安装思科安全终端Linux连接器

目录

简介

本文档介绍如何安装和验证适用于基于Red Hat Enterprise Linux(RHEL)和Debian的系统的思科安全终端Linux连接器。

作者：Juan Carlos Castillero，编辑者：Cisco TAC工程师Yeraldin Sanchez。

先决条件

要求

Cisco 建议您了解以下主题：

- Linux连接器上的Linux计算机支持的操作系统(OS)

使用的组件

本文档中的信息基于以下软件和硬件版本：

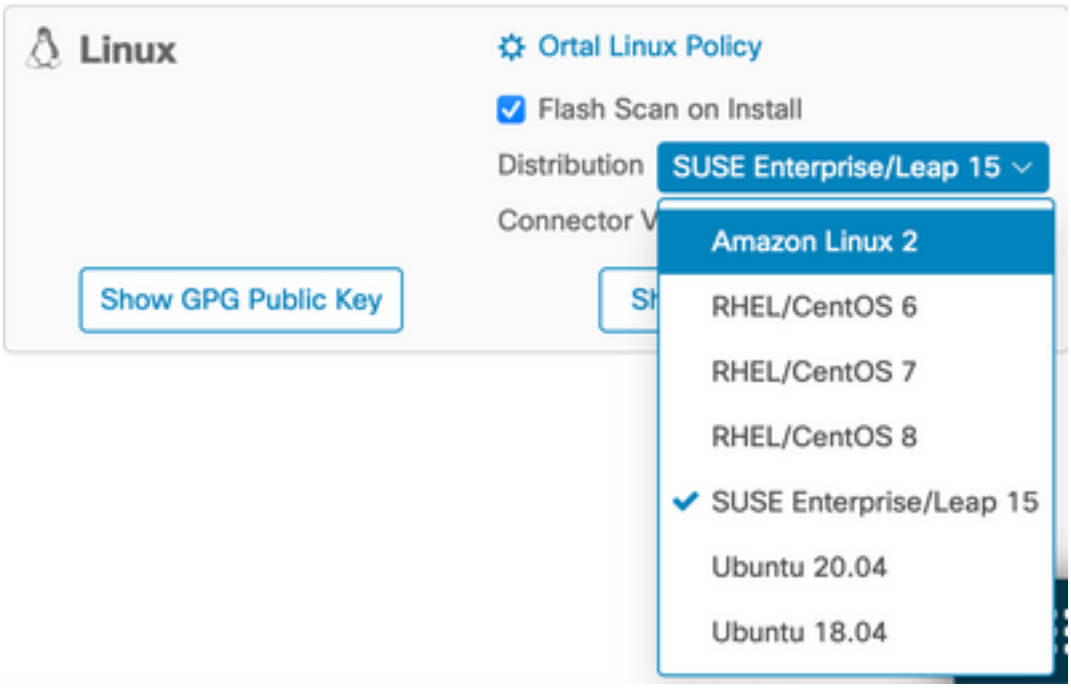
- 安全终端Linux连接器安装程序Red Hat Package Manager(RPM)
- 安全终端Linux连接器安装程序Debian包管理器(dpkg)
- 用于验证更新的GNU隐私保护(GPG)密钥（可选）
- Linux连接器安装程序DPKG（Debian包管理系统）

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

RHEL/CentOS/Amazon Linux 2/SUSE 15

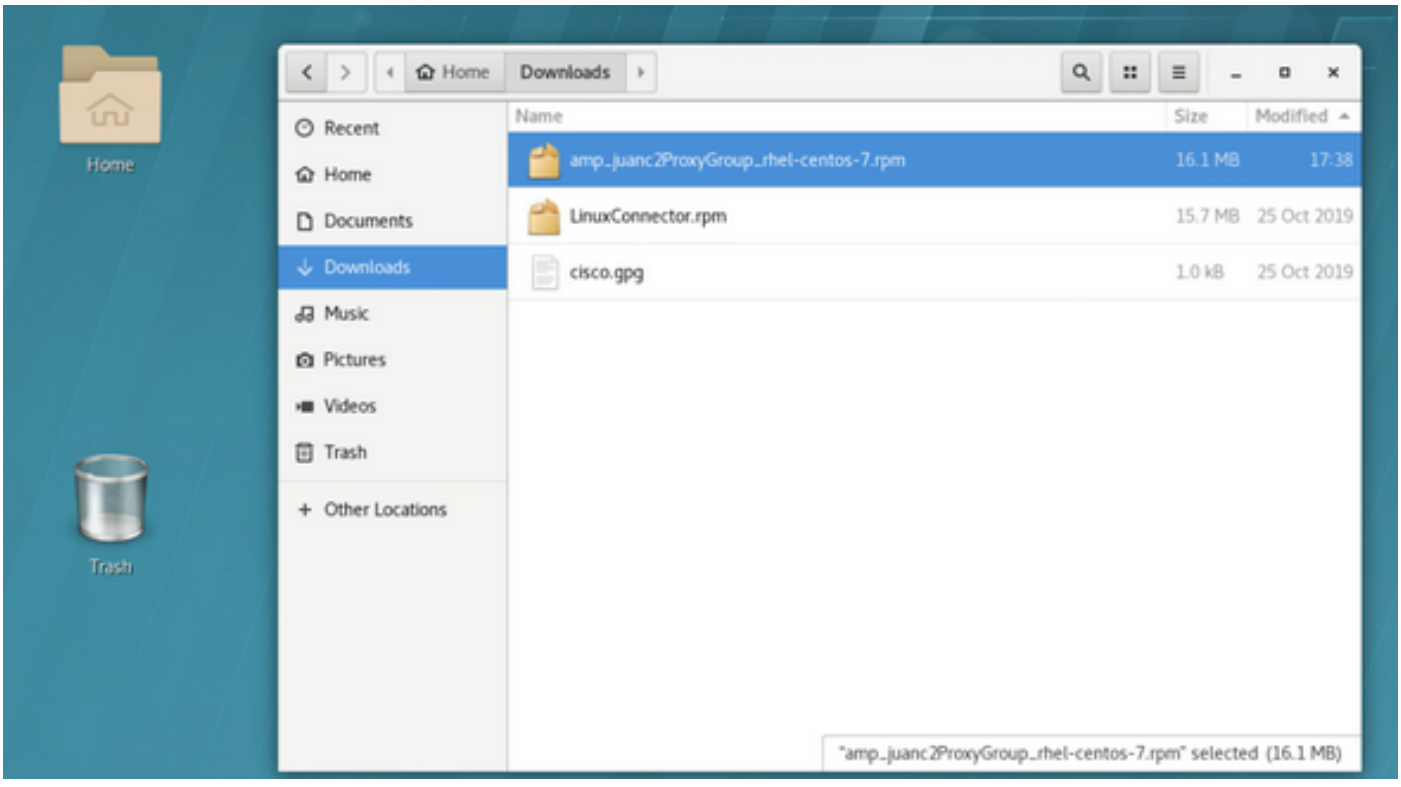
配置

步骤1.从思科安全终端门户下载Linux RPM软件包，如图所示。



注意：请注意，由于两个不同的连接器具有显着不同的架构，因此操作系统分布非常重要。

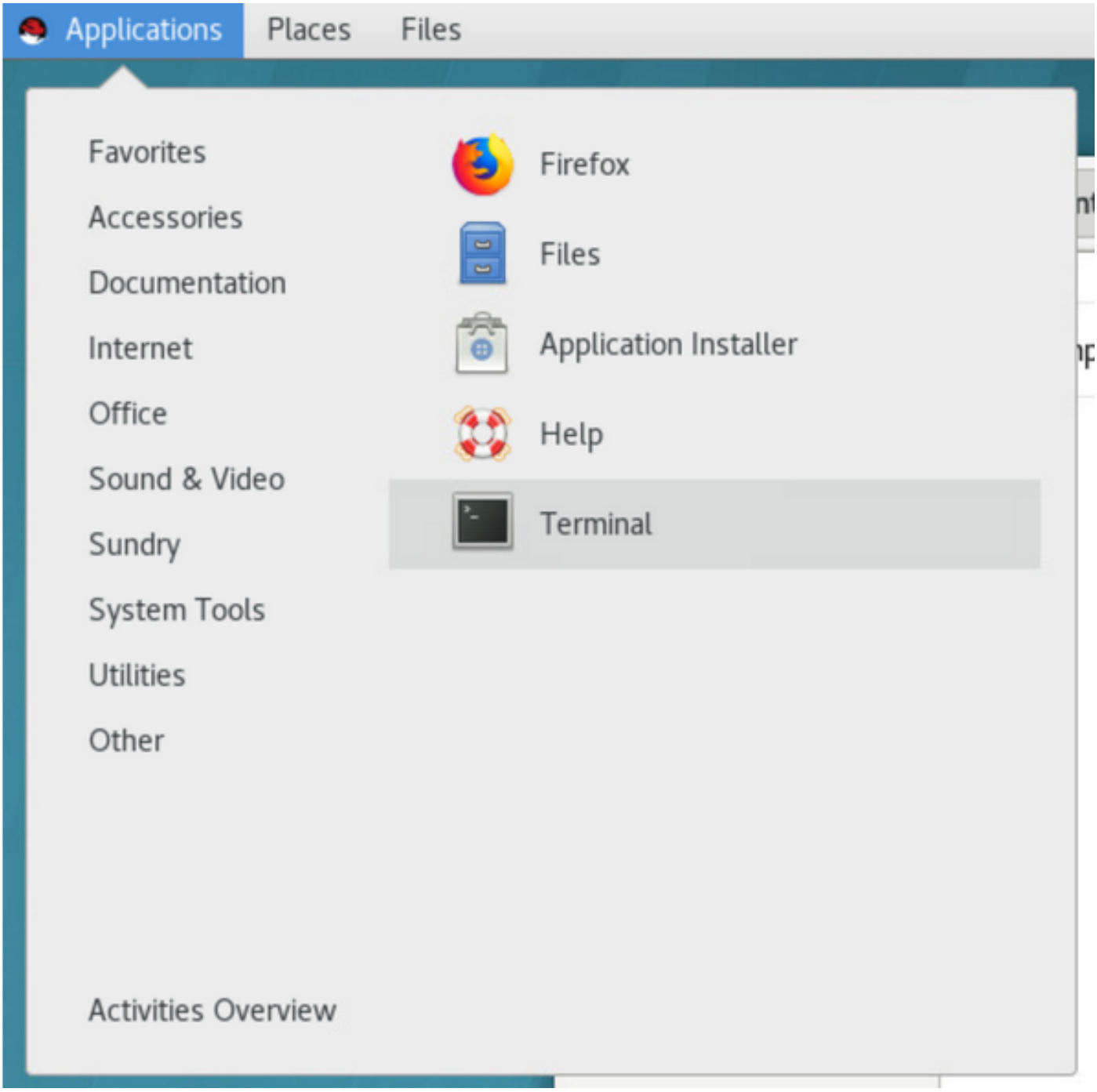
步骤2.将RPM包移动到相关终端，从控制面板直接下载或手动将其移动到终端。在本例中，使用图形用户界面(UI)，虽然可能（通常也是常见的）以最少的安装进行工作，在这种情况下，需要知道如何处理Linux终端并找到其RPM软件包。



步骤3.要安装Linux连接器，请执行以下命令：**sudo yum localinstall [rpm package] -y**(或**SUSE 15上的sudo zypper install -y [rpm package]**)

其中，[rpm package]是文件的名称，例如“amp_Audit.rpm”。 运行atd服务时，需要安装RPM软件包。

如图所示，如果GUI正在使用，请打开终端。



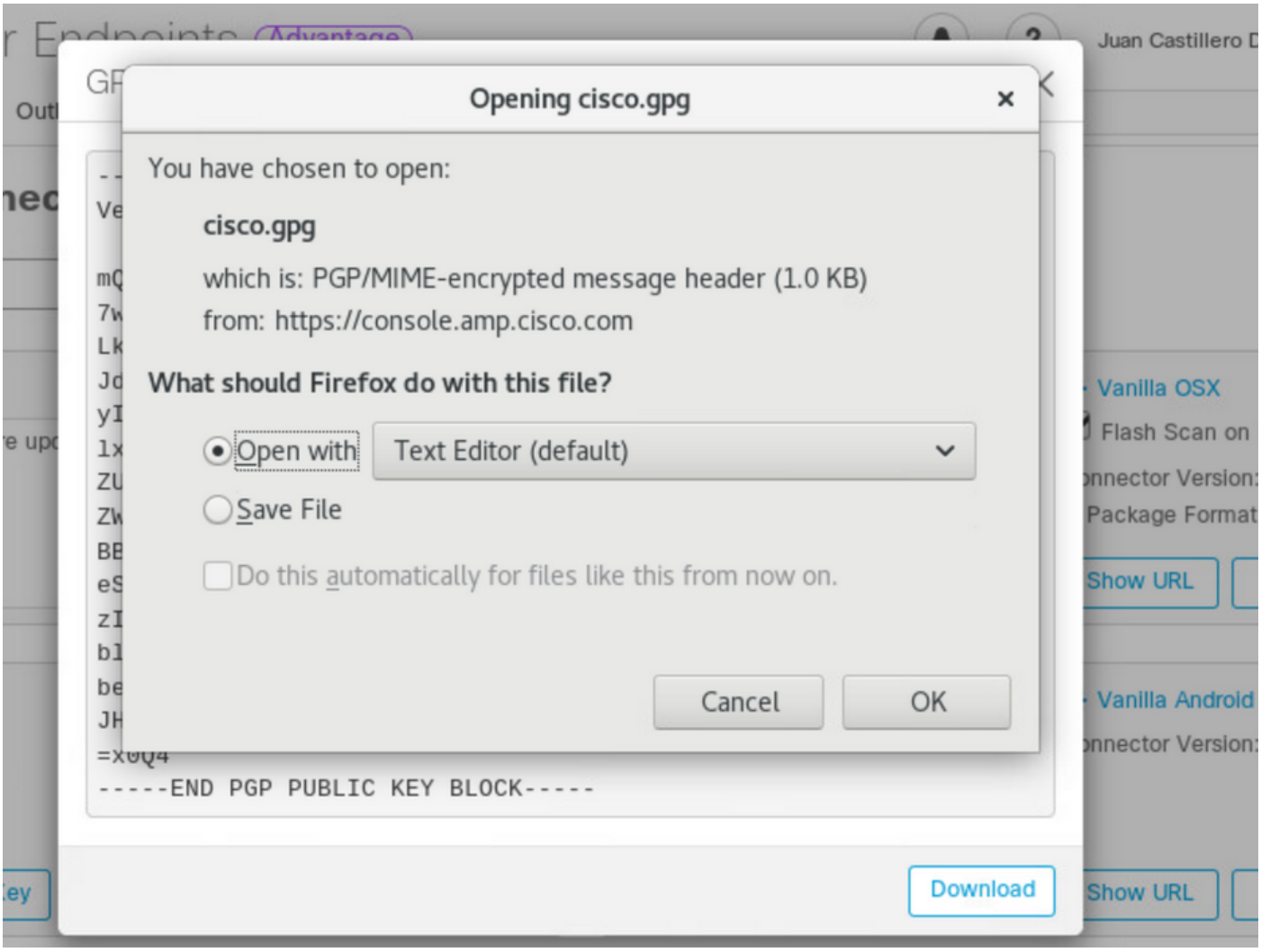
安装开始后，无需用户输入，这是一个自动过程，如图所示。

如何导入GPG密钥

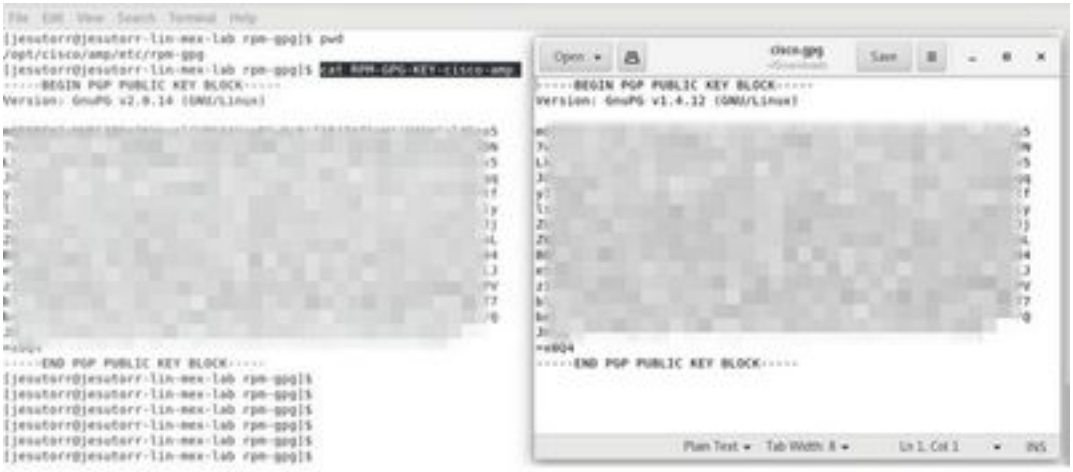
可以从“下载连接器”(Download Connector)页面复制GPG公钥，以验证RPM包的签名。连接器无需GPG键即可安装;但是， 用户 如果他们计划通过RHEL上的策略推送连接器更新，则需要将GPG密钥导入其RPM数据库。

注意：从连接器版本1.17.0开始，自动安装用于在连接器更新期间验证升级包的GPG密钥。

步骤1.验证GPG密钥，点击Download Connector页面上的GPG Public Key链接。将密钥与位于/opt/cisco/amp/etc/rpm-gpg/RPM-GPG-Key-cisco-amp的密钥进行比较。



步骤2.从终端运行命令以导入密钥：**sudo rpm -import /opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp**。



步骤3.检验密钥是否已安装，从终端运行命令：**rpm -q gpg-pubkey —qf '%{name}-%{version}-%{release} —> %{summary}\n'**。

步骤4.在输出中查找Sourcefire的GPG密钥。更新程序由系统的init守护程序运行，当更新可用时

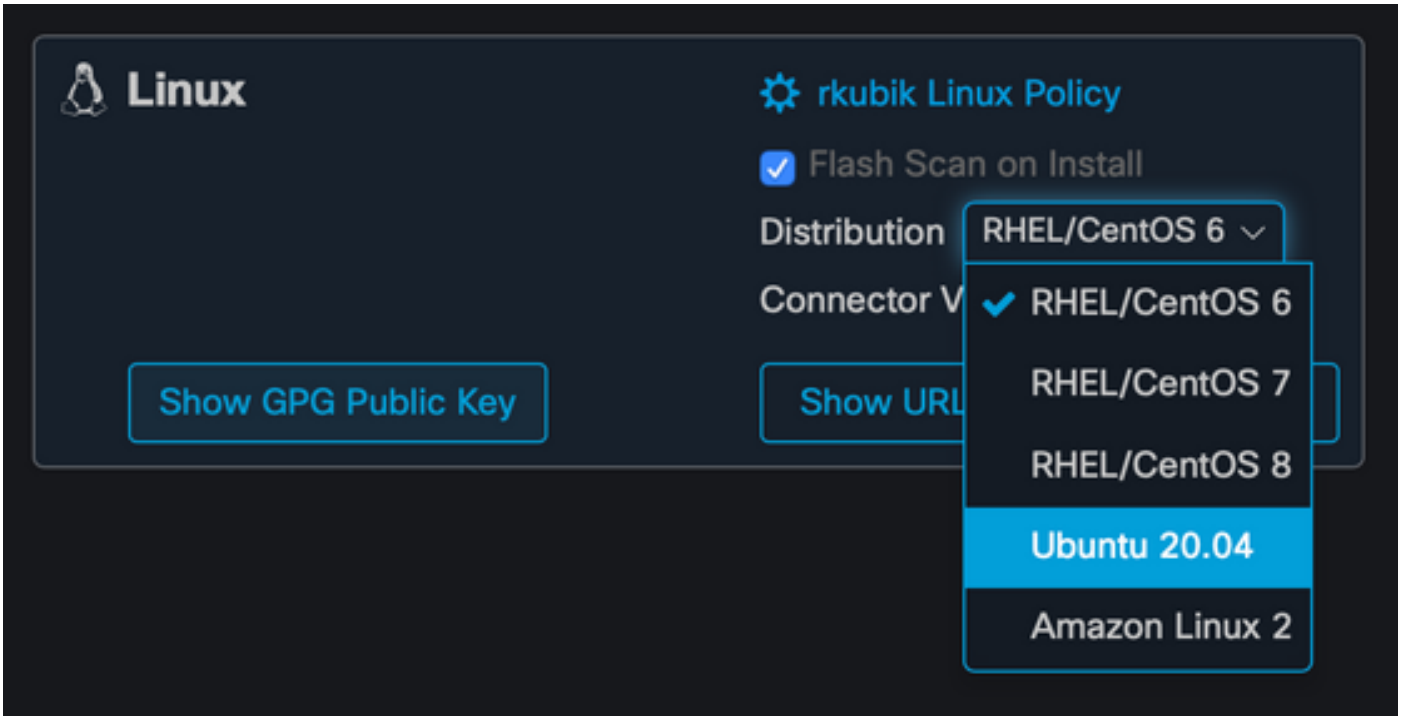
，会自动触发RPM升级过程。某些SELinux配置禁止此行为并导致更新程序失败。

如果怀疑是这种情况，请检查系统的审核日志(例如，**/var/log/audit/audit.log**)，并搜索与ampupdater相关的拒绝事件。您可能需要调整SELinux规则以允许更新程序运行。

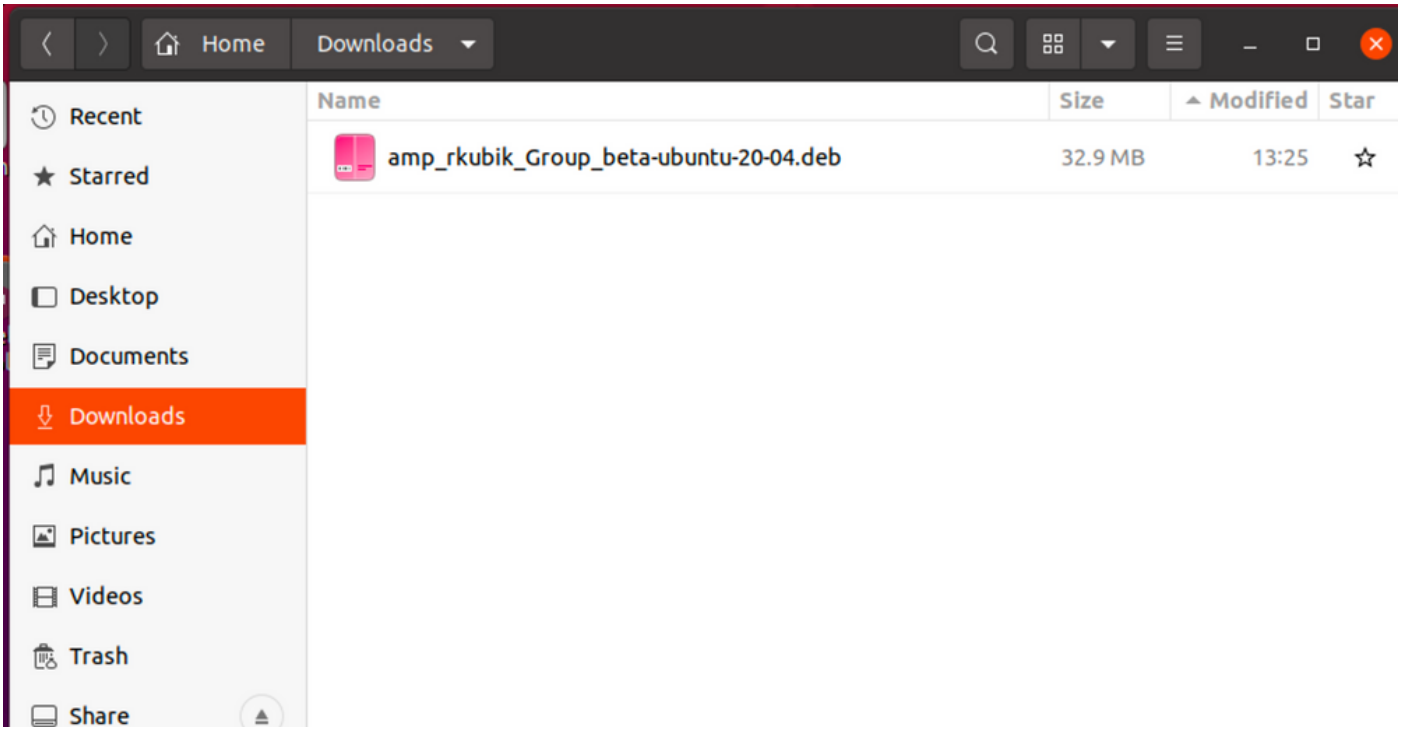
乌邦图

配置

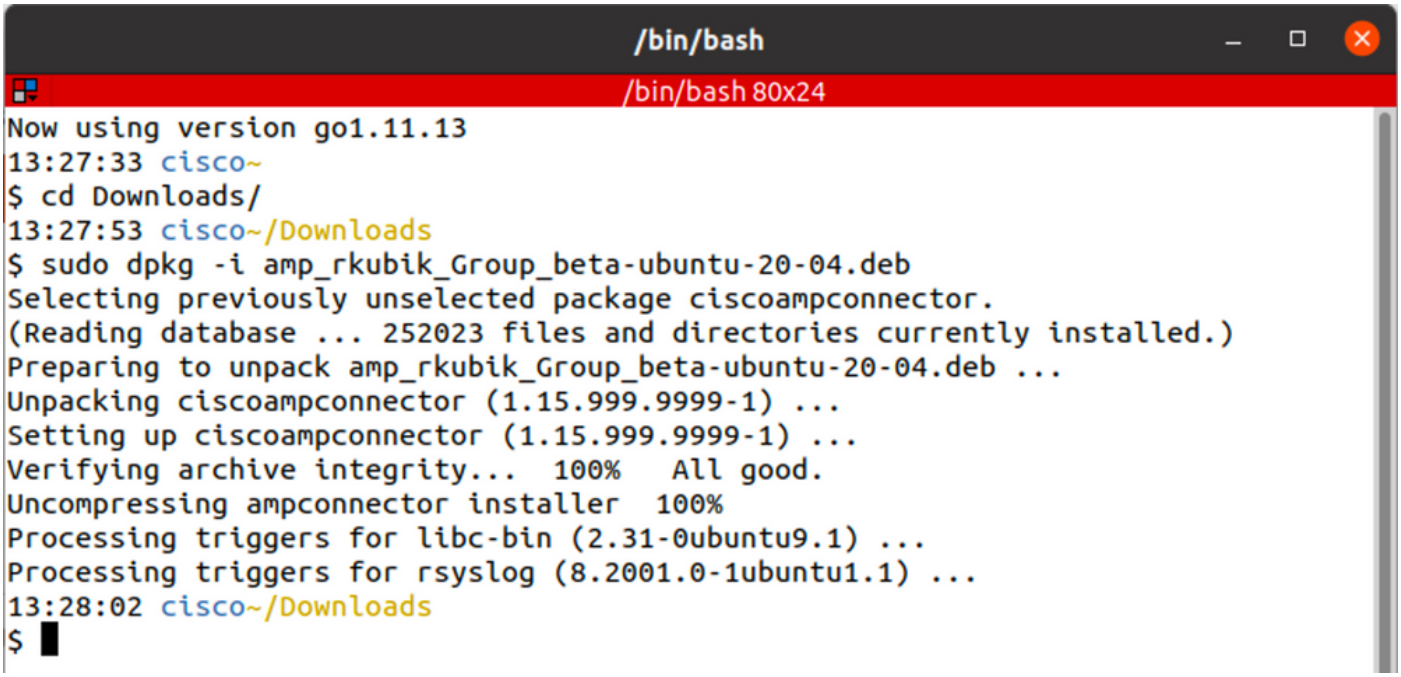
步骤1.从思科安全终端门户下载Linux DEB软件包，如图所示。



步骤2.将DEB软件包移动到相关终端，从控制面板直接下载或手动将其移动到终端。在本例中，使用图形用户界面(UI)，虽然可能（通常也是常见）以最小的安装进行工作，但在这种情况下，需要知道如何处理Linux终端并查找其DEB软件包。



步骤3.要安装Linux连接器，请执行以下命令：**sudo dpkg -i [deb package]**其中[deb package]是文件的名称，例如“amp_Audit.deb”。 安装开始后，无需用户输入，这是一个自动过程，如图所示。



如何导入GPG密钥

可以从“下载连接器”(Download Connector)页面复制GPG公钥，以验证DEB包的签名。该连接器可安装，无需GPG键;但是，如果用户计划通过Ubuntu上的策略推送连接器更新，则需要将GPG密钥导入到其拆除密钥环中。有关如何导入GPG密钥并验证连接器是否未在Ubuntu上修改的详细信息，请参阅https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/216524-amp-for-endpoints-ubuntu-connector.html#anc6

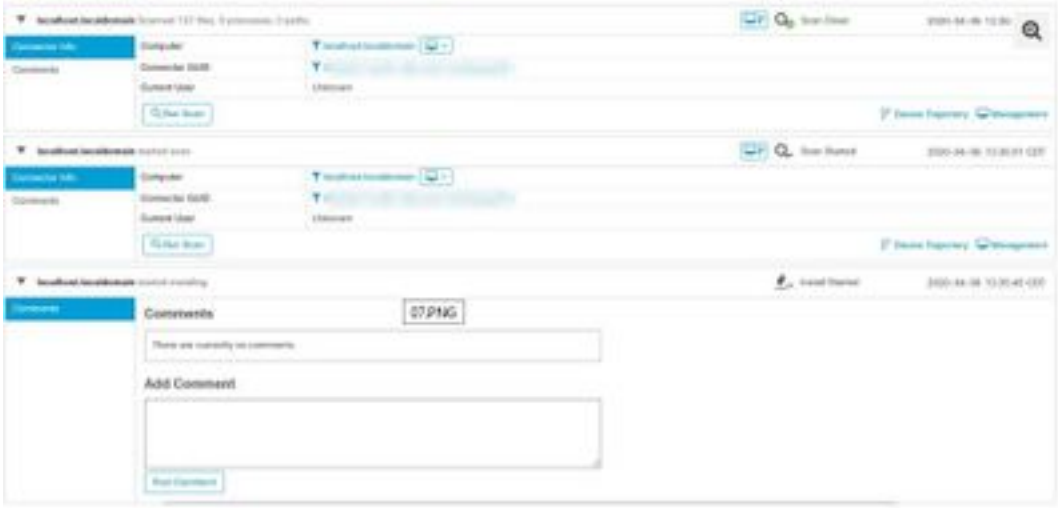
注意：从连接器版本1.17.0开始，自动安装用于在连接器更新期间验证升级包的GPG密钥。要验证此GPG密钥，请点击“下载连接器”(Download Connector)页面上的“GPG公钥”(GPG Public Key)链接，并将其与安装在**/opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-Key-cisco-amp的密钥进行比较**。

验证

使用本部分可确认配置能否正常运行。

要验证安装是否成功，请运**行AMP CLI**。在/opt/cisco/amp/bin/ampcli中可以找到Linux**连接器命令行界面**。它可以在交互模式下运行，也可以执行单个命令，然后退出。运行命令**。/ampcli —help**以查看可用选项和命令的完整列表。连接器生成的所有日志文件都可在**/var/log/cisco中找到。**

Cisco Secure控制台上还显示安装事件，如果下载RPM软件包时请求了闪存扫描，则也会显示该事件。



故障排除

目前没有针对此配置的故障排除信息。

相关信息

- [在Linux视频中安装面向终端的AMP连接器]
- [技术支持和文档 - Cisco Systems]