

Configurar registros de eventos consolidados para AWS S3 Push

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar los registros de eventos consolidados que se enviarán a una cubeta S3 en un dispositivo de seguridad de correo electrónico (ESA) o Cloud Email Security (CES).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ESA que ejecuta Async OS 13.0 o superior
- Acceso administrativo al dispositivo
- Cuenta de Amazon Web Services (AWS) y acceso para crear y administrar la cubeta S3

Componentes Utilizados

La información de este documento se basa en todos los modelos de hardware y dispositivos virtuales ESA soportados que ejecutan Async OS 13.0 o superior. Para verificar la información de versión del dispositivo desde la CLI, ingrese el comando `version`. En la GUI, seleccione **Monitor > System Status**.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier configuración.

Antecedentes

A partir de Async OS 13.0 y superiores, ESA permite la configuración de registros basados en Unified Common Event Format (CEF) conocidos como registros de eventos consolidados que utilizan ampliamente los proveedores de SIEM. Consulte las notas de la versión ESA 13.0 [aquí](#).

Los registros CEF también se pueden configurar para enviarlos a una cubeta AWS S3 aparte de la descarga manual, SCP y la inserción de Syslog.

Nota: Los pasos proporcionados para la configuración de AWS se basan en la información disponible en el momento de escribir este artículo.

Configurar

1. Navegue hasta la consola en la nube de AWS para recopilar S3 Bucket Name, S3 Access Key y S3 Secret Key.

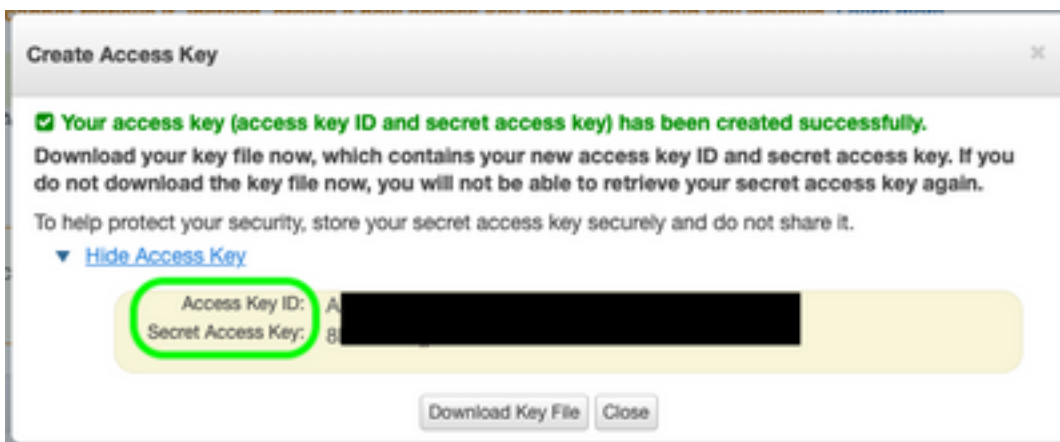
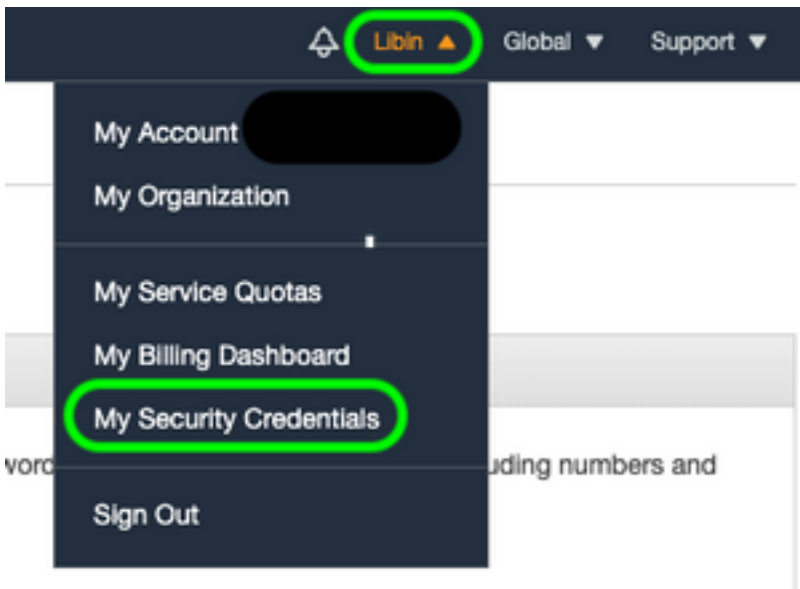
Para el nombre de depósito S3:

Una vez que haya iniciado sesión en AWS Cloud, utilice el menú desplegable Services (Servicios) para seleccionar S3 o utilice la barra de búsqueda de la parte superior para buscar S3. Cree una cubeta con opciones predeterminadas o nombre de captura para una de las cubetas existentes que se va a utilizar.



Para clave de acceso S3 y clave secreta S3:

Haga clic en el nombre de su cuenta en la parte superior derecha y, en el menú desplegable, seleccione "Mis credenciales de seguridad". En la página abierta, haga clic en "Access keys (access key ID and secret access key)" (Clave de acceso y clave de acceso secreta). Cree una nueva clave de acceso, vea o descargue los detalles clave.




Precaución: NO comparta claves de acceso en foros públicos. Asegúrese de que esta información se almacena de forma segura.

2. Navegue hasta ESA con registros CEF configurados bajo **Administración del sistema > Suscripciones de registro** y haga clic en el nombre del **registro**.
3. Seleccione **Rollover de registro por tamaño de archivo** o **Rollover por tiempo** o ambos y los registros se enviarán en función de la condición que sea la primera verdadera.

Rollover by File Size:	<input type="text" value="10M"/> Maximum <i>(Add a trailing K or M to indicate size units)</i>
Rollover by Time:	<input type="text" value="Daily Rollover"/> Time of day: <input type="text" value="12:00"/> <i>(HH:MM)</i>

4. Seleccione AWS S3 Push e introduzca la información recopilada en el paso 1.

 AWS S3 Push
S3 Bucket Name: <input type="text" value="esa"/>
S3 Access Key: <input type="text" value="Axxxxxxxxxxxxxxxx"/>
S3 Secret Key: <input type="text" value="+xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"/>

5. Enviar y registrar cambios.

Si los registros CEF ya estaban presentes en el dispositivo, los archivos de registro existentes se enviarán inmediatamente y deberían aparecer en la cubeta S3 configurada. La siguiente programación de la transferencia de registro se realizará en función del tamaño y el tiempo de renovación configurados.

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Utilice los registros s3_client disponibles en el dispositivo para realizar un seguimiento de los registros que se están pulsando o de los errores que se conectan a ellos.

Successful log push

```
Fri Feb 19 11:21:38 2021 Info: S3_CLIENT: Uploaded 3 file(s) to the S3 Bucket esa for the subscription: cef
```

```
Fri Feb 19 12:03:16 2021 Info: S3_CLIENT: Uploading files to S3 Bucket esa for the subscription: cef
```

```
Fri Feb 19 12:03:22 2021 Info: S3_CLIENT: Uploaded 1 file(s) to the S3 Bucket esa for the subscription: cef
```

Unsuccessful log push

```
Fri Feb 19 12:34:10 2021 Info: S3_CLIENT: Uploading files to S3 Bucket esa for the subscription: cef
```

```
Fri Feb 19 12:34:11 2021 Warning: S3_CLIENT: ERROR: Upload Failed to S3 bucket esa. Reason: Failed to upload /data/pub/cef/s11.@20210219T120000.s to esa/s11.@20210219T120000.s: An error occurred (InvalidAccessKeyId) when calling the PutObject operation: The AWS Access Key Id you provided does not exist in our records.
```

```
Fri Feb 19 12:34:11 2021 Warning: S3_CLIENT: Uploading files to S3 Bucket esa encountered one or more failures for the subscription: cef.
```

```
Upload failed for the following:
```

```
[u's11.@20210219T120000.s']
```

Re-check your configuration.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Guías de usuario final de Cisco Email Security Appliance](#)
- [Notas de la versión de Cisco Email Security Appliance e información general](#)
- [CES Single Log Line \(SLL\)](#)
- [AWS creando cubeta S3](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)