Configuración de la integración de QRadar con Umbrella Log Management y S3

Contenido

Introducción

Este documento describe cómo configurar QRadar para ingerir registros desde una cubeta AWS S3 para la administración de registros de Umbrella.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

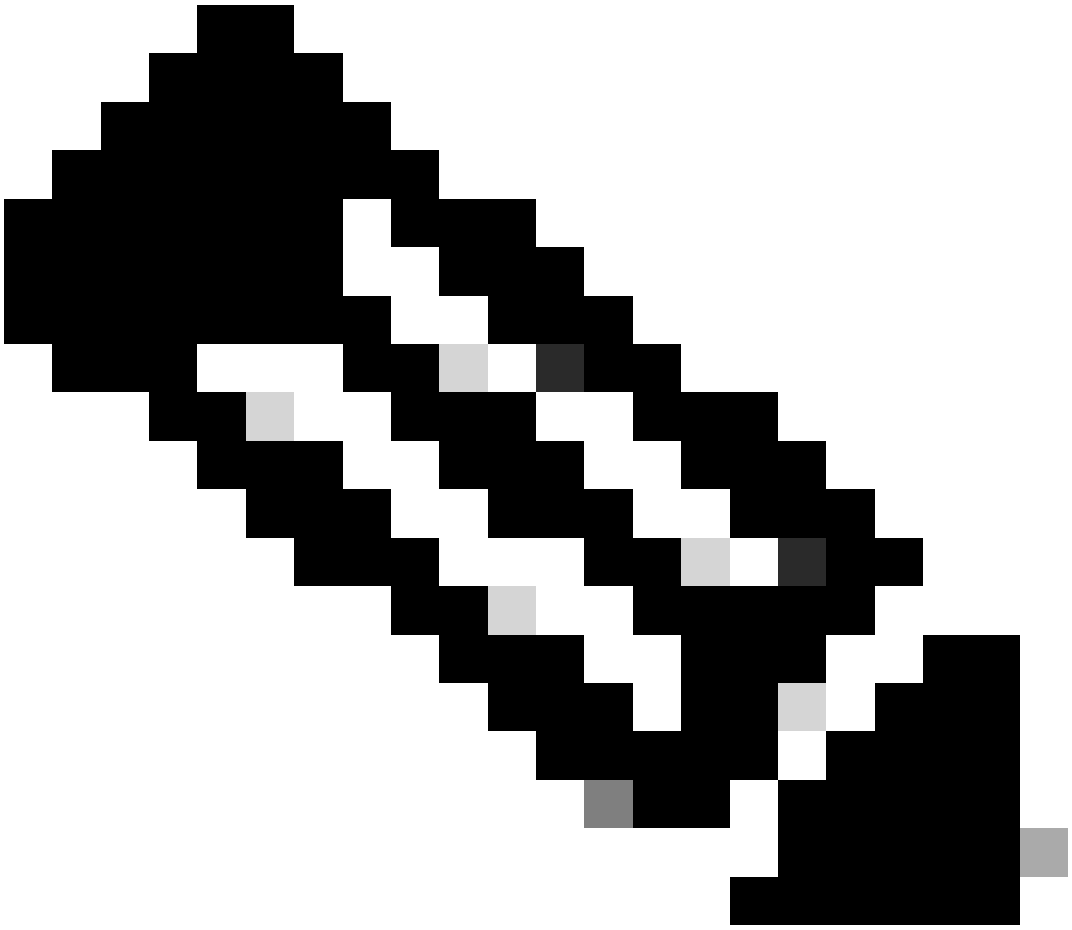
- Este documento asume que su cubeta Amazon AWS S3 se ha configurado en Umbrella (Configuraciones > Administración de registro) y se muestra verde con los registros recientes que se han cargado. Para obtener más información sobre cómo configurar esta función, lea este artículo: Download Logs from Umbrella Log Management in AWS S3
- Además de los derechos administrativos de los dispositivos QRadar, la configuración de Amazon S3 y el panel de Umbrella, estas instrucciones suponen que el administrador de QRadar está familiarizado con la creación de archivos LSX (Extensión de origen de registro).

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview



> Nota: El mejor método de configuración de QRadar para su uso con Cisco Umbrella es a través de la aplicación Cisco Cloud Security. Solo continúe con este método si la aplicación no se puede configurar.

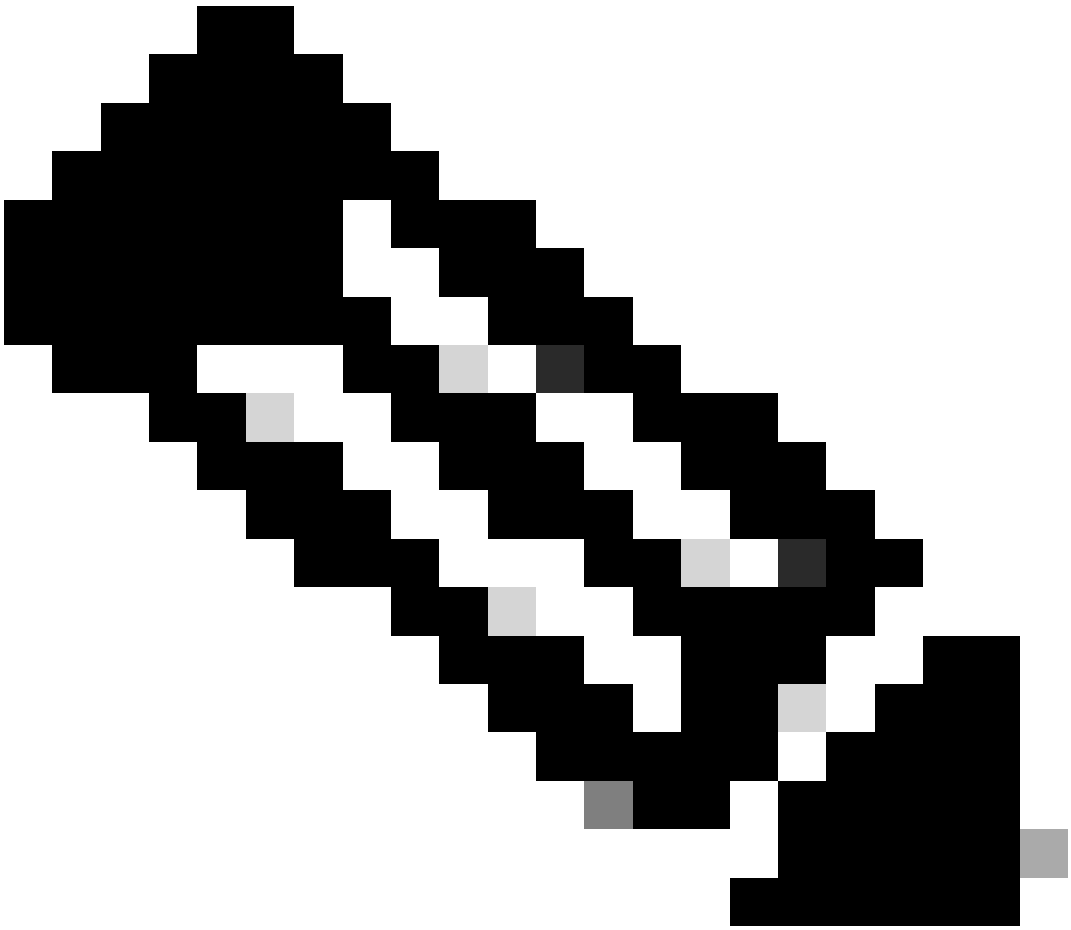
QRadar de IBM es un popular SIEM para el análisis de registros. Proporciona una interfaz potente

para analizar grandes fragmentos de datos, como los registros proporcionados por Cisco Umbrella para el tráfico DNS de su organización.

En este artículo se describe cómo configurar y ejecutar QRadar para que pueda extraer los registros de su cubeta S3 y consumirlos. Hay dos etapas principales:

- Configure sus credenciales de seguridad de AWS S3 para permitir el acceso de QRadar a los registros.
- Configure QRadar para que apunte a su cubo.

Si está utilizando el bloque de memoria S3 administrado por Cisco, por favor utilice estas instrucciones en el artículo Descargar registros desde la administración de registros de Umbrella mediante la CLI de AWS.



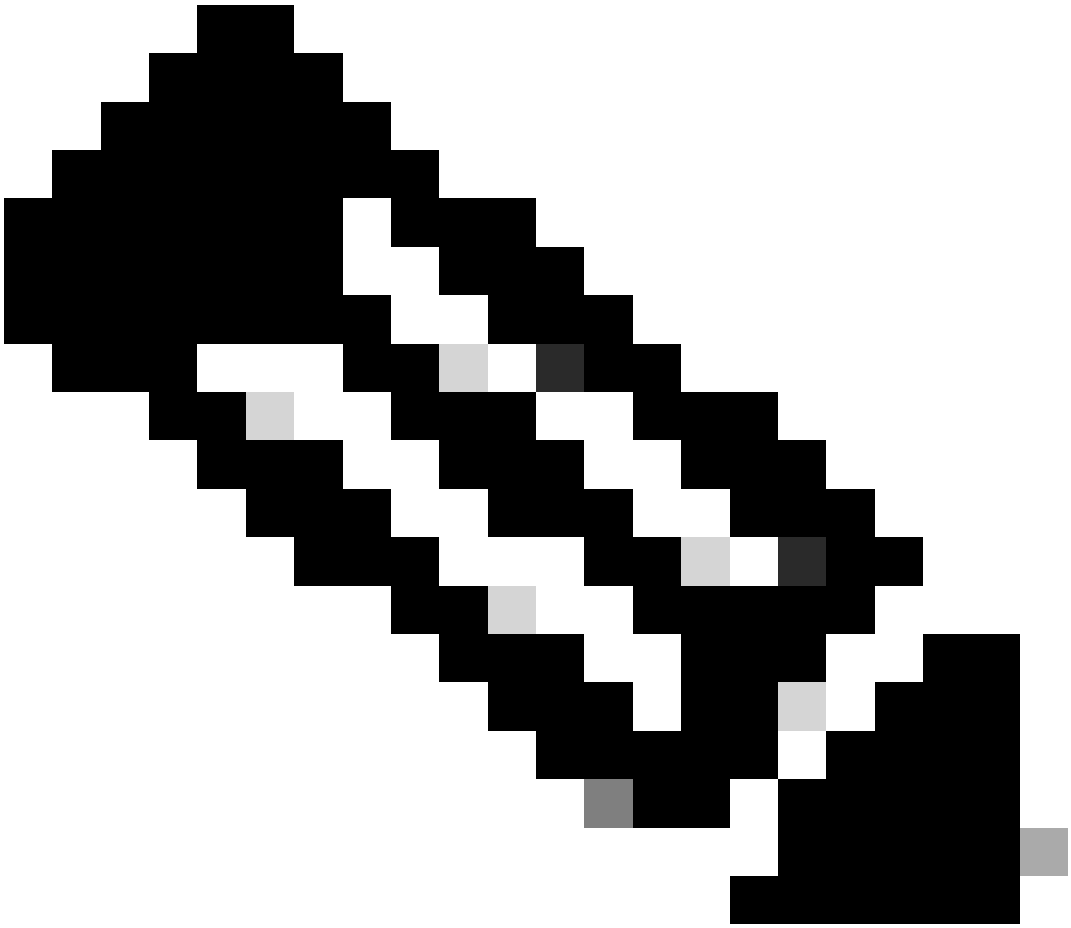
Nota: Esta integración se ha probado tanto con depósitos S3 gestionados por el cliente como con depósitos S3 gestionados por Cisco. La información que se trata en este artículo está actualizada en este momento (octubre de 2019). Puede cambiar en función de la forma en que interactúan QRadar y AWS Services. Este documento es un

---

documento activo. Si tiene comentarios o ha encontrado trucos o sugerencias que podrían ayudar a otros clientes, póngase en contacto con el servicio de asistencia de Cisco Umbrella.

El soporte para QRadar debe proceder de IBM, ya que Cisco no puede ofrecer soporte directo para hardware o software de terceros. Si tiene algún problema al conectar el panel de Umbrella a la cubeta de S3, Cisco Umbrella puede ofrecerle asistencia. Gran parte de la información que se encuentra en este artículo también se puede encontrar en el sitio web de IBM.

Etapa 1: Configuración de sus credenciales de seguridad en AWS



Nota: Estos pasos son los mismos que los descritos en el artículo que describe cómo configurar una herramienta para descargar los registros de su cubeta (Descargar Registros de Umbrella Log Management en AWS S3). Si ya ha realizado estos pasos,

puede saltar a la etapa 2, aunque más tarde necesitará las credenciales de seguridad de su usuario de IAM para autenticar QRadar en su cubeta.

Paso 1

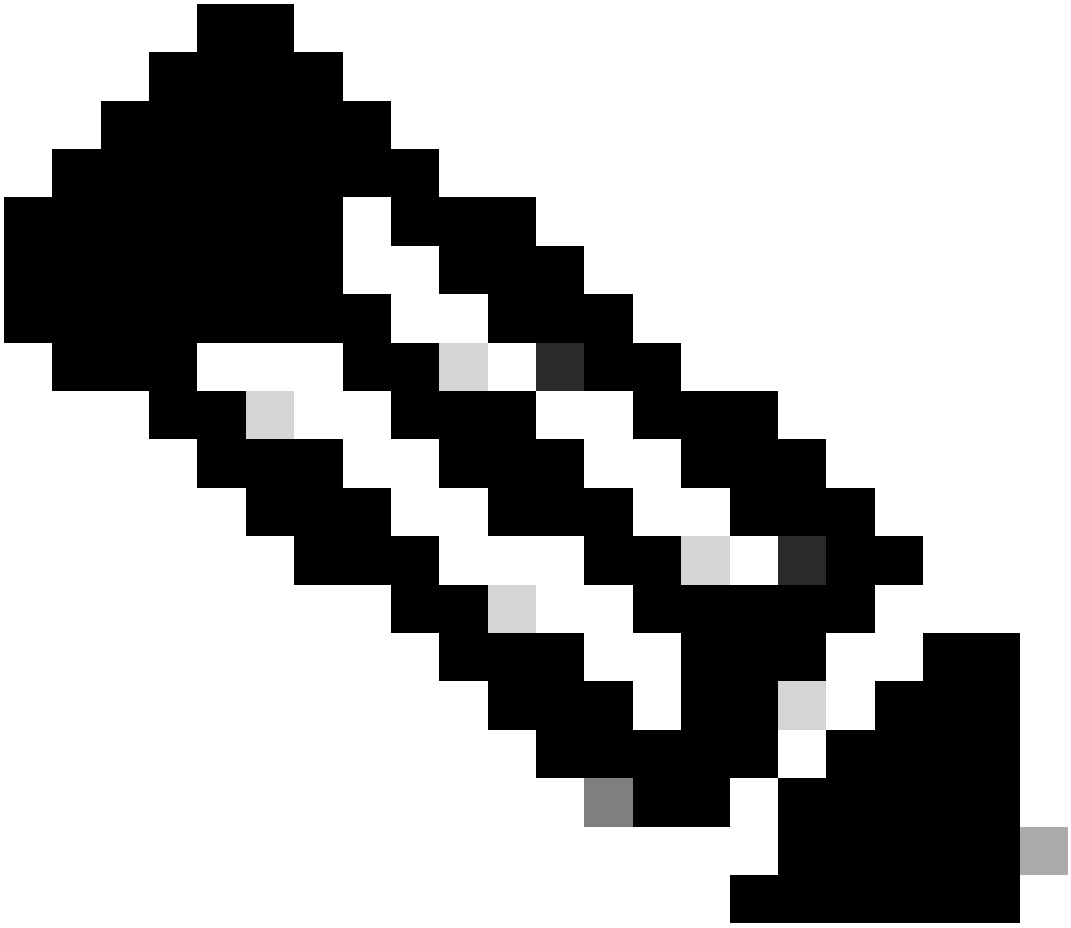
1. Agregue una clave de acceso a su cuenta de Amazon Web Services para permitir el acceso remoto a su herramienta local y brinde la capacidad de cargar, descargar y modificar archivos en S3:

1. Inicie sesión en AWS.
2. Seleccione el nombre de su cuenta en la esquina superior derecha.
3. En el menú desplegable, seleccione Security Credentials.

2. A continuación, se le pedirá que utilice las mejores prácticas de Amazon y que cree un usuario de AWS Identity and Access Management (IAM). Básicamente, un usuario de IAM se asegura de que la cuenta que s3cmd utiliza para acceder a su cubeta no sea la cuenta maestra (por ejemplo, su cuenta) para toda su configuración de S3. Al crear usuarios IAM individuales para las personas que acceden a su cuenta, puede proporcionar a cada usuario IAM un conjunto único de credenciales de seguridad. También puede conceder diferentes permisos a cada usuario de IAM. Si es necesario, puede cambiar o revocar los permisos de un usuario de IAM en cualquier momento. Para obtener más información sobre los usuarios de IAM y las prácticas recomendadas de AWS, lea la documentación de AWS.

Paso 2

1. Seleccione Get Started with IAM Users para crear un usuario IAM para acceder a su cubeta S3. A continuación, se le llevará a una pantalla en la que podrá crear un usuario IAM.
2. Seleccione Nuevos Usuarios y rellene los campos.



Nota: La cuenta de usuario no puede contener espacios.

3. Después de crear la cuenta de usuario, solo se le da una oportunidad para tomar dos piezas críticas de información que contienen sus credenciales de seguridad de usuario de Amazon. Umbrella sugiere que descargue estos mediante el botón en la parte inferior derecha para hacer una copia de seguridad de ellos. No están disponibles después de esta etapa de la configuración. Asegúrese de anotar el Id. de clave de acceso y la Clave de acceso secreta, ya que son necesarios en un paso posterior.

Paso 3

A continuación, agregue una política para el usuario de IAM de modo que tenga acceso a la cubeta S3:

1. Seleccione el usuario que acaba de crear y, a continuación, desplácese hacia abajo por las propiedades de los usuarios hasta que aparezca el botón Adjuntar directiva.

2. Seleccione Adjuntar política e introduzca "s3" en el filtro de tipo de política. Esto muestra dos resultados:

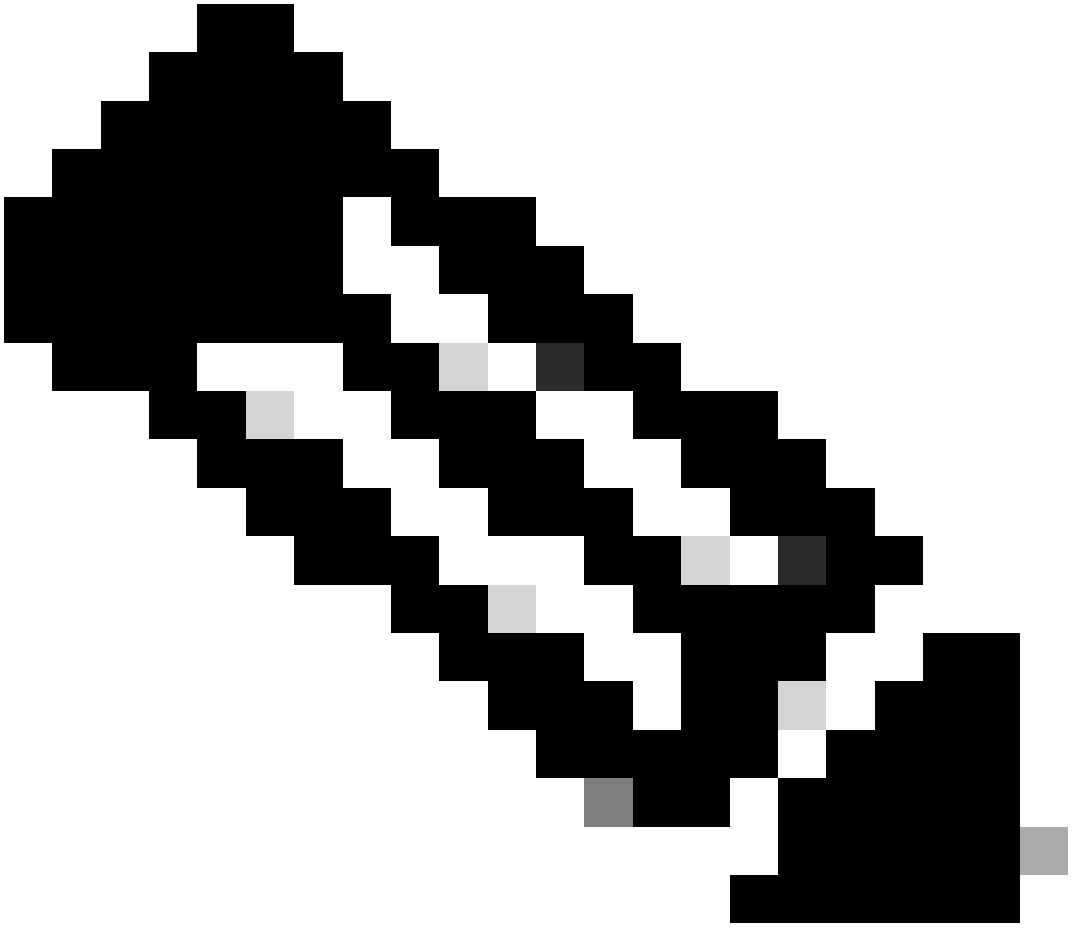
- AmazonS3FullAccess
- AmazonS3ReadOnlyAccess

3. Seleccione AmazonS3FullAccess, y luego seleccione Adjuntar política en la esquina inferior derecha.

Etapa 2: Configuración de QRadar para extraer los datos de registro de DNS de la cubeta S3

QRadar hace uso del servicio AWS CloudTrail, que es un servicio web que registra las llamadas API de AWS para su cuenta y le entrega archivos de registro.

Antes de que QRadar acceda a Amazon S3, complete este procedimiento de IBM para obtener el certificado de servidor de Amazon. Esta parte es difícil, así que asegúrese de completar las instrucciones exactamente.



Nota: En las pruebas, debe utilizar el navegador Firefox para que esto funcione como se espera.

Para obtener el certificado de servidor de Amazon, debe mover el certificado en formato DER al dispositivo QRadar adecuado. El dispositivo QRadar que requiere el certificado es el dispositivo asignado en el campo Target Event Collector en el origen de registro de Amazon AWS CloudTrail.

Antes de comenzar

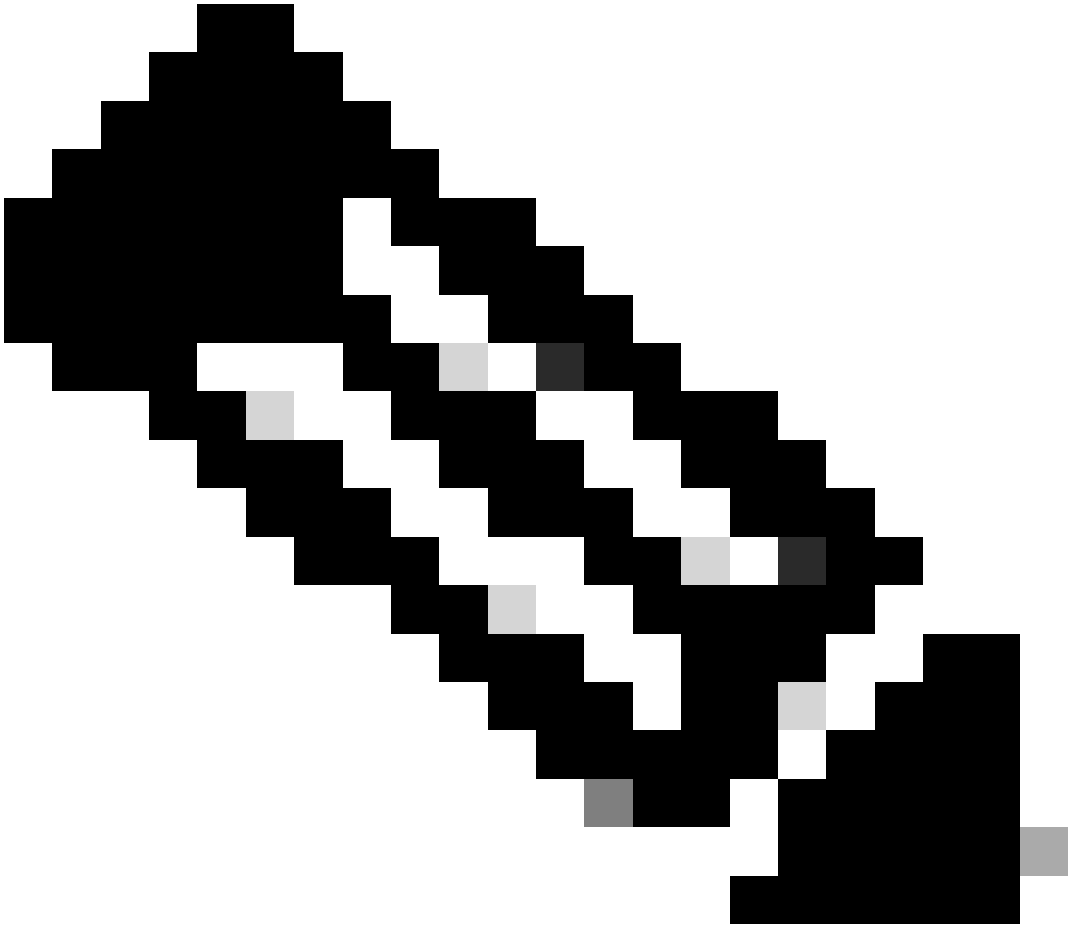
- El certificado debe estar en formato .DER.
- La extensión .DER distingue entre mayúsculas y minúsculas y debe estar en mayúsculas.
- Si el certificado se exporta en minúsculas, el origen de registro puede experimentar problemas de recopilación de eventos.

Pasos iniciales

1. Acceda a su cubeta de AWS CloudTrail S3: `https://<bucketname>.s3.amazonaws.com`

2. Utilice Firefox para exportar el certificado SSL de AWS como un certificado (.DER). Firefox puede crear el certificado necesario con la extensión .DER:

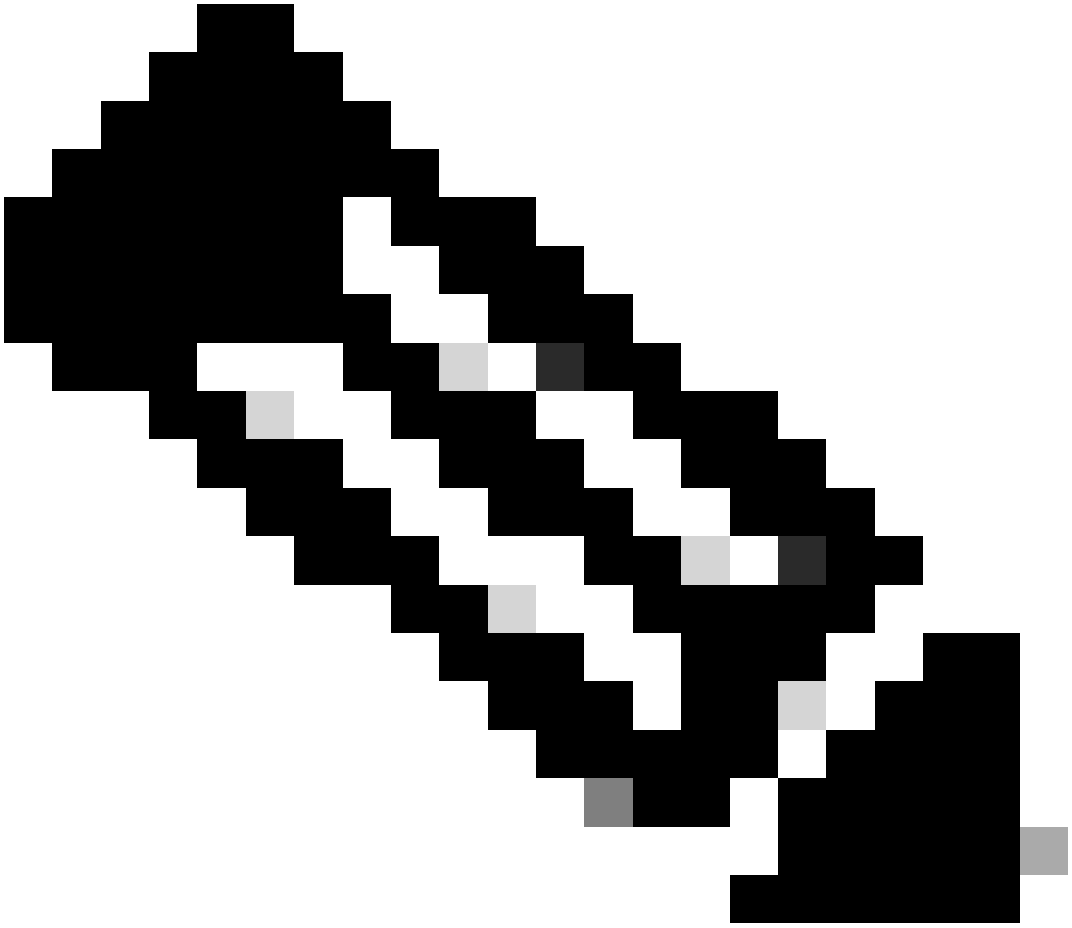
1. Seleccione el icono Identidad del sitio (el icono de candado de la barra de direcciones).
2. Seleccione Más información > Ver certificado y seleccione la pestaña Detalles.
3. Seleccione Exportar para exportar en el formato .DER del certificado.



Nota: La extensión .DER distingue entre mayúsculas y minúsculas y debe estar en mayúsculas.

---

3. Copie el certificado .DER en el directorio /opt/QRadar/conf/trusted_certificates del dispositivo QRadar que administra el origen de registro de Amazon AWS CloudTrail. Puede utilizar WinSCP para copiarlo.



Nota: El dispositivo QRadar que administra el origen de registro se identifica mediante el campo Target Event Collect en el origen de registro de Amazon AWS CloudTrail. El dispositivo QRadar que administra el origen de registro de Amazon AWS CloudTrail debe tener una copia del certificado .DER en /opt/QRadar/conf/trusted_certificates.

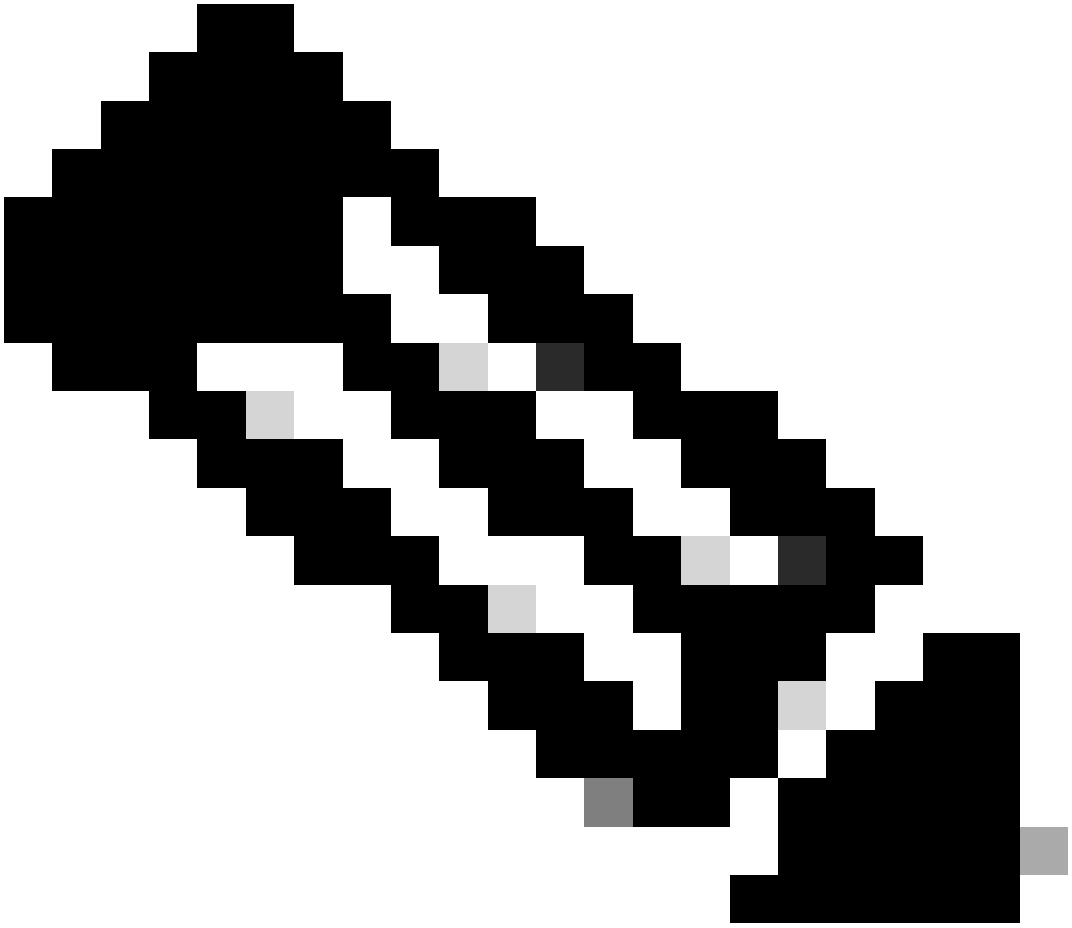
4. Inicie sesión en la interfaz de usuario de QRadar como usuario administrativo.

5. Seleccione la pestaña Admin.

6. Seleccione el icono Orígenes de Log.

7. Seleccione la fuente de registro de Amazon AWS CloudTrail.

8. En el menú de navegación, seleccione Enable/Disable para deshabilitar y, a continuación, vuelva a habilitar la fuente de registro de CloudTrail de Amazon AWS.



Nota: Cuando un administrador fuerza el origen de registro de deshabilitado a habilitado, esto permite que el protocolo se conecte a la cubeta de Amazon AWS como se define en el origen de registro. A continuación, se realiza una comprobación de certificados como parte de la primera comunicación.

9. Si sigue teniendo problemas, compruebe que el campo Identificador de origen de registro contiene el nombre de depósito correcto de Amazon AWS y que la ruta del directorio remoto es correcta en la configuración del origen de registro.

Finalizar la configuración de QRadar

1. En QRadar asegúrese de que todos sus protocolos, DSM y otra información estén actualizados. Seleccione LogFileProtocol con estas configuraciones (la frecuencia, la hora de inicio, la periodicidad y otra información pueden ser diferentes).

2. En la pestaña Orígenes de Log, introduzca un Nombre de Origen de Log y una Descripción de Origen de Log. Estos pueden ser lo que quieras.

3. Introduzca el nombre del depósito S3, la clave de acceso de AWS, la clave secreta de AWS y el directorio remoto (probablemente dnslogs, pero depende de la configuración). Agregar un identificador de origen de registro como el año puede ayudar a filtrar para que solo se extraigan los registros con "2019" en ellos.

4. Cree un LSX (Extensión de origen de registro) que pueda analizar los eventos de Cisco Umbrella. (Así es como se ve después de la importación en QRadar.) Más información sobre cómo crear exactamente LSX se puede encontrar en el sitio web de IBM. Esto es solo un ejemplo. Los datos que desea extraer de los registros varían en función del caso práctico.

5. Compruebe dos veces que la clave de acceso de AWS y la clave secreta de AWS se han copiado y pegado correctamente en la configuración de origen de registro.

6. Seleccione el procesador GZIP y un generador de eventos de varias líneas basadas en RegEx. La forma más sencilla de obtener un evento por línea es mediante un modelo de inicio de RegEx de:

```
("\d{4}-\d{2}-\d{2}\s\d{2}:\d{2}:\d{2}",")
```

Asegúrese de seleccionar la extensión de origen de registro y la condición de uso y, a continuación, guarde el origen de registro.

7. Realice una implementación completa en QRadar.

Su origen de registro luego utiliza RestAPI para conectarse a su cubeta con las credenciales y claves que usted proporcionó y comenzar a extraer eventos.

Additional Information

Activar registro de depósito

Para habilitar el registro de cubeta, lea la documentación de AWS y complete los procedimientos descritos. De forma predeterminada, el registro está deshabilitado. Una vez habilitada, una nueva carpeta llamada /logs reside en la raíz de la cubeta para mostrarle la información de GETS, PUTS y DELETES.

Gestión del ciclo de registro

Cuando utiliza S3, puede administrar el ciclo de vida de los datos dentro de la cubeta para ampliar el tiempo durante el cual desea conservar los registros. Dependiendo del propósito para el que esté utilizando la administración de registros externa, la duración puede ser muy corta o muy larga. Por ejemplo, puede simplemente descargar los registros de la cubeta S3 después de 24 horas y almacenarlos sin conexión, o retenerlos indefinidamente en la nube.

De forma predeterminada, Amazon almacena los datos en una cubeta indefinidamente, pero el almacenamiento ilimitado aumenta el costo de mantenimiento de la cubeta. Para obtener más información sobre los ciclos de vida S3, lea la documentación de AWS.

Para configurar el ciclo de vida de la cubeta:

1. Seleccione Propiedades > Ciclo de vida.

2. Seleccione Agregar una Regla y, a continuación, Aplicar la Regla a toda la cubeta (o a una subcarpeta si la ha configurado como tal).

3. Seleccione una acción sobre objetos, como Suprimir o Archivar, y seleccione el período de tiempo y si desea utilizar el almacenamiento Glacier para ayudar a reducir los costes de Amazon. (Glacier es almacenamiento "frío" fuera de línea, que, aunque más lento de acceso, es mucho menos costoso.)

Si prefiere administrar los registros mediante otro método (por ejemplo, en su solución de copia de seguridad interna), puede simplemente descargar los registros de S3 y conservarlos de otra manera.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).