AWS S3プッシュの統合イベントログの設定

内容

概要

このドキュメントでは、Eメールセキュリティアプライアンス(ESA)またはクラウドEメールセキュリティ(CES)のS3バケットにプッシュされる統合イベントログを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Async OS 13.0以降を実行するESA
- アプライアンスへの管理アクセス
- アマゾンウェブサービス(AWS)アカウントと、S3バケットを作成および管理するためのアクセス

使用するコンポーネント

このドキュメントの情報は、サポートされているすべてのESAハードウェアモデルと、Async OS 13.0以降を実行する仮想アプライアンスに基づいています。CLIからアプライアンスのバージョン情報を確認するには、versionコマンドを入力します。GUIで、[Monitor] > [**System Status]の順に選択します**。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。ネットワークが稼働中の場合は、設定が及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

Async OS 13.0以降では、ESAでは、SIEMベンダーによって広く使用されている統合イベントログと呼ばれるUnified Common Event Format(CEF)ベースのロギングを設定できます。ESA 13.0リリースノートを参照してください。

CEFログは、手動ダウンロード、SCP、およびSyslogプッシュとは別に、AWS S3バケットにプッシュするように設定することもできます。

> **注**：AWSの設定に関する手順は、この記事の作成時点で入手可能な情報に基づいています。

設定

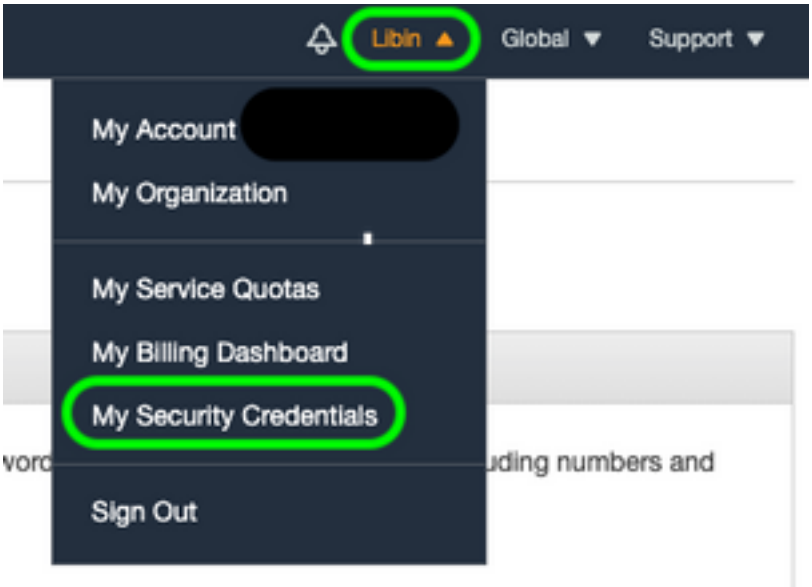
1. AWS Cloudコンソールに移動して、S3バケット名、S3アクセスキー、およびS3秘密キーを収集します。

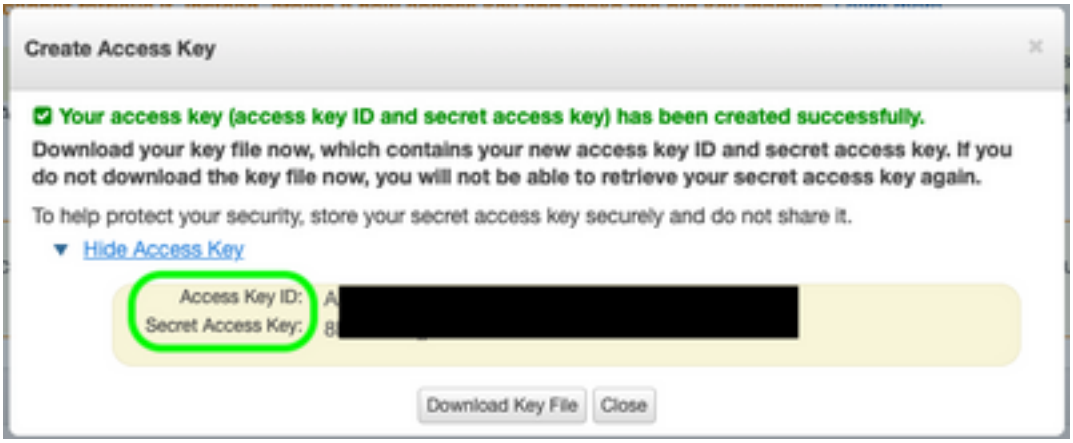
S3バケット名：

AWS Cloudにログインしたら、[サービス]ドロップダウンを使用してS3を選択するか、上部の検索バーを使用してS3を検索します。デフォルトのオプションを使用してバケットを作成するか、使用する既存のバケットの1つをキャプチャします。

S3アクセスキーとS3秘密キーの場合：

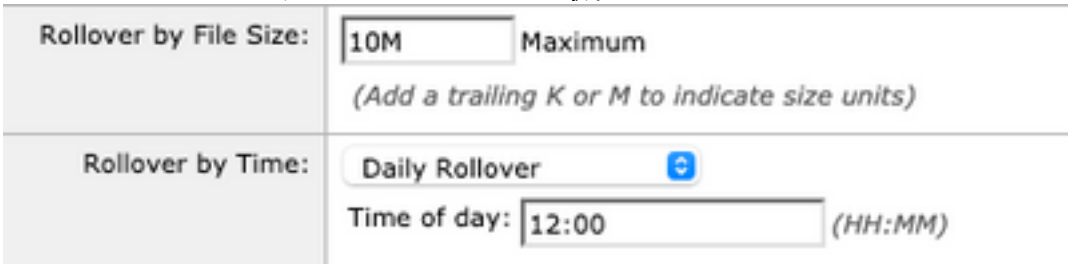
右上のアカウント名をクリックし、ドロップダウンから[My Security Credentials]を選択します。開いているページで、[Access keys (access key ID and secret access key)]をクリックします。新しいアクセスキーの作成、キーの詳細の表示またはダウンロード



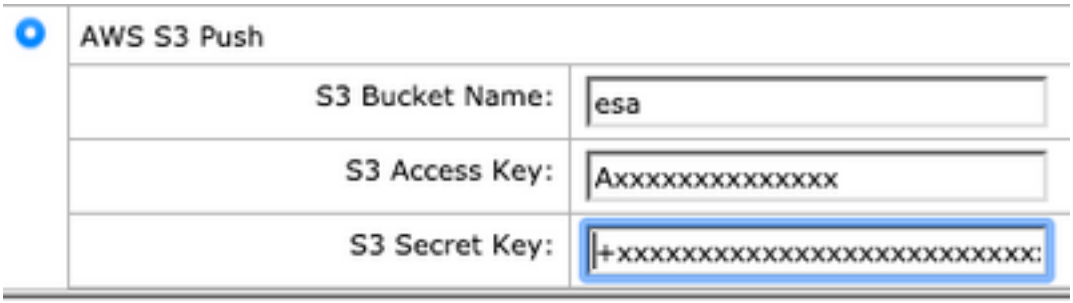


注意：公開フォーラムでアクセスキーを共有しないでください。この情報が安全に保存されていることを確認します。

2. [System Administration] > [Log Subscriptions]で設定したCEFログを使用してESAに移動し、ログの名前をクリックします。
3. ログを選択する「**ファイルのサイズによるロールオーバ**」または「**時間によるロールオーバ**」を選択します。どちらの条件が最初に満たされるかに基づいてログがプッシュされます。



4. [AWS S3 Push]を選択し、ステップ1で収集した情報を入力します。



5.変更を送信して確定します。

CEFログがアプライアンスにすでに存在する場合、既存のログファイルは即座にプッシュされ、設定されているS3バケットに表示されます。ログプッシュの次のスケジュールは、設定されたロールオーバーサイズと時間に基づいて実行されます。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

デバイスで使用可能なs3_clientログを使用して、プッシュされるログまたはデバイスに接続するエラーを追跡します。

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.
```

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco Eメールセキュリティアプライアンスエンドユーザガイド
- Cisco Eメールセキュリティアプライアンスリリースノートと一般情報
- CESシングルログ回線(SLL)
- AWS S3バケットの作成
- **テクニカル サポートとドキュメント – Cisco Systems**