Konsolidierte Ereignisprotokolle für AWS S3 Push konfigurieren

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[Konfiguration](#)
[Überprüfung](#)
[Fehlerbehebung](#)
[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie konsolidierte Ereignisprotokolle so konfiguriert werden, dass sie auf einer E-Mail-Security-Appliance (ESA) oder Cloud E-Mail Security (CES) in eine S3-Gruppe verschoben werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ESA mit Async OS 13.0 oder höher
- Administratorzugriff auf die Appliance
- Amazon Web Services (AWS)-Konto und Zugriff zum Erstellen und Verwalten der S3-Bucket

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf allen unterstützten ESA-Hardwaremodellen und virtuellen Appliances, auf denen Async OS 13.0 oder höher ausgeführt wird. Um die Versionsinformationen der Appliance über die CLI zu überprüfen, geben Sie den Befehl version ein. Wählen Sie in der GUI **Monitor > Systemstatus aus**.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen einer Konfiguration verstehen.

Hintergrundinformationen

Ab Async OS 13.0 und höher ermöglicht die ESA die Konfiguration der CEF-basierten Protokollierung (Unified Common Event Format), die auch als konsolidierte Ereignisprotokolle bezeichnet wird und bei SIEM-Anbietern häufig zum Einsatz kommt. Weitere Informationen finden Sie hier in den Versionshinweisen zum ESA 13.0.

CEF-Protokolle können auch so konfiguriert werden, dass sie neben dem manuellen Download, SCP und Syslog-Push an eine AWS S3-Bucket gesendet werden.

> **Hinweis:** Die für die AWS-Konfiguration bereitgestellten Schritte basieren auf Informationen, die zum Zeitpunkt der Erstellung dieses Artikels verfügbar sind.

Konfiguration

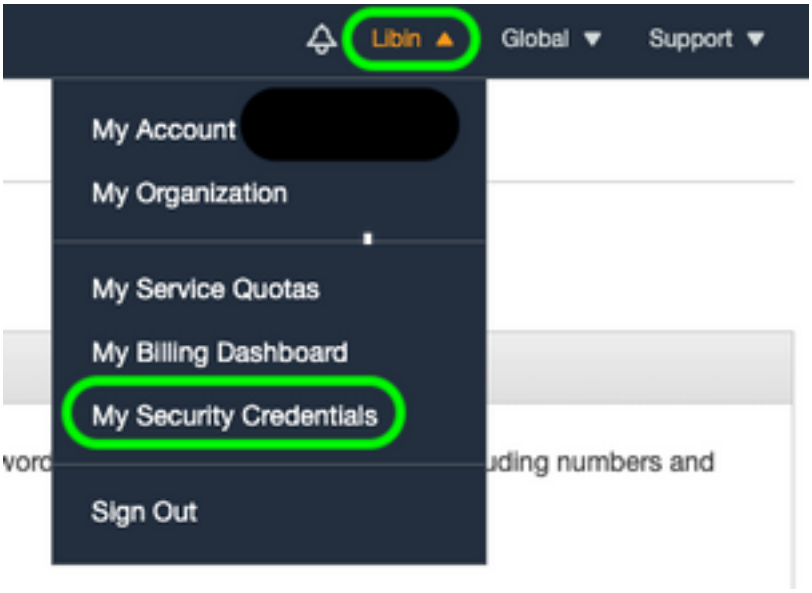
1. Navigieren Sie zur AWS-Cloud-Konsole, um den S3-Bucketnamen, den S3-Zugriffsschlüssel und den S3-Geheimschlüssel zu erfassen.

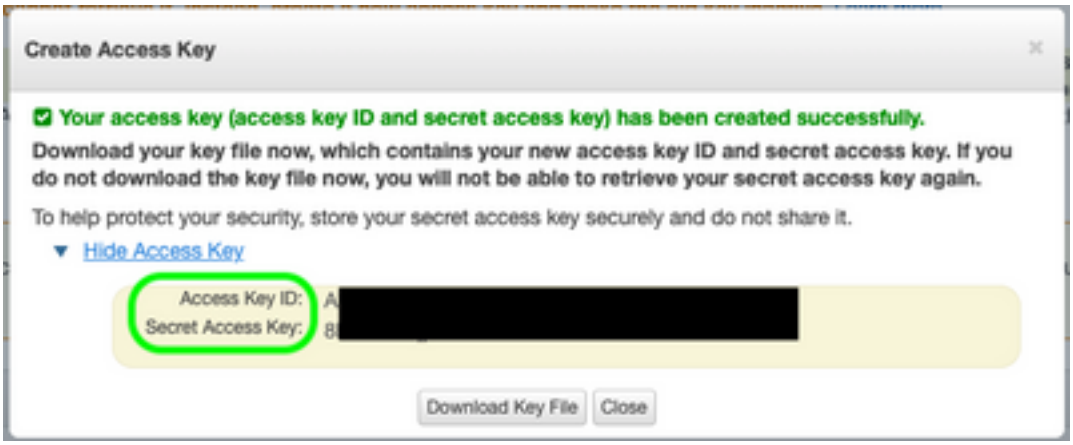
Für S3-Bucket-Namen:

Wenn Sie sich in der AWS-Cloud angemeldet haben, wählen Sie im Dropdown-Menü Services (Dienste) S3 aus, oder suchen Sie in der Suchleiste oben nach S3. Erstellen Sie eine Gruppe mit Standardoptionen oder einen Namen für die Erfassung einer vorhandenen Gruppe.

Für S3-Zugriffsschlüssel und S3-Geheimschlüssel:

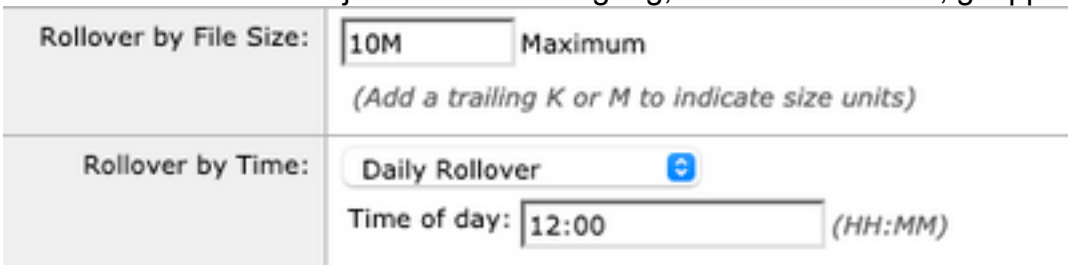
Klicken Sie oben rechts auf Ihren Kontonamen, und wählen Sie im Dropdown-Menü "Meine Sicherheitsanmeldeinformationen" aus. Klicken Sie auf der geöffneten Seite auf "Zugriffsschlüssel (Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel)". Erstellen eines neuen Zugriffsschlüssels, Anzeigen oder Herunterladen der Schlüsseldetails



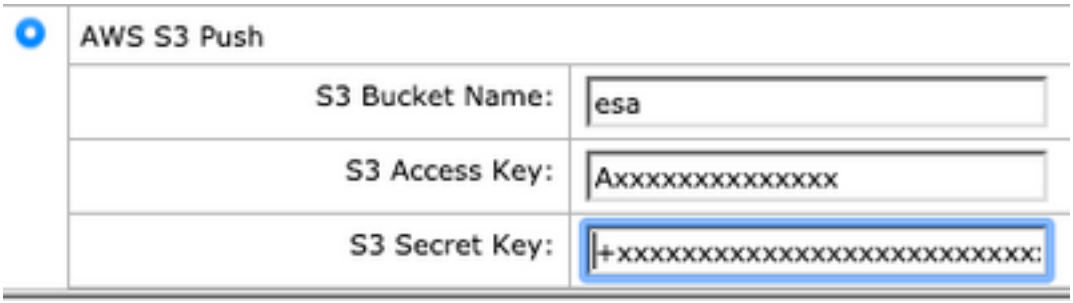


Vorsicht: Teilen Sie KEINE Zugriffsschlüssel in öffentlichen Foren. Stellen Sie sicher, dass diese Informationen sicher gespeichert sind.

2. Navigieren Sie zu ESA mit CEF-Protokollen, die unter **Systemverwaltung > Protokoll-Subscriptions** konfiguriert sind, und klicken Sie auf den Namen des **Protokolls**.
3. Wählen Sie Log **Rollover nach Dateigröße** oder **Rollover nach Zeit** oder beide aus, und die Protokolle werden je nach der Bedingung, die zuerst wahr ist, getippt.



4. Wählen Sie AWS S3 Push aus, und geben Sie die in Schritt 1 erfassten Informationen ein.



5. Änderungen senden und bestätigen.

Wenn auf der Appliance bereits CEF-Protokolle vorhanden waren, werden die vorhandenen Protokolldateien sofort gesendet und sollten in der konfigurierten S3-Bucket angezeigt werden. Der nächste Zeitplan für das Push-Protokoll wird basierend auf der Größe und der konfigurierten Zeit des Rollovers ausgeführt.

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Verwenden Sie die s3_client-Protokolle, die auf dem Gerät verfügbar sind, um die Protokolle zu verfolgen, die gesendet werden, oder alle Fehler, die eine Verbindung mit dem Gerät herstellen.

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.
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Versionshinweise und allgemeine Informationen zur Cisco Email Security Appliance
- CES Single Log Line (SLL)
- AWS erstellt S3-Bucket
- **Technischer Support und Dokumentation für Cisco Systeme**