Cisco Secure Endpoint Linux Connector su sistemi basati su Debian

Sommario

In questo articolo vengono descritte le modifiche e le procedure che gli amministratori possono eseguire per distribuire il connettore Cisco Secure Endpoint Linux sui sistemi basati su Debian:

- Debian 10 e più recente.
- Ubuntu 18.04 e versioni successive.

Requisiti minimi del sistema operativo

Per informazioni sulla compatibilità del sistema operativo, consultare l'articolo sulla compatibilità del sistema operativo del connettore Linux di Cisco Secure Endpoint.

Impostazione ambiente

Il connettore Linux sui sistemi basati su Debian utilizza eBPF per il monitoraggio di file e rete. Nel computer deve essere installato il pacchetto software linux-headers corretto. In caso contrario, il connettore genererà l'errore 11 (Dipendenza sistema mancante) e verrà eseguito in uno stato degradato senza monitoraggio di file e rete. Per ulteriori informazioni sulla risoluzione di questo errore, consultare l'articolo Errore dello sviluppatore del kernel Linux.

Dipendenze

Il connettore Linux dipende dai pacchetti di sistema che sono inclusi nell'installazione di base dei sistemi basati su Debian, ma se una dipendenza è mancante verrà visualizzato il seguente messaggio:

```
ciscoampconnector depends on
```

Utilizzare il comando seguente per installare le dipendenze mancanti richieste dal connettore Linux:

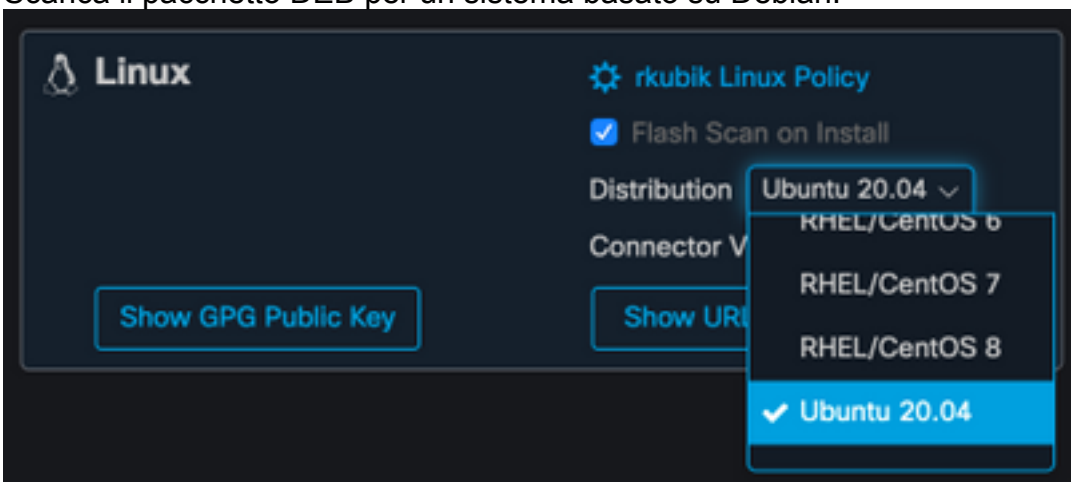
```
sudo apt install
```

Verifica del pacchetto DEB

Il pacchetto DEB del connettore Linux contiene una firma per verificare che il pacchetto software scaricato appartenga a Cisco.

Download del pacchetto DEB

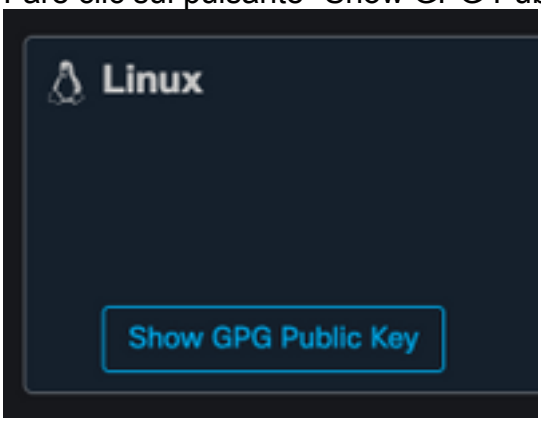
1. Accedere alla console AMP for Endpoints.
2. Scarica il pacchetto DEB per un sistema basato su Debian.



3. Trasferite il pacchetto DEB sul sistema basato su Debian. Ad esempio: amp_ciscoampconnector.deb.

Recupero della chiave pubblica GPG

1. Fare clic sul pulsante "Show GPG Public Key", come mostrato nell'immagine seguente.



2. Se la versione del connettore è precedente alla 1.17.0, scaricare e trasferire o copiare la chiave pubblica nel computer. Ad esempio: cisco.gpg. Se la versione del connettore è almeno 1.17.0, il tasto GPG è disponibile in /opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-KEY-cisco-amp.

Verifica del pacchetto DEB

Il pacchetto DEB viene firmato utilizzando lo strumento Debsigs e può essere verificato utilizzando debsig-verify.

1. Installare lo strumento debsig-verify.
   `sudo apt-get install debsig-verify`
2. Importare la chiave pubblica GPG di Cisco nella sequenza di chiavi di debug. **Nota:** a partire dalla versione 1.17.0, il file debsig.gpg verrà creato automaticamente e il passaggio 2 potrà essere ignorato.
   `sudo mkdir -p /usr/share/debsig/keyrings/914E5BE0F2FD178F sudo gpg --dearmor --output /usr/share/debsig/keyrings/914E5BE0F2FD178F/debsig.gpg cisco.gpg`
3. Creare la directory dei criteri.
   `sudo mkdir -p /etc/debsig/policies/914E5BE0F2FD178F`
4. Copiare il contenuto del criterio seguente in un nuovo file "/etc/debsig/policies/914E5BE0F2FD178F/ciscoampconnector.pol".

5. Verificare la firma DEB con debsig-verify.
   `debsig-verify amp_ciscoampconnector.deb`
   L'output dovrebbe essere il seguente:
   `debsig: Verified package from 'Cisco AMP for Endpoints' (Debsig)`

Nota: Il passo 5 può essere ripetuto per qualsiasi pacchetto basato su Debian scaricato dalla console AMP for Endpoints.

Installazione

Per installare il connettore, eseguire il seguente comando dove [deb package] è il nome del file, ad esempio amp_test.deb:

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

IMPORTANTE! Se nell'ambiente sono in esecuzione altri prodotti di sicurezza, è possibile che il programma di installazione del connettore venga rilevato come minaccia. Per installare correttamente il connettore, aggiungere Cisco Secure a un elenco di dispositivi consentiti o escludere Cisco Secure negli altri prodotti di sicurezza, quindi riprovare.

IMPORTANTE! Durante l'installazione del connettore, vengono creati sul sistema un utente e un gruppo denominati cisco-amp-scan-svc. Se l'utente o il gruppo esiste già ma è configurato in modo diverso, il programma di installazione tenterà di eliminarlo e quindi di ricrearlo con la configurazione necessaria. Se non è possibile creare l'utente e il gruppo con la configurazione necessaria, il programma di installazione non riuscirà.

Disinstallazione

Consultare la Guida per l'utente di Secure Endpointper istruzioni sulla disinstallazione

Cronologia delle revisioni

10 dicembre 2020

- Versione iniziale

12 aprile 2022

- Il contenuto è applicabile sia a Debian che a Ubuntu.