Installation du connecteur Cisco Secure Endpoint Linux

Contenu

Introduction

Ce document décrit comment installer et vérifier le connecteur Cisco Secure Endpoint Linux pour Red Hat Enterprise Linux (RHEL) et les systèmes basés sur Debian.

Contribué par Juan Carlos Castillero et édité par Yeraldin Sanchez, Ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Machines Linux sur un connecteur Linux Système d'exploitation (OS) pris en charge

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

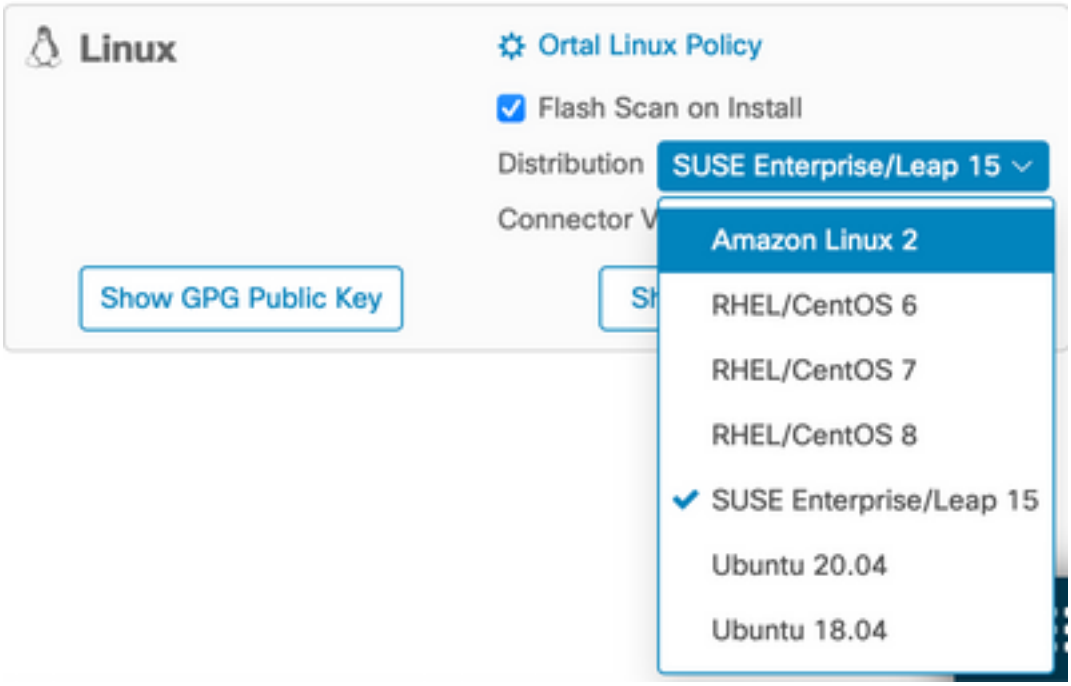
- Un installateur de connecteur Linux Secure Endpoint Red Hat Package Manager (RPM)
- Un installateur de connecteurs Linux Secure Endpoint Debian Package Manager (dpkg)
- Clé GNU Privacy Guard (GPG) pour vérifier les mises à jour (facultatif)
- Un installateur de connecteurs Linux DPKG (Debian Package Management System)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

RHEL/CentOS/Amazon Linux 2/SUSE 15

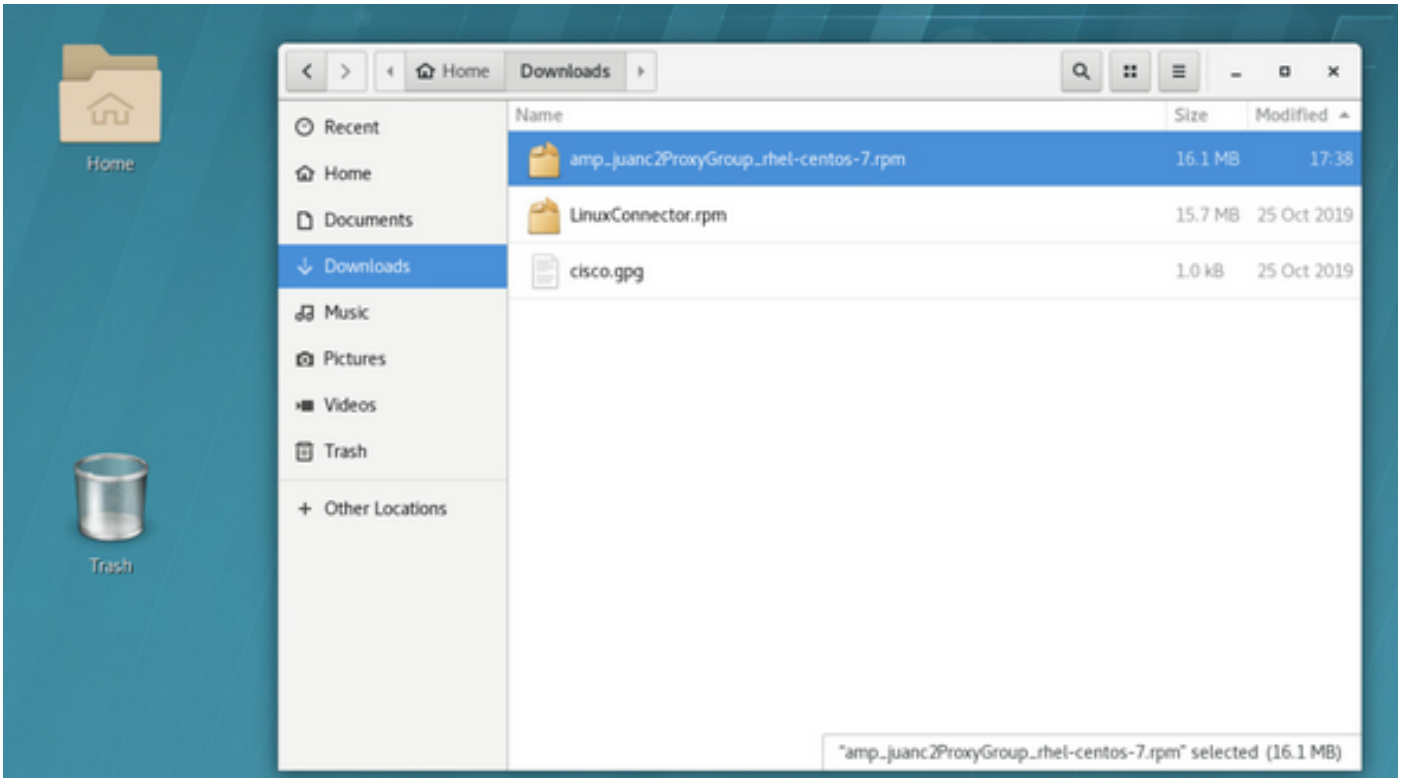
Configurations

Étape 1. Téléchargez le package RPM Linux depuis le portail Cisco Secure Endpoint, comme illustré dans l'image.



> **Note**: N'oubliez pas que la distribution du système d'exploitation est importante car les deux connecteurs ont des architectures radicalement différentes.

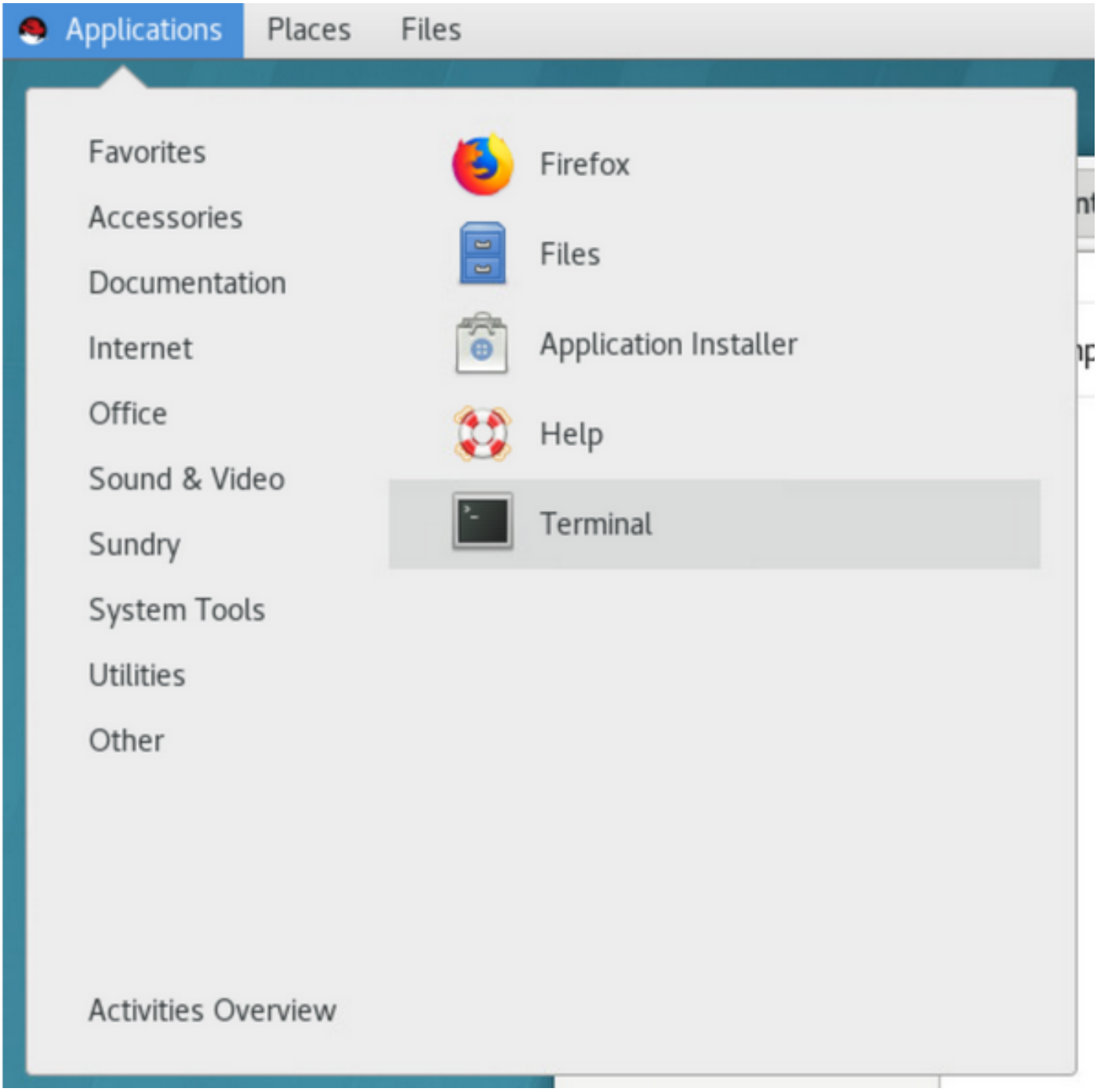
Étape 2. Déplacez le package RPM vers le point de terminaison en question, soit le téléchargez directement à partir du tableau de bord, soit le déplacez manuellement vers les points de terminaison. Dans cet exemple, une interface utilisateur graphique (UI) est utilisée, bien qu'il soit possible, et souvent courant, de travailler avec une installation minimale, auquel cas il est nécessaire de savoir comment gérer le terminal Linux et trouver leur paquet RPM.



Étape 3. Pour installer le connecteur Linux, exécutez la commande suivante : **sudo yum localinstall [paquet rpm] -y** (ou **sudo zypper install -y [paquet rpm]** sur SUSE 15)

où [paquet rpm] est le nom du fichier, par exemple, « amp_Audit.rpm ». Le package RPM doit être installé pendant l'exécution du service atd.

Si l'interface utilisateur graphique est utilisée, ouvrez le terminal, comme l'illustre l'image.



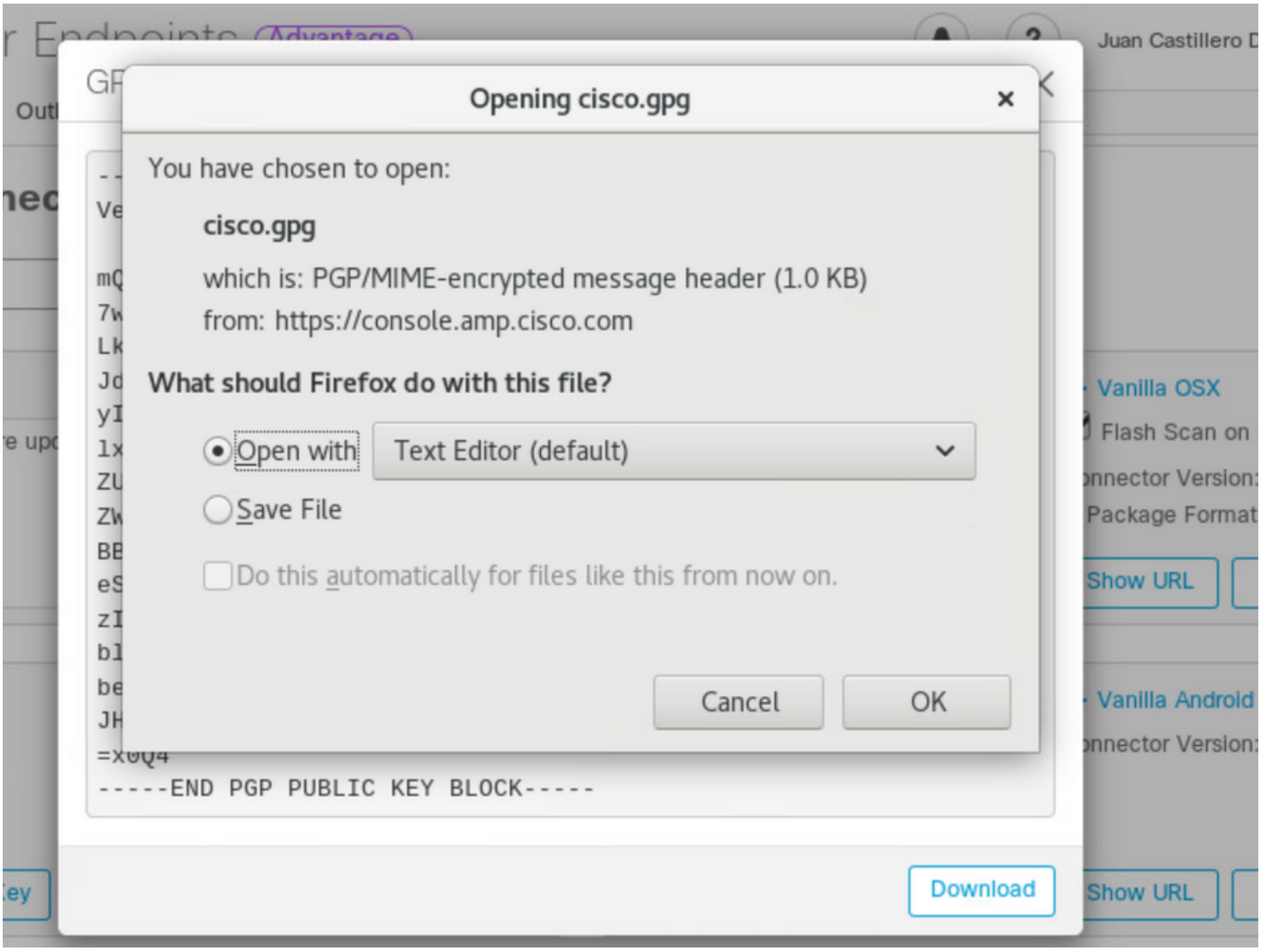
Une fois l'installation commencée, aucune entrée utilisateur n'est requise, il s'agit d'un processus automatique, comme illustré dans l'image.

Comment importer la clé GPG

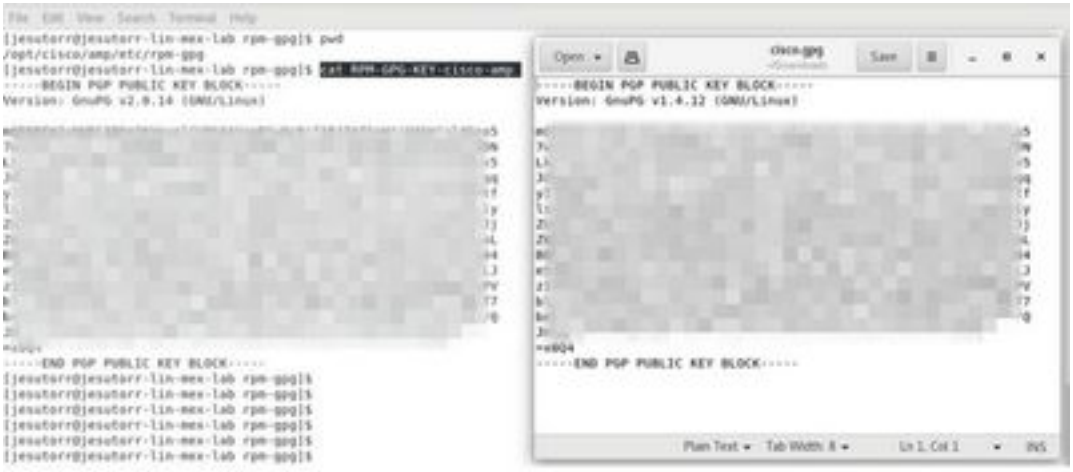
La clé publique GPG peut être copiée à partir de la page Download Connector pour vérifier la signature du package RPM. Le connecteur peut être installé sans la clé GPG; cependant, un utilisateur doit importer la clé GPG dans leur base de données RPM s'ils prévoient de pousser les mises à jour des connecteurs via une stratégie sur RHEL.

Note: À partir de la version 1.17.0 du connecteur, la clé GPG utilisée pour vérifier les packages de mise à niveau lors des mises à jour du connecteur est installée automatiquement.

Étape 1. Vérifiez la clé GPG, cliquez sur le lien Clé publique GPG sur la page Download Connector. Comparez la clé à celle de **/opt/cisco/amp/etc/rpm-gpg/RPM-GPG-Key-cisco-amp**.



Étape 2. Exécutez la commande à partir d'un terminal pour importer la clé : **sudo rpm —import /opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp**.



Étape 3. Vérifiez que la clé a été installée, exécutez la commande à partir du terminal : **rpm -q gpg-pubkey —qf '%{name}-%{version}-%{release} —> %{summary}\n'**.

Étape 4. Recherchez une clé GPG de Sourcefire dans le résultat. Le Updater est exécuté par le

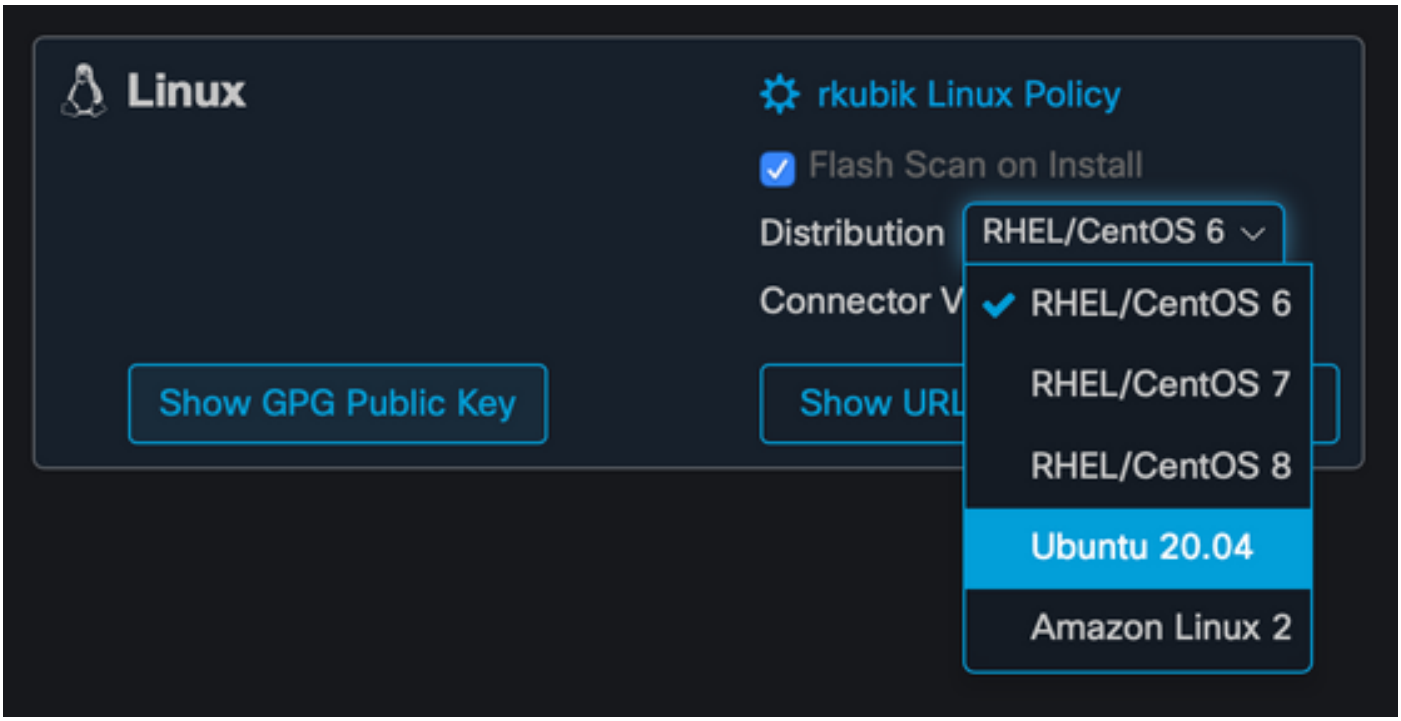
démon d'initialisation du système et lorsqu'une mise à jour est disponible, déclenche automatiquement le processus de mise à niveau RPM. Certaines configurations SELinux interdisent ce comportement et provoquent l'échec du Updater.

Si vous pensez que c'est le cas, examinez le journal d'audit du système (par exemple, **/var/log/audit/audit.log**) et recherchez les événements de refus liés à ampupdater. Vous devrez peut-être ajuster les règles SELinux pour permettre à Updater de fonctionner.

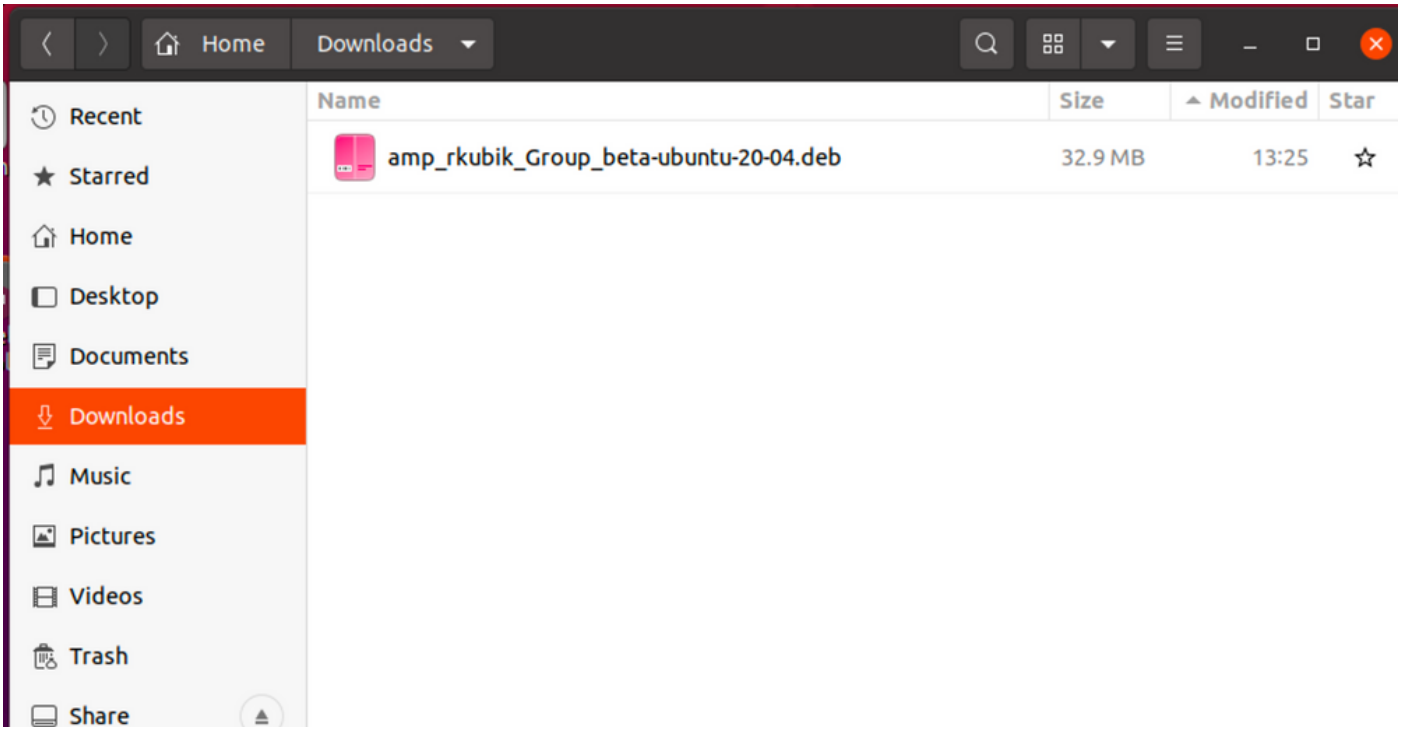
Ubuntu

Configurations

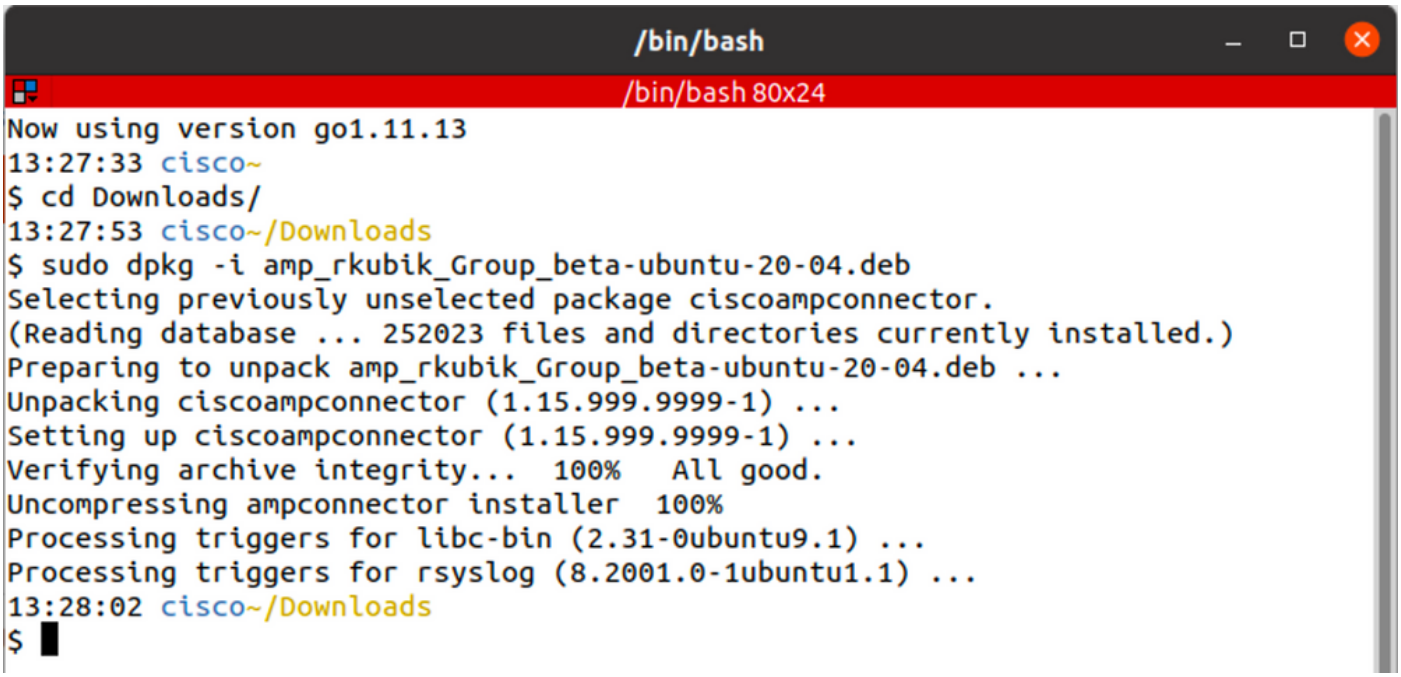
Étape 1. Téléchargez le package DEB Linux depuis le portail Cisco Secure Endpoint, comme illustré dans l'image.



Étape 2. Déplacez le package DEB vers le point de terminaison en question, soit le téléchargez directement à partir du tableau de bord, soit le déplacez manuellement vers les points de terminaison. Dans cet exemple, une interface utilisateur graphique (UI) est utilisée, bien qu'il soit possible, et souvent courant, de travailler avec une installation minimale, auquel cas il est nécessaire de savoir comment gérer le terminal Linux et trouver leur paquet DEB.



Étape 3. Pour installer le connecteur Linux, exécutez la commande suivante : **sudo dpkg -i [paquet deb]** où [paquet deb] est le nom du fichier, par exemple, « amp_Audit.deb ». Une fois l'installation commencée, aucune entrée utilisateur n'est requise, il s'agit d'un processus automatique, comme illustré dans l'image.



Comment importer la clé GPG

La clé publique GPG peut être copiée à partir de la page Download Connector pour vérifier la signature du paquet DEB. Le connecteur peut être installé sans la clé GPG ; cependant, un utilisateur devrait importer la clé GPG dans sa clé de débit s'il prévoit de pousser les mises à jour des connecteurs via une stratégie sur Ubuntu. Pour plus d'informations sur l'importation de la clé GPG et la vérification que le connecteur n'a pas été modifié sur Ubuntu, consultez https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/216524-amp-for-endpoints-ubuntu-connector.html#anc6

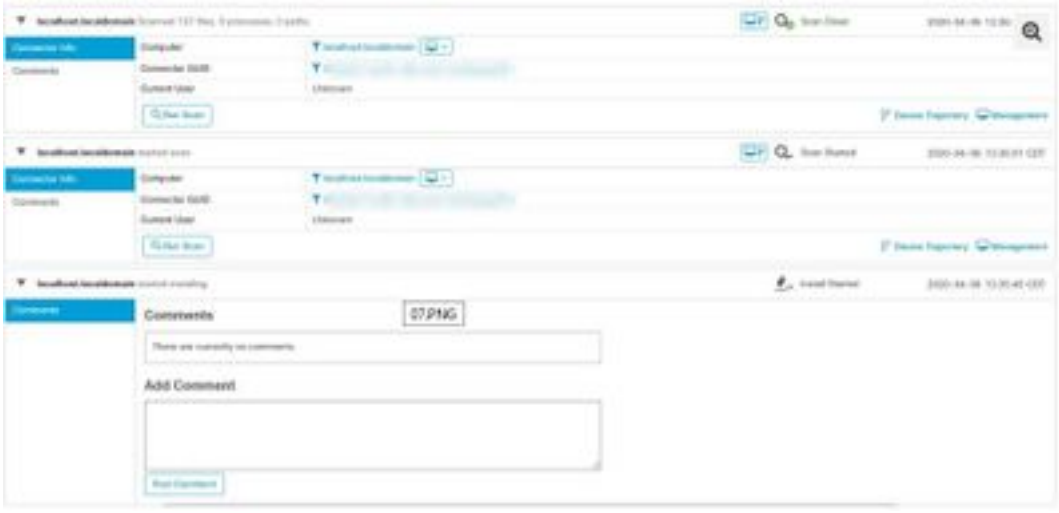
Note: À partir de la version 1.17.0 du connecteur, la clé GPG utilisée pour vérifier les packages de mise à niveau lors des mises à jour du connecteur est installée automatiquement. Pour vérifier cette clé GPG, cliquez sur le lien Clé publique GPG sur la page du connecteur de téléchargement et comparez-la à la clé qui a été installée sur **/opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-Key-cisco-amp**.

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Afin de vérifier l'installation réussie, exécutez l'**interface de ligne de commande AMP**. L'interface de ligne de commande du connecteur Linux se trouve sur **/opt/cisco/amp/bin/ampcli**. Il peut être exécuté en mode interactif ou exécuter une seule commande, puis quitter. Exécutez la commande **./ampcli —help** pour afficher une liste complète des options et commandes disponibles. Tous les fichiers journaux générés par le connecteur se trouvent dans **/var/log/cisco.**

Un événement d'installation apparaît également sur la console Cisco Secure, si des analyses Flash ont été demandées lors du téléchargement du package RPM, elles s'affichent également.



Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Installer le connecteur AMP for Endpoints dans la vidéo Linux

- Support et documentation techniques - Cisco Systems