# AMP for Endpoints Linux Connector on Ubuntu

## 목차


이 문서에서는 관리자가 Ubuntu에 AMP for Endpoints Linux Connector를 구축하는 데 수행할 수 있는 변경 사항 및 단계에 대해 설명합니다.

## 최소 OS 요구 사항

Ubuntu의 OS 호환성은 AMP [for Endpoints Linux Connector OS Compatibility](#)(AMP for Linux Connector OS 호환성) 문서의 "Ubuntu LTS" 테이블을 참조하십시오.

## 환경 설정

Ubuntu의 AMP for Endpoints Linux Connector는 파일 및 네트워크 모니터링에 eBPF를 사용합니다.시스템에 올바른 linux-headers 소프트웨어 패키지가 설치되어 있어야 합니다. 그렇지 않으면 커넥터가 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

AMP for Endpoints Linux Connector는 Ubuntu의 기본 설치에 포함된 시스템 패키지에 따라 달라집니다.이러한 패키지가 시스템에 없는 경우 다음 오류 메시지가 표시됩니다.

```
ciscoampconnector depends on rsyslog; however: Package rsyslog is not installed.
```

AMP for Endpoints Linux Connector에 필요한 종속성을 설치하려면 다음 명령을 사용합니다.

```
sudo apt install rsyslog logrotate cron libpcre2-8-0
```

## 설치

Connector를 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 AMP for Endpoints Connector 설치 프로그램을 위협으로 탐지할 가능성이 있습니다.커넥터를 성공적으로 설치하려면 허용된 목록에 AMP를 추가하거나 다른 보안 제품에서 AMP를 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

AMP for Endpoints Linux Connector를 제거하려면 다음 명령을 실행합니다.

```
sudo dpkg --remove ciscoampconnector
```

**참고:**이렇게 하면 기록, 격리된 파일, cisco-amp-scan-svc 사용자 및 그룹을 비롯한 로컬 데이터가 남게 됩니다.Connector를 다시 설치하지 않고 나머지 파일을 제거하려면 다음 명령을 실행합니다.

```
sudo dpkg --purge ciscoampconnector
```

**참고:**Ubuntu Software Center를 사용하여 AMP for Endpoint Linux Connector를 제거하면 로컬 데이터도 남겨집니다.

# 개정 기록

2020년 12월 10일

- 초기 버전