

思科安全終端Linux聯結器的安裝

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

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

[組態](#)

[如何匯入GPG金鑰](#)

[烏本圖](#)

[組態](#)

[如何匯入GPG金鑰](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹如何為基於Red Hat Enterprise Linux(RHEL)和Debian的系統安裝和驗證Cisco Secure Endpoint Linux聯結器。

由Juan Carlos Castellero撰寫，由Cisco TAC工程師Yeraldin Sanchez編輯。

必要條件

需求

思科建議您瞭解以下主題：

- Linux聯結器支援的作業系統(OS)上的Linux電腦

採用元件

本文中的資訊係根據以下軟體和硬體版本：

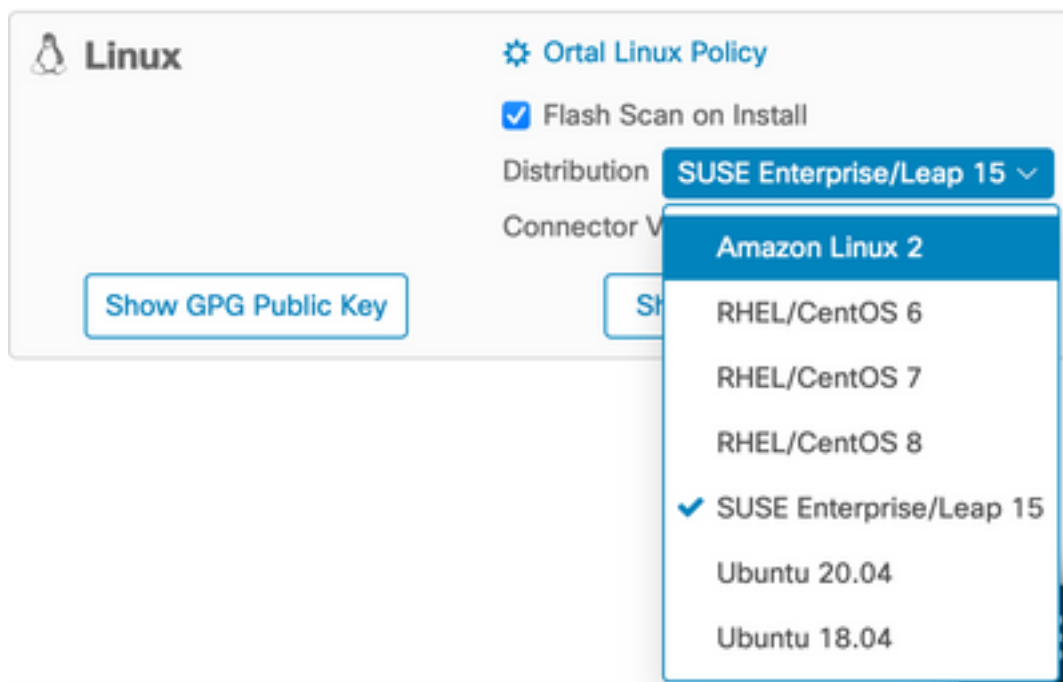
- 安全終端Linux聯結器安裝程式Red Hat Package Manager(RPM)
- 安全終端Linux聯結器安裝程式Debian軟體包管理器(dpkg)
- 用於驗證更新的GNU Privacy Guard(GPG)金鑰 (可選)
- Linux聯結器安裝程式DPKG (Debian軟體包管理系統)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

RHEL/CentOS/Amazon Linux 2/SUSE 15

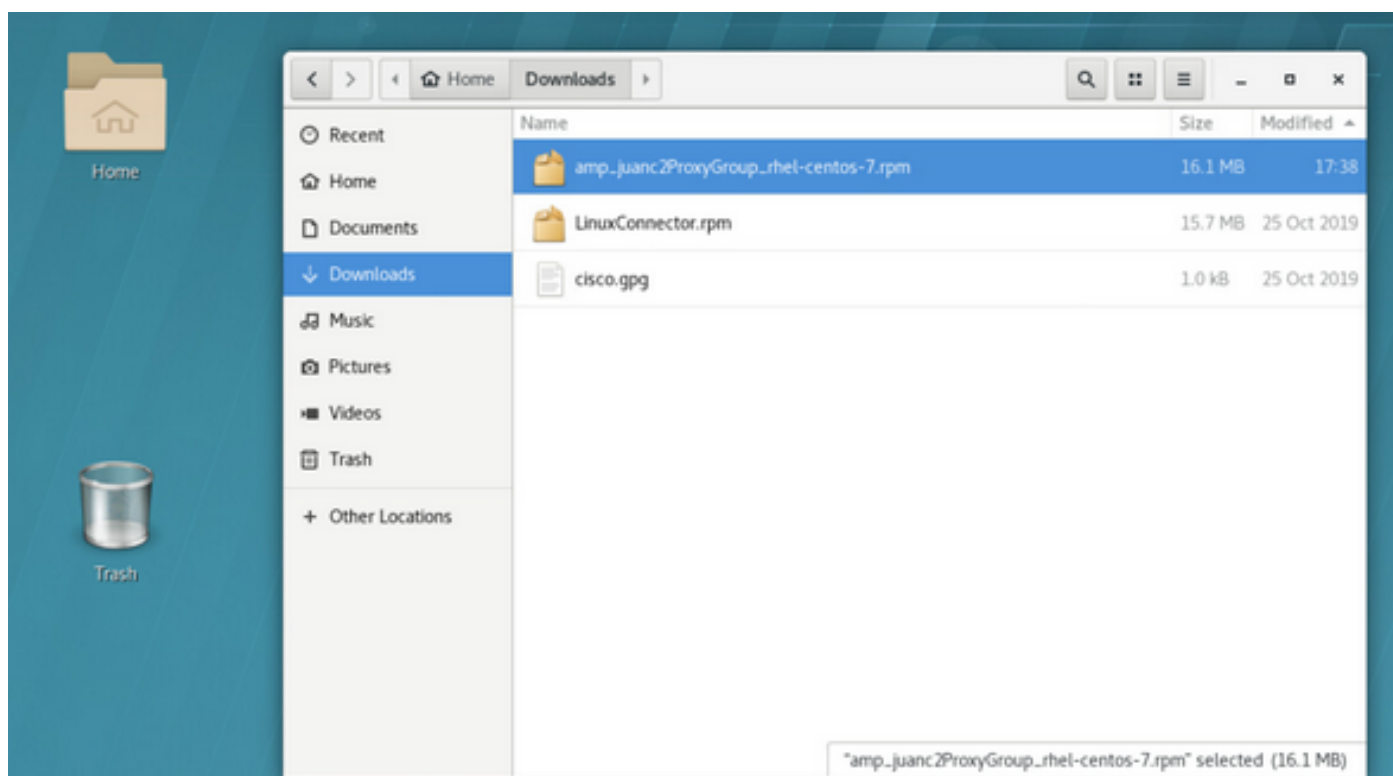
組態

步驟1.從思科安全終端門戶下載Linux RPM程式包，如下圖所示。



附註：請記住，作業系統分佈很重要，因為兩個不同的連結器都具有截然不同的架構。

步驟2.將RPM軟體包移動到相關終結點，或者直接從儀表板下載該軟體包，或者手動將其移動到終結點。在本例中，圖形使用者介面(UI)被使用，儘管它可能，而且經常是常見的，使用最小的安裝，在這種情況下，需要知道如何處理Linux終端並找到其RPM程式包。



步驟3.為了安裝Linux連結器，請執行以下命令：`sudo yum localinstall [rpm package] -y(或sudo zypper install -y [rpm package] on SUSE 15)`

其中[rpm package]是檔案的名稱，例如「amp_Audit.rpm」。Atd服務運行時，需要安裝RPM包。

```
File Edit View Search Terminal Help
[jenator@jenator-lin-ssl-Lab Downloads] sudo yum localinstall amp_juice2ProxyGroup_rhel-centos-7.rpm -y
[sudo] password for jenator:
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_juice2ProxyGroup_rhel-centos-7.rpm: ciscoampconnector-1.12.2.082-1.el7.x86_64
Marking amp_juice2ProxyGroup_rhel-centos-7.rpm as an update to ciscoampconnector-1.10.2.030-1.el7.x86_64
Resolving dependencies
--> Marking transaction check
--> Package ciscoampconnector.x86_64 0:1.10.2.030-1.el7 will be updated
--> Package ciscoampconnector.x86_64 0:1.12.2.082-1.el7 will be an update
--> Finished Dependency Resolution

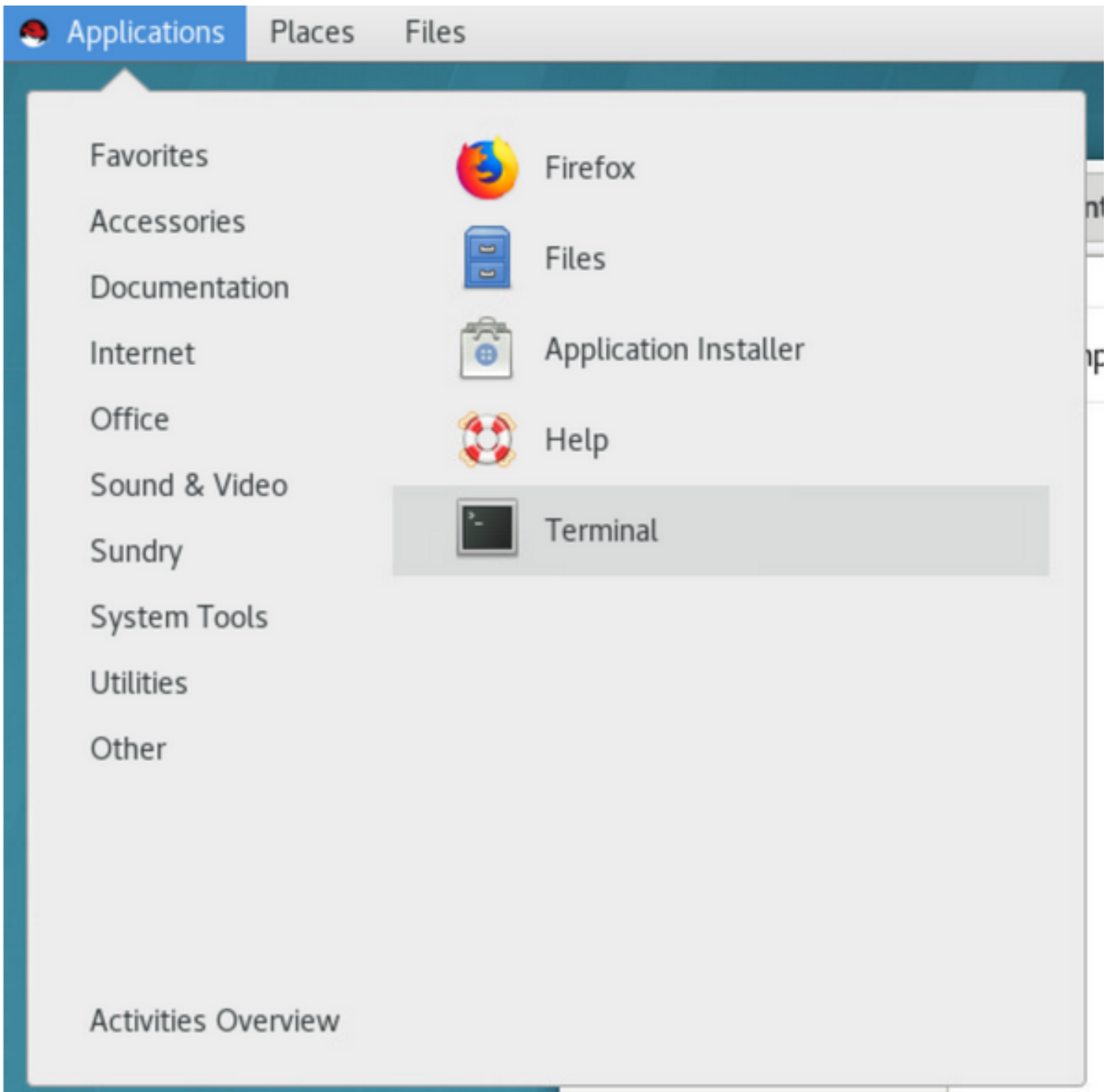
Dependencies Resolved

-----
Package                Arch          Version           Repository          Size
-----
Updating:
ciscoampconnector      x86_64        1.12.2.082-1.el7 /amp_juice2ProxyGroup_rhel-centos-7 43 M
-----
Transaction Summary

Upgrade 1 Package

Total size: 43 M
Downloading packages:
Marking transaction check
Marking transaction test
Transaction test succeeded
Marking transaction
Policy used to /opt/cisco/amp/etc/policy.xml.amp.rhel
```

如果正在使用GUI，請開啟終端，如下圖所示。



安裝開始後，無需使用者輸入，這是一個自動過程，如圖所示。

```
File Edit View Search Terminal Help
Updating:
ciscoampconnector x86_64 1.12.2.602-1.el7 /amp_buanc3ProxyGroup_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.amgsave
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.amgsave
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 1/2
Updated:
ciscoampconnector.x86_64 0:1.12.2.602-1.el7
Complete!
[[jensfarm@esxtar-rhel-mex-lab Downloads]$
```

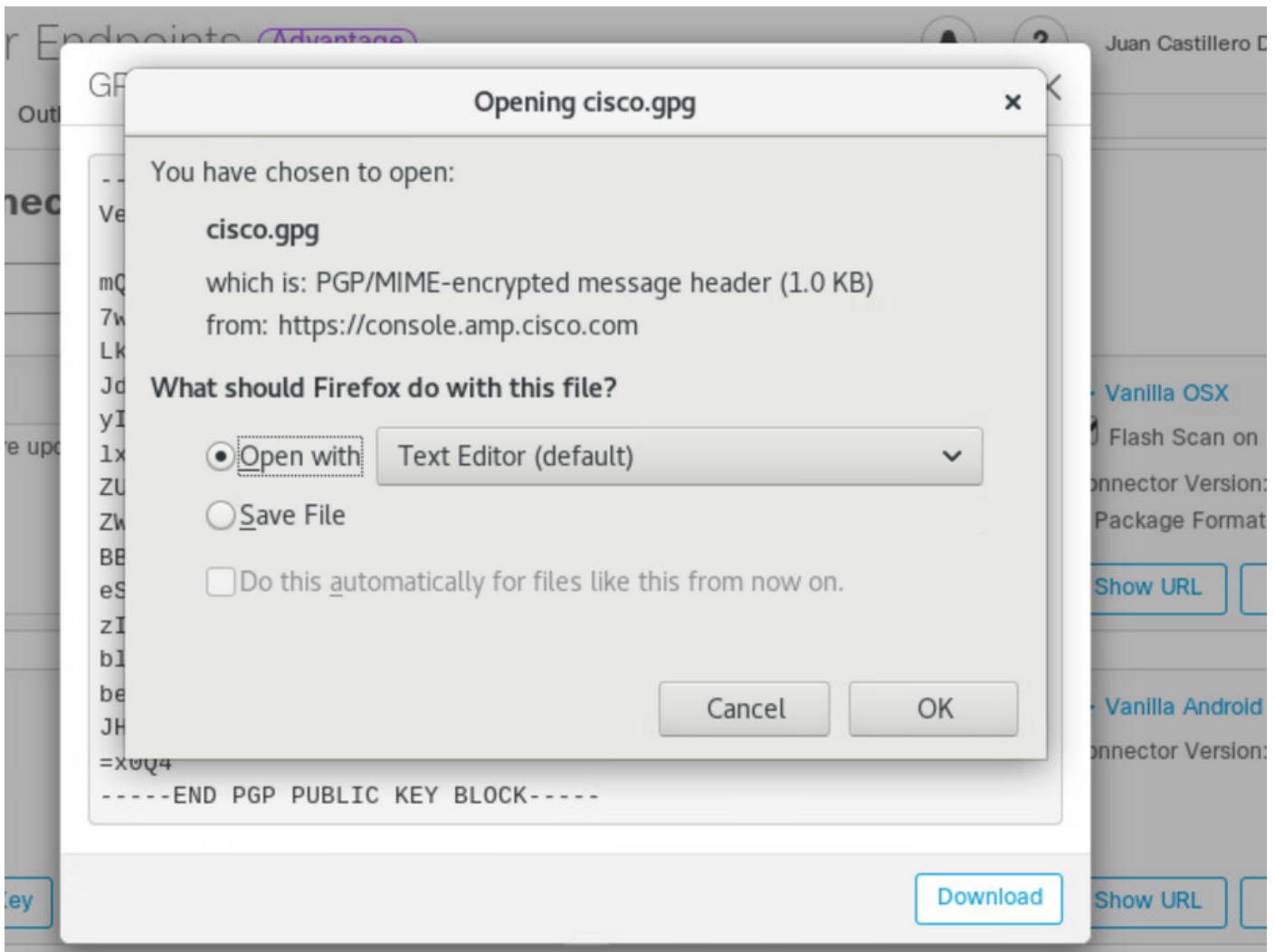
如何匯入GPG金鑰

可以從「下載連結器」(Download Connector)頁面複製GPG公鑰以驗證RPM軟體包的簽名。可以不使用GPG金鑰安裝連結器;但是, 使用者 如果他們計畫通過RHEL上的策略推送連結器更新, 則需要將GPG金鑰匯入其RPM DB.

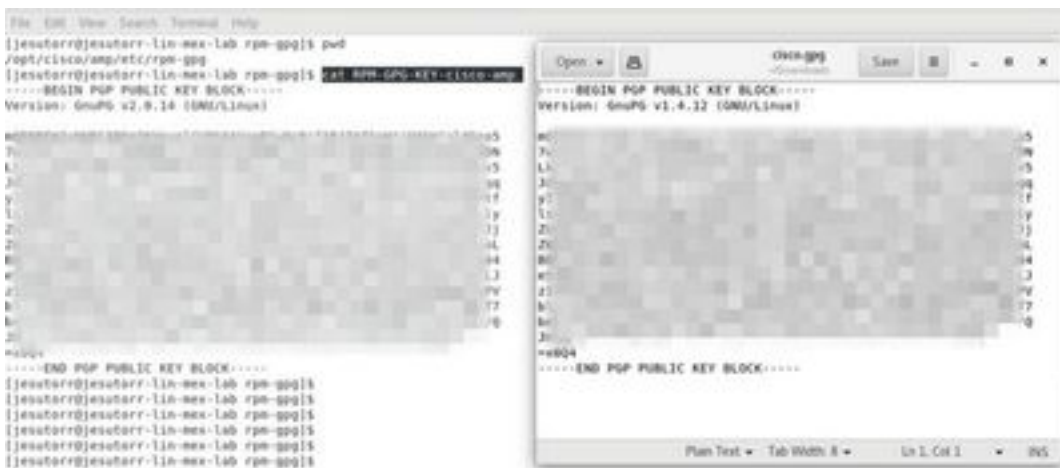
附註: 從連結器版本1.17.0開始, 將自動安裝用於在連結器更新期間驗證升級軟體包的GPG金鑰。

步驟1. 驗證GPG金鑰, 點選Download Connector頁面上的GPG Public Key連結。將金鑰與 `at/opt/cisco/amp/etc/rpm-gpg/RPM-GPG-Key-cisco-amp` 的金鑰進行比較。





步驟2.從終端機執行命令以匯入金鑰：`sudo rpm --import /opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp`。



步驟3.驗證是否已安裝金鑰，從終端運行命令：`rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n'`。



步驟4.在輸出中查詢Sourcefire的GPG金鑰。更新程式由系統的init守護程式運行，當更新可用時

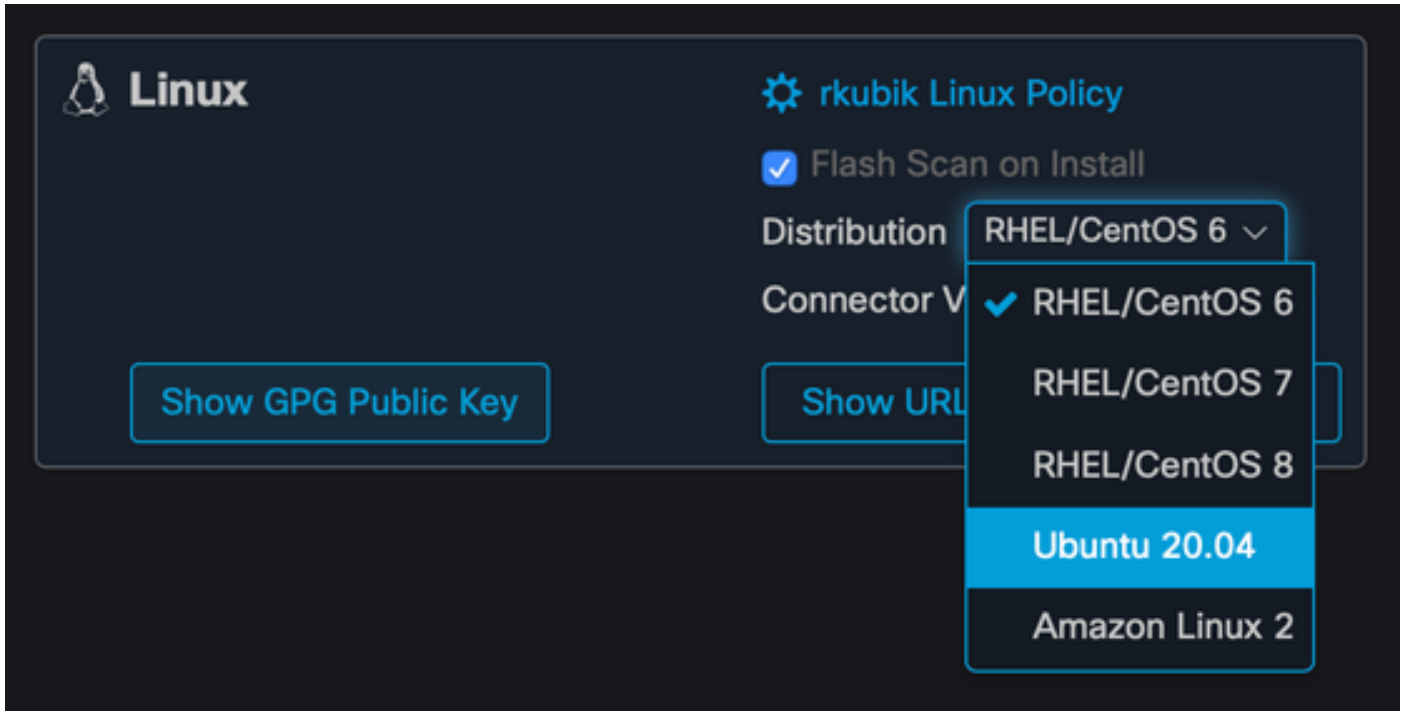
，將自動觸發RPM升級過程。某些SELinux配置禁止此行為並導致更新程式失敗。

如果懷疑是這種情況，請檢查系統的稽核日誌(如/var/log/audit/audit.log)，並搜尋與截肢者有關的拒絕事件。您可能需要調整SELinux規則以允許更新程式運行。

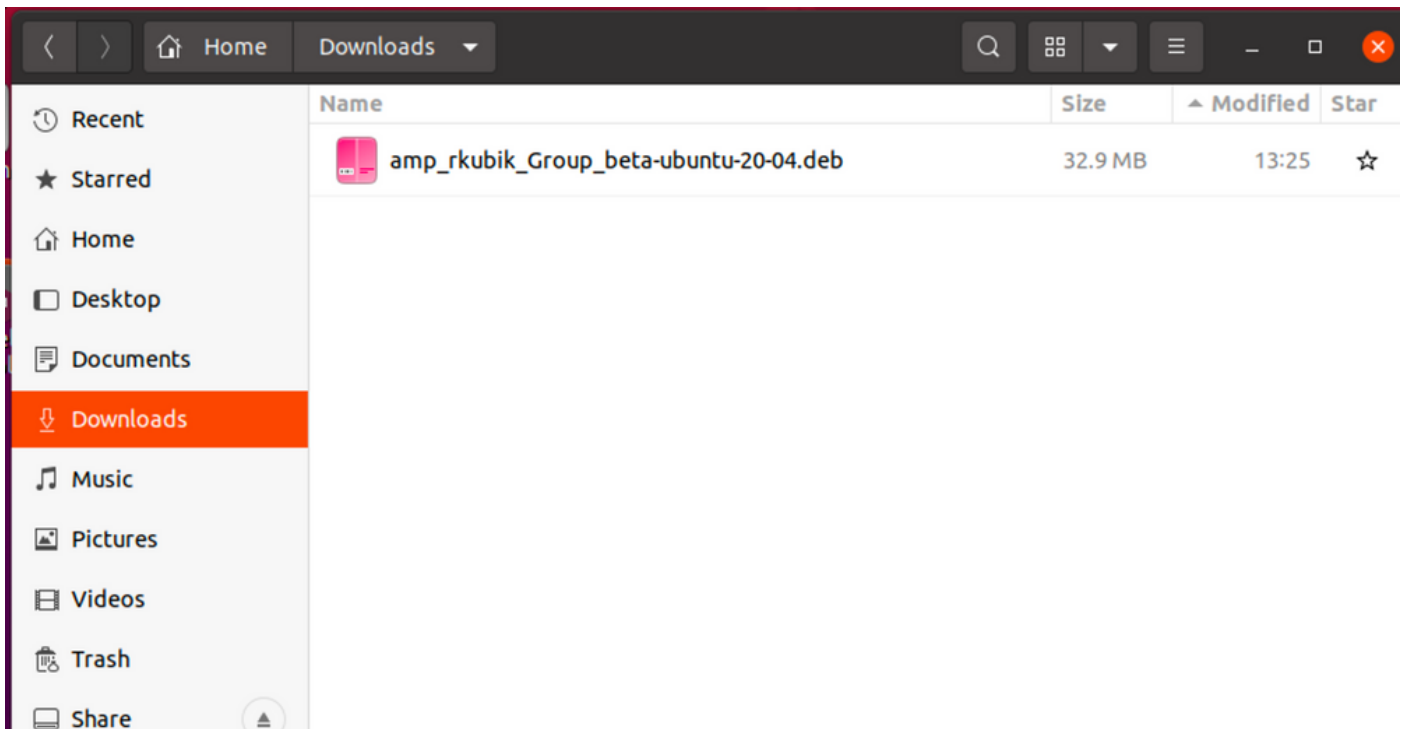
烏本圖

組態

步驟1.從思科安全終端門戶下載Linux DEB程式包，如下圖所示。



步驟2.將DEB包移動到相關終結點，或者直接從儀表板下載該包，或者手動將其移動到終結點。在本例中，圖形使用者介面(UI)被使用，儘管它可能，而且經常是常見的，以最小安裝工作，在這種情況下，需要知道如何處理Linux終端並找到其DEB程式包。



步驟3.為了安裝Linux聯結器，請執行以下命令：`sudo dpkg -i [deb package]`，其中[deb package]是檔案的名稱，例如「amp_Audit.deb」。安裝開始後，無需使用者輸入，這是一個自動過程，如圖所示。

```

/bin/bash
/bin/bash 80x24
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
$ █
```

如何匯入GPG金鑰

可以從「下載聯結器」(Download Connector)頁面複製GPG公鑰，以驗證DEB軟體包的簽名。聯結器可以不帶GPG金鑰安裝;但是，如果用戶計畫通過Ubuntu上的策略推送聯結器更新，則需要將GPG金鑰匯入到其借項金鑰環中。有關如何匯入GPG金鑰並驗證聯結器是否未在Ubuntu上修改的詳細資訊，請參閱<https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/216524-amp-for-endpoints-ubuntu-connector.html#anc6>

附註：從聯結器版本1.17.0開始，將自動安裝用於在聯結器更新期間驗證升級軟體包的GPG金鑰。若要驗證此GPG金鑰，請按一下「下載聯結器」(Download Connector)頁面上的「GPG公鑰」(GPG Public Key)連結，並將其與安裝在/opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-Key-cisco-

amp的金鑰進行比較。

驗證

使用本節內容，確認您的組態是否正常運作。

要驗證安裝是否成功，請運行AMP CLI。Linux聯結器命令列介面位於`/opt/cisco/amp/bin/ampcli`。它可以在互動模式下運行，或者執行單個命令然後退出。運行命令`./ampcli —help`以檢視可用選項和命令的完整清單。聯結器生成的所有日誌檔案可在`/var/log/cisco`中找到。

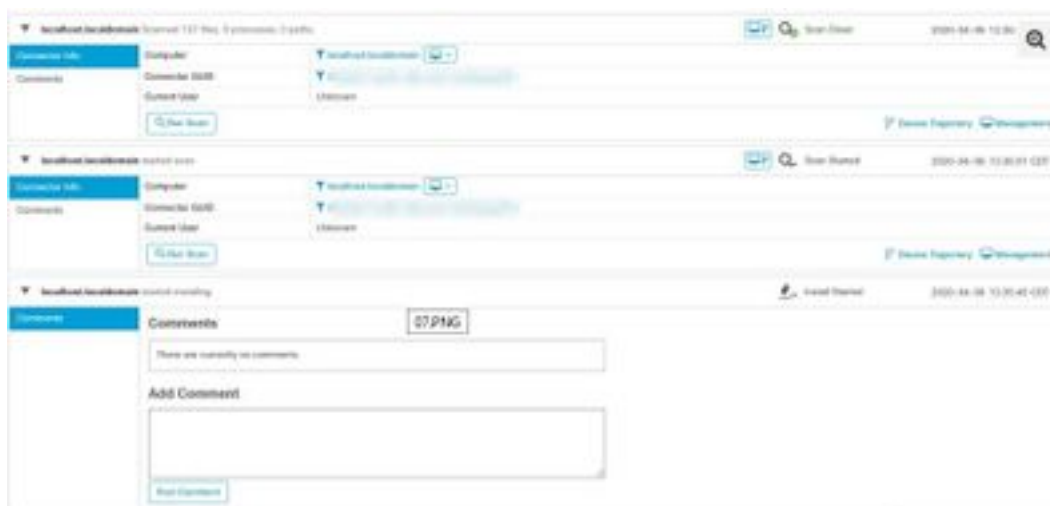
```
File Edit View Search Terminal Help
[preuser@preuser-lin-ml-lab ~]$ cd /opt/cisco/amp/bin/
[preuser@preuser-lin-ml-lab bin]$ pwd
/opt/cisco/amp/bin
[preuser@preuser-lin-ml-lab bin]$ ls
ampcli  ampcli.man  ampcli.service  cisco-amp-helper  lib64  lib64/asmpack.so.0  lib64/asm  lib64/asm.0.2.0
ampcli.man  ampcli.service  ampcli.service  lib64/asmack.so  lib64/asmack.so.0.1.0  lib64/asm.0  modules
[preuser@preuser-lin-ml-lab bin]$ ./ampcli

ampcli - AMP for Endpoints Connector Command Line Interface
Interactive mode

Enter 'q' or Ctrl+C to Exit

[debug] 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:      JavaScript-Linux (451200)
Command-line: Enabled
Faults:      None
ampcli █
```

如果下載RPM軟體包時請求了快閃記憶體掃描，則思科安全控制檯上也會顯示安裝事件。



疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- [在Linux影片中安裝面向終端的AMP聯結器](#)
- [技術支援與文件 - Cisco Systems](#)