Instalação do Cisco Secure Endpoint Linux Connector

Contents

Introduction

Este documento descreve como instalar e verificar o conector Cisco Secure Endpoint Linux para sistemas baseados em Red Hat Enterprise Linux (RHEL) e Debian.

Contribuído por Juan Carlos Castillero e editado por Yeraldin Sanchez, Engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Máquinas Linux em um sistema operacional (SO) compatível com conector Linux

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

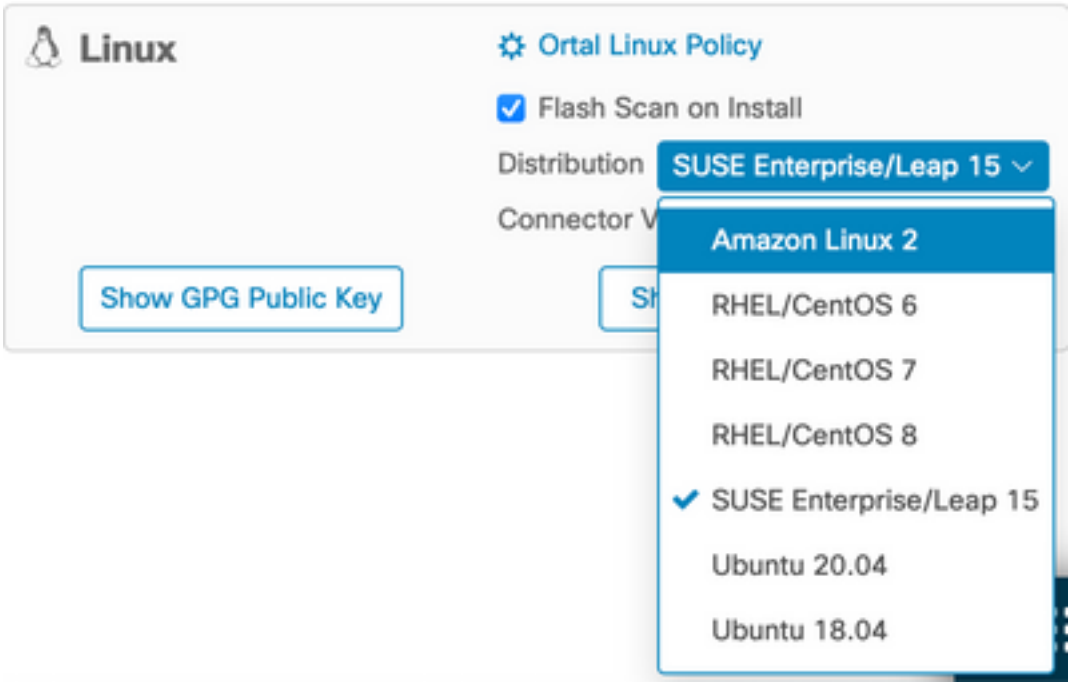
- Um instalador de conector Linux Secure Endpoint Red Hat Package Manager (RPM)
- Um instalador de conector Linux Secure Endpoint Debian Package Manager (dpkg)
- Uma chave GNU Privacy Guard (GPG) para verificar atualizações (opcional)
- Um instalador de conector Linux DPKG (Debian Package Management 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

RHEL/CentOS/Amazon Linux 2/SUSE 15

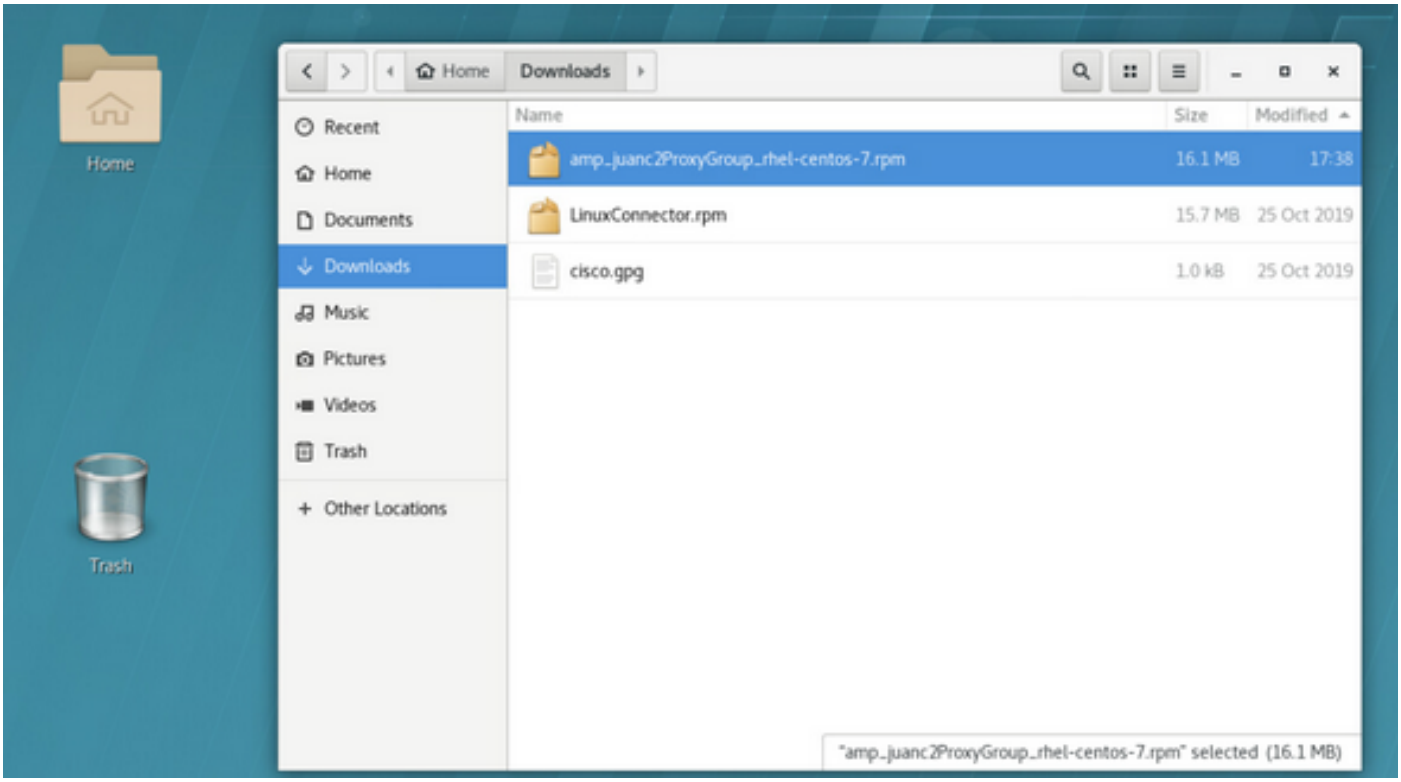
Configurações

Etapa 1. Baixe o pacote RPM do Linux do Cisco Secure Endpoint Portal, como mostrado na imagem.



> **Note**: Lembre-se de que a distribuição do SO é importante, pois ambos os conectores diferentes têm arquiteturas drasticamente diferentes.

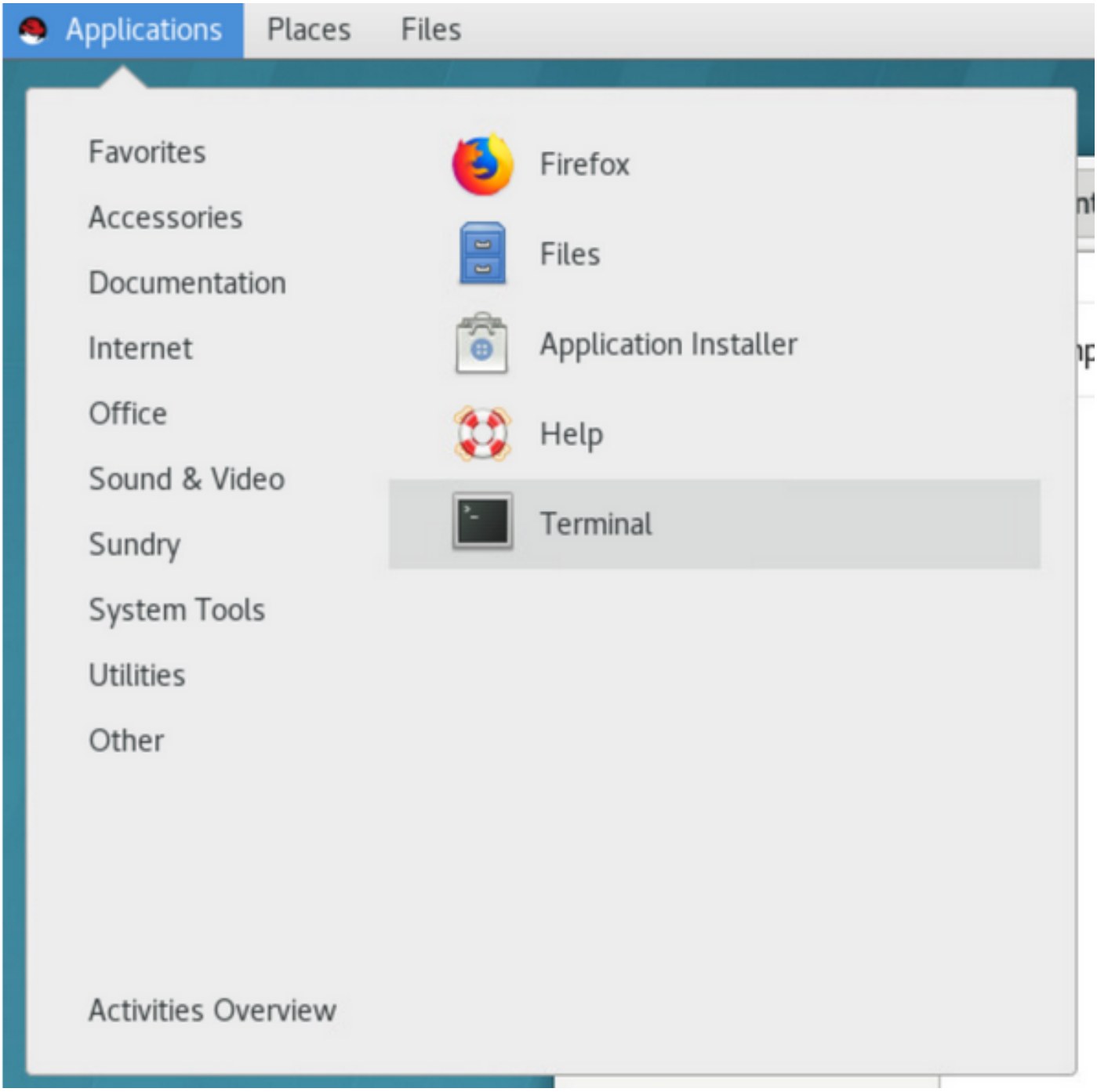
Etapa 2. Mova o pacote RPM para o endpoint em questão, faça o download diretamente do painel ou mova-o manualmente para os endpoints. Para este exemplo, uma Interface Gráfica de Usuário (UI) é usada, embora seja possível, e geralmente comum, trabalhar com uma instalação mínima, caso em que é necessário saber como lidar com o terminal Linux e encontrar seu pacote RPM.



Etapa 3. Para instalar o conector Linux, execute o comando: **sudo yum localinstall [pacote rpm] -y** (ou **sudo zypper install -y [pacote rpm]** no SUSE 15)

onde [rpm package] é o nome do arquivo, por exemplo, "amp_Audit.rpm". O pacote RPM precisa ser instalado enquanto o serviço atd é executado.

Se a GUI estiver em uso, abra o terminal, como mostrado na imagem.



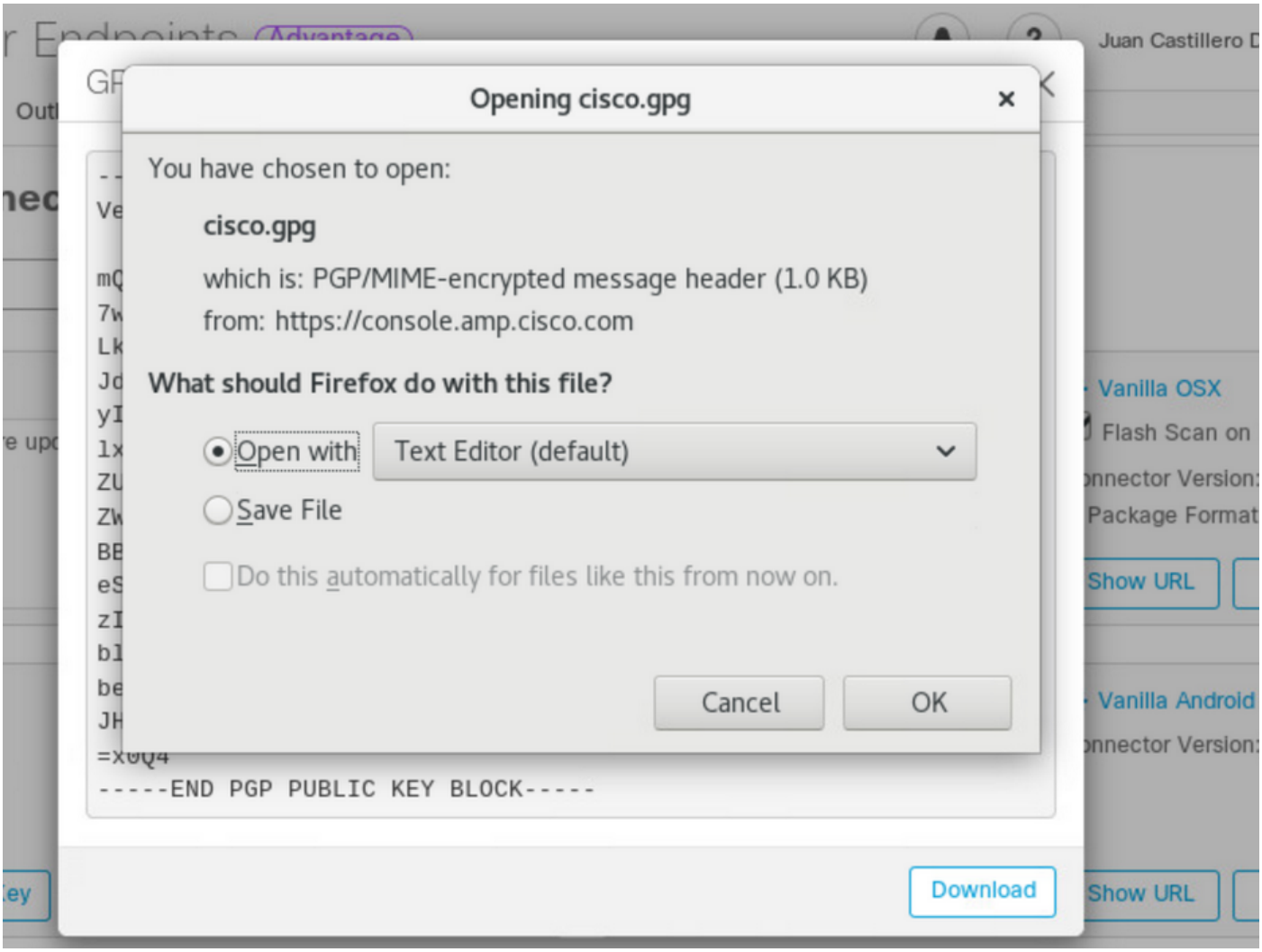
Quando a instalação começa, não é necessária nenhuma entrada do usuário, é um processo automático, como mostrado na imagem.

Como importar a chave GPG

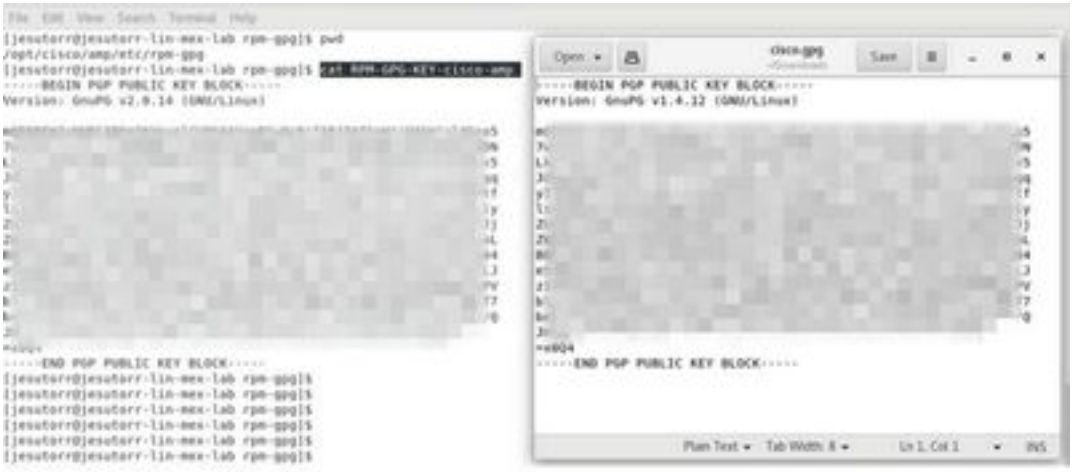
A chave pública GPG pode ser copiada da página Download Connector para verificar a assinatura do pacote RPM. O conector pode ser instalado sem a chave GPG; no entanto, um usuário precisariam importar a chave GPG para o seu RPM DB se planejarem enviar atualizações de conector por meio da política no RHEL.

Note: A partir do conector versão 1.17.0, a chave GPG usada para verificar os pacotes de atualização durante as atualizações dos conectores é instalada automaticamente.

Etapa 1. Verifique a chave GPG e clique no link Chave pública GPG na página Conector de download. Compare a chave com a chave em **/opt/cisco/amp/etc/rpm-gpg/RPM-GPG-Key-cisco-amp**.



Etapa 2. Execute o comando de um terminal para importar a chave: **sudo rpm — import /opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp**.



Etapa 3. Verifique se a chave foi instalada, execute o comando a partir do terminal: **rpm -q gpg-pubkey —qf '%{name}-%{version}-%{release} —> %{summary}\n'**.

Etapa 4. Procure uma chave GPG da Sourcefire na saída. O Atualizador é executado pelo

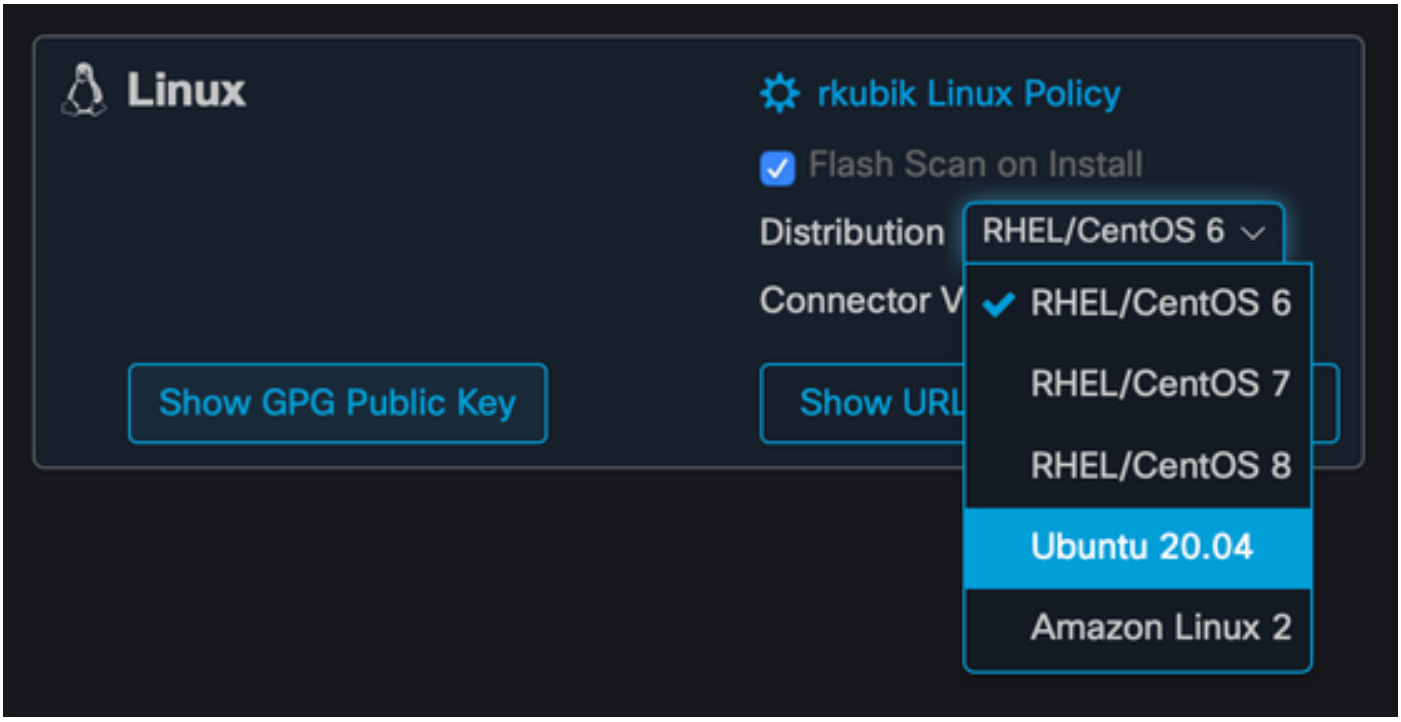
daemon de inicialização do sistema e quando uma atualização está disponível, aciona automaticamente o processo de atualização do RPM. Algumas configurações do SELinux proíbem esse comportamento e fazem com que o Updater falhe.

Se suspeitar que seja esse o caso, examine o log de auditoria do sistema (por exemplo, **/var/log/audit/audit.log**) e pesquise por eventos de negação relacionados ao ampupdater. Talvez seja necessário ajustar as regras do SELinux para permitir que o Updater funcione.

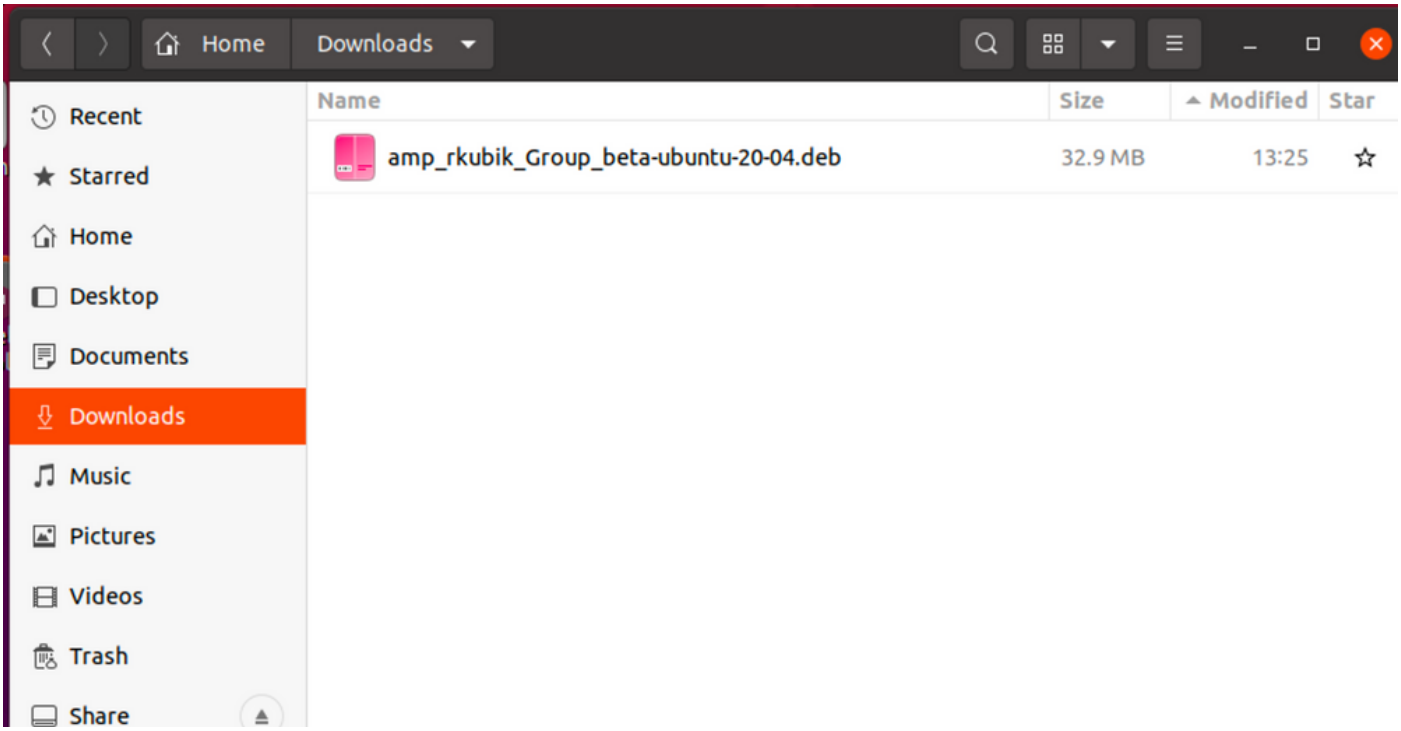
Ubuntu

Configurações

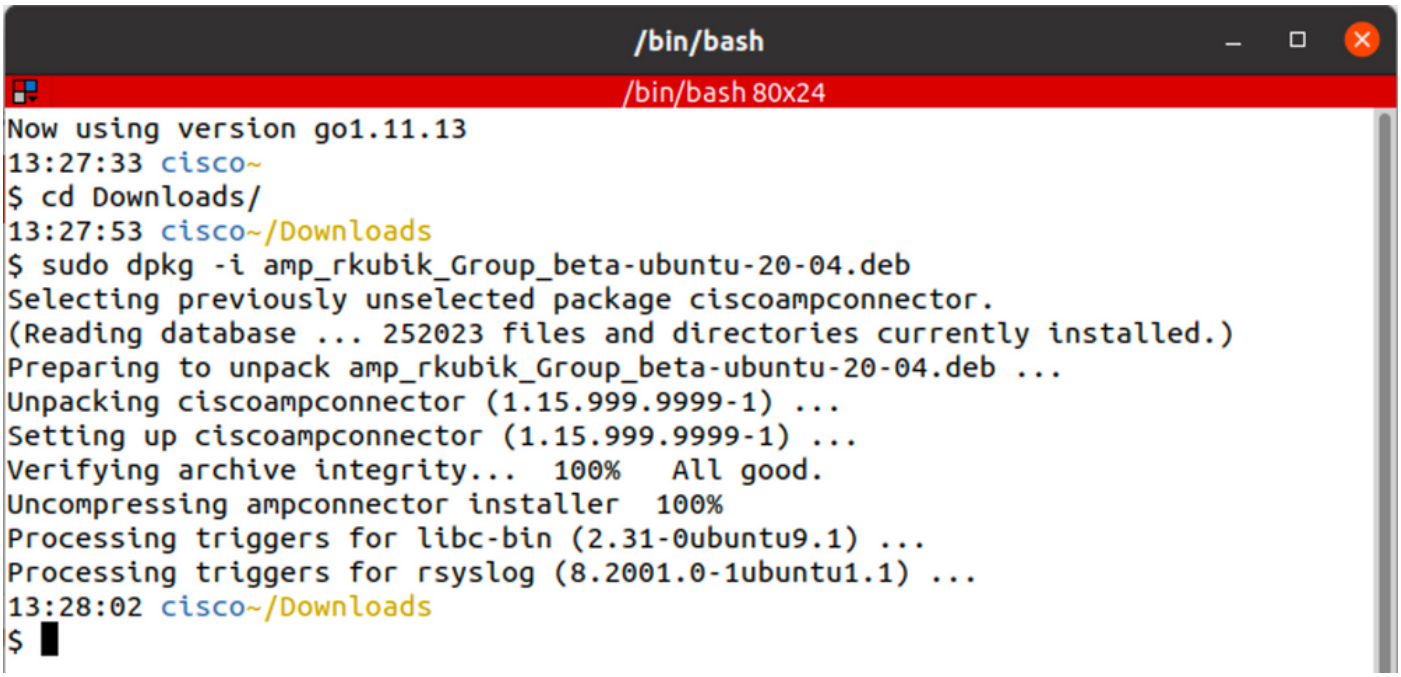
Etapa 1. Baixe o pacote Linux DEB do Cisco Secure Endpoint Portal, como mostrado na imagem.



Etapa 2. Mova o pacote DEB para o endpoint em questão, baixe-o diretamente do painel ou mova-o manualmente para os endpoints. Para este exemplo, uma Interface Gráfica de Usuário (UI) é usada, embora seja possível, e geralmente comum, trabalhar com uma instalação mínima, caso em que é necessário saber como lidar com o terminal Linux e encontrar seu pacote DEB.



Etapa 3. Para instalar o conector Linux, execute o comando: **sudo dpkg -i [deb package]** onde [deb package] é o nome do arquivo, por exemplo, "amp_Audit.deb". Quando a instalação começa, não é necessária nenhuma entrada do usuário, é um processo automático, como mostrado na imagem.



Como importar a chave GPG

A chave pública GPG pode ser copiada da página Download Connector para verificar a assinatura do pacote DEB. O conector pode ser instalado sem a chave GPG; no entanto, um usuário precisaria importar a chave GPG para o seu keyring debsig se planejasse enviar atualizações de conectores por meio da política do Ubuntu. Para obter mais informações sobre como importar a chave GPG e verificar se o conector não foi modificado no Ubuntu, consulte https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/216524-amp-for-endpoints-ubuntu-connector.html#anc6

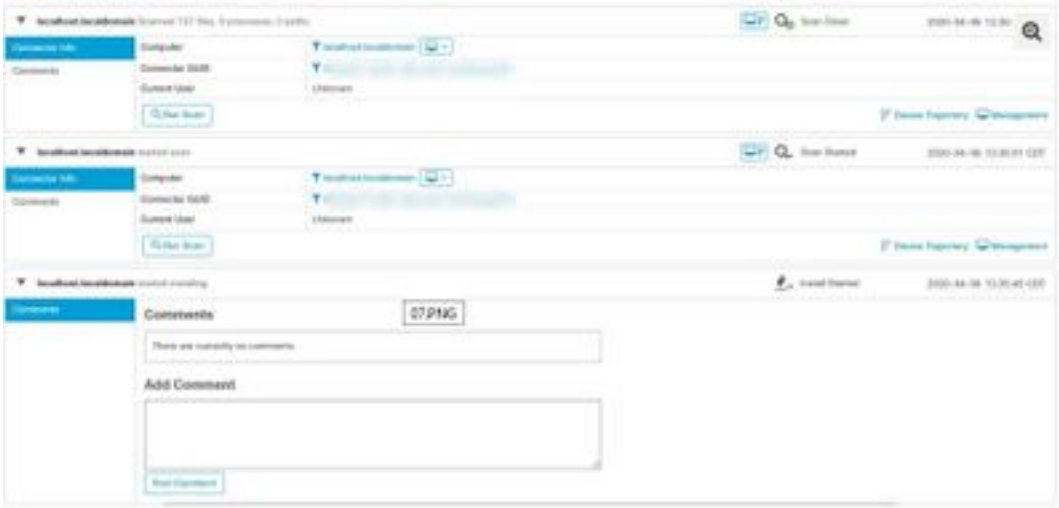
Note: A partir do conector versão 1.17.0, a chave GPG usada para verificar os pacotes de atualização durante as atualizações dos conectores é instalada automaticamente. Para verificar essa chave GPG, clique no link Chave pública GPG na página Conector de download e compare-o com a chave instalada em **/opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-Key-cisco-amp**.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Para verificar a instalação bem-sucedida, execute a **CLI do AMP**. A interface de linha de comando do conector Linux pode ser encontrada em **/opt/cisco/amp/bin/ampcli**. Ele pode ser executado no modo interativo ou executar um único comando e depois sair. Execute o comando **./ampcli —help** para ver uma lista completa de opções e comandos disponíveis. Todos os arquivos de log gerados pelo conector podem ser encontrados em **/var/log/cisco.**

Um evento de instalação também é exibido no console Cisco Secure, se as verificações flash forem solicitadas quando o pacote RPM for baixado, elas também serão exibidas.



Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Instalar o conector AMP para endpoints em vídeo Linux

- Suporte Técnico e Documentação - Cisco Systems