Configura log eventi consolidati per Push AWS S3

Sommario

Introduzione

In questo documento viene descritto come configurare i registri eventi consolidati da inviare a un bucket S3 su un'Email Security Appliance (ESA) o Cloud Email Security (CES).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ESA con Async OS 13.0 o superiore
- Accesso amministrativo all'accessorio
- Account Amazon Web Services (AWS) e accesso per creare e gestire il bucket S3

Componenti usati

Le informazioni di questo documento si basano su tutti i modelli hardware ESA supportati e sulle appliance virtuali che eseguono Async OS 13.0 o versioni successive. Per verificare le informazioni sulla versione dell'accessorio dalla CLI, immettere il comando version. Nella GUI, selezionare **Monitor > System Status** (Monitor > Stato del sistema).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dalla configurazione.

Premesse

A partire dalla versione Async OS 13.0, ESA consente la configurazione della registrazione basata su CEF (Unified Common Event Format), nota come Consolidated Event Log, ampiamente utilizzata dai fornitori SIEM. Fare riferimento qui alle note di rilascio del SEC 13.0.

I log CEF possono anche essere configurati per essere spostati in un bucket AWS S3 oltre al download manuale, SCP e Syslog push.

> **Nota:** I passaggi forniti per la configurazione di AWS si basano sulle informazioni disponibili al momento della scrittura di questo articolo.

Configurazione

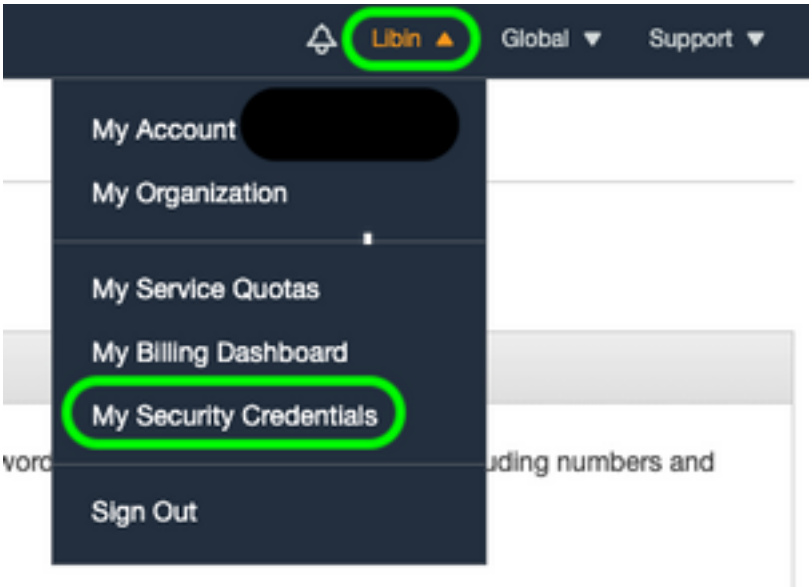
1. Passare alla console di AWS Cloud per raccogliere il nome del bucket S3, la chiave di accesso S3 e la chiave privata S3.

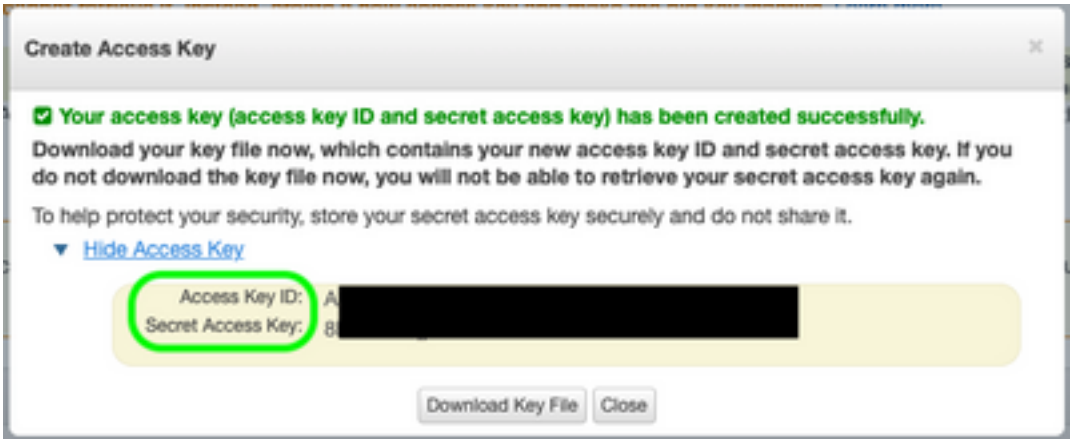
Nome bucket S3:

Una volta eseguito l'accesso a AWS Cloud, usare l'elenco a discesa Servizi per selezionare S3 o usare la barra di ricerca nella parte superiore per trovare S3. Creare il bucket con le opzioni predefinite o acquisire il nome di uno dei bucket esistenti da usare.

Per la chiave di accesso S3 e la chiave segreta S3:

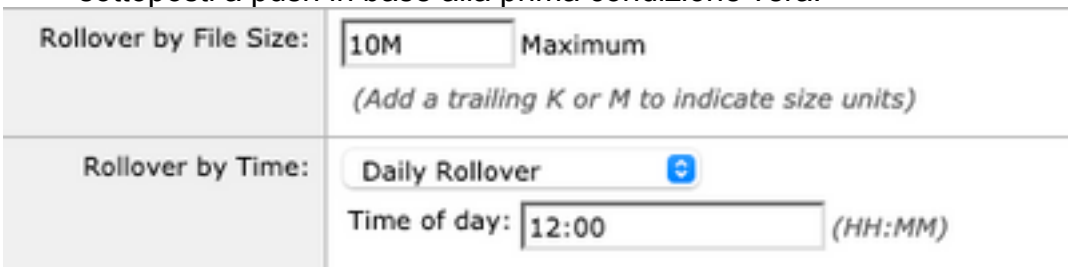
Fare clic sul nome dell'account in alto a destra e dal menu a discesa selezionare "Credenziali di sicurezza". Nella pagina di apertura, fare clic su "Tasti di accesso (ID chiave di accesso e chiave di accesso segreta). Creare una nuova chiave di accesso, visualizzarne o scaricarne i dettagli.



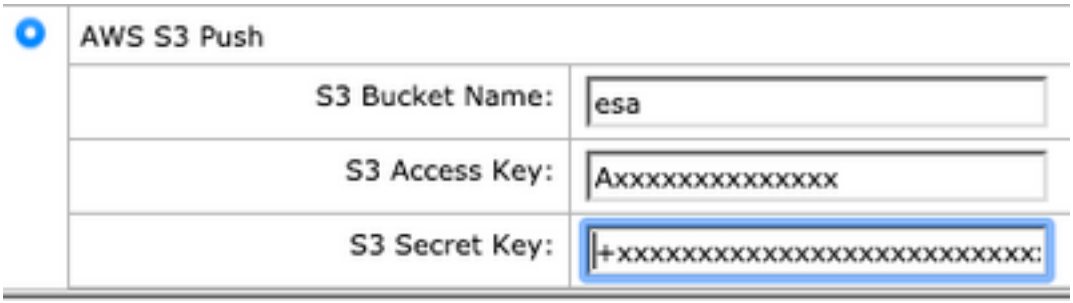


Attenzione: NON condividere i tasti di scelta nei forum pubblici. Assicurarsi che le informazioni siano archiviate in modo sicuro.

2. Passare a ESA con log CEF configurati in **Amministrazione di sistema > Sottoscrizioni log** e fare clic sul nome del **log**.
3. Selezionare **Rollover per dimensione file** o **Rollover per tempo** o entrambi; i log verranno sottoposti a push in base alla prima condizione vera.



4. Selezionare AWS S3 Push, inserire le informazioni raccolte nel passo 1.



5. Sottomettere e confermare le modifiche.

Se sull'accessorio erano già presenti registri CEF, i file di registro esistenti vengono immediatamente sottoposti a push e devono essere visualizzati nel bucket S3 configurato. La pianificazione successiva del log push verrà eseguita in base alle dimensioni e all'ora di rollover configurate.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Utilizzare i log s3_client disponibili nel dispositivo per tenere traccia dei log sottoposti a push o di eventuali errori che si connettono al dispositivo.

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.
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Guide per l'utente finale di Cisco Email Security Appliance
- Note di rilascio e informazioni generali su Cisco Email Security Appliance
- SLL (Single Log Line) CES
- AWS creazione bucket S3
- **Documentazione e supporto tecnico – Cisco Systems**