تثبيت موصل Cisco Secure Endpoint Linux

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
نظام التشغيل RHEL/CentOS/Amazon Linux 2/SUSE 15
التكوينات
كيفية استيراد مفتاح GPG
أوبونتو
التكوينات
كيفية استيراد مفتاح GPG
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يوضح هذا المستند كيفية تثبيت موصل Linux الآمن من Cisco لـ Red Hat Enterprise Linux (RHEL) والأنظمة المستندة إلى Debian والتحقق من ذلك.

ساهم في التحرير خوان كارلوس كاستيليرو ويارديني سانشيز، مهندسو TAC من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- أجهزة Linux على موصل Linux الذي يدعم نظام التشغيل

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

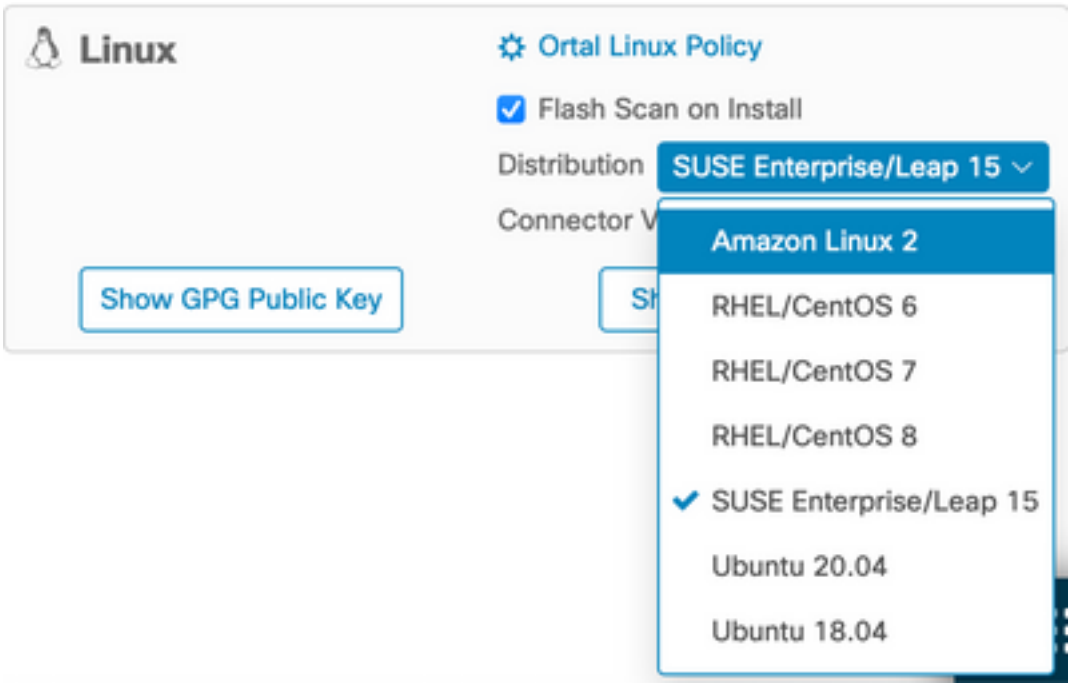
- برنامج Secure Endpoint Linux Connector Installer Red Hat Package Manager (RPM)
- مدير حزمة Debian لمثبت موصل نقطة النهاية الآمنة Linux (dpkg)
- مفتاح حماية خصوصية GNU (GPG) للتحقق من التحديثات (إختياري)
- DPKG لمثبت موصل Linux (نظام Debian لإدارة الحزم)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

نظام التشغيل RHEL/CentOS/Amazon Linux 2/SUSE 15

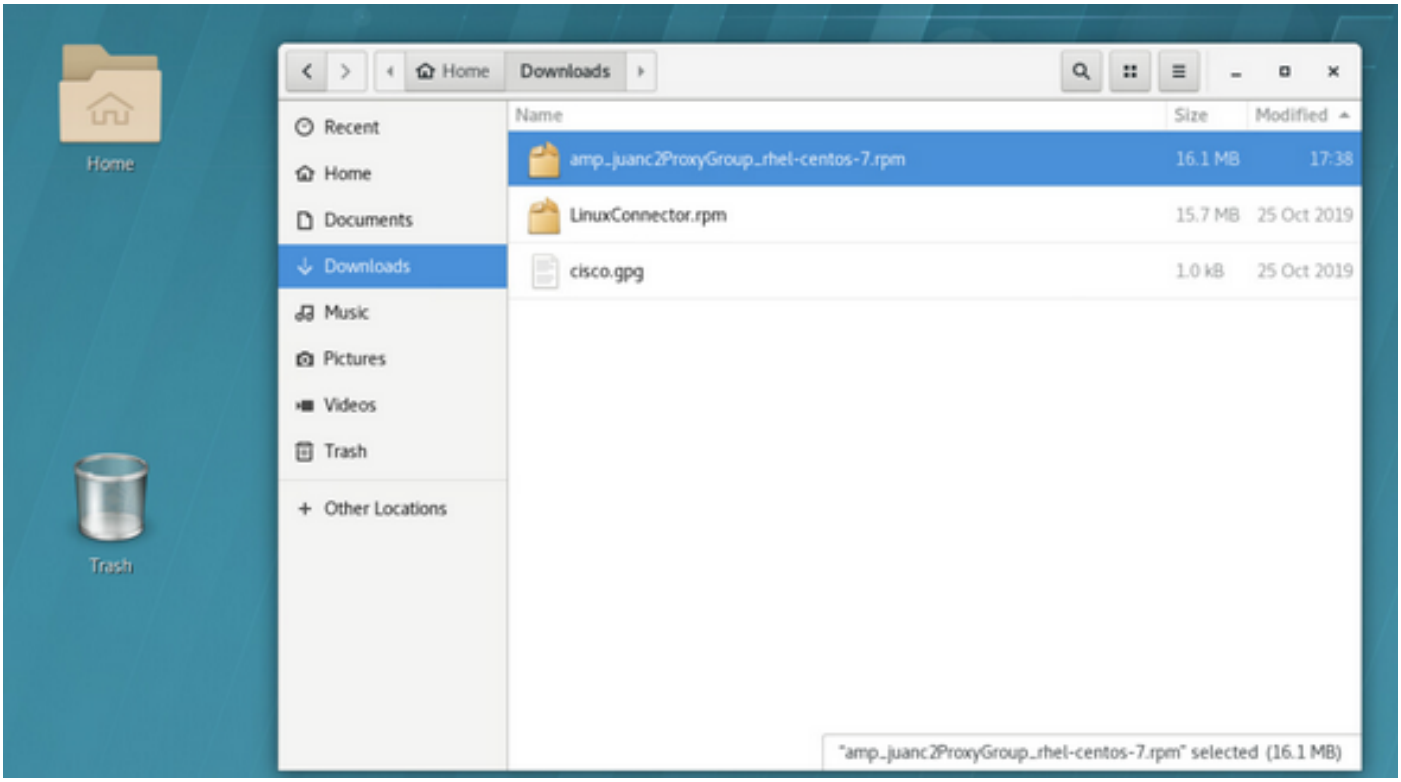
التكوينات

الخطوة 1. قم بتنزيل حزمة RPM من Linux من بوابة نقطة النهاية الآمنة من Cisco، كما هو موضح في الصورة.



ملاحظة: تذكر أن توزيع نظام التشغيل مهم لأن كل الموصلين المختلفين لهما بنيات مختلفة بشكل كبير.

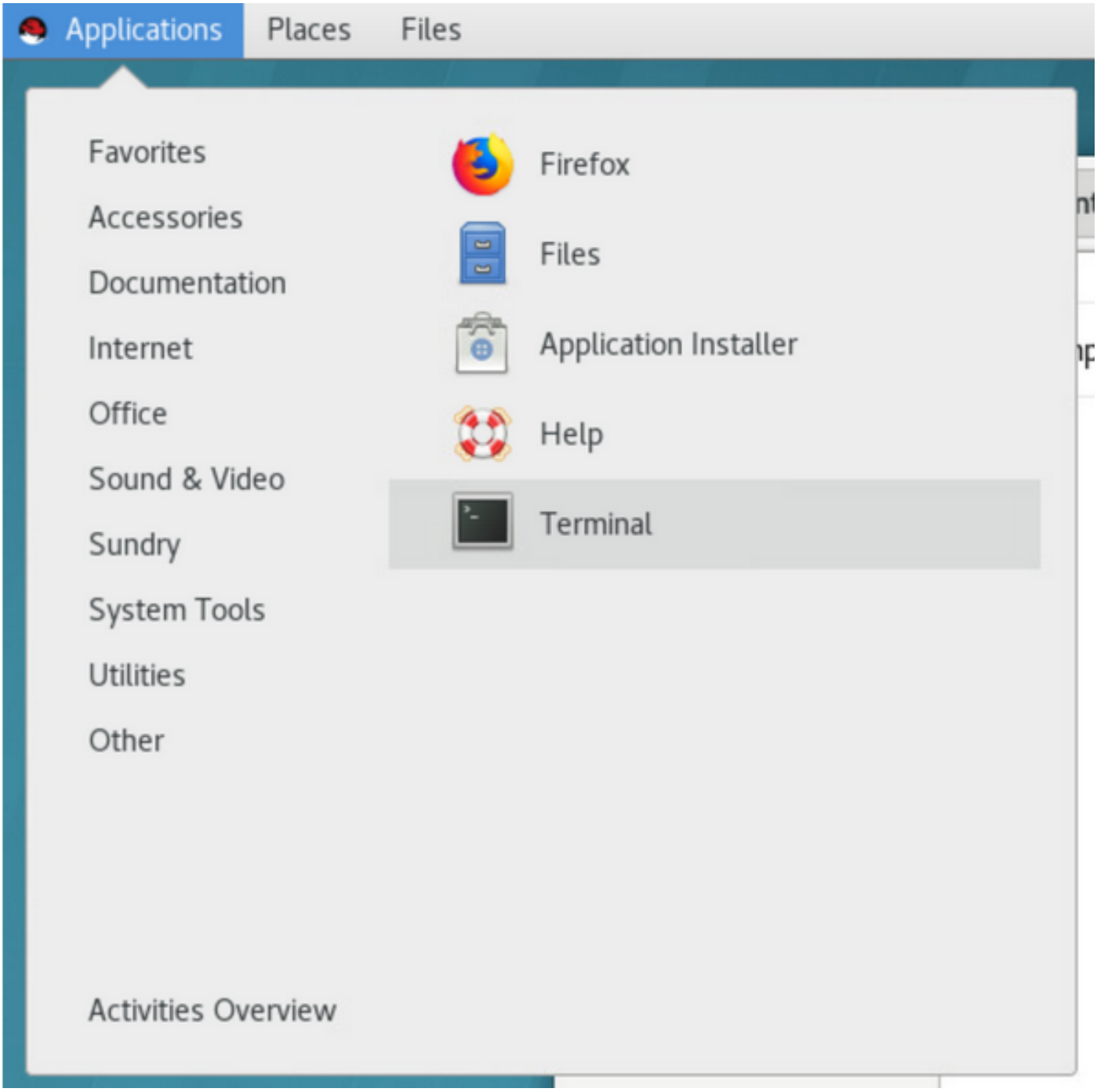
الخطوة 2. قم بنقل حزمة RPM إلى نقطة النهاية المعنية، إما أن تقوم بتنزيلها مباشرة من لوحة المعلومات أو أن تنقلها يدويا إلى نقاط النهاية. على سبيل المثال، يتم إستخدام واجهة مستخدم رسومية (UI)، على الرغم من أنه من الممكن، والشائع غالبا، العمل بأقل تثبيت، وفي هذه الحالة، فإنها مطلوبة لمعرفة كيفية التعامل مع محطة ليونكس الطرفية والعثور على حزمة RPM الخاصة بهم.



الخطوة 3. من أجل تثبيت موصل Linux، قم بتنفيذ الأمر: **تثبيت برنامج Sudo yum محلي [حزمة RPM] -y** (أو **تثبيت برنامج Sudo Zypper -y [حزمة RPM]** على SUSE 15)

حيث [حزمة RPM] هو اسم الملف، على سبيل المثال، "amp_Audit.rpm". يجب تثبيت حزمة RPM أثناء تشغيل خدمة ATD.

إذا كانت واجهة المستخدم الرسومية قيد الاستخدام، افتح الوحدة الطرفية، كما هو موضح في الصورة.



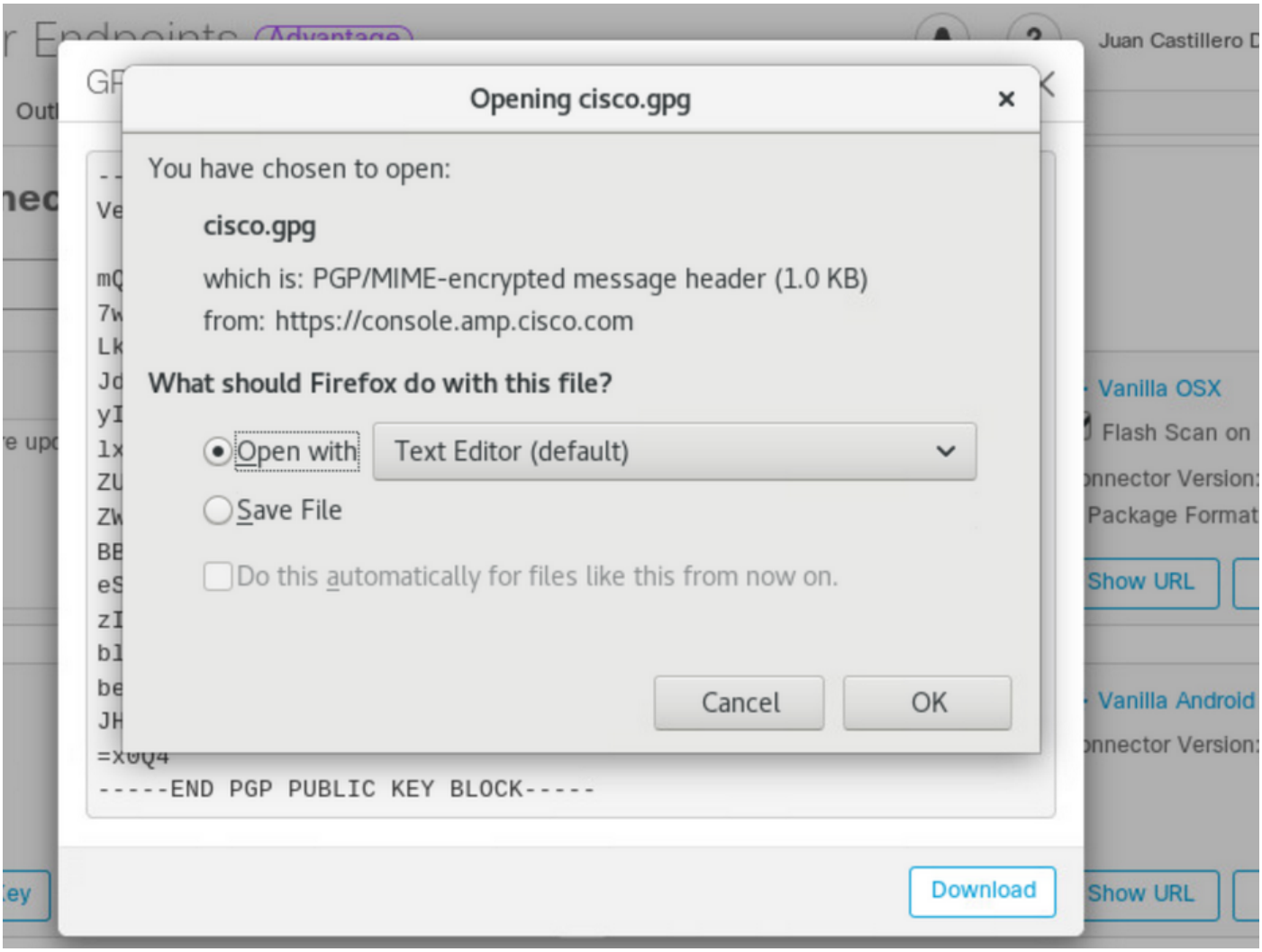
بمجرد بدء التثبيت، لا يتطلب أي إدخال مستخدم، فهي عملية تلقائية، كما هو موضح في الصورة.

كيفية إستيراد مفتاح GPG

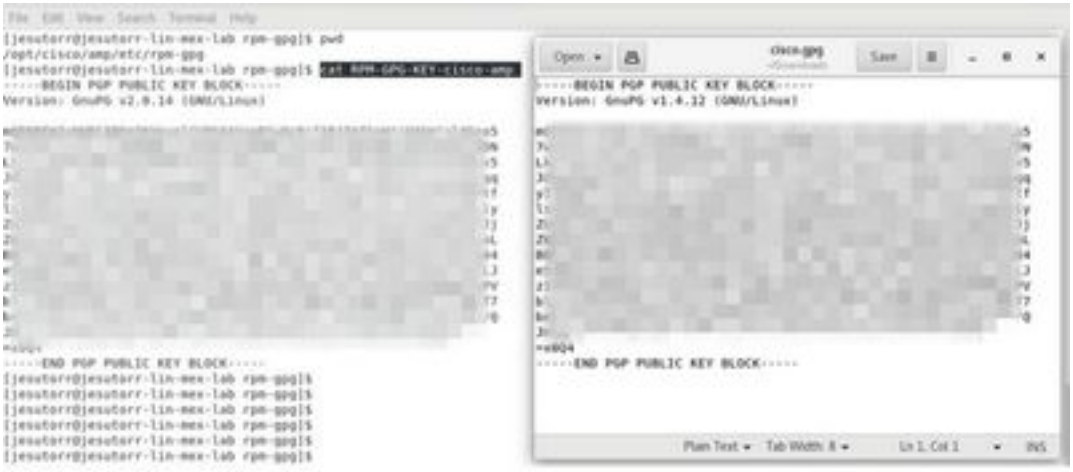
يمكن نسخ مفتاح GPG العام من صفحة تنزيل الموصل للتحقق من توقيع حزمة RPM. يمكن تثبيت الموصل بدون مفتاح GPG؛ ومع ذلك، مستخدم قد تحتاج إلى إستيراد مفتاح GPG إلى قاعدة بيانات RPM الخاصة بها إذا كانت تخطط لدفع تحديثات الموصل عبر سياسة على RHEL.

ملاحظة: ابتداء من الإصدار 1.17.0 من الموصل، يتم تثبيت مفتاح GPG المستخدم للتحقق من حزم الترقية أثناء تثبيت تحديثات الموصل تلقائيا.

الخطوة 1. تحقق من مفتاح GPG، انقر فوق إرتباط مفتاح GPG العام في صفحة تنزيل الموصل. قارن المفتاح بالمفتاح at/opt/cisco/amp/etc/rpm-gpg/rpm-gpg-key-cisco-amp.



الخطوة 2. قم بتشغيل الأمر من وحدة طرفية لاستيراد المفتاح: **sudo rpm —import /opt/cisco/amp/etc/rpm-gpg/RPM-gpg-key-cisco-amp**.



الخطوة 3. تحقق من تثبيت المفتاح، قم بتشغيل الأمر من المحطة الطرفية: **rpm -q gpg-pubkey —qf '%{name}-%{version}-%{release} —> %{summary}\n'**.

الخطوة 4. ابحث عن مفتاح GPG من Sourcefire في الإخراج. يتم تشغيل المحدث بواسطة

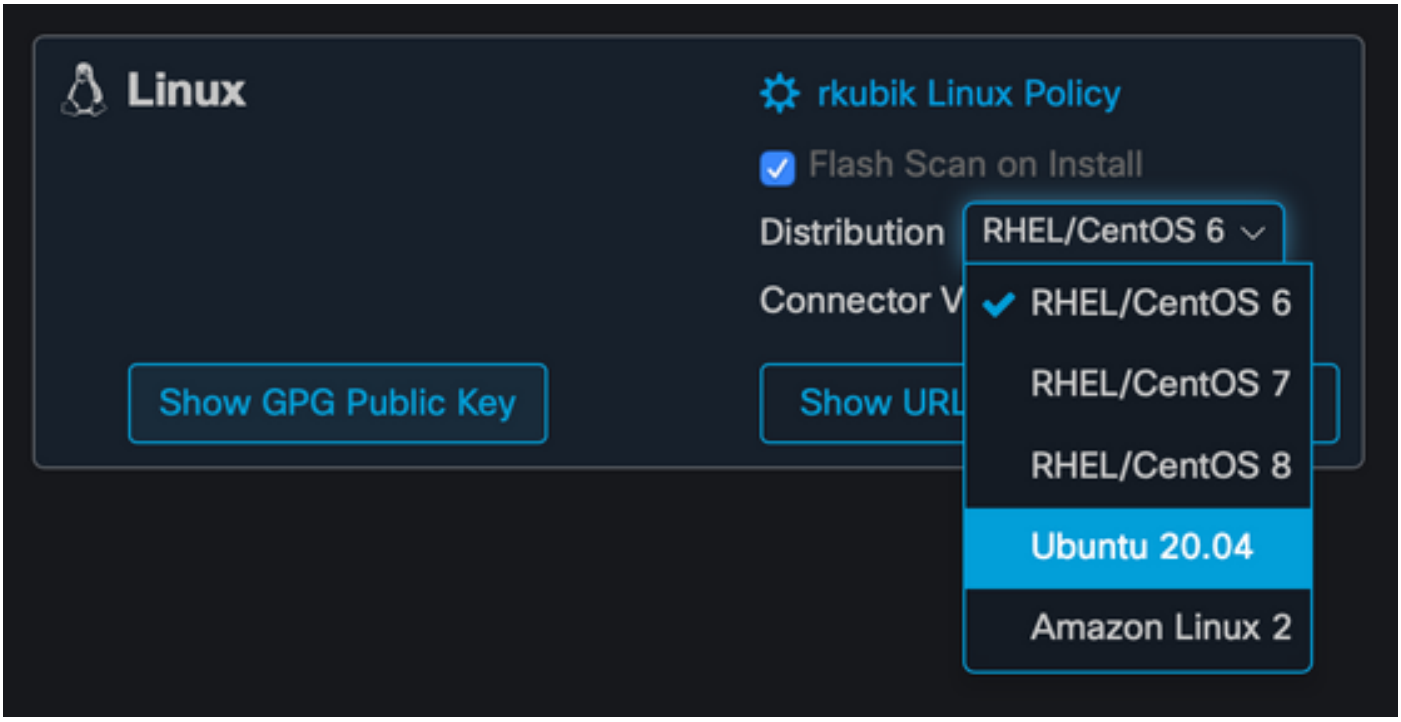
البرنامج الخفي الخاص بالنظام وعند توفر تحديث، يتم تشغيل عملية ترقية RPM تلقائيا. تمنع بعض تكوينات SELinux هذا السلوك وتتسبب في فشل المحدث.

إذا كنت تشك في أن هذه هي الحالة، افحص سجل التدقيق الخاص بالنظام (على سبيل المثال، **/var/log/audit/audit.log**) وابحث عن أحداث الرفض المتعلقة بالجهاز العميل. قد تحتاج إلى ضبط قواعد SELinux للسماح ل Updater بالعمل.

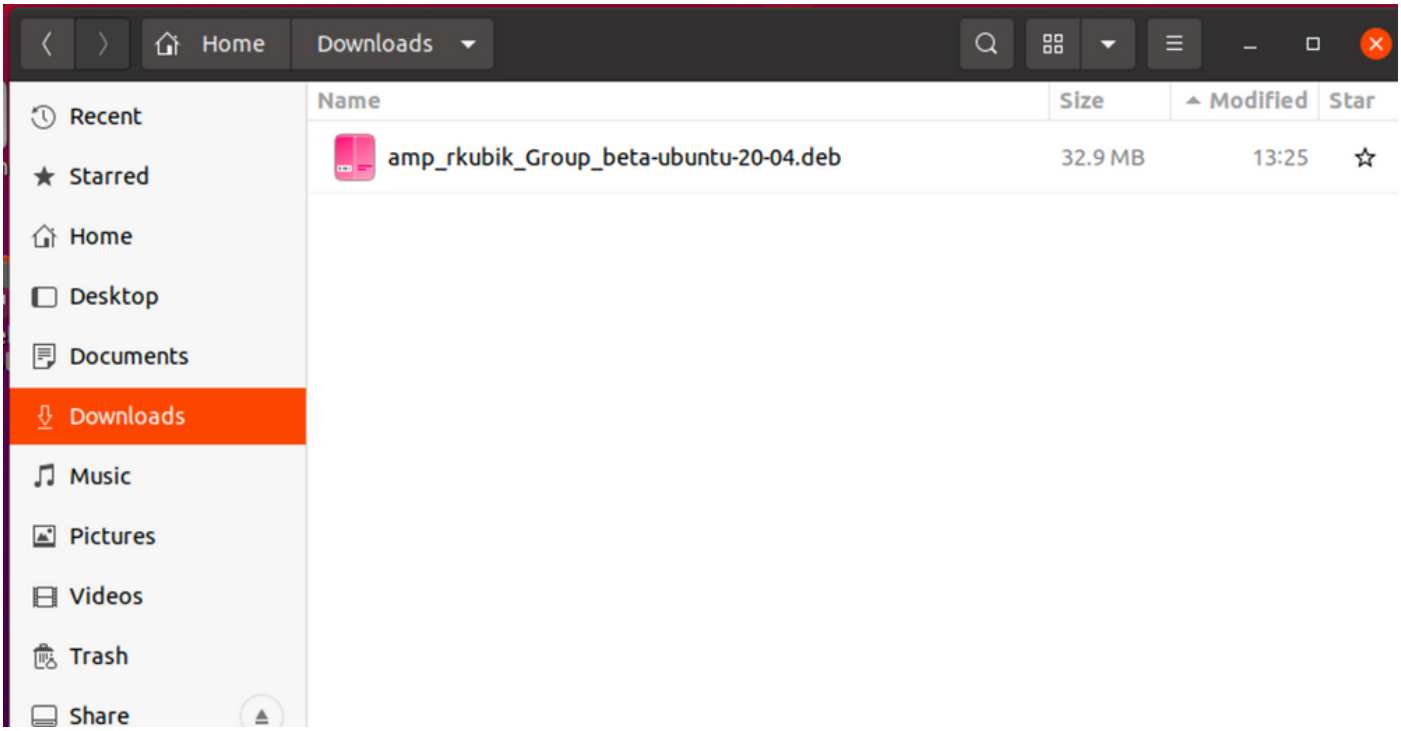
وأوبونتو

التكوينات

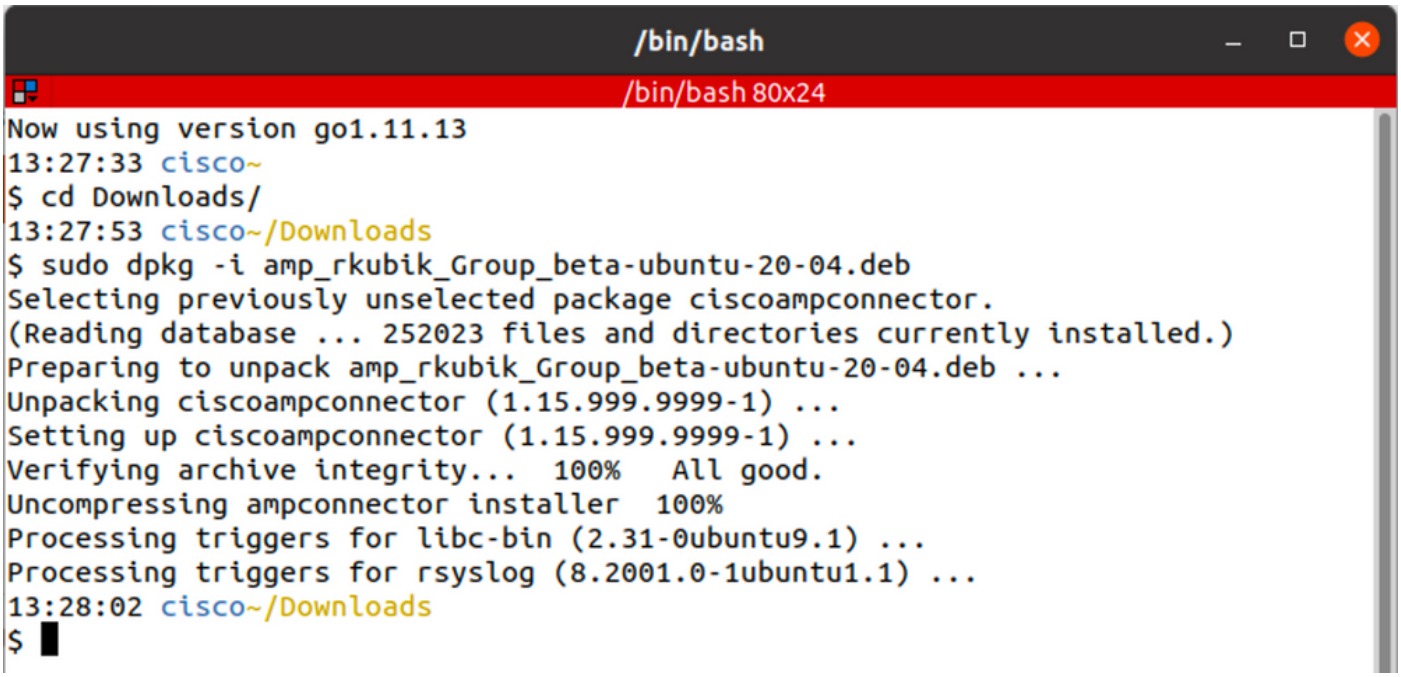
الخطوة 1. قم بتنزيل حزمة Linux DEB من بوابة نقطة النهاية الآمنة من Cisco، كما هو موضح في الصورة.



الخطوة 2. انقل حزمة DEB إلى نقطة النهاية المعنية، إما أن تقوم بتنزيلها مباشرة من لوحة المعلومات أو أن تنقلها يدويا إلى نقاط النهاية. على سبيل المثال، يتم إستخدام واجهة مستخدم رسومية (UI)، رغم أنه من الممكن، وغالبا ما يكون شائعا، العمل بأقل تثبيت، وفي هذه الحالة، يلزم معرفة كيفية التعامل مع محطة ليونكس الطرفية والعثور على حزمة DEB الخاصة بها.



الخطوة 3. لتثبيت موصل Linux، قم بتنفيذ الأمر: **sudo dpkg -i [حزمة deb]** حيث يكون [حزمة deb] هو اسم الملف، على سبيل المثال، "amp_audit.deb". بمجرد بدء التثبيت، ال يتطلب أي إدخال مستخدم، فهي عملية تلقائية، كما هو موضح في الصورة.



كيفية إستيراد مفتاح GPG

يمكن نسخ مفتاح GPG العام من صفحة تنزيل الموصل للتحقق من توقيع حزمة DEB. يمكن تثبيت الموصل بدون مفتاح GPG، ومع ذلك، سيحتاج المستخدم إلى إستيراد مفتاح GPG إلى حلقة مفاتيح DEBSIG الخاصة به إذا كان يخطط لدفع تحديثات الموصل عبر نهج Ubuntu. لمزيد من المعلومات حول كيفية إستيراد مفتاح GPG والتحقق من عدم تعديل الموصل على Ubuntu، راجع https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/216524-amp-for-endpoints-ubuntu-connector.html#anc6

ملاحظة: ابتداء من الإصدار 1.17.0 من الموصل، يتم تثبيت مفتاح GPG المستخدم للتحقق من حزم الترقية أثناء تثبيت تحديثات الموصل تلقائيا. للتحقق من مفتاح GPG هذا،

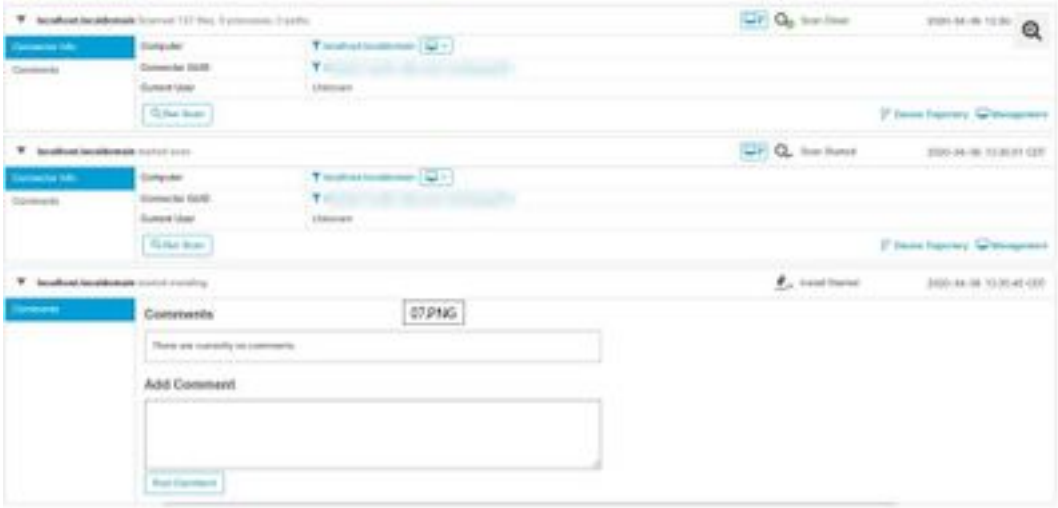
انقر فوق إرتباط مفتاح GPG العام في صفحة Download Connector وقارنه بالمفتاح الذي تم تثبيته في /opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-Key-cisco-amp.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

للتحقق من التثبيت الناجح، قم بتشغيل واجهة سطر أوامر AMP. يمكن العثور على واجهة سطر الأوامر لموصل Linux في /opt/cisco/amp/bin/ampcli. يمكن تشغيله في الوضع التفاعلي أو تنفيذ أمر واحد ثم الإنهاء. قم بتشغيل الأمر ./ampcli — ساعد على رؤية قائمة كاملة من الخيارات والأوامر المتوفرة. يمكن العثور على جميع ملفات السجل التي تم إنشاؤها بواسطة الموصل في /var/log/cisco.

يظهر حدث تثبيت أيضا على وحدة التحكم الآمنة من Cisco، إذا كان قد تم طلب عمليات مسح خاطف عند تنزيل حزمة RPM، فإنها تظهر أيضا.



استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- قم بتركيب AMP لموصل نقاط النهاية في فيديو ليزوكس
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).