Cisco Secure Endpoint Linux Connector auf Debian-basierten Systemen

Inhalt

Dieser Artikel beschreibt die Änderungen und Schritte, die Administratoren durchführen können, um den Cisco Secure Endpoint Linux-Connector auf Debian-basierten Systemen bereitzustellen:

- Debian 10 und höher.
- Ubuntu 18.04 und neuer.

Betriebssystem-Mindestanforderungen

Informationen zur Betriebssystemkompatibilität finden Sie im Artikel zur Kompatibilität von Cisco Secure Endpoint Linux Connector OS.

Umgebungseinrichtung

Der Linux-Connector auf Debian-basierten Systemen verwendet eBPF für die Datei- und Netzwerküberwachung. Auf dem Computer muss das richtige Linux-Header-Softwarepaket installiert sein. Andernfalls löst der Anschluss den Fehler 11 (Fehlende Systemabhängigkeit) aus und läuft ohne Datei- und Netzwerküberwachung in einem heruntergestuften Zustand. Eine Anleitung zur Behebung dieses Fehlers finden Sie im Linux Kernel-Devel Fault Artikel.

Abhängigkeiten

Der Linux-Connector hängt von Systempaketen ab, die in der Basisinstallation von Debian-basierten Systemen enthalten sind, aber wenn eine Abhängigkeit fehlt, erscheint die folgende Meldung:

```
ciscoampconnector depends on
```

Verwenden Sie den folgenden Befehl, um alle fehlenden Abhängigkeiten zu installieren, die vom Linux-Anschluss benötigt werden:

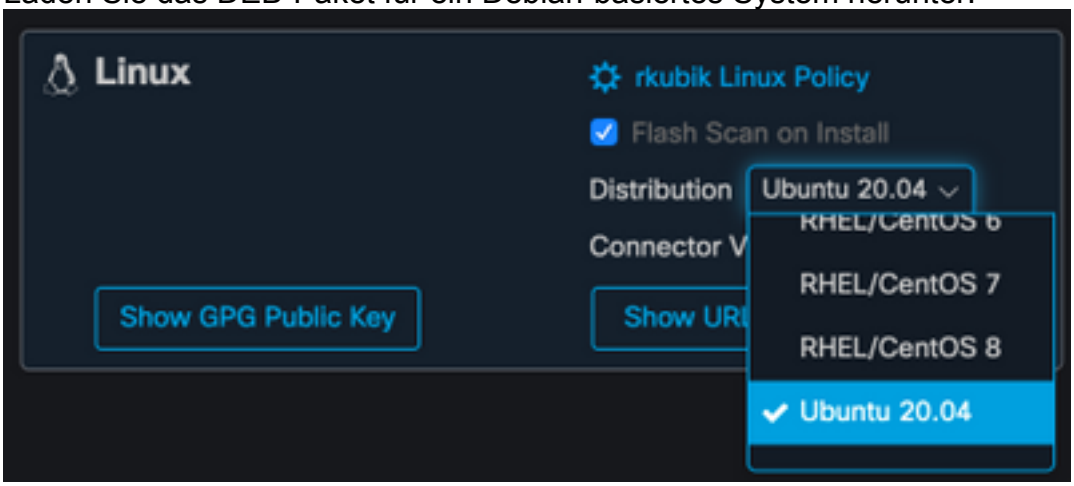
```
sudo apt install
```

Überprüfen des DEB-Pakets

Das Linux Connector DEB-Paket enthält eine Signatur, um zu überprüfen, ob das heruntergeladene Softwarepaket zu Cisco gehört.

DEB-Paket herunterladen

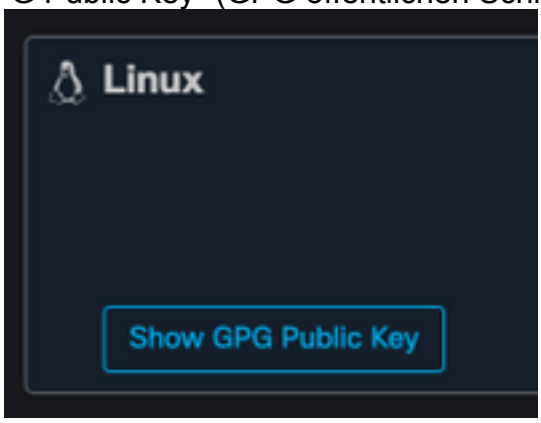
1. Zugriff auf die AMP für Endgeräte-Konsole
2. Laden Sie das DEB-Paket für ein Debian-basiertes System herunter.



3. Übertragen Sie das DEB-Paket auf das Debian-basierte System. Beispiele: amp_ciscoampconnection.deb.

Abrufen des öffentlichen GPG-Schlüssels

1. Klicken Sie auf "Show GPG Public Key" (GPG öffentlichen Schlüssel anzeigen), wie in der Abbildung unten gezeigt.



2. Wenn die Connector-Version älter als 1.17.0 ist, laden Sie den öffentlichen Schlüssel herunter und übertragen Sie ihn, oder kopieren Sie ihn auf den Computer. Beispiele: cisco.gpg. Wenn die Anschlussversion mindestens 1.17.0 ist, ist der GPG-Schlüssel unter /opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-KEY-cisco-amp verfügbar.

Überprüfen des DEB-Pakets

Das DEB-Paket wird mit dem Debsigs-Tool signiert und kann mittels Debsig-Verification verifiziert werden.

1. Installieren Sie das Debsig-Verification-Tool.
   ```
   sudo apt-get install debsig-verify
   ```
2. Importieren Sie den öffentlichen Cisco GPG-Schlüssel in den Debsigs-Keyring. **Hinweis:** Ab Version 1.17.0 wird die Datei debsig.gpg automatisch erstellt, sodass Schritt 2 übersprungen werden kann.
   ```
   sudo mkdir -p /usr/share/debsig/keyrings/914E5BE0F2FD178F sudo gpg --dearmor --output
   /usr/share/debsig/keyrings/914E5BE0F2FD178F/debsig.gpg cisco.gpg
   ```
3. Erstellen Sie ein Richtlinienverzeichnis.
   ```
   sudo mkdir -p /etc/debsig/policies/914E5BE0F2FD178F
   ```
4. Kopieren Sie den Richtlinieninhalt unten in eine neue Datei "/etc/debsig/policies/914E5BE0F2FD178F/ciscoampconnector.pol".

5. Überprüfen Sie die DEB-Signatur mit "debsig-verify".
   ```
   debsig-verify amp_ciscoampconnector.deb
   ```
   Die Ausgabe sollte wie folgt aussehen:
   ```
   debsig: Verified package from 'Cisco AMP for Endpoints' (Debsig)
   ```

Anmerkung: Schritt 5 kann für alle Debian-basierten Pakete wiederholt werden, die von der AMP für Endpoints-Konsole heruntergeladen wurden.

Installation

Um den Connector zu installieren, führen Sie den folgenden Befehl aus, wobei [deb-Paket] der Name der Datei ist, z. B. amp_test.deb:

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

WICHTIG! Wenn Sie andere Sicherheitsprodukte in Ihrer Umgebung ausführen, besteht die Möglichkeit, dass diese das Installationsprogramm des Connectors als Bedrohung erkennen. Um den Connector erfolgreich zu installieren, fügen Sie Cisco Secure zu einer zulässigen Liste hinzu, oder schließen Sie Cisco Secure in den anderen Sicherheitsprodukten aus, und versuchen Sie es erneut.

WICHTIG! Während der Anschlussinstallation wird im System ein Benutzer und eine Gruppe mit dem Namen cisco-amp-scan-svc erstellt. Wenn dieser Benutzer oder diese Gruppe bereits vorhanden, aber anders konfiguriert ist, versucht das Installationsprogramm, diese zu löschen und dann mit der erforderlichen Konfiguration erneut zu erstellen. Das Installationsprogramm schlägt fehl, wenn der Benutzer und die Gruppe nicht mit der erforderlichen Konfiguration erstellt werden konnten.

Deinstallation

Weitere Informationen finden Sie im Benutzerhandbuch für sichere Endgerätefür Anweisungen zur Deinstallation

Revisionsverlauf

10. Dezember 2020

- Erstversion

12. April 2022

- Inhalte gelten sowohl für Debian als auch für Ubuntu.