Debian 기반 시스템의 Cisco Secure Endpoint Linux Connector

목차

이 문서에서는 관리자가 Debian 기반 시스템에 Cisco Secure Endpoint Linux 커넥터를 구축하기 위해 수행할 수 있는 변경 사항 및 단계에 대해 설명합니다.

- Debian 10 이상.
- Ubuntu 18.04 이상

최소 OS 요구 사항

OS 호환성은 Cisco Secure Endpoint Linux Connector OS 호환성 문서를 참조하십시오.

환경 설정

Debian 기반 시스템의 Linux 커넥터는 파일 및 네트워크 모니터링에 eBPF를 사용합니다. 시스템에 올바른 linux 헤더 소프트웨어 패키지가 설치되어 있어야 합니다. 그렇지 않으면 커넥터에서 결함 11(시스템 종속성 없음)을 발생시키고 파일 및 네트워크 모니터링 없이 성능이 저하된 상태로 실행됩니다. 이 결함 해결에 대한 지침은 Linux 커널-디바이스 결함 문서에서 을 참조하십시오.

종속성

Linux 커넥터는 Debian 기반 시스템의 기본 설치에 포함된 시스템 패키지에 종속되지만 종속성이 누락된 경우 다음 메시지가 나타납니다.

```
ciscoampconnector depends on
```

Linux 커넥터에 필요한 누락된 종속성을 설치하려면 다음 명령을 사용합니다.

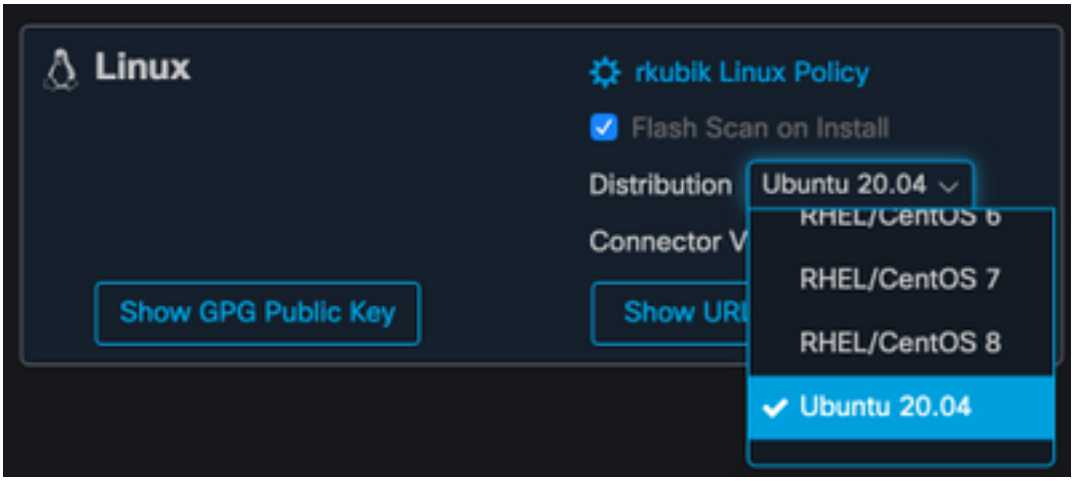
```
sudo apt install
```

DEB 패키지 확인

Linux 커넥터 DEB 패키지에는 다운로드한 소프트웨어 패키지가 Cisco에 속하는지 확인하는 서명이 포함되어 있습니다.

DEB 패키지 다운로드

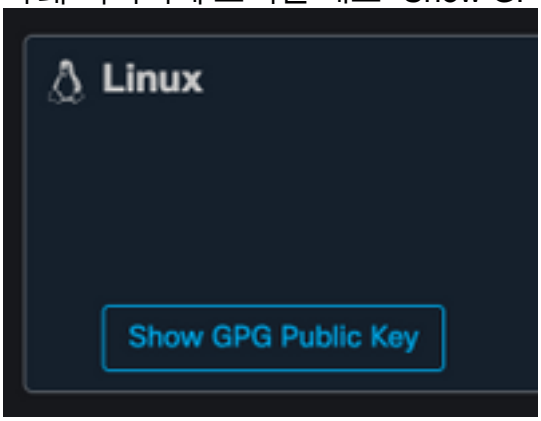
1. AMP for Endpoints 콘솔에 액세스합니다.
2. Debian 기반 시스템용 DEB 패키지를 다운로드합니다.



3. DEB 패키지를 Debian 기반 시스템으로 전송합니다. 예를 들면 다음과 같습니다. amp_ciscoampconnector.deb

GPG 공개 키 검색

1. 아래 이미지에 표시된 대로 "Show GPG Public Key(GPG 공개 키 표시)" 버튼을 클릭합니다.



2. 커넥터 버전이 1.17.0 이전이면 공개 키를 다운로드하여 전송하거나 컴퓨터에 복사합니다. 예를 들면 다음과 같습니다. cisco.gpg. 커넥터 버전이 1.17.0 이상인 경우 GPG 키는 /opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-KEY-cisco-amp에서 사용할 수 있습니다.

DEB 패키지 확인

DEB 패키지는 debsigs 툴을 사용하여 서명되며 debsig-verify를 사용하여 확인할 수 있습니다.

1. debsig-verify 툴을 설치합니다.
   ```
   sudo apt-get install debsig-verify
   ```
2. Cisco GPG Public Key를 Debsigs 키링으로 가져옵니다. **참고:** 버전 1.17.0부터 2단계를 건너뛸 수 있도록 debsig.gpg 파일이 자동으로 생성됩니다.
   ```
   sudo mkdir -p /usr/share/debsig/keyrings/914E5BE0F2FD178F sudo gpg --dearmor --output
   /usr/share/debsig/keyrings/914E5BE0F2FD178F/debsig.gpg cisco.gpg
   ```

3. 정책 디렉터리를 만듭니다.
   ```
   sudo mkdir -p /etc/debsig/policies/914E5BE0F2FD178F
   ```
4. 아래 정책 내용을 새 파일 "/etc/debsig/policies/914E5BE0F2FD178F/ciscoampconnector.pol"에 복사합니다.

5. debsig-verify로 DEB 서명을 확인합니다.
   ```
   debsig-verify amp_ciscoampconnector.deb
   ```
   출력은 다음과 같습니다.
   ```
   debsig: Verified package from 'Cisco AMP for Endpoints' (Debsig)
   ```

참고: AMP for Endpoints 콘솔에서 다운로드한 모든 Debian 기반 패키지에 대해 5단계를 반복할 수 있습니다.

설치

커넥터를 설치하려면 다음 명령을 실행합니다. 여기서 [deb package]는 파일의 이름입니다(예: amp_test.deb).

```
sudo dpkg -i [deb package]
```

중요! 환경에서 다른 보안 제품을 실행하는 경우 커넥터 설치 프로그램을 위협으로 감지할 가능성이 있습니다. 커넥터를 성공적으로 설치하려면 허용된 목록에 Cisco Secure를 추가하거나 다른 보안 제품에서 Cisco Secure를 제외한 후 다시 시도하십시오.

중요! 커넥터 설치 중에 cisco-amp-scan-svc라는 사용자 및 그룹이 시스템에 생성됩니다. 이 사용자 또는 그룹이 이미 존재하지만 다르게 구성된 경우, 설치 관리자가 삭제를 시도한 다음 필요한 구성으로 다시 만듭니다. 사용자 및 그룹을 필요한 구성으로 만들 수 없으면 설치 프로그램이 실패합니다.

제거

자세한 내용은 보안 엔드포인트 사용 설명서제거 지침

개정 기록

2020년 12월 10일

- 초기 버전

2022년 4월 12일

- 콘텐츠는 Debian과 Ubuntu 모두에 적용됩니다.