DebianベースシステムのCisco Secure Endpoint Linux Connector

内容

この記事では、管理者がDebianベースのシステムにCisco Secure Endpoint Linuxコネクタを導入するために実行できる変更と手順について説明します。

- Debian 10以降。
- Ubuntu 18.04以降。

OSの最小要件

OSの互換性については、『Cisco Secure Endpoint Linux Connector OSの互換性』の記事を参照してください。

環境の設定

DebianベースのシステムのLinuxコネクタは、eBPFを使用してファイルとネットワークを監視します。正しいlinux-headersソフトウェアパッケージがインストールされている必要があります。インストールされていない場合、コネクタは障害11（システムの依存関係が欠落している）を発生させ、ファイルやネットワークを監視せずに機能低下状態で動作します。この障害を解決するためのガイダンスは、Linux Kernel-Devel Faultの記事に掲載されています。

依存関係

Linuxコネクタは、Debianベースのシステムのベースインストールに含まれているシステムパッケージに依存しますが、依存関係がない場合は次のメッセージが表示されます。

```
ciscoampconnector depends on
```

次のコマンドを使用して、Linuxコネクタに必要な依存関係がない場合にインストールします。

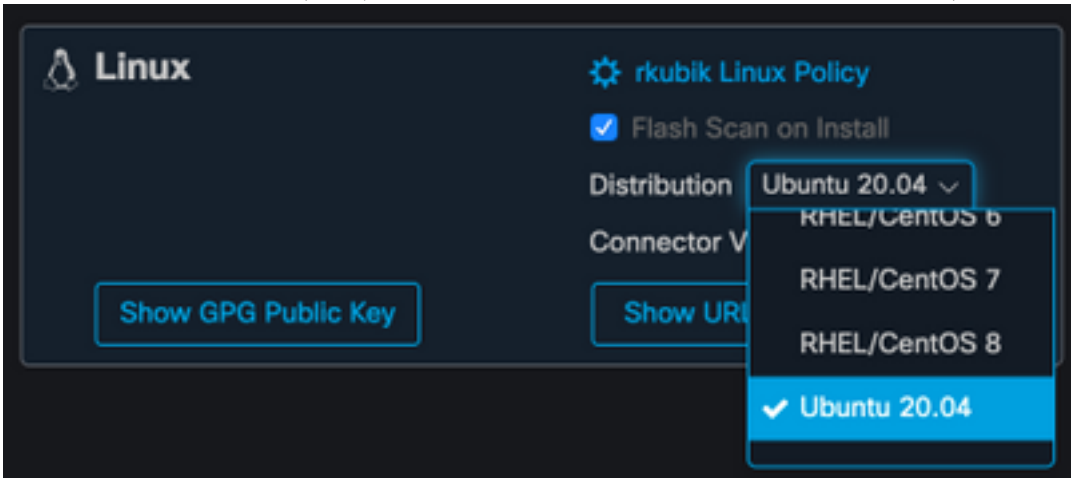
```
sudo apt install
```

DEBパッケージの確認

LinuxコネクタDEBパッケージには、ダウンロードしたソフトウェアパッケージがシスコに属していることを確認するための署名が含まれています。

DEBパッケージのダウンロード

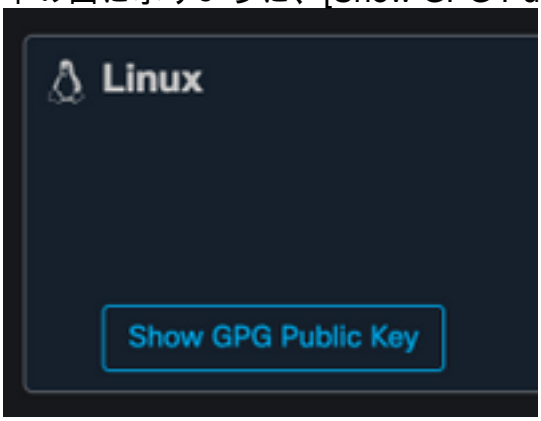
1. AMP for Endpointsコンソールにアクセスします。
2. Debianベースのシステム用のDEBパッケージをダウンロードします。



3. DEBパッケージをDebianベースのシステムに転送します。以下に、いくつかの例を示します。amp_ciscoampconnector.deb

GPG公開キーの取得

1. 下の図に示すように、[Show GPG Public Key]ボタンをクリックします。



2. コネクタのバージョンが1.17.0より前の場合は、コンピュータに公開キーをダウンロードして転送するか、コピーします。以下に、いくつかの例を示します。cisco.gpg.コネクタのバージョンが1.17.0以上の場合、GPGキーは/opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-KEY-cisco-ampで使用できます。

DEBパッケージの確認

DEBパッケージはdebsigsツールを使用して署名され、debsig-verifyを使用して検証できます。

1. debug-verifyツールをインストールします。
```
sudo apt-get install debsig-verify
```

2. Cisco GPG公開キーをデバッグキーリングにインポートします。**注：**バージョン1.17.0以降では、debsig.gpgファイルが自動的に作成されるため、ステップ2はスキップできます。
   ```
   sudo mkdir -p /usr/share/debsig/keyrings/914E5BE0F2FD178F sudo gpg --dearmor --output /usr/share/debsig/keyrings/914E5BE0F2FD178F/debsig.gpg cisco.gpg
   ```
3. ポリシーディレクトリを作成します。
   ```
   sudo mkdir -p /etc/debsig/policies/914E5BE0F2FD178F
   ```
4. 次のポリシーの内容を新しいファイル「/etc/debsig/policies/914E5BE0F2FD178F/ciscoampconnector.pol」にコピーします。

5. debug-verifyを使用してDEBシグニチャを確認します。
   ```
   debsig-verify amp_ciscoampconnector.deb
   ```
   出力は次のようになります。
   ```
   debsig: Verified package from 'Cisco AMP for Endpoints' (Debsig)
   ```

注：ステップ5は、AMP for Endpointsコンソールからダウンロードしたdebianベースのパッケージに対して繰り返すことができます。

設置

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。[deb package]にはファイルの名前を指定します（たとえば、amp_test.deb）。

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

重要：環境内の他のセキュリティ製品を実行している場合は、コネクタのインストーラが脅威として検出される可能性があります。コネクタを正常にインストールするには、許可リストにCisco Secureを追加するか、他のセキュリティ製品のCisco Secureを除外して、もう一度やり直してください。

重要：コネクタのインストール中に、cisco-amp-scan-svcという名前のユーザとグループがシステムに作成されます。このユーザまたはグループがすでに存在するが、設定が異なる場合、インストーラは必要な設定で削除を試み、再作成を試みます。必要な設定でユーザとグループを作成できなかった場合、インストーラは失敗します。

アンインストール

セキュアエンドポイントユーザガイドアンインストール手順

改訂履歴

2020年12月10日

- 初期バージョン

2022年4月12日

- コンテンツはDebianとUbuntuの両方に適用されます。