AWS S3 Push에 대한 통합 이벤트 로그 구성

목차

소개

이 문서에서는 ESA(Email Security Appliance) 또는 CES(Cloud Email Security)의 S3 버킷에 푸시될 통합 이벤트 로그를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Async OS 13.0 이상을 실행하는 ESA
- 어플라이언스에 대한 관리 액세스
- Amazon Web Services(AWS) 계정 및 S3 버킷 생성 및 관리 액세스

사용되는 구성 요소

이 문서의 정보는 지원되는 모든 ESA 하드웨어 모델 및 Async OS 13.0 이상을 실행하는 가상 어플라이언스를 기반으로 합니다.CLI에서 어플라이언스의 버전 정보를 확인하려면 version 명령을 입력합니다.GUI에서 Monitor(모니터) **> System Status(시스템 상태)를** 선택합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 컨피그레이션의 잠재적인 영향을 이해해야 합니다.

배경 정보

Async OS 13.0 이상을 시작으로, ESA는 SIEM 공급업체에서 널리 사용되는 Consolidated Event Logs라고 하는 CEF(Unified Common Event Format) 기반 로깅을 구성할 수 있습니다.여기에서 ESA 13.0 릴리스 정보를 참조하십시오.

CEF 로그는 수동 다운로드, SCP 및 Syslog 푸시를 제외하고 AWS S3 버킷에 푸시되도록 구성할 수도 있습니다.

> **참고:**AWS 구성에 대해 제공되는 단계는 이 문서가 작성될 때 제공되는 정보를 기반으로 합니다.

구성

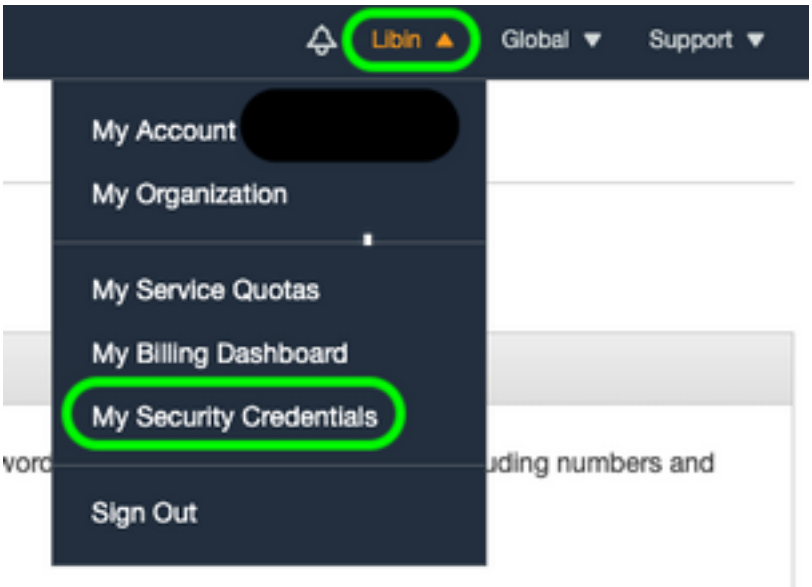
1. S3 버킷 이름, S3 액세스 키 및 S3 비밀 키를 수집하려면 AWS 클라우드 콘솔로 이동합니다.

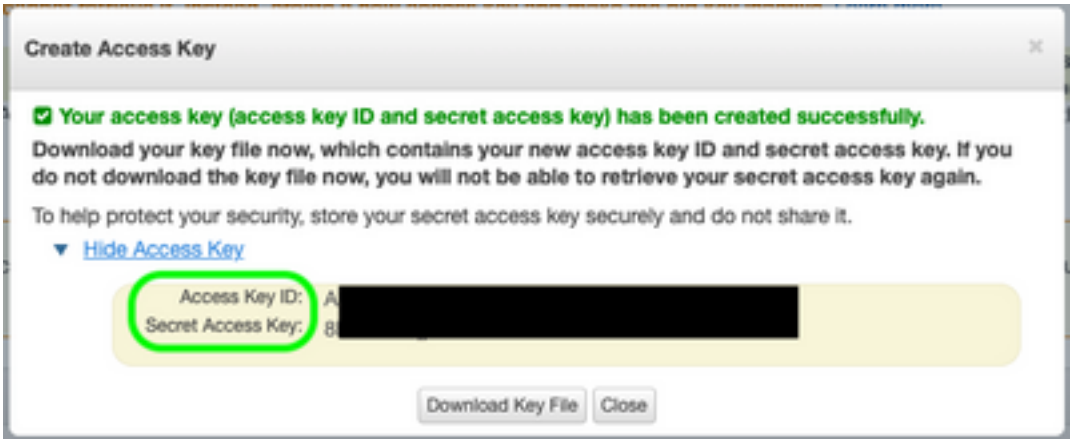
S3 버킷 이름:

AWS Cloud에 로그인한 후 서비스 드롭다운을 사용하여 S3를 선택하거나 맨 위의 검색 바를 사용하여 S3를 찾습니다. 사용할 기존 버킷 중 하나에 대한 기본 옵션 또는 캡처 이름을 사용하여 버킷을 생성합니다.

S3 액세스 키 및 S3 비밀 키의 경우:

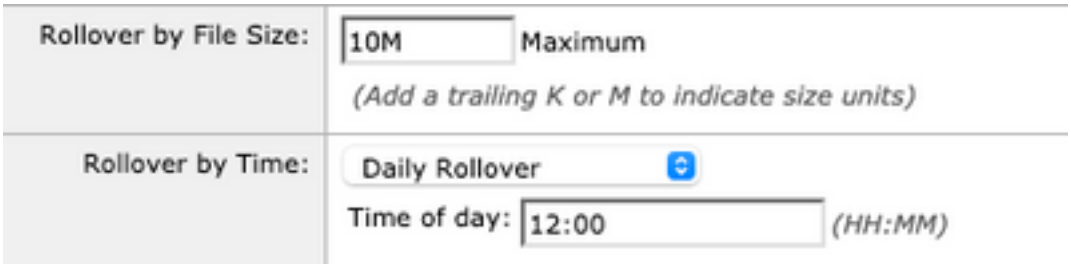
오른쪽 상단의 계정 이름을 클릭하고 드롭다운에서 "My Security Credentials(내 보안 자격 증명)"를 선택합니다.열려 있는 페이지에서 "Access keys (access key ID and secret access key)(액세스 키 ID 및 비밀 액세스 키)를 클릭합니다. 새 액세스 키를 만들거나 키 세부 정보를 보거나 다운로드합니다.



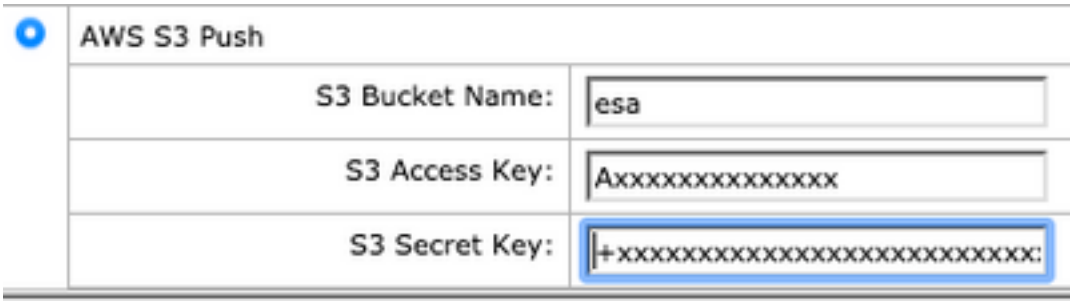


주의:공개 포럼에서 액세스 키를 공유하지 마십시오.이 정보가 안전하게 저장되었는지 확인합니다.

2. **System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션)**에서 구성된 ESA with CEF logs configured(CEF 로그가 있는 ESA로 이동하고 **로그** 이름을 클릭합니다.
3. Log Rollover **by File Size(파일 크기별** 롤오버) 또는 **Rollover by Time(시간별 롤오버)**을 선택하거나 둘 다 선택한 다음 첫 번째 True인 조건을 기준으로 로그가 푸시됩니다.



4. AWS S3 푸시를 선택하고 1단계에서 수집한 정보를 입력합니다.



5. 변경사항을 실행하고 커밋합니다.

CEF 로그가 어플라이언스에 이미 있는 경우, 기존 로그 파일은 즉시 푸시되며 구성된 S3 버킷에 나타나야 합니다.다음 로그 푸시 일정은 구성된 롤오버 크기 및 시간에 따라 이루어집니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

디바이스에서 사용 가능한 s3_client 로그를 활용하여 푸시되는 로그 또는 디바이스에 연결된 오류를 추적합니다.

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.
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco Email Security Appliance 최종 사용자 가이드
- Cisco Email Security Appliance 릴리스 정보 및 일반 정보
- CES SLL(Single Log Line)
- S3 버킷 생성 AWS
- **기술 지원 및 문서 – Cisco Systems**