Installazione del connettore Cisco Secure Endpoint Linux

Sommario

Introduzione

Questo documento descrive come installare e verificare il connettore Cisco Secure Endpoint Linux per i sistemi basati su Red Hat Enterprise Linux (RHEL) e Debian.

Contributo di Juan Carlos Castillero e curato da Yeraldin Sanchez, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Computer Linux su un sistema operativo supportato da un connettore Linux

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Un programma di installazione del connettore Linux dell'endpoint sicuro Red Hat Package Manager (RPM)
- Un programma di installazione per il connettore Linux dell'endpoint sicuro Debian Package Manager (dpkg)

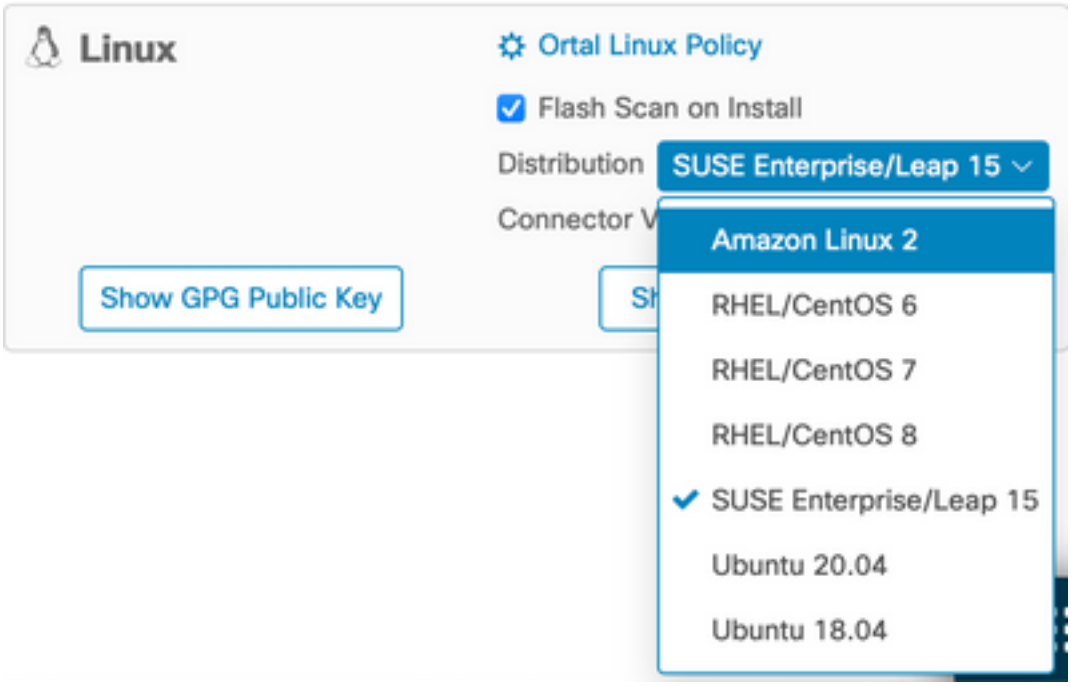
- Una chiave GNU Privacy Guard (GPG) per verificare gli aggiornamenti (opzionale)
- Un programma di installazione del connettore Linux DPKG (Debian Package Management System)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

RHEL/CentOS/Amazon Linux 2/SUSE 15

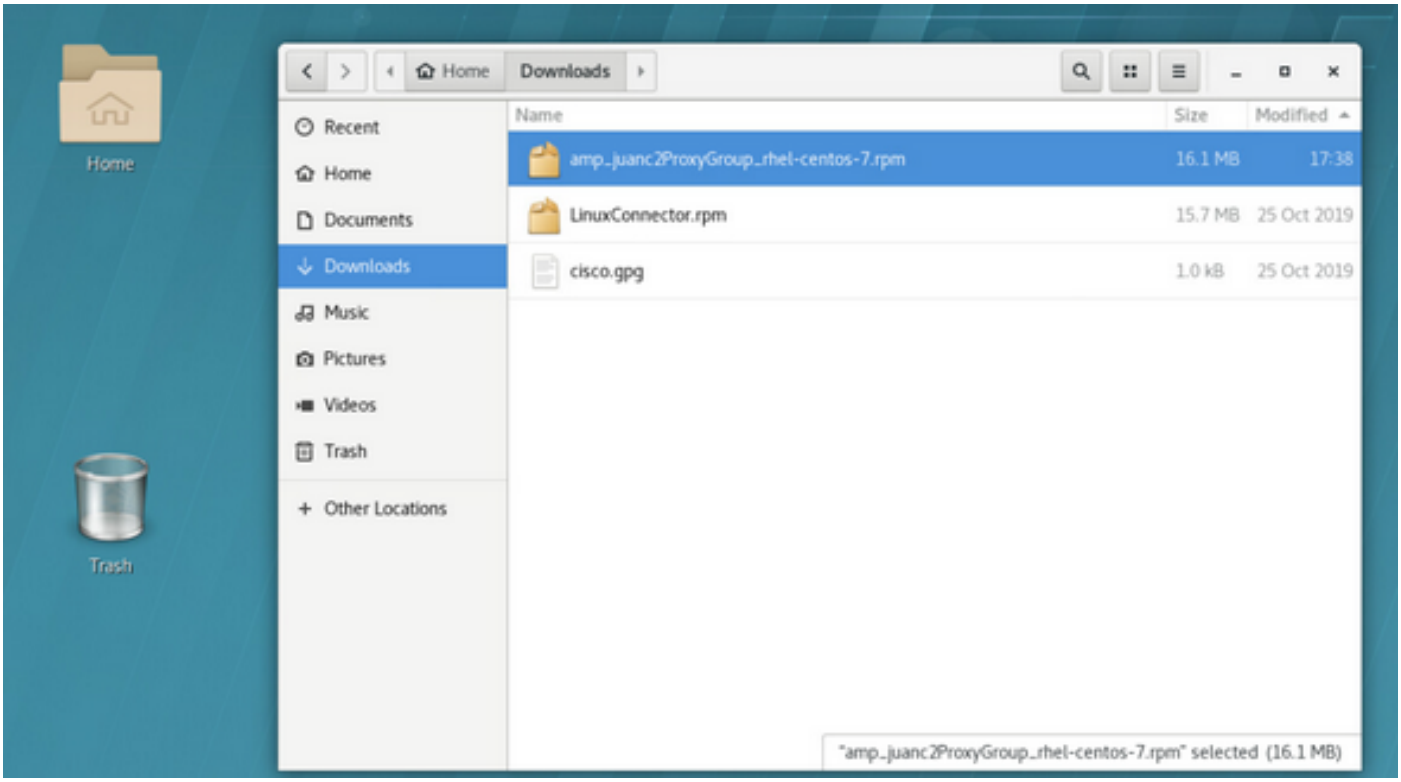
Configurazioni

Passaggio 1. Scaricare il pacchetto Linux RPM dal Cisco Secure Endpoint Portal, come mostrato nell'immagine.



> **Nota:** È importante tenere presente che la distribuzione del sistema operativo è importante in quanto entrambi i connettori hanno architetture completamente diverse.

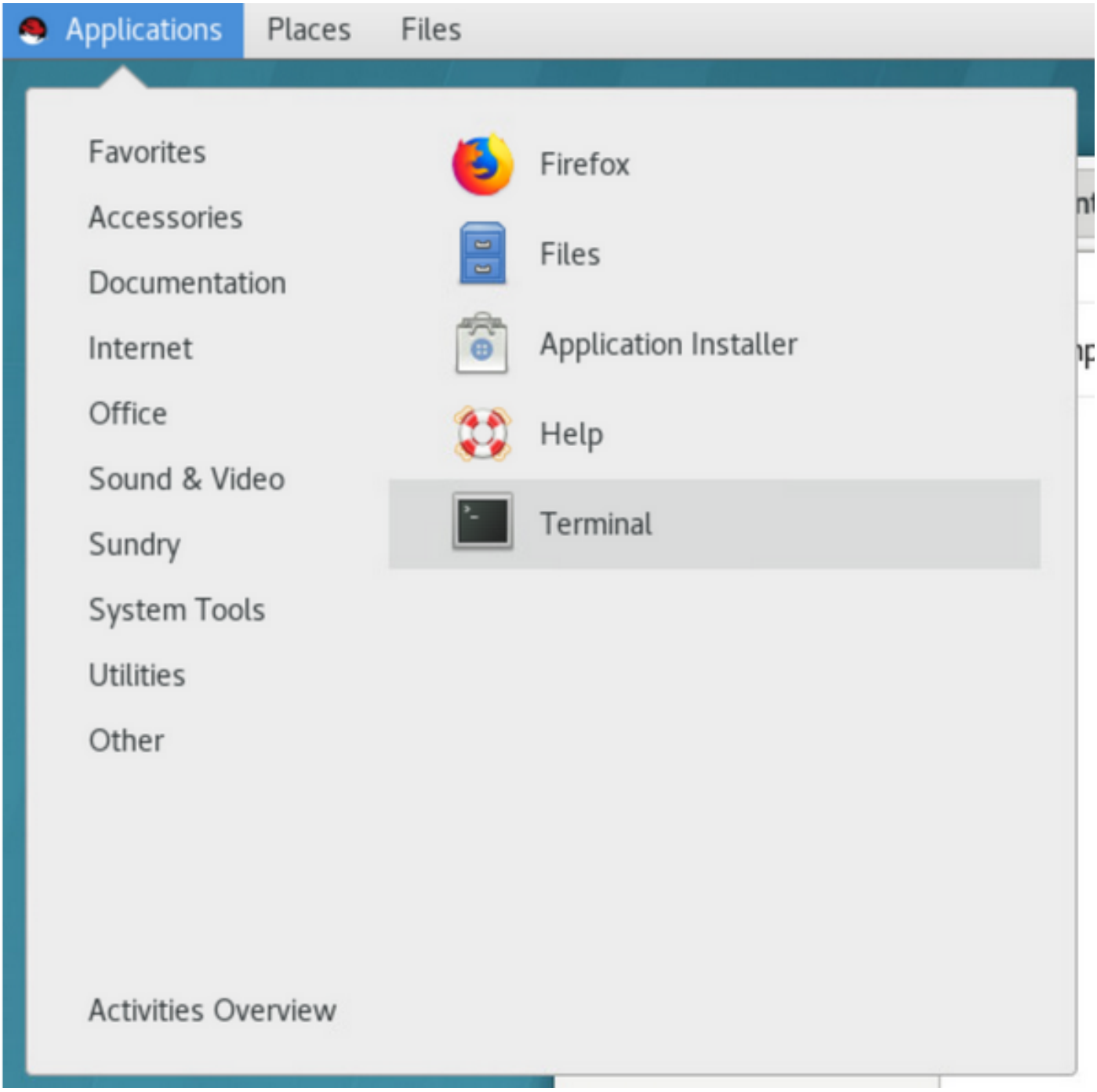
Passaggio 2. Spostare il pacchetto RPM nell'endpoint in questione, scaricarlo direttamente dal dashboard o spostarlo manualmente negli endpoint. In questo esempio viene utilizzata un'interfaccia utente grafica (UI, Graphic User Interface), sebbene sia possibile, e spesso comune, lavorare con un'installazione minima. In questo caso, è necessario sapere come gestire il terminale Linux e trovare il pacchetto RPM.



Passaggio 3. Per installare il connettore Linux, eseguire il comando: **sudo yum localinstall [pacchetto rpm] -y** (o **sudo zypper install -y [pacchetto rpm]** su SUSE 15)

dove [rpm package] è il nome del file, ad esempio "amp_Audit.rpm". È necessario installare il pacchetto RPM durante l'esecuzione del servizio atd.

Se la GUI è in uso, aprire il terminale, come mostrato nell'immagine.



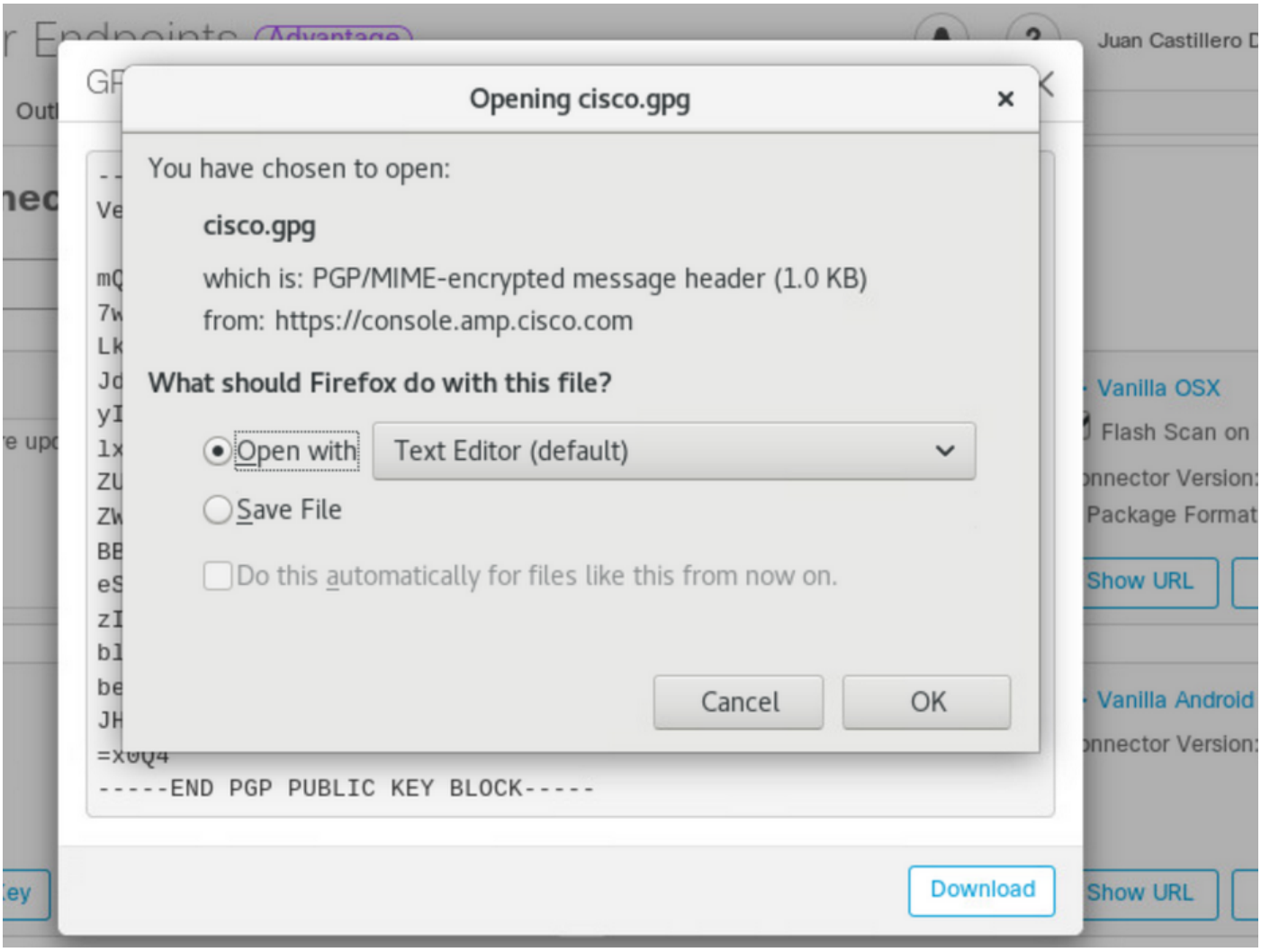
Una volta avviata l'installazione, non è necessario alcun input da parte dell'utente, ma si tratta di un processo automatico, come mostrato nell'immagine.

Come importare il tasto GPG

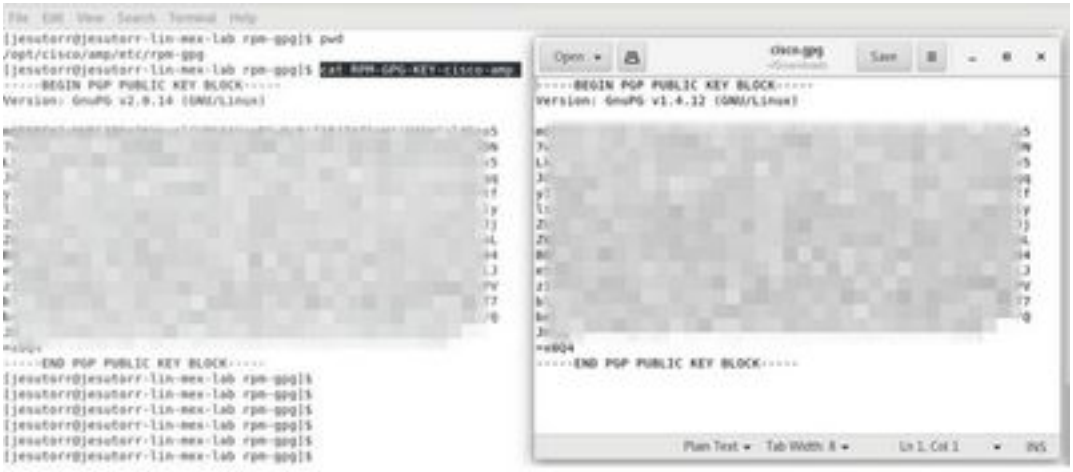
La chiave pubblica GPG può essere copiata dalla pagina Download Connector per verificare la firma del pacchetto RPM. Il connettore può essere installato senza il tasto GPG; tuttavia, un utente deve importare la chiave GPG nel database RPM se prevede di eseguire il push degli aggiornamenti del connettore tramite criteri RHEL.

Nota: A partire dalla versione 1.17.0 del connettore, il tasto GPG utilizzato per verificare i pacchetti di aggiornamento durante gli aggiornamenti del connettore viene installato automaticamente.

Passaggio 1. Verificare la chiave GPG, quindi fare clic sul collegamento Chiave pubblica GPG nella pagina Download Connector. Confrontare la chiave con quella su **/opt/cisco/amp/etc/rpm-gpg/RPM-GPG-Key-cisco-amp**.



Passaggio 2. Eseguire il comando da un terminale per importare la chiave: **sudo rpm —import /opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp**.



Passaggio 3. Verificare che la chiave sia stata installata, quindi eseguire il comando dal terminale: **rpm -q gpg-pubkey —qf '%{name}-%{version}-%{release} —> %{summary}\n'**.

Passaggio 4. Cercare nell'output una chiave GPG di Sourcefire. Il programma di aggiornamento

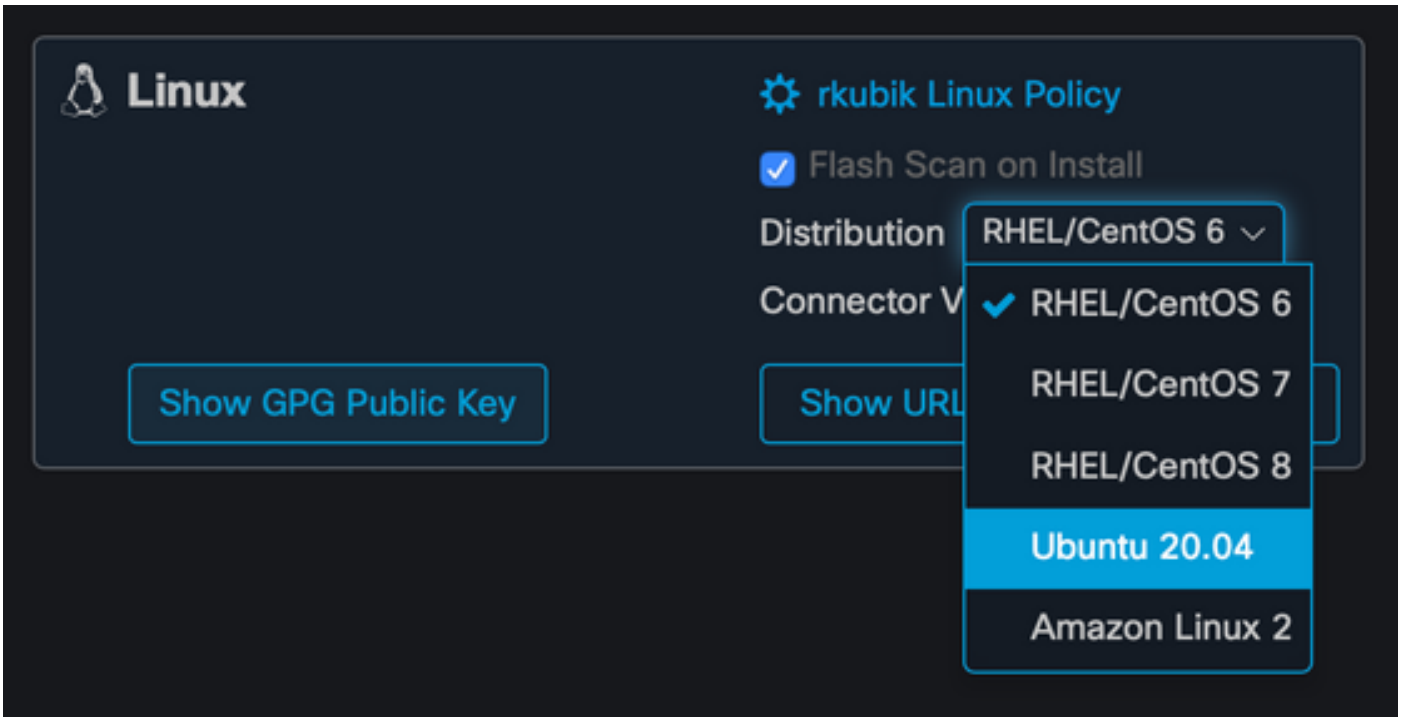
viene eseguito dal daemon di inizializzazione del sistema e, quando è disponibile un aggiornamento, attiva automaticamente il processo di aggiornamento RPM. Alcune configurazioni SELinux vietano questo comportamento e causano il fallimento dell'Updater.

Se si sospetta che questo sia il caso, esaminare il registro di controllo del sistema (ad esempio, **/var/log/audit/audit.log**) e cercare gli eventi di rifiuto correlati a ampupdater. Potrebbe essere necessario regolare le regole SELinux per consentire il funzionamento di Updater.

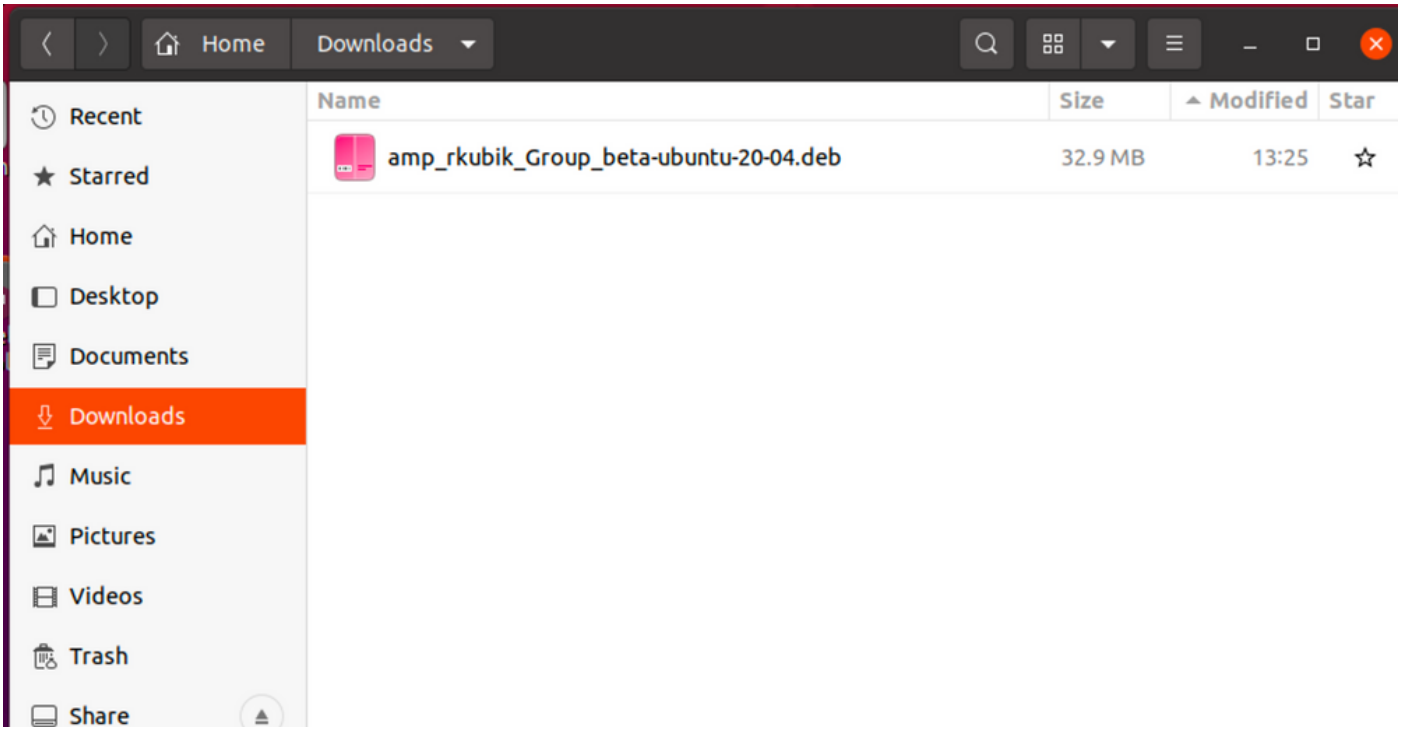
Ubuntu

Configurazioni

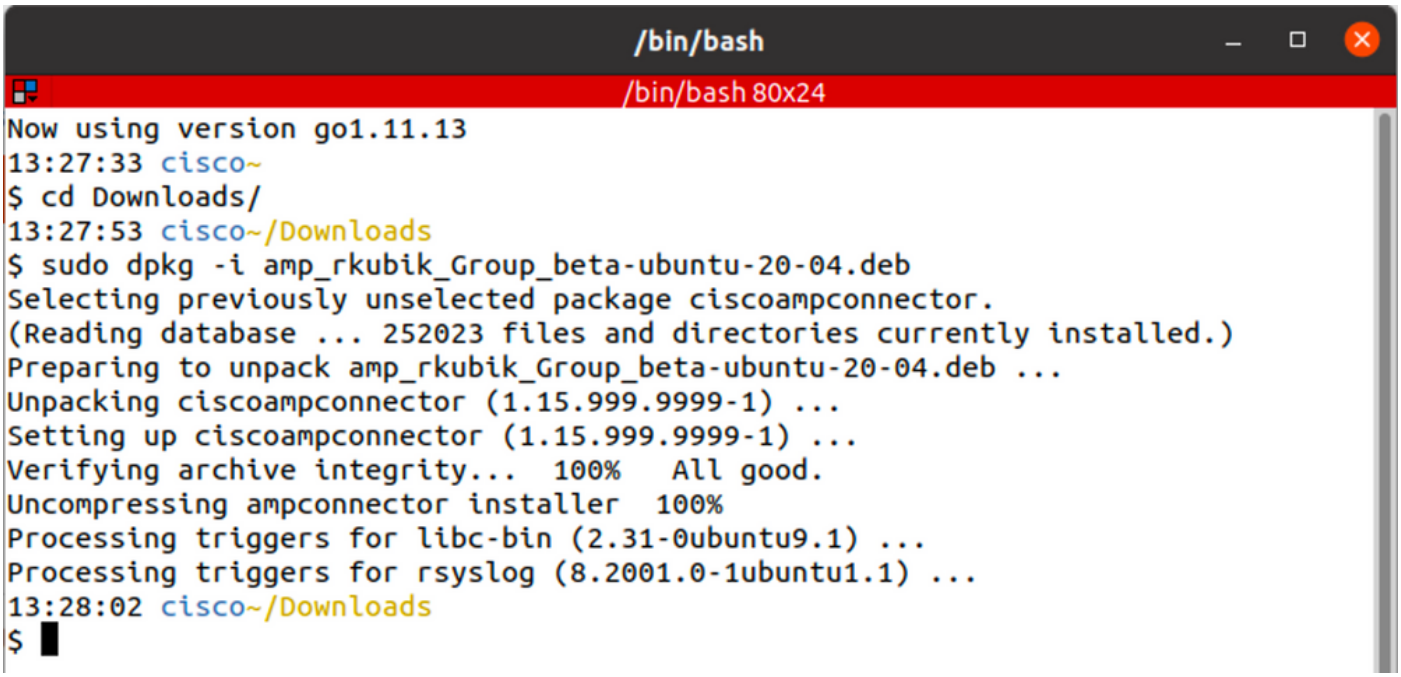
Passaggio 1. Scaricare il pacchetto Linux DEB da Cisco Secure Endpoint Portal, come mostrato nell'immagine.



Passaggio 2. Spostare il pacchetto DEB sull'endpoint in questione, scaricarlo direttamente dal dashboard o spostarlo manualmente sugli endpoint. In questo esempio viene utilizzata un'interfaccia utente grafica (UI, Graphic User Interface), anche se è possibile, e spesso comune, lavorare con un'installazione minima. In questo caso, è necessario sapere come gestire il terminale Linux e trovare il pacchetto DEB.



Passaggio 3. Per installare il connettore Linux, eseguire il comando: **sudo dpkg -i [pacchetto deb]** dove [pacchetto deb] è il nome del file, ad esempio "amp_Audit.deb". Una volta avviata l'installazione, non è necessario alcun input da parte dell'utente, ma si tratta di un processo automatico, come mostrato nell'immagine.



Come importare il tasto GPG

La chiave pubblica GPG può essere copiata dalla pagina Download Connector per verificare la firma del pacchetto DEB. Il connettore può essere installato senza il tasto GPG; tuttavia, un utente dovrebbe importare la chiave GPG nel suo keyring debsig se ha intenzione di spingere gli aggiornamenti del connettore tramite la policy su Ubuntu. Per ulteriori informazioni su come importare il tasto GPG e verificare che il connettore non sia stato modificato su Ubuntu, vedere https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/216524-amp-for-endpoints-ubuntu-connector.html#anc6

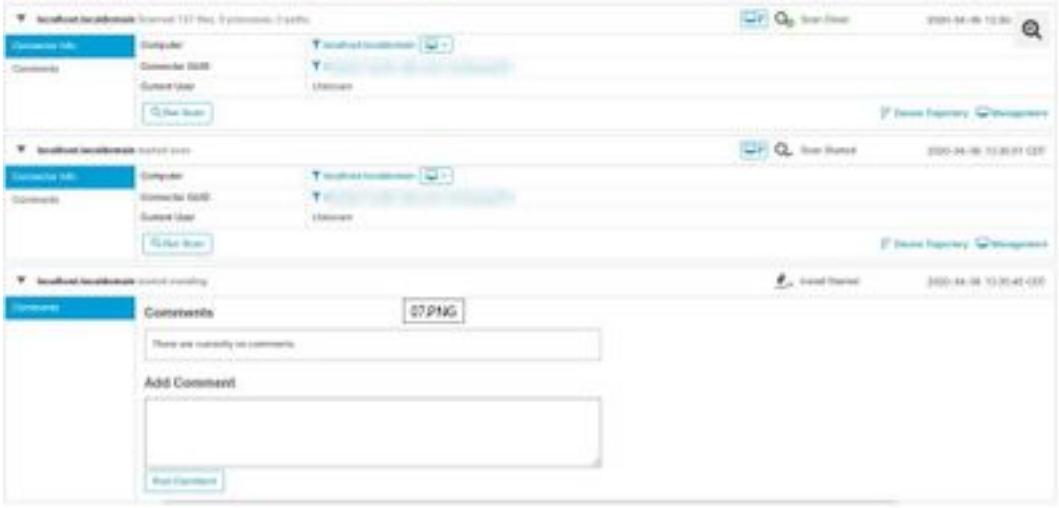
Nota: A partire dalla versione 1.17.0 del connettore, il tasto GPG utilizzato per verificare i pacchetti di aggiornamento durante gli aggiornamenti del connettore viene installato automaticamente. Per verificare questa chiave GPG, fare clic sul collegamento Chiave pubblica GPG nella pagina Download Connector e confrontarla con la chiave installata in **/opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-Key-cisco-amp**.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Per verificare il corretto completamento dell'installazione, eseguire **AMP CLI**. L'interfaccia della riga di comando del connettore Linux è disponibile in **/opt/cisco/amp/bin/ampcli**. Può essere eseguito in modalità interattiva oppure eseguire un unico comando e uscire. Eseguire il comando **./ampcli —** per visualizzare un elenco completo delle opzioni e dei comandi disponibili. Tutti i file di registro generati dal connettore si trovano in **/var/log/cisco.**

Sulla console Cisco Secure viene visualizzato anche un evento di installazione. Se sono state richieste scansioni flash durante il download del pacchetto RPM, verranno visualizzate anche queste.



Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Installare AMP for Endpoints Connector in un video Linux
- Documentazione e supporto tecnico – Cisco Systems