基于Debian的系统上的思科安全终端Linux连接器

目录

[最低操作系统要求](#)
[环境设置](#)
[依赖项](#)
[验证DEB包](#)
[下载DEB包](#)
[检索GPG公钥](#)
[验证DEB包](#)
[安装](#)
[卸载](#)
[修订历史纪录](#)
本文介绍管理员在基于Debian的系统上部署思科安全终端Linux连接器时可采取的更改和步骤：

- 德比10及更高。
- Ubuntu 18.04及更高版本。

最低操作系统要求

有关操作系统兼容性，请参阅“Cisco Secure Endpoint Linux Connector OS Compatibility（思科安全终端Linux连接器操作系统兼容性）”文章。

环境设置

基于Debian的系统上的Linux连接器使用eBPF进行文件和网络监控。计算机必须安装正确的linux-headers软件包，否则连接器将引发故障11（缺少系统依赖项），并在不进行文件和网络监控的情况下以降级状态运行。有关解决此故障的指导，请参阅《Linux内核级故障》一文的部分。

依赖项

Linux连接器取决于基于Debian的系统基本安装中包含的系统包，但如果依赖项缺少，则会显示以下消息：

```
ciscoampconnector depends on
```

使用以下命令安装Linux连接器所需的任何缺失依赖项：

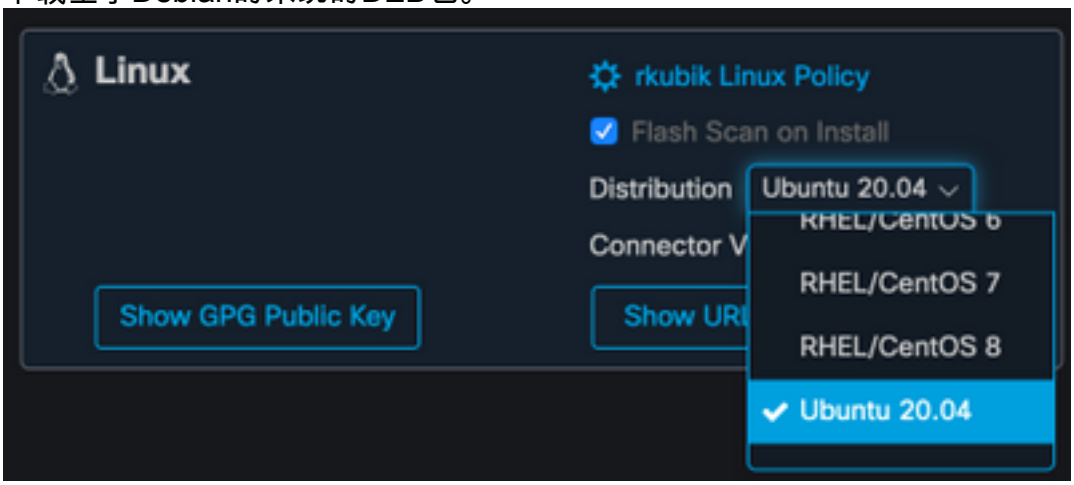
```
sudo apt install
```

验证DEB包

Linux连接器DEB软件包包含用于验证下载的软件包是否属于思科的签名。

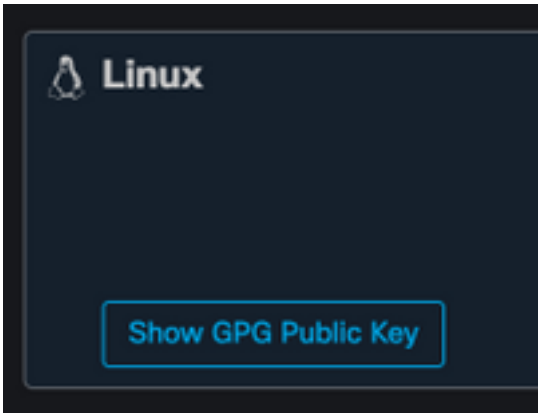
下载DEB包

1. 访问面向终端的AMP控制台。
2. 下载基于Debian的系统的DEB包。



3. 将DEB包传输到基于Debian的系统。例如：amp_ciscoampconnector.deb

检索GPG公钥



1. 单击“显示GPG公钥”按钮，如下图所示。
2. 如果连接器版本低于1.17.0，请下载并传输或将公钥复制到计算机。例如：cisco.gpg。如果连接器版本至少为1.17.0，则GPG密钥在/opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-KEY-cisco-amp中可用。

验证DEB包

DEB软件包使用调试工具签名，可以使用调试验证进行验证。

1. 安装拆卸验证工具。
   ```
   sudo apt-get install debsig-verify
   ```
2. 将Cisco GPG公钥导入调试密钥环。**注意：**自1.17.0版起，将自动创建debsig.gpg文件，以便跳过步骤2。
   ```
   sudo mkdir -p /usr/share/debsig/keyrings/914E5BE0F2FD178F sudo gpg --dearmor --output
   /usr/share/debsig/keyrings/914E5BE0F2FD178F/debsig.gpg cisco.gpg
   ```
3. 创建策略目录。
   ```
   sudo mkdir -p /etc/debsig/policies/914E5BE0F2FD178F
   ```
4. 将以下策略内容复制到新文件“/etc/debsig/policies/914E5BE0F2FD178F/ciscoampconnector.pol”中。

5. 使用debsig-verify验证DEB签名。

```
debsig-verify amp_ciscoampconnector.deb
```

输出应如下所示：

```
debsig: Verified package from 'Cisco AMP for Endpoints' (Debsig)
```

注意：对于从面向终端的AMP控制台下载的任何基于Debian的包，可以重复第5步。

安装

要安装连接器，请执行以下命令，其中[deb package]是文件的名称，例如amp_test.deb:

```
sudo dpkg -i [deb package]
```

重要！如果您在环境中运行其他安全产品，则它们可能会将连接器安装程序检测为威胁。要成功安装连接器，请将Cisco Secure添加到允许的列表或在其他安全产品中排除Cisco Secure，然后重试。

重要！在连接器安装期间，会在系统上创建名为cisco-amp-scan-svc的用户和组。如果此用户或组已存在，但配置方式不同，则安装程序将尝试删除这些用户或组，然后使用必要的配置重新创建它们。如果无法使用必要的配置创建用户和组，安装程序将失败。

卸载

请参阅 安全终端用户指南卸载说明

修订历史纪录

2020年12月10日

- 初始版本

2022年4月12日

- 内容适用于Debian和Ubuntu。