Geconsolideerde Event Logs voor AWS S3 Push configureren

Inhoud

Inleiding

Dit document beschrijft hoe u de geconsolideerde logboeken voor gebeurtenissen die op een S3-emmer moeten worden geüpload op een e-mail security applicatie (ESA) of Cloud Email Security (CES), kunt configureren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ESA met Async OS 13.0 of hoger
- Administratieve toegang tot het apparaat
- Amazon Web Services (AWS)-account en toegang tot het maken en beheren van de S3-emmer

Gebruikte componenten

De informatie in dit document is gebaseerd op alle ondersteunde ESR-hardwaremodellen en virtuele apparaten die Async OS 13.0 of hoger gebruiken. Om de versieinformatie van het apparaat van de CLI te verifiëren, voert u de versieopdracht in. Selecteer in de GUI de optie **Monitor > systeemstatus**.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg ervoor dat u de potentiële impact van om het even welke configuratie begrijpt.

Achtergrondinformatie

Met ingang van Async OS 13.0 en hoger maakt het ESR de configuratie mogelijk van Unified Common Event Format (CEF)-gebaseerde vastlegging die bekend staat als Geconsolideerde Event Logs, die door SIEM-verkopers op grote schaal wordt gebruikt. Raadpleeg hier de aantekeningen bij de vrijgave van ESR 13.0.

CEF-logbestanden kunnen ook zo worden geconfigureerd dat ze naar een AWS S3-emmer worden geduwd, behalve dat ze handmatig kunnen worden gedownload, SCP en Syslog.

> **Opmerking:** De stappen die voor de AWS-configuratie zijn meegeleverd, zijn gebaseerd op informatie die beschikbaar is op het moment dat dit artikel wordt geschreven.

Configureren

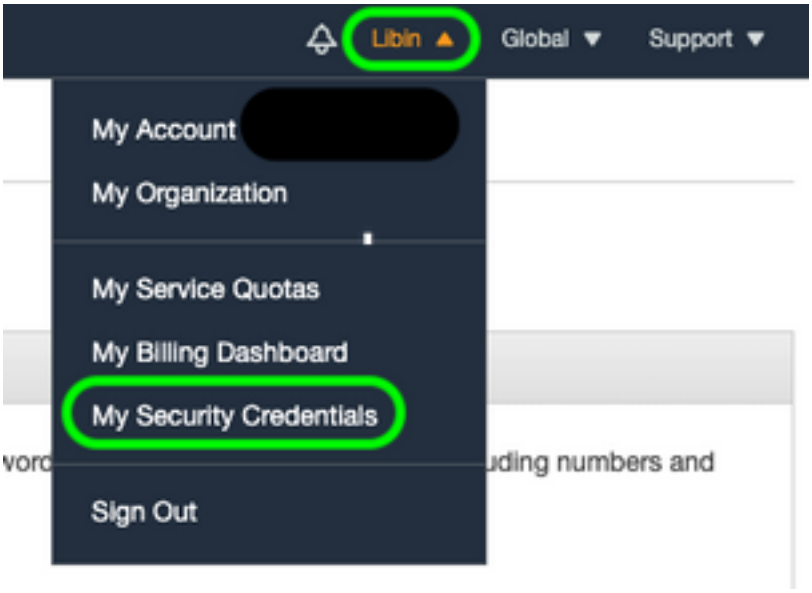
1. Navigeer naar AWS Cloud-console om S3 Bucket Name, S3 Access Key en S3 Secret Key te verzamelen.

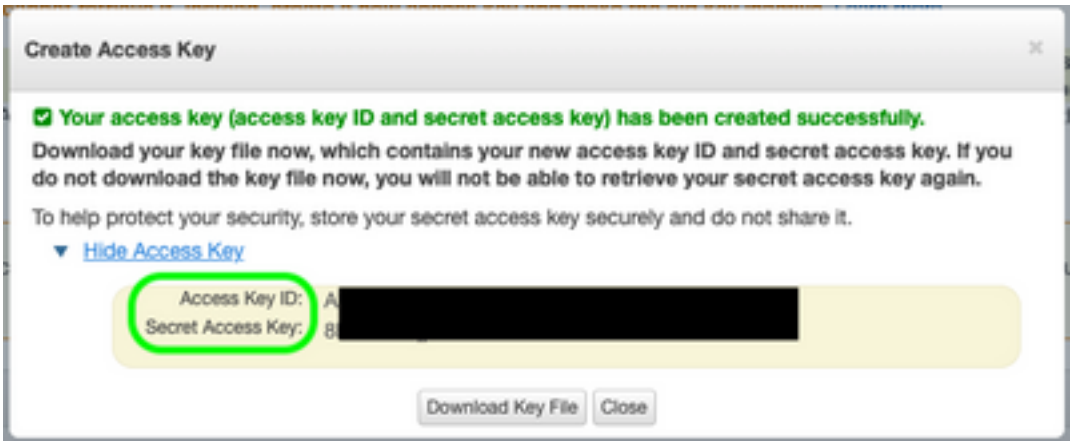
Voor S3 Bucket-naam:

Na inloggen op AWS Cloud, gebruik de optie Services om S3 te selecteren of gebruik de zoekbalk bovenaan om S3 te vinden. Maak een emmer met standaardopties of neem een naam op voor een van de bestaande emmers die gebruikt moeten worden.

Voor S3 Access Key en S3 security applicatie:

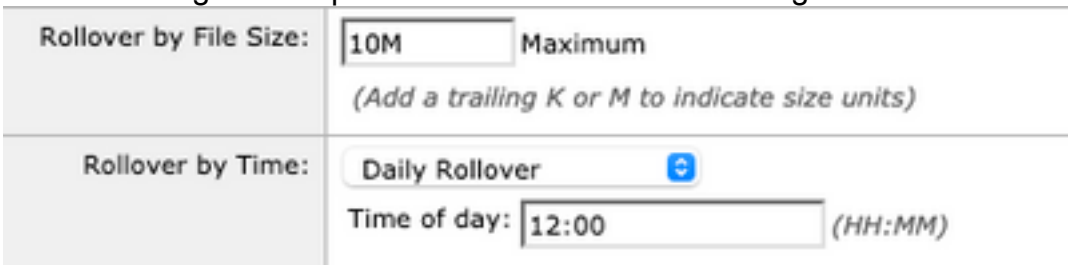
Klik rechtsboven op uw rekeningnaam en selecteer in de vervolgkeuzelijst "Mijn security geloofsbrieven". Klik in de open pagina op "Access Keys" (toegangssleutel-ID en geheime toegangssleutel). Nieuwe toegangssleutel maken, de belangrijkste details bekijken of downloaden.



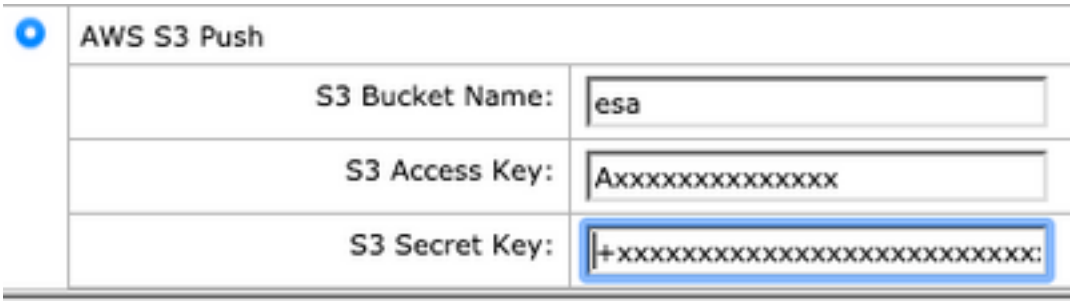


Voorzichtig: DEELT GEEN toegangssleutels op openbare forums. Zorg ervoor dat deze informatie goed wordt opgeslagen.

2. Navigeer naar ESA met CEF-logbestanden ingesteld onder **Systeembeheer > Log Abonneties** en klik op de naam van het **logbestand**.
3. Selecteer logrotatie **door bestandsgrootte** of **Rollover tegen tijd** of beide logbestanden worden geduwd op basis van welke conditie eerst geldt.



4. Selecteer AWS S3 Push, voer de informatie in die in Stap 1 verzameld werd.



5. Wijzigingen indienen en beloven.

Als CEF-logbestanden al op het apparaat aanwezig waren, worden de bestaande logbestanden direct geduwd en moeten ze in de S3-emmer worden weergegeven. Volgend schema van logdruk zal gebeuren op basis van de omloopgrootte en de ingestelde tijd.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Gebruik de s3_client logbestanden op het apparaat om logbestanden te volgen die geduwd worden of fouten die er op aansluiten.

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/sll.@20210219T120000.s to esa/sll.@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'sll.@20210219T120000.s']

Re-check your configuration.
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Cisco e-mail security eindgebruikershandleidingen
- Cisco e-mail security release opmerkingen en algemene informatie
- CES single-Log Line (SLL)
- AWS creëren S3-emmer
- **Technische ondersteuning en documentatie – Cisco Systems**