

Installation des Cisco Secure Endpoint Linux Connectors

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[RHEL/CentOS/Amazon Linux 2/SUSE 15](#)

[Konfigurationen](#)

[Importieren des GPG-Schlüssels](#)

[Ubuntu](#)

[Konfigurationen](#)

[Importieren des GPG-Schlüssels](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt, wie der Cisco Secure Endpoint Linux Connector für Red Hat Enterprise Linux (RHEL) und Debian-basierte Systeme installiert und verifiziert wird.

Verfasst von Juan Carlos Castellero und herausgegeben von Yeraldin Sanchez, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Linux-Computer auf einem Linux-Anschluss unterstützen Betriebssystem (OS)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Ein Secure Endpoint Linux Connector Installer Red Hat Package Manager (RPM)
- Ein Secure Endpoint Linux Connector Installer Debian Package Manager (dpkg)
- Ein GNU Privacy Guard (GPG)-Schlüssel zum Überprüfen von Updates (optional)

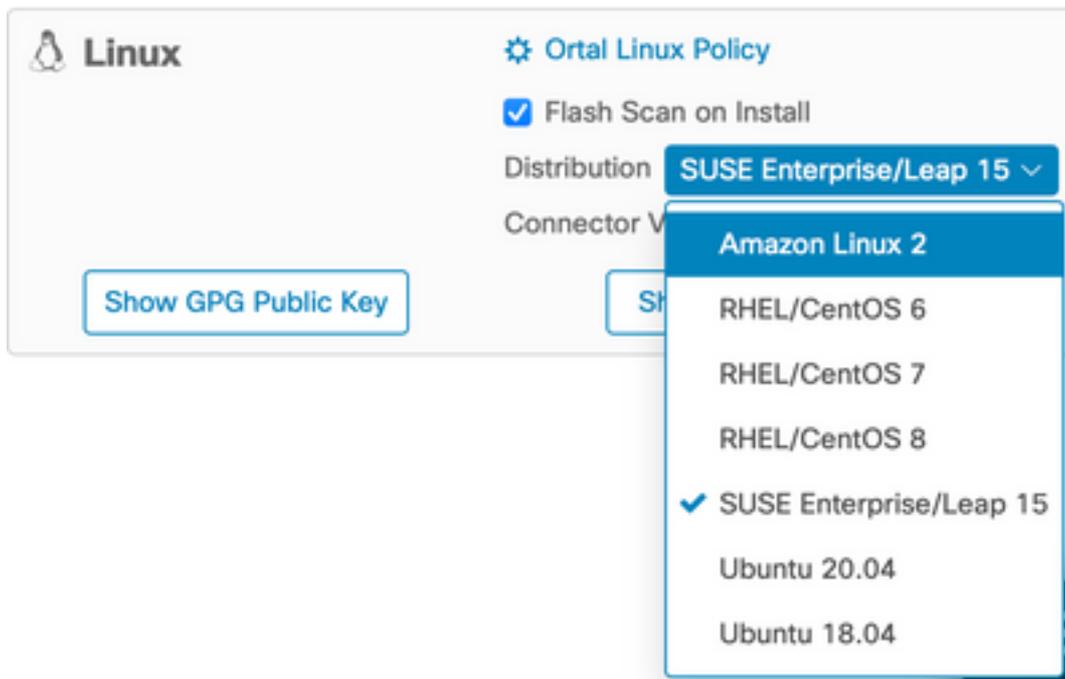
- Ein Linux Connector Installer DPKG (Debian Package Management System)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

RHEL/CentOS/Amazon Linux 2/SUSE 15

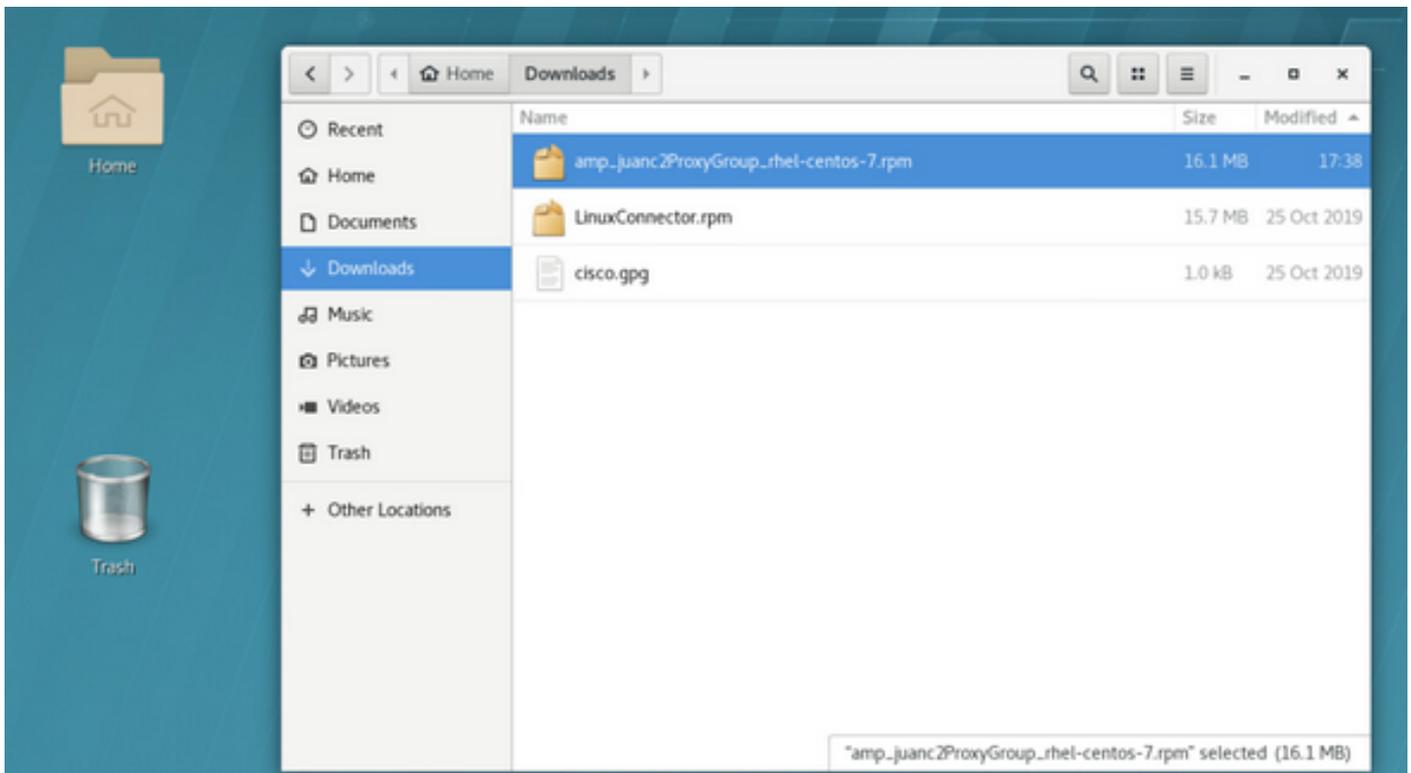
Konfigurationen

Schritt 1: Laden Sie das Linux RPM-Paket vom Cisco Secure Endpoint Portal herunter, wie im Bild gezeigt.



Anmerkung: Beachten Sie, dass die Verteilung des Betriebssystems wichtig ist, da beide Connectors äußerst unterschiedliche Architekturen haben.

Schritt 2: Verschieben Sie das RPM-Paket an den betreffenden Endpunkt, indem Sie es entweder direkt vom Dashboard herunterladen oder manuell auf die Endpunkte verschieben. In diesem Beispiel wird eine grafische Benutzeroberfläche (Graphic User Interface, UI) verwendet, obwohl es möglich und häufig üblich ist, mit einer Minimalinstallation zu arbeiten. In diesem Fall muss man wissen, wie man das Linux-Terminal handhabt und das RPM-Paket findet.



Schritt 3: Um den Linux-Anschluss zu installieren, führen Sie den folgenden Befehl aus: **sudo yum localinstall [rpm-Paket] -y** (oder **sudo zypper install -y [rpm-Paket]** auf SUSE 15)

wobei [rpm-Paket] der Name der Datei ist, zum Beispiel "amp_Audit.rpm". Das RPM-Paket muss installiert werden, während der ATD-Dienst ausgeführt wird.

```

File Edit View Search Terminal Help
[jenator@jenatorr-lin-aws-lab Downloads] sudo yum localinstall amp_juanc2ProxyGroup_rhel-centos-7.rpm -y
[sudo] password for jenator:
Loaded plugins: langpacks, product-id, search-disabled-repos, subscription-manager
This system is not registered with an entitlement server. You can use subscription-manager to register.
Examining amp_juanc2ProxyGroup_rhel-centos-7.rpm: ciscoampconnector-1.12.2.002-1.el7.x86_64
Marking amp_juanc2ProxyGroup_rhel-centos-7.rpm as an update to ciscoampconnector-1.10.2.030-1.el7.x86_64
Resolving Dependencies
--> Missing transaction check
--> Package ciscoampconnector.x86_64 0:1.10.2.030-1.el7 will be updated
--> Package ciscoampconnector.x86_64 0:1.12.2.002-1.el7 will be an update
--> Finished Dependency Resolution

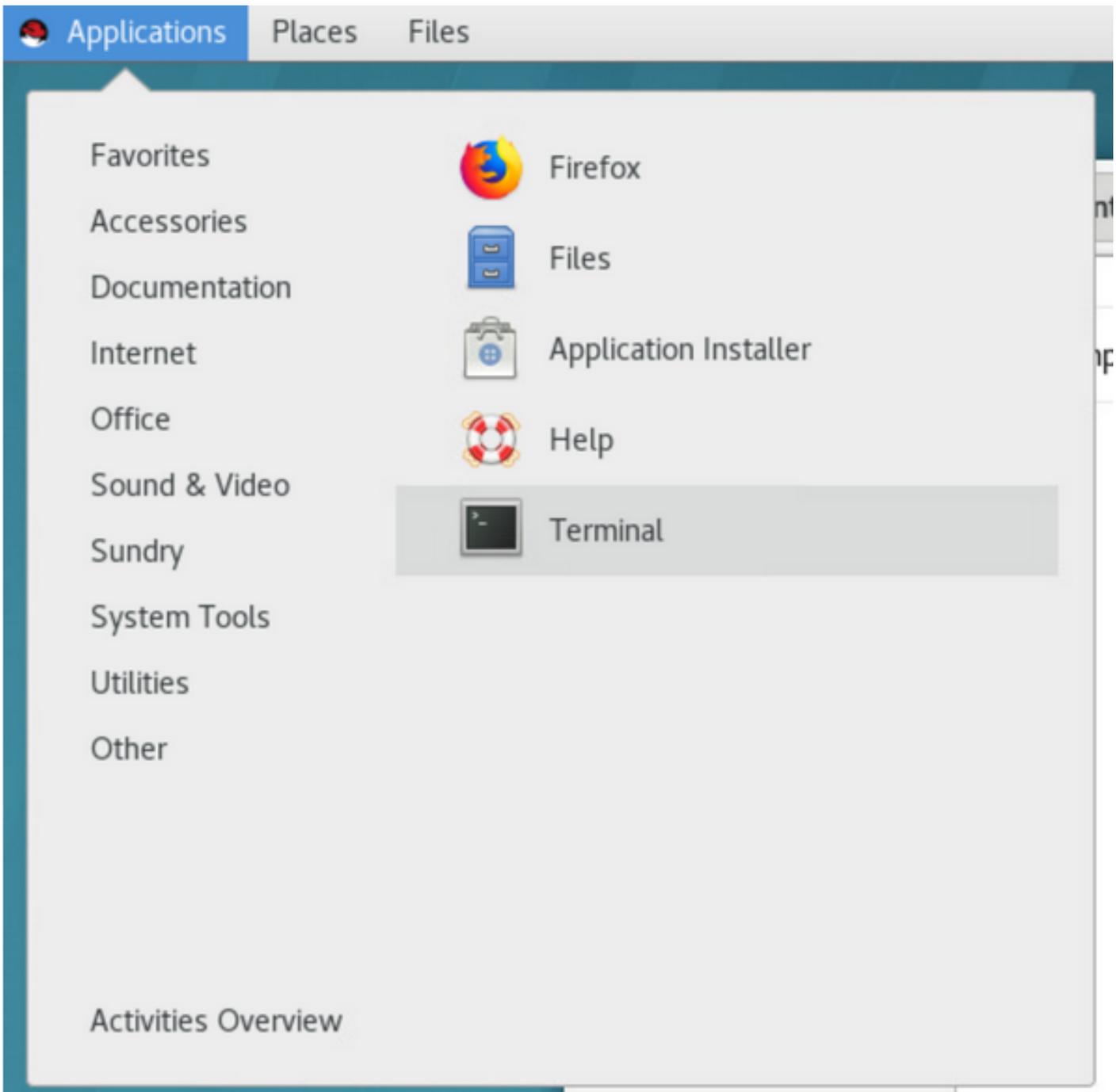
Dependencies Resolved

=====
Package                Arch          Version           Repository         Size
-----
Updating:
ciscoampconnector      x86_64        1.12.2.002-1.el7 /amp_juanc2ProxyGroup_rhel-centos-7 43 K
Transaction Summary
-----
Upgrade 1 Package

Total size: 43 K
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Policy saved to /opt/cisco/amp/atsc/policy.xml.ampsave

```

Wenn die Benutzeroberfläche verwendet wird, öffnen Sie das Terminal, wie im Bild gezeigt.



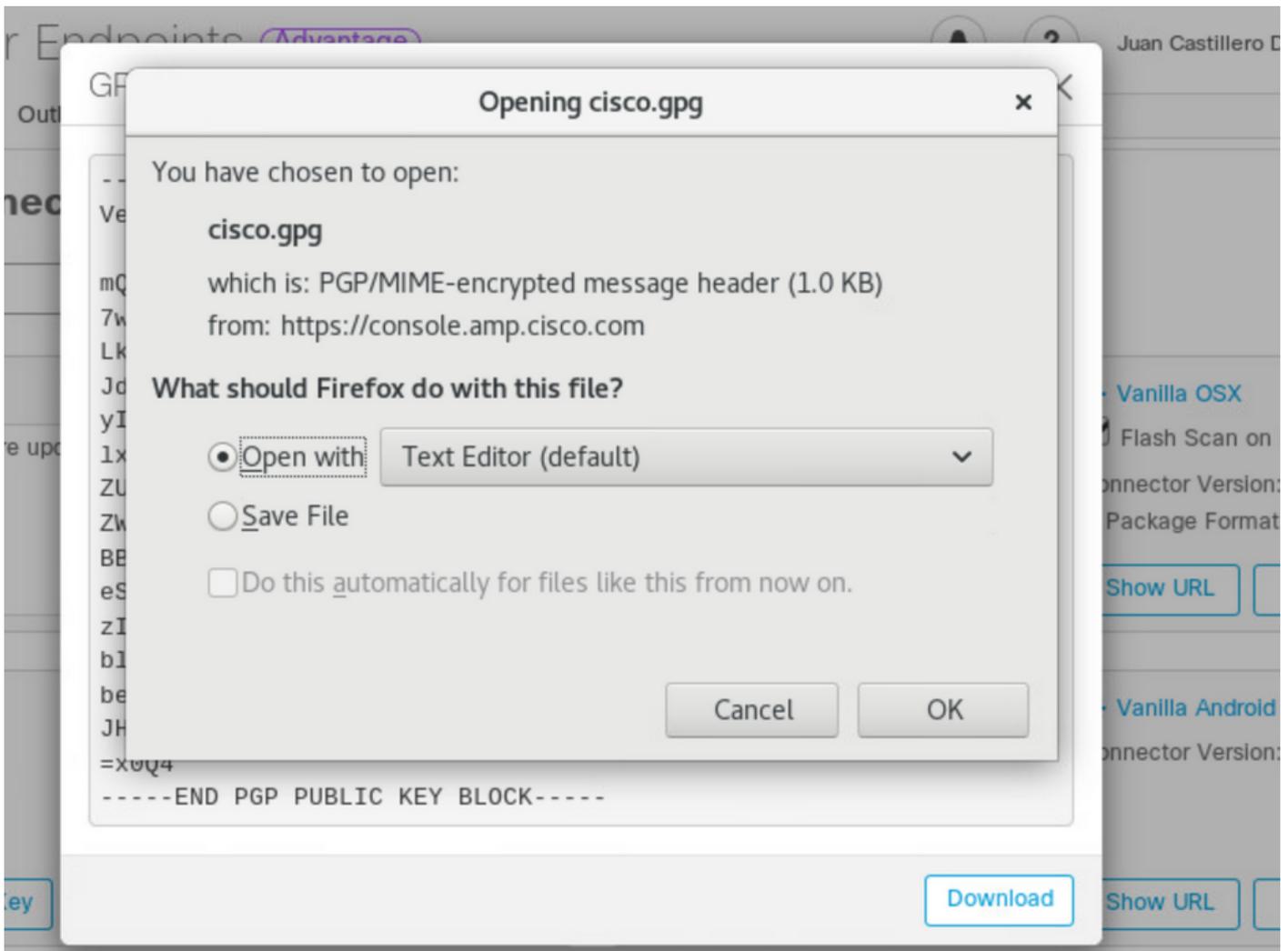
Nach Beginn der Installation ist keine Benutzereingabe erforderlich, sondern ein automatischer Prozess, wie im Bild gezeigt.

```
File Edit View Search Terminal Help
ipating:
ciscoampconnector x86_64 1.12.2.602-1.el7 /amp_proxyGroup_rhel-centos-7 43 M
-----
Transaction Summary
-----
Upgrade 1 Package

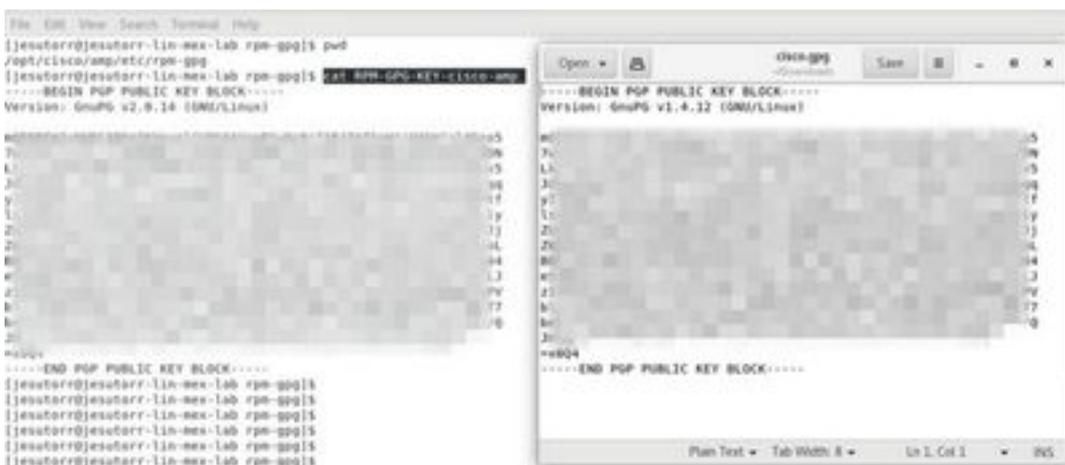
Total size: 43 M
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Policy saved to /opt/cisco/amp/etc/policy.xml.amgsave
Verifying archive integrity... 100% All good.
Uncompressing ampconnector installer 100%
  Updating : ciscoampconnector-1.12.2.602-1.el7.x86_64 1/2
warning: /opt/cisco/amp/etc/policy.xml created as /opt/cisco/amp/etc/policy.xml.rpmnew
Policy restored from /opt/cisco/amp/etc/policy.xml.amgsave
Verifying archive integrity... 100% All good.
Uncompressing ampconnector installer 100%
Redirecting to /bin/systemctl restart rsyslog.service
Cleaning : ciscoampconnector-1.10.2.630-1.el7.x86_64 2/2
Verifying : ciscoampconnector-1.12.2.602-1.el7.x86_64 1/2
Verifying : ciscoampconnector-1.10.2.630-1.el7.x86_64 2/2

Updated:
ciscoampconnector.x86_64 0:1.12.2.602-1.el7

Complete!
[[jcsutor@jesutarr-1in-mex-lab Downloads]$
```

Schritt 2: Führen Sie den Befehl von einem Terminal aus, um den Schlüssel zu importieren: `sudo rpm --import /opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp`.



Schritt 3: Überprüfen Sie, ob der Schlüssel installiert wurde, führen Sie den Befehl vom Terminal aus: `rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} -> %{summary}\n`.



Schritt 4: Suchen Sie in der Ausgabe nach einem GPG-Schlüssel von Sourcefire. Der Updater

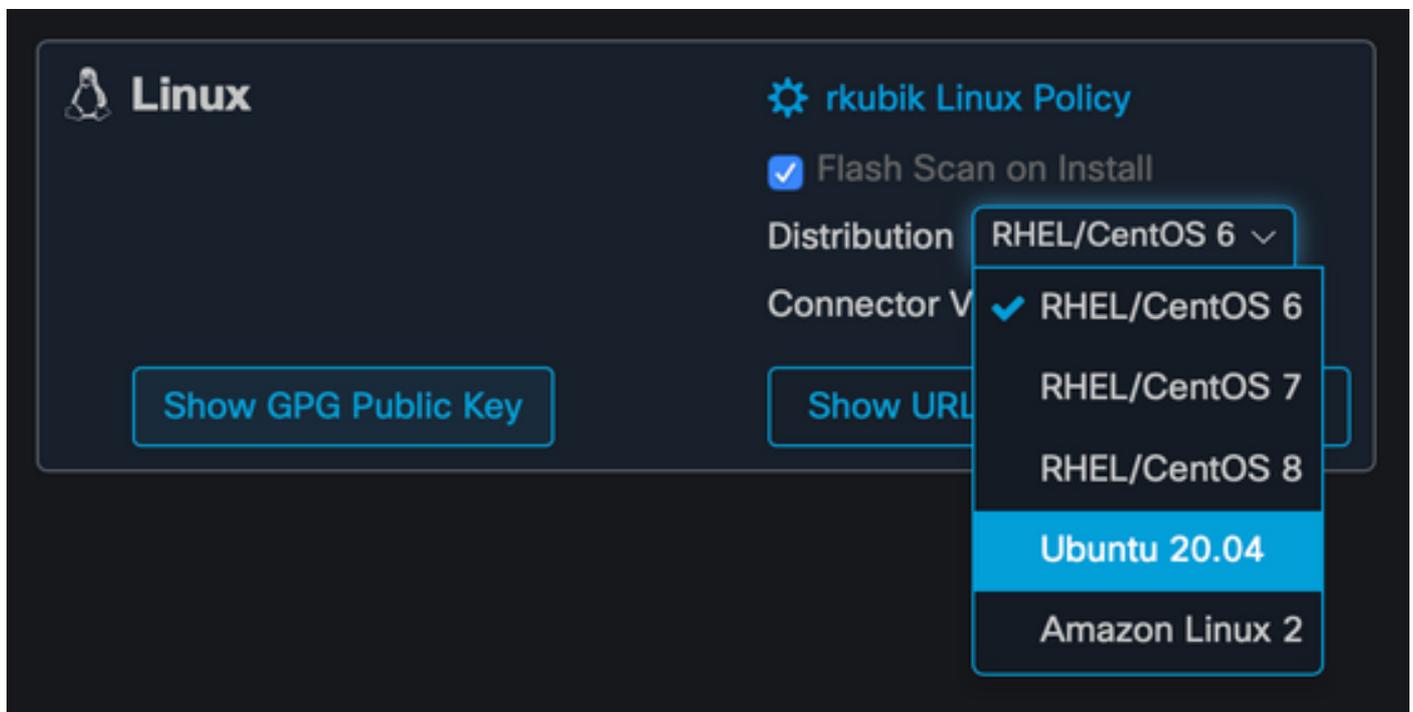
wird über den init-Daemon des Systems ausgeführt, und wenn ein Update verfügbar ist, wird automatisch der RPM-Upgrade-Prozess ausgelöst. Einige SELinux-Konfigurationen verbieten dieses Verhalten und führen zum Ausfall des Updaters.

Wenn Sie vermuten, dass dies der Fall ist, überprüfen Sie das Überwachungsprotokoll des Systems (z. B. `/var/log/audit/audit.log`) und suchen Sie nach Denial-Ereignissen im Zusammenhang mit Ampupdater. Sie müssen möglicherweise SELinux-Regeln anpassen, damit Updater funktioniert.

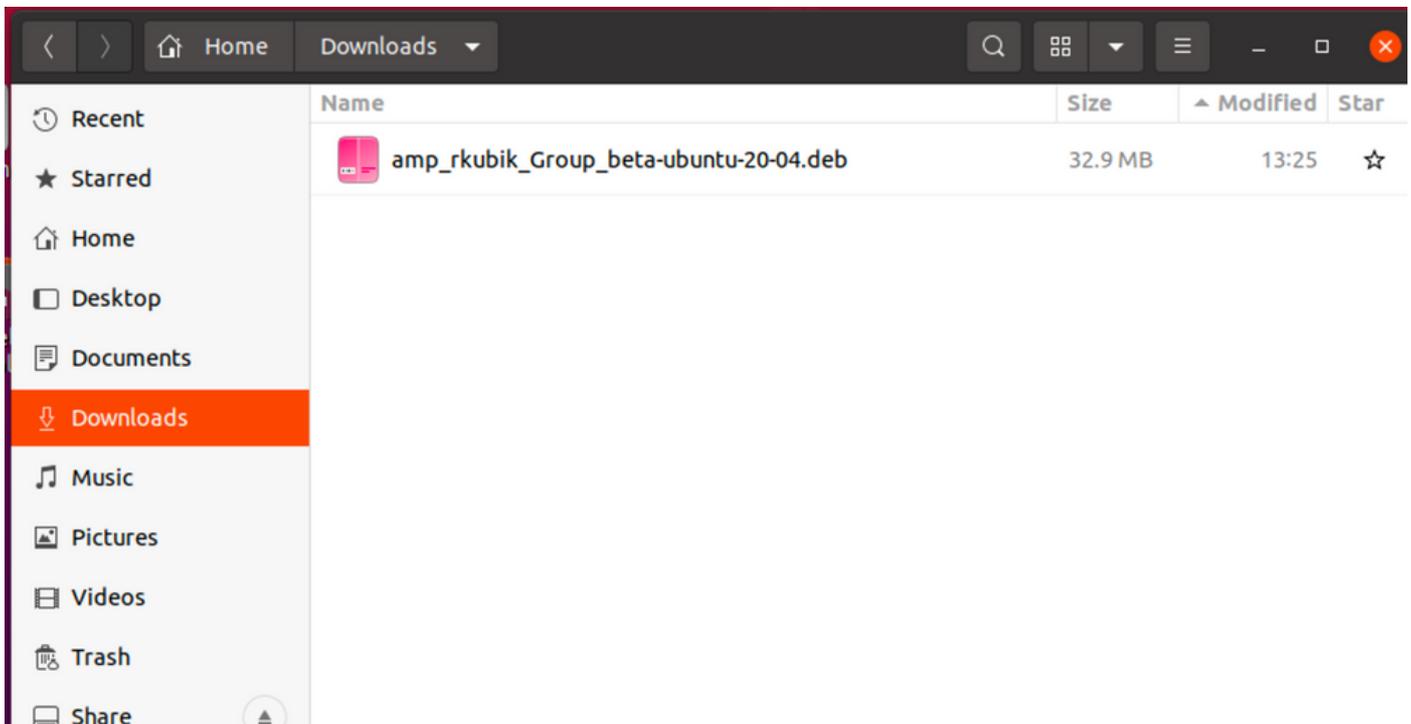
Ubuntu

Konfigurationen

Schritt 1: Laden Sie das Linux DEB-Paket vom Cisco Secure Endpoint Portal herunter, wie im Bild gezeigt.



Schritt 2: Verschieben Sie das DEB-Paket an den betreffenden Endpunkt, indem Sie es entweder direkt vom Dashboard herunterladen oder manuell auf die Endpunkte verschieben. In diesem Beispiel wird eine grafische Benutzeroberfläche (Graphic User Interface, UI) verwendet, obwohl es möglich und häufig üblich ist, mit einer Minimalinstallation zu arbeiten. In diesem Fall muss man wissen, wie man das Linux-Terminal behandelt und das DEB-Paket findet.



Schritt 3: Um den Linux-Anschluss zu installieren, führen Sie den folgenden Befehl aus: **sudo dpkg -i [deb-Paket]**, wobei [deb-Paket] der Name der Datei ist, zum Beispiel "amp_Audit.deb". Nach Beginn der Installation ist keine Benutzereingabe erforderlich, sondern ein automatischer Prozess, wie im Bild gezeigt.

```

/bin/bash
/bin/bash 80x24
Now using version go1.11.13
13:27:33 cisco~
$ cd Downloads/
13:27:53 cisco~/Downloads
$ sudo dpkg -i amp_rkubik_Group_beta-ubuntu-20-04.deb
Selecting previously unselected package ciscoampconnector.
(Reading database ... 252023 files and directories currently installed.)
Preparing to unpack amp_rkubik_Group_beta-ubuntu-20-04.deb ...
Unpacking ciscoampconnector (1.15.999.9999-1) ...
Setting up ciscoampconnector (1.15.999.9999-1) ...
Verifying archive integrity... 100% All good.
Uncompressing ampconnector installer 100%
Processing triggers for libc-bin (2.31-0ubuntu9.1) ...
Processing triggers for rsyslog (8.2001.0-1ubuntu1.1) ...
13:28:02 cisco~/Downloads
$ █
```

Importieren des GPG-Schlüssels

Der öffentliche GPG-Schlüssel kann von der Seite Download Connector kopiert werden, um die Signierung des DEB-Pakets zu überprüfen. Der Anschluss kann ohne GPG-Schlüssel installiert werden. Ein Benutzer müsste jedoch den GPG-Schlüssel in seinen Debsig-Keyring importieren, wenn er die Verbindungsupdates mithilfe der Ubuntu-Richtlinie weiterleiten möchte. Weitere Informationen zum Importieren des GPG-Schlüssels und zum Überprüfen, dass der Anschluss unter Ubuntu nicht modifiziert wurde, finden Sie unter <https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/216524-amp-for-endpoints-ubuntu-connector.html#anc6>

Anmerkung: Ab der Connector-Version 1.17.0 wird der GPG-Schlüssel, der zur Verifizierung von Upgrade-Paketen während der Connector-Updates verwendet wird, automatisch installiert. Um diesen GPG-Schlüssel zu überprüfen, klicken Sie auf der Seite Download Connector auf den Link GPG Public Key (GPG-Schlüssel), und vergleichen Sie ihn mit dem Schlüssel, der unter `/opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-Key-cisco-amp` installiert wurde.

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Um die erfolgreiche Installation zu überprüfen, führen Sie die **AMP-CLI aus**. Die Befehlszeilenschnittstelle für den Linux-Anschluss finden Sie unter `/opt/cisco/amp/bin/ampcli`. Es kann im interaktiven Modus ausgeführt werden oder es kann ein einzelner Befehl ausgeführt und dann beendet werden. Führen Sie den Befehl `./ampcli —help aus`, um eine vollständige Liste der verfügbaren Optionen und Befehle anzuzeigen. Alle vom Connector generierten Protokolldateien sind in `/var/log/cisco` zu finden.

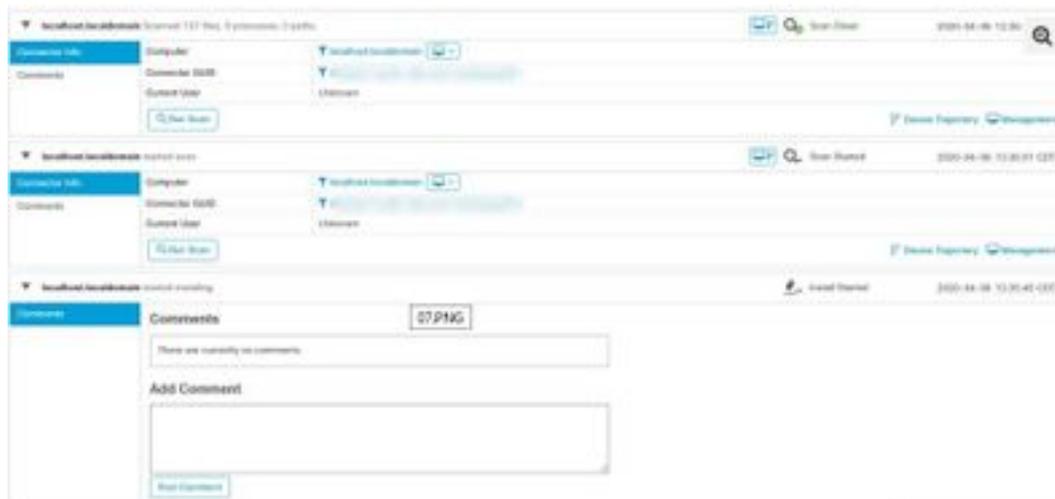
```
File Edit View Search Terminal Help
[preuser@preuser-lin-ns-lab ~]$ cd /opt/cisco/amp/bin/
[preuser@preuser-lin-ns-lab bin]$ pwd
/opt/cisco/amp/bin
[preuser@preuser-lin-ns-lab bin]$ ls
ampcli  ampcli.rpm  ampcli.service  ampcli.service.rpm  cisco-amp-helper  libampcli.so.1.0  libampcli.so.1.0.rpm  libampcli.so.1.0.rpm.rpm
[preuser@preuser-lin-ns-lab bin]$ ./ampcli

ampcli - AMP for Endpoints Connector Command Line Interface
Interactive mode

Enter 'q' or Ctrl+C to Exit

[logger] Set maximum reported log level to notice
Trying to connect...
Connected.
ampcli> status
Status: Connected
Mode: Normal
Scan: Ready for scan
Last Scan: 2020-02-29 03:26 PM
Policy: Jabotize-Linux (4025000)
Command Line: Enabled
Faults: None
ampcli>
```

Auf der Cisco Secure Console wird auch eine Installationsveranstaltung angezeigt. Wenn beim Herunterladen des RPM-Pakets Flash-Scans angefordert wurden, werden diese ebenfalls angezeigt.



Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [Installation des AMP für Endpoints-Anschlusses in Linux-Video](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)