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:

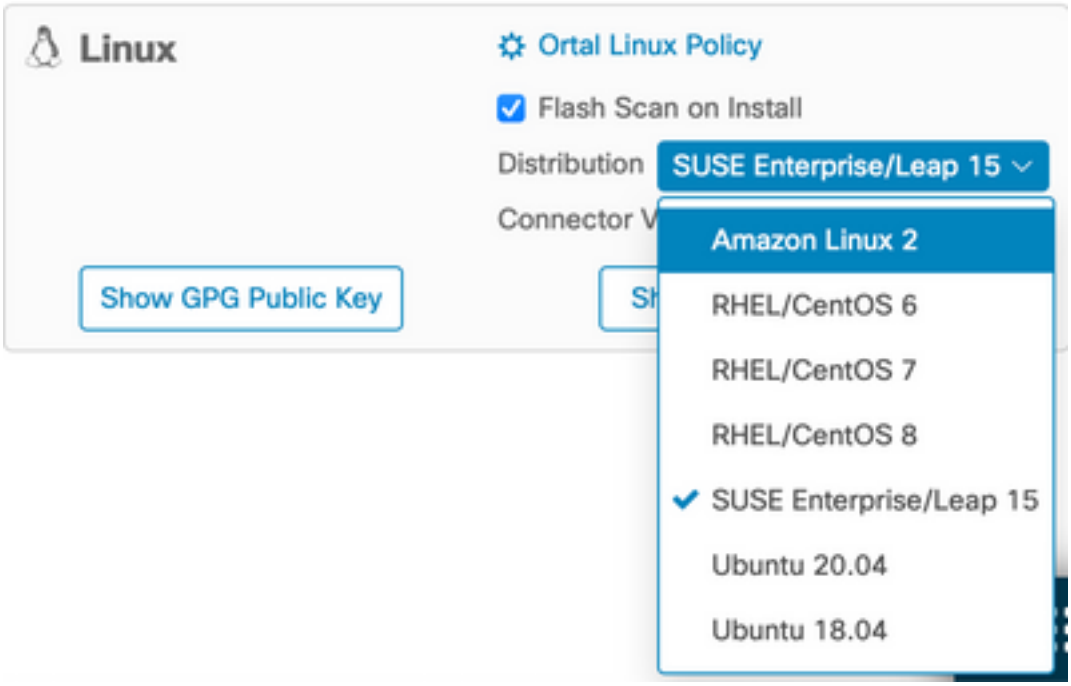
- Een Secure Endpoint Linux-installatieprogramma van een Red Hat Packet Manager (RPM)
- Een Secure Endpoint Linux-installatieautomaat - Debian Package Manager (dpkg)
- Een GNU Privacy Guard (GPG) toets om updates te controleren (optioneel)
- Een DLKG-installatieprogramma (Debian Package Management System)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

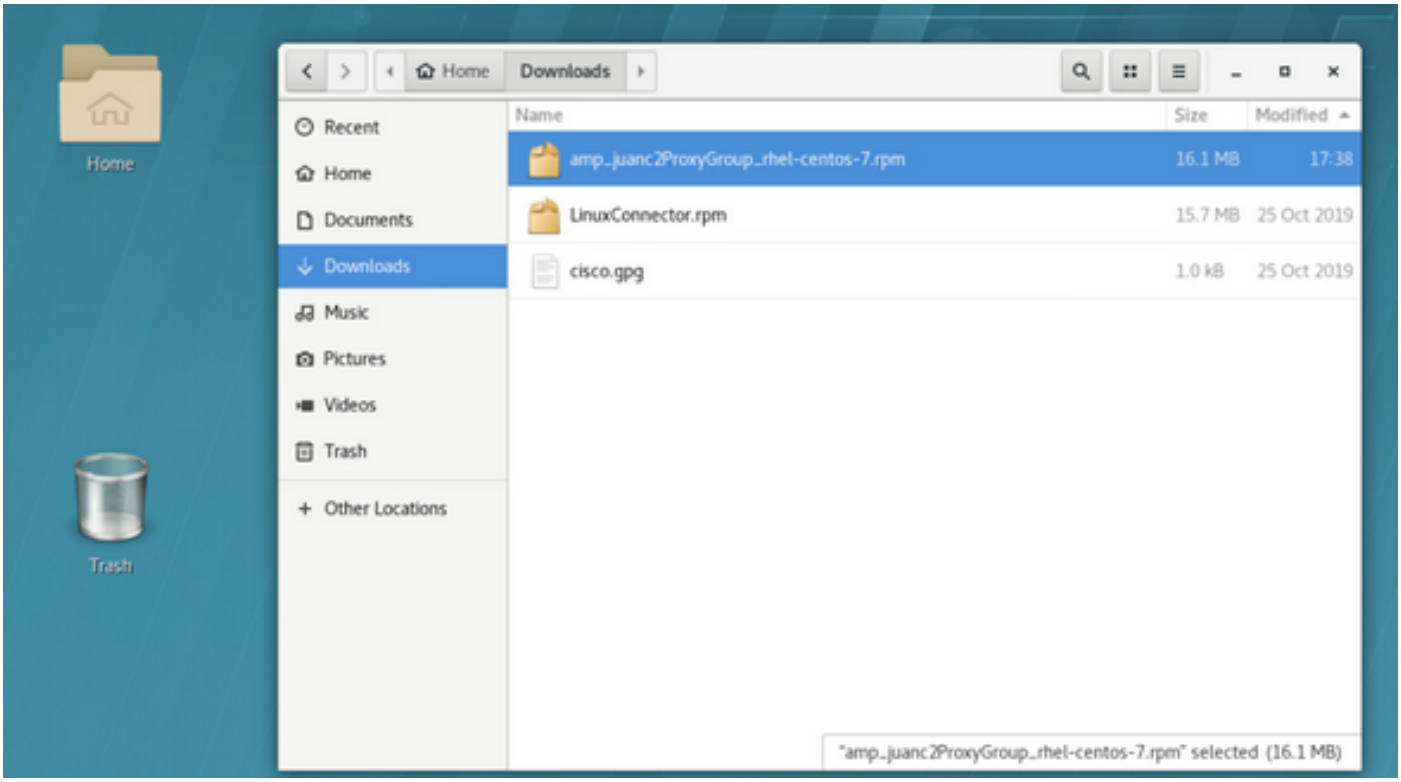
Configuraties

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.

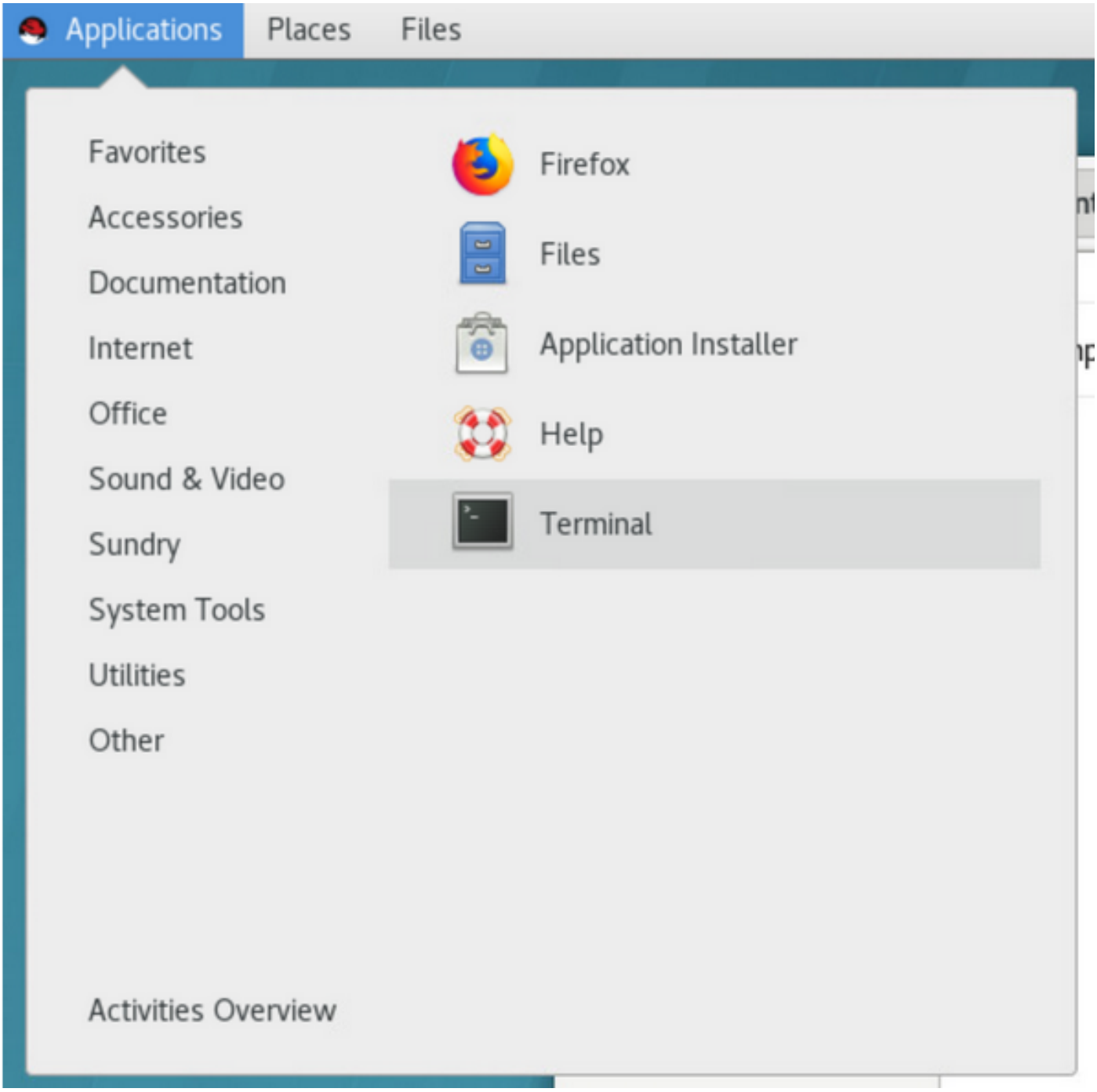
Stap 2. Verplaats het RPM-pakket naar het desbetreffende eindpunt, download het direct van het dashboard of verplaats het handmatig naar de eindpunten. Bijvoorbeeld, wordt een Graphic User Interface (UI) gebruikt, alhoewel het mogelijk en vaak gebruikelijk is om met een minimale installatie te werken. 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.

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



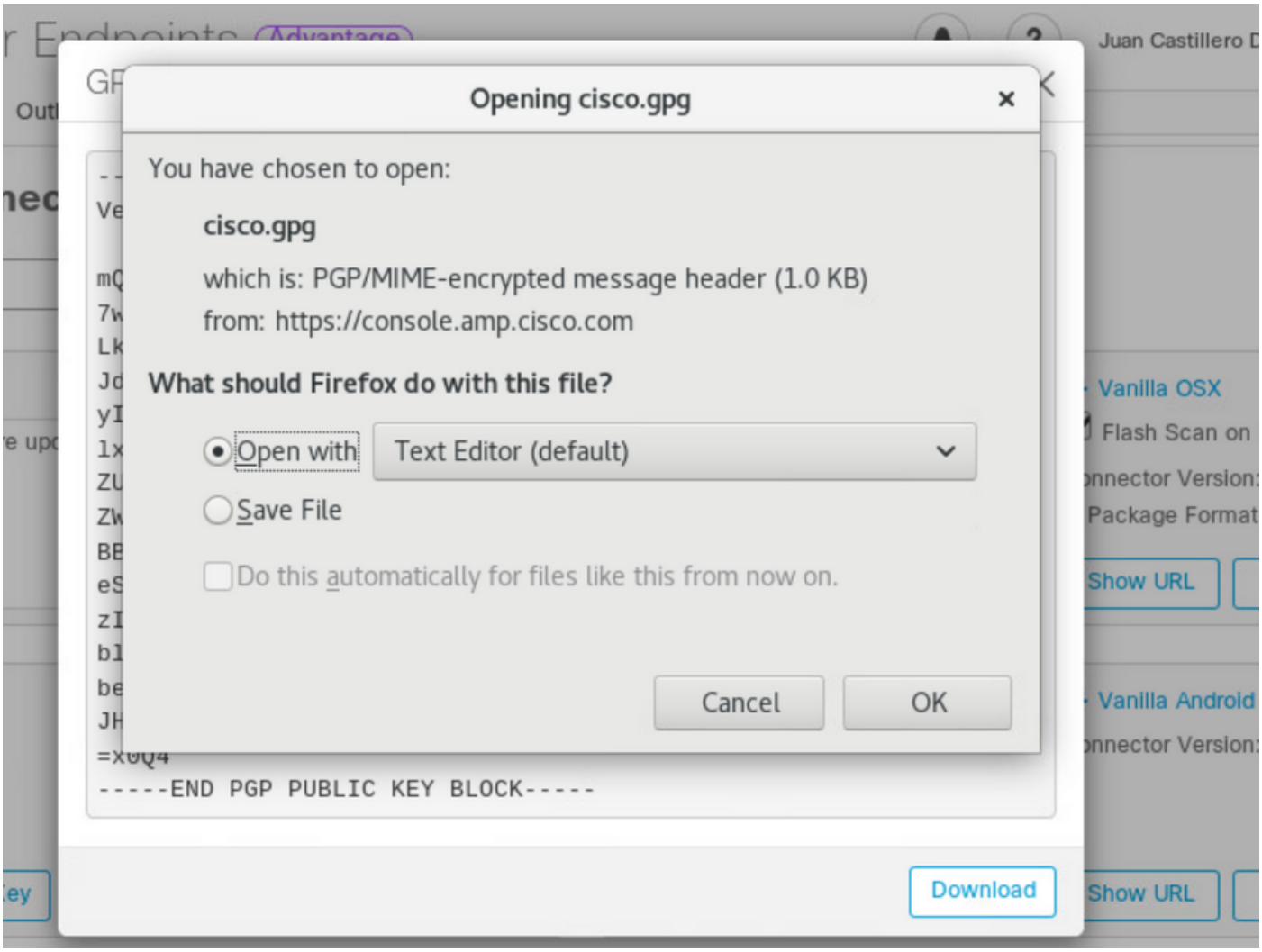
Nadat de installatie is begonnen, is er geen gebruikersinvoer vereist. Het is een automatisch proces, zoals in de afbeelding wordt weergegeven.

Hoe de GPG-toets te importeren

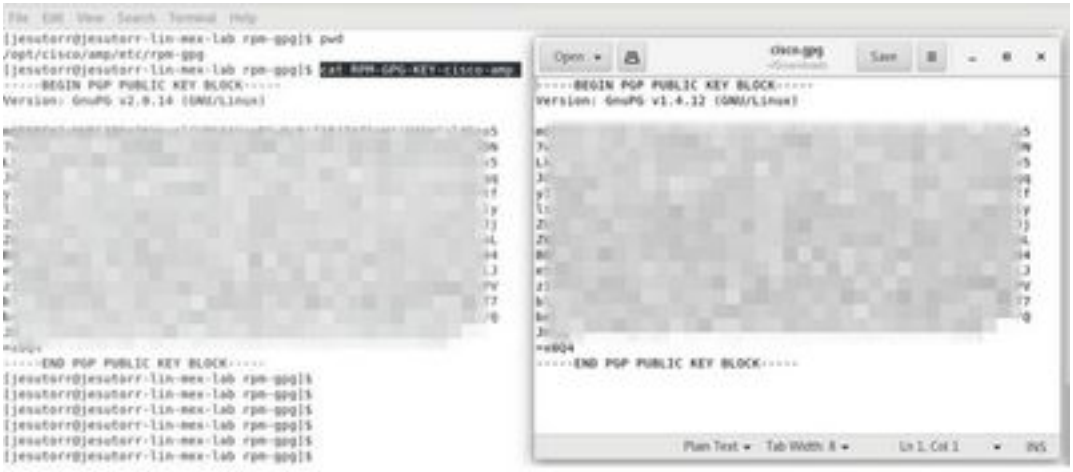
De openbare sleutel van GPG kan van de pagina van de Download Connector worden gekopieerd om de ondertekening van het RPM - pakket te verifiëren. De connector kan worden geïnstalleerd zonder de GPG-toets; echter : een gebruiker De GPG-toets zou in hun RPM-DB moeten importeren indien zij voornemens zijn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

Opmerking: Om te beginnen met verbindingsversie 1.17.0, wordt de GPG-toets die wordt gebruikt om upgradepakketten te controleren tijdens verbindingsupdates 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**.



Stap 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**.



Stap 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'**.

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

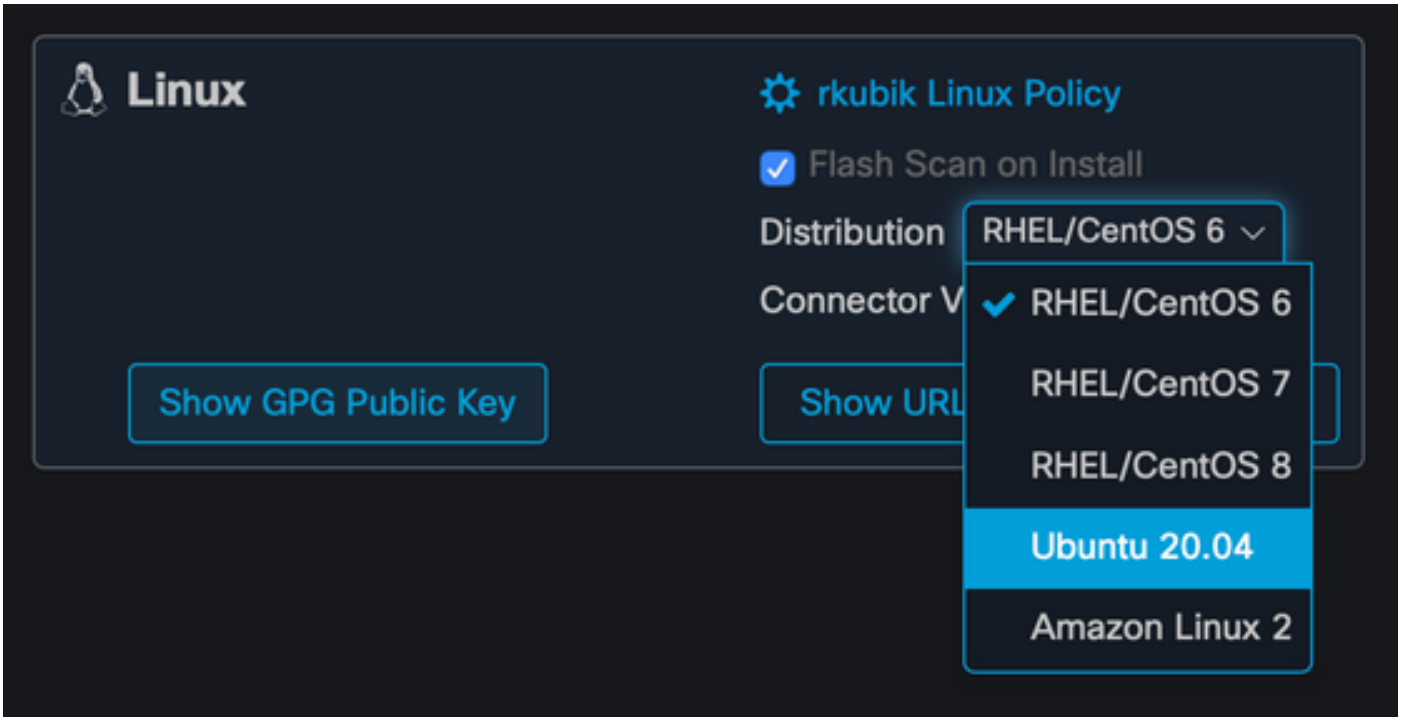
ingang van het systeem en wanneer een update beschikbaar is, start automatisch het RPM-upgradeproces. Sommige SELinux-configuraties verbieden dit gedrag en veroorzaken de Updater om te falen.

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

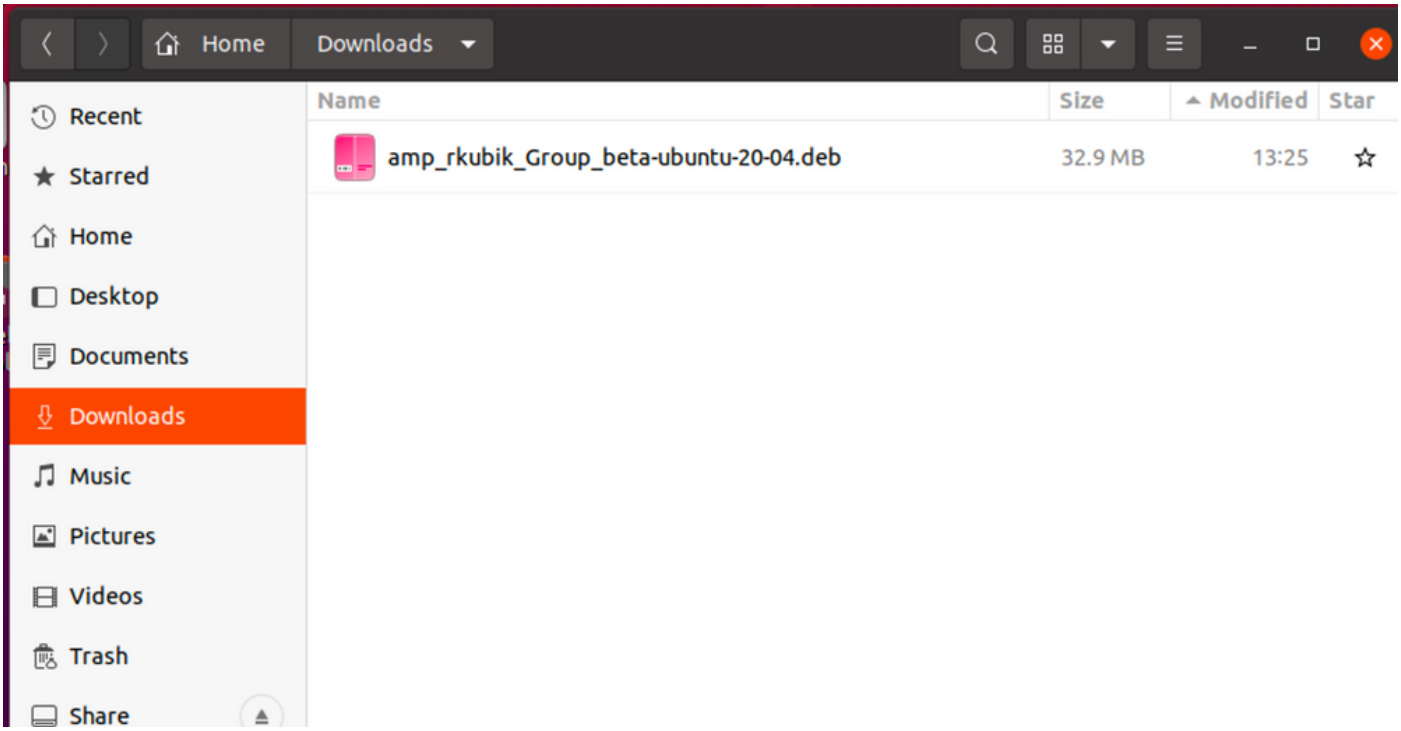
Ubuntu

Configuraties

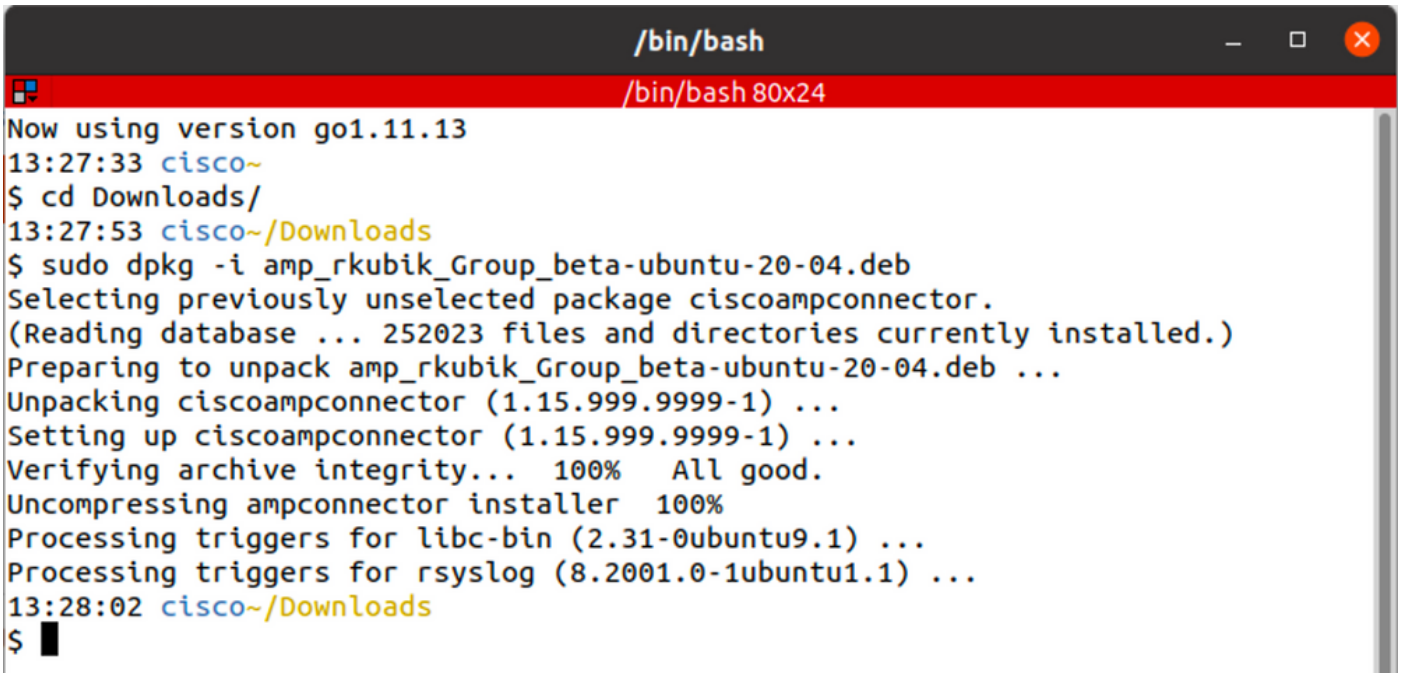
Stap 1. Download het Linux DEB-pakket van Cisco Secure Endpoint Portal, zoals in de afbeelding.



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.



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 verbindingsupdates 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

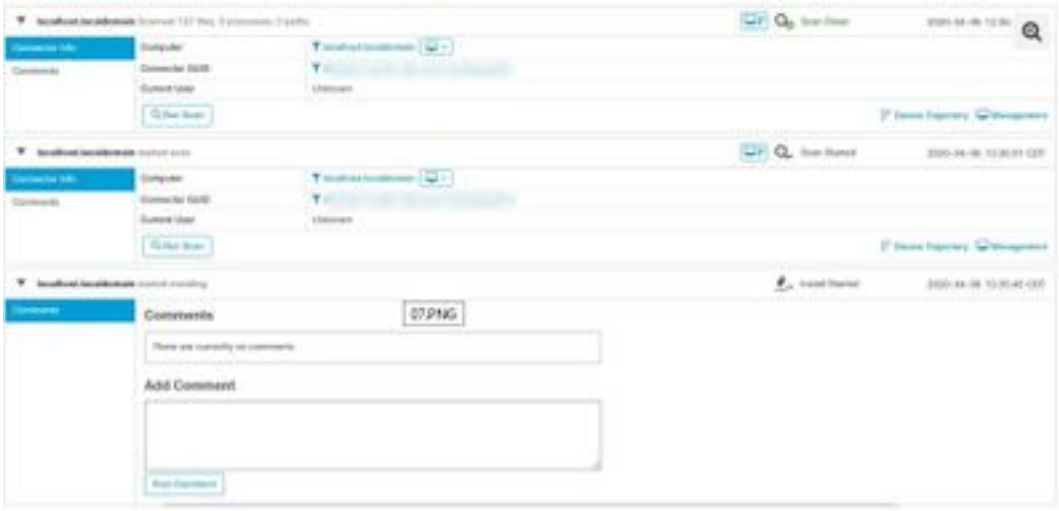
Opmerking: Om te beginnen met verbindingsversie 1.17.0, wordt de GPG-toets die wordt gebruikt om upgradepakketten te controleren tijdens verbindingsupdates automatisch geïnstalleerd. Om deze GPG-toets te controleren klikt u op de GPG Public Key link op de pagina van de Download Connector en vergelijkt 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.**

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