Conector de Cisco Secure Endpoint Linux en sistemas basados en Debian

Contenido

Este artículo describe los cambios y pasos que los administradores pueden realizar para implementar el conector de Cisco Secure Endpoint Linux en sistemas basados en Debian:

- Debian 10 y posterior.
- Ubuntu 18.04 y posterior.

Requisitos mínimos del SO

Consulte el artículo Compatibilidad del SO de Cisco Secure Endpoint Linux Connector para la Compatibilidad del SO.

Configuración del entorno

El conector Linux en sistemas basados en Debian utiliza eBPF para monitorear archivos y redes. La máquina debe tener instalado el paquete de software linux-header correcto, de lo contrario el conector generará la falla 11 (Falta la dependencia del sistema) y se ejecutará en un estado degradado sin supervisión de archivos y red. Se puede encontrar la guía para resolver este error en el artículo Linux Kernel-Devel Fault.

Dependencias

El conector Linux depende de los paquetes del sistema que se incluyen en la instalación básica de sistemas basados en Debian, pero si falta una dependencia, aparecerá el siguiente mensaje:

```
ciscoampconnector depends on
```

Utilice el siguiente comando para instalar cualquier dependencia que falte y que requiera el conector Linux:

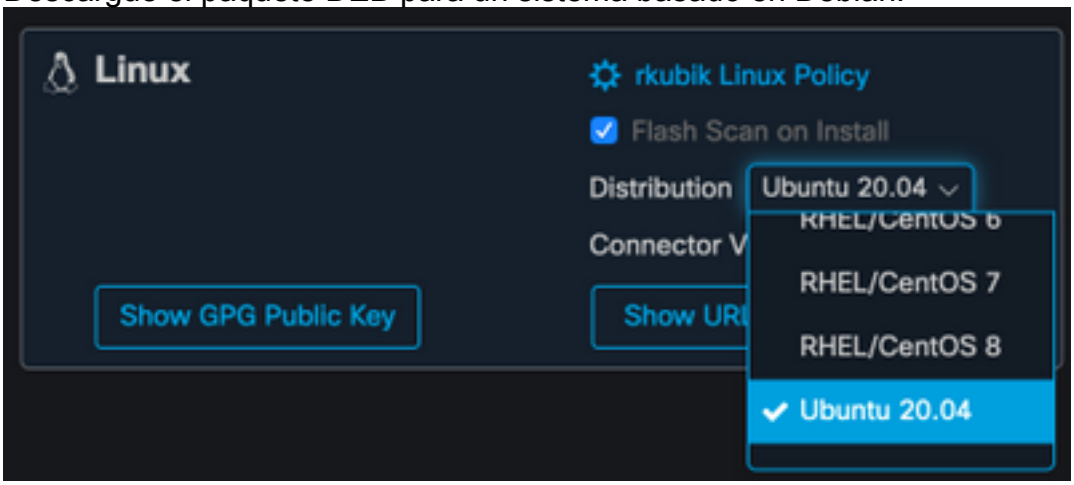
```
sudo apt install
```

Verificación del paquete DEB

El paquete DEB del conector Linux contiene una firma para verificar que el paquete de software descargado pertenece a Cisco.

Descarga del paquete DEB

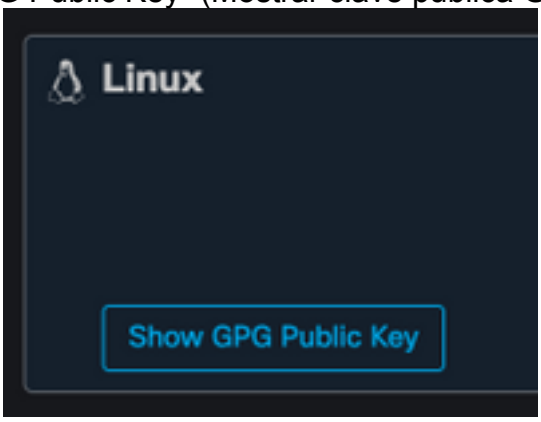
1. Acceda a la consola de AMP para terminales.
2. Descargue el paquete DEB para un sistema basado en Debian.



3. Transfiera el paquete DEB al sistema basado en Debian. Por ejemplo: amp_ciscoampconnector.deb

Recuperación de la Clave Pública GPG

1. Haga clic en el botón "Show GPG Public Key" (Mostrar clave pública GPG), como se muestra en la siguiente imagen.



2. Si la versión del conector es anterior a 1.17.0, descargue y transfiera o copie la clave pública en la máquina. Por ejemplo: cisco.gpg. Si la versión del conector es al menos 1.17.0, la clave GPG está disponible en /opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-KEY-cisco-amp.

Verificación del paquete DEB

El paquete DEB se firma con la herramienta de registros y se puede verificar con descifrar-verificar.

1. Instale la herramienta de verificación de errores.
```
sudo apt-get install debsig-verify
```

2. Importe la clave pública GPG de Cisco en la llanura de claves de los registros. **Nota:** A partir de la versión 1.17.0, el archivo debsig.gpg se creará automáticamente para que se pueda saltar el paso 2.
   ```
   sudo mkdir -p /usr/share/debsig/keyrings/914E5BE0F2FD178F sudo gpg --dearmor --output /usr/share/debsig/keyrings/914E5BE0F2FD178F/debsig.gpg cisco.gpg
   ```
3. Crear directorio de políticas.
   ```
   sudo mkdir -p /etc/debsig/policies/914E5BE0F2FD178F
   ```
4. Copie el contenido de la política siguiente en un nuevo archivo "/etc/debsig/policies/914E5BE0F2FD178F/ciscoampconnector.pol".

5. Verifique la firma DEB con debug-verify.
   ```
   debsig-verify amp_ciscoampconnector.deb
   ```
   El resultado debe verse de la siguiente manera:
   ```
   debsig: Verified package from 'Cisco AMP for Endpoints' (Debsig)
   ```

Nota: El paso 5 se puede repetir para cualquier paquete basado en Debian descargado desde la consola de AMP para terminales.

Instalación

Para instalar el conector, ejecute el siguiente comando donde [deb package] es el nombre del archivo, por ejemplo amp_test.deb:

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

¡IMPORTANTE! Si ejecuta otros productos de seguridad en su entorno, existe la posibilidad de que detecten el instalador del conector como una amenaza. Para instalar correctamente el conector, agregue Cisco Secure a una lista permitida o excluya Cisco Secure en los demás productos de seguridad e inténtelo de nuevo.

¡IMPORTANTE! Durante la instalación del conector, se crea en el sistema un usuario y un grupo denominado cisco-amp-scan-svc. Si este usuario o grupo ya existe pero está configurado de forma diferente, el instalador intentará eliminarlos y, a continuación, volver a crearlos con la configuración necesaria. El instalador fallará si el usuario y el grupo no se han podido crear con la configuración necesaria.

Desinstalación

Consulte la Guía del usuario de terminales segurospara obtener instrucciones de desinstalación

Historial de revisión

10 de diciembre de 2020

- Versión inicial

12 de abril de 2022

- El contenido es aplicable tanto a Debian como a Ubuntu.