

Installatie van de Cisco Secure Endpoint Linux-connector

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

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

[Configuraties](#)

[Hoe de GPG-toets te importeren](#)

[Ubuntu](#)

[Configuraties](#)

[Hoe de GPG-toets te importeren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe de Cisco Secure Endpoint Linux-connector voor Red Hat Enterprise Linux (RHEL) en Debian-gebaseerde systemen moet worden geïnstalleerd en geverifieerd.

Bijgedragen door Juan Carlos Castillero en bewerkt door Yeraldin Sanchez, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Linux-machines op een Linux-connector ondersteund besturingssysteem (OS)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

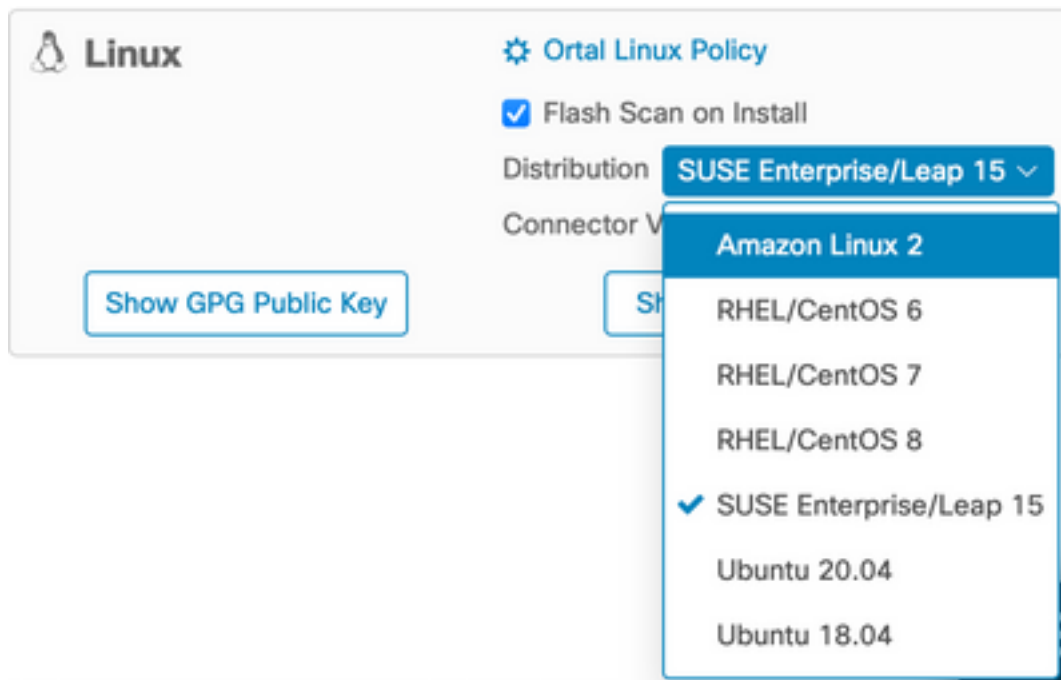
- Een Secure Endpoint Linux-installatieprogramma van een Red Hat Packet Manager (RPM)
- Een Secure Endpoint Linux-installatieautomaat - Debian Package Manager (dpkg)
- Een GNU Privacy Guard (GPG) toets om updates te controleren (optioneel)
- Een DLKG-installatieprogramma (Debian Package Management System) voor Linux-connectors

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

RHEL/CentOS/Amazon Linux 2/SUSE 15

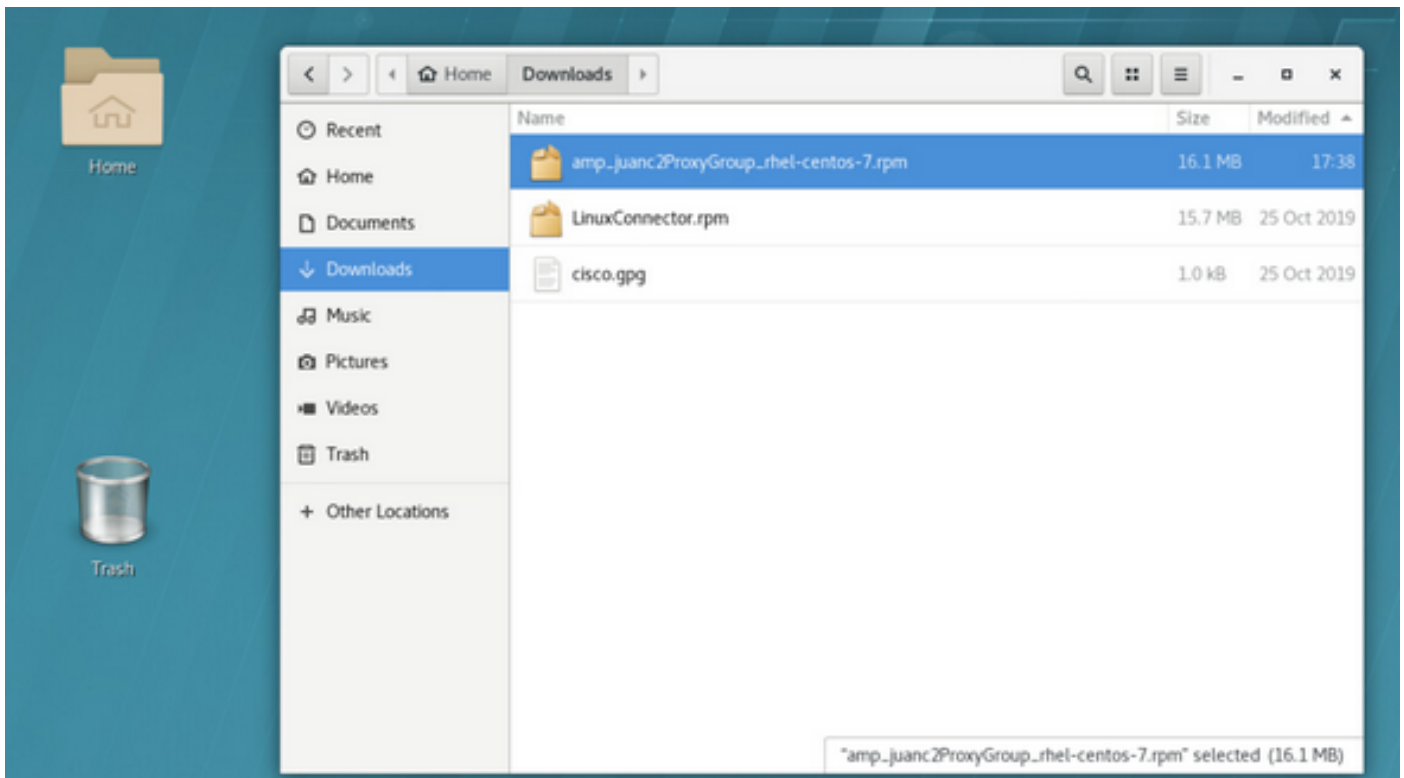
Configuraties

Stap 1. Download het Linux RPM-pakket van Cisco Secure Endpoint Portal, zoals in de afbeelding.



Opmerking: Denk eraan dat de OS-distributie belangrijk is omdat beide connectors zeer verschillende architecturen hebben.

Stap 2. Verplaats het RPM-pakket naar het desbetreffende eindpunt, download het direct van het dashboard of verplaats het handmatig naar de eindpunten. Bijvoorbeeld, wordt een Graphic User Interface (UI) gebruikt, alhoewel het mogelijk en vaak gebruikelijk is om met een minimale installatie te werken. In dat geval moet het weten hoe de Linux-terminal te behandelen en hun RPM-pakket te vinden.



Stap 3. Voer de opdracht uit om de Linux-connector te installeren: **voor een optimale installatie [rpm pakket] -y** (of **sudozyper-installatie -y [rpm pakket]** op SUSE 15)

waar [rpm Package] de naam van het bestand is, bijvoorbeeld "amp_Audit.rpm". Het RPM-pakket moet tijdens de uitvoering van de aangepaste service worden geïnstalleerd.

```

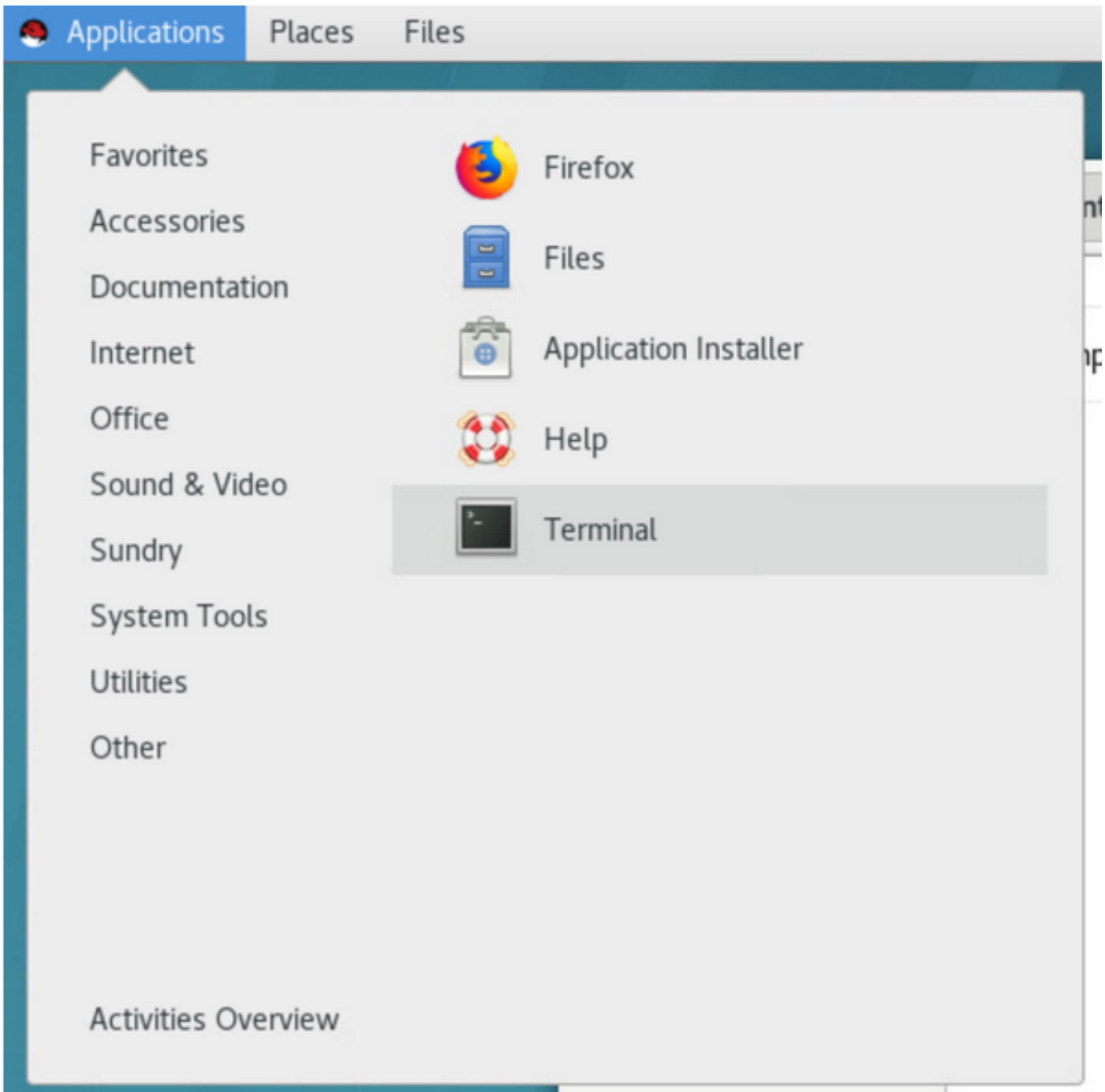
File Edit View Search Terminal Help
[jenator@jenator-lin-ops-lab Downloads] sudo yum localinstall amp_juanc2ProxyGroup_rhel-centos-7.rpm -y
[sudo] password for jenator:
Loaded plugins: langpacks, product-id, search-disabled-repos, subscription-manager
This system is not registered with an entitlement server. You can use subscription-manager to register.
Examining amp_juanc2ProxyGroup_rhel-centos-7.rpm: ciscoampconnector-1.12.1.002-1.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
--> Missing transaction check
--> Package ciscoampconnector.x86_64 0:1.10.2.030-1.el7 will be updated
--> Package ciscoampconnector.x86_64 0:1.12.1.002-1.el7 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                Arch          Version                Repository              Size
-----
Updating:
ciscoampconnector      x86_64        1.12.1.002-1.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/etc/policy.xml.unsaved
  
```

Als de GUI in gebruik is, opent u de terminal, zoals in de afbeelding.



Nadat de installatie is begonnen, is er geen gebruikersinvoer vereist. Het is een automatisch proces, zoals in de afbeelding wordt weergegeven.

```
File Edit View Search Terminal Help
ipatching:
ciscoampconnector x86_64 1.12.2.602-1.el7 /amp_proxyGroup_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.ampsave
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.ampsave
Verifying archive integrity... 100% All good.
Uncompressing ampconnector installer 100%
Redirecting to /bin/systemctl restart rsyslog.service
  Cleanup : ciscoampconnector-1.12.2.600-1.el7.x86_64 2/2
  Verifying : ciscoampconnector-1.12.2.602-1.el7.x86_64 1/2
  Verifying : ciscoampconnector-1.12.2.600-1.el7.x86_64 2/2

Updated:
ciscoampconnector.x86_64 0:1.12.2.602-1.el7
Complete!
[[jcsutor@jesutarr-1in-mex-lab Downloads]$
```

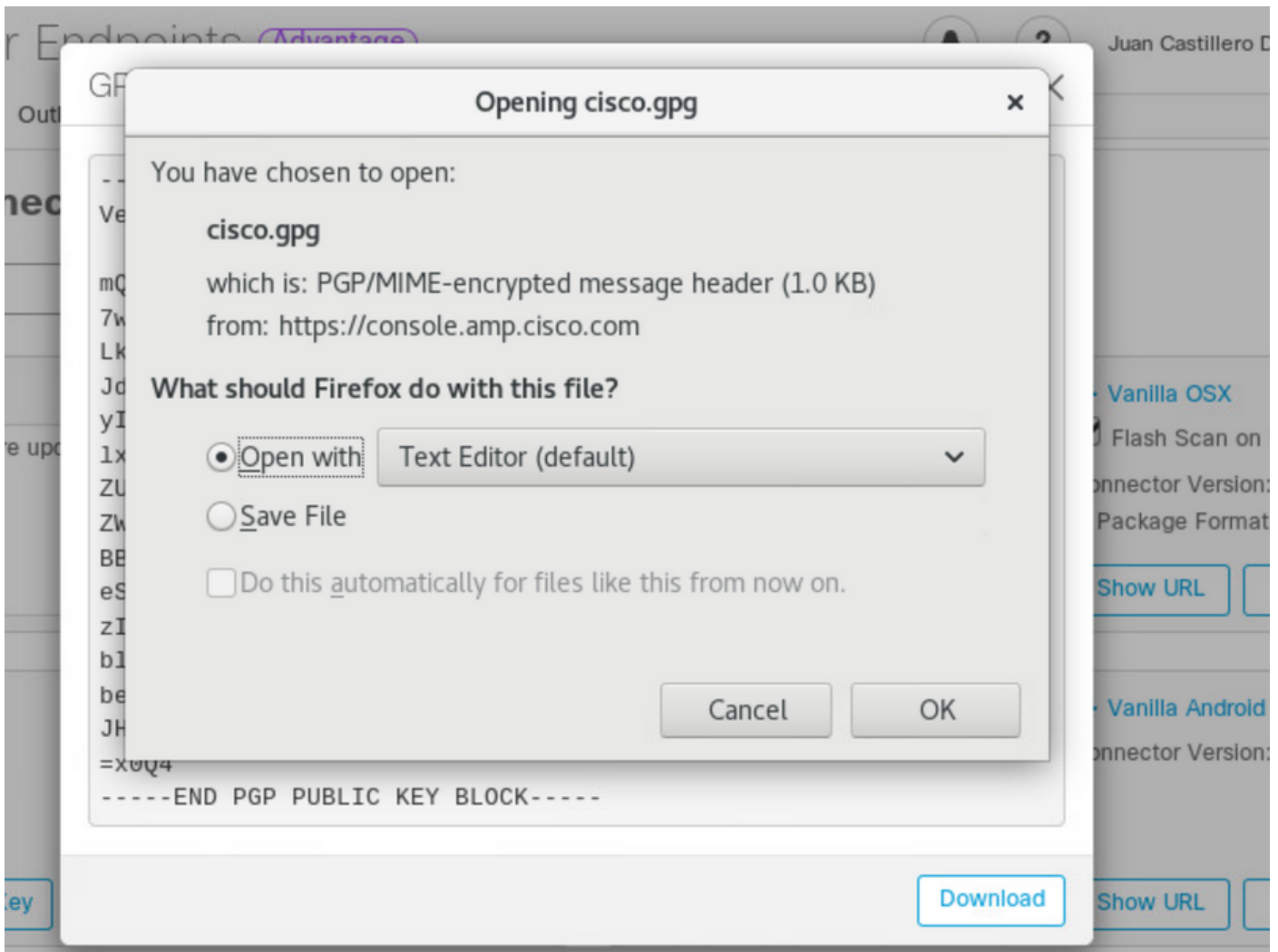
Hoe de GPG-toets te importeren

De openbare sleutel van GPG kan van de pagina van de Download Connector worden gekopieerd om de ondertekening van het RPM - pakket te verifiëren. De connector kan worden geïnstalleerd zonder de GPG-toets; echter : een gebruiker De GPG-toets zou in hun RPM-DB moeten importeren indien zij voornemens zijn de aansluitupdates via het RHEL-beleid te drukken.

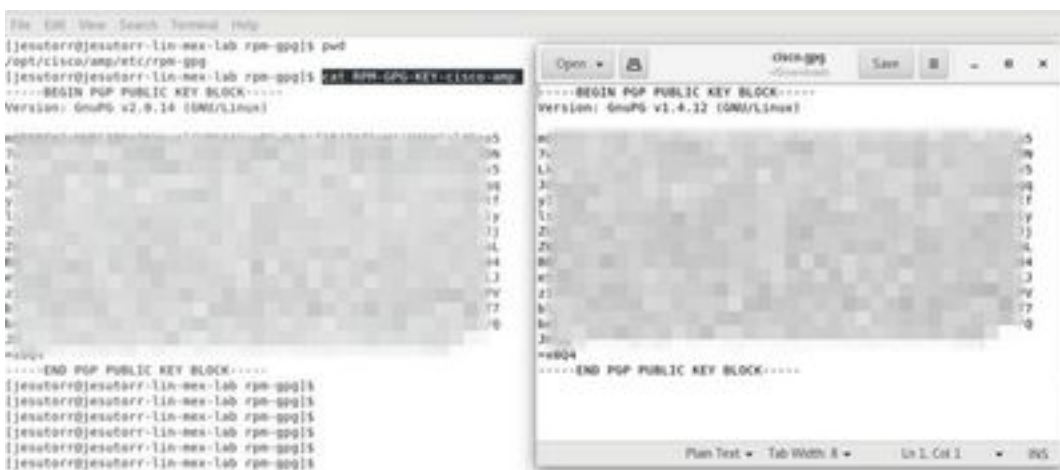
Opmerking: Om te beginnen met verbindingversie 1.17.0, wordt de GPG-toets die wordt gebruikt om upgradepakketten te controleren tijdens verbindingupdates automatisch geïnstalleerd.

Stap 1. Controleer de GPG-toets en klik op de GPG Public Key link op de pagina van de Download Connector. Vergelijk de toets met die bij **PHP/opt/cisco/amp/etc/rpm-gpg/RPM-GPG-Key-cisco-amp**.





Step 2. Start de opdracht van een terminal om de toets te importeren: **sudo-rpm —import/opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp.**



Step 3. Controleer dat de toets is geïnstalleerd en voer de opdracht vanuit de terminal uit: **rpm -q gpg-pubkey —qf "% {naam}-% {versie}-% {release} —> % {samenvatting}n'.**



Step 4. Zoek een GPG-toets van Sourcefire in de uitvoer. De Updater wordt uitgevoerd door de

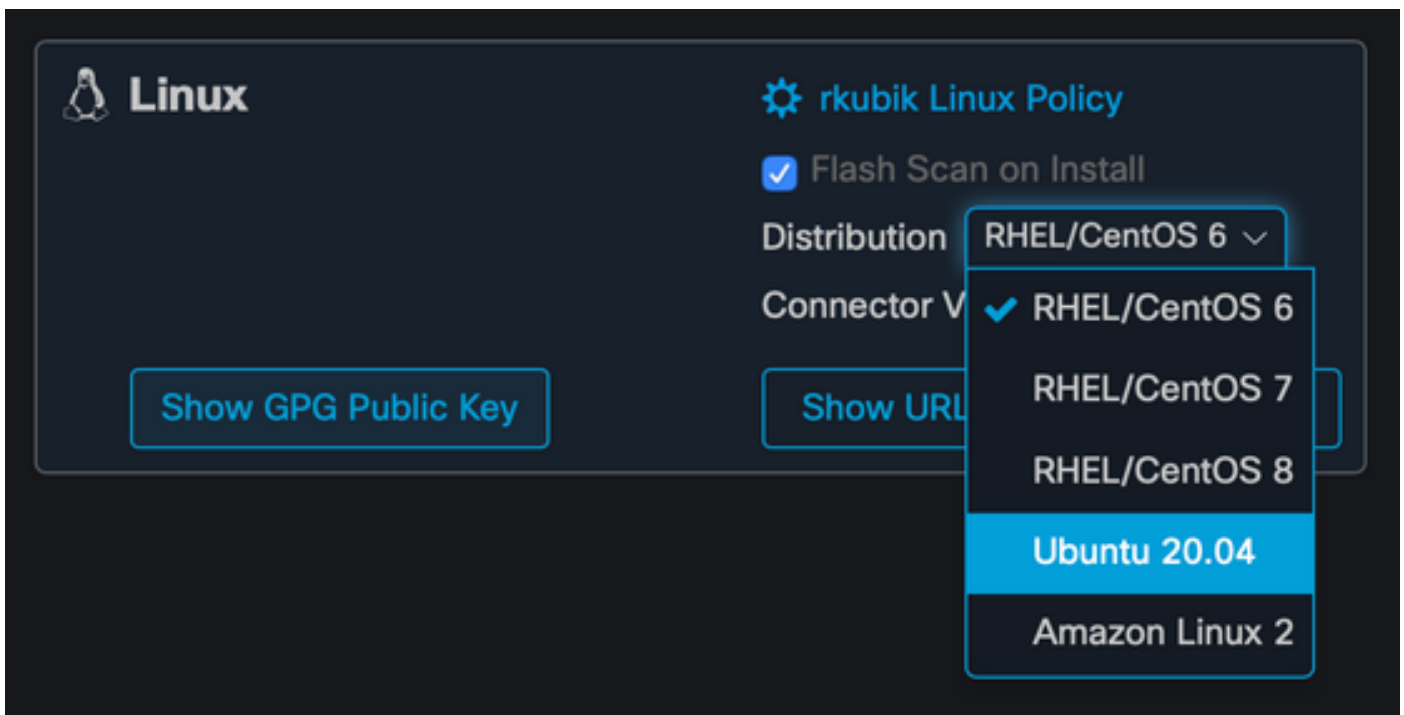
ingang van het systeem en wanneer een update beschikbaar is, start automatisch het RPM-upgradeproces. Sommige SELinux-configuraties verbieden dit gedrag en veroorzaken de Updater om te falen.

Als u vermoedt dat dit het geval is, bekijk dan het auditlogboek van het systeem (bijv. `/var/log/audit/audit.log`) en zoek naar ontkenningsebeurtenissen gerelateerd aan ampupdate. Het kan nodig zijn de SELinux-regels aan te passen zodat Updater kan functioneren.

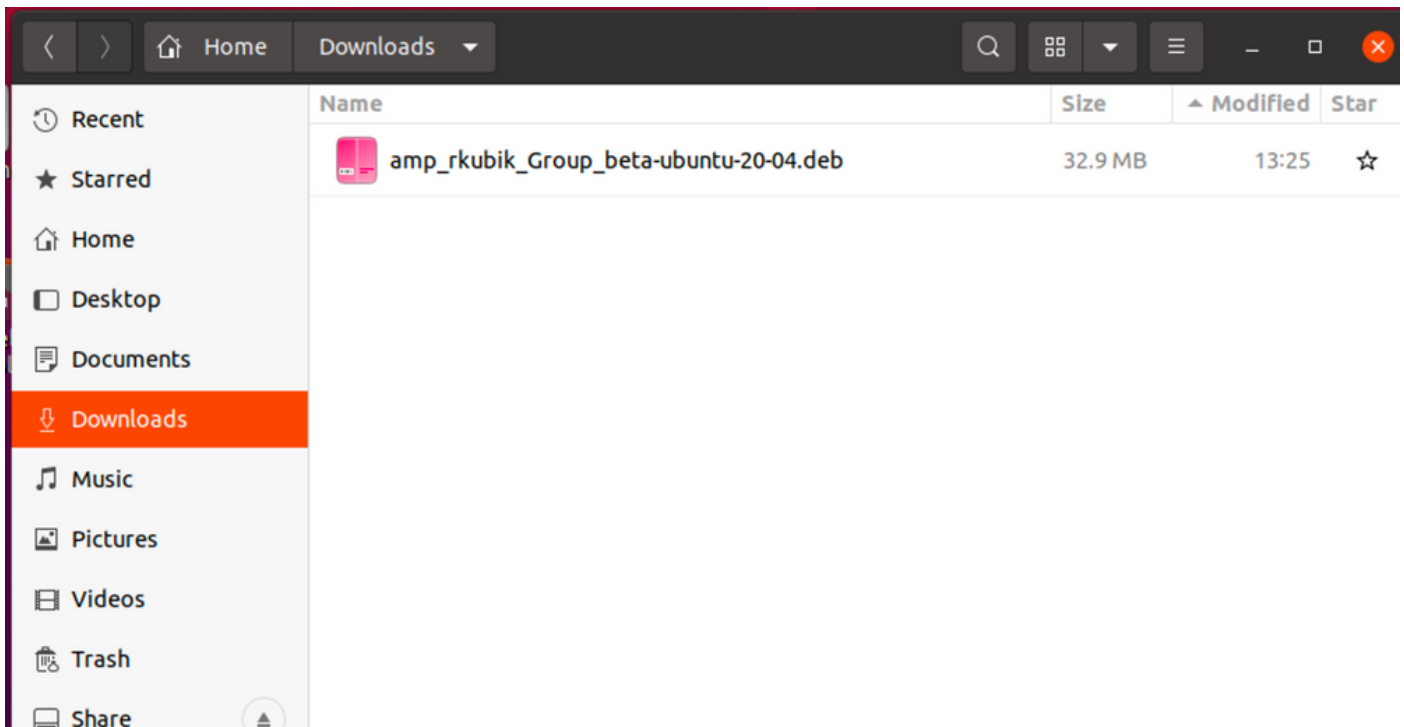
Ubuntu

Configuraties

Stap 1. Download het Linux DEB-pakket van Cisco Secure Endpoint Portal, zoals in de afbeelding.



Stap 2. Verplaats het DEB-pakket naar het desbetreffende eindpunt, of download het direct vanaf het dashboard of verplaats het handmatig naar de eindpunten. Bijvoorbeeld, wordt een Graphic User Interface (UI) gebruikt, alhoewel het mogelijk en vaak gebruikelijk is om met een minimale installatie te werken. In dat geval moet het weten hoe de Linux-terminal te behandelen en hun DEB-pakket te vinden.



Stap 3. Voer de opdracht uit om de Linux-connector te installeren: `sudo dpkg -i [deb Package]` is de naam van het bestand, bijvoorbeeld "amp_Audit.deb". Nadat de installatie is begonnen, is er geen gebruikersinvoer vereist. Het is een automatisch proces, zoals in de afbeelding wordt weergegeven.

```

/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
$ █
```

Hoe de GPG-toets te importeren

De openbare sleutel van GPG kan van de pagina van de Download Connector worden gekopieerd om de ondertekening van het DEB - pakket te verifiëren. De connector kan worden geïnstalleerd zonder de GPG-toets; Een gebruiker zou echter de GPG-toets in zijn debsig-toetsenbord moeten importeren als hij van plan is om via het Ubuntu-beleid de verbindingupdates te sturen. Zie <https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/216524-amp-for-endpoints-ubuntu-connector.html#anc6> voor meer informatie over het importeren van de GPG-toets en het controleren of de connector niet is gewijzigd op Ubuntu

Opmerking: Om te beginnen met bindingsversie 1.17.0, wordt de GPG-toets die wordt gebruikt om upgradepakketten te controleren tijdens bindingsupdates automatisch geïnstalleerd. Om deze GPG-toets te controleren klikt u op de GPG Public Key link op de pagina van de Download Connector en vergelijkt u deze met de toets die is geïnstalleerd op `//opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-Key-cisco-amp`.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Voer de **AMP CLI** uit om de succesvolle installatie te controleren. De Linux-opdrachtregel-interface is te vinden op `/opt/cisco/amp/bin/ampcli`. U kunt deze functie uitvoeren in interactieve modus of een opdracht uitvoeren om de machine uit te voeren. Start de opdracht `./ampcli — help -` om een volledige lijst met opties en opdrachten te zien. Alle logbestanden die door de connector zijn gegenereerd, zijn te vinden in `Var/log/cisco`.

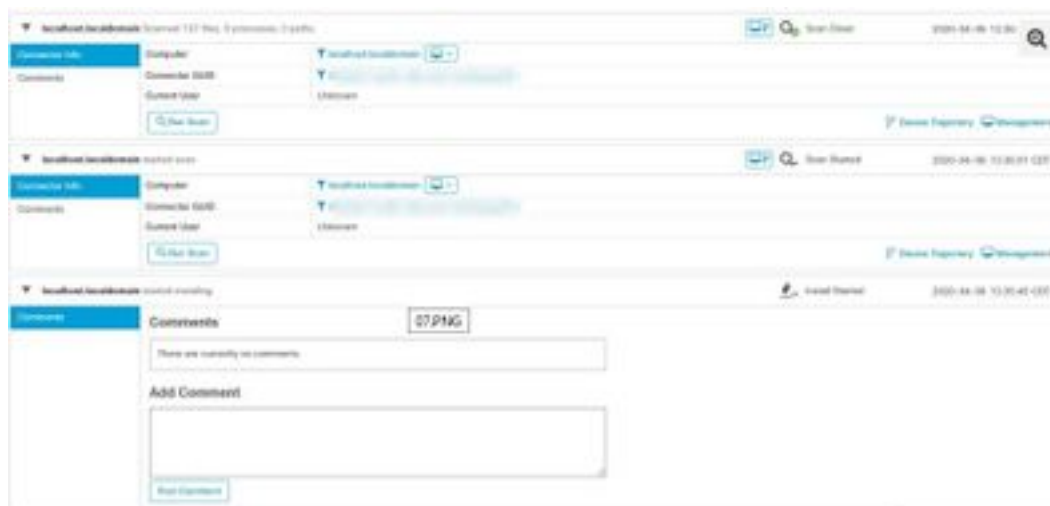
```
File Edit View Search Terminal Help
[preuser@preuser-lin-mx-lab ~]$ cd /opt/cisco/amp/bin/
[preuser@preuser-lin-mx-lab bin]$ pwd
/opt/cisco/amp/bin
[preuser@preuser-lin-mx-lab bin]$ ls
ampcli  ampcli.rpm  ampcli.rpm.sig  ampcli.rpm.sig.gpg  cisco-amp-helper  lib/ampcli.so.0  lib/ampcli.so.0.rpm  lib/ampcli.so.0.rpm.gpg
ampcli.rpm.sig.gpg  ampcli.rpm.sig.gpg.gpg  lib/ampcli.so  lib/ampcli.so.0.rpm  lib/ampcli.so.0.rpm.gpg
[preuser@preuser-lin-mx-lab bin]$ ./ampcli

ampcli - AMP for Endpoints Connector Command Line Interface
Interaction 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 02:26 PM
Policy: Jabotrix-Linux (821200)
Command Line: Enabled
Faults: None
ampcli █
```

Een installatie-gebeurtenis verschijnt ook op de Cisco Secure-console, als er behoefte is aan scannen wanneer het RPM-pakket is gedownload, dan verschijnen deze ook.



Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- [Installeer de Advanced Malware Protection voor endpoints in de Linux-video](#)

- [Technische ondersteuning en documentatie – Cisco Systems](#)