為AWS S3推送配置整合的事件日誌

目錄

簡介

本文檔介紹如何配置要推送到Email Security Appliance(ESA)或Cloud Email Security(CES)上的S3儲存桶的整合事件日誌。

必要條件

需求

思科建議您瞭解以下主題：

- 運行Async OS 13.0或更高版本的ESA
- 對裝置的管理訪問許可權
- Amazon Web Services(AWS)帳戶和訪問許可權，用於建立和管理S3儲存桶

採用元件

本文檔中的資訊基於所有受支援的ESA硬體型號和運行Async OS 13.0或更高版本的虛擬裝置。要從CLI驗證裝置的版本資訊，請輸入version命令。在GUI中，選擇**Monitor > System Status**。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何組態可能造成的影響。

背景資訊

從Async OS 13.0及更高版本開始，ESA允許配置SIEM供應商廣泛使用的統一公共事件格式(CEF)日誌記錄（稱為整合事件日誌）。請參閱此處的ESA 13.0發行說明。

除了手動下載、SCP和Syslog推送之外，還可以將CEF日誌配置為推送到AWS S3儲存桶。

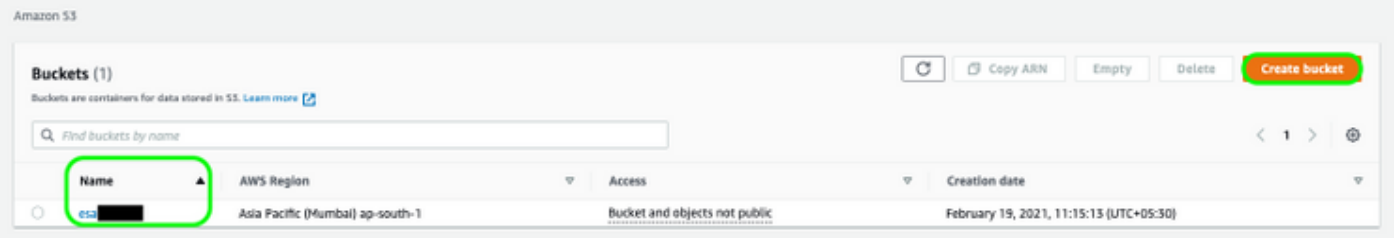
> **附註**：為AWS配置提供的步驟基於撰寫本文時可用的資訊。

設定

1.導航至AWS雲控制檯，以收集S3儲存段名稱、S3訪問金鑰和S3金鑰。

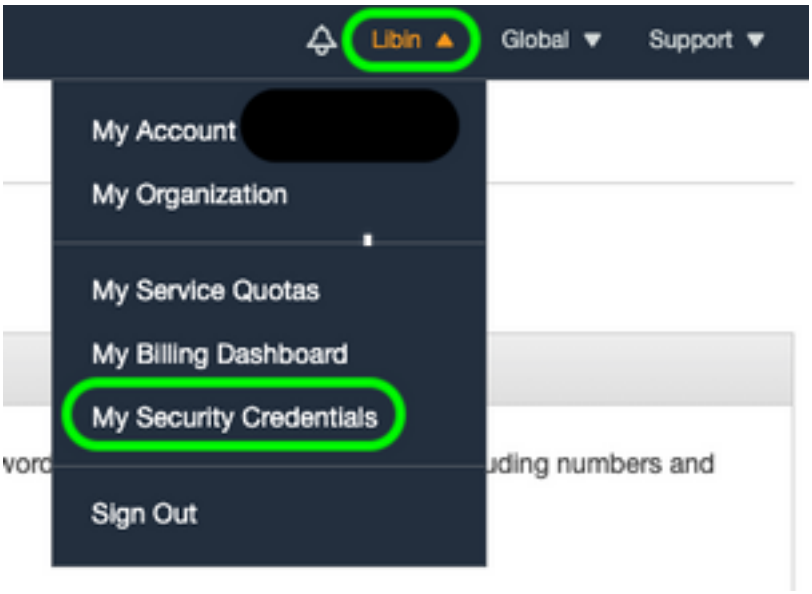
對於S3儲存桶名稱：

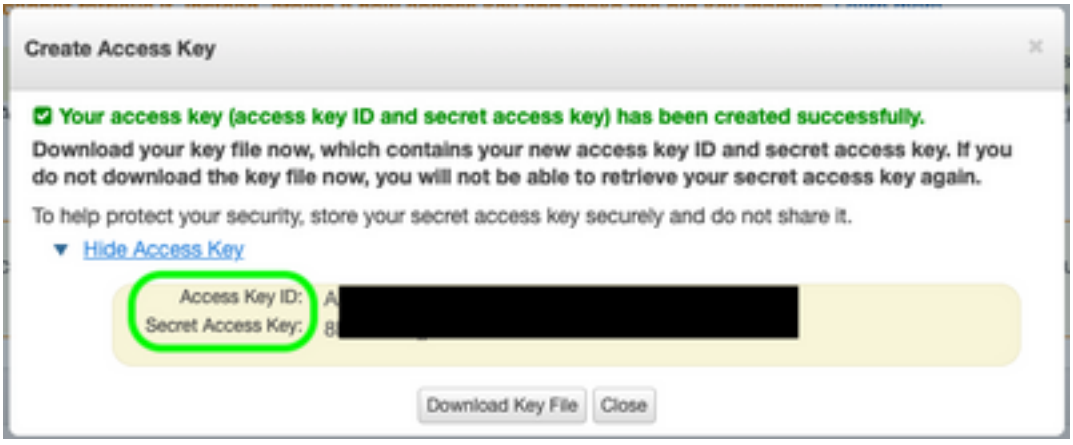
登入到AWS Cloud後，使用「服務」下拉選單選擇S3或使用頂部的搜尋欄查詢S3。使用預設選項或捕獲名稱為要使用的現有儲存桶之一建立儲存桶。



對於S3訪問金鑰和S3金鑰：

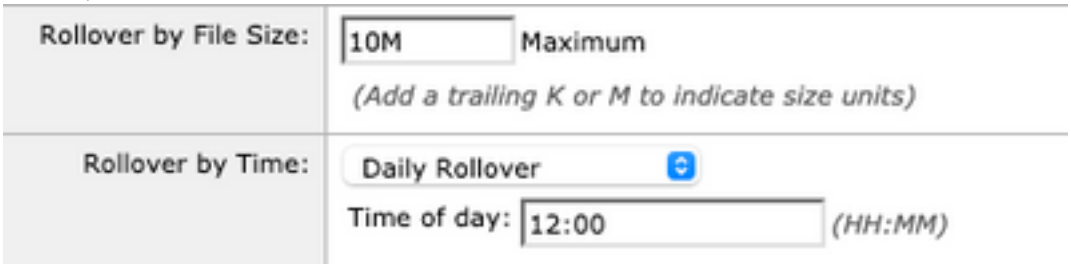
按一下右上方的帳戶名稱，然後從下拉選單中選擇「我的安全憑據」。在開啟頁面上，按一下「訪問金鑰（訪問金鑰ID和金鑰訪問金鑰）」。 建立新的訪問金鑰，檢視或下載金鑰詳細資訊。



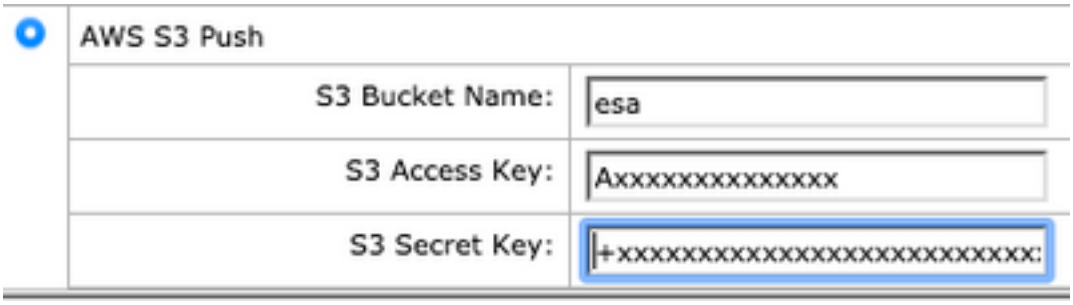


注意：請勿在公共論壇上共用訪問金鑰。確保安全地儲存此資訊。

2. 導航到ESA，在**系統管理>日誌訂閱**下配置了CEF日誌，然後按一下日誌的**名稱**。
3. 選擇log **Rollover by File Size**或**Rollover by Time**或同時選擇兩者，系統會根據第一個為真的情況推送日誌。



4.選擇AWS S3 Push，輸入在步驟1中收集的資訊。



5.提交和提交更改。

如果裝置上已經存在CEF日誌，則現有日誌檔案將立即推送，並顯示在配置的S3儲存桶中。根據配置的滾動更新大小和時間，將執行下一個日誌推送計畫。

驗證

使用本節內容，確認您的組態是否正常運作。

利用裝置上可用的s3_client日誌，以跟蹤正在推送的日誌或連線到該日誌的任何錯誤。

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.
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 思科電子郵件安全裝置最終使用手冊
- 思科電子郵件安全裝置版本說明和一般資訊
- CES單一記錄線路(SLL)
- AWS建立S3儲存桶
- **技術支援與文件 - Cisco Systems**