
Recon:EC2/Portscan	TTPs/Discovery/Recon:EC2-Portscan
Recon:IAMUser/MaliciousIPCaller	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller
Recon:IAMUser/MaliciousIPCaller.Custom	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom
Recon:IAMUser/NetworkPermissions	TTPs/Discovery/Recon:IAMUser-NetworkPermissions
Recon:IAMUser/ResourcePermissions	TTPs/Discovery/Recon:IAMUser-ResourcePermissions
Recon:IAMUser/TorIPCaller	TTPs/Discovery/Recon:IAMUser-TorIPCaller
Recon:IAMUser/UserPermissions	TTPs/Discovery/Recon:IAMUser-UserPermissions
ResourceConsumption:IAMUser/ComputeResources	Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources
Stealth:IAMUser/CloudTrailLoggingDisabled	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled
Stealth:IAMUser/LoggingConfigurationModified	TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified
Stealth:IAMUser/PasswordPolicyChange	TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange

GuardDuty tipo de búsqueda	Tipo de resultado de ASFF
Stealth:S3/ServerAccessLoggingDisabled	TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled
Trojan:EC2/BlackholeTraffic	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic
Trojan:EC2/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS
Trojan:EC2/DGADomainRequest.B	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B
Trojan:EC2/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS
Trojan:EC2/DNSDataExfiltration	TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration
Trojan:EC2/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS
Trojan:EC2/DropPoint	Effects/Data Exfiltration/Trojan:EC2-DropPoint
Trojan:EC2/DropPoint!DNS	Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS
Trojan:EC2/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS
Trojan:Lambda/BlackholeTraffic	TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic
Trojan:Lambda/DropPoint	Effects/Data Exfiltration/Trojan:Lambda-DropPoint
Trojan:Runtime/BlackholeTraffic	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic

GuardDuty tipo de búsqueda	Tipo de resultado de ASFF
Trojan:Runtime/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS
Trojan:Runtime/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS
Trojan:Runtime/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!DNS
Trojan:Runtime/DropPoint	Effects/Data Exfiltration/Trojan:Runtime-DropPoint
Trojan:Runtime/DropPoint!DNS	Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS
Trojan:Runtime/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom
UnauthorizedAccess:EC2/MetadataDNSRebind	TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind
UnauthorizedAccess:EC2/RDPBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce
UnauthorizedAccess:EC2/SSHBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce
UnauthorizedAccess:EC2/TorClient	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient
UnauthorizedAccess:EC2/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/UnauthorizedAccess:IAMUser-ConsoleLogin

GuardDuty tipo de búsqueda	Tipo de resultado de ASFF
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/MaliciousIPCaller	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom
UnauthorizedAccess:IAMUser/TorIPCaller	TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom
UnauthorizedAccess:Lambda/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient
UnauthorizedAccess:Lambda/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
UnauthorizedAccess:Runtime/MetadataDNSRebind	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind
UnauthorizedAccess:Runtime/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay
UnauthorizedAccess:Runtime/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient

GuardDuty tipo de búsqueda	Tipo de resultado de ASFF
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom
UnauthorizedAccess:S3/TorIPCaller	TTPs/UnauthorizedAccess:S3-TorIPCaller

Resultado típico de GuardDuty

GuardDuty envía las conclusiones a Security Hub mediante el formato AWS de búsqueda de seguridad (ASFF).

A continuación se muestra un ejemplo de un hallazgo típico de GuardDuty.


```
  {
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws::securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
  "UpdatedAt": "2020-09-30T12:14:00.206Z",
  "Severity": {
    "Product": 2,
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356.",
  "Description": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
 instance by guessing the SSH password.",
  "SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
```

```
  "ProductFields": {
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
 "Unknown",
    "aws/guardduty/service/archived": "false",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
 "199.241.229.197",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
    "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
 "46717",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
    "aws/guardduty/service/serviceName": "guardduty",
    "aws/guardduty/service/evidence": "",
    "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
 "172.31.43.6",
    "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",
    "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
 "INBOUND",
    "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
    "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
 "SSH",
    "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
    "aws/guardduty/service/additionalInfo": "",
    "aws/guardduty/service/resourceRole": "TARGET",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
    "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
    "aws/guardduty/service/count": "74",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asn": "209",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
isp": "CenturyLink",
```

```
    "aws/securityhub/FindingId": "arn:aws::securityhub:us-east-1::product/
aws/guardduty/arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws::ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "18.234.130.16",
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475",
          "LaunchedAt": "2020-08-03T23:21:57Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```


Habilitación y configuración de la integración

Para usar la integración con AWS Security Hub, debe habilitar Security Hub. Para obtener información acerca de cómo habilitar Security Hub, consulte la Configuración de Security Hub en la Guía del usuario de AWS Security Hub .

Al habilitar ambos GuardDuty y Security Hub, la integración se habilita automáticamente. GuardDutycomienza inmediatamente a enviar los resultados a Security Hub.

Interrupción de la publicación de resultados en Security Hub

Para dejar de enviar resultados a Security Hub, puede utilizar la consola de Security Hub o la API.

Consulte Deshabilitar y habilitar el flujo de hallazgos desde una integración (consola) o Inhabilitar el flujo de hallazgos desde una integración (API de Security Hub, AWS CLI) en la Guía del AWS Security Hub usuario.

Integración con Amazon S3

Amazon Detective le ayuda a analizar e investigar rápidamente los eventos de seguridad en una o más AWS cuentas mediante la generación de visualizaciones de datos que representan la forma en que sus recursos se comportan e interactúan a lo largo del tiempo. Detective crea visualizaciones de los hallazgos de GuardDuty.

El Detective recopila los detalles de los hallazgos de todos los tipos de hallazgos y proporciona acceso a los perfiles de las entidades para investigar las diferentes entidades que están involucradas en el hallazgo. Una entidad puede ser una dirección IP externaCuenta de AWS, un AWS recurso dentro de una cuenta o una dirección IP externa que ha interactuado con tus recursos. La consola GuardDuty permite pasar a Amazon Detective desde las siguientes entidades, según el Cuenta de AWS tipo de búsqueda: rol de IAM, usuario o sesión de rol, agente de usuario, usuario federado, instancia de Amazon EC2 o dirección IP.

Contenido

Habilitación de la integración

Para utilizar Amazon Detective con GuardDuty, primero debe activar Amazon Detective. Para obtener información sobre cómo activar Detective, consulte Configuración de Amazon Detective en la Guía de administración de Amazon Detective.

Cuando habilita GuardDuty y Detective, la integración se activa automáticamente. Una vez activado, Detective recopilará inmediatamente los datos de tus hallazgos de GuardDuty.

> **Note**
>
> GuardDuty envía los resultados al Detective en función de la frecuencia de exportación de los hallazgos de GuardDuty. De forma predeterminada, la frecuencia de exportación de las actualizaciones de los hallazgos existentes es de 6 horas. Para garantizar que Detective reciba las actualizaciones más recientes de sus hallazgos, le recomendamos que cambie la frecuencia de exportación a 15 minutos en cada región en la que utilice Detective con GuardDuty. Para obtener más información, consulte Paso 5: Establecer la frecuencia para exportar los hallazgos activos actualizados.

Pasar de un hallazgo de GuardDuty a Amazon Detective

1. Abra la consola de en https://console.aws.amazon.com/guardduty.
2. Elija un único hallazgo de la tabla de hallazgos.
3. Seleccione Investigar con Detective en el panel de detalles de búsqueda.
4. Elige un aspecto del hallazgo para investigarlo con Amazon Detective. Esto abre la consola de Detectives para ese hallazgo o entidad.

Si el pivote no se comporta como se esperaba, consulte Solución de problemas del pivote en la Guía del usuario de Amazon Detective.

> **Note**
>
> Si archivas un hallazgo de GuardDuty en la consola de Detectives, ese hallazgo también se archiva en la consola GuardDuty.

Uso de la integración con un entorno de múltiples cuentas de GuardDuty

Si administra un entorno de varias cuentas en GuardDuty, debe añadir sus cuentas de miembro a Amazon Detective para poder ver las visualizaciones de datos de los detectives sobre los hallazgos y las entidades de esas cuentas.

Se recomienda utilizar la misma cuenta de administrador de GuardDuty que la cuenta de administrador de Detective. Para obtener más información sobre cómo añadir cuentas de miembros en Detective, consulta Cómo invitar cuentas de miembros.

> **Note**
>
> Detective es un servicio regional, lo que significa que debes habilitar Detective y añadir tus cuentas de miembro en cada región en la que quieras usar la integración.

Suspender o deshabilitar GuardDuty

Puedes usar la GuardDuty consola para suspender o deshabilitar el GuardDuty servicio. No se te cobrará por usarlo GuardDuty cuando el servicio esté suspendido.

- Todas las cuentas de los miembros deben disociarse o eliminarse antes de poder suspenderlas o deshabilitarlas GuardDuty.
- Si las suspende GuardDuty, dejará de supervisar la seguridad de su AWS entorno ni generará nuevos hallazgos. Sus hallazgos actuales permanecen intactos y no se ven afectados por la GuardDuty suspensión. Puedes optar por volver a activarla GuardDuty más adelante.
- Cuando la inhabilitas GuardDuty en una cuenta, solo se deshabilitará para la que esté seleccionada Región de AWS actualmente. Si desea deshabilitarla por completo GuardDuty, debe deshabilitarla en cada región en la que esté habilitada.
- Si la desactiva GuardDuty, los datos encontrados y la GuardDuty configuración se perderán y no se podrán recuperar. Si quieres guardar tus hallazgos actuales, debes exportarlos antes de confirmar la desactivación GuardDuty. Para obtener más información sobre cómo exportar resultados, consulte Exportación de resultados.

Para suspender o deshabilitar GuardDuty

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, seleccione Configuración.
3. En la GuardDuty sección Suspender, selecciona Suspender GuardDuty o Desactivar GuardDuty y, a continuación, confirma la acción.

Para volver a activarla GuardDuty después de la suspensión

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. En el panel de navegación, seleccione Configuración.
3. Selecciona Volver a activar. GuardDuty

Suscripción a los anuncios de Amazon GuardDuty SNS

En esta sección se proporciona información sobre la suscripción a Amazon SNS (Simple Notification Service) GuardDuty para recibir anuncios sobre tipos de búsqueda publicados recientemente, actualizaciones de los tipos de búsqueda existentes y otros cambios de funcionalidad. Las notificaciones están disponibles en todos los formatos que admite Amazon SNS.

El GuardDuty SNS envía anuncios sobre las actualizaciones del GuardDuty servicio AWS a cualquier cuenta suscrita. Para recibir notificaciones sobre los resultados de su cuenta, consulte Creación de respuestas personalizadas a GuardDuty los hallazgos con Amazon CloudWatch Events.

> **Note**
>
> Su usuario de IAM debe disponer de los permisos `sns::subscribe` para suscribirse a un tema de SNS.

Puede suscribir una cola de Amazon SQS a este tema de notificación, pero debe utilizar un ARN de tema que esté en la misma región. Para obtener más información, consulte Tutorial: Subscribing an Amazon SQS queue to an Amazon SNS topic en la Guía para desarrolladores de Amazon Simple Queue Service.

También puedes usar una AWS Lambda función para activar eventos cuando se reciben notificaciones. Para obtener más información, consulte Invocación de funciones de Lambda mediante notificaciones de Amazon SNS en la Guía para desarrolladores de Amazon Simple Queue Service.

Los ARN de tema de Amazon SNS para cada región se muestran a continuación.

AWS Región	ARN del tema de Amazon SNS
`us-east-1`	`arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements`
`us-east-2`	`arn:aws:sns:us-east-2:118283430703:G`

AWS Región	ARN del tema de Amazon SNS
	uardDutyAnnouncements
us-west-1	arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements
us-west-2	arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements
ca-central-1	arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements
ca-west-1	arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements
eu-north-1	arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements
eu-west-1	arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements

AWS Región	ARN del tema de Amazon SNS
eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements
eu-west-3	arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements
eu-central-1	arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements
eu-central-2	arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements
ap-east-1	arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements
ap-northeast-1	arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements
ap-northeast-2	arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements

AWS Región	ARN del tema de Amazon SNS
ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements
ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements
ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements

AWS Región	ARN del tema de Amazon SNS
me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements
me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements
eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements

AWS Región	ARN del tema de Amazon SNS
ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements
ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements
il-central-1	arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements

Para suscribirse al correo electrónico de notificación de GuardDuty actualización en AWS Management Console

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En la lista de regiones, elija la misma región que la del ARN del tema al que desea suscribirse. En este ejemplo se utiliza la región `us-west-2`.
3. En el panel de navegación izquierdo, elija Subscriptions (Suscripciones), Create subscription (Crear suscripción).
4. En el cuadro de diálogo Create Subscription (Crear suscripción), en Topic ARN (ARN del tema), pegue el ARN del tema: `arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements`.
5. En Protocolo, seleccione Correo electrónico. En Endpoint (Punto de enlace), escriba una dirección de correo electrónico que pueda utilizar para recibir la notificación.
6. Seleccione Crear suscripción.
7. En tu aplicación de correo electrónico, abre el mensaje de AWS Notificaciones y abre el enlace para confirmar la suscripción.

   El navegador web muestra una respuesta de confirmación de Amazon SNS.

Para suscribirse al correo electrónico de notificación de GuardDuty actualización con el AWS CLI

1. Ejecute el siguiente comando con la AWS CLI:

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. En tu aplicación de correo electrónico, abre el mensaje de AWS Notificaciones y abre el enlace para confirmar la suscripción.

   El navegador web muestra una respuesta de confirmación de Amazon SNS.

Formato de los mensajes de Amazon SNS

A continuación se muestra un ejemplo de mensaje de notificación de GuardDuty actualización sobre nuevos hallazgos:


```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FINDINGS\",\"findingDetails
\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"findingDescription\":\"This finding informs you that an EC2 instance in your AWS
 environment is making connections to a Tor Guard or an Authority node. Tor is software
 for enabling anonymous communication. Tor Guards and Authority nodes act as initial
 gateways into a Tor network. This traffic can indicate that this EC2 instance is
 acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised.\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
```

```
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

El valor Mensaje analizado (sin las comillas de escape) se muestra a continuación:

```
{
    "version": "1",
    "type": "NEW_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "findingDescription": "This finding informs you that an EC2 instance in your
 AWS environment is making connections to a Tor Guard or an Authority node. Tor is
 software for enabling anonymous communication. Tor Guards and Authority nodes act as
 initial gateways into a Tor network. This traffic can indicate that this EC2 instance
 is acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised."
    }]
}
```

A continuación se muestra un ejemplo de mensaje de notificación de GuardDuty actualización sobre las actualizaciones de GuardDuty funcionalidad:

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FEATURES\",\"featureDetails
\":[{\"featureDescription\":\"Customers with high-volumes of global CloudTrail
 events should see a net positive impact on their GuardDuty costs.\",\"featureLink
\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_data-
sources.html#guardduty_cloudtrail\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
```

```
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

El valor Mensaje analizado (sin las comillas de escape) se muestra a continuación:

```
{
    "version": "1",
    "type": "NEW_FEATURES",
    "featureDetails": [{
        "featureDescription": "Customers with high-volumes of global CloudTrail events
 should see a net positive impact on their GuardDuty costs.",
        "featureLink": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_data-sources.html#guardduty_cloudtrail"
    }]
}
```

A continuación, se muestra un ejemplo GuardDuty de mensaje de notificación de actualización sobre los resultados actualizados:

```
{
    "Type": "Notification",
    "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message": "{\"version\":\"1\",\"type\":\"UPDATED_FINDINGS\",
\"findingDetails\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"description\":\"Increased severity value from 5 to 8.\"}]}",
    "Timestamp": "2018-03-09T00:25:43.483Z",
    "SignatureVersion": "1",
    "Signature": "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
```

```
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

El valor Mensaje analizado (sin las comillas de escape) se muestra a continuación:

```
{
    "version": "1",
    "type": "UPDATED_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "description": "Increased severity value from 5 to 8."
    }]
}
```

Cuotas para Amazon GuardDuty

La cuenta de AWS tiene cuotas predeterminadas para cada servicio de AWS (estas cuotas anteriormente se denominaban “límites”). A menos que se indique lo contrario, cada cuota es específica de la región de . Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para ver las cuotas GuardDuty, abra la consola Service Quotas. En el panel de navegación, elige AWSservicios y selecciona Amazon GuardDuty.

Para solicitar un aumento de cuota, consulte Solicitud de un aumento de cuota en la Guía de usuario de Service Quotas.

Tu AWS cuenta tiene las siguientes cuotas de Amazon GuardDuty por región.

> **Note**
>
> Para conocer las cuotas específicas de la protección contra GuardDuty malware, consulteCuotas de protección contra malware.

Recurso	Valor predeterminado	Comentarios
Detectores	1	El número máximo de recursos del detector que puede crear por cuenta de AWS por región. No puede solicitar un aumento de cuota.
Filtros	100	El número máximo de filtros guardados por cuenta de AWS por región.

Recurso	Valor predeterminado	Comentarios
		No puede solicitar un aumento de cuota.
Periodo de conservación de hallazgos	90 días	El número máximo de días que se guarda un hallazgo. No puede solicitar un aumento de cuota.
Direcciones IP y rangos de CIDR por lista de IP de confianza	2,000	Número máximo de direcciones IP y rangos de CIDR que se pueden incluir en una misma lista de IP de confianza. No puede solicitar un aumento de cuota.
Direcciones IP y rangos de CIDR por lista de amenazas	250.000	Número máximo de direcciones IP y rangos de CIDR que se pueden incluir en una lista de amenazas. No puede solicitar un aumento de cuota.

Recurso	Valor predeterminado	Comentarios
Tamaño máximo de archivo	35 MB	Tamaño máximo del archivo utilizado para cargar una lista de direcciones IP o rangos de CIDR con el fin de incluirlos en una lista de IP de confianza o en una lista de amenazas. No puede solicitar un aumento de cuota.
Cuentas de los miembros (por invitación)	5000	El número máximo de cuentas de miembro asociadas a una cuenta de administrador.
Cuentas de miembros	50 000	El número máximo de cuentas de miembro asociadas a una cuenta de administrador hasta la cuentaAWS Organizations. Esto incluye las cuentas de miembro que se agregan a la organización mediante invitación.

Recurso	Valor predeterminado	Comentarios
Conjuntos de información de amenazas	6	El número máximo de conjuntos de inteligencia de amenazas que puede agregar por cuenta de AWS por región. No puede solicitar un aumento de cuota.
Conjuntos de IP de confianza	1	El número máximo de conjuntos de IP de confianza que se pueden cargar y activar en cada cuenta de AWS por región. No puede solicitar un aumento de cuota.

Solución de problemas de Amazon GuardDuty

Cuando recibas problemas relacionados con la realización de una acción específica GuardDuty, consulta los temas de esta sección.

Temas

Cuestiones generales en GuardDuty

Se produce un error de acceso al exportar GuardDuty los resultados. ¿Cómo puedo resolver este problema?

Tras configurar los ajustes para exportar las conclusiones, si no GuardDuty es posible exportar las conclusiones, se mostrará un mensaje de error en la página de configuración de la GuardDuty consola. Esto puede ocurrir cuando ya no GuardDuty pueda acceder al recurso de destino, por ejemplo, si se eliminó su bucket de Amazon S3 o se modificó el permiso de acceso al bucket. Esto también puede ocurrir cuando ya no GuardDuty pueda acceder a la AWS KMS clave que se utilizó para cifrar los datos de su bucket de Amazon S3. Cuando GuardDuty no puede exportar, envía una notificación al correo electrónico asociado a la cuenta para proporcionar información sobre este problema.

Para resolver el problema, asegúrate de que existan los recursos correspondientes y de GuardDuty que tengas los permisos para acceder a los recursos necesarios. Si no resuelve el problema antes de que finalice el período de retención de hallazgos de 90 días GuardDuty, sus hallazgos no se exportarán. GuardDuty deshabilitará la búsqueda de la configuración de exportación para esta cuenta en la región específica. Incluso después de esta fecha de retención, puede actualizar los ajustes de configuración para volver a exportar los resultados en la región específica.

Para obtener más información, consulte Exportación de resultados.

Problemas de protección contra malware

Estoy iniciando un análisis de malware bajo demanda, pero se produce un error de falta de permisos necesarios.

Si recibe un error que indica que no tiene los permisos necesarios para iniciar un análisis de malware bajo demanda en una instancia de Amazon EC2, compruebe que ha adjuntado la política AWS política gestionada: AmazonGuardDutyFullAccess a su rol de IAM.

Si eres miembro de una AWS organización y sigues recibiendo el mismo error, conéctate con tu cuenta de administración. Para obtener más información, consulte AWS Organizations SCP: acceso denegado.

Recibo un error **`iam:GetRole`** al trabajar con Protección contra malware.

Si recibes este error`Unable to get role: AWSServiceRoleForAmazonGuardDutyMalwareProtection`, significa que te falta el permiso para activar el análisis de malware GuardDuty iniciado o para utilizar el análisis de malware bajo demanda. Compruebe que ha adjuntado la política AWS política gestionada: AmazonGuardDutyFullAccess a su rol de IAM.

Soy un GuardDuty administrador de cuentas que necesito habilitar el análisis GuardDuty de malware iniciado, pero no uso la política AWS administrada: AmazonGuardDutyFullAccess administrar. GuardDuty

- Configura la función de IAM que utilizas GuardDuty para disponer de los permisos necesarios para habilitar el análisis de malware GuardDuty iniciado por iniciación. Para obtener más información sobre los permisos necesarios, consulte Creating a service-linked role for Malware Protection.
- Adjunte AWS política gestionada: AmazonGuardDutyFullAccess al rol de IAM. Esto te ayudará a habilitar la detección de malware GuardDuty iniciada por primera vez en las cuentas de los miembros.

Problemas de monitoreo del tiempo de ejecución

Mi AWS Step Functions flujo de trabajo está fallando inesperadamente

Si el GuardDuty contenedor contribuyó al error del flujo de trabajo, consulteSolución de problemas de cobertura. Si el problema persiste, para evitar que el flujo de trabajo falle a causa del GuardDuty contenedor, lleve a cabo uno de los siguientes pasos:

- Añada la `false` etiqueta`GuardDutyManaged`: al clúster de Amazon ECS asociado.
- Deshabilite la configuración automática del agente AWS Fargate (solo para ECS) a nivel de cuenta. Añada la etiqueta de inclusión`GuardDutyManaged`: `true` al clúster de Amazon ECS asociado que desee seguir supervisando con el agente GuardDuty automatizado.

Solución de problemas de memoria insuficiente en Runtime Monitoring (solo compatible con Amazon EC2)

En esta sección, se proporcionan los pasos para solucionar problemas cuando se produce un error de memoria insuficiente debido Límite de CPU y memoria a la implementación manual del agente de GuardDuty seguridad.

Si `systemd` cancela el GuardDuty agente debido a `out-of-memory` un problema y considera que es razonable proporcionarle más memoria, puede actualizar el límite. GuardDuty

1. Con el permiso de root, abra`/lib/systemd/system/amazon-guardduty-agent.service`.
2. Busque `MemoryLimit` `MemoryMax` y actualice ambos valores.

```
MemoryLimit=256MB
MemoryMax=256MB
```

3. Tras actualizar los valores, reinicie el GuardDuty agente mediante el siguiente comando:

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. Ejecute el siguiente comando para ver el estado:

```
sudo systemctl status amazon-guardduty-agent
```

El resultado esperado mostrará el nuevo límite de memoria:

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

Problemas relacionados con la gestión de varias cuentas

Quiero administrar varias cuentas, pero no tengo el permiso AWS Organizations de administración necesario.

Si recibes este error`The request failed because you do not have required AWS Organization master permission.`, significa que te falta el permiso para activar el análisis GuardDuty de malware iniciado en varias cuentas de tu organización. Para obtener más información sobre cómo conceder permisos a la cuenta de administración, consulte[Establecer un acceso confiable para permitir la detección GuardDuty de malware iniciada](#).

Otras cuestiones de solución de problemas

Si no encuentra un escenario adecuado para su problema, consulte las siguientes opciones de solución de problemas:

- Para obtener información sobre problemas generales de IAM al acceder a https://console.aws.amazon.com/guardduty/, consulte Solución de problemas de GuardDuty identidad y acceso a Amazon.
- Para obtener información sobre problemas de autenticación y autorización al acceder AWS AWS Console Home, consulte Solución de problemas de IAM.

Regiones y puntos de conexión

Para ver Regiones de AWS dónde GuardDuty está disponible Amazon, consulta los GuardDuty puntos de enlace de Amazon en. Referencia general de Amazon Web Services

Le recomendamos que habilite todas GuardDuty las opciones compatibles Regiones de AWS. Esto permite GuardDuty generar información sobre actividades no autorizadas o inusuales, incluso en las regiones que no utiliza activamente. Esto también permite GuardDuty monitorear AWS CloudTrail los eventos para las personas con soporte Regiones de AWS, y reduce su capacidad para detectar actividades que involucren servicios globales.

Disponibilidad de características específicas por región

Una lista de las diferencias regionales para especificar la disponibilidad de las GuardDuty funciones.

ListFindings y GetFindingsStatistics API

ListFindingsLas API GetFindingsStatisticsy tienen un `consoleOnly` indicador temporal. Cuando utilizas una de estas API o ambas, el `consoleOnly` indicador significa que la API puede obtener resultados hasta un límite máximo de 1000.

GuardDuty características con disparidad regional

GuardDuty Protección contra malware

GuardDuty admite la función de protección contra malware en las Zonas Locales AWS Dedicadas.

GuardDuty Supervisión del tiempo de ejecución

La función de supervisión del tiempo de ejecución no está disponible actualmente en la región Canadá Oeste (Calgary).

GuardDuty Protección RDS

La siguiente lista especifica los Regiones de AWS lugares en los que actualmente no se admite la protección RDS:

- Oeste de Canadá (Calgary)
- Asia-Pacífico (Hyderabad)
- Europa (España)
- Europa (Zúrich)

- Medio Oriente (EAU)
- Israel (Tel Aviv)
- Asia-Pacífico (Melbourne)

Las siguientes API de la Amazon GuardDuty API Reference pueden tener diferencias regionales debido a la falta de disponibilidad de algunas de las fuentes de datos o características especificadas Regiones de AWS anteriormente:

- CreateDetector
- UpdateDetector
- UpdateMemberDetectors
- UpdateOrganizationConfiguration
- GetDetector
- GetMemberDetectors
- DescribeOrganizationConfiguration

Tipos de resultados de Amazon EC2: DefenseEvasion:EC2/UnusualDoHActivity y DefenseEvasion:EC2/UnusualDoTActivity

En la siguiente tabla se muestra Regiones de AWS dónde GuardDuty está disponible, pero estos dos tipos de búsqueda de Amazon EC2 aún no son compatibles.

Región de AWS	Código de región
Asia Pacífico (Seúl)	ap-northeast-2
Asia-Pacífico (Osaka)	ap-northeast-3
Asia-Pacífico (Yakarta)	ap-southeast-3

AWS GovCloud (US) Regiones

Para obtener la información más reciente, consulta Amazon GuardDuty en la Guía AWS GovCloud (US) del usuario.

Regiones de China

Para obtener información más actualizada, consulte Feature availability and implementation differences.

GuardDuty acciones y parámetros heredados

Amazon GuardDuty ha dejado en desuso algunas de las acciones y parámetros de la API, pero aún los admite. La práctica recomendada consiste en utilizar las acciones y los parámetros nuevos de la API que sustituyen a las opciones heredadas. En la tabla siguiente se comparan las acciones y los parámetros heredados y los nuevos.

Acciones y parámetros heredados	Acciones y parámetros nuevos	Comparación
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	Con la misma implementación en ambas acciones, GuardDuty usa el término `Administrator` in`DisassociateFromAdministratorAccount` .
`autoEnable` parámetro en DescribeOrganizationConfigurationy UpdateOrganizationConfiguration	`autoEnableOrganizationMembers`	Con `autoEnableOrganizationMembers` él, la cuenta de GuardDuty administrador puede auditar y aplicar cualquiera de los valores GuardDuty para todas las cuentas de los miembros. Con las API, la actualización de la configuración de todas las cuentas de miembros puede tardar hasta 24 horas en efectuarse. Para obtener más información sobre los posibles valores del `autoEnableOrganizationMembers` campo, consulte autoEnableOrganizationMiembros
Parámetro `dataSources` en las API que figuran	`features`	A partir de marzo de 2023, podrá configurar Protección contra malware en Amazon GuardDuty y utilizar los nuevos planes de GuardDuty protección`features`. Los planes

Acciones y parámetros heredados	Acciones y parámetros nuevos	Comparación
en GuardDuty Cambios en la API en marzo de 2023.		de protección lanzados antes de marzo de 2023, tales como Protección contra malware, siguen admitiendo la configuración con `dataSources` . Si utiliza las API para configurar un plan de protección, cada solicitud a la API puede incluir `dataSources` o `features`, pero no ambas opciones.

Historial de documentos de Amazon GuardDuty

En la siguiente tabla se describen los cambios importantes en la documentación desde la última versión de la Guía del GuardDuty usuario de Amazon. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Se ha actualizado la experiencia de la consola para configurar los resultados de exportación	GuardDuty ha actualizado la experiencia de la consola para exportar las conclusiones generadas en su Cuentas de AWS cuenta a un bucket de Amazon S3. Para obtener más información, consulte Exportación de GuardDuty los resultados.	1 de abril de 2024
Funcionalidad actualizada en Runtime Monitoring	Runtime Monitoring publicó una nueva versión 1.1.0 del agente de seguridad para el recurso Amazon EC2. Esta versión admite la configuración GuardDuty automática de agentes en Runtime Monitoring para instancias de Amazon EC2. Para obtener información sobre las notas de la versión, consulte el agente GuardDuty de seguridad para la instancia Amazon EC2.	28 de marzo de 2024
Disponibilidad general de Runtime Monitoring para instancias de Amazon EC2	GuardDuty anuncia la disponibilidad general (GA) de Runtime Monitoring para instancias de Amazon EC2. Ahora, tiene la opción de	28 de marzo de 2024

habilitar la configuración automática del agente que le permite GuardDuty instalar y administrar el agente de seguridad para sus instancias de Amazon EC2 en su nombre. Con el agente GuardDuty automatizado, también puede usar etiquetas de inclusión o exclusión como información GuardDuty para instalar y administrar el agente de seguridad solo en instancias seleccionadas de Amazon EC2. Para obtener más información, consulte Cómo funciona Runtime Monitoring con las instancias de Amazon EC2.

Lista de nuevos tipos de hallazgos publicados junto con esta GA

- Ejecución: Tiempo de ejecución/ SuspiciousTool
- Ejecución: Tiempo de ejecución/SuspiciousCommand
- DefenseEvasionEjecución: Runtime/ ----SEP----:Runtime/ SuspiciousCommand
- DefenseEvasion:Runtime/ ----SEP----:Runtime/ PtraceAntiDebugging

- Ejecución: Tiempo de ejecución/ Malicious FileExecuted

Amazon GuardDuty ha actualizado el rol vinculado a servicios (SLR)	Utilice AWS Systems Manager acciones para gestionar las asociaciones de SSM en las instancias de Amazon EC2 al GuardDuty habilitar Runtime Monitoring con un agente automatizado para Amazon EC2. Cuando la configuración GuardDuty automática de agentes está deshabilitada, solo GuardDuty tiene en cuenta las instancias de EC2 que tienen una etiqueta de inclusión (:). `GuardDutyManaged true` • La siguiente lista muestra los nuevos permisos: `"ssm:DescribeAssociation", "ssm:DeleteAssociation", "ssm:UpdateAssociation", "ssm:CreateAssociation", "ssm:StartAssociationsOnce", "ssm:AddTagsToResource", "ssm:CreateAssociation", "ssm:UpdateAssociation", "ssm:SendCommand", "ssm:GetCommandInvocation"`	26 de marzo de 2024

Funcionalidad actualizada en Runtime Monitoring	Con la última versión del agente de GuardDuty seguridad (complemento) v1.5.0 para Amazon EKS, Runtime Monitoring ahora admite la configuración de parámetros específicos del agente de GuardDuty seguridad, como la configuración de la CPU y la memoria, la configuración y la `PriorityClass` configuración de la política de DNS. Para obtener más información, consulte Configuración de los parámetros del agente GuardDuty de seguridad (complemento EKS).	7 de marzo de 2024
Funcionalidad actualizada en Runtime Monitoring	Runtime Monitoring publicó una nueva versión 1.5.0 del agente para los recursos de Amazon EKS. Para obtener información sobre las notas de la versión, consulte el historial de versiones del agente complementario de EKS.	7 de marzo de 2024

Support for Canada West (Calgary)	Amazon ya GuardDuty está disponible en la región Canadá Oeste (Calgary) . GuardDuty Es posible que algunos de los planes de protección incluidos no estén disponibles en esta región. Para obtener la información más reciente, consulte Regiones y puntos de conexión.	6 de marzo de 2024
Funcionalidad actualizada en Runtime Monitoring	Las versiones 1.0.0 y 1.1.0 del agente de GuardDuty seguridad para los clústeres de Amazon EKS dejarán de ser compatibles a partir del 14 de mayo de 2024. Para obtener información sobre los pasos que puede tomar antes de que finalice el soporte estándar, consulte el agente de GuardDuty seguridad para los clústeres de Amazon EKS.	16 de febrero de 2024

Funcionalidad actualizada en Runtime Monitoring	Runtime Monitoring es compatible con la última versión 1.29 de Kubernetes con la versión 1.4.1 del agente de seguridad existente. El soporte está disponible desde el lanzamiento de esta versión de Kubernetes. Para obtener información sobre las versiones de Kubernetes compatibles, consulta las versiones de Kubernetes compatibles con el agente de seguridad. GuardDuty	16 de febrero de 2024

Funcionalidad actualizada en Runtime Monitoring: disponibilidad regional	GuardDuty La monitorización del tiempo de ejecución ahora admite Amazon VPC compartida dentro de la misma. AWS Organizations GuardDuty El rol vinculado a un servicio (SLR) tiene un nuevo permiso `organizations:DescribeOrganization` que ayuda a recuperar el ID de la organización de la cuenta de Amazon VPC compartida para establecer la política de puntos finales. Para obtener información sobre los requisitos previos para usar un punto de enlace de Amazon VPC compartido en Runtime Monitoring, consulte Support for shared Amazon VPC. Esta capacidad está disponible en todas las regiones en las que se GuardDuty admite la monitorización del tiempo de ejecución.	12 de febrero de 2024

Funcionalidad actualizada en la supervisión del tiempo de ejecución: disponibilidad regional	GuardDuty La monitorización del tiempo de ejecución ahora admite Amazon VPC compartida dentro de la misma. AWS Organizations GuardDuty El rol vinculado a un servicio (SLR) tiene un nuevo permiso `organizations:DescribeOrganization` que ayuda a recuperar el ID de la organización de la cuenta de Amazon VPC compartida para establecer la política de puntos finales. Para obtener información sobre los requisitos previos para usar un punto de enlace de Amazon VPC compartido en Runtime Monitoring, consulte Support for shared Amazon VPC. Actualmente, esta capacidad está disponible en algunas de las. Regiones de AWS Para obtener más información, consulte Puntos de conexión y Regiones de .	9 de febrero de 2024
Funcionalidad actualizada con soporte para la nueva Regiones de AWS : protección contra malware	La protección contra malware ahora permite escanear los volúmenes de EBS cifrados Claves administradas por AWS en la región EE.UU. Oeste (Oregón).	6 de febrero de 2024

Funcionalidad actualizada con soporte para la nueva Regiones de AWS : protección contra malware	La protección contra malware ahora permite escanear los volúmenes de EBS Claves administradas por AWS cifrados con lo siguiente: Regiones de AWS • Asia-Pacífico (Singapur) (`ap-southeast-1`) • Europa (Fráncfort) (`eu-central-1`) • Asia-Pacífico (Osaka) (`ap-northeast-3`) • Este de EE. UU. (Ohio) (`us-east-2`) • Europa (Milán) (`eu-south-1`) • Asia-Pacífico (Tokio) (`ap-northeast-1`) • Asia-Pacífico (Seúl) (`ap-northeast-2`) • Canadá (centro) (`ca-central-1`) • Europa (Irlanda) (`eu-west-1`) • Este de EE. UU. (Norte de Virginia) (`us-east-1`)	5 de febrero de 2024

Funcionalidad actualizada en Runtime Monitoring	GuardDuty Runtime Monitoring ha publicado una nueva versión del agente de GuardDuty seguridad (v1.0.2) para las instancias de Amazon EC2. Esta versión del agente incluye soporte para las AMI más recientes de Amazon ECS. Para obtener más información sobre el historial de versiones de los agentes, consulte el agente de GuardDuty seguridad para instancias de Amazon EC2.	2 de febrero de 2024

Funcionalidad actualizada con soporte para la nueva versión Regiones de AWS : Malware Protection	Malware Protection ahora admite el escaneo de los volúmenes de Amazon EBS Claves administradas por AWS cifrados con lo siguiente: Regiones de AWS • Europa (Londres) (`eu-west-2`) • Europa (Estocolmo) (`eu-north-1`) • Asia Pacífico (Hong Kong) (`ap-east-1`) • África (Ciudad del Cabo) (`af-south-1`) • Medio Oriente (Baréin) (`me-south-1`) • Asia-Pacífico (Hyderabad) (`ap-south-2`) • Europa (España) (`eu-south-2`) • Asia-Pacífico (Melbourne) (`ap-southeast-4`) • Asia-Pacífico (Sídney) (`ap-southeast-2`) • Israel (Tel Aviv) (`il-central-1`)	31 de enero de 2024

Se actualizó la administración de cuentas con AWS Organizations	Se reorganizó el contenido en Administrar cuentas con AWS Organizations. , agregó pasos para cambiar la cuenta de GuardDuty administrador delegado y actualizó Entendiendo la relación entre la cuenta de GuardDuty administrador y las cuentas de los miembros.	30 de enero de 2024
Funcionalidad actualizada con soporte para nuevas Regiones de AWS	La protección contra malware ahora permite escanear los volúmenes de EBS Claves administradas por AWS cifrados con lo siguiente: Regiones de AWS • Asia-Pacífico (Yakarta) (`ap-southeast-3`) • Oeste de EE. UU. (Norte de California) (`us-west-1`) • Medio Oriente (EAU) (`me-central-1`) • Europa (Zúrich) (`eu-central-2`) • Asia-Pacífico (Bombay) (`ap-south-1`) • América del Sur (São Paulo) (`sa-east-1`)	29 de enero de 2024

Funcionalidad actualizada en Malware Protection	La protección contra malware ahora permite escanear los volúmenes de EBS cifrados mediante Claves administr adas por AWS. La función vinculada al servicio (SLR) de Malware Protection tiene dos nuevos permisos: y. `GetSnapshotBlock` `ListSnapshotBlocks` Estos permisos le permitirá n GuardDuty recuperar la instantánea de un volumen de EBS (cifrado mediante Clave administrada de AWS) Cuenta de AWS y copiarla a la cuenta de GuardDuty servicio antes de iniciar el análisis de software malicioso. Actualmen te, esta funcionalidad solo está disponible en Europa (París) (`eu-west-3`). Para obtener más información, consulte Volúmenes compatibles con el análisis de software malicioso.	25 de enero de 2024

Funcionalidad actualizada en Runtime Monitoring	GuardDuty Runtime Monitoring ha publicado una nueva versión del agente de GuardDuty seguridad (v1.0.1) con mejoras y ajustes generales del rendimiento. Para obtener más información sobre el historial de versiones de los agentes, consulte el agente de GuardDuty seguridad para instancias de Amazon EC2.	23 de enero de 2024
Funcionalidad actualizada en Runtime Monitoring	Runtime Monitoring publicó una nueva versión 1.4.1 del agente para los recursos de Amazon EKS. Para más información, consulte EKS add-on agent release history.	16 de enero de 2024
Runtime Monitoring lanzó el nuevo agente v1.4.0 para los recursos de Amazon EKS	Runtime Monitoring publicó una nueva versión 1.4.0 del agente para los recursos de Amazon EKS. Para más información, consulte EKS add-on agent release history.	21 de diciembre de 2023

Se agregaron tipos de hallazgos basados en el S3 y en el aprendizaje AWS CloudTrail automático (ML) a Europa (Zúrich), Europa (España), Asia Pacífico (Hyderabad), Asia Pacífico (Melbourne) e Israel (Tel Aviv)	El siguiente S3 y CloudTrail los hallazgos que identifican el comportamiento anómalo mediante el modelo GuardDuty de aprendizaje automático (ML) de detección de anomalías ya están disponibles en las regiones de Europa (Zúrich), Europa (España), Asia Pacífico (Hyderabad), Asia Pacífico (Melbourne) e Israel (Tel Aviv): • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior	21 de diciembre de 2023

	• Persistence:IAMUser/AnomalousBehavior • PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty admite 50 000 cuentas de miembros a través de AWS Organizations	Un GuardDuty administrador delegado ahora puede gestionar un máximo de 50 000 cuentas de miembros mediante AWS Organizations. Esto también incluye un máximo de 5000 cuentas de miembros asociadas a la cuenta de GuardDuty administrador mediante invitación.	20 de diciembre de 2023

GuardDuty El soporte de monitorización del tiempo de ejecución se amplió a 19 Regiones de AWS	Runtime Monitoring ya está disponible en Asia Pacífico (Yakarta), Europa (París), Asia Pacífico (Osaka), Asia Pacífico (Seúl), Oriente Medio (Bahréin), Europa (España), Asia Pacífico (Hyderabad), Asia Pacífico (Melbourne), Israel (Tel Aviv), EE.UU. Oeste (Norte de California), Europa (Londres) , Asia Pacífico (Hong Kong), Europa (Milán), Oriente Medio (Emiratos Árabes Unidos), Sudamérica (São Paulo)), Asia Pacífico (Bombay), Canadá (Central), África (Ciudad del Cabo), Europa (Zúrich).	6 de diciembre de 2023
GuardDuty amplía la capacidad de monitorización del tiempo de ejecución	Además de detectar amenazas en sus clústeres de Amazon EKS, GuardDuty anuncia la disponibilidad general de Runtime Monitorin g para detectar amenazas en sus cargas de trabajo de Amazon ECS y una versión preliminar para detectar amenazas en sus instancias de Amazon EC2. Para obtener más información sobre los dispositivos compatibles Regiones de AWS actua lmente con Runtime Monitorin g, consulte Regiones y puntos de conexión.	26 de noviembre de 2023

Amazon GuardDuty ha actualizado el rol vinculado a servicios (SLR)	GuardDuty ha añadido nuevos permisos para utilizar las acciones de Amazon ECS a fin de gestionar y recuperar información sobre los clústeres de Amazon ECS y gestionar la configuración de la cuenta de Amazon ECS con `guarddutyActivate` . Las acciones relacionadas con Amazon ECS también recuperan la información sobre las etiquetas asociadas GuardDuty. • Se han agregado los siguientes permisos como parte de la GuardDuty expansión de la capacidad de monitoreo del tiempo de ejecución: `"ecs:ListClusters", "ecs:DescribeClusters", "ecs:PutAccountSettingDefault"`	26 de noviembre de 2023
Se actualizaron las políticas AWS administradas	GuardDuty agregó un nuevo permiso, `organizations:ListAccounts` a AmazonGuardDutyFullAccessPolicy y AmazonGuardDutyReadOnlyAccess.	16 de noviembre de 2023

GuardDuty publicó nuevos tipos de búsqueda que utilizan EKS Audit Log Monitoring.	EKS Audit Log Monitoring ahora admite los siguientes tipos de búsquedas en Asia Pacífico (Melbourne) (`ap-southeast-4`). • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	11 de noviembre de 2023

GuardDuty publicó nuevos tipos de hallazgos que utilizan EKS Audit Log Monitoring.	EKS Audit Log Monitoring ahora admite los siguiente s tipos de búsquedas en las regiones de Asia Pacífico (Hyderabad`ap-south-2`) (), Europa (Zúrich`eu-centra l-2`) () y Europa (España) (`eu-south-2`). • CredentialAccess:K ubernetes/Anomalou sBehavior.SecretsAccessed • PrivilegeEscalation:Kuberne tes/AnomalousBehav ior.RoleBindingCreated • Execution:Kubernetes/ AnomalousBehavior.ExecIn Pod • PrivilegeEscalation:Kuberne tes/AnomalousBehav ior.WorkloadDeployed!Privil egedContainer • PrivilegeEscalation:Kuberne tes/AnomalousBehav ior.WorkloadDeployed! ContainerWithSensitiveMo unt • Execution:Kubernetes/ AnomalousBehavior.Worklo adDeployed • PrivilegeEscalation:Kuberne tes/AnomalousBehav ior.RoleCreated	10 de noviembre de 2023

- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

GuardDuty publicó nuevos tipos de hallazgos que utilizan EKS Audit Log Monitoring.	El monitoreo de registros de auditoría de EKS ahora admite los siguientes tipos de búsqueda. Estos tipos de búsqueda aún no están disponibles en las regiones de Asia Pacífico (Hyderaba `dap-south-2`) (), Europa (Zúrich`eu-central-2`) (), Europa (España) (`eu-south-2`) y Asia Pacífico (Melbourn e) (`ap-southeast-4`). • CredentialAccess:K ubernetes/Anomalou sBehavior.SecretsAccessed • PrivilegeEscalation:Kuberne tes/AnomalousBehav ior.RoleBindingCreated • Execution:Kubernetes/ AnomalousBehavior.ExecIn Pod • PrivilegeEscalation:Kuberne tes/AnomalousBehav ior.WorkloadDeployed!Privil egedContainer • PrivilegeEscalation:Kuberne tes/AnomalousBehav ior.WorkloadDeployed! ContainerWithSensitiveMo unt • Execution:Kubernetes/ AnomalousBehavior.Worklo adDeployed	8 de noviembre de 2023

	• PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	
La supervisión en tiempo de ejecución de EKS ha lanzado el nuevo agente v1.3.1	EKS Runtime Monitoring ha publicado una nueva versión del agente, la 1.3.1, que incluye importantes parches y actualizaciones de seguridad.	23 de octubre de 2023
Nuevo atributo de filtro para resultados	GuardDuty ha agregado un nuevo criterio para filtrar los hallazgos generados. El sufijo del dominio de solicitud de DNS proporciona el dominio de segundo y nivel superior implicado en la actividad que provocó GuardDuty la generación del hallazgo.	17 de octubre de 2023
La supervisión en tiempo de ejecución de EKS ha lanzado un nuevo agente de la versión 1.3.0 compatible con la versión 1.28 de Kubernetes	EKS Runtime Monitoring lanzó una nueva versión del agente 1.3.0 que es compatible con la versión 1.28 de Kubernetes. Se ha agregado compatibilidad con Ubuntu. Para más información, consulte EKS add-on agent release history.	5 de octubre de 2023

Se agregaron tipos de hallazgos basados en el S3 y en el aprendizaje AWS CloudTrail automático (ML) a las regiones de Asia Pacífico (Yakarta) y Medio Oriente (Emiratos Árabes Unidos)	El siguiente S3 y CloudTrail los hallazgos que identifican el comportamiento anómalo mediante el modelo GuardDuty de aprendizaje automático (ML) de detección de anomalías ya están disponibles en las regiones de Asia Pacífico (Yakarta) y Oriente Medio (Emiratos Árabes Unidos): • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior	20 de septiembre de 2023

	• PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty EKS Runtime Monitoring introduce la administración de los agentes GuardDuty de seguridad a nivel de clúster	EKS Runtime Monitoring añade soporte para administrar el agente de GuardDuty seguridad de los clústeres de EKS individuales a fin de monitorear los eventos de tiempo de ejecución solo desde estos clústeres selectivos. La supervisión en tiempo de ejecución de EKS amplía esta capacidad con la compatibilidad con etiquetas.	13 de septiembre de 2023
GuardDuty Malware Protection amplía el soporte a más Regiones de AWS	La protección contra malware ya está disponible en las regiones Asia-Pacífico (Hyderabad), Asia-Pacífico (Melbourne), Europa (Zúrich) y Europa (España).	11 de septiembre de 2023

GuardDuty ya está disponible en la región de Israel (Tel Aviv)	Se agregó la región de Israel (Tel Aviv) a la lista de Regiones de AWS lugares donde ahora GuardDuty está disponible. Los siguientes planes de protección ya están disponibles en la región Israel (Tel Aviv): • GuardDuty Protección EKS incluye la supervisión de registros de auditoría de EKS y la supervisión en tiempo de ejecución de EKS. • GuardDuty Protección Lambda. • GuardDuty Protección contra malware. • GuardDuty Protección S3. Para obtener más información sobre la disponibilidad de planes de protección en la región Israel (Tel Aviv), consulte Regiones y puntos de conexión.	24 de agosto de 2023

GuardDuty se agregó una configuración de activación automática para su organización a nivel de plan de protección	Actualice la configuración organizativa de los planes de protección de su región. Las posibles opciones de configuración son activar para todas las cuentas, habilitar automáticamente para las cuentas nuevas o no habilitar automáticamente para ninguna cuenta de su organización.	16 de agosto de 2023
Los tipos de detección S3 que identifican el comportamiento anómalo mediante GuardDuty el modelo de aprendizaje automático (ML) con detección de anomalías ya están disponibles en Asia Pacífico (Osaka)	Los siguientes tipos de resultados ya están disponibles en la región Asia-Pacífico (Osaka): • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	10 de agosto de 2023

La supervisión en tiempo de ejecución de EKS ya está disponible en la región Asia-Pacífico (Melbourne)	El monitoreo de tiempo de ejecución de GuardDuty EKS dentro de EKS Protection proporciona detección de amenazas en tiempo de ejecución para los clústeres de Amazon EKS en AWS el entorno. Ya es compatible con la región Asia-Pacífico (Melbourne).	8 de agosto de 2023
Se actualizó la lista de GuardDuty hallazgos que invocan el análisis GuardDuty de malware iniciado	Algunos tipos de búsqueda de EKS Runtime Monitorin g ahora pueden invocar un análisis GuardDuty de malware iniciado en su. Cuenta de AWS	19 de julio de 2023
GuardDuty admite 10 000 cuentas de miembros a través de AWS Organizations	Una cuenta de GuardDuty administrador ahora puede gestionar un máximo de 10 000 cuentas de miembros mediante AWS Organizat ions. Esto también incluye un máximo de 5000 cuentas de miembros asociadas a la cuenta de GuardDuty administrador mediante invitación.	29 de junio de 2023

La supervisión en tiempo de ejecución de EKS anuncia tres nuevos tipos de resultados.	La supervisión en tiempo de ejecución de EKS admite tres nuevos tipos de resultados que se basan en la técnica de inyección de procesos. Los nuevos tipos de búsqueda son: Runtime/ DefenseEv asion .Proc, :Runtime/ .Ptrace y:Runtime/. ProcessInjection DefenseEvasion ProcessIn jection DefenseEvasion ProcessInjection VirtualMe moryWrite.	22 de junio de 2023
La supervisión en tiempo de ejecución de EKS ha lanzado un nuevo agente de la versión 1.2.0 compatible con la versión 1.27 de Kubernetes	EKS Runtime Monitoring lanzó una nueva versión del agente 1.2.0 que también es compatible con instancia s basadas en ARM64. Se ha agregado compatibilidad con Bottlerocket. Para más información, consulte EKS add-on agent release history.	16 de junio de 2023
GuardDuty La consola proporciona una vista resumida de sus hallazgos.	El panel de resumen de la GuardDuty consola proporcio na una vista agregada de los GuardDuty hallazgos. En la actualidad, el panel muestra los datos a través de varios widgets de las últimas 10 000 conclusiones generadas para tu cuenta (o cuentas de miembros si eres GuardDuty administrador) de la región actual.	12 de junio de 2023

La supervisión de registros de auditoría de EKS ya está disponible en las regiones Asia-Pacífico (Hyderabad), Asia-Pacífico (Melbourne), Europa (Zúrich) y Europa (España)	Habilite la supervisión de registros de auditoría de EKS (en la protección de EKS) en sus cuentas para supervisar los registros de auditoría de Kubernetes de sus clústeres de Amazon EKS y analizarl os para detectar posibles actividades maliciosas o sospechosas.	1 de junio de 2023
La supervisión de registros de auditoría de EKS ya está disponible en Medio Oriente (EAU)	El monitoreo de registros de auditoría de EKS ya está disponible en Oriente Medio (Emiratos Árabes Unidos). Habilite la supervisión de registros de auditoría de EKS en sus cuentas para supervisa r los registros de auditoría de Kubernetes de sus clústeres de Amazon EKS y analizarl os para detectar posibles actividades maliciosas o sospechosas.	3 de mayo de 2023

GuardDuty Malware Protection anuncia un análisis de malware bajo demanda	La protección contra malware le ayuda a detectar la posible presencia de malware en los volúmenes de Amazon EBS asociados a sus instancias y cargas de trabajo de contenedores de Amazon EC2. Ahora ofrece dos tipos de escaneos: GuardDuty iniciados y bajo demanda. GuardDuty-el análisis de malware iniciado inicia automáticamente un análisis sin agente en los volúmenes de Amazon EBS solo cuando GuardDuty genera uno de los hallazgos que invoca el análisis de malware iniciado. GuardDuty Para iniciar un análisis de malware bajo demanda para instancias de Amazon EC2 en su cuenta, puede proporcionar el nombre de recurso de Amazon (ARN) asociado a esa instancia de Amazon EC2. Para obtener más información sobre las diferencias entre ambos tipos de análisis, consulte Protección contra malware. • GuardDuty-análisis de malware iniciado • Análisis de malware bajo demanda	27 de abril de 2023

GuardDuty anuncia Lambda Protection	La protección de Lambda le ayuda a identificar posibles amenazas de seguridad en sus funciones de AWS Lambda . • Tipos de búsqueda de Lambda Protection • Corregir una función Lambda potencialmente comprometida	20 de abril de 2023
GuardDuty ya está disponible en la región de Asia Pacífico (Melbourne)	Se agregó Asia Pacífico (Melbourne) a la lista de Regiones de AWS lugares donde GuardDuty está disponible. Para obtener información sobre las caracterí sticas disponibles en esta región, consulte Regiones y puntos de conexión.	19 de abril de 2023

GuardDuty se agregaron 3 nuevos tipos de hallazgos de EC2	GuardDuty presenta nuevos tipos de hallazgos para detectar el uso de soluciona dores de DNS externos y tecnologías de DNS cifrado. Para obtener información sobre los Regiones de AWS lugares en los que se admiten estos tipos de búsqueda, consulte Regiones y puntos finales. • DefenseEvasion:EC2/ UnusualDNSResolver • DefenseEvasion:EC2/ UnusualDoHActivity • DefenseEvasion:EC2/ UnusualDoTActivity	5 de abril de 2023

GuardDuty anuncia la monitorización del tiempo de ejecución de EKS en EKS Protection	El monitoreo de tiempo de ejecución de EKS dentro de EKS Protection proporcio na detección de amenazas en tiempo de ejecución para los clústeres de Amazon EKS en AWS el entorno. Utiliza un agente complemen tario (`aws-guardduty-agent`) de Amazon EKS que recopila los eventos de tiempo de ejecución de sus cargas de trabajo de EKS. Tras GuardDuty recibir estos eventos de tiempo de ejecución, los supervisa y analiza para identific ar posibles amenazas de seguridad sospechosas. Para más información, consulte Detalles de los resultados y Tipos de resultados de la Supervisión en tiempo de ejecución de EKS.	30 de marzo de 2023

GuardDuty añade una nueva funcionalidad: `autoEnableOrganizationMembers`	Amazon GuardDuty añade una nueva opción de configuración de la organización que ayuda a los GuardDuty administradores a auditar y hacer cumplir (si GuardDuty es necesario) lo que está habilitado para `ALL` los miembros de su organización. La práctica recomendada ahora es utilizar `autoEnableOrganizationMembers` en lugar de `autoEnable`. `autoEnable` está en desuso, pero sigue siendo compatible. Esta nueva funcionalidad afecta a las siguientes API: • DescribeOrganizationConfiguration • UpdateOrganizationConfiguration • DisassociateMembers • DeleteMembers • DisassociateFromAdministratorAccount • StopMonitoringMembers	23 de marzo de 2023

La función de protección RDS de Amazon ya GuardDuty está disponible de forma general.	GuardDuty RDS Protection supervisa y perfila la actividad de inicio de sesión de RDS para identificar comportamientos de inicio de sesión sospechosos en las instancias de la base de datos de Amazon Aurora. Para más información sobre las Regiones de AWS que admiten la protección de RDS, consulte Regiones y puntos de conexión.	16 de marzo de 2023
GuardDuty anuncia la activación de funciones	Anteriormente, la GuardDuty API permitía configurar tanto las funciones como las fuentes de datos, pero ahora todos los nuevos tipos de GuardDuty protección se configurarán como funciones y no como fuentes de datos. GuardDuty seguirá admitiendo las fuentes de datos a través de la API, pero no añadirá una nueva API. La activación de las funciones afecta al comportamiento de las API utilizadas para habilitarlas GuardDuty o al tipo de protección que contienen GuardDuty. Si administras tus GuardDuty cuentas mediante una plantilla de API, SDK o CFN, consulta los cambios en la GuardDuty API en marzo de 2023.	16 de marzo de 2023

GuardDuty La protección contra el malware ya está disponible en la región de Oriente Medio (EAU)	La función de protección contra malware GuardDuty es compatible con la región de Oriente Medio (EAU). Para obtener más información, consulte Puntos de conexión y Regiones de .	13 de marzo de 2023
Amazon GuardDuty ha actualizado el rol vinculado a servicios (SLR)	GuardDuty agregó los siguientes permisos nuevos para admitir la próxima función de monitoreo del tiempo de ejecución de GuardDuty EKS. • Utilice las acciones de Amazon EKS para administrar y recuperar información sobre los clústeres de EKS y administrar los complementos de EKS en los clústeres de EKS. Las acciones de EKS también recuperan la información sobre las etiquetas asociadas a ellas GuardDuty. `"eks:ListClusters", "eks:DescribeCluster", "ec2:DescribeVpcEndpointServices", "ec2:DescribeSecurityGroups"`	8 de marzo de 2023

Amazon GuardDuty ha actualizado el rol vinculado a servicios (SLR)	La GuardDuty SLR se ha actualizado para permitir la creación de una SLR de protección contra malware después de activar la protección contra malware.	21 de febrero de 2023
GuardDuty requiere TLS v1.2 o posterior	Para comunicarse con AWS los recursos, GuardDuty requiere y es compatible con TLS v1.2 o una versión posterior. Para más informaci ón, consulte Protección de los datos y Seguridad de la infraestructura.	14 de febrero de 2023
GuardDuty ya está disponible en la región de Asia Pacífico (Hyderabad)	Se agregó la región Asia-Pacífico (Hyderabad) a la lista de Regiones de AWS lugares donde está disponible. GuardDuty Para obtener más información, consulte Puntos de conexión y Regiones de .	14 de febrero de 2023
La guía GuardDuty del usuario de Amazon está alineada con las mejores prácticas de IAM	Se ha actualizado la guía para implementar las prácticas recomendadas de IAM. Para obtener más información, consulte prácticas recomenda das de seguridad en IAM.	10 de febrero de 2023
GuardDuty ya está disponibl e en la región de Europa (España)	Se agregó Europa (España) a la lista de Regiones de AWS lugares donde GuardDuty está disponible. Para obtener más información, consulte Puntos de conexión y Regiones de .	8 de febrero de 2023

GuardDuty ya está disponible en la región de Europa (Zúrich)	Se agregó Europa (Zúrich) a la lista de Regiones de AWS lugares donde GuardDuty está disponible. Para obtener más información, consulte Puntos de conexión y Regiones de .	12 de diciembre de 2022
Versión preliminar de una nueva función: GuardDuty RDS Protection	GuardDuty RDS Protection supervisa y perfila la actividad de inicio de sesión de RDS para identificar comportamientos de inicio de sesión sospechosos en las instancias de la base de datos de Amazon Aurora. Actualmente, estará disponible para una versión preliminar en cinco Regiones de AWS. Para obtener más información, consulte Puntos de conexión y Regiones de .	30 de noviembre de 2022
GuardDuty ya está disponible en la región de Oriente Medio (Emiratos Árabes Unidos)	Se agregó Oriente Medio (EAU) a la lista de Regiones de AWS lugares donde GuardDuty está disponible. Para obtener más información, consulte Puntos de conexión y Regiones de .	6 de octubre de 2022

Se agregó contenido para una nueva función: la protección contra GuardDuty malware	GuardDuty La protección contra malware es una mejora opcional de Amazon GuardDuty. Si bien GuardDuty identifica los recursos en riesgo, Malware Protection detecta el malware que puede ser la fuente del peligro. Con la protección contra malware habilitada, cada vez que GuardDuty detecta un comportamiento sospechoso en una instancia de Amazon EC2 o una carga de trabajo de contenedor indicativa de GuardDuty malware, Malware Protection inicia un análisis sin agente de los volúmenes de EBS adjuntos a las cargas de trabajo de la instancia o contenedor de EC2 afectadas para detectar la presencia de malware. Para obtener información sobre el funcionamiento de la protección contra malware y la configuración de esta función, consulte Protección contra malware. GuardDuty • Para obtener información sobre los resultados de la Protección contra el malware, consulte Detalles de los resultados.	26 de julio de 2022

	• Para obtener información sobre cómo corregir la instancia de EC2 comprometida y un contenedor independiente, consulte Solucionar los problemas de seguridad detectados por. GuardDuty • Para obtener información sobre la auditoría de CloudWatch los registros de análisis de malware y los motivos por los que se omite un recurso durante el análisis de software malicioso, consulte Descripción CloudWatch de los registros y los motivos de omisión. • Para obtener información sobre las detecciones de amenazas con falsos positivos, consulte Notificación de falsos positivos en GuardDuty Malware Protection.	
Se ha retirado un tipo de resultado	Se ha retirado Exfiltration:S3/ObjectRead.Unusual.	5 de julio de 2022

Se agregaron nuevos tipos de detección de S3 que identifican el comportamiento anómalo mediante el modelo GuardDuty de aprendizaje automático (ML) de detección de anomalías.	Se han agregado los siguientes tipos de resultados de S3 nuevos. Estos tipos de resultados identifican si una solicitud de API ha invocado una entidad de IAM de forma anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Para obtener más información sobre cada uno de estos nuevos resultados, consulte Tipos de resultados de S3. • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	5 de julio de 2022

Se agregó contenido de protección GuardDuty EKS para GuardDuty	GuardDuty ahora puede generar resultados para sus recursos de Amazon EKS mediante la supervisión de los registros de auditoría de Kubernetes. Para obtener información sobre cómo configurar esta función, consulte Protección EKS en Amazon GuardDuty. Para ver una lista de las conclusiones que GuardDuty se pueden generar para los recursos de Amazon EKS, consulte las conclusiones de Kubernetes. Se ha agregado una nueva guía de corrección para respaldar la corrección de estos resultados en la Guía de corrección de resultados de Kubernetes.	25 de enero de 2022
Se ha agregado 1 resultado nuevo	Se ha agregado un nuevo resultado UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS. Este hallazgo le informa cuando una AWS cuenta ajena a su entorno accede a las credenciales de su instancia. AWS	20 de enero de 2022

Se han actualizado los tipos de resultados para ayudar a identificar los problemas relacionados con log4j	Amazon GuardDuty ha actualizado los siguiente s tipos de búsqueda para ayudar a identificar y priorizar los problemas relaciona dos con los CVE-2021-44228 y CVE-2021-45046: Backdoor:EC2/C&CActivity.B; Backdoor:EC2/C&CActivity.B! NetworkPortUnusualDNS; comportamiento: EC2/.	22 de diciembre de 2021
Cambios en los resultados	UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltrat ion se ha cambiado por UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltrat ion.OutsideAWS. Esta versión mejorada del resultado descubre las ubicaciones habituales en las que se utilizan sus credenciales para reducir los resultados del tráfico que se direcciona a través de las redes locales. UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltrat ion.OutsideAWS	7 de septiembre de 2021
GuardDuty Actualización a SLR	La GuardDuty SLR se ha actualizado con nuevas acciones para mejorar la precisión de la localización.	3 de agosto de 2021

Se ha agregado información sobre el origen de datos de cada tipo de resultado.	Las descripciones de los hallazgos ahora contienen información sobre las fuentes de datos que se GuardDuty utilizan para generar ese hallazgo.	10 de mayo de 2021
Se han retirado 13 tipos de resultados.	Se han retirado 13 hallazgos para reemplazarlos por nuevos AnomalousBehavoir hallazgos. Persistence:IAMUser/NetworkPermissions, Persistence:IAMUser/ResourcePermissionsPersistence:IAMUser/UserPermissions, PrivilegeEscalation:IAMUser/AdministrativePermissions, Recon:IAMUser/NetworkPermissions, Recon:IAMUser/ResourcePermissions, Recon:IAMUser/UserPermissions, ResourceConsumption:IAMUser/ComputeResourcesStealth:IAMUser/LoggingConfigurationModified, Discovery:S3/BucketEnumeration.Unusual, Impact:S3/ObjectDelete.Unusual, Impact:S3/PermissionsModification.Unusual.	12 de marzo de 2021

Se han agregado 8 nuevos tipos de resultados para detectar comportamientos anómalos.	Se han agregado 8 nuevos tipos de resultados de IAMUser en función del comportamiento anómalo de las entidades principales de IAM. CredentialAccess:IAMUser/AnomalousBehavior, DefenseEvasion:IAMUser/AnomalousBehavior, Discovery:IAMUser/AnomalousBehavior, Exfiltration:IAMUser/AnomalousBehavior, Impact:IAMUser/AnomalousBehavior, InitialAccess:IAMUser/AnomalousBehavior, Persistence:IAMUser/AnomalousBehavior, PrivilegeEscalation:IAMUser/AnomalousBehavior.	12 de marzo de 2021
Se han agregado los resultados de EC2 en función de la reputación del dominio.	Se han agregado 4 nuevos tipos de resultados de impacto en función de la reputación del dominio. Impact:EC2/AbusedDomainRequest.Reputation , Impact:EC2/BitcoinDomainRequest.Reputation, Impact:EC2/MaliciousDomainRequest.Reputation. También se ha agregado un nuevo resultado de EC2 para C&CActivity. Impact:EC2/SuspiciousDomainRequest.Reputation	27 de enero de 2021

Se han agregado 4 nuevos tipos de resultados.	Se han agregado 3 nuevos resultados de Malicious IPCaller de S3. Discovery:S3/MaliciousIPCaller, Exfiltration:S3/MaliciousIPCaller, Impact:S3/MaliciousIPCaller. También se ha agregado un nuevo resultado de EC2 para C&CActivity. Backdoor:EC2/C&CActivity.B	21 de diciembre de 2020
Se ha retirado el tipo de resultado UnauthorizedAccess:EC2/TorIPCaller.	El tipo de UnauthorizedAccess:EC2/TorIPCaller hallazgo ahora está retirado de GuardDuty. Más información.	1 de octubre de 2020
Se ha agregado el tipo de resultado Impact:EC2/WinRmBruteForce.	Se ha agregado un nuevo resultado de impacto, Impact:EC2/WinRmBruteForce. Más información.	17 de septiembre de 2020
Se ha agregado el tipo de resultado Impact:EC2/PortSweep.	Se ha agregado un nuevo resultado de impacto, Impact:EC2/PortSweep. Más información.	17 de septiembre de 2020
GuardDuty ahora está disponible en las regiones de África (Ciudad del Cabo) y Europa (Milán).	Se han añadido África (Ciudad del Cabo) y Europa (Milán) a la lista de AWS regiones en las que GuardDuty está disponible. Más información	31 de julio de 2020

Se agregaron nuevos detalles de uso para monitorear GuardDuty los costos.	Ahora puedes usar nuevas métricas para consultar los datos de los costos de GuardDuty uso de tu cuenta y de las cuentas que administras. Encontrará nueva información general sobre los costos de uso en la consola, en https://console.aws.amazon.com/guardduty/. Se puede acceder a información más detallada a través de la API.	31 de julio de 2020
Se agregó contenido sobre la protección de S3 mediante la supervisión de eventos de datos de S3 en GuardDuty.	GuardDuty La protección de S3 ahora está disponible mediante la supervisión de los eventos del plano de datos de S3 como nueva fuente de datos. Las cuentas nuevas tendrán esta característica habilitada automáticamente. Si ya la está utilizando, GuardDuty puede habilitar la nueva fuente de datos para usted o para sus cuentas de miembros.	31 de julio de 2020
Se han agregado 14 resultados de S3 nuevos.	Se han agregado 14 nuevos tipos de resultados de S3 para los orígenes del plano de control y del plano de datos de S3.	31 de julio de 2020

Se ha agregado compatibilidad adicional para los resultados de S3 y se han cambiado 2 nombres de tipos de resultados existentes.	GuardDuty los resultados ahora incluyen más detalles sobre los hallazgos relacionados con los cubos de S3. Se ha cambiado el nombre de los tipos de resultados existentes que estaban relacionados con la actividad de S3: Policy:IAMUser/S3BlockPublicAccessDisabled se ha cambiado a Policy:S3/BucketBlockPublicAccessDisabled. Stealth:IAMUser/S3ServerAccessLoggingDisabled se ha cambiado a Stealth:S3/ServerAccessLoggingDisabled.	28 de mayo de 2020

Se agregó contenido para la AWS Organizations integración.	GuardDuty ahora se integra con los administradores AWS Organizations delegados para permitirle administrar GuardDuty las cuentas de su organización. Al configurar un administrador delegado como su cuenta de GuardDuty administrador, puede habilitar automáticamente la administración GuardDuty de cualquier miembro de la organización mediante la cuenta de administrador delegado. También puede habilitar automáticamente las cuentas de GuardDuty los nuevos AWS Organizations miembros. Más información.	20 de abril de 2020
Se ha agregado contenido para la característica Exportar los resultados.	Se agregó contenido que describe la función Export Findings de GuardDuty.	14 de noviembre de 2019
Se ha agregado el tipo de resultado UnauthorizedAccess:EC2/MetadataDNSRebind.	Se ha agregado un nuevo resultado no autorizado, UnauthorizedAccess:EC2/MetadataDNSRebind. Más información.	10 de octubre de 2019
Se ha agregado el tipo de resultado Stealth:IAMUser/S3ServerAccessLoggingDisabled.	Se ha agregado un nuevo resultado invisible, Stealth:IAMUser/S3ServerAccessLoggingDisabled. Más información.	10 de octubre de 2019

Se ha agregado el tipo de resultado Policy:IAMUser/S3BlockPublicAccessDisabled.	Se ha agregado un nuevo resultado de política, Policy:IAMUser/S3BlockPublicAccessDisabled. Más información.	10 de octubre de 2019
Se ha retirado el tipo de resultado Backdoor:EC2/XORDDOS.	El tipo de Backdoor:EC2/XORDDOS hallazgo ahora está retirado de GuardDuty. Obtenga más información	12 de junio de 2019
Se ha agregado el tipo de resultado PrivilegeEscalation.	El tipo de resultado Privilege Escalation detecta cuando los usuarios intentan asignar privilegios escalados y más permisivos a sus cuentas. Más información	14 de mayo de 2019
GuardDuty ya está disponible en la región de Europa (Estocolmo).	Se ha añadido Europa (Estocolmo) a la lista de AWS regiones en las que GuardDuty está disponible. Más información	9 de mayo de 2019
Se ha agregado un nuevo tipo de resultado, Recon:EC2/PortProbeEMRUnprotectedPort.	Este resultado le informa de que un puerto sensible relacionado con ERM en una instancia EC2 no está bloqueado y se está sondeando activamente. Más información	8 de mayo de 2019

Se han agregado 5 tipos de resultados nuevos que detectan si las instancias de EC2 se están utilizando posiblemente para llevar a cabo ataques de denegación de servicio (DoS).	Estos resultados le informan de las instancias EC2 de su entorno cuyo comportamiento puede indicar que se están utilizando para llevar a cabo ataques de denegación de servicio (DoS). Más información	8 de marzo de 2019
Se ha agregado un nuevo tipo de resultado: Policy:IAMUser/RootCredentialUsage	Policy:IAMUser/RootCredentialUsageEl tipo de búsqueda le informa de que sus credenciales de inicio de sesión de usuario raíz Cuenta de AWS se utilizan para realizar solicitudes programáticas a los AWS servicios. Más información	24 de enero de 2019
Se ha retirado el tipo de resultado UnauthorizedAccess:IAMUser/UnusualASNCaller	Se ha retirado el tipo de resultado UnauthorizedAccess:IAMUser/UnusualASNCaller. Ahora recibirá notificaciones sobre la actividad invocada desde redes inusuales a través de otros tipos de búsquedas activas GuardDuty . El tipo de resultado generado dependerá de la categoría de la API que se invocó desde una red inusual. Más información	21 de diciembre de 2018

Se han agregado dos nuevos tipos de resultados: PenTest:IAMUser/ParrotLinux y PenTest:IAMUser/PentooLinux	El tipo de resultado PenTest:IAMUser/ParrotLinux le informa de que un equipo que ejecuta Parrot Security Linux está haciendo llamadas a la API con las credencias les que pertenecen a su cuenta de AWS . El tipo de resultado PenTest:IAMUser/PentooLinux le informa de que una máquina que ejecuta Pentoo Linux está haciendo llamadas a la API con las credenciales que pertenecen a su cuenta de AWS . Más información	21 de diciembre de 2018
Se agregó soporte para el tema SNS de GuardDuty anuncios de Amazon	Ahora puede suscribirse al tema SNS de GuardDuty anuncios para recibir notificaciones sobre los tipos de búsqueda publicados recientemente, las actualizaciones de los tipos de búsqueda existentes y otros cambios en las funciones. Las notificaciones están disponibles en todos los formatos que admite Amazon SNS. Más información	21 de noviembre de 2018

Se han agregado dos nuevos tipos de resultados: UnauthorizedAccess:EC2/TorClient y UnauthorizedAccess:EC2/TorRelay	UnauthorizedAccess:EC2/TorClientAl buscar el tipo, se indica que una instancia de EC2 de su AWS entorno se está conectando a un nodo de Tor Guard o de Authority . UnauthorizedAccess:EC2/TorRelaybuscar el tipo le informa de que una instancia EC2 de su AWS entorno se está conectando a una red Tor, lo que sugiere que actúa como un repetidor de Tor. Más información	16 de noviembre de 2018
Se ha agregado un nuevo tipo de resultado: CryptoCurrency:EC2/BitcoinTool.B	Este hallazgo te indica que una instancia de EC2 de tu AWS entorno está consultando un nombre de dominio asociado a Bitcoin u otra actividad relacionada con las criptomonedas. Más información	9 de noviembre de 2018
Se agregó soporte para actualizar la frecuencia de las notificaciones enviadas a Events CloudWatch	Ahora puede actualizar la frecuencia de las notificaciones que se envían a CloudWatch Events para que se repitan posteriormente los hallazgos existentes. Los valores posibles son 15 minutos, una hora o seis horas, que es el valor predeterminado. Más información	9 de octubre de 2018

Se han agregado regiones compatibles	Se agregó soporte regional para AWS GovCloud (EE. UU.-Oeste) Más información	25 de julio de 2018
Se agregó soporte para en AWS CloudFormation StackSets GuardDuty	Puedes usar la GuardDuty plantilla Enable Amazon para habilitar GuardDuty simultáne amente en varias cuentas. Más información	25 de junio de 2018
Se agregó soporte para reglas de GuardDuty archivado automático	Los clientes ya pueden crear reglas de archivado automátic o detalladas para la supresión de resultados. En el caso de los hallazgos que coincidan con una regla de archivado automático, los marca GuardDuty automáticamente como archivados. Esto permite a los clientes ajustar aún más GuardDuty para mantener solo los hallazgos relevantes en la tabla de hallazgos actual. Más información	4 de mayo de 2018
GuardDuty está disponible en la región de Europa (París)	GuardDuty ya está disponibl e en Europa (París), lo que le permite ampliar la supervisi ón continua de la seguridad y la detección de amenazas en esta región. Más información	29 de marzo de 2018
Ahora AWS CloudFormation es GuardDuty posible crear cuentas de administrador y cuentas de miembros a través de ellas.	Para más información, consulte `AWS::GuardDuty::master` y `AWS::GuardDuty::member`.	6 de marzo de 2018

Se agregaron nueve nuevas detecciones de anomalías CloudTrail basadas en bases.	Estos nuevos tipos de búsqueda se activan automáticamente GuardDuty en todas las regiones compatibles. Más información	28 de febrero de 2018
Se han agregado nuevas detecciones de inteligencia de amenazas (tipos de resultados).	Estos nuevos tipos de búsqueda se activan automáticamente GuardDuty en todas las regiones compatibles. Más información	5 de febrero de 2018
Aumento del límite para las cuentas GuardDuty de los miembros.	Con esta versión, puede añadir hasta 1000 cuentas de GuardDuty miembros por AWS cuenta (cuenta de GuardDuty administrador). Más información	25 de enero de 2018
Cambios en la carga y posterior administración de las listas de direcciones IP confiables y las listas de amenazas para las cuentas de GuardDuty administrador y las cuentas de los miembros.	Con esta versión, los usuarios de GuardDuty cuentas de administrador pueden cargar y gestionar listas de IP fiables y listas de amenazas. Los usuarios de GuardDuty las cuentas de los miembros no pueden cargar ni gestionar listas. Las listas de direccion es IP fiables y las listas de amenazas que carga la cuenta de administrador están sujetas a la GuardDuty funcional idad de las cuentas de los miembros. Más información	25 de enero de 2018

Actualizaciones anteriores

Cambio	Descripción	Fecha
Publicación inicial	Publicación inicial de la Guía del GuardDuty usuario de Amazon.	28 de noviembre de 2017

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.