Configure Consolidated Event Logs for AWS S3 Push

Contents

Introduction

This document describes how to configure consolidated event logs to be pushed to an S3 bucket on an Email Security Appliance (ESA) or Cloud Email Security (CES).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ESA running Async OS 13.0 or higher
- Administrative access to the appliance
- Amazon Web Services (AWS) account and access to create and manage the S3 bucket

Components Used

The information in this document is based on all supported ESA hardware models and virtual appliances running Async OS 13.0 or higher. In order to verify version information of the appliance from the CLI, enter the version command. In the GUI, select **Monitor > System Status**.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any configuration.

Background Information

Starting Async OS 13.0 and above, ESA allows for the configuration of Unified Common Event Format (CEF)-based logging known as Consolidated Event Logs which is widely used by SIEM

vendors. Please refer to the ESA 13.0 release notes here.

CEF logs can also be configured to be pushed to an AWS S3 bucket apart from manual download, SCP and Syslog push.

> **Note**: Steps provided for AWS configuration are based on information available at the time of this article being written.

Configure

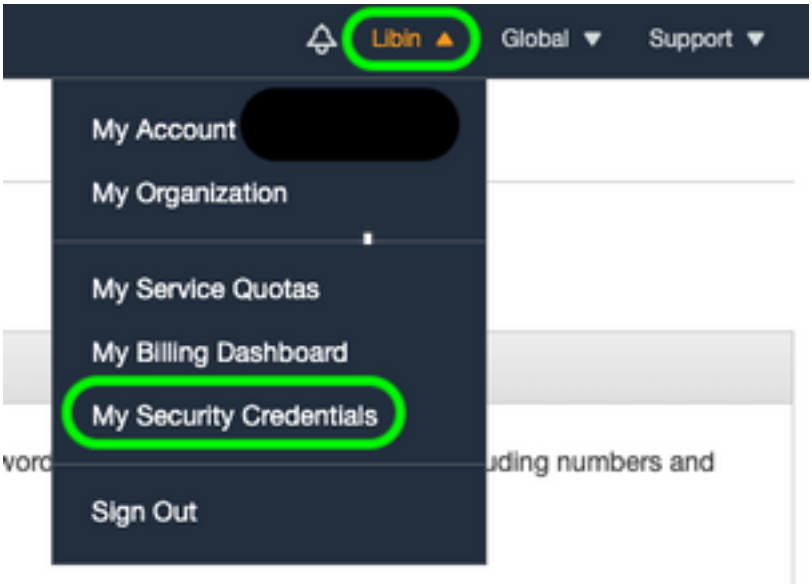
1. Navigate to AWS Cloud console in order to collect S3 Bucket Name, S3 Access Key and S3 Secret Key.

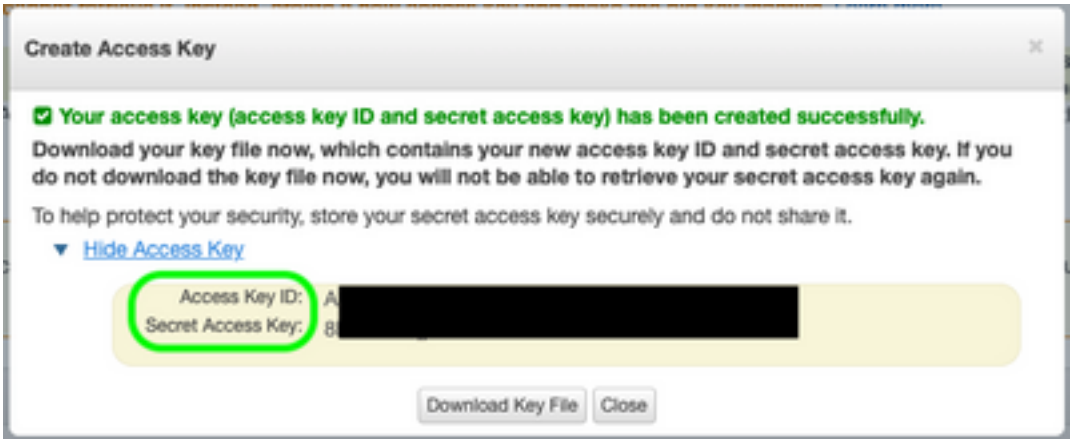
For S3 Bucket Name:

Once logged in on AWS Cloud, use the Services dropdown to select S3 or use the search bar at the top to find S3. Create bucket with default options or capture name for one of the existing buckets to be used.

For S3 Access Key and S3 Secret Key:

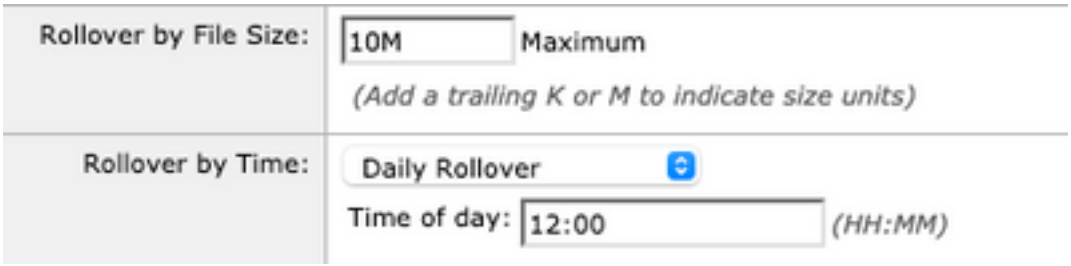
Click on your account name at the top right and from the drop down select “My Security Credentials”. On the open page, click “Access keys (access key ID and secret access key). Create New Access Key, view or download the key details.



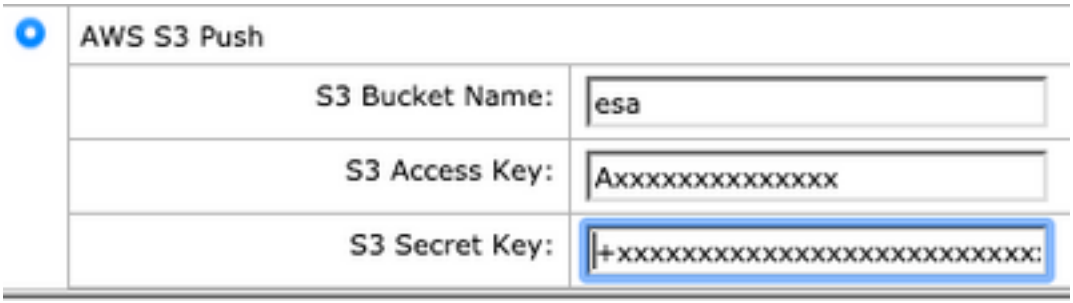


Caution: Do NOT share access keys on public forums. Ensure this information is stored securely.

2. Navigate to ESA with CEF logs configured under **System Administration > Log Subscriptions** and click on the name of the **log**.
3. Select log **Rollover by File Size** or **Rollover by Time** or both and logs will be pushed based on whichever condition is first true.



4. Select AWS S3 Push, enter the information collected in Step 1.



5. Submit and Commit changes.

If CEF logs were already present on the appliance, the existing log files will be pushed immediately and should appear in the S3 bucket configured. Next schedule of log push will happen based on the rollover size and time configured.

Verify

Use this section in order to confirm that your configuration works properly.

Utilize s3_client logs available on the device in order to track logs being pushed or any errors that connect to it.

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.
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- Cisco Email Security Appliance End-User Guides
- Cisco Email Security Appliance Release Notes and General Information
- CES Single Log Line (SLL)
- AWS Creating S3 Bucket
- **Technical Support & Documentation - Cisco Systems**