

Instalação do Cisco Secure Endpoint Linux Connector

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

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

[Configurações](#)

[Como importar a chave GPG](#)

[Ubuntu](#)

[Configurações](#)

[Como importar a chave GPG](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

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:

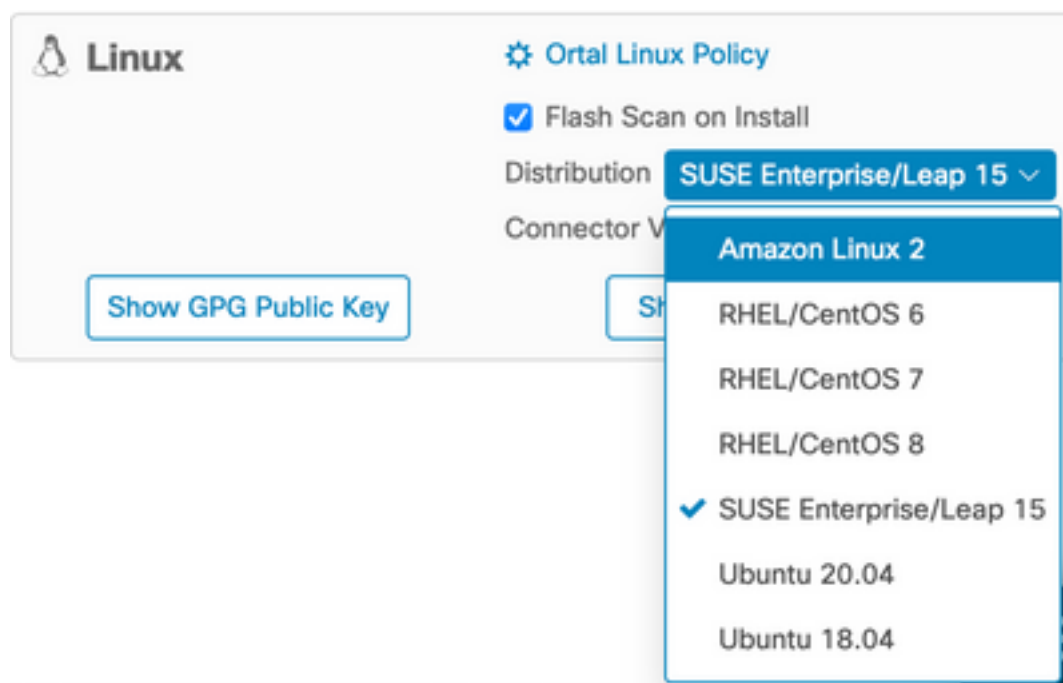
- Um instalador de conector Linux Secure Endpoint Red Hat Package Manager (RPM)
- Um instalador de conector Linux Secure Endpoint Debian Package Manager (dpkg)
- Uma chave GNU Privacy Guard (GPG) para verificar atualizações (opcional)
- Um instalador de conector Linux DPKG (Debian Package Management 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

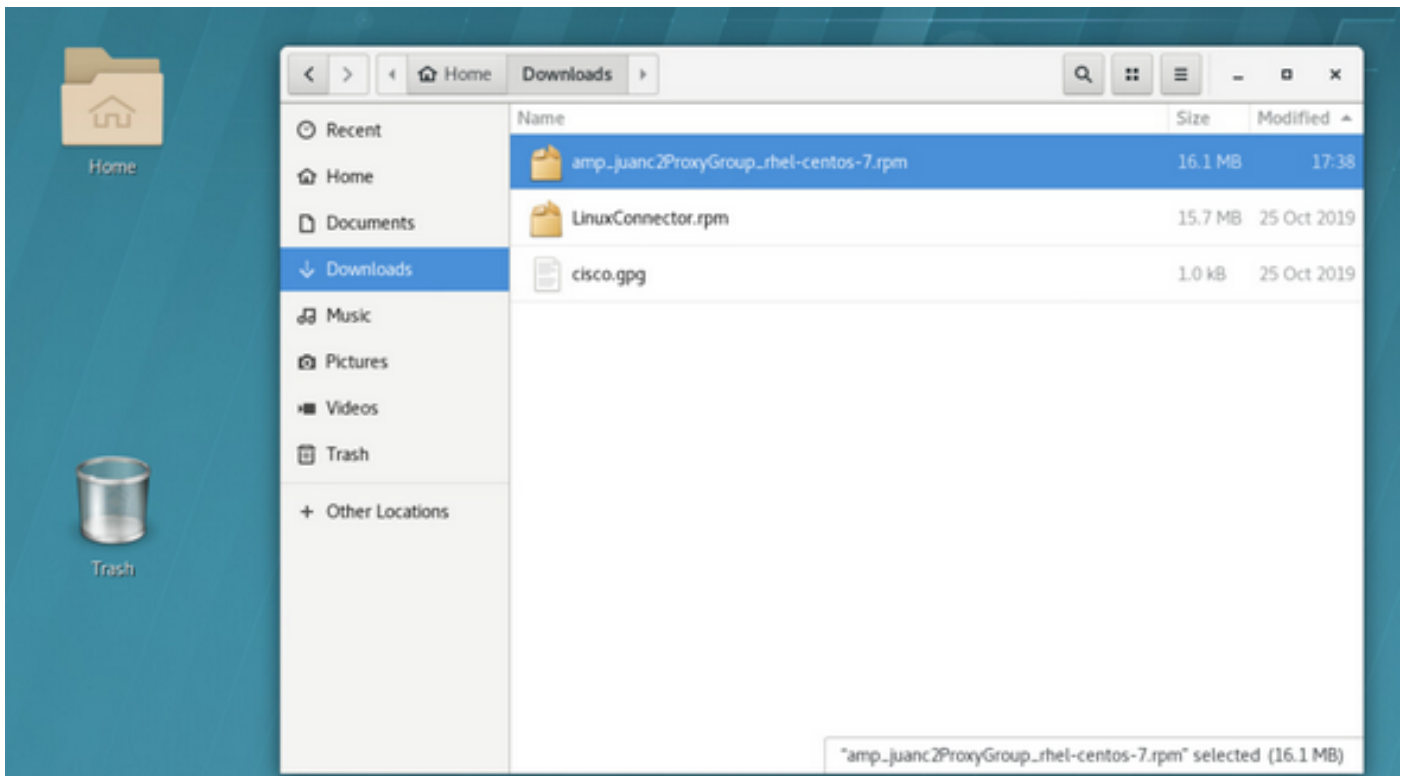
Configurações

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.

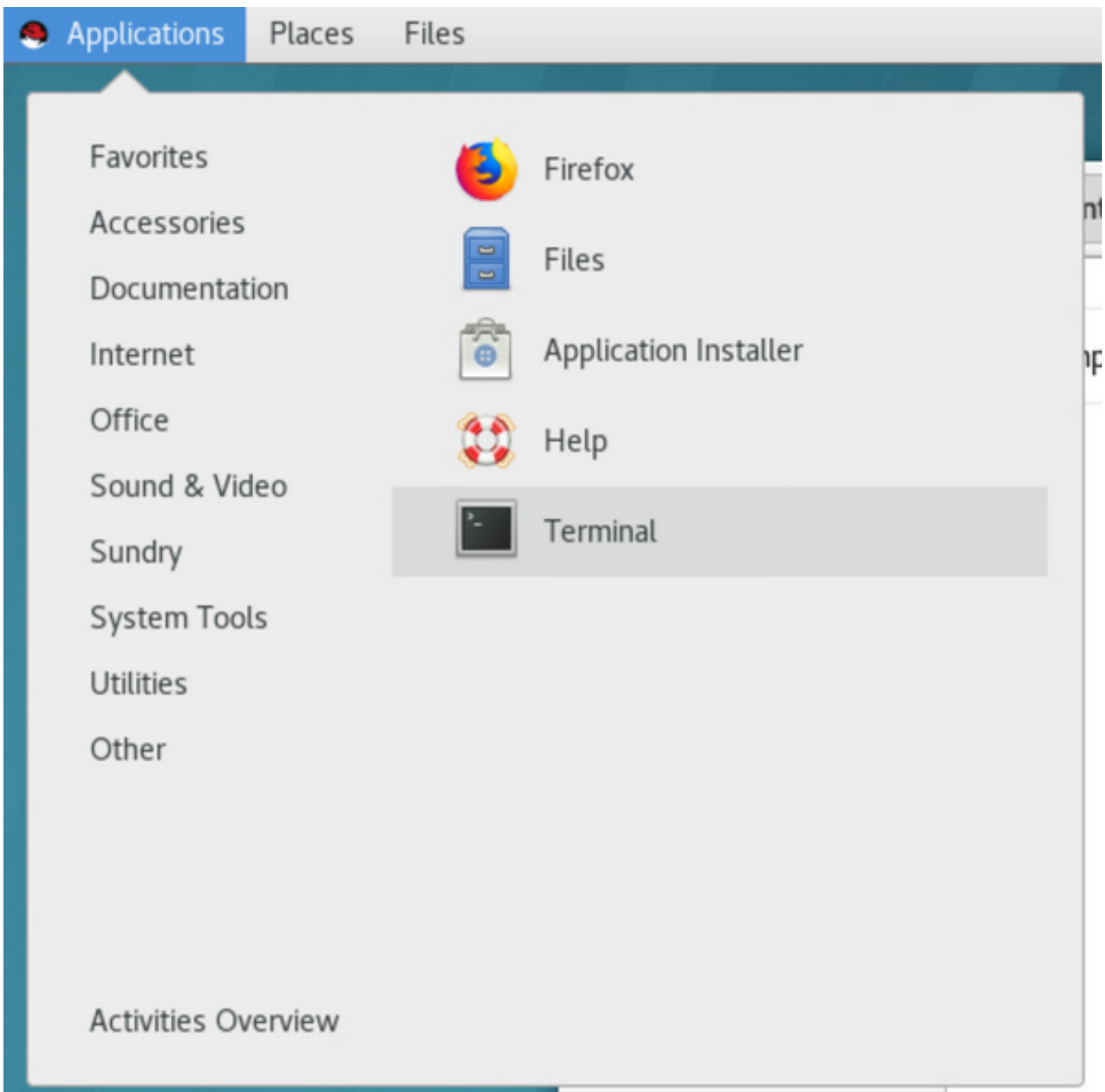
```
File Edit View Search Terminal Help
[jesuitor@jesuitor-11m-aaa-lab Downloads] sudo yum localinstall amp_juanc2ProxyGroup_rhel-centos-7.rpm -y
[sudo] password for jesuitor:
Loaded plugins: langpacks, product-id, search-disabled-repos, subscription-manager
This system is not registered with an entitlement 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
```

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.

```
File Edit View Search Terminal Help
ipating:
ciscoampconnector x86_64 1.12.2.602-1.el7 /amp_juanc2ProxyGroup_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-1.12.2.630-1.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 2/2

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

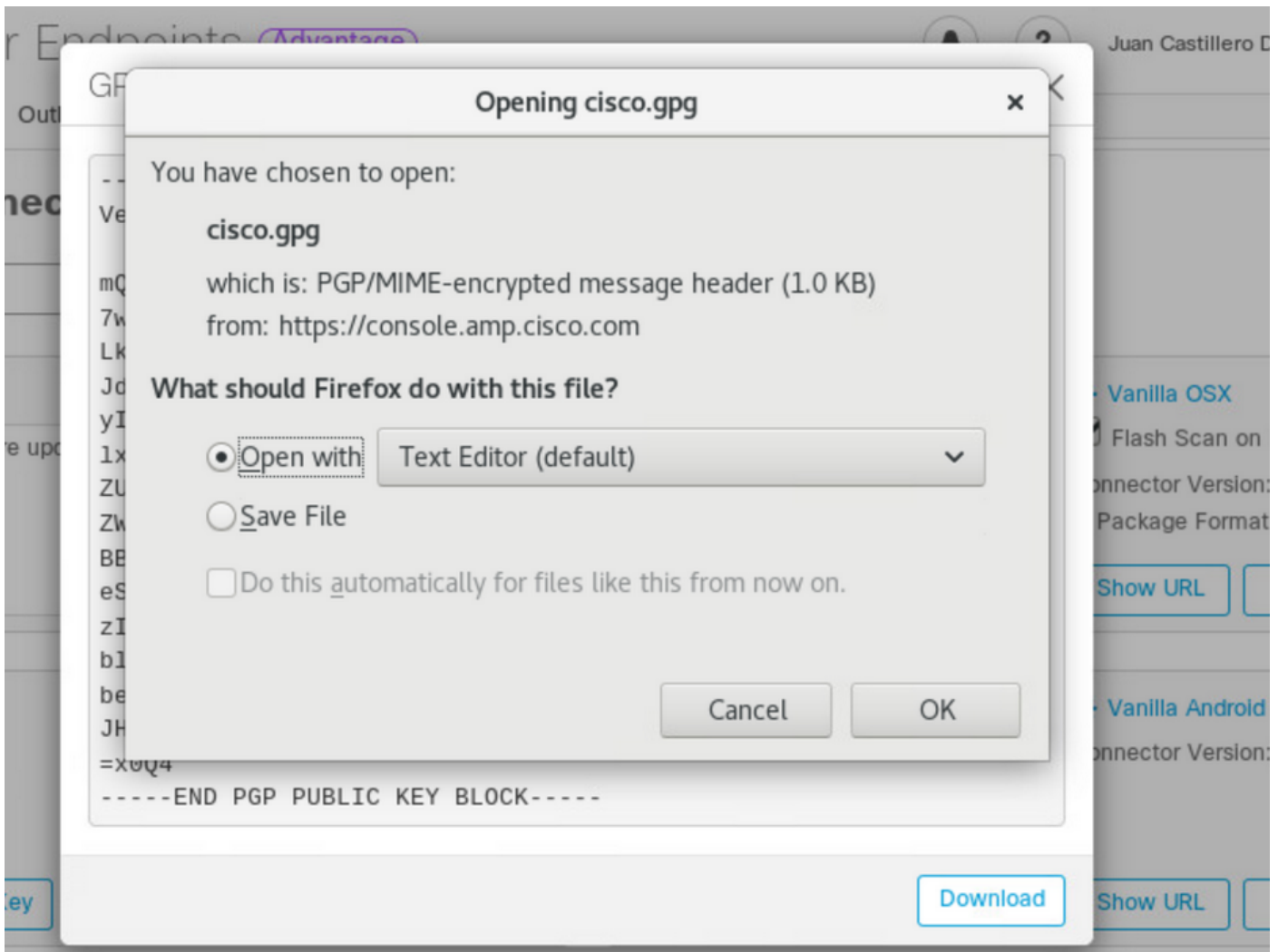
Como importar a chave GPG

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.

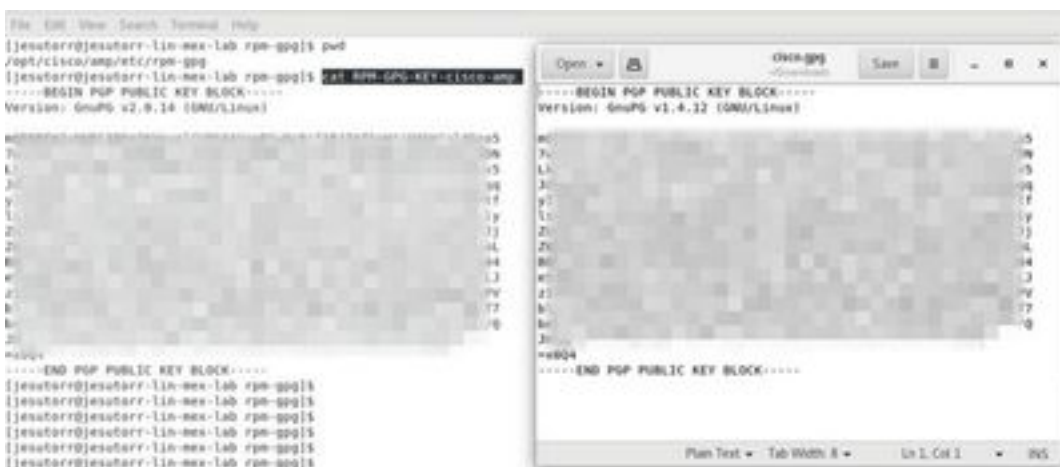
Note: A partir do conector versão 1.17.0, a chave GPG usada para verificar os pacotes de atualização durante as atualizações dos conectores é instalada automaticamente.

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

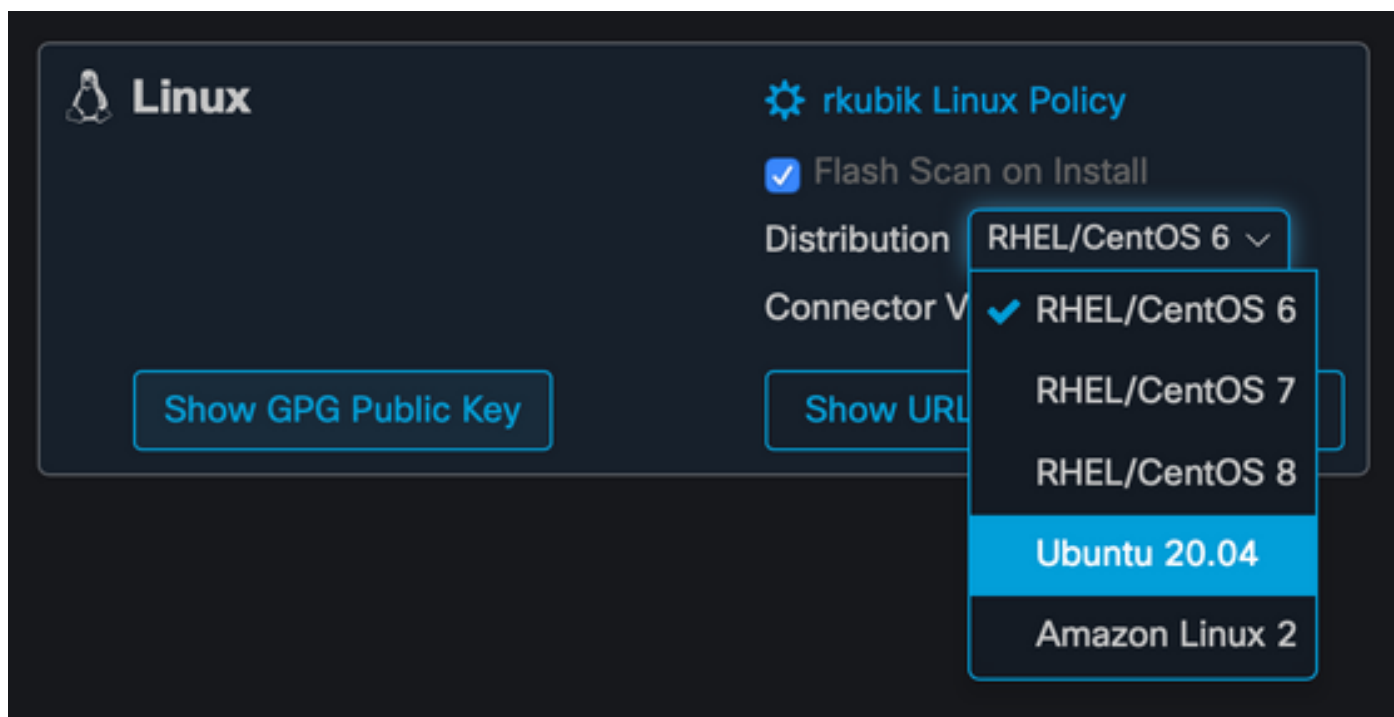
daemon de inicialização do sistema e quando uma atualização está disponível, aciona automaticamente o processo de atualização do RPM. Algumas configurações do SELinux proíbem esse comportamento e fazem com que o Updater falhe.

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.

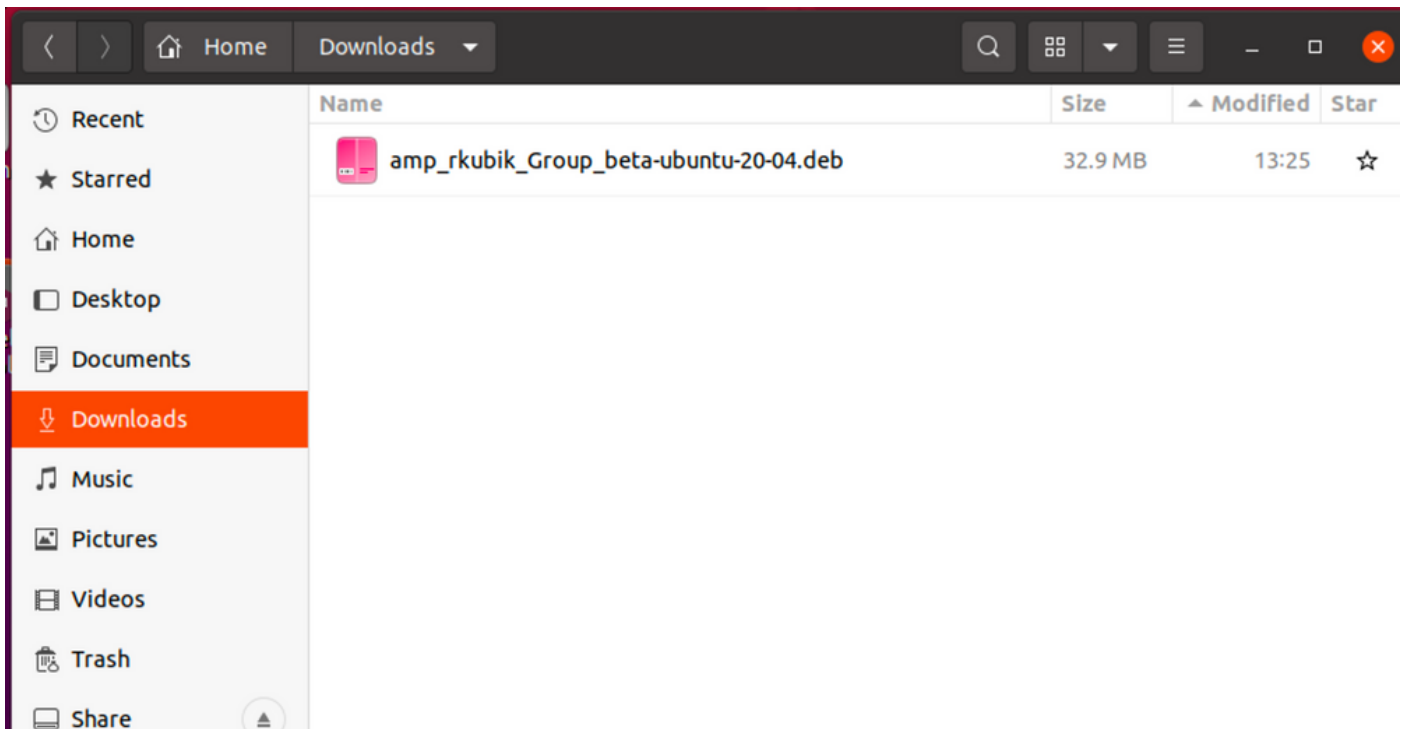
Ubuntu

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.

```
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
$ █
```

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`.

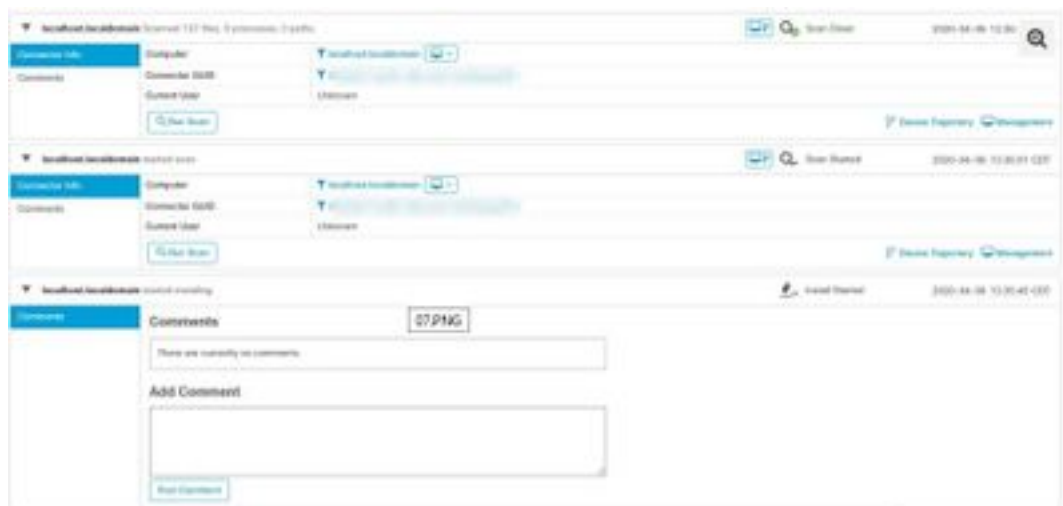
```
File Edit View Search Terminal Help
[preuser@preuser-lin-nsx-lab ~]$ cd /opt/cisco/amp/bin/
[preuser@preuser-lin-nsx-lab bin]$ pwd
/opt/cisco/amp/bin
[preuser@preuser-lin-nsx-lab bin]$ ls
ampcli  ampcli  ampcli.service  ampcli.service  cisco-amp-helper  libcurl.so.8.2.0  libcurl.so.8.2.0
ampcli.service  ampcli.service  ampcli.service  ampcli.service  libcurl.so.8.2.0  libcurl.so.8.2.0  libcurl.so.8.2.0
[preuser@preuser-lin-nsx-lab bin]$ ./ampcli

ampcli - AMP for Endpoints Connector Command Line Interface
Interactive mode

Enter 'q' or Ctrl+C to Exit

[Debugger] 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: JMSA-Fix-Linux (453200)
Command-Line: Enabled
Faults: None
ampcli>
```

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](#)