Cisco Secure Endpoint Linux Connector sur les systèmes basés sur Debian

Contenu

Cet article décrit les changements et les étapes que les administrateurs peuvent effectuer pour déployer le connecteur Cisco Secure Endpoint Linux sur les systèmes basés sur Debian :

- Debian 10 et versions ultérieures.
- Ubuntu 18.04 et plus récent.

Configuration système minimale requise

Consultez l'article Cisco Secure Endpoint Linux Connector OS Compatibility pour obtenir la compatibilité du système d'exploitation.

Configuration de l'environnement

Le connecteur Linux sur les systèmes basés sur Debian utilise eBPF pour la surveillance des fichiers et du réseau. Le package logiciel linux-headers correct doit être installé sur l'ordinateur. Sinon, le connecteur déclenchera la défaillance 11 (Dépendance système manquante) et s'exécutera dans un état dégradé sans surveillance des fichiers et du réseau. Des conseils pour résoudre ce problème se trouvent dans l'article Linux Kernel-Devel Fault.

Dépendances

Le connecteur Linux dépend des paquets système qui sont inclus dans l'installation de base des systèmes basés sur Debian, mais si une dépendance manque, le message suivant s'affiche :

```
ciscoampconnector depends on
```

Utilisez la commande suivante pour installer les dépendances manquantes requises par le connecteur Linux :

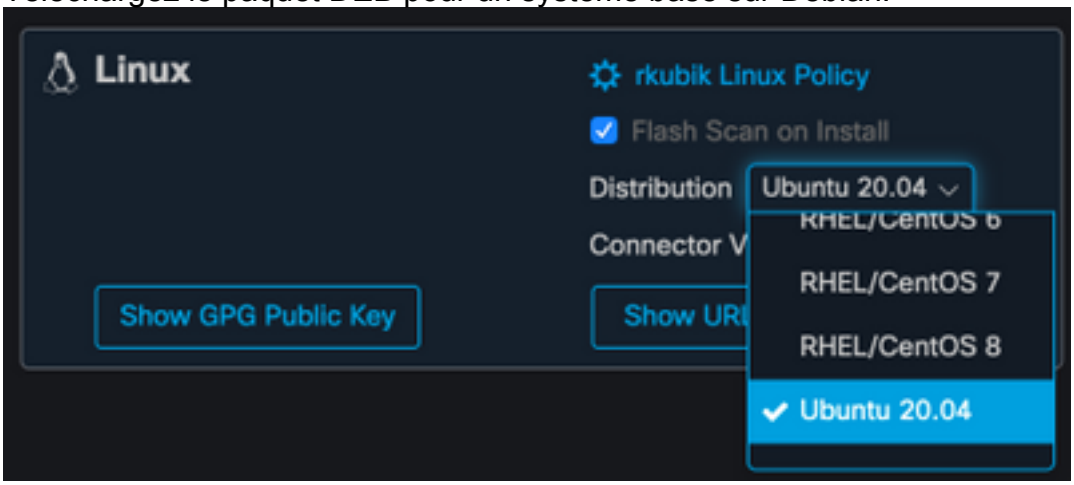
```
sudo apt install
```

Vérification du package DEB

Le paquet DEB du connecteur Linux contient une signature pour vérifier que le paquet logiciel téléchargé appartient à Cisco.

Téléchargement du package DEB

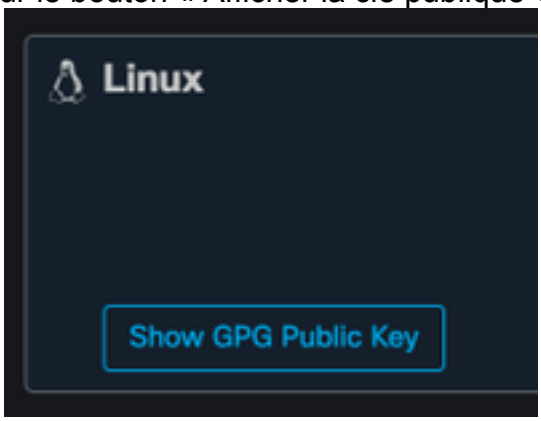
1. Accédez à la console AMP for Endpoints.
2. Téléchargez le paquet DEB pour un système basé sur Debian.



3. Transférez le paquet DEB vers le système Debian. Exemple : amp_ciscoampconnector.deb.

Récupération de la clé publique GPG

1. Cliquez sur le bouton « Afficher la clé publique GPG », comme indiqué dans l'image ci-dessous.



2. Si la version du connecteur est antérieure à 1.17.0, téléchargez et transférez ou copiez la clé publique sur la machine. Exemple : cisco.gpg Si la version du connecteur est au moins 1.17.0, la clé GPG est disponible dans /opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-KEY-cisco-amp.

Vérification du package DEB

Le paquet DEB est signé à l'aide de l'outil debsigs et peut être vérifié à l'aide de debsig-verify.

1. Installez l'outil debsig-verify.
   ```
   sudo apt-get install debsig-verify
   ```
2. Importez la clé publique GPG Cisco dans la clé debsigs. **Remarque :** à partir de la version

1.17.0, le fichier debsig.gpg sera créé automatiquement afin que l'étape 2 puisse être ignorée.
```
sudo mkdir -p /usr/share/debsig/keyrings/914E5BE0F2FD178F sudo gpg --dearmor --output /usr/share/debsig/keyrings/914E5BE0F2FD178F/debsig.gpg cisco.gpg
```
3. Créer un répertoire de stratégie.
```
sudo mkdir -p /etc/debsig/policies/914E5BE0F2FD178F
```
4. Copiez le contenu de la stratégie ci-dessous dans un nouveau fichier "/etc/debsig/policies/914E5BE0F2FD178F/ciscoampconnector.pol« .

5. Vérifiez la signature DEB avec debsig-verify.
```
debsig-verify amp_ciscoampconnector.deb
```
Le résultat doit être le suivant :
```
debsig: Verified package from 'Cisco AMP for Endpoints' (Debsig)
```

Note: L'étape 5 peut être répétée pour tous les paquets basés sur Debian téléchargés depuis la console AMP for Endpoints.

Installation

Pour installer le connecteur, exécutez la commande suivante où [package deb] est le nom du fichier, par exemple amp_test.deb :

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

IMPORTANT ! Si vous exécutez d'autres produits de sécurité dans votre environnement, il est possible qu'ils détectent le programme d'installation du connecteur comme une menace. Afin d'installer correctement le connecteur, ajoutez Cisco Secure à une liste autorisée ou excluez Cisco Secure dans les autres produits de sécurité et réessayez.

IMPORTANT ! Lors de l'installation du connecteur, un utilisateur et un groupe nommé cisco-amp-scan-svc sont créés sur le système. Si cet utilisateur ou ce groupe existe déjà mais est configuré différemment, le programme d'installation tente de le supprimer, puis de le recréer avec la configuration nécessaire. Le programme d'installation échouera si l'utilisateur et le groupe n'ont pas pu être créés avec la configuration nécessaire.

Désinstallation

Reportez-vous à la section Guide d'utilisation des terminaux sécurisés pour les instructions de désinstallation

Historique des révisions

10 décembre 2020

- Version initiale

12 avril 2022

- Le contenu est applicable à Debian et à Ubuntu.