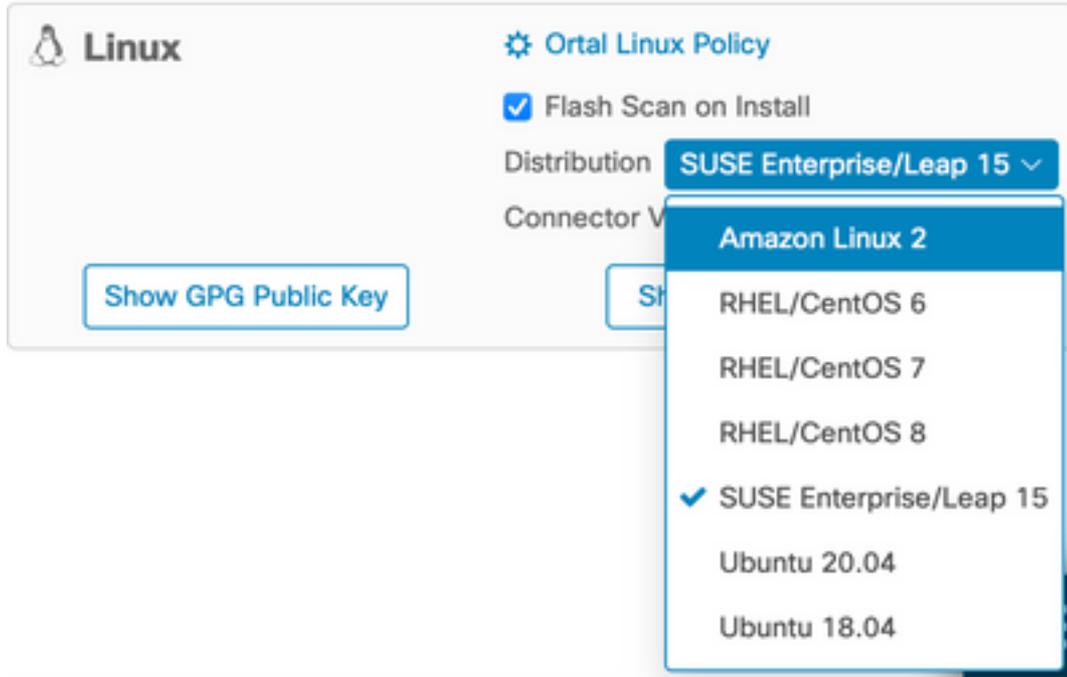


RHEL/CentOS/Amazon Linux 2/SUSE 15 لي غشت لى ماظن

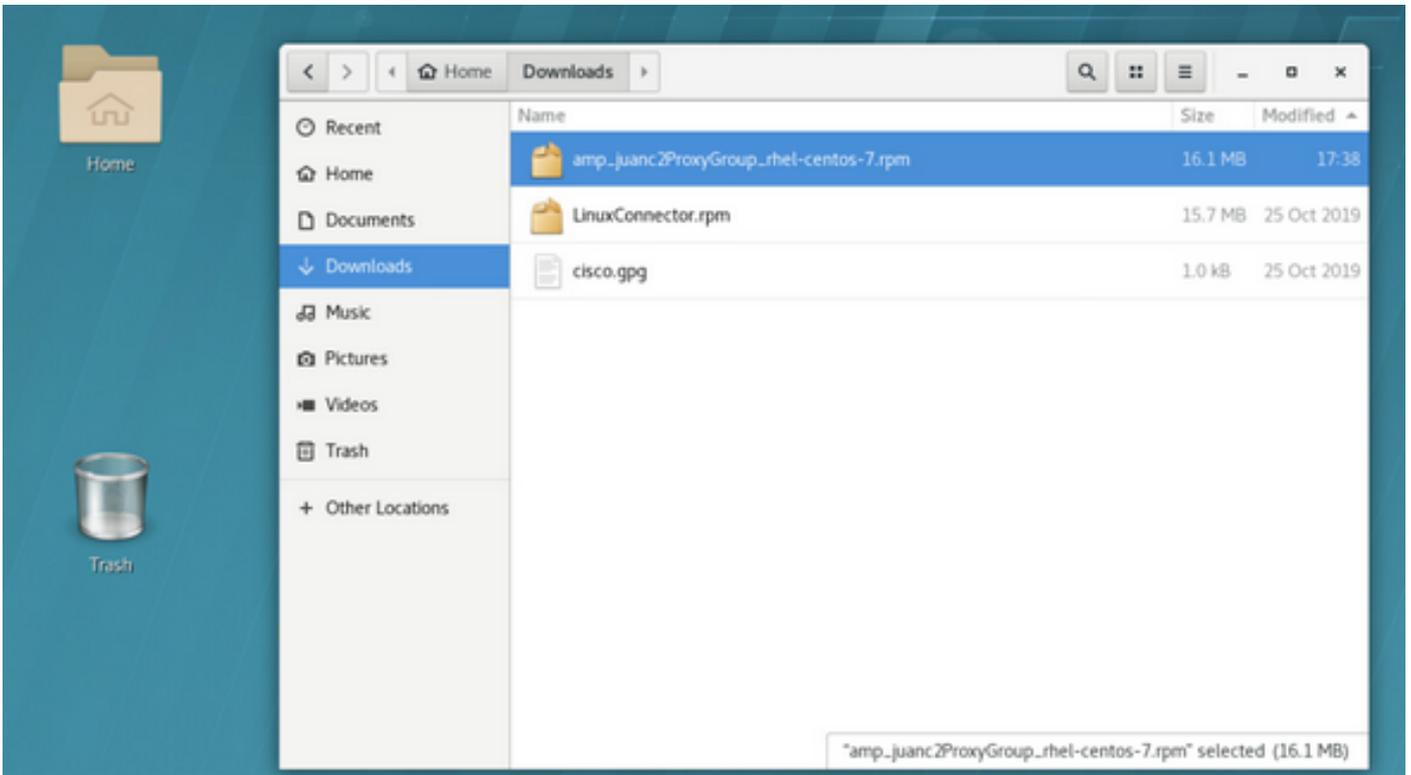
تاني وك تلى

وه امك، Cisco، نم ة نم آلا ة ياهن لى ة طقن ة باوب نم Linux نم RPM ة مزح لى زنتب مق 1. ة و طخ لى ة روص لى ف ح صوم.



امهل نى ف لى تخم لى نى لى صوم لى الك نأ لى مهم لى غشت لى ماظن عى زوت نأ ركذت: **ة طخ لى م** رى بى لى ك ش ب ة ف لى تخم تاي ن ب.

ة رشابم اهل لى زنتب موقت نأ ام، ة ي نى عمل ة ياهن لى ة طقن لى RPM ة مزح لى قن ب مق 2. ة و طخ لى م اذ خت س ا م تى، ل ا ث م ل لى ب س لى لى. ة ياهن لى طاقن لى لى اى و دى اهل قنت نأ و ا ت ا م و لى عمل ة ح و لى نم لى ق ا ب لى م لى، ا ب لى لى عى ا ش لى و، نى ك م لى نم ه ن ا نم م غ ر لى لى، (UI) ة ي م و س ر م د خ ت س م ة ه ج ا و س ك و نى لى ة ط ح م ع م لى م ا ع ت لى ة ي ف ي ك ة ف ر ع م لى ة ب و لى ط م ا ه ن ا ف، ة ل ا ح لى ه ذ ه لى ف و، تى ب ت ت م ه ب ة ص ا خ لى RPM ة مزح لى لى ر و ث ع لى و ة ي ف ر ط لى.



إلحم Sudo yum جمانرب تيبتت: رمالا ذيفنتب مق، Linux لصوم تيبتت لجا نم 3. ةوطخلال SUSE 15) لىل [RPM ةمزح] Sudo Zypper -y جمانرب تيبتت (وا [RPM ةمزح] -y)

RPM ةمزح تيبتت بجي، "amp_Audit.rpm"، لاثمالا لىبس لىل، فللما مسا وه [RPM ةمزح] شيح ATD. ةمدخ ليغشت ءانثأ

```

File Edit View Search Terminal Help
[jesuitar@jesuitar-11m-aaa-lab Downloads] sudo yum localinstall amp_juanc2ProxyGroup_rhel-centos-7.rpm -y
[sudo] password for jesuitar:
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

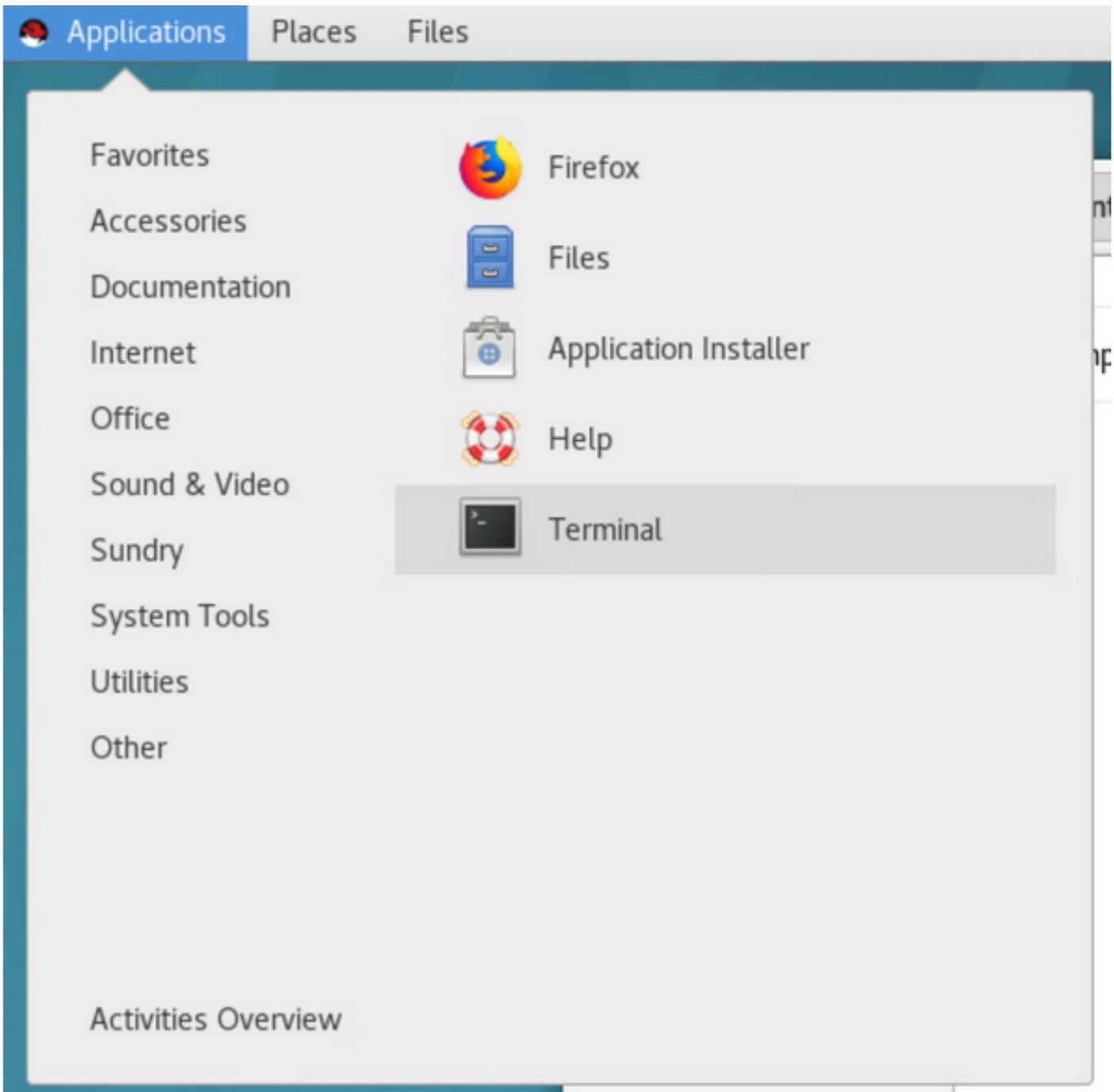
Dependencies Resolved

=====
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/rtc/policy.xml.unsaved

```

يف حضورم وه امك، ةيفرطالا ةدحولال حتفا، مادختسالال ديقي ةيموسرلا مدختسملال ةهجاو تناك اذا ةروصلال.



في حضوره وه امك ،ةيئاقلت ةيلمع يهف ،مدختسم لاخداي بلطتي ال ،تيثتال ادب درجمب ةروصل.

```
File Edit View Search Terminal Help
ipating:
ciscoampconnector x86_64 1.12.2.602-1.el7 /amp_juanc2ProxyGroup_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
Cleanup : ciscoampconnector-1.12.2.630-1.el7.x86_64 2/2
Verifying : ciscoampconnector-1.12.2.602-1.el7.x86_64 1/2
Verifying : ciscoampconnector-1.12.2.630-1.el7.x86_64 2/2

Updated:
ciscoampconnector.x86_64 0:1.12.2.602-1.el7
Complete!
[[jcsutor@jesutarr-1in-mex-lab Downloads]$
```

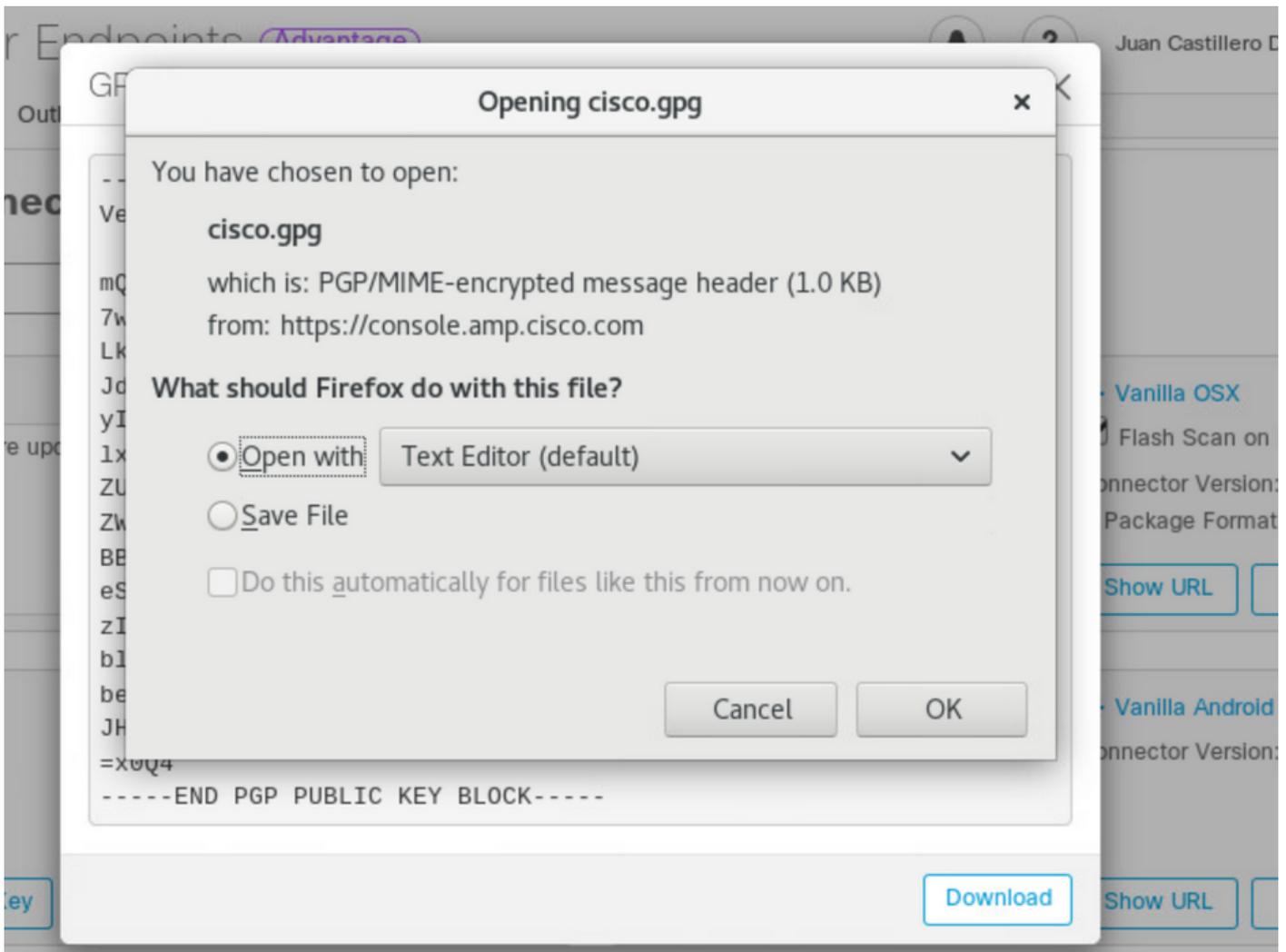
حاجات فم داريتسا في ك

RPM مزمح عي قوت نم ققحتلل لوصوملا ليزنت ةحفص نم ماعلا GPG حاجات فم خسن نكمي حاجات فم داريتسا لىل حاجت دق مدختسم ،كلذ عمو ؛GPG حاجات فم نودب لوصوملا تيبتت نكمي ربع لوصوملا تاثيردحت ع فدل ططخت تناك اذا اهب ةصاخلا RPM تانايب ةدعاق لىل GPG رهلل ةساي.

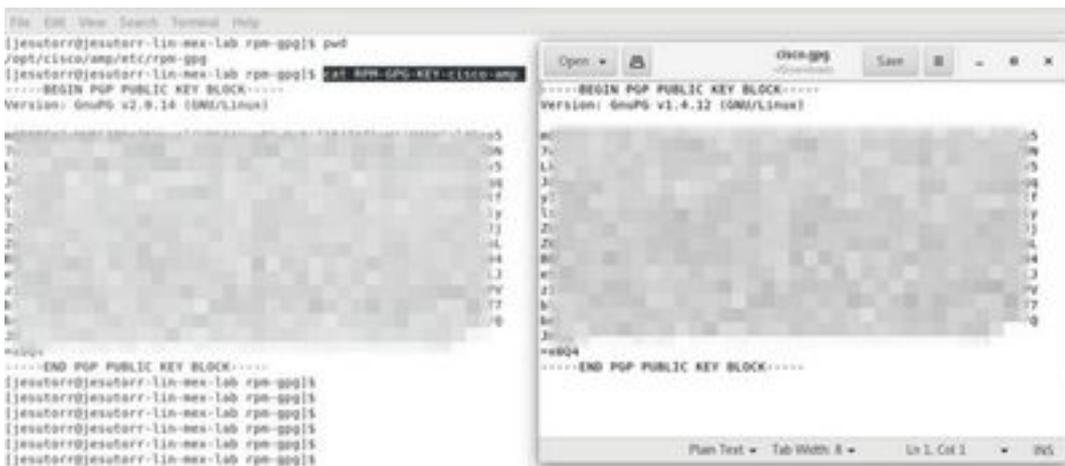
ققحتلل مدختسملا GPG حاجات فم تيبتت متي ،لوصوملا نم 1.17.0 رادصلا نم عادتبا :**ةظحالم** ايئاقلت لوصوملا تاثيردحت تيبتت اناثا ةيقرتلا مزمح نم

ليزنت ةحفص في ماعلا GPG حاجات فم طابتر ا قوف رقنا ،GPG حاجات فم نم ققحت 1. ةوطخلا لىل لوصوملا `at/opt/cisco/amp/etc/rpm-gpg/rpm-gpg-key-cisco-amp` حاجات فم لابق لوصوملا .





2. عوطخلال: حاتفملا داري ت سال ةي فرط ة دحو نم رمالا لي غشتب مق `sudo rpm --import /opt/cisco/amp/etc/rpm-gpg/RPM-gpg-key-cisco-amp`.



3. عوطخلال: ةي فرطال ا طحملال نم رمالا لي غشتب مق ، حاتفملا تي بثت نم ق قحت `rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} -> %{summary}\n'`.



4. عوطخلال: ة س اوب ث دحملال لي غشت متي . جارخالال ي Sourcefire نم GPG حاتفملا نع ث حبا.

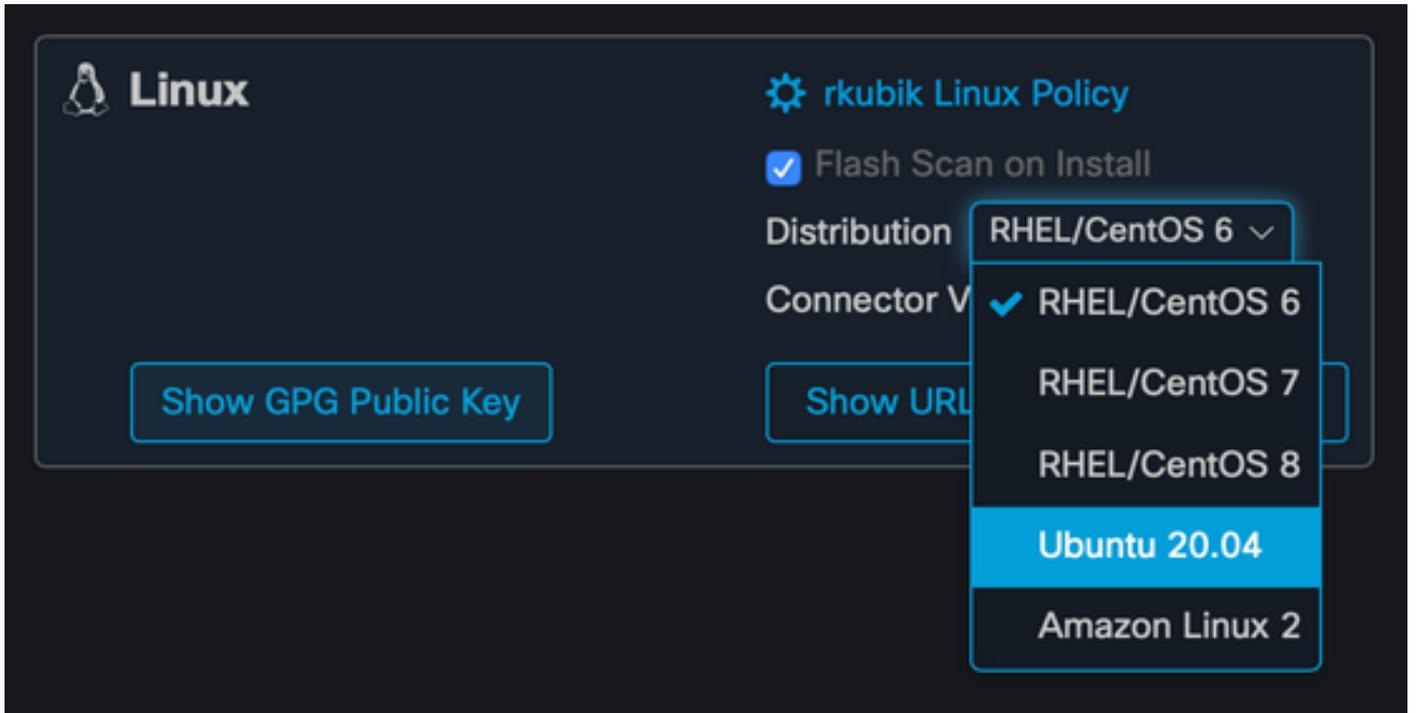
RPM ةيقرت ةيلمع ليغشت متي ،ثيدحت رفوت دنعو ماطنلاب صاخلا يفخلا جم انربلا
ثدحلال ش ف ي ف ببستتوكولسالا اذه SELinux تانيوكت ضعب عنمت .ايئاقلت

ل ببس يلع) ماطنلاب صاخلا قيقدتلا لجس صحفاف ،ةلاحلا يه هذه نأ يف كشت تنك اذا
جاتحت دق .للمعلا زاهجلا بةقلعتملا ضفرلا ثادحأ نع ثحباو (/var/log/audit/audit.log ،لاثملا
للمعلا Updater ل حامسلا ل SELinux دعاوق طبض يلا

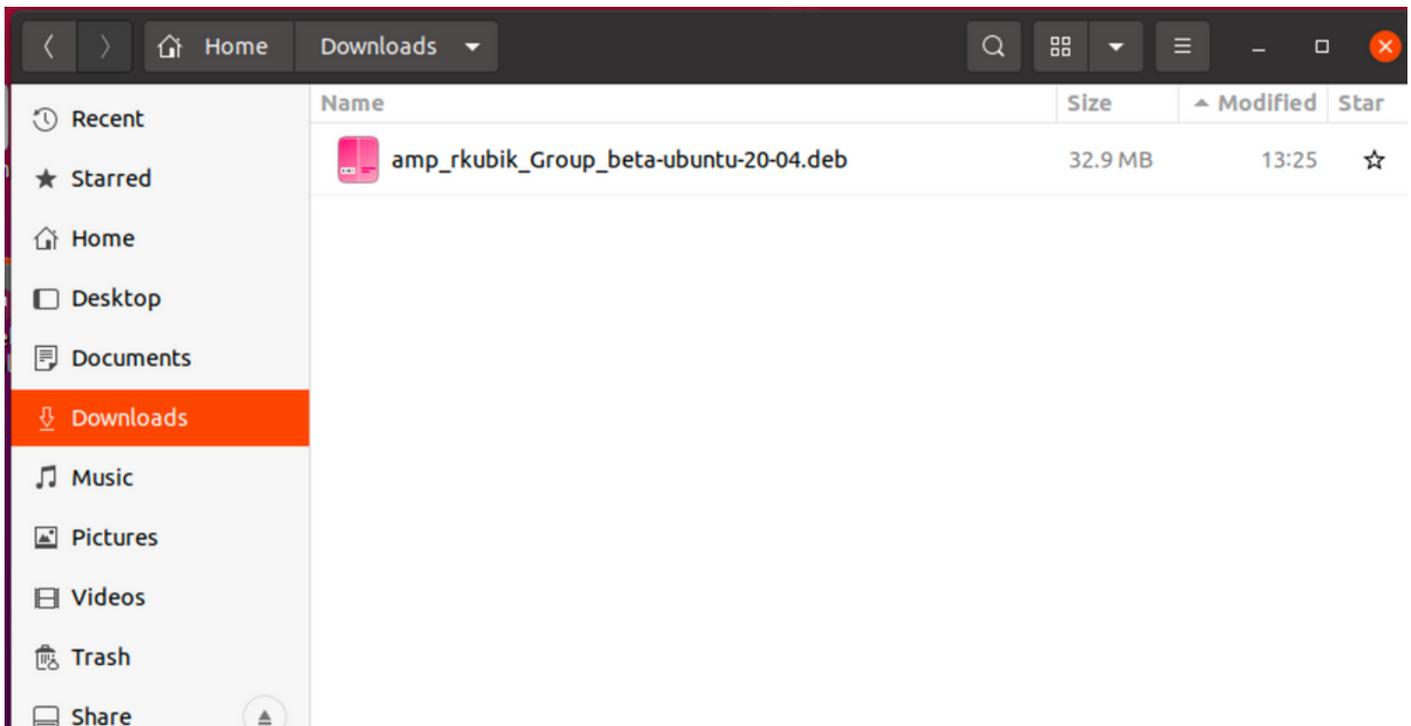
وتنوبوأ

تانيوكتلا

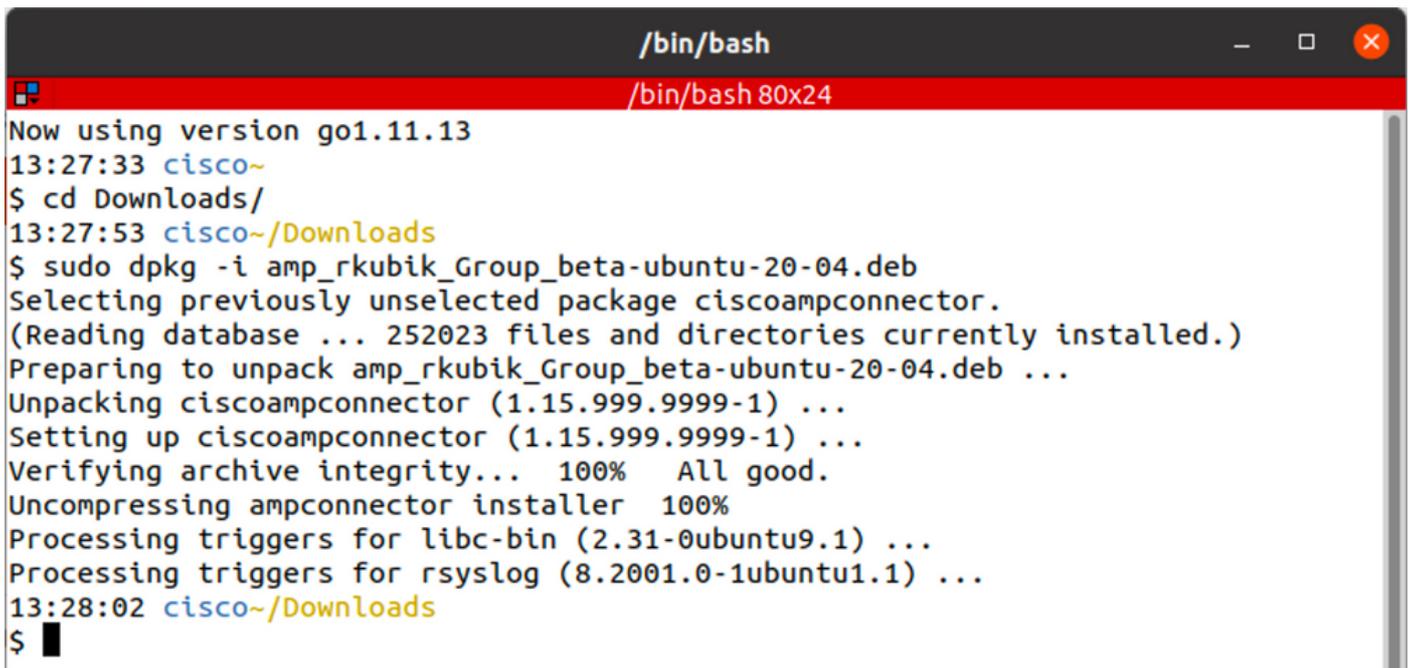
حضوم وه امك ،Cisco نم ةنمآلا ةياهنلا ةطقن ةباب نم Linux DEB ةمزح لي زنتب مق 1. ةوطخلا
ةروصلا يف



نم ةرشابم اهلي زنتب موقت نأ ام ،ةينعمل ةياهنلا ةطقن يلا DEB ةمزح لقنا 2. ةوطخلا
مادختسا متي ،لاثملا لببس يلع .ةياهنلا طاقن يلا ايودي اهلقنت نأ وأ تامولعمل ةحول
،تيتبثت لقاب لمعل ،اعئاش نوكي ام ابلاغو ،نكمملا نم هنا مغر ،(UI) ةيموسر مدختسم ةهجاو
ةمزح يلع روثعلاو ةيفرطلا سكونيل ةطحم عم لماعتلا ةيفيك ةفرعم مزلي ،ةلاحلا هذه يفو
اهب ةصاخلا DEB



ةمزح] نو كي شح [ةمزح] `sudo dpkg -i`: رمألا ذيفن تب مق Linux ل صوم تي بتل 3. ةوطخل
بلطتي ال، تي بتل ادب درجم ب. "amp_audit.deb"، ل اثم ل ل بس يلع، فللمل مسا وه [ةمزح] deb
ةروصل ي ف ح صوم وه امك، ةي اقلت ةي لمع ي هف، مدختسم لاخذ ا ي



GPG حاتم داريتس ا ةي فيك

DEB ةمزح عي قوت نم ققحتل ل ل صوم ل ليزنت ةحفص نم ماعل GPG حاتم خسن نكم ي
حاتم داريتس ا ي ل مدختسم ل ا حاحيس، كلذ عم و، GPG حاتم نودب ل صوم ل تي بتل نكم ي
جهن ربع ل صوم ل ا تاثير دحت ع فدل طاطخي ناك اذا هب ةصاخل DEBSIG حياتم ةقلح ي ل GPG
ليدعت مدع نم ققحتل ل او GPG حاتم داريتس ا ةي فيك لوح تامولعمل نم ديزمل Ubuntu.
عجار، <https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/216524-amp-for-endpoints-ubuntu-connector.html#anc6>

ققحتل ل مدختسم ل GPG حاتم تي بتل متي، ل صوم ل نم 1.17.0 رادص ا نم عادتبا: **ةظحال م**
اذه، GPG حاتم نم ققحتل ل. اي اقلت ل صوم ل ا تاثير دحت تي بتل ا نثا ةي قرتل ل مزح نم

يذلل حاتفم لابل ه نراقو Download Connector حاتفم طاب ترا قوف رقنا
م ت ي ه ت ي ب ث ت م /opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-Key-cisco-amp.

ة ح ص ل ا ن م ق ق ح ت ل ا

ح ح ص ل ك ش ب ن ي و ك ت ل ا ل م ع د ي ك أ ت ل م س ق ل ا ا ذ ه م د خ ت س ا

ة ح ا و ي ل ع ر و ث ع ل ا ن ك م ي . AMP ر م ا و ا ر ط س ة ه ج ا و ل ي غ ش ت ب م ق ، ح ج ا ن ل ا ت ي ب ث ت ل ا ن م ق ق ح ت ل ا ل
ع ض و ل ا ي ف ه ل ي غ ش ت ن ك م ي . /opt/cisco/amp/bin/ampcli ي ف Linux ل ص و م ل ر م ا و ا ل ا ر ط س
م ة ئ ا ق ة ي ؤ ر ي ل ع د ع ا س — .ampcli ر م ا ل ا ل ي غ ش ت ب م ق . ء ا ه ن ا ل م ث د ح ا و ر م ا ذ ي ف ن ت و ا ي ل ع ا ف ت ل ا
م ت ي ت ل ل ج س ل ا ت ا ف ل م ع ي م ج ي ل ع ر و ث ع ل ا ن ك م ي . ة ر ف و ت م ل ا ر م ا و ا ل ا ت ا ر ا ي خ ل ا ن م ة ل م ا ك
م ت ي ت ل ل ج س ل ا ت ا ف ل م ع ي م ج ي ل ع ر و ث ع ل ا ن ك م ي . ة ر ف و ت م ل ا ر م ا و ا ل ا ت ا ر ا ي خ ل ا ن م ة ل م ا ك
م ت ي ت ل ل ج س ل ا ت ا ف ل م ع ي م ج ي ل ع ر و ث ع ل ا ن ك م ي . ة ر ف و ت م ل ا ر م ا و ا ل ا ت ا ر ا ي خ ل ا ن م ة ل م ا ك
م ت ي ت ل ل ج س ل ا ت ا ف ل م ع ي م ج ي ل ع ر و ث ع ل ا ن ك م ي . ة ر ف و ت م ل ا ر م ا و ا ل ا ت ا ر ا ي خ ل ا ن م ة ل م ا ك

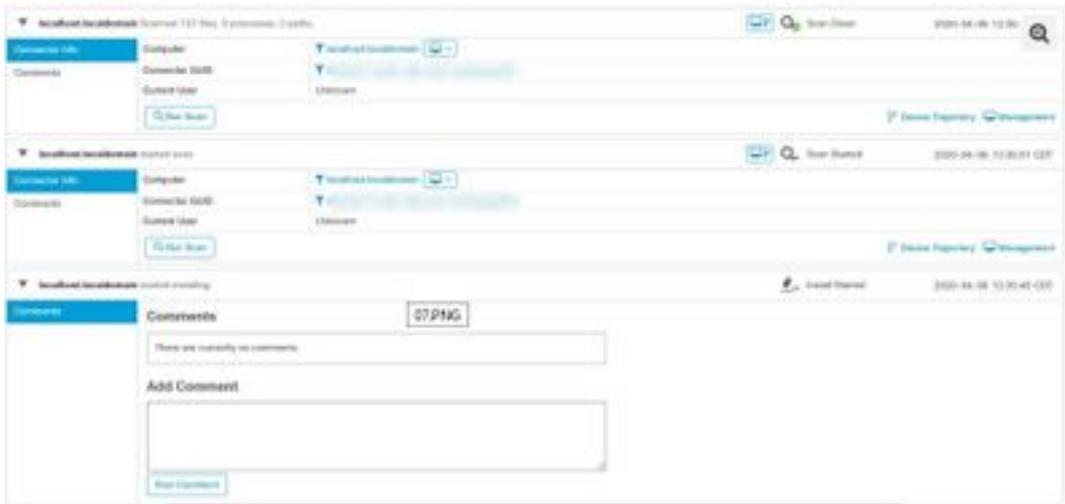
```
File Edit View Search Terminal Help
[jesuiter@jesuiter-lin-osa-lab ~]$ cd /opt/cisco/amp/bin/
[jesuiter@jesuiter-lin-osa-lab bin]$ pwd
/opt/cisco/amp/bin
[jesuiter@jesuiter-lin-osa-lab bin]$ ls
ampcli  ampcli.rpm  ampcli.rpm.gpg  cisco-amp-helper  libclamav.so.0  libclamav.so.0.10.0  libclamav.so.0.10.0.rpm
ampcli.rpm.gpg  ampcli.rpm.gpg.gpg  ampcli.rpm.gpg.gpg  libclamav.so.0.10.0  libclamav.so.0.10.0.rpm
[jesuiter@jesuiter-lin-osa-lab bin]$ ./ampcli

ampcli - AMP for Endpoints Connector Command Line Interface
Interaction 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: 2020-02-20 02:26 PM
Policy: Jabarra-Linux (823268)
Command Line: Enabled
Fails: None
ampcli>
```

ح س م ت ا ي ل م ع ب ل ط م ت د ق ن ا ك ا ذ ا ، Cisco ن م ة ن م ا ل م ك ح ت ل ا ة د ح و ي ل ع ا ض ي ا ت ي ب ث ت ش د ح ر ه ظ ي
ا ض ي ا ر ه ظ ت ا ه ن ا ف ، RPM ة م ز ح ل ي ز ن ت د ن ع ف ط ا خ



ا ه ح ا ل ص ا و ا ط خ ا ل ا ف ا ش ك ت س ا

ن ي و ك ت ل ا ا ذ ه ل ا ه ح ا ل ص ا و ا ط خ ا ل ا ف ا ش ك ت س ا ل ة د د ح م ت ا م و ل ع م ا ي ل ا ح ر ف و ت ت ا ل

ة ل ص ت ا ذ ت ا م و ل ع م

- [س ك و ن ي ل و ي د ي ف ي ف ة ي ا ه ن ل ا ط ا ق ن ل ص و م ل AMP ب ي ك ر ت ب م ق](#)
- [Cisco Systems - ت ا د ن ت س م ل ا و ي ن ق ت ل ا م ع د ل ا](#)

