

Cisco Secure Endpoint Linux Connector 설치

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[RHEL/CentOS/Amazon Linux 2/SUSE 15](#)

[구성](#)

[GPG 키를 가져오는 방법](#)

[우분투](#)

[구성](#)

[GPG 키를 가져오는 방법](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 RHEL(Red Hat Enterprise Linux) 및 Debian 기반 시스템용 Cisco Secure Endpoint Linux 커넥터를 설치하고 확인하는 방법에 대해 설명합니다.

기고자: 후안 카를로스 카틸레로, Yeraldin Sanchez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Linux 커넥터의 Linux 시스템에서 지원되는 운영 체제(OS)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

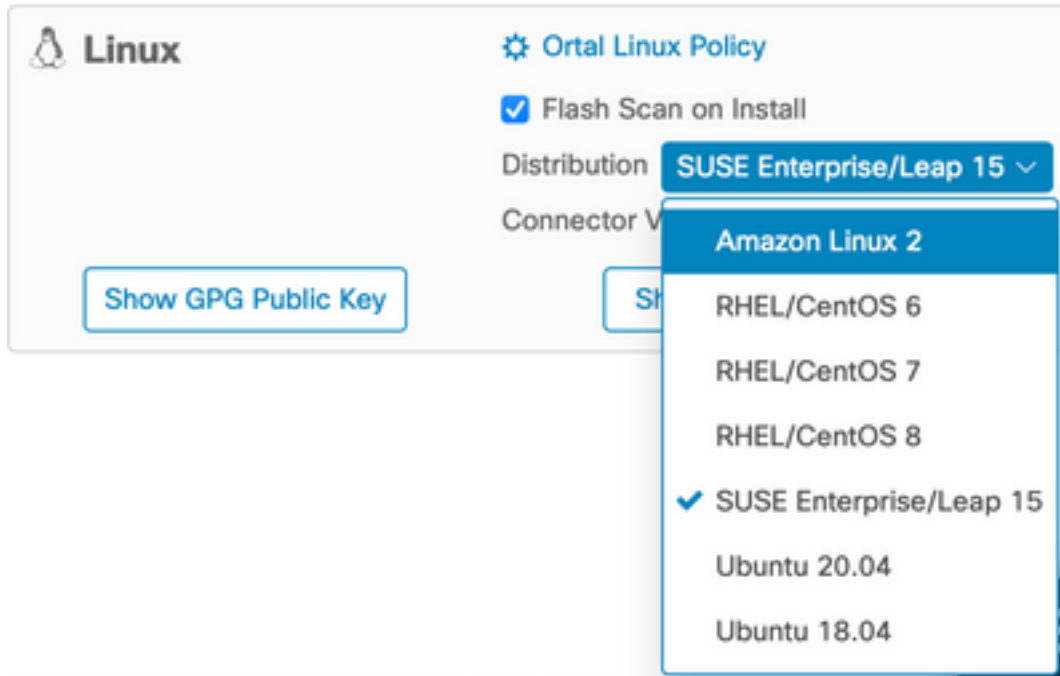
- 보안 엔드포인트 Linux 커넥터 설치 프로그램 Red Hat Package Manager(RPM)
- 보안 엔드포인트 Linux 커넥터 설치 프로그램 Debian Package Manager(dpkg)
- 업데이트를 확인하는 GPG(GNU Privacy Guard) 키(선택 사항)
- Linux 커넥터 설치 프로그램 DPKG(Debian Package Management System)

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

RHEL/CentOS/Amazon Linux 2/SUSE 15

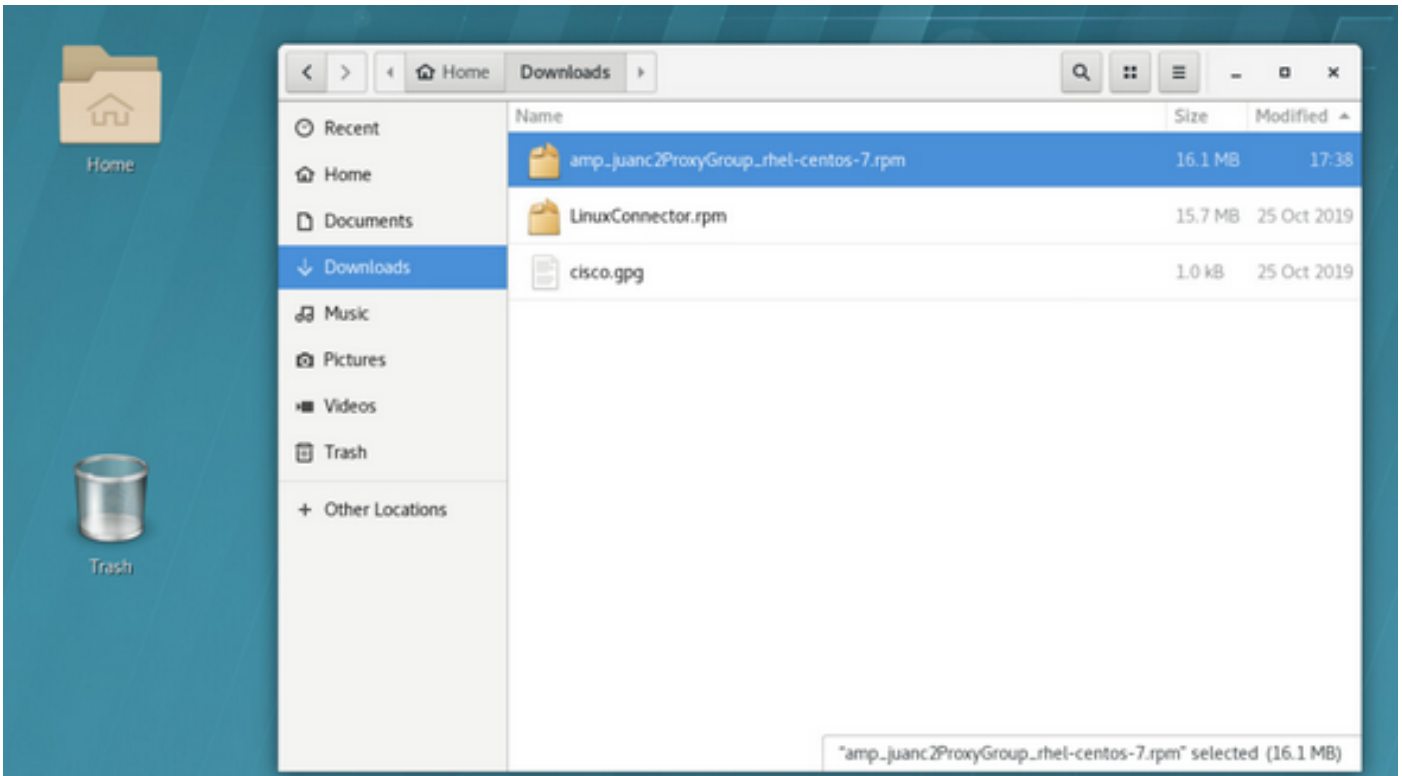
구성

1단계. 이미지에 표시된 대로 Cisco Secure Endpoint Portal에서 Linux RPM 패키지를 다운로드합니다.



참고: 서로 다른 두 커넥터의 아키텍처가 크게 다르기 때문에 OS 배포는 중요합니다.

2단계. RPM 패키지를 문제의 엔드포인트로 이동하여 대시보드에서 직접 다운로드하거나 수동으로 엔드포인트로 이동합니다. 이 예에서는 최소한의 설치로 작업할 수 있지만 그래픽 사용자 인터페이스(UI)를 사용합니다. 이 경우 Linux 터미널을 처리하고 RPM 패키지를 찾는 방법을 알아야 합니다.



3단계. Linux 커넥터를 설치하려면 다음 명령을 실행합니다. `sudo yum localinstall [rpm package] -y` (또는 `sudo zypper install -y [rpm package]` on SUSE 15)

여기서 [rpm package]는 파일의 이름입니다(예: "amp_Audit.rpm"). atd 서비스가 실행되는 동안 RPM 패키지를 설치해야 합니다.

```

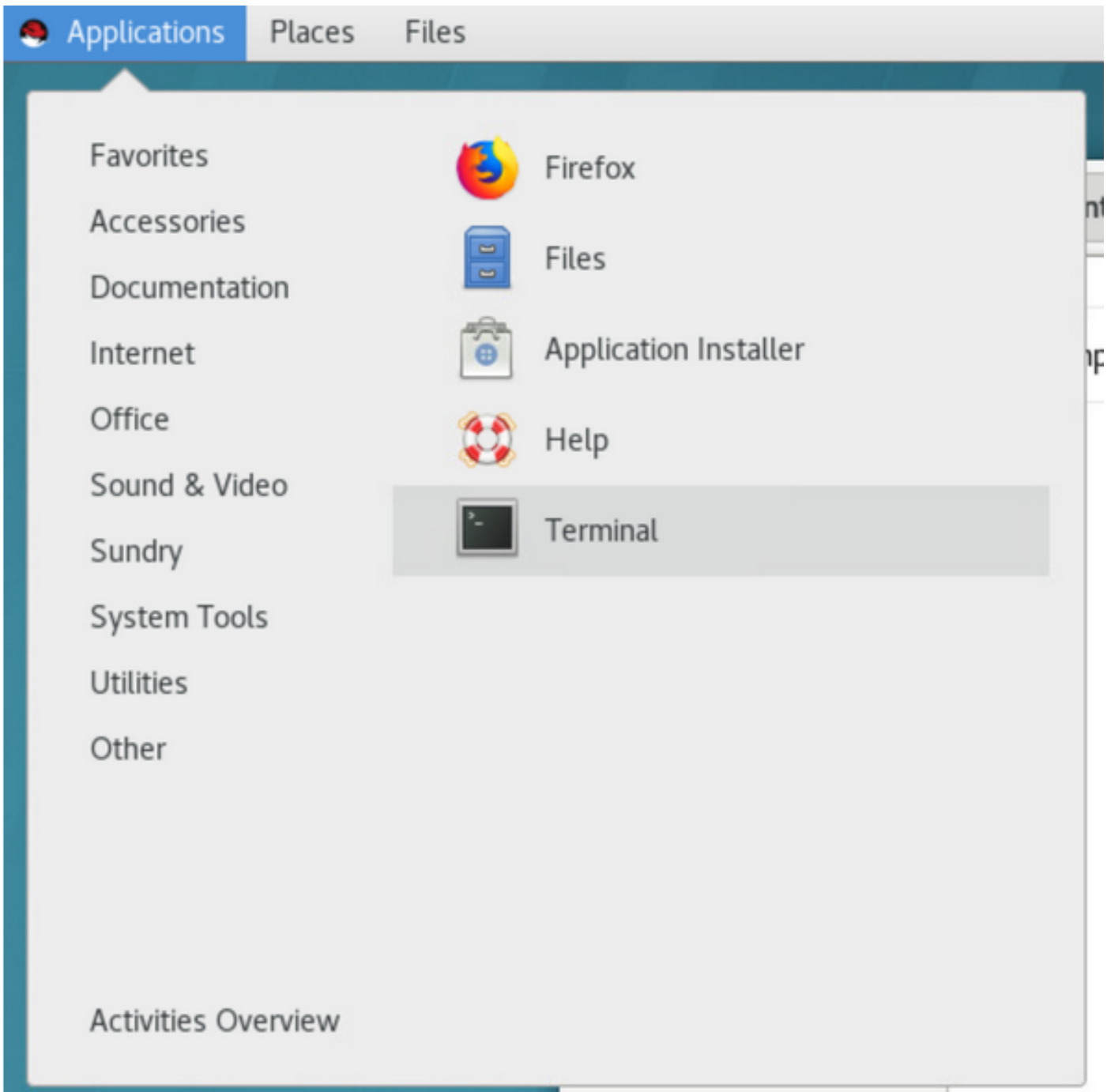
File Edit View Search Terminal Help
[jenator@jenator-11n-ws-lab Downloads] $ sudo yum localinstall amp_juanc2ProxyGroup_rhel-centos-7.rpm -y
[sudo] password for jenator:
Loaded plugins: langpacks, product-id, search-disabled-repos, subscription-manager
This system is not registered with an entitlement server. You can use subscription-manager to register.
Examining amp_juanc2ProxyGroup_rhel-centos-7.rpm: ciscoampconnector-1.12.2.002-1.el7.x86_64
Marking amp_juanc2ProxyGroup_rhel-centos-7.rpm as an update to ciscoampconnector-1.10.2.030-1.el7.x86_64
Resolving Dependencies
-> Running transaction check
->> Package ciscoampconnector.x86_64 0:1.10.2.030-1.el7 will be updated
->> Package ciscoampconnector.x86_64 0:1.12.2.002-1.el7 will be an update
-> Finished Dependency Resolution

Dependencies Resolved

=====
Package                Arch          Version           Repository        Size
-----
Updating:
ciscoampconnector      x86_64        1.12.2.002-1.el7 /amp_juanc2ProxyGroup_rhel-centos-7 43 K
Transaction Summary
-----
Upgrade 1 Package

Total size: 43 K
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Policy saved to /opt/cisco/amp/atc/policy.xml.unsaved
  
```

GUI가 사용 중인 경우 이미지에 표시된 대로 터미널을 엽니다.



설치가 시작되면 이미지에 표시된 대로 사용자 입력이 필요하지 않습니다.

```
File Edit View Search Terminal Help
Updating:
  ciscoampconnector          x86_64          1.12.2.602-1.el7          /amp_buanc3ProxyGroup_rhel-centos-7          43 M
-----
Transaction Summary
-----
Upgrade 1 Package

Total size: 43 M
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Policy saved to /opt/cisco/amp/etc/policy.xml.amgsave
Verifying archive integrity... 100% All good.
Uncompressing ampconnector installer 100%
  updating : ciscoampconnector-1.12.2.602-1.el7.x86_64          1/2
warning: /opt/cisco/amp/etc/policy.xml created as /opt/cisco/amp/etc/policy.xml.rpmnew
Policy restored from /opt/cisco/amp/etc/policy.xml.amgsave
Verifying archive integrity... 100% All good.
Uncompressing ampconnector installer 100%
Redirecting to /bin/systemctl restart rsyslog.service
  Cleanup : ciscoampconnector-1.12.2.630-1.el7.x86_64          2/2
  Verifying : ciscoampconnector-1.12.2.602-1.el7.x86_64          1/2
  Verifying : ciscoampconnector-1.12.2.630-1.el7.x86_64          1/2

Updated:
  ciscoampconnector.x86_64 0:1.12.2.602-1.el7

Complete!
[[jensfarm@esxtarr-1in-mex-lab Downloads]$
```

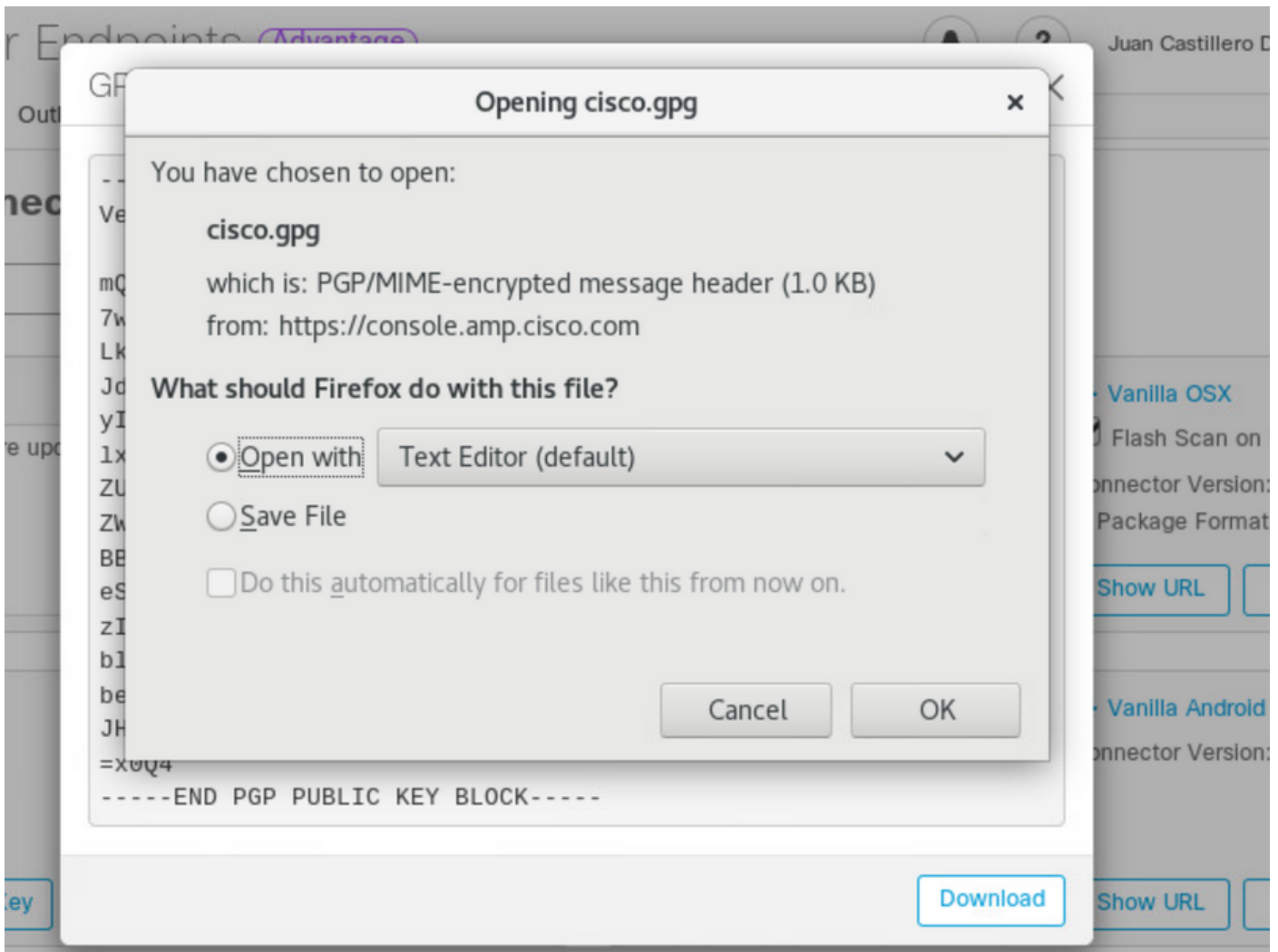
GPG 키를 가져오는 방법

Download Connector(커넥터 다운로드) 페이지에서 GPG 공개 키를 복사하여 RPM 패키지의 서명을 확인할 수 있습니다. GPG 키 없이 커넥터를 설치할 수 있습니다.; 하지만 사용자 RHEL에서 정책을 통해 커넥터 업데이트를 푸시할 계획이라면 GPG 키를 RPM DB로 가져와야 합니다..

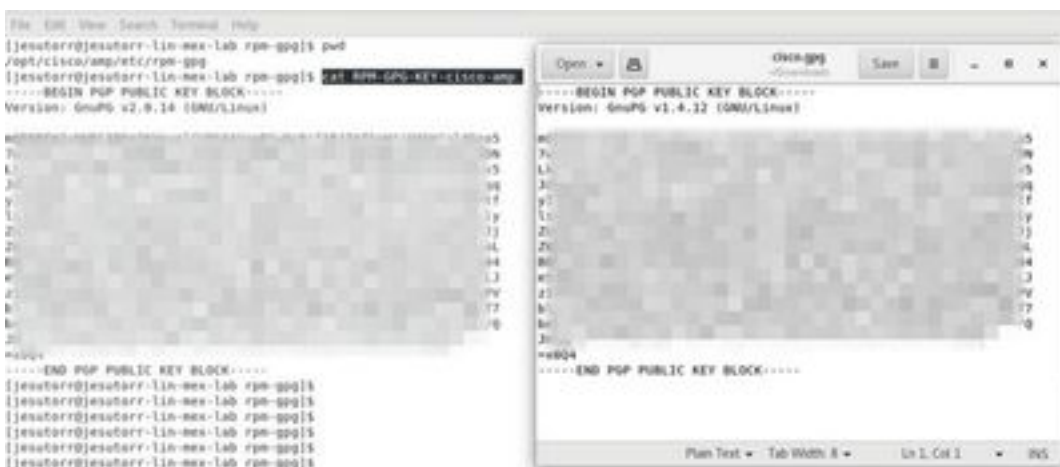
참고: 커넥터 버전 1.17.0부터 커넥터 업데이트 중에 업그레이드 패키지를 확인하는 데 사용되는 GPG 키가 자동으로 설치됩니다.

1단계. GPG 키를 확인하고 Download Connector(커넥터 다운로드) 페이지에서 GPG Public Key(GPG 공개 키) 링크를 클릭합니다. 키를 `/opt/cisco/amp/etc/rpm-gpg/RPM-GPG-Key-cisco-amp`의 키와 비교합니다.





2단계. 터미널에서 명령을 실행하여 키를 가져옵니다. `sudo rpm --import /opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp.`



3단계. 키가 설치되었는지 확인하고 터미널에서 명령을 실행합니다. `rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n'.`



4단계. 출력에서 Sourcefire에서 GPG 키를 찾습니다. Updater는 시스템의 init 데몬에 의해 실행되

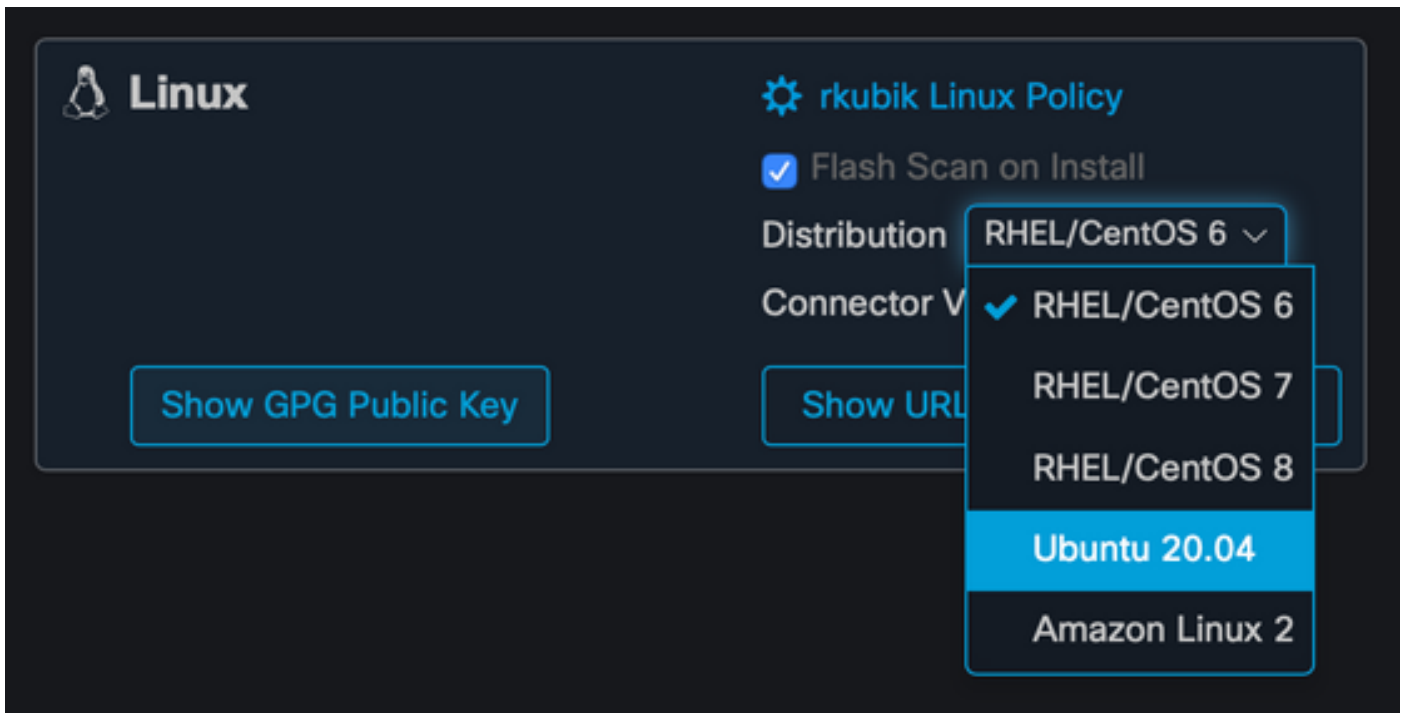
며, 업데이트가 사용 가능한 경우 RPM 업그레이드 프로세스가 자동으로 트리거됩니다. 일부 SELinux 컨피그레이션에서는 이 동작을 금지하고 업데이터 오류가 발생합니다.

이 경우 시스템의 감사 로그(예: `/var/log/audit/audit.log`)를 살펴보고, 앰퍼더와 관련된 거부 이벤트를 검색합니다. 업데이트 프로그램이 작동하도록 하려면 SELinux 규칙을 조정해야 할 수 있습니다.

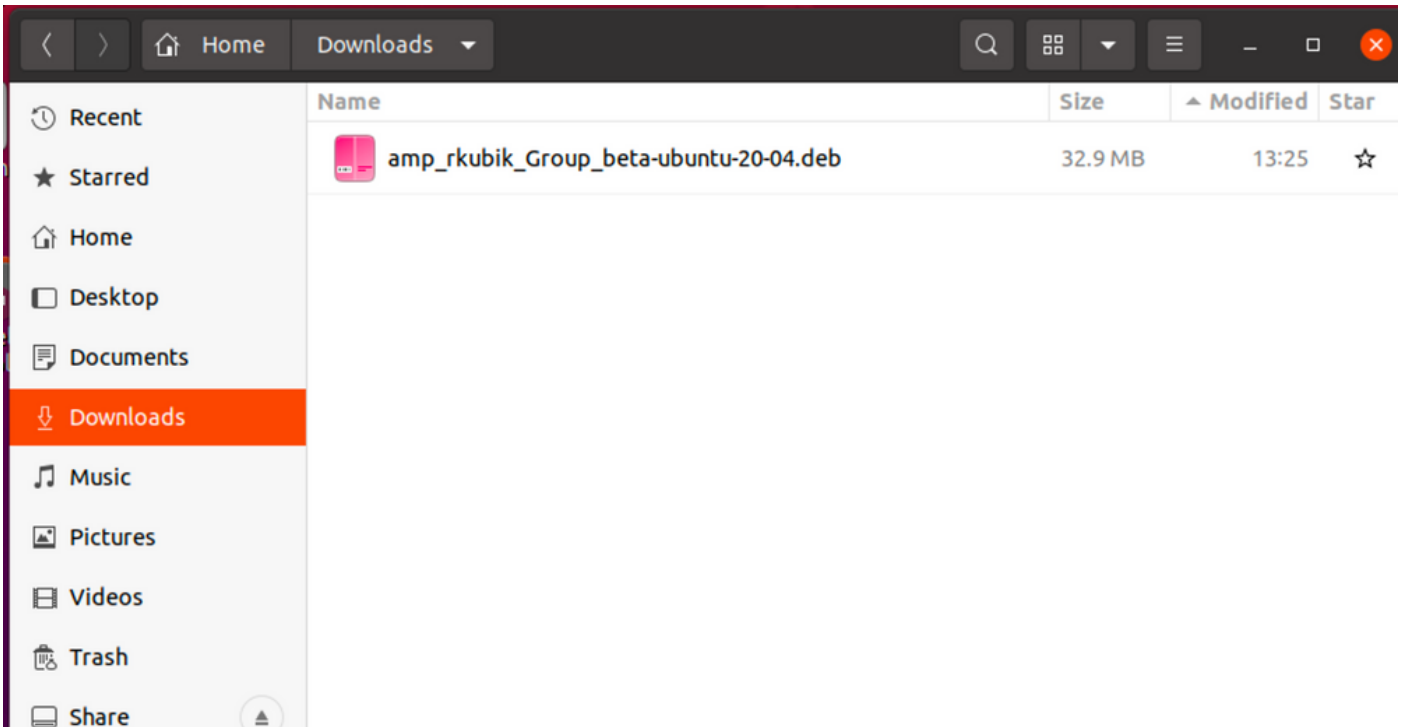
우분투

구성

1단계. 이미지에 표시된 대로 Cisco Secure Endpoint Portal에서 Linux DEB 패키지를 다운로드합니다.



2단계. DEB 패키지를 문제의 엔드포인트로 이동하여 대시보드에서 직접 다운로드하거나 수동으로 엔드포인트로 이동합니다. 이 예에서는 최소 설치를 위해 그래픽 사용자 인터페이스(UI)를 사용할 수 있지만 일반적으로 사용됩니다. 이 경우 Linux 터미널을 처리하고 DEB 패키지를 찾는 방법을 알아야 합니다.



3단계. Linux 커넥터를 설치하려면 다음 명령을 실행합니다. `sudo dpkg -i [deb package]` 여기서 [deb package]는 파일의 이름입니다(예: "amp_Audit.deb"). 설치가 시작되면 이미지에 표시된 대로 사용자 입력이 필요하지 않습니다.

```
/bin/bash
/bin/bash 80x24
Now using version go1.11.13
13:27:33 cisco~
$ cd Downloads/
13:27:53 cisco~/Downloads
$ sudo dpkg -i amp_rkubik_Group_beta-ubuntu-20-04.deb
Selecting previously unselected package ciscoampconnector.
(Reading database ... 252023 files and directories currently installed.)
Preparing to unpack amp_rkubik_Group_beta-ubuntu-20-04.deb ...
Unpacking ciscoampconnector (1.15.999.9999-1) ...
Setting up ciscoampconnector (1.15.999.9999-1) ...
Verifying archive integrity... 100% All good.
Uncompressing ampconnector installer 100%
Processing triggers for libc-bin (2.31-0ubuntu9.1) ...
Processing triggers for rsyslog (8.2001.0-1ubuntu1.1) ...
13:28:02 cisco~/Downloads
$ █
```

GPG 키를 가져오는 방법

Download Connector(커넥터 다운로드) 페이지에서 GPG 공개 키를 복사하여 DEB 패키지의 서명을 확인할 수 있습니다. GPG 키 없이 커넥터를 설치할 수 있습니다. 그러나 사용자는 Ubuntu의 정책을 통해 커넥터 업데이트를 푸시하려는 경우 GPG 키를 디버그 키링으로 가져와야 합니다. GPG 키를 가져오고 Ubuntu에서 커넥터가 수정되지 않았는지 확인하는 방법에 대한 자세한 내용은 <https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/216524-amp-for-endpoints-ubuntu-connector.html#anc6>을 참조하십시오.

참고: 커넥터 버전 1.17.0부터 커넥터 업데이트 중에 업그레이드 패키지를 확인하는 데 사용되는 GPG 키가 자동으로 설치됩니다. 이 GPG 키를 확인하려면 Download Connector(커넥터 다운로드)

페이지에서 GPG Public Key(GPG 공개 키) 링크를 클릭하고 /opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-Key-cisco-amp에 설치된 키와 비교합니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

성공적인 설치를 확인하려면 **AMP CLI를 실행합니다**. Linux 커넥터 명령줄 인터페이스는 /opt/cisco/amp/bin/ampcli에서 찾을 수 있습니다. 인터랙티브 모드에서 실행하거나 단일 명령을 실행한 다음 종료할 수 있습니다. 명령./ampcli —help를 실행하여 사용 가능한 옵션 및 명령의 전체 목록을 확인합니다. 커넥터에서 생성된 모든 로그 파일은 /var/log/cisco에서 찾을 수 있습니다.

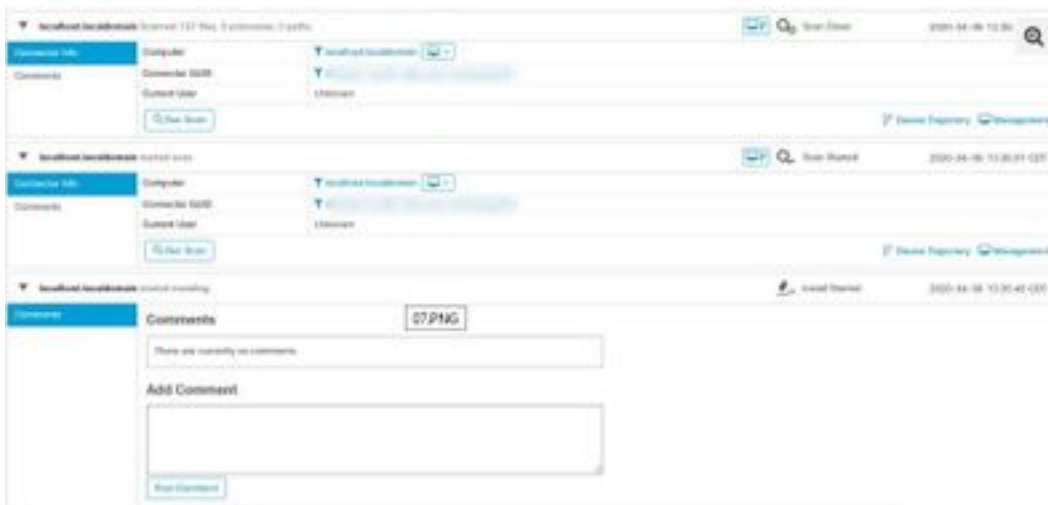
```
File Edit View Search Terminal Help
[preuser@preuser-lin-ma-lab ~]$ cd /opt/cisco/amp/bin/
[preuser@preuser-lin-ma-lab bin]$ pwd
/opt/cisco/amp/bin
[preuser@preuser-lin-ma-lab bin]$ ls
ampcli  ampcli  ampcli.service  ampcli.service  cisco-amp-helper  libLampack.so.8  libLampack.so.8.LB  libLampack.so.8.LB  libLampack.so.8.LB
[preuser@preuser-lin-ma-lab bin]$ ./ampcli

ampcli - AMP for Endpoints Connector Command Line Interface
Interactive mode

Enter 'q' or Ctrl+C to Exit

[logger] Set maximum reported log level to notice
Trying to connect...
Connected.
ampcli> status
Status: Connected
Mode: Normal
Scan: Ready for scan
Last Scan: 2020-02-20 03:26 PM
Policy: Jabotize-Linux (4252060)
Command Line: Enabled
Faults: None
ampcli>
```

또한 Cisco Secure Console에 설치 이벤트가 나타나며, RPM 패키지를 다운로드할 때 플래시 스캔이 요청되면 해당 이벤트도 표시됩니다.



문제 해결

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

관련 정보

- [Linux 비디오에 AMP for Endpoints Connector 설치](#)
- [기술 지원 및 문서 - Cisco Systems](#)