Cisco Secure Endpoint Linux Connectorのインストール

内容

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)

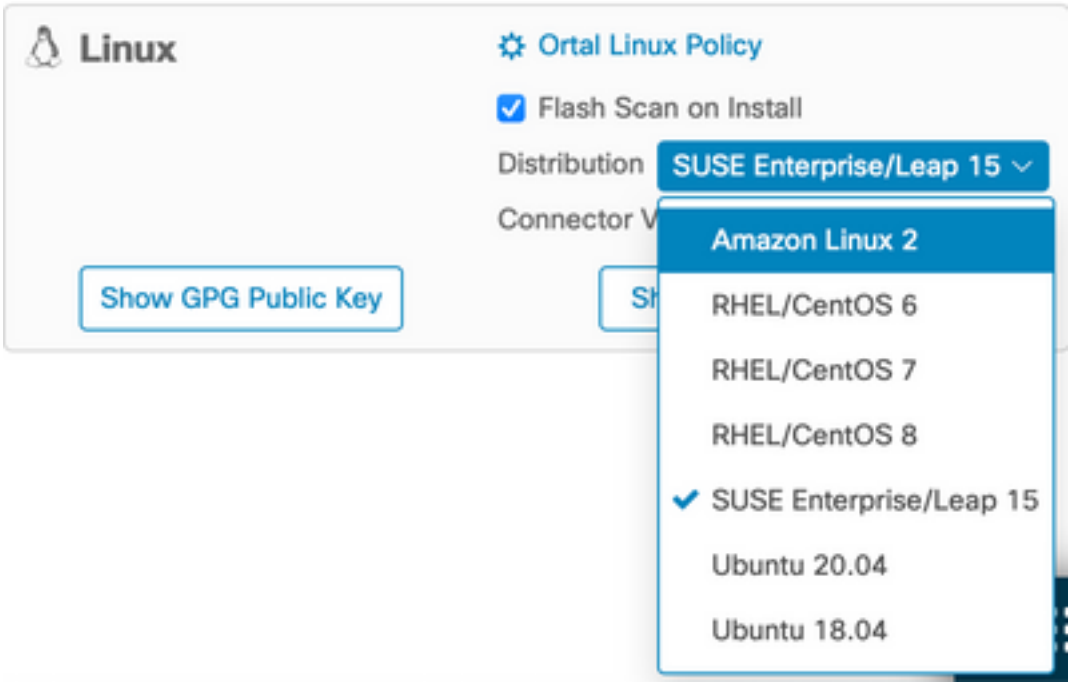
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

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

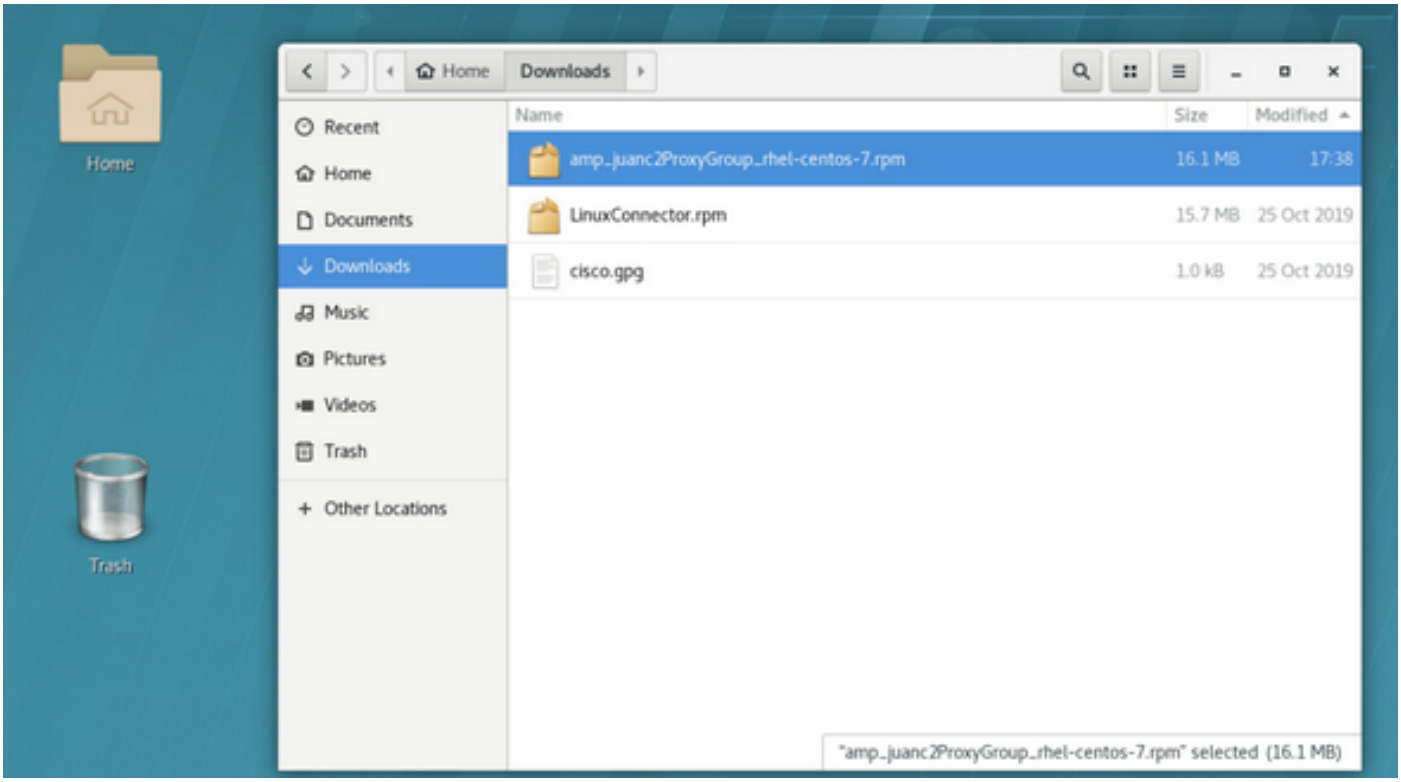
設定

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。

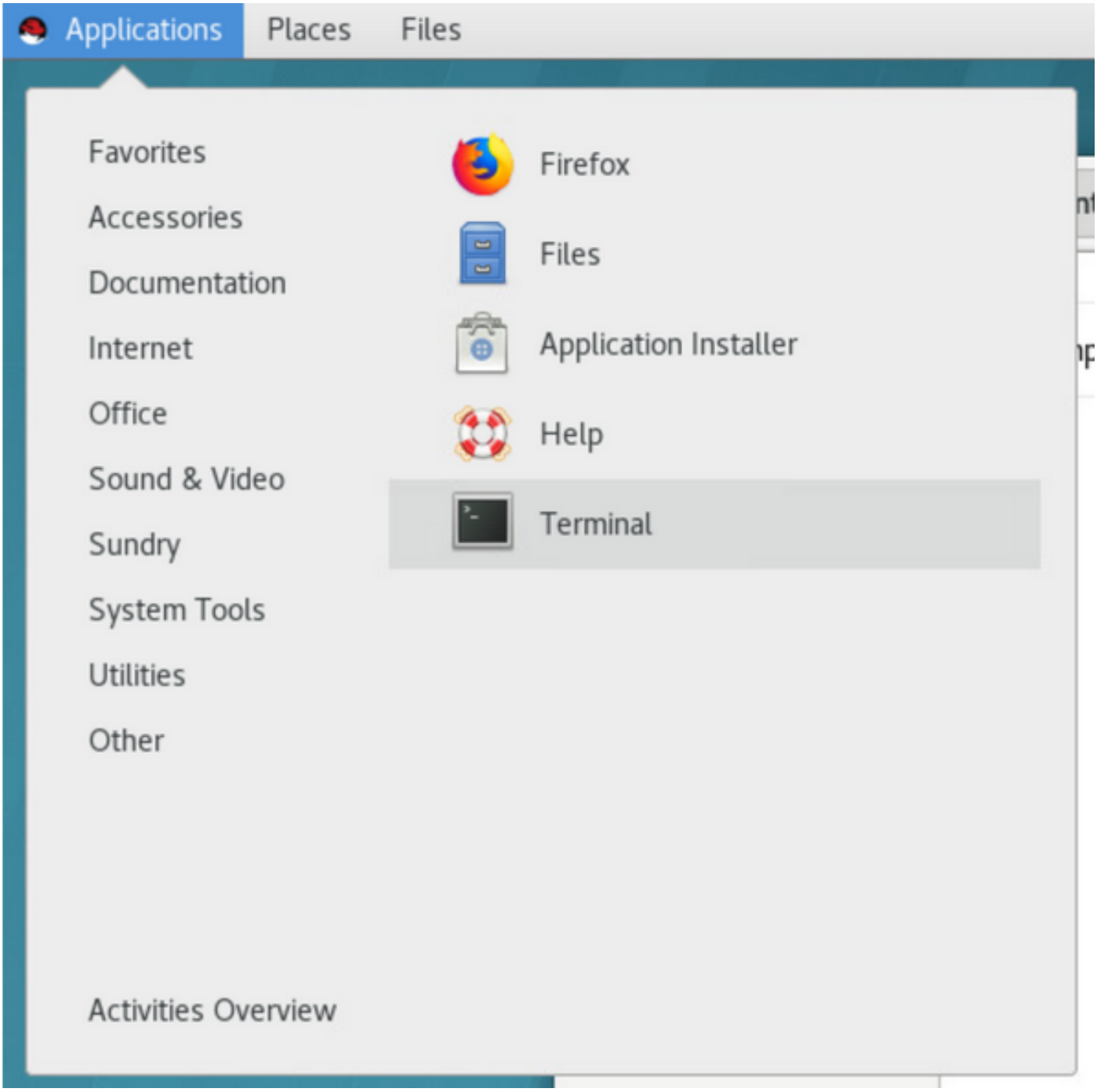
ステップ2:RPMパッケージを該当するエンドポイントに移動し、ダッシュボードから直接ダウンロードするか、手動でエンドポイントに移動します。この例では、Graphic User Interface（UI；グラフィックユーザインターフェイス）を使用していますが、最小限のインストールで作業することは可能で、しばしば一般的です。その場合は、Linux端末の扱い方を知って、RPMパッケージを見つける必要があります。



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。

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。



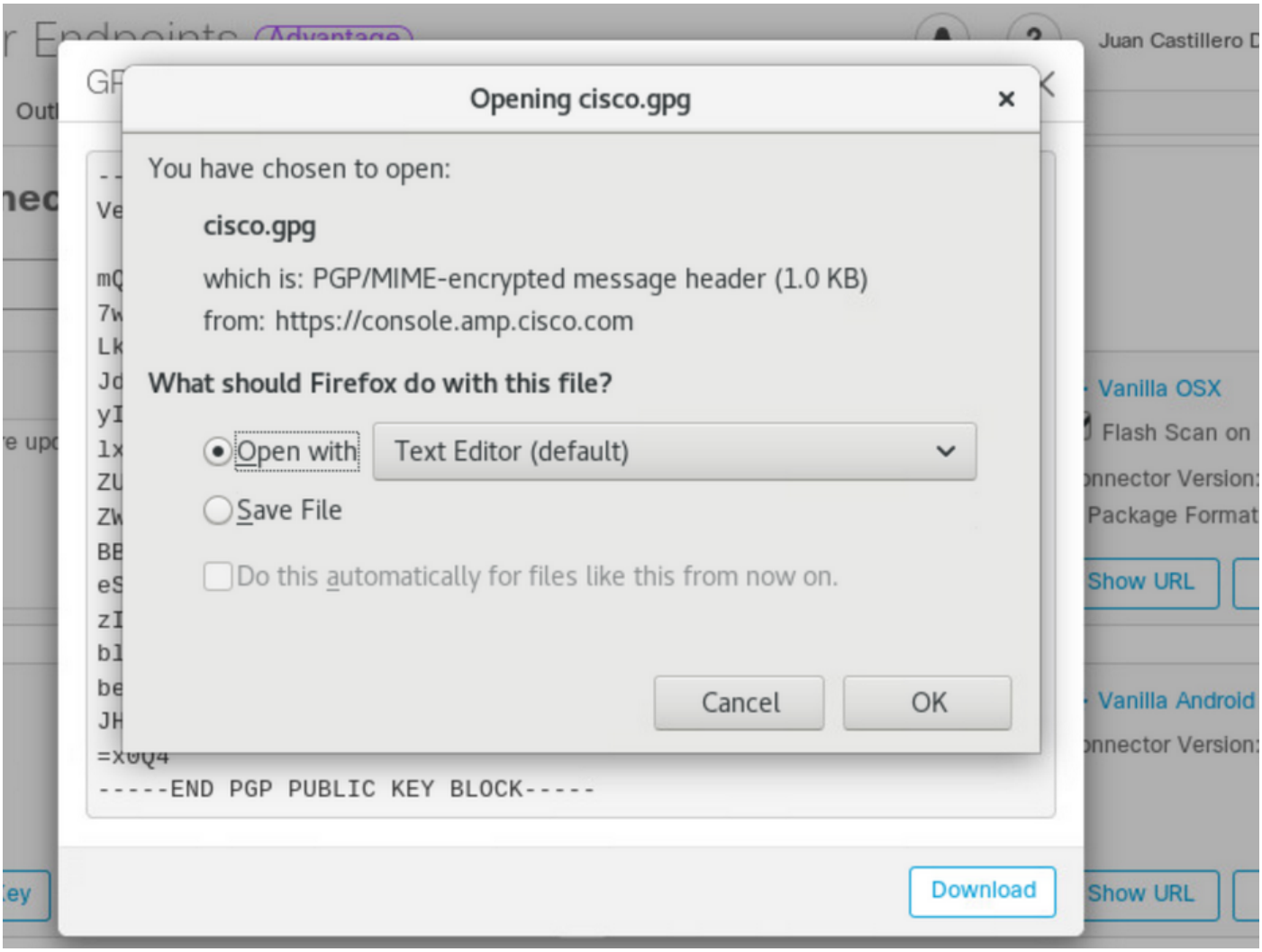
インストールが開始されると、ユーザの入力は必要ありません。これは図に示すように自動的に行われます。

GPGキーをインポートする方法

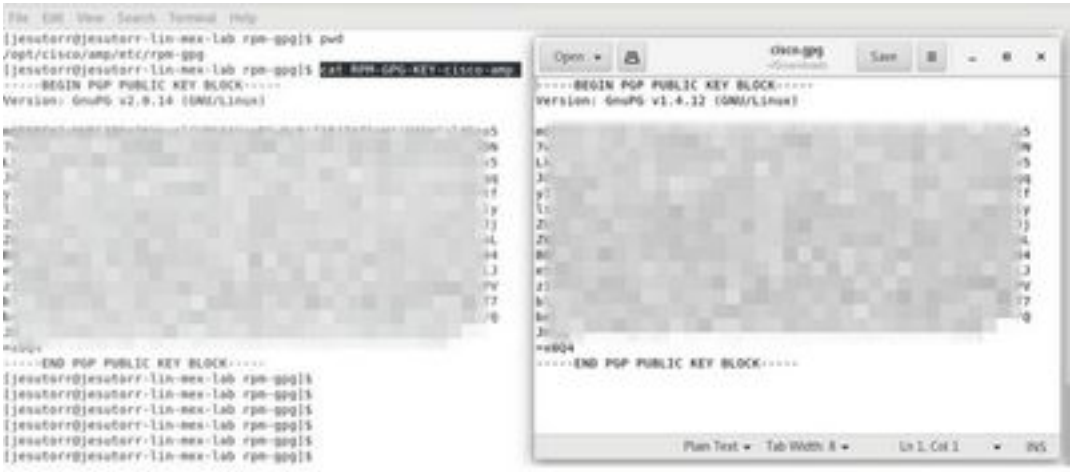
GPG公開キーは、Download Connectorページからコピーして、RPMパッケージの署名を確認できます。コネクタはGPGキーなしでインストールできます;ただし, ユーザー RHELのポリシーを使用してコネクタのアップデートをプッシュする場合は、GPGキーをRPM DBにインポートする必要があります.

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

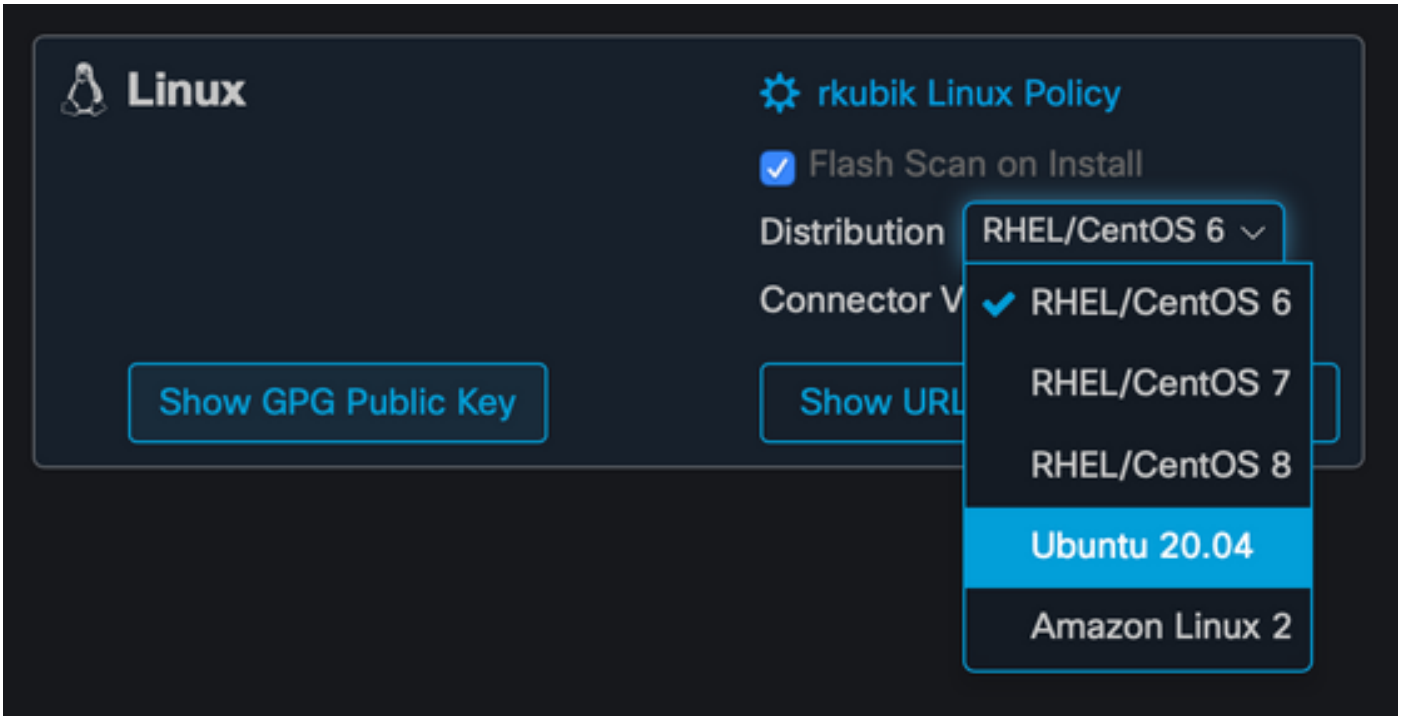
て実行され、アップデートが利用可能になると、自動的にRPMアップグレードプロセスがトリガーされます。一部のSELinux設定では、この動作を禁止し、Updaterが失敗します。

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。

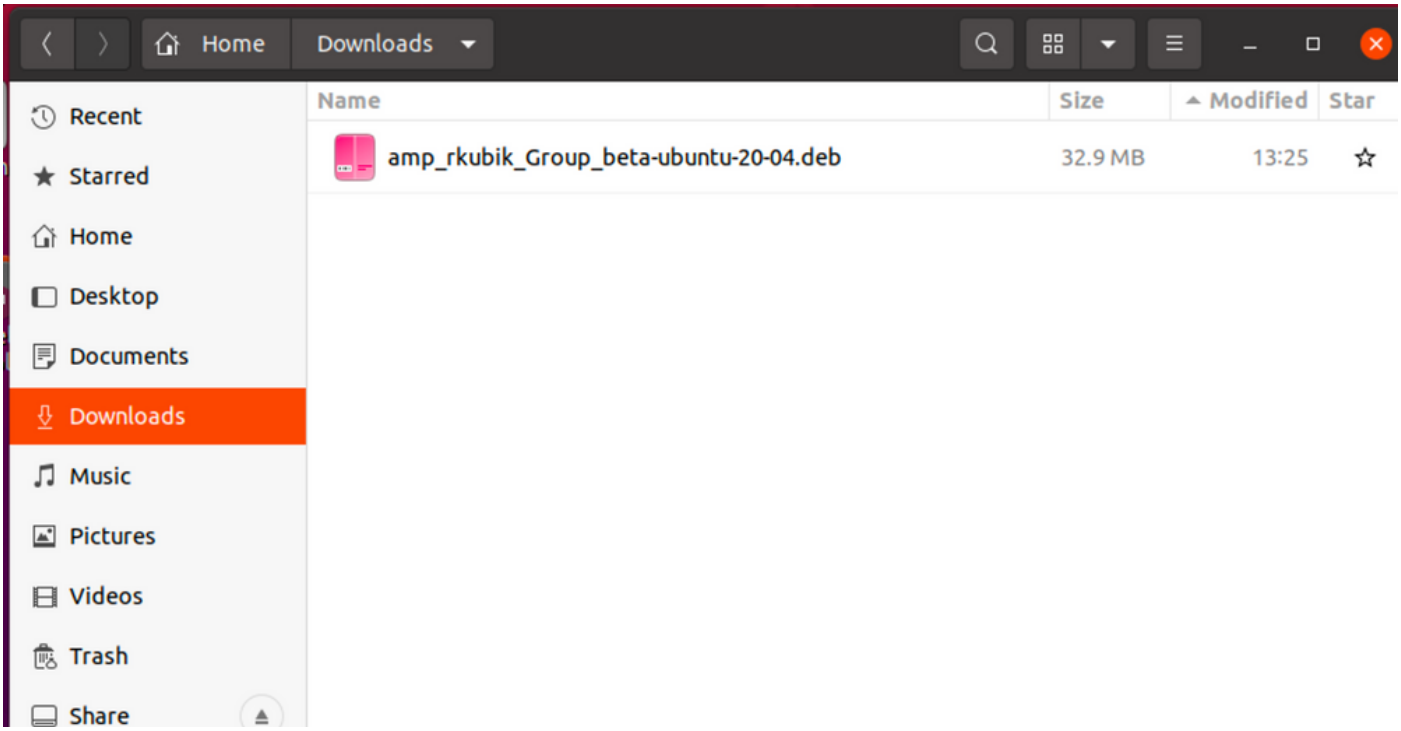
Ubuntu

設定

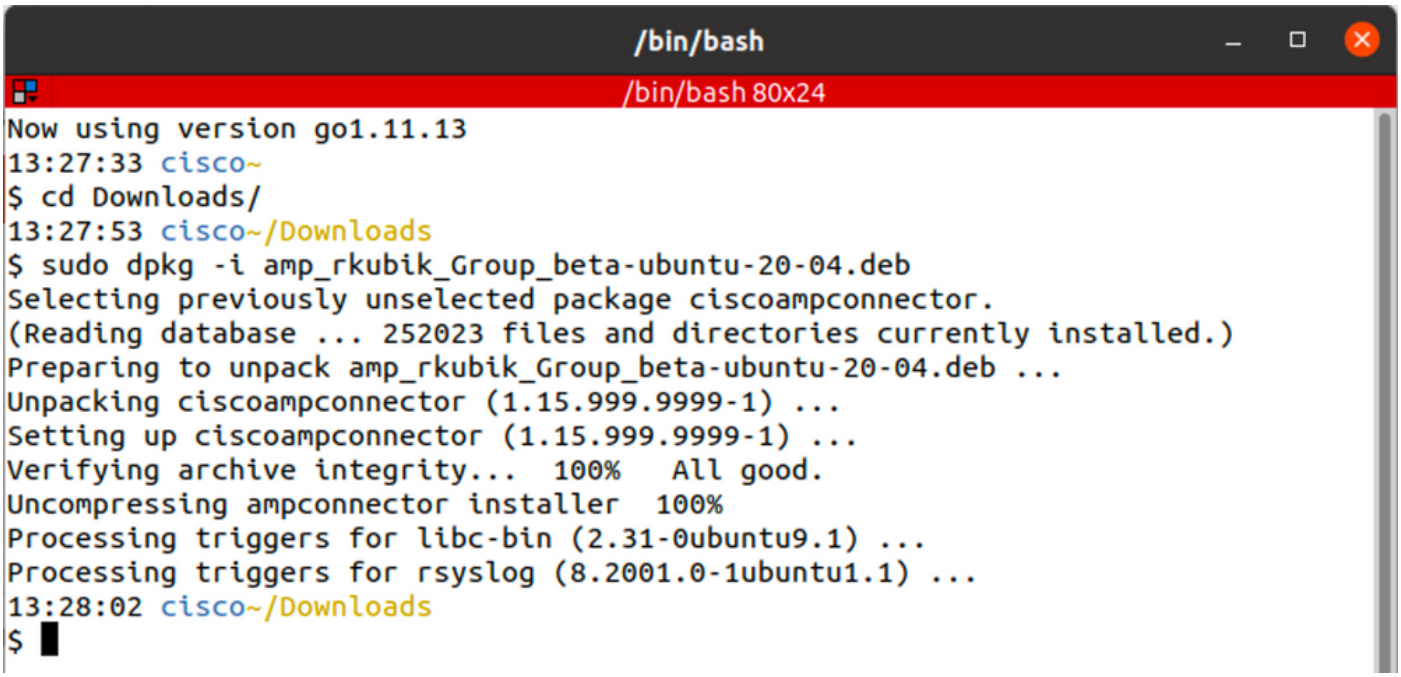
ステップ1：図に示すように、Cisco Secure Endpoint PortalからLinux DEBパッケージをダウンロードします。



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。



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

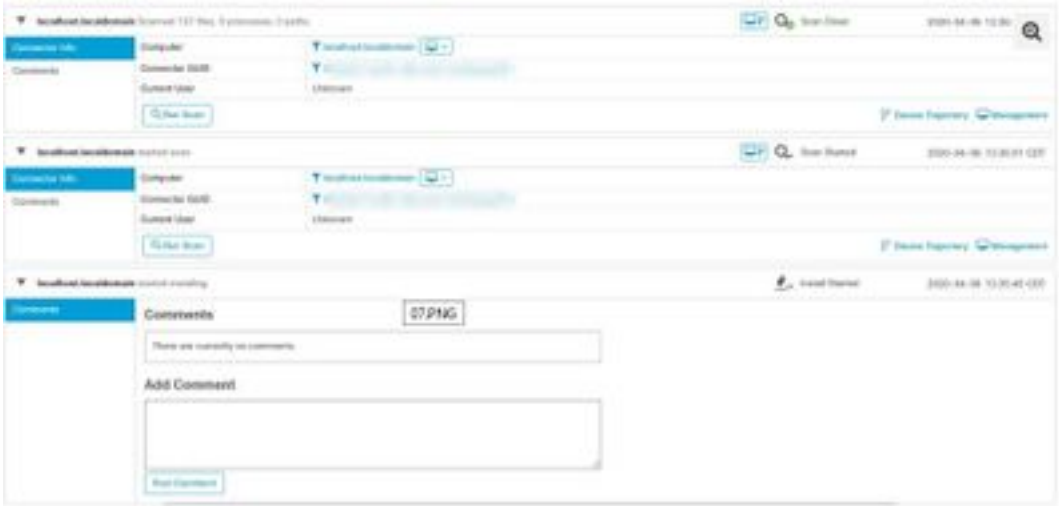
確認するために使用されるGPGキーが自動的にインストールされます。このGPGキーを確認するには、[Download Connector]ページの[GPG Public Key]リンクをクリックし、/opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-Key-cisco-ampにインストールされたキーと比較します。

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。

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。



トラブルシュート

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