

Cisco Secure Endpoint Linux Connectorのインストール

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

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

[設定](#)

[GPGキーをインポートする方法](#)

[Ubuntu](#)

[設定](#)

[GPGキーをインポートする方法](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Red Hat Enterprise Linux(RHEL)およびDebianベースのシステム用のCisco Secure Endpoint Linuxコネクタをインストールして確認する方法について説明します。

著者 : Cisco TACエンジニア、Juan Carlos Castillero、編集 : Yeraldin Sanchez

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Linuxコネクタ上のLinuxマシンでサポートされるオペレーティングシステム(OS)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Secure Endpoint LinuxコネクタインストーラRed Hat Package Manager(RPM)
- Secure Endpoint LinuxコネクタインストーラDebian Package Manager(dpkg)
- アップデートを確認するためのGNUプライバシーガード(GPG)キー (オプション)
- LinuxコネクタインストーラDPKG(Debian Package Management System)

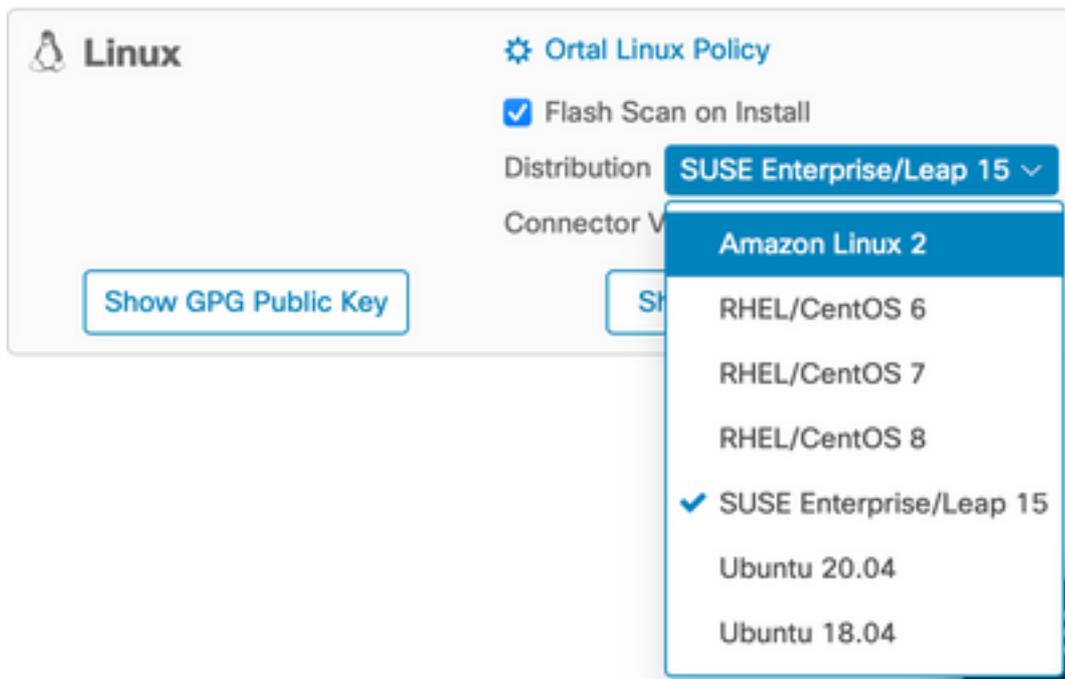
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

RHEL/CentOS/Amazon Linux 2/SUSE 15

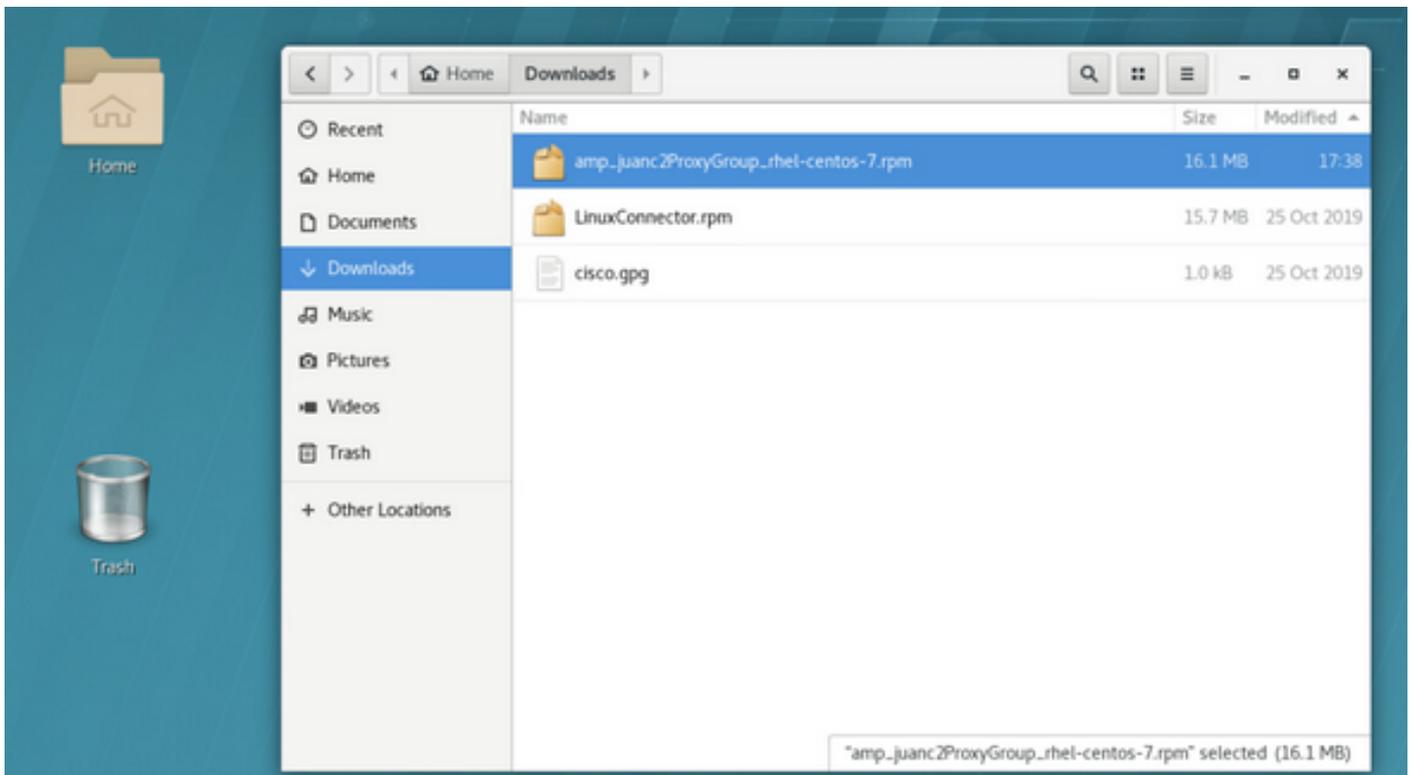
設定

ステップ1：図に示すように、Cisco Secure Endpoint PortalからLinux RPMパッケージをダウンロードします。



注：OSの配布は両方のコネクタがアーキテクチャが大きく異なるため、重要であることに注意してください。

ステップ2:RPMパッケージを該当するエンドポイントに移動し、ダッシュボードから直接ダウンロードするか、手動でエンドポイントに移動します。この例では、Graphic User Interface (UI；グラフィックユーザインターフェイス)を使用していますが、最小限のインストールで作業することは可能で、しばしば一般的です。その場合は、Linux端末の扱い方を知って、RPMパッケージを見つける必要があります。



ステップ3:Linuxコネクタをインストールするには、次のコマンドを実行します。**sudo yum localinstall [rpm package] -y** (または**sudo zypper install -y [rpm package]** on SUSE 15)

ここで、[rpm package]はファイルの名前です。たとえば、「amp_Audit.rpm」などです。atdサービスの実行中にRPMパッケージをインストールする必要があります。

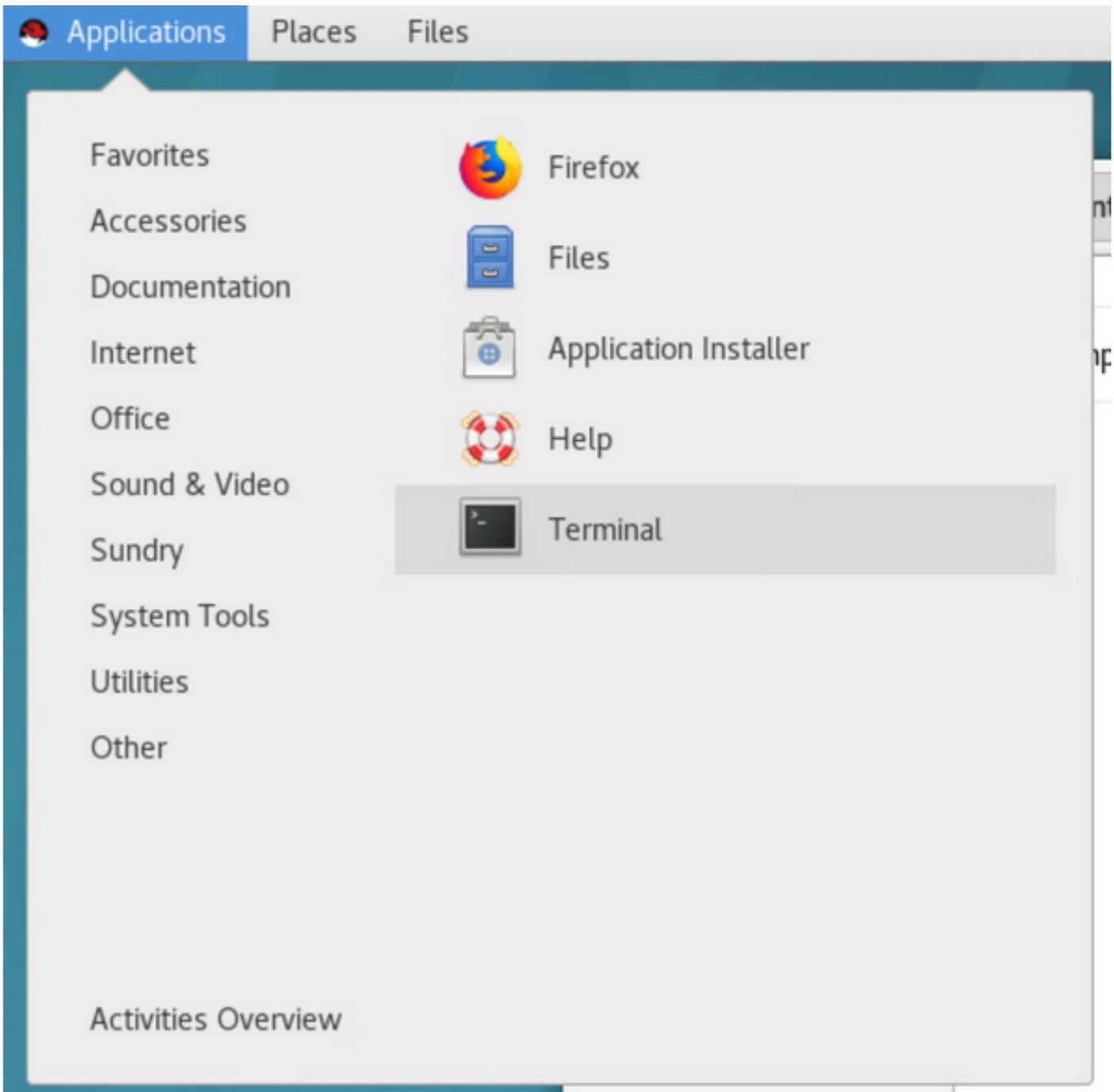
```
File Edit View Search Terminal Help
[jenator@jenator-lin-ssl-lab Downloads] sudo yum localinstall amp_juanc2ProxyGroup_rhel-centos-7.rpm -y
[sudo] password for jenator:
Loaded plugins: langpacks, product-id, search-disabled-repos, subscription-manager
This system is not registered with an entitlement server. You can use subscription-manager to register.
Examining amp_juanc2ProxyGroup_rhel-centos-7.rpm: ciscoampconnector-1.12.1.682-1.el7.x86_64
Marking amp_juanc2ProxyGroup_rhel-centos-7.rpm as an update to ciscoampconnector-1.10.2.638-1.el7.x86_64
Resolving Dependencies
--> Missing transaction check
--> Package ciscoampconnector.x86_64 0:1.10.2.638-1.el7 will be updated
--> Package ciscoampconnector.x86_64 0:1.12.1.682-1.el7 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                Arch          version                Repository              Size
-----
Updating:
ciscoampconnector      x86_64        1.12.1.682-1.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.unsaved
```

GUIを使用している場合は、図に示すように端末を開きます。



インストールが開始されると、ユーザの入力は必要ありません。これは図に示すように自動的に行われます。

```
File Edit View Search Terminal Help
ipatching:
ciscoampconnector      x86_64      1.12.2.602-1.el7      /amp_proxyGroup_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 at /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      2/2

Updated:
  ciscoampconnector.x86_64 0:1.12.2.602-1.el7

Complete!
[[jcsutor@jesutarr-lin-mex-lab Downloads]$
```

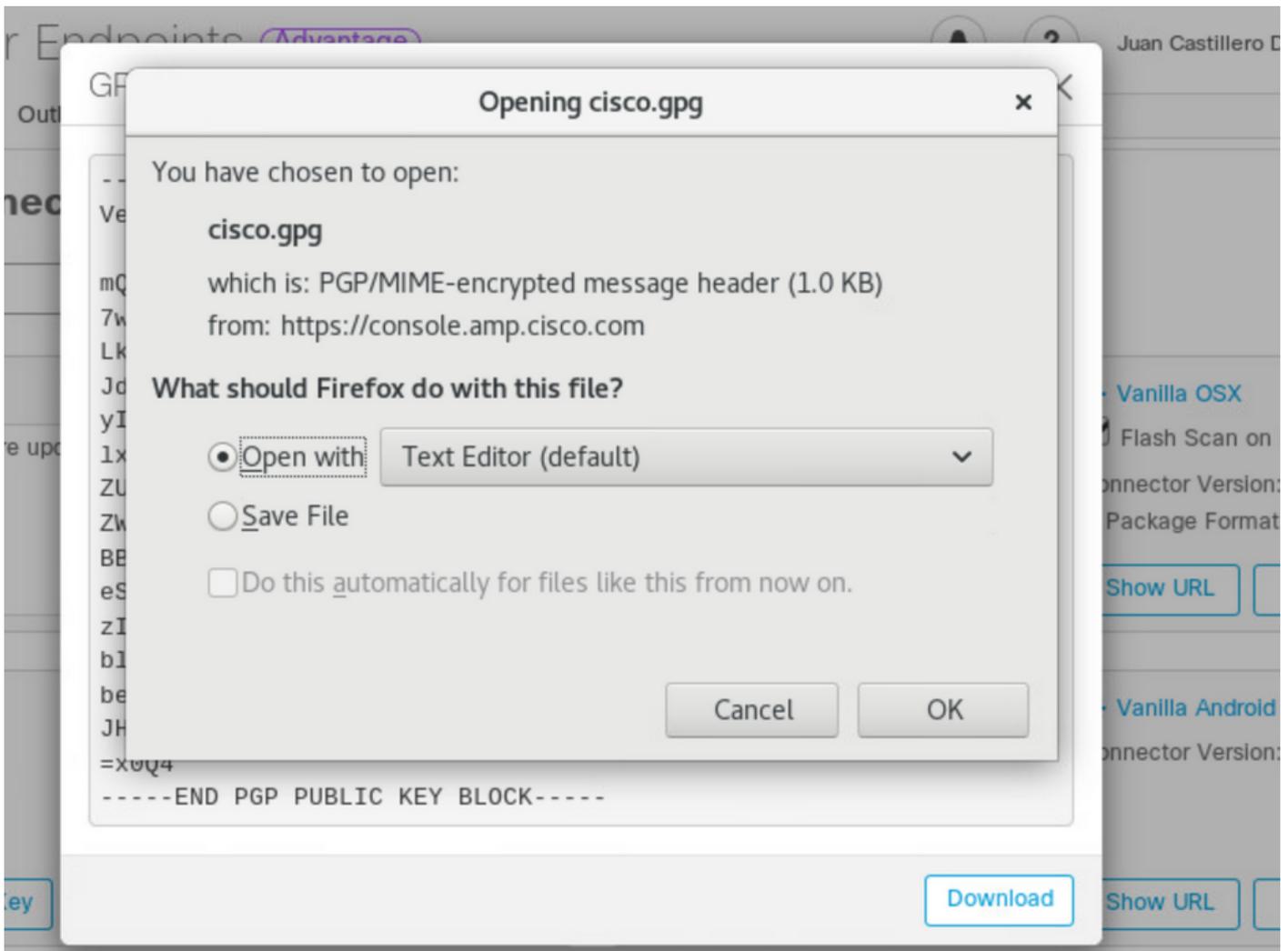
GPGキーをインポートする方法

GPG公開キーは、Download Connectorページからコピーして、RPMパッケージの署名を確認できます。コネクタはGPGキーなしでインストールできます;ただし、ユーザー RHELのポリシーを使用してコネクタのアップデートをプッシュする場合は、GPGキーをRPM DBにインポートする必要があります。

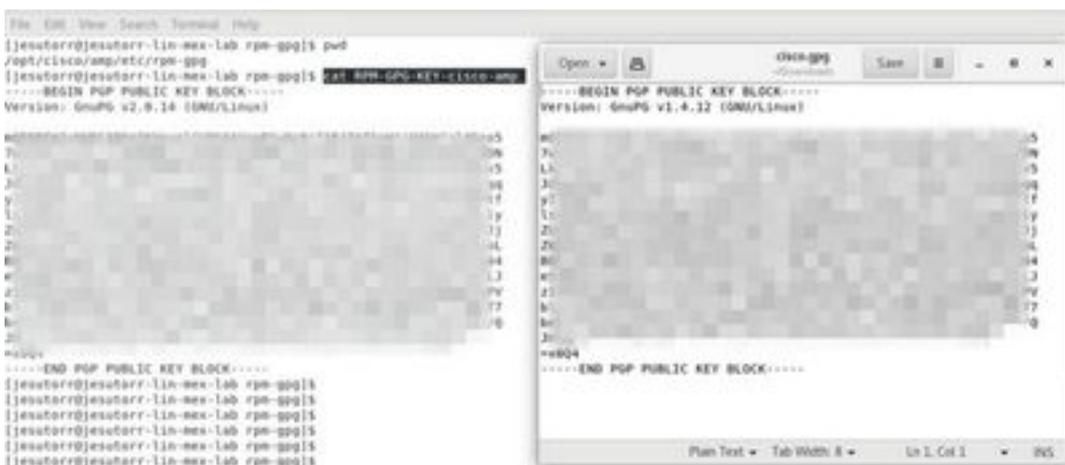
注：コネクタバージョン1.17.0以降、コネクタのアップデート中にアップグレードパッケージを確認するために使用されるGPGキーが自動的にインストールされます。

ステップ1:GPGキーを確認し、[Download Connector]ページで[GPG Public Key]リンクをクリックします。/opt/cisco/amp/etc/rpm-gpg/RPM-GPG-Key-cisco-ampのキーと比較します。





ステップ2 : 端末からコマンドを実行して、キーをインポートします。 `sudo rpm --import /opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp`。



ステップ3 : キーがインストールされたことを確認し、ターミナルからコマンドを実行します。 `rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n'`。



ステップ4 : 出力でSourcefireからGPGキーを探します。Updaterはシステムのinitデーモンによっ

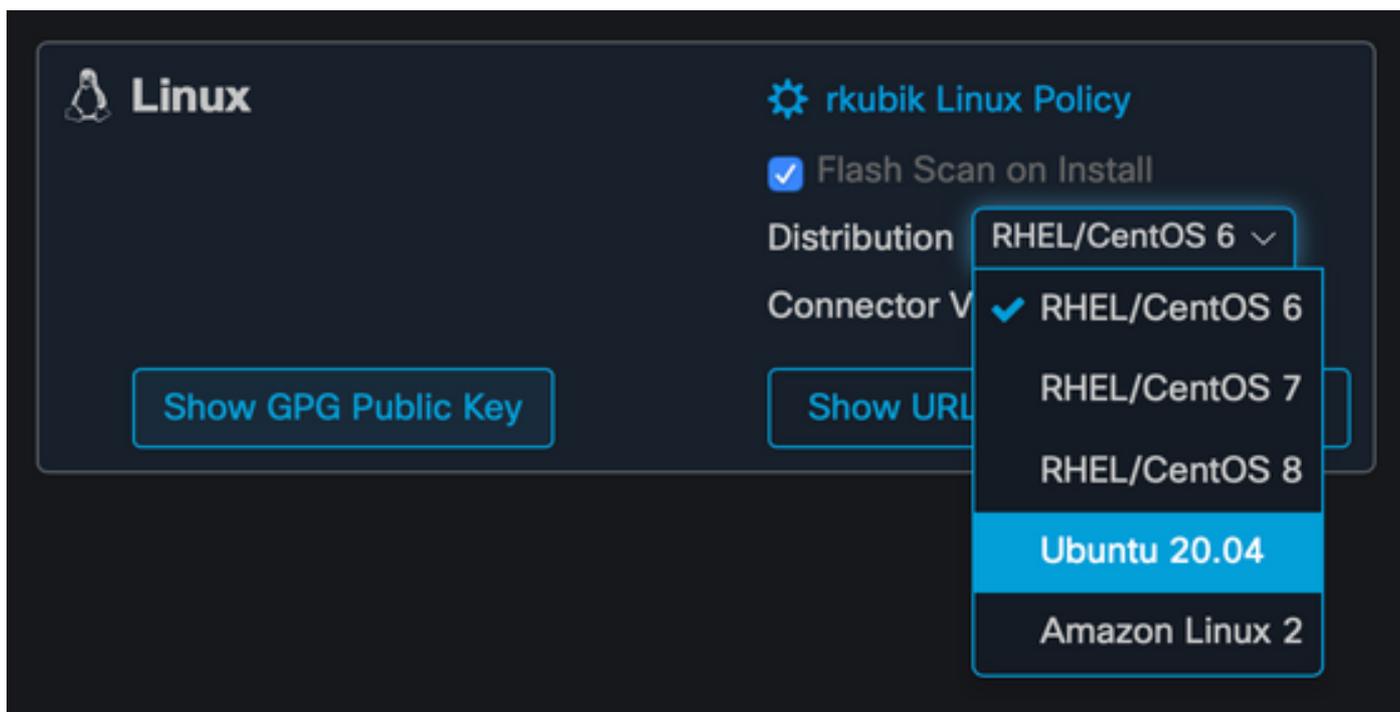
て実行され、アップデートが利用可能になると、自動的にRPMアップグレードプロセスがトリガーされます。一部のSELinux設定では、この動作を禁止し、Updaterが失敗します。

この場合は、システムの監査ログ(/var/log/audit/audit.logなど)を調べ、管理者に関連する拒否イベントを検索します。Updaterが機能するようにSELinuxルールを調整する必要があります。

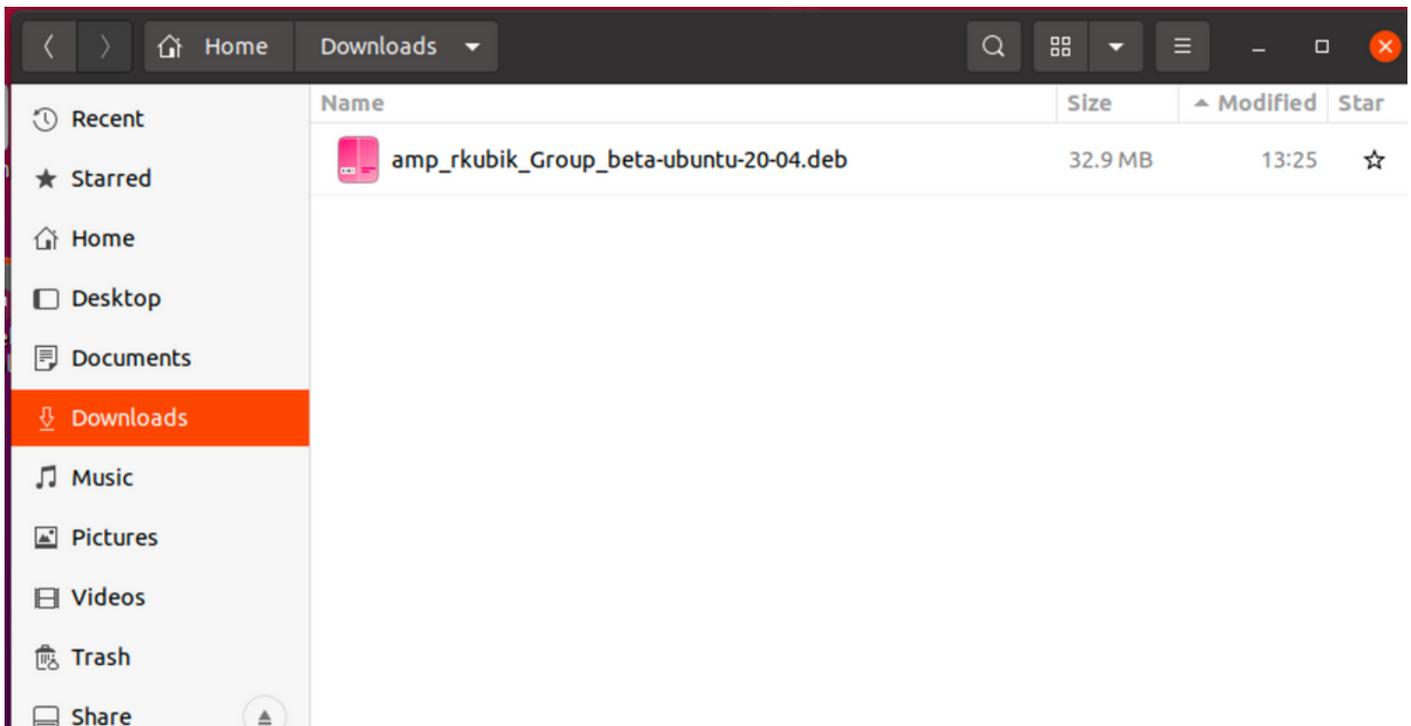
Ubuntu

設定

ステップ1: 図に示すように、Cisco Secure Endpoint PortalからLinux DEBパッケージをダウンロードします。



ステップ2: DEBパッケージを該当するエンドポイントに移動し、ダッシュボードから直接ダウンロードするか、手動でエンドポイントに移動します。この例では、Graphic User Interface (UI; グラフィックユーザインターフェイス) を使用して、最小限のインストールで作業することが可能で、多くの場合は一般的です。この場合は、Linux端末の処理方法を知って、DEBパッケージを見つける必要があります。



ステップ3:Linuxコネクタをインストールするには、次のコマンドを実行します。**sudo dpkg -i [deb package]**ここで、[deb package]はファイルの名前です (「amp_Audit.deb」など)。インストールが開始されると、ユーザの入力は必要ありません。これは図に示すように自動的に行われます。

```

/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
$ █
```

GPGキーをインポートする方法

GPG公開キーは、Download Connectorページからコピーして、DEBパッケージの署名を確認できます。コネクタはGPGキーなしでインストールできます。ただし、Ubuntuのポリシーを通じてコネクタの更新をプッシュする予定の場合は、ユーザーがGPGキーをデバッグキーリングにインポートする必要があります。GPGキーをインポートし、コネクタがUbuntuで変更されていないことを確認する方法の詳細については、<https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/216524-amp-for-endpoints-ubuntu-connector.html#anc6>を参照してください

注：コネクタバージョン1.17.0以降、コネクタのアップデート中にアップグレードパッケージを

確認するために使用されるGPGキーが自動的にインストールされます。このGPGキーを確認するには、[Download Connector]ページの[GPG Public Key]リンクをクリックし、`/opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-Key-cisco-amp`にインストールされたキーと比較します。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

正常にインストールされたことを確認するには、AMP CLIを実行します。Linuxコネクタのコマンドラインインターフェイスは`/opt/cisco/amp/bin/ampcli`にあります。インタラクティブ・モードで実行することも、1つのコマンドを実行して終了することもできます。コマンド`./ampcli --help`を実行して、利用可能なオプションとコマンドの全リストを表示します。コネクタによって生成されたすべてのログファイルは`/var/log/cisco`にあります。

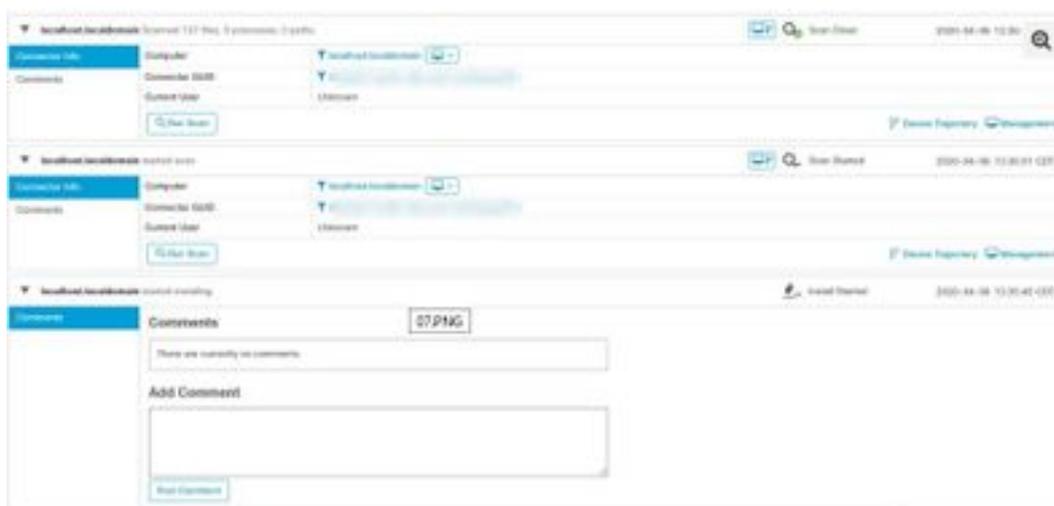
```
File Edit View Search Terminal Help
[jesuiter@jesuiter-lin-nsx-lab ~]$ cd /opt/cisco/amp/bin/
[jesuiter@jesuiter-lin-nsx-lab bin]$ pwd
/opt/cisco/amp/bin
[jesuiter@jesuiter-lin-nsx-lab bin]$ ls
ampcli  ampcli.ampcli  ampcli.service  ampcli.support  cisco-amp-helper  lib64/ampcli.so.0  lib64/ampcli.so  lib64/ampcli.so.0.2.0
ampcli.man  ampcli.service  ampcli.service  ampcli.service  lib64/ampcli.so  lib64/ampcli.so.0.2.0  lib64/ampcli.so  ampcli
[jesuiter@jesuiter-lin-nsx-lab bin]$ ./ampcli

ampcli - AMP for Endpoints Connector Command Line Interface
Interactive mode

Enter 'q' or Ctrl+C to Exit

[Debugger] Set minimum 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: Jigsaw-Linux (451200)
Command-Line: Enabled
Faults: None
ampcli █
```

また、Cisco Secureコンソールにもインストールイベントが表示されます。RPMパッケージのダウンロード時にフラッシュスキャンが要求された場合は、フラッシュスキャンも表示されます。



トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [LinuxビデオでのAMP for Endpoints Connectorのインストール](#)

- [テクニカル サポートとドキュメント – Cisco Systems](#)