Cisco Secure Endpoint Linux-connector op debiële systemen

Inhoud

Dit artikel beschrijft de wijzigingen en stappen die beheerders kunnen nemen om de Cisco Secure Endpoint Linux-connector op op Debian-gebaseerde systemen in te zetten:

- Debiër 10 en nieuwer.
- Ubuntu 18.04 en nieuwer.

Minimale OS-vereisten

Raadpleeg het Cisco Secure Endpoint Linux-connector compatibiliteitsartikel voor OS-compatibiliteit.

Instellen omgeving

De Linux-connector op Debian-gebaseerde systemen gebruikt eBPF voor bestands- en netwerkbewaking. De machine moet het juiste linux-headersoftwarepakket hebben geïnstalleerd anders zal de connector fout 11 (ontbrekende systeemafhankelijkheid) verhogen en in een aangetaste toestand draaien zonder bewaking van bestanden en netwerken. Richtlijnen voor het oplossen van deze fout zijn te vinden in het artikel van de Linux Kernel-Devel.

Dependentie

De Linux-connector is afhankelijk van systeempakketten die zijn opgenomen in de basisinstallatie van op Debian gebaseerde systemen, maar als een afhankelijkheid ontbreekt, verschijnt het volgende bericht:

```
ciscoampconnector depends on
```

Gebruik de volgende opdracht om ontbrekende afhankelijkheden te installeren die vereist zijn door de Linux-connector:

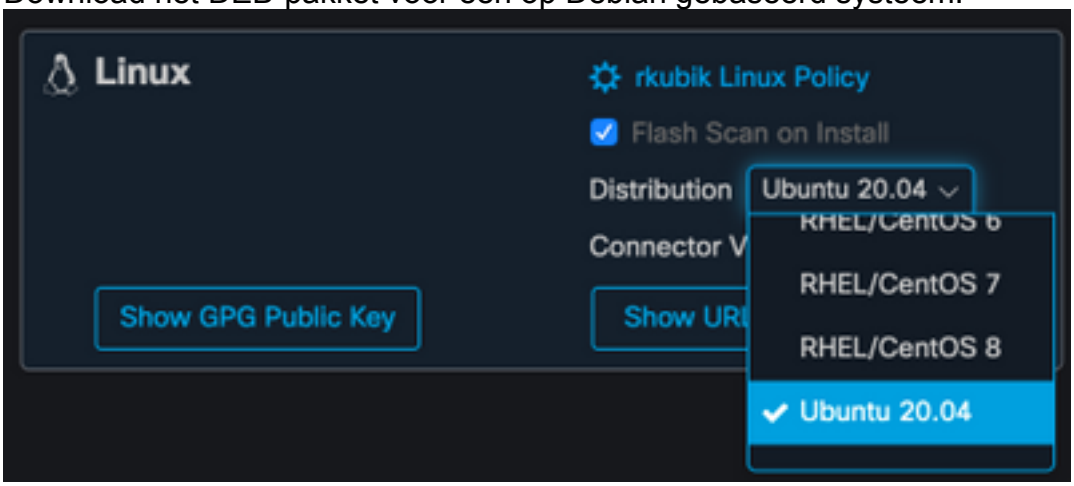
```
sudo apt install
```

Controle van het DEB-pakket

Het Linux-connector DEB-pakket bevat een handtekening om te controleren of het gedownload softwarepakket aan Cisco behoort.

Het DEB-pakket downloaden

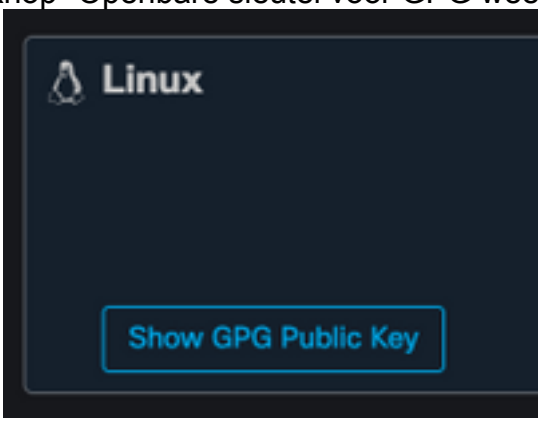
1. Toegang tot de Advanced Malware Protection voor endpoints.
2. Download het DEB-pakket voor een op Debian gebaseerd systeem.



3. Breng het DEB-pakket over op het Debiër-systeem. Bijvoorbeeld: amp_ciscoampconnector.deb.

De GPG openbare sleutel ophalen

1. Klik op de knop "Openbare sleutel voor GPG weergeven" zoals in de onderstaande afbeelding.



2. Als de verbindingsversie eerder dan 1.17.0 is, kunt u de openbare toets naar de machine downloaden en overdragen of kopiëren. Bijvoorbeeld: cisco.gpg. Als de verbindingsversie ten minste 1.17.0 is, is de GPG-toets beschikbaar in het cisco/opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-KEY-cisco-amp.

Controle van het DEB-pakket

Het DEB-pakket is ondertekend met behulp van het debiteurengereedschap en kan worden geverifieerd met behulp van debsig-verify-verificatie.

1. Installeer het gereedschap waarmee u de debiteurencontrole uitvoert.
   ```
   sudo apt-get install debsig-verify
   ```
2. Importeer de openbare sleutel van Cisco GPG in de dieptensleutel. **Opmerking:** Vanaf versie 1.17.0 wordt het debsig.gpg-bestand automatisch gemaakt zodat stap 2 kan worden overgeslagen.
   ```
   sudo mkdir -p /usr/share/debsig/keyrings/914E5BE0F2FD178F sudo gpg --dearmor --output
   /usr/share/debsig/keyrings/914E5BE0F2FD178F/debsig.gpg cisco.gpg
   ```
3. Beleidsmap maken
   ```
   sudo mkdir -p /etc/debsig/policies/914E5BE0F2FD178F
   ```
4. Kopieer de onderstaande beleidsinhoud naar een nieuw bestand "/etc/debsig/policies/914E5BE0F2FD178F/ciscoampconnector.pol".

5. Controleer de DEB-handtekening met debsig-verify.
   ```
   debsig-verify amp_ciscoampconnector.deb
   ```
   De output moet als volgt uitzien:
   ```
   debsig: Verified package from 'Cisco AMP for Endpoints' (Debsig)
   ```

Opmerking: Stap 5 kan worden herhaald voor alle op Debian gebaseerde pakketten die van de AMP voor Endpoints console worden gedownload.

Installatie

Om de connector te installeren voert u de volgende opdracht uit waarbij [deb Package] de naam van het bestand is, bijvoorbeeld amp_test.deb:

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

BELANGRIJK! Als u andere beveiligingsproducten in uw omgeving gebruikt, bestaat de mogelijkheid dat deze de installatieprogramma's van de connector als een bedreiging zullen detecteren. Om de connector met succes te installeren, voegt u Cisco Secure toe aan een toegestane lijst of sluit u Cisco Secure in de andere beveiligingsproducten uit en probeer het nogmaals.

BELANGRIJK! Tijdens de installatie van de connector worden op het systeem gebruikers en groepen met de naam cisco-amp-scan-svc aangemaakt. Als deze gebruiker of groep al bestaat maar anders is geconfigureerd, zal het installatieprogramma proberen deze te verwijderen en dan opnieuw te maken met de gewenste configuratie. Het installatieprogramma faalt als de gebruiker en de groep niet met de benodigde configuratie kunnen worden gemaakt.

Oninstallatie

Raadpleeg het Secure-endpointgebruikershandleidingvoor installatie-instructies

Historie herziening

10 december 2020

- Eerste versie

12 april 2022

- Inhoud is van toepassing op zowel Debian als Ubuntu.