Implementación de Cisco Secure Endpoint Linux Connector

Contenido

Introducción

En este artículo se describen los pasos que los administradores pueden seguir para implementar el conector de Cisco Secure Endpoint Linux en sistemas basados en RPM y en Debian.

Requirements

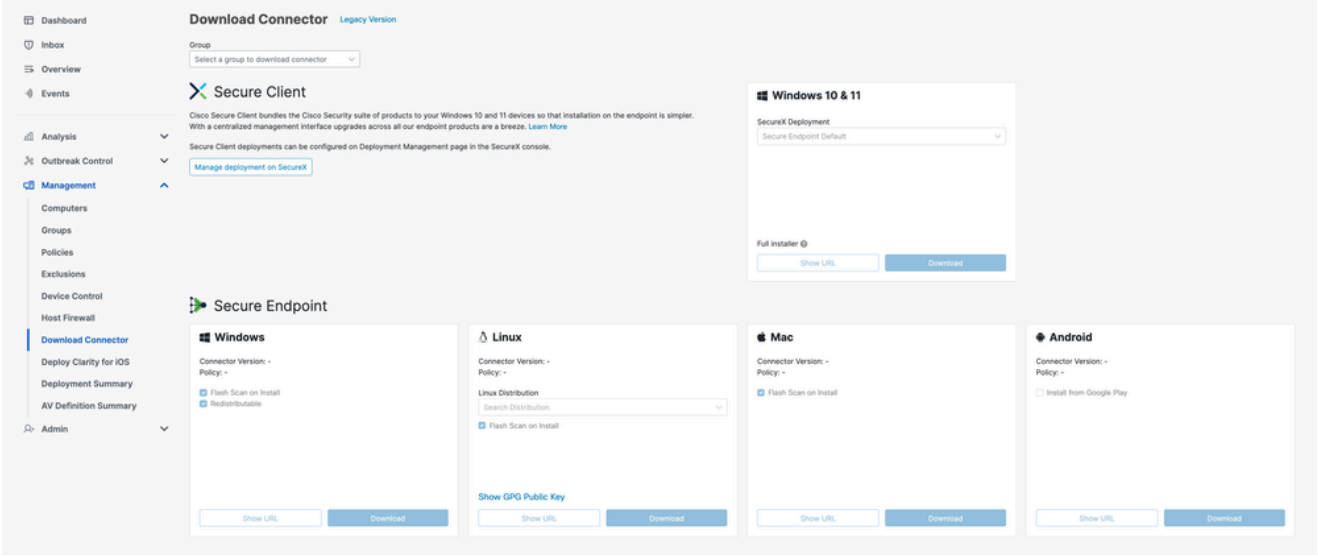
Consulte el artículo de compatibilidad del sistema operativo del conector de Linux de Cisco Secure Endpoint para obtener información sobre la compatibilidad del sistema operativo.

Consulte la Guía del Usuario de Secure Endpoint para conocer los requisitos recomendados del sistema Linux.

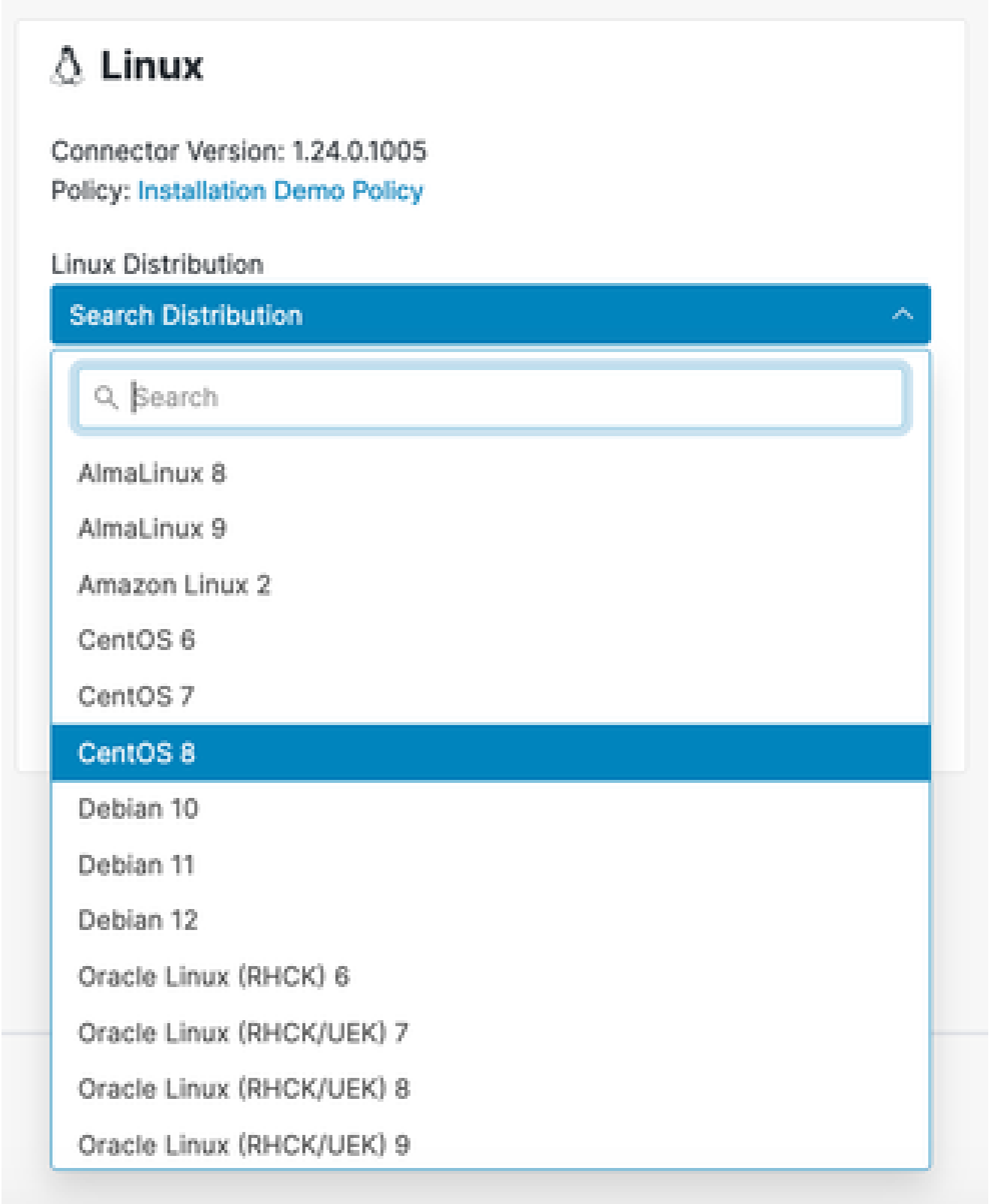
Implementación del conector de Linux

Descargar el paquete del conector de Linux

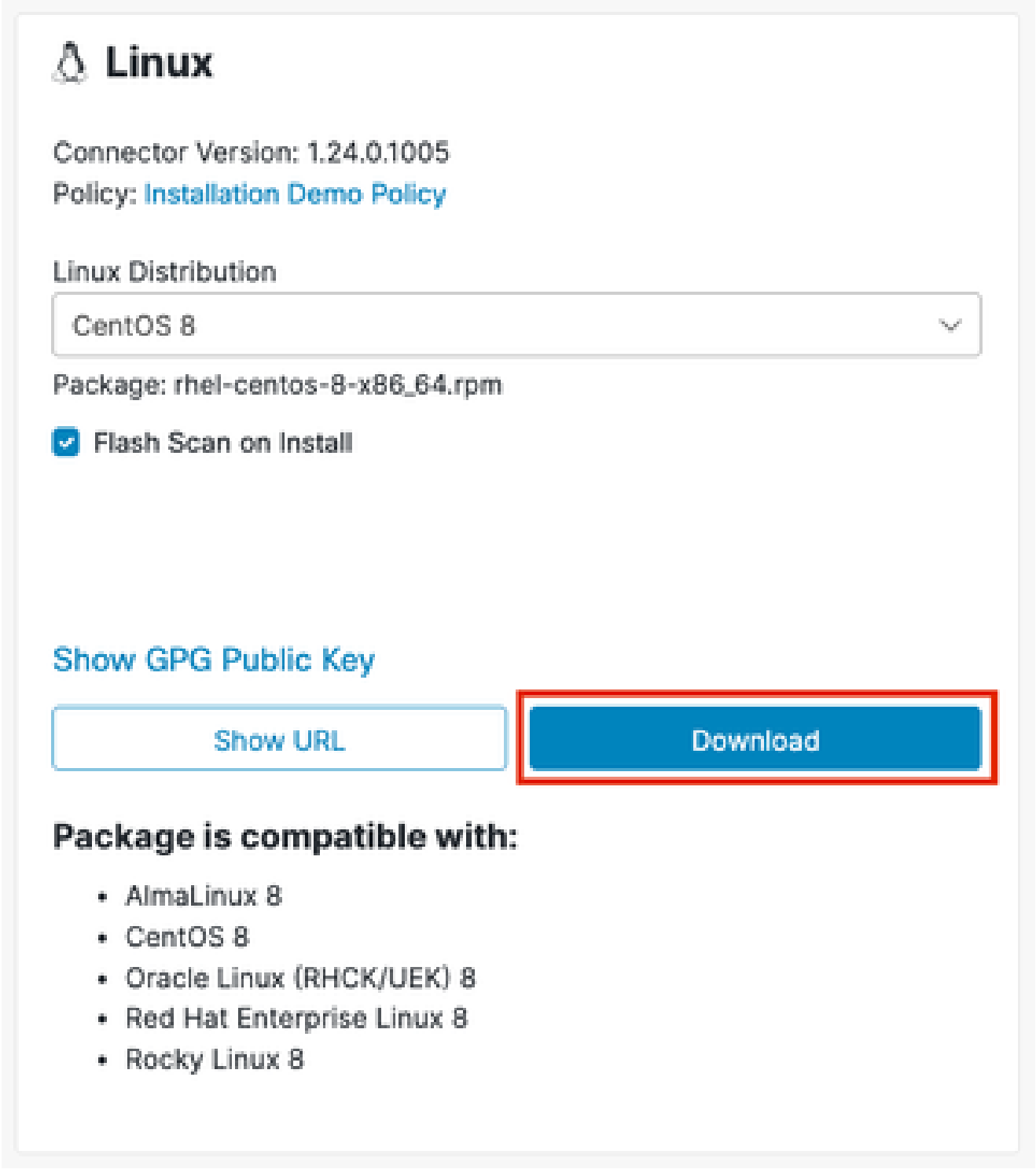
1. En Secure Endpoint Console, desplácese a la página `Download Connector`.



2. Seleccione el paquete de conectores de Linux adecuado mediante el menú desplegable "Linux Distribution" (Distribución de Linux) para elegir una distribución.



3. Haga clic en el botón `Download` para comenzar a descargar el paquete seleccionado.



4. Transfiera el paquete descargado al terminal.

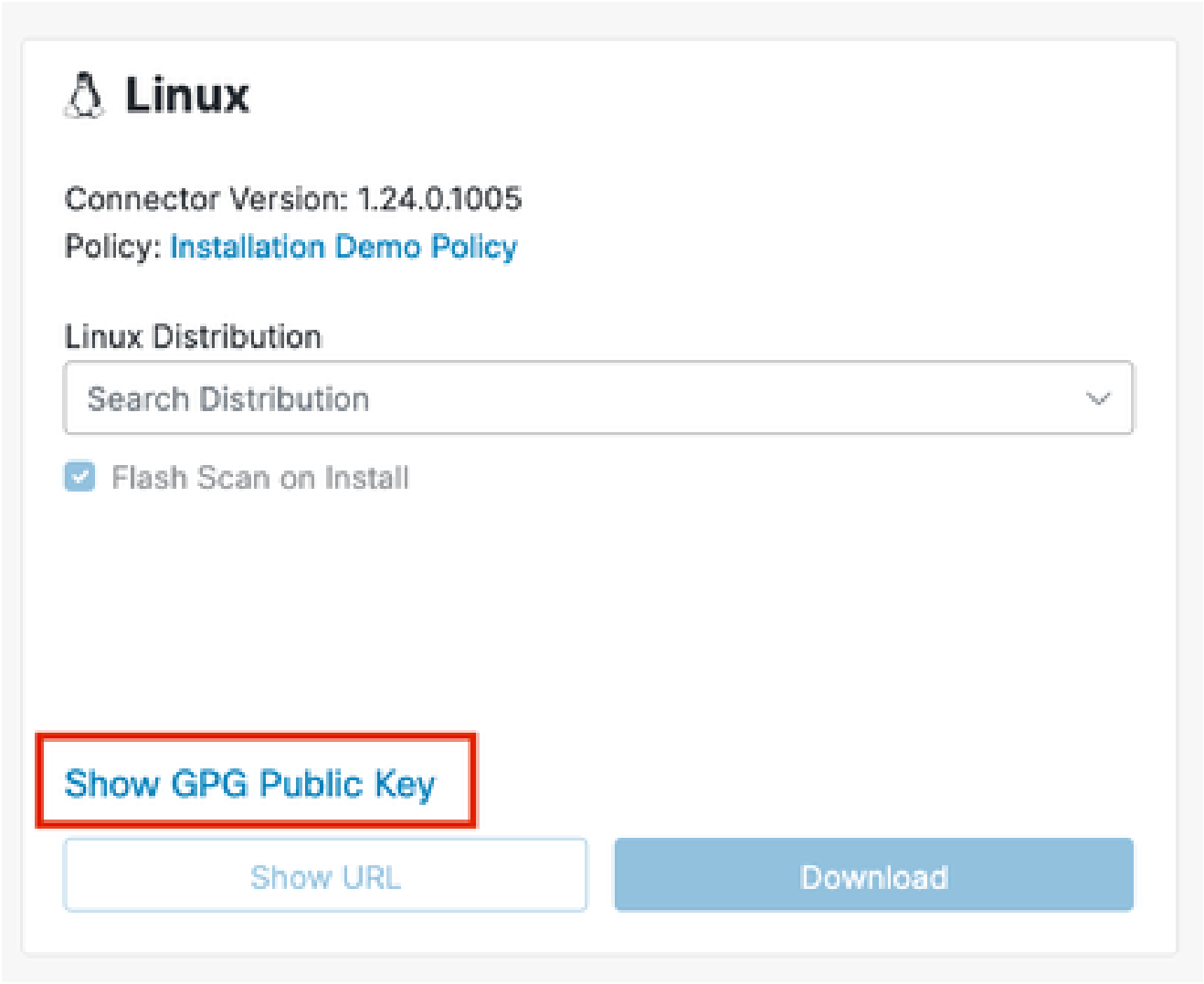
Verificar el paquete del conector de Linux

El conector Linux se puede instalar sin la clave pública GPG de Cisco. Sin embargo, si planea enviar las actualizaciones del conector a través de la política, deberá instalar la clave pública en el terminal. Para distribuciones basadas en RPM, importe la clave en la base de datos RPM. Para distribuciones basadas en Debian, importe la clave en el anillo de claves de depuración.

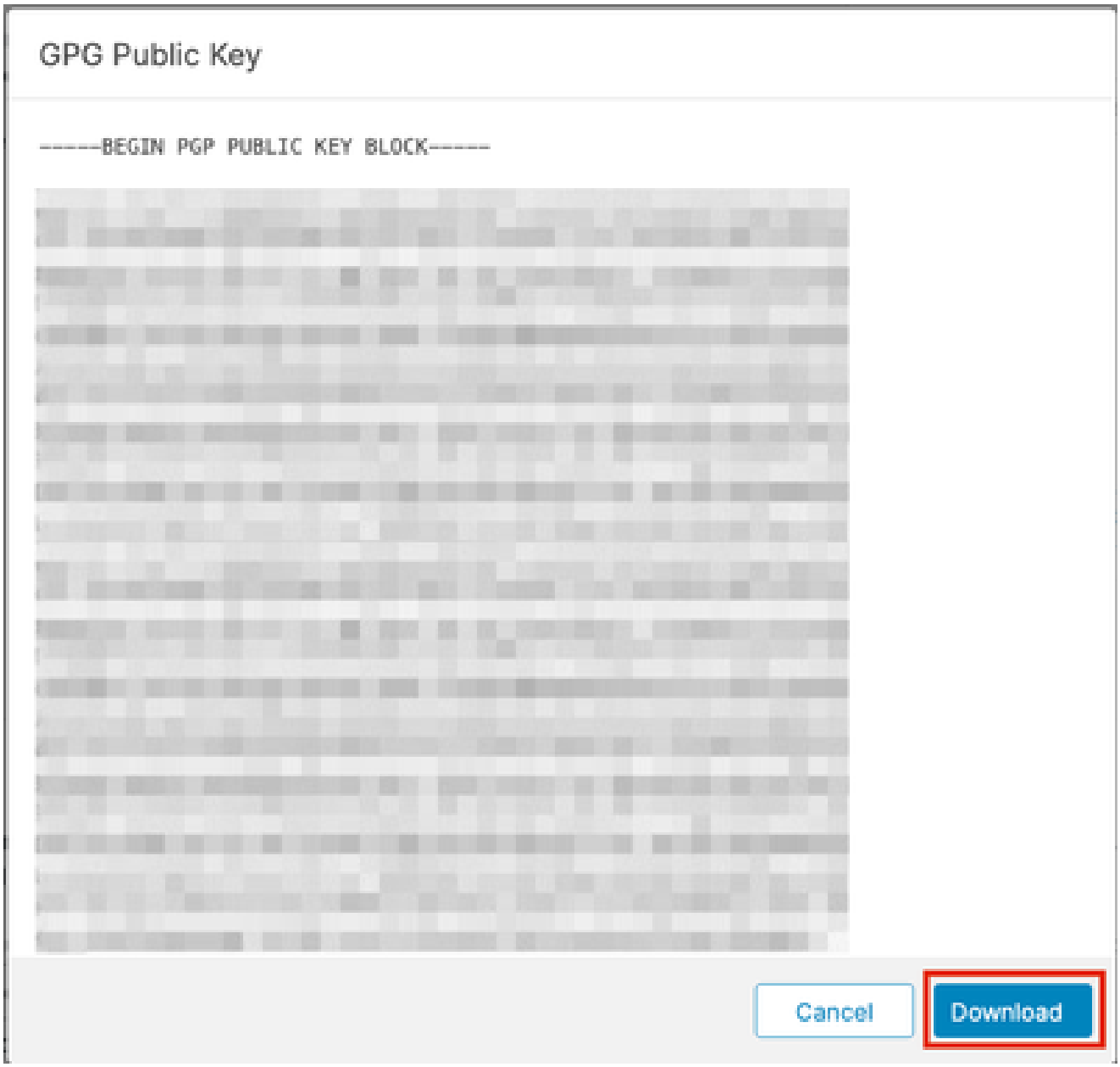
Esta sección describe cómo importar la clave pública GPG de Cisco en su sistema y cómo verificar el paquete de conector descargado usando la clave importada.

Recuperar la clave pública GPG de Cisco

1. En la página Secure Endpoint Console `Download Connector`, seleccione el enlace `Show GPG Public Key` de la sección Linux.



2. La clave pública GPG de Cisco aparecerá en una ventana emergente. Seleccione `Descargar` en esta ventana emergente para descargar la clave en su sistema. La clave aparecerá como `cisco.gpg` en la carpeta Downloads (Descargas).



3. Transfiera la clave descargada al terminal.

basado en RPM

El paquete RPM está firmado y se puede verificar mediante el administrador de paquetes RPM.

1. Importe la clave pública GPG de Cisco en la base de datos RPM.

   ```
   sudo rpm --import cisco.gpg
   ```

2. Verifique que se haya instalado la clave pública GPG de Cisco.

   ```
   rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n'
   ```

   Debería ver la siguiente clave pública en la lista:

   ```
   gpg-pubkey-34532611-6477a906 --> Cisco, Inc. <support@cisco.com> public key
   ```

3. Verifique el paquete del conector Linux usando RPM. Ejemplo:

```
rpm -K amp_Installation_Demo_rhel-centos-8-x86_64.rpm
```

Se debe mostrar el siguiente resultado:

```
amp_Installation_Demo_rhel-centos-8-x86_64.rpm: digests signatures OK
```

basado en Debian

El paquete Debian se firma usando la herramienta de verificación de firmas de paquetes Debian (debsig) y se puede verificar usando debsig-verify.

1. Instale la herramienta `de verificación de` desbaste.

```
sudo apt-get install debsig-verify
```

2. Importe la clave pública GPG de Cisco en el anillo de claves de depuración. Nota: A partir de la versión 1.17.0, el archivo debsig.gpg se creará automáticamente para que se pueda omitir 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. Cree el directorio de políticas.

```
sudo mkdir -p /etc/debsig/policies/914E5BE0F2FD178F
```

4. Copie el contenido de la directiva siguiente en un nuevo archivo "/etc/debsig/policies/914E5BE0F2FD178F/ciscoampconnector.pol".

```
<?xml version="1.0"?>
<!DOCTYPE Policy SYSTEM "https://www.debian.org/debsig/1.0/policy.dtd">
<Policy xmlns="https://www.debian.org/debsig/1.0/">
 <Origin Name="Debsig" id="914E5BE0F2FD178F" Description="Cisco AMP for Endpoints"/>
 <Selection>
     <Required Type="origin" File="debsig.gpg" id="914E5BE0F2FD178F"/>
 </Selection>
 <Verification MinOptional="0">
     <Required Type="origin" File="debsig.gpg" id="914E5BE0F2FD178F"/>
 </Verification>
</Policy>
```

5. Verifique la firma con `debsig-verify`. Ejemplo:

```
debsig-verify ubuntu-20-04-amd64.deb
```

Se debe mostrar el siguiente resultado:

```
debsig: Verified package from 'Cisco AMP for Endpoints' (Debsig)
```

Instalación del paquete del conector de Linux

Instalación de los encabezados del núcleo

La mayoría de las distribuciones Linux modernas utilizan versiones del núcleo que soportan eBPF, que el conector utiliza para monitorear el sistema. Para determinar la versión del núcleo de su punto final, ejecute el siguiente comando:

```
uname -r
```

Si su versión de distribución coincide con alguna de las siguientes, el conector utilizará eBPF para la supervisión del sistema:

- Distribuciones basadas en RPM con una versión de kernel de 3.10.0-940 o posterior (EL7 / Enterprise Linux 7.9 es la distribución más antigua con esta versión de kernel).
- Distribuciones basadas en Debian con una versión del núcleo de 4.18 o posterior.

Puede encontrar más detalles sobre el mapeo entre la distribución y la versión del núcleo aquí.

Si eBPF está soportado en su terminal, entonces los encabezados correctos del núcleo deben estar instalados para que el conector monitoree el sistema. Si su terminal no tiene instalados los encabezados correctos del núcleo, el conector generará la falla 11 (Falta la dependencia del sistema) y se ejecutará en un estado degradado sin supervisión de archivos, procesos o redes.

Refiérase al artículo Linux Kernel-Devel Fault para obtener orientación sobre cómo instalar los encabezados correctos del núcleo.

Instale el conector

¡IMPORTANTE! Si está ejecutando 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 de permitidos o excluya Cisco Secure de los otros 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 eliminarlo y, a continuación, volver a crearlo con la configuración necesaria. El instalador fallará si el usuario y el grupo no se pudieron crear con la configuración necesaria.

basado en RPM

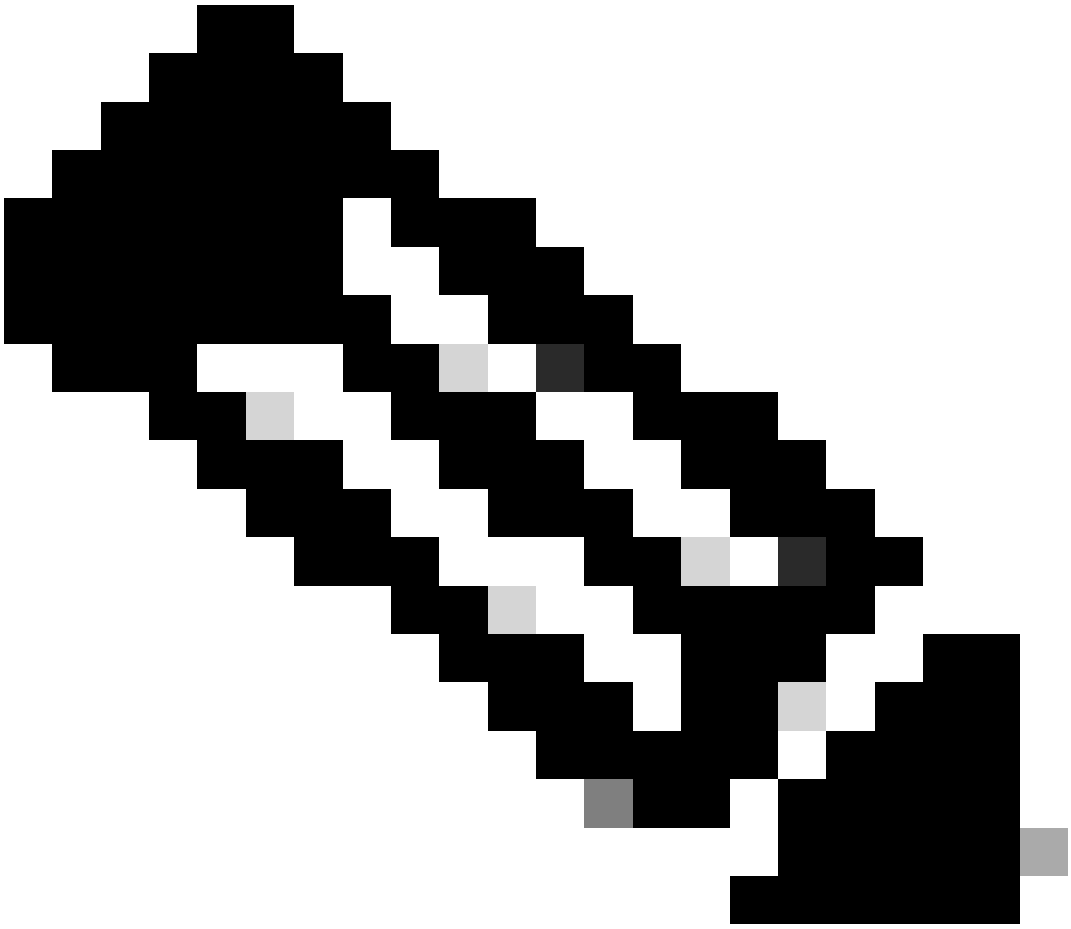
Para instalar el conector, ejecute uno de los siguientes comandos donde [rpm package] es el nombre del archivo, por ejemplo `amp_Installation_Demo_rhel-centos-8-x86_64.rpm`:

- Vía YUM:

  ```
  sudo yum localinstall -y [rpm package]
  ```

- Vía Zypper:

  ```
  sudo zypper install -y [rpm package]
  ```



Nota: La instalación a través de yum o zypper se encargará de la instalación de cualquier dependencia necesaria.

---

basado en Debian

Para instalar el conector, ejecute el siguiente comando donde [deb package] es el nombre del archivo, por ejemplo `amp_Installation_Demo_ubuntu-20-04-amd64.deb`:

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

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

```
 ciscoampconnector depends on <package_name>; however:
  Package <package_name> is not installed.
```

Donde `<package_name>` es el nombre de la dependencia que falta. Utilice el siguiente comando para instalar cualquier dependencia que falte requerida por el conector Linux:

```
sudo apt install <package_name>
```

Puede volver a intentar instalar el conector una vez que se hayan instalado todas las dependencias que faltan.

Comparar clave pública GPG de Cisco

Si la versión del conector de Linux es al menos 1.17.0, la clave pública GPG de Cisco utilizada para verificar los paquetes de actualización durante las actualizaciones del conector se instala automáticamente en las siguientes ubicaciones:

- Basado en RPM: `/opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp`
- Basado en Debian: `/opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-KEY-cisco-amp`

Compare la clave instalada por el conector con la recuperada de Secure Endpoint Console.

Verificar instalación

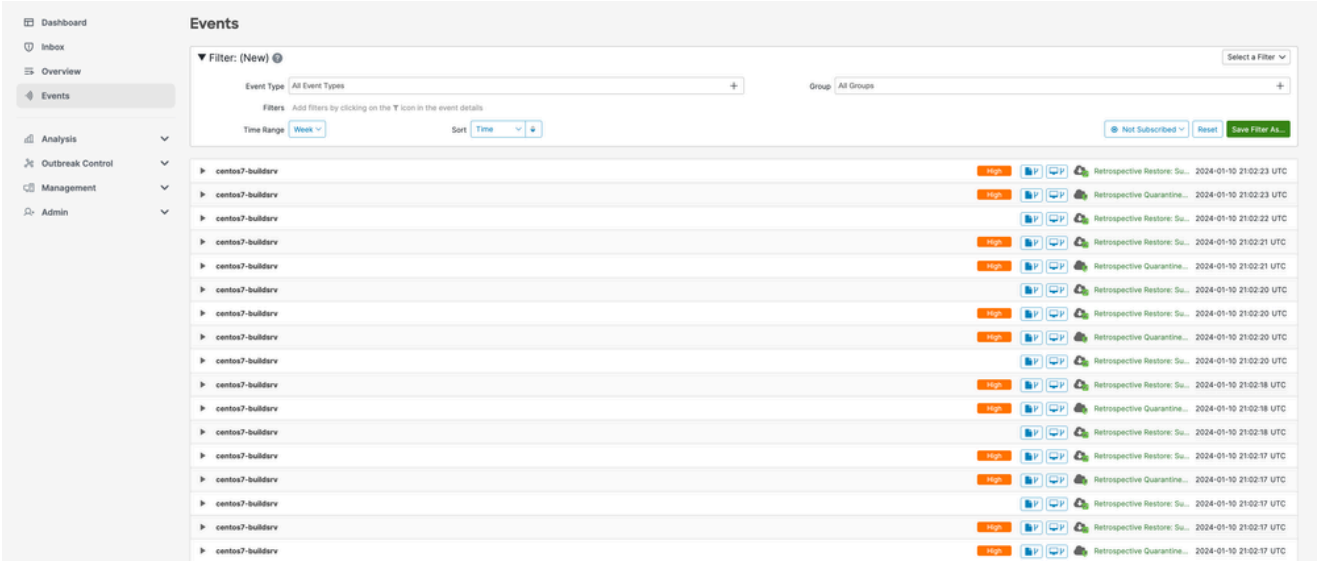
La interfaz de línea de comandos del conector Linux se puede utilizar para verificar la correcta instalación en el conector Linux. Estado de ejecución `/opt/cisco/amp/bin/ampcli`. Si el conector se instaló correctamente, debería ver que está `conectado` y que no tiene fallas al ejecutar el comando `/opt/cisco/amp/bin/ampcli/ampcli/ampcli status`:

```
$ /opt/cisco/amp/bin/ampcli status
Trying to connect...
```

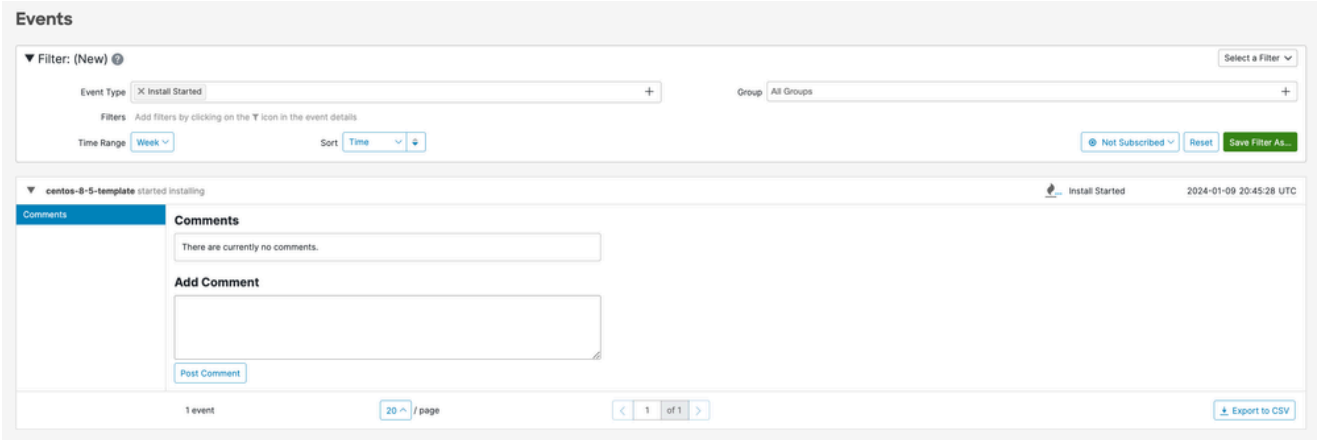
```
Connected.
Status:                    Connected
Mode:                     Normal
Scan:                     Ready for scan
Last Scan:                 2024-01-09 01:45:49 PM
Policy:                    Installation Demo Policy (#9606)
Command-line:             Enabled
Orbital:                  Enabled (Running)
Behavioural Protection: Protect
Faults:                    None
```

Para verificar que el conector está conectado, puede confirmar la existencia del evento de instalación en Secure Endpoint Console:

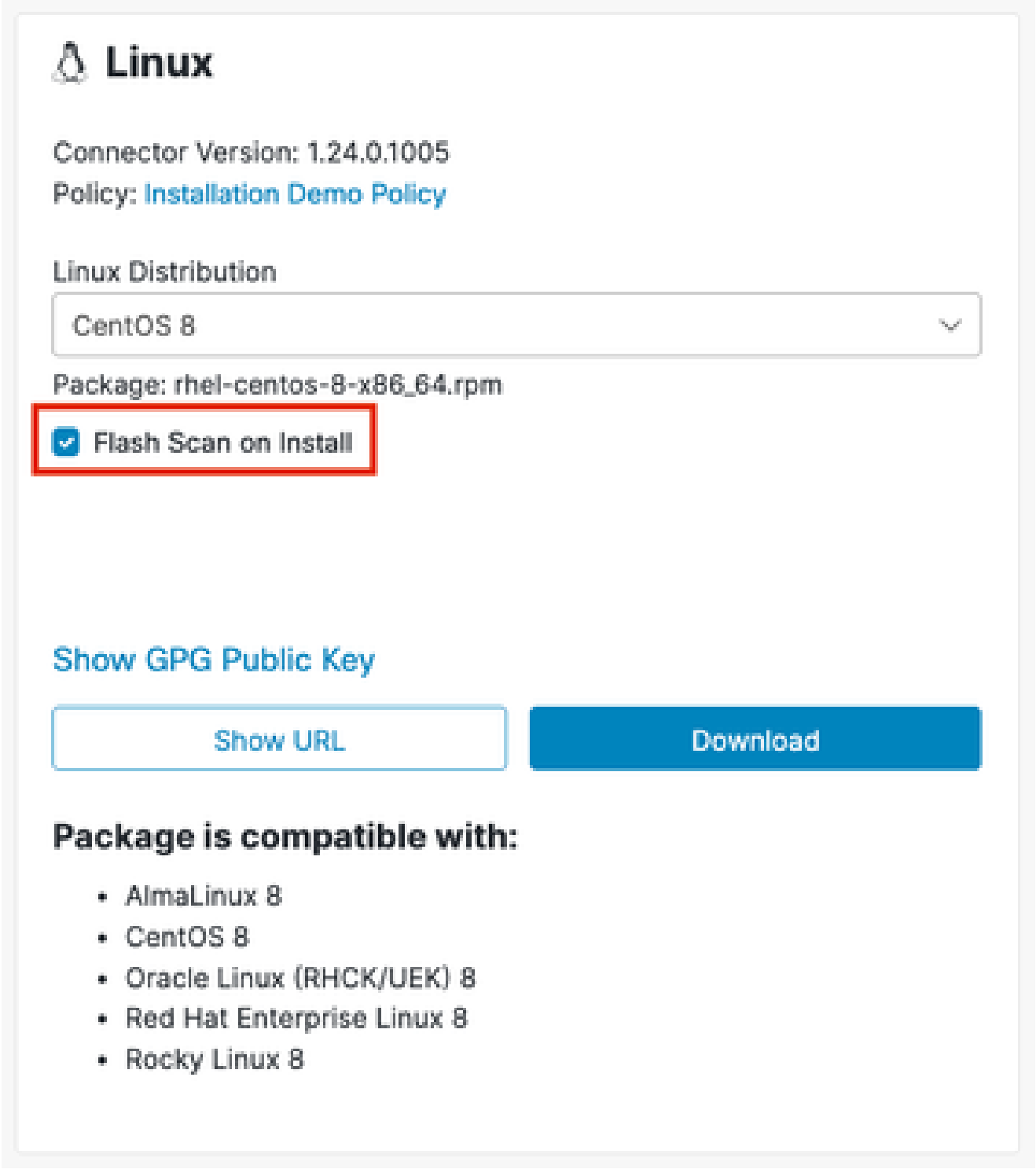
1. Vaya a la página `Eventos`.



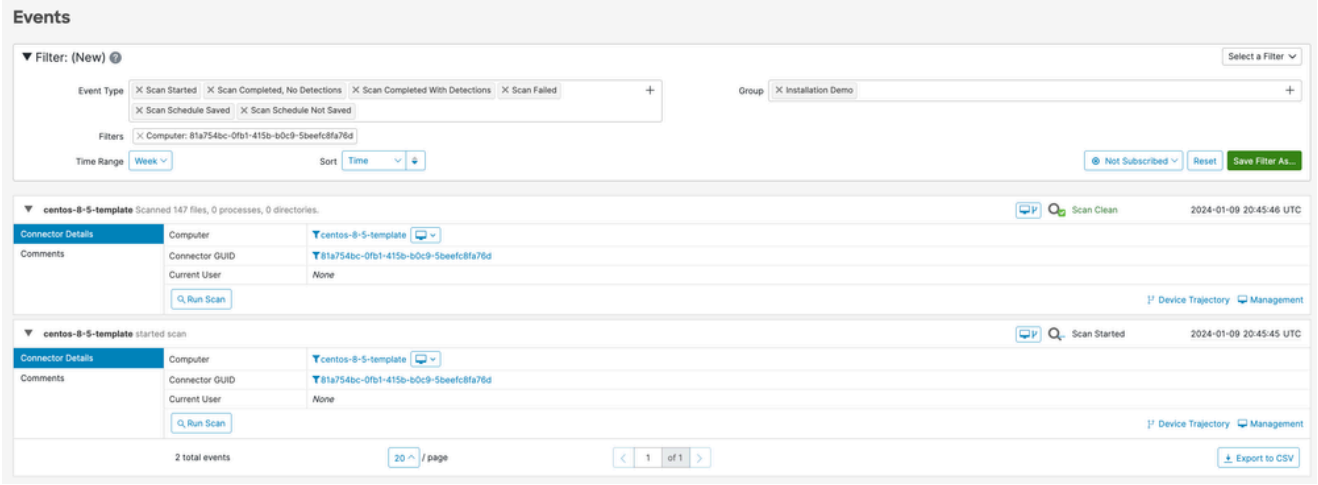
2. Busque el evento de instalación del conector. Debe clasificarse en el tipo de evento `Install Started`.



3. Si seleccionó la casilla de verificación `Flash Scan on Install` al descargar el conector, también puede confirmar que existen dos eventos de análisis.



4. Localice los eventos de análisis para su conector filtrándolos por los tipos de eventos `Scan`. Nota: también puede restringir la búsqueda agregando filtros para el GUID de grupo y conector. Debería ver dos eventos correspondientes al inicio y al final del análisis.



Desinstalación del conector de Linux

basado en RPM

1. Desinstale el conector Linux mediante el administrador de paquetes de sistemas.
   - Vía YUM:

     ```
     sudo yum remove ciscoampconnector -y
     ```

   - Vía Zypper:

     ```
     sudo zypper remove -y ciscoampconnector
     ```

2. Purgue el conector de Linux ejecutando el script de purga proporcionado.

   ```
   /opt/cisco/amp/bin/purge_amp_local_data
   ```

basado en Debian

1. Desinstale el conector Linux mediante el administrador de paquetes de sistemas.

   ```
   sudo dpkg --remove cisco-orbital ciscoampconnector
   ```

2. Purgue el conector de Linux ejecutando el script de purga proporcionado.

   ```
   sudo dpkg --purge cisco-orbital ciscoampconnector
   ```

Consulte la Guía del usuario de Secure Endpoint para obtener instrucciones más detalladas sobre la desinstalación.

Vea también

- Instalación de Cisco Secure Endpoint Connector en vídeo RHEL
- Falla de Linux Kernel-Devel
  - Resolver vídeo de falla de desarrollo de núcleo de Linux de Cisco Secure Endpoint
- Guía del usuario de terminales seguros
- Soporte Técnico y Documentación - Cisco Systems
- Solución de problemas de Secure Endpoint Linux Faults
- Verifique la compatibilidad del sistema operativo del conector de Linux de terminal seguro

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).