配置AWS S3推送的整合事件日志

目录

简介

本文档介绍如何配置要推送到邮件安全设备(ESA)或云邮件安全(CES)上S3存储桶的整合事件日志。

先决条件

要求

Cisco 建议您了解以下主题：

- 运行异步OS 13.0或更高版本的ESA
- 对设备的管理访问
- Amazon Web Services(AWS)帐户和访问权限，用于创建和管理S3存储桶

使用的组件

本文档中的信息基于运行Async OS 13.0或更高版本的所有支持的ESA硬件型号和虚拟设备。要从CLI验证设备的版本信息，请输入version命令。在GUI中，选择“监**控”>“系统状态**”。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解任何配置的潜在影响。

背景信息

启动Async OS 13.0及更高版本后，ESA允许配置基于统一通用事件格式(CEF)的日志记录，称为统一事件日志，SIEM供应商广泛使用。请参阅此处的ESA 13.0版本说明。

除手动下载、SCP和系统日志推送外，CEF日志还可配置为推送到AWS S3存储桶。

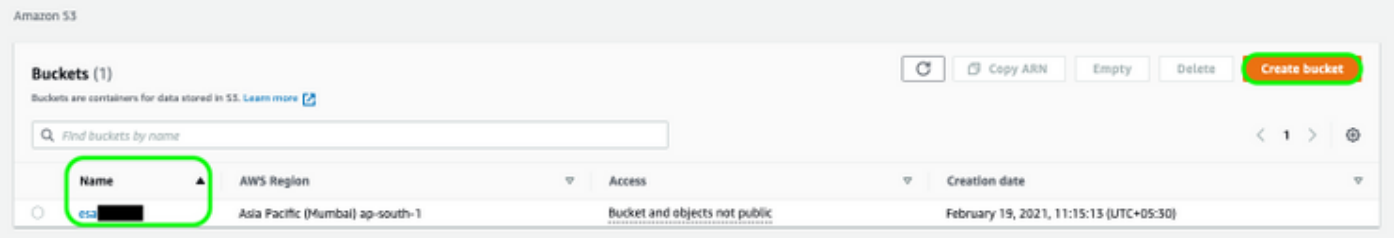
> **注意：**为AWS配置提供的步骤基于撰写本文时可用的信息。

配置

1.导航至AWS云控制台以收集S3存储段名称、S3访问密钥和S3密钥。

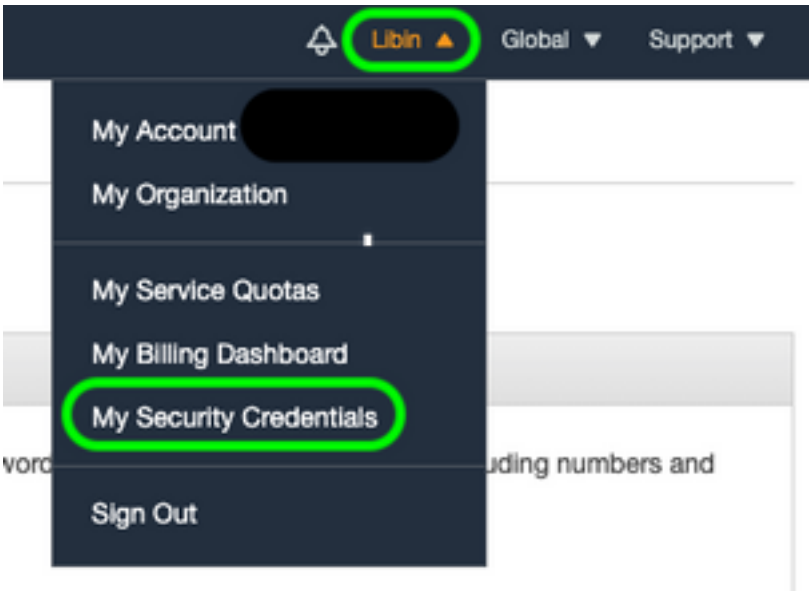
对于S3存储段名称：

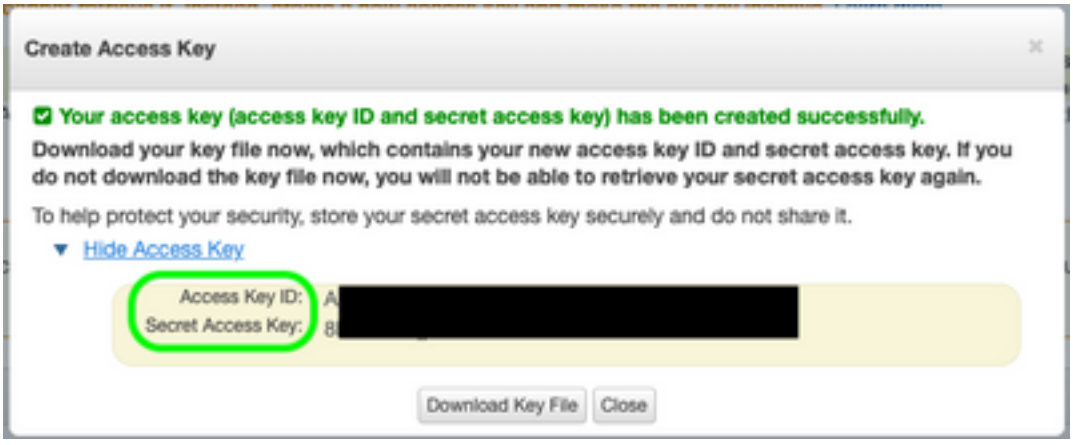
登录AWS云后，使用“服务”下拉列表选择S3，或使用顶部的搜索栏查找S3。创建包含默认选项的存储桶或捕获名称，以用于要使用的现有存储桶之一。



对于S3访问密钥和S3密钥：

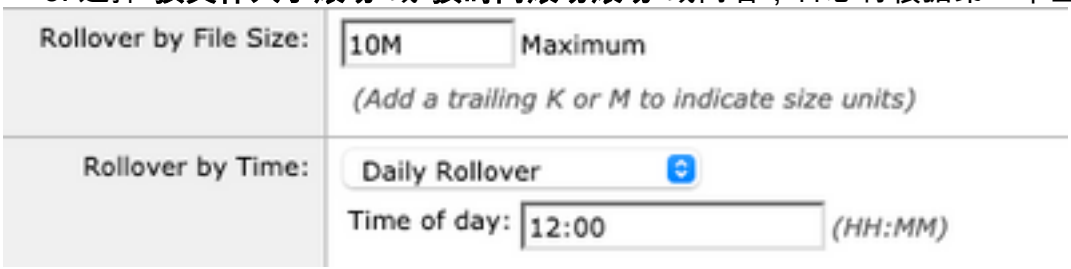
点击右上角的帐户名称，然后从下拉菜单中选择“My Security Credentials”。在打开的页面上，点击“访问密钥（访问密钥ID和密钥访问密钥）”。 创建新访问密钥，查看或下载密钥详细信息。



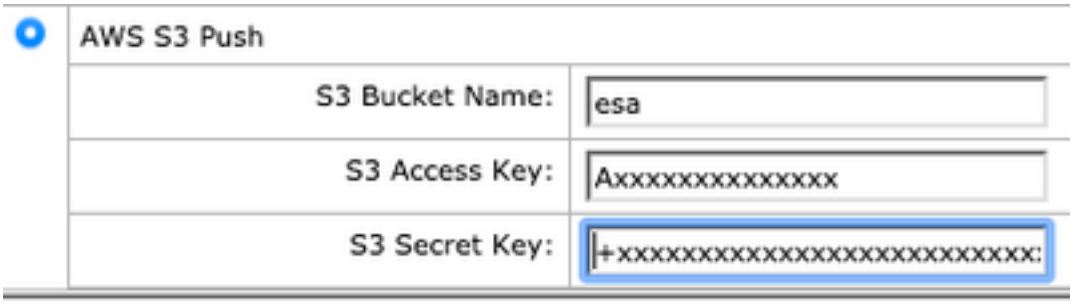


警告：请勿在公共论坛上共享访问密钥。确保此信息存储安全。

2. 导航至在System Administration > Log Subscriptions下配置了CEF日**志的ESA，然**后单击日志的名**称**。
3. 选择“**按文件大小滚动**”或“**按时间滚动滚动**”或两者，日志将根据第一个正确的情况推送。



4.选择AWS S3推送，输入在步骤1中收集的信息。



5.提交并提交更改。

如果设备上已存在CEF日志，则会立即推送现有日志文件，并应显示在配置的S3存储桶中。根据配置的滚动更新大小和时间，将执行下一个日志推送计划。

验证

使用本部分可确认配置能否正常运行。

利用设备上可用的s3_client日志来跟踪推送的日志或连接到它的任何错误。

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.
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 思科邮件安全设备最终用户指南
- 思科邮件安全设备版本说明和一般信息
- CES单日志行(SLL)
- AWS创建S3存储桶
- **技术支持和文档 - Cisco Systems**