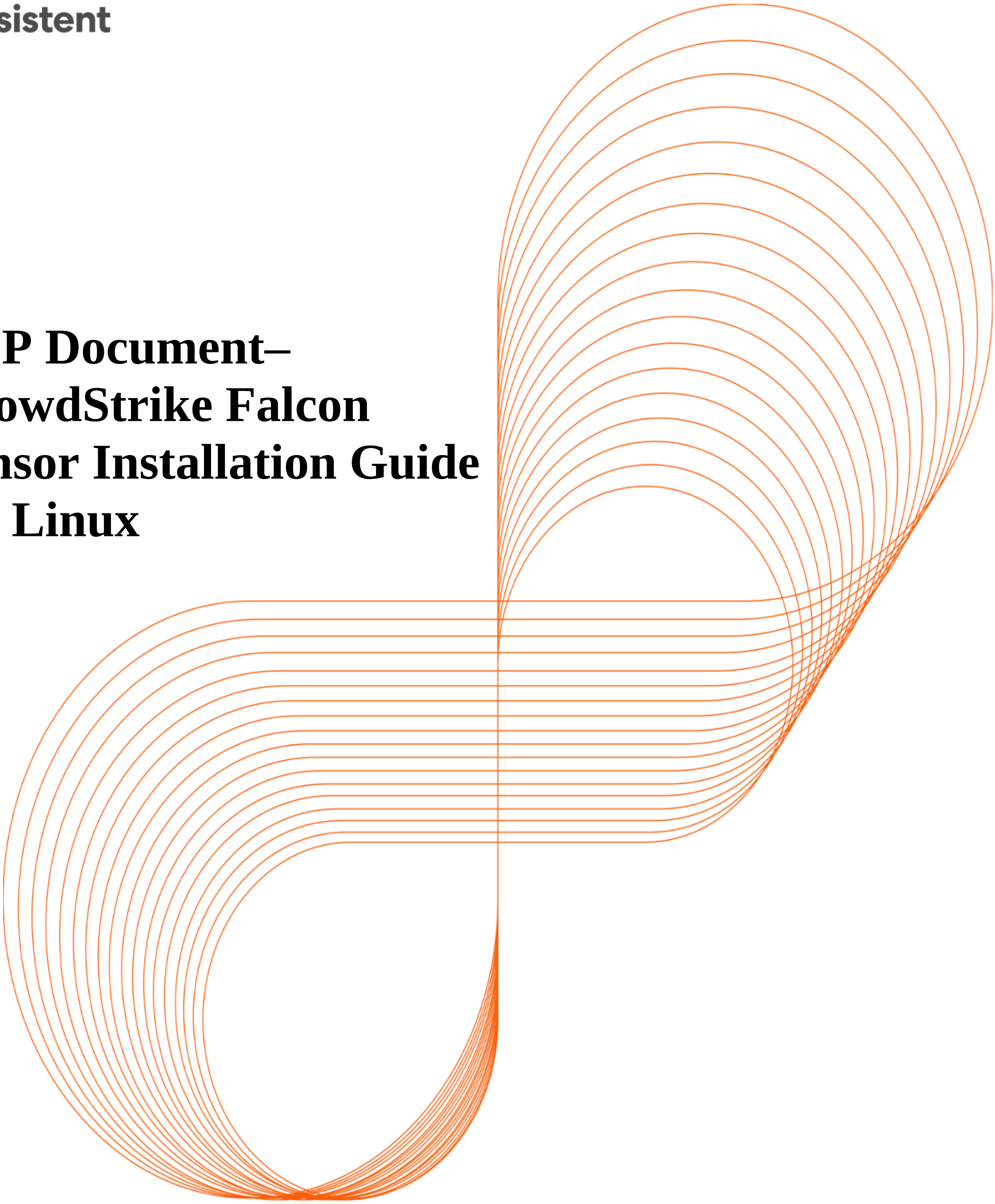
SOP Document– CrowdStrike Falcon Sensor Installation Guide for Linux



Document Control

Document Name	SOP Document – CrowdStrike Falcon Sensor Installation Guide for Linux
Executive Summary	This document provides information regarding CrowdStrike Falcon Sensor Installation in Persistent environment
Revision no.	1.0
Effective from date	09-Jan-2023
Classification	Internal Use Only

Authorization

Owner	EIS System & Security Team

Revision History

Revision	Description	Reviewed By	Approved By & Date	Effective Date
1.0	Initial Draft	Vishal J. Pilliwar	Dinesh Pardeshi	09 Jan 2023

CONTENTS

CROWDSTRIKE FALCON SENSOR AGENT INSTALLATION ON UBUNTU

To install the Falcon sensor on the nodes, perform these procedures:

- Installing the Falcon sensor.
- Verifying the installation.

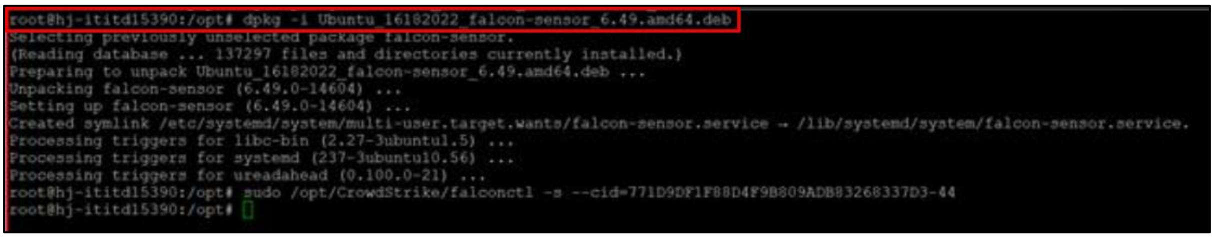
Installing the Falcon sensor

1. Download or copy the package from below Central path to the Linux host
   CrowdStrike Agent Setup

2. Run the installer, substituting **Ubuntu 16182022 falcon-sensor_6.49.0-14604_amd64.deb** with your installer's file name.

   Installing the sensor requires sudo privileges.

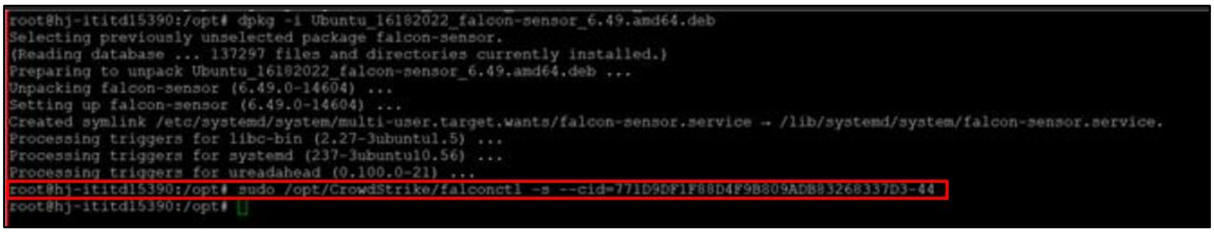
   - Ubuntu: **sudo dpkg -i Ubuntu 16182022 falcon-sensor_6.49.0-14604_amd64.deb**



```
root@hj-ititd15390:/opt# dpkg -i Ubuntu_16182022_falcon-sensor_6.49.amd64.deb
Selecting previously unselected package falcon-sensor.
(Reading database ... 137297 files and directories currently installed.)
Preparing to unpack Ubuntu_16182022_falcon-sensor_6.49.amd64.deb ...
Unpacking falcon-sensor (6.49.0-14604) ...
Setting up falcon-sensor (6.49.0-14604) ...
Created symlink /etc/systemd/system/multi-user.target.wants/falcon-sensor.service → /lib/systemd/system/falcon-sensor.service.
Processing triggers for libc-bin (2.27-3ubuntu1.5) ...
Processing triggers for systemd (237-3ubuntu10.56) ...
Processing triggers for ureadahead (0.100.0-21) ...
root@hj-ititd15390:/opt# sudo /opt/CrowdStrike/falconctl -s --cid=771D9DF1F88D4F9B809ADB83268337D3-44
root@hj-ititd15390:/opt# 
```

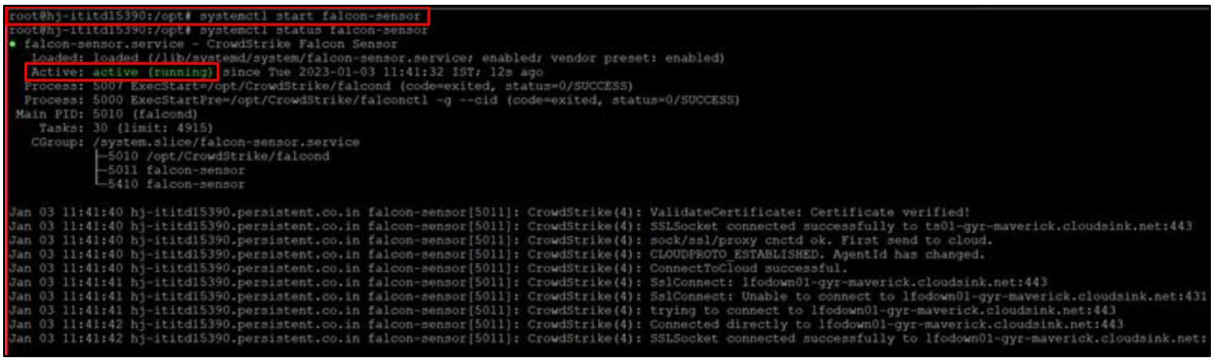
3. After Installing the sensor Activate using below command:

sudo /opt/CrowdStrike/falconctl -s -cid=771D9DF1F88D4F9B809ADB83268337D3-44



```
root@hj-ititd15390:/opt# dpkg -i Ubuntu_16182022_falcon-sensor_6.49.amd64.deb
Selecting previously unselected package falcon-sensor.
(Reading database ... 137297 files and directories currently installed.)
Preparing to unpack Ubuntu_16182022_falcon-sensor_6.49.amd64.deb ...
Unpacking falcon-sensor (6.49.0-14604) ...
Setting up falcon-sensor (6.49.0-14604) ...
Created symlink /etc/systemd/system/multi-user.target.wants/falcon-sensor.service → /lib/systemd/system/falcon-sensor.service.
Processing triggers for libc-bin (2.27-3ubuntu1.5) ...
Processing triggers for systemd (237-3ubuntu10.56) ...
Processing triggers for ureadahead (0.100.0-21) ...
root@hj-ititd15390:/opt# sudo /opt/CrowdStrike/falconctl -s --cid=771D9DF1F88D4F9B809ADB83268337D3-44
root@hj-ititd15390:/opt# 
```

4. Start the sensor manually. This step is not required for versions 4.0 and earlier.
   - Hosts with SysVinit: sudo service falcon-sensor start
   - Hosts with Systemd: sudo systemctl start falcon-sensor



```
root@hj-ititd15390:/opt# systemctl start falcon-sensor
root@hj-ititd15390:/opt# systemctl status falcon-sensor
● falcon-sensor.service - CrowdStrike Falcon Sensor
   Loaded: loaded (/lib/systemd/system/falcon-sensor.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-01-03 11:41:32 IST; 12s ago
  Process: 5007 ExecStart=/opt/CrowdStrike/falcond (code=exited, status=0/SUCCESS)
  Process: 5000 ExecStartPre=/opt/CrowdStrike/falconctl -g --cid (code=exited, status=0/SUCCESS)
 Main PID: 5010 (falcond)
    Tasks: 30 (limit: 4915)
   CGroup: /system.slice/falcon-sensor.service
           ├─5010 /opt/CrowdStrike/falcond
           ├─5011 falcon-sensor
           └─5410 falcon-sensor

Jan 03 11:41:40 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): ValidateCertificate: Certificate verified!
Jan 03 11:41:40 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): SSLSocket connected successfully to ts01-gyr-maverick.cloudsink.net:443
Jan 03 11:41:40 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): sock/ssl/proxy cnctd ok. First send to cloud.
Jan 03 11:41:40 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): CLOUDPROTO_ESTABLISHED. AgentId has changed.
Jan 03 11:41:40 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): ConnectToCloud successful.
Jan 03 11:41:41 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): SslConnect: lfodown01-gyr-maverick.cloudsink.net:443
Jan 03 11:41:41 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): SslConnect: Unable to connect to lfodown01-gyr-maverick.cloudsink.net:431
Jan 03 11:41:41 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): trying to connect to lfodown01-gyr-maverick.cloudsink.net:443
Jan 03 11:41:42 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): Connected directly to lfodown01-gyr-maverick.cloudsink.net:443
Jan 03 11:41:42 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): SSLSocket connected successfully to lfodown01-gyr-maverick.cloudsink.net:
```

Verifying sensor installation

You can verify an installation by using the Falcon console or a terminal on the host.

Falcon console

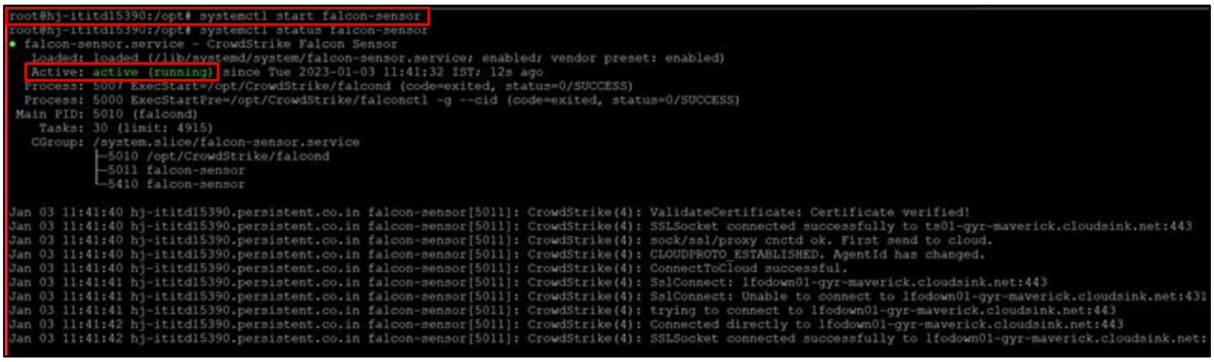
After the sensor is installed, the host connects to the Falcon console. You can confirm a sensor installation by reviewing your hosts.

To view a complete list of newly installed sensors, use the Sensor Report in the Falcon console.

Host

To validate that the Falcon sensor for Linux is running on a host, run this command at a terminal:

ps -e | grep falcon-sensor



```
root@hj-ititd15390:/opt# systemctl start falcon-sensor
root@hj-ititd15390:/opt# systemctl status falcon-sensor
● falcon-sensor.service - CrowdStrike Falcon Sensor
   Loaded: loaded (/lib/systemd/system/falcon-sensor.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-01-03 11:41:32 IST; 12s ago
  Process: 5007 ExecStart=/opt/CrowdStrike/falcond (code=exited, status=0/SUCCESS)
  Process: 5000 ExecStartPre=/opt/CrowdStrike/falconctl -g --cid (code=exited, status=0/SUCCESS)
 Main PID: 5010 (falcond)
    Tasks: 30 (limit: 4915)
   CGroup: /system.slice/falcon-sensor.service
           ├─5010 /opt/CrowdStrike/falcond
           ├─5011 falcon-sensor
           └─5410 falcon-sensor

Jan 03 11:41:40 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): ValidateCertificate: Certificate verified!
Jan 03 11:41:40 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): SSLSocket connected successfully to ts01-gyr-maverick.cloudsink.net:443
Jan 03 11:41:40 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): sock/ssl/proxy cnctd ok. First send to cloud.
Jan 03 11:41:40 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): CLOUDPROTO_ESTABLISHED. AgentId has changed.
Jan 03 11:41:40 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): ConnectToCloud successful.
Jan 03 11:41:41 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): SslConnect: lfodown01-gyr-maverick.cloudsink.net:443
Jan 03 11:41:41 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): SslConnect: Unable to connect to lfodown01-gyr-maverick.cloudsink.net:431
Jan 03 11:41:41 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): trying to connect to lfodown01-gyr-maverick.cloudsink.net:443
Jan 03 11:41:42 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): Connected directly to lfodown01-gyr-maverick.cloudsink.net:443
Jan 03 11:41:42 hj-ititd15390.persistent.co.in falcon-sensor[5011]: CrowdStrike(4): SSLSocket connected successfully to lfodown01-gyr-maverick.cloudsink.net:
```

CROWDSTRIKE FALCON SENSOR AGENT INSTALLATION ON RHEL 7

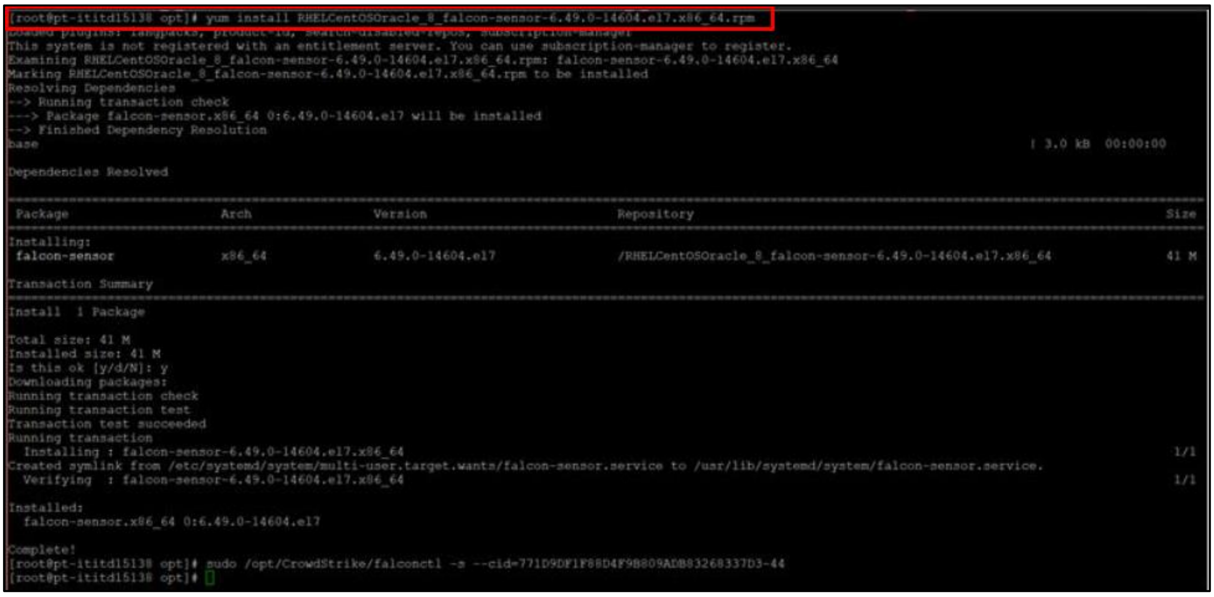
To install the Falcon sensor on the nodes, perform these procedures:

- Installing the Falcon sensor.
- Verifying the installation.

Installing the Falcon sensor

1. Download or copy the package from below Central path to the Linux host
   CrowdStrike Agent Setup

2. Run the installer, substituting **RHELCentOSOracle 7 falcon-sensor-6.49.0-14606.el7.s390x.rpm** with your installer's file name.
   - RHEL, CentOS, Amazon Linux: **sudo yum install RHELCentOSOracle 7 falcon-sensor-6.49.0-14606.el7.s390x.rpm**

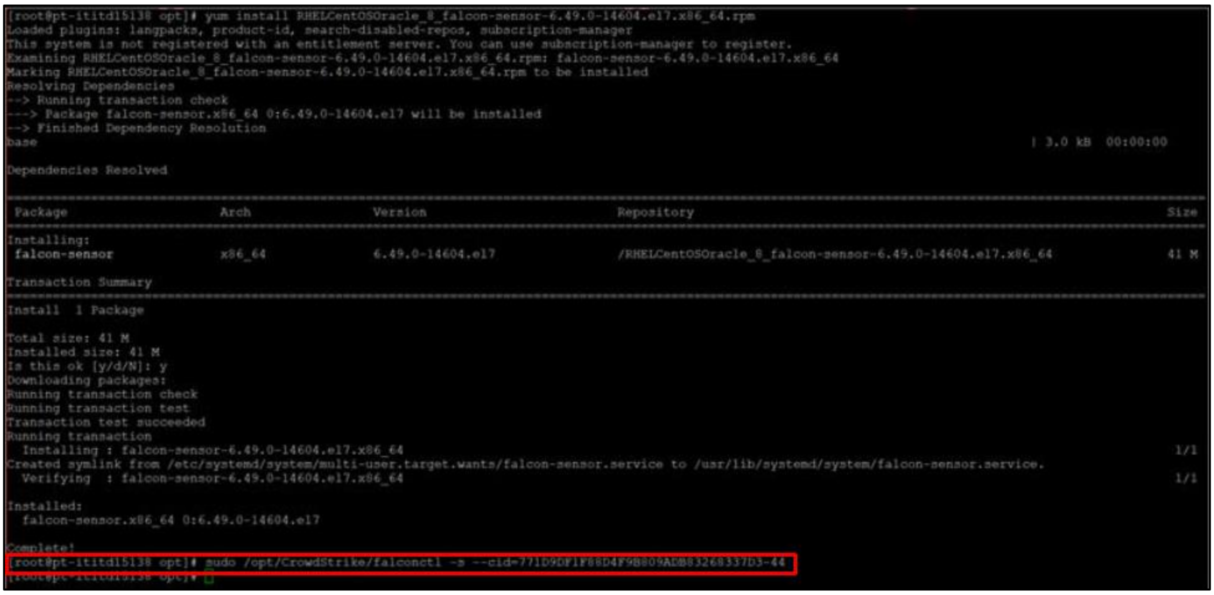


```
[root@pt-ititd15138 opt]# yum install RHELCentOSOracle_8_falcon-sensor-6.49.0-14604.el7.x86_64.rpm
Loaded plugins: langpacks, product-id, search-disabled-repos, subscription-manager
This system is not registered with an entitlement server. You can use subscription-manager to register.
Examining RHELCentOSOracle_8_falcon-sensor-6.49.0-14604.el7.x86_64.rpm: falcon-sensor-6.49.0-14604.el7.x86_64
Marking RHELCentOSOracle_8_falcon-sensor-6.49.0-14604.el7.x86_64.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package falcon-sensor.x86_64 0:6.49.0-14604.el7 will be installed
--> Finished Dependency Resolution
base                                                                                            | 3.0 kB  00:00:00

Dependencies Resolved

=====================================================================================================================
 Package               Arch             Version                    Repository                                    Size
=====================================================================================================================
Installing:
 falcon-sensor         x86_64           6.49.0-14604.el7           /RHELCentOSOracle_8_falcon-sensor-6.49.0-14604.el7.x86_64   41 M

Transaction Summary
=====================================================================================================================
Install  1 Package

Total size: 41 M
Installed size: 41 M
Is this ok [y/d/N]: y
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : falcon-sensor-6.49.0-14604.el7.x86_64                                                                1/1
Created symlink from /etc/systemd/system/multi-user.target.wants/falcon-sensor.service to /usr/lib/systemd/system/falcon-sensor.service.
  Verifying  : falcon-sensor-6.49.0-14604.el7.x86_64                                                                1/1

Installed:
  falcon-sensor.x86_64 0:6.49.0-14604.el7

Complete!
[root@pt-ititd15138 opt]# sudo /opt/CrowdStrike/falconctl -s --cid=771D9DF1F88D4F9B809ADB83268337D3-44
[root@pt-ititd15138 opt]# 
```

Note: While Installing CrowdStrike Sensor in RHEL 7, if you are getting any error then you can also use RHEL 8 package in place of RHEL 7

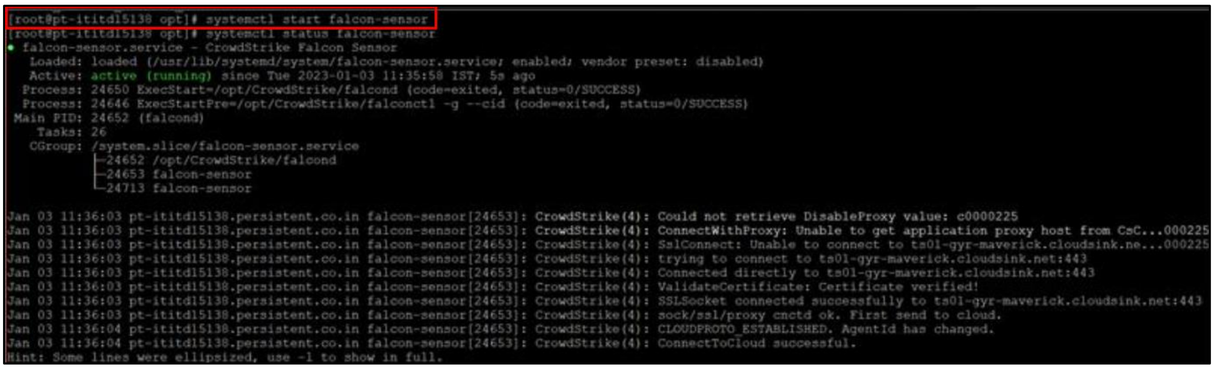
3. After Installing the sensor Activate using below command:

sudo /opt/CrowdStrike/falconctl -s -cid=771D9DF1F88D4F9B809ADB83268337D3-44



```
[root@pt-ititd15138 opt]# yum install RHELCentOSOracle_8_falcon-sensor-6.49.0-14604.el7.x86_64.rpm
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 RHELCentOSOracle_8_falcon-sensor-6.49.0-14604.el7.x86_64.rpm: falcon-sensor-6.49.0-14604.el7.x86_64
Marking RHELCentOSOracle_8_falcon-sensor-6.49.0-14604.el7.x86_64.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package falcon-sensor.x86_64 0:6.49.0-14604.el7 will be installed
--> Finished Dependency Resolution
base                                                                                                   | 3.0 kB  00:00:00

Dependencies Resolved

================================================================================================================================
 Package                   Arch               Version                     Repository                                        Size
================================================================================================================================
Installing:
 falcon-sensor             x86_64             6.49.0-14604.el7            /RHELCentOSOracle_8_falcon-sensor-6.49.0-14604.el7.x86_64   41 M

Transaction Summary
================================================================================================================================
Install  1 Package

Total size: 41 M
Installed size: 41 M
Is this ok [y/d/N]: y
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : falcon-sensor-6.49.0-14604.el7.x86_64                                                                      1/1
Created symlink from /etc/systemd/system/multi-user.target.wants/falcon-sensor.service to /usr/lib/systemd/system/falcon-sensor.service.
  Verifying  : falcon-sensor-6.49.0-14604.el7.x86_64                                                                      1/1

Installed:
  falcon-sensor.x86_64 0:6.49.0-14604.el7

Complete!
[root@pt-ititd15138 opt]# sudo /opt/CrowdStrike/falconctl -s --cid=771D9DF1F88D4F9B809ADB83268337D3-44
[root@pt-ititd15138 opt]#
```

4. Start the sensor manually. This step is not required for versions 4.0 and earlier.
    - Hosts with SysVinit: **sudo service falcon-sensor start**
    - Hosts with Systemd: **sudo systemctl start falcon-sensor**



```
[root@pt-ititd15138 opt]# systemctl start falcon-sensor
[root@pt-ititd15138 opt]# systemctl status falcon-sensor
● falcon-sensor.service - CrowdStrike Falcon Sensor
   Loaded: loaded (/usr/lib/systemd/system/falcon-sensor.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-01-03 11:35:58 IST; 5s ago
  Process: 24650 ExecStart=/opt/CrowdStrike/falcond (code=exited, status=0/SUCCESS)
  Process: 24646 ExecStartPre=/opt/CrowdStrike/falconctl -g --cid (code=exited, status=0/SUCCESS)
 Main PID: 24652 (falcond)
    Tasks: 26
   CGroup: /system.slice/falcon-sensor.service
           ├─24652 /opt/CrowdStrike/falcond
           ├─24653 falcon-sensor
           └─24713 falcon-sensor

Jan 03 11:36:03 pt-ititd15138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): Could not retrieve DisableProxy value: c0000225
Jan 03 11:36:03 pt-ititd15138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): ConnectWithProxy: Unable to get application proxy host from CsC...000225
Jan 03 11:36:03 pt-ititd15138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): SslConnect: Unable to connect to ts01-gyr-maverick.cloudsink.ne...000225
Jan 03 11:36:03 pt-ititd15138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): trying to connect to ts01-gyr-maverick.cloudsink.net:443
Jan 03 11:36:03 pt-ititd15138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): Connected directly to ts01-gyr-maverick.cloudsink.net:443
Jan 03 11:36:03 pt-ititd15138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): ValidateCertificate: Certificate verified!
Jan 03 11:36:03 pt-ititd15138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): SSLSocket connected successfully to ts01-gyr-maverick.cloudsink.net:443
Jan 03 11:36:03 pt-ititd15138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): sock/ssl/proxy cnctd ok. First send to cloud.
Jan 03 11:36:04 pt-ititd15138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): CLOUDPROTO_ESTABLISHED. AgentId has changed.
Jan 03 11:36:04 pt-ititd15138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): ConnectToCloud successful.
Hint: Some lines were ellipsized, use -l to show in full.
```

Verifying sensor installation

You can verify an installation by using the Falcon console or a terminal on the host.

Falcon console

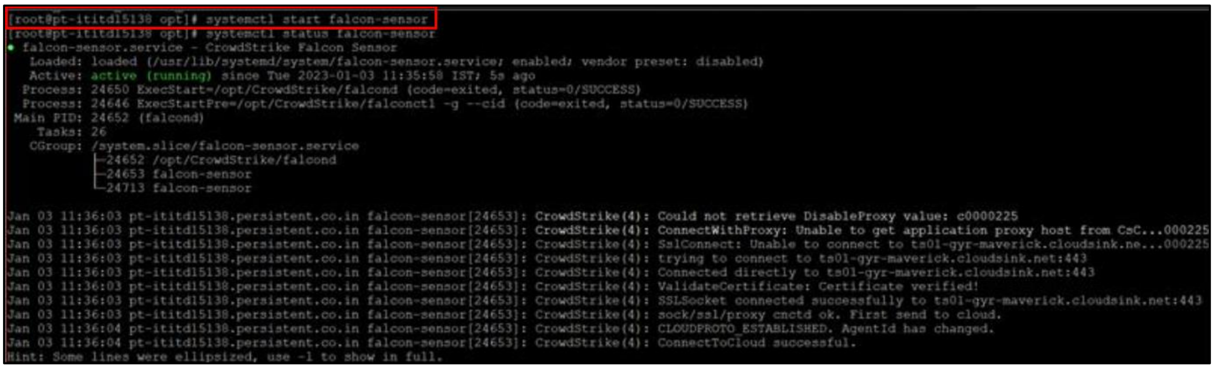
After the sensor is installed, the host connects to the Falcon console. You can confirm a sensor installation by reviewing your hosts.

To view a complete list of newly installed sensors, use the Sensor Report in the Falcon console.

Host

To validate that the Falcon sensor for Linux is running on a host, run this command at a terminal:

ps -e | grep falcon-sensor



```
[root@pt-ititdl5138 opt]# systemctl start falcon-sensor
[root@pt-ititdl5138 opt]# systemctl status falcon-sensor
● falcon-sensor.service - CrowdStrike Falcon Sensor
   Loaded: loaded (/usr/lib/systemd/system/falcon-sensor.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-01-03 11:35:58 IST; 5s ago
  Process: 24650 ExecStart=/opt/CrowdStrike/falcond (code=exited, status=0/SUCCESS)
  Process: 24646 ExecStartPre=/opt/CrowdStrike/falconctl -g --cid (code=exited, status=0/SUCCESS)
 Main PID: 24652 (falcond)
    Tasks: 26
   CGroup: /system.slice/falcon-sensor.service
           ├─24652 /opt/CrowdStrike/falcond
           ├─24653 falcon-sensor
           └─24713 falcon-sensor

Jan 03 11:36:03 pt-ititdl5138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): Could not retrieve DisableProxy value: c0000225
Jan 03 11:36:03 pt-ititdl5138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): ConnectWithProxy: Unable to get application proxy host from CsC...000225
Jan 03 11:36:03 pt-ititdl5138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): SslConnect: Unable to connect to ts01-gyr-maverick.cloudsink.ne...000225
Jan 03 11:36:03 pt-ititdl5138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): trying to connect to ts01-gyr-maverick.cloudsink.net:443
Jan 03 11:36:03 pt-ititdl5138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): Connected directly to ts01-gyr-maverick.cloudsink.net:443
Jan 03 11:36:03 pt-ititdl5138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): ValidateCertificate: Certificate verified!
Jan 03 11:36:03 pt-ititdl5138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): SSLSocket connected successfully to ts01-gyr-maverick.cloudsink.net:443
Jan 03 11:36:03 pt-ititdl5138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): sock/ssl/proxy cnctd ok. First send to cloud.
Jan 03 11:36:04 pt-ititdl5138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): CLOUDPROTO_ESTABLISHED. AgentId has changed.
Jan 03 11:36:04 pt-ititdl5138.persistent.co.in falcon-sensor[24653]: CrowdStrike(4): ConnectToCloud successful.
Hint: Some lines were ellipsized, use -l to show in full.
```

CROWDSTRIKE FALCON SENSOR AGENT INSTALLATION ON RHEL 8

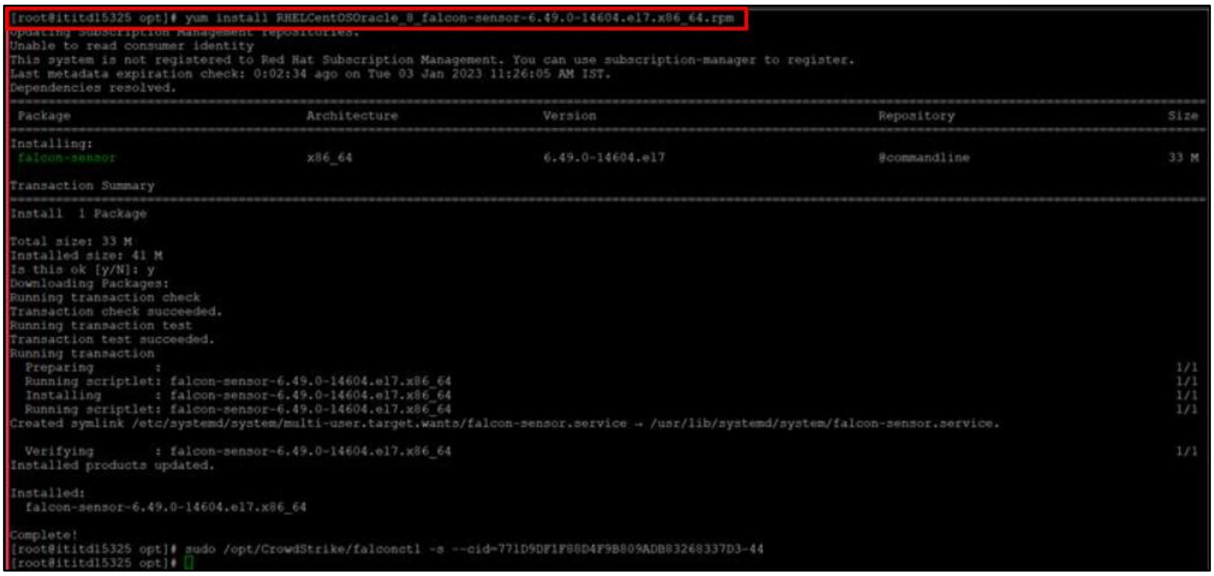
To install the Falcon sensor on the nodes, perform these procedures:

- Installing the Falcon sensor.
- Verifying the installation.

Installing the Falcon sensor

1. Download or copy the package from below Central path to the Linux host
   CrowdStrike Agent Setup

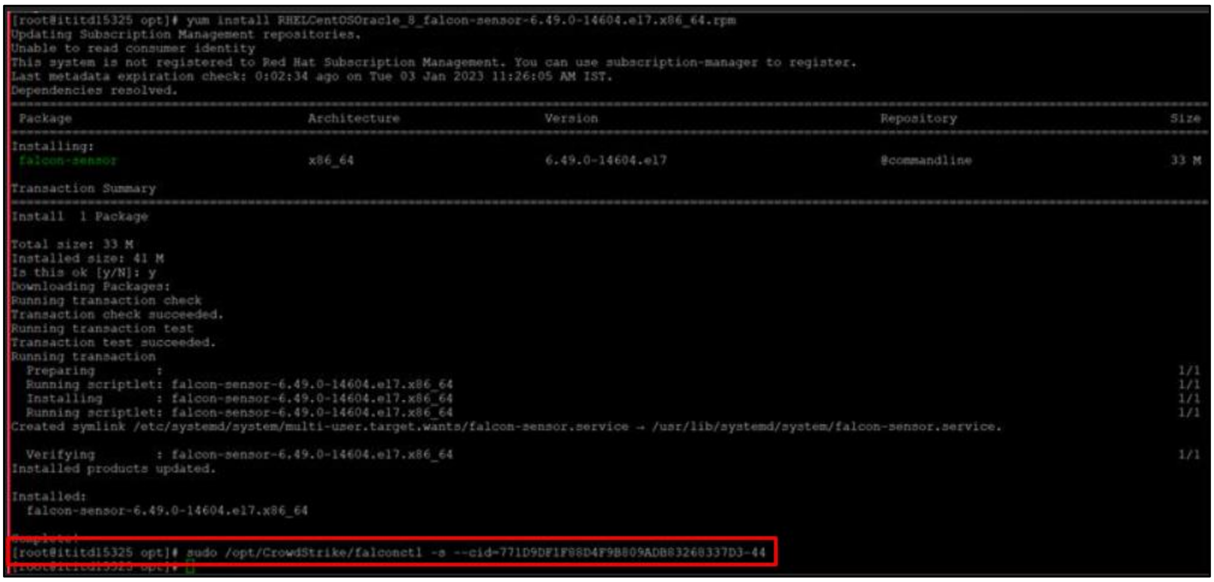
2. Run the installer, substituting **RHELCentOSOracle 8 falcon-sensor-6.49.0-14604.el7.x86_64.rpm** with your installer's file name.
   - RHEL, CentOS, Amazon Linux: **sudo yum install RHELCentOSOracle 8 falcon-sensor-6.49.0-14604.el7.x86_64.rpm**



```
[root@ititd15325 opt]# yum install RHELCentOSOracle_8_falcon-sensor-6.49.0-14604.el7.x86_64.rpm
Updating Subscription Management repositories.
Unable to read consumer identity
This system is not registered to Red Hat Subscription Management. You can use subscription-manager to register.
Last metadata expiration check: 0:02:34 ago on Tue 03 Jan 2023 11:26:05 AM IST.
Dependencies resolved.
==============================================================================================================================
 Package                         Architecture                Version                            Repository              Size
==============================================================================================================================
Installing:
 falcon-sensor                   x86_64                      6.49.0-14604.el7                   @commandline            33 M

Transaction Summary
==============================================================================================================================
Install  1 Package

Total size: 33 M
Installed size: 41 M
Is this ok [y/N]: y
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                                                                     1/1
  Running scriptlet: falcon-sensor-6.49.0-14604.el7.x86_64                                                               1/1
  Installing       : falcon-sensor-6.49.0-14604.el7.x86_64                                                               1/1
  Running scriptlet: falcon-sensor-6.49.0-14604.el7.x86_64                                                               1/1
Created symlink /etc/systemd/system/multi-user.target.wants/falcon-sensor.service → /usr/lib/systemd/system/falcon-sensor.service.

  Verifying        : falcon-sensor-6.49.0-14604.el7.x86_64                                                               1/1
Installed products updated.

Installed:
  falcon-sensor-6.49.0-14604.el7.x86_64

Complete!
[root@ititd15325 opt]# sudo /opt/CrowdStrike/falconctl -s --cid=771D9DF1F88D4F9B809ADB83268337D3-44
[root@ititd15325 opt]#
```

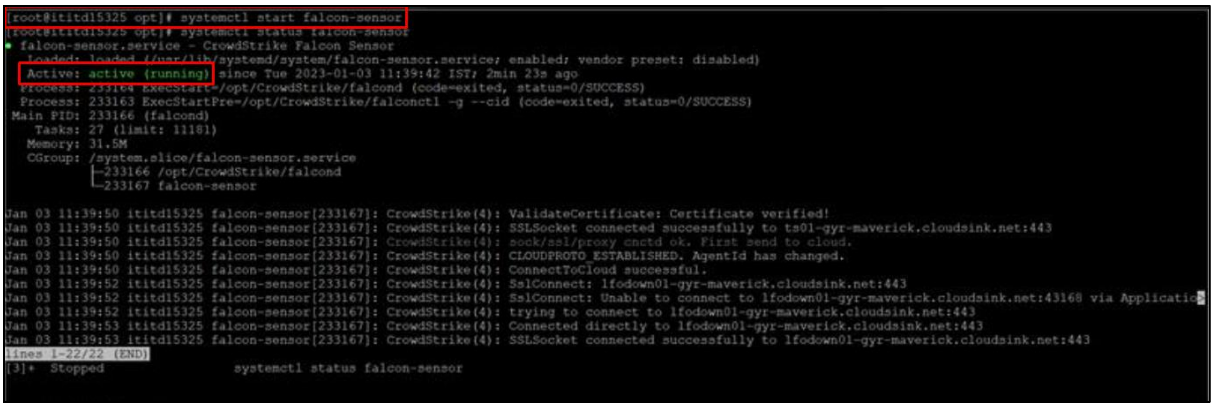
3. After Installing the sensor Activate using below command:

sudo /opt/CrowdStrike/falconctl -s -cid=771D9DF1F88D4F9B809ADB83268337D3-44



```
[root@ititd15325 opt]# yum install RHELCentOSOracle_8_falcon-sensor-6.49.0-14604.el7.x86_64.rpm
Updating Subscription Management repositories.
Unable to read consumer identity
This system is not registered to Red Hat Subscription Management. You can use subscription-manager to register.
Last metadata expiration check: 0:02:34 ago on Tue 03 Jan 2023 11:26:05 AM IST.
Dependencies resolved.
==========================================================================================================================
 Package                     Architecture             Version                          Repository                  Size
==========================================================================================================================
Installing:
 falcon-sensor               x86_64                   6.49.0-14604.el7                 @commandline                33 M

Transaction Summary
==========================================================================================================================
Install  1 Package

Total size: 33 M
Installed size: 41 M
Is this ok [y/N]: y
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                                                                1/1
  Running scriptlet: falcon-sensor-6.49.0-14604.el7.x86_64                                                          1/1
  Installing       : falcon-sensor-6.49.0-14604.el7.x86_64                                                          1/1
  Running scriptlet: falcon-sensor-6.49.0-14604.el7.x86_64                                                          1/1
Created symlink /etc/systemd/system/multi-user.target.wants/falcon-sensor.service → /usr/lib/systemd/system/falcon-sensor.service.

  Verifying        : falcon-sensor-6.49.0-14604.el7.x86_64                                                          1/1
Installed products updated.

Installed:
  falcon-sensor-6.49.0-14604.el7.x86_64

Complete!
[root@ititd15325 opt]# sudo /opt/CrowdStrike/falconctl -s --cid=771D9DF1F88D4F9B809ADB83268337D3-44
[root@ititd15325 opt]# 
```

4. Start the sensor manually. This step is not required for versions 4.0 and earlier.
    - Hosts with SysVinit: **sudo service falcon-sensor start**
    - Hosts with Systemd: **sudo systemctl start falcon-sensor**



```
[root@ititd15325 opt]# systemctl start falcon-sensor
[root@ititd15325 opt]# systemctl status falcon-sensor
● falcon-sensor.service - CrowdStrike Falcon Sensor
   Loaded: loaded (/usr/lib/systemd/system/falcon-sensor.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-01-03 11:39:42 IST; 2min 23s ago
  Process: 233164 ExecStart=/opt/CrowdStrike/falcond (code=exited, status=0/SUCCESS)
  Process: 233163 ExecStartPre=/opt/CrowdStrike/falconctl -g --cid (code=exited, status=0/SUCCESS)
 Main PID: 233166 (falcond)
    Tasks: 27 (limit: 11181)
   Memory: 31.5M
   CGroup: /system.slice/falcon-sensor.service
           ├─233166 /opt/CrowdStrike/falcond
           └─233167 falcon-sensor

Jan 03 11:39:50 ititd15325 falcon-sensor[233167]: CrowdStrike(4): ValidateCertificate: Certificate verified!
Jan 03 11:39:50 ititd15325 falcon-sensor[233167]: CrowdStrike(4): SSLSocket connected successfully to ts01-gyr-maverick.cloudsink.net:443
Jan 03 11:39:50 ititd15325 falcon-sensor[233167]: CrowdStrike(4): sock/ssl/proxy cnctd ok. First send to cloud.
Jan 03 11:39:50 ititd15325 falcon-sensor[233167]: CrowdStrike(4): CLOUDPROTO_ESTABLISHED. AgentId has changed.
Jan 03 11:39:50 ititd15325 falcon-sensor[233167]: CrowdStrike(4): ConnectToCloud successful.
Jan 03 11:39:52 ititd15325 falcon-sensor[233167]: CrowdStrike(4): SslConnect: lfodown01-gyr-maverick.cloudsink.net:443
Jan 03 11:39:52 ititd15325 falcon-sensor[233167]: CrowdStrike(4): SslConnect: Unable to connect to lfodown01-gyr-maverick.cloudsink.net:43168 via Applicatio
Jan 03 11:39:52 ititd15325 falcon-sensor[233167]: CrowdStrike(4): trying to connect to lfodown01-gyr-maverick.cloudsink.net:443
Jan 03 11:39:53 ititd15325 falcon-sensor[233167]: CrowdStrike(4): Connected directly to lfodown01-gyr-maverick.cloudsink.net:443
Jan 03 11:39:53 ititd15325 falcon-sensor[233167]: CrowdStrike(4): SSLSocket connected successfully to lfodown01-gyr-maverick.cloudsink.net:443
lines 1-22/22 (END)
[3]+  Stopped                 systemctl status falcon-sensor
```

Verifying sensor installation

You can verify an installation by using the Falcon console or a terminal on the host.

Falcon console

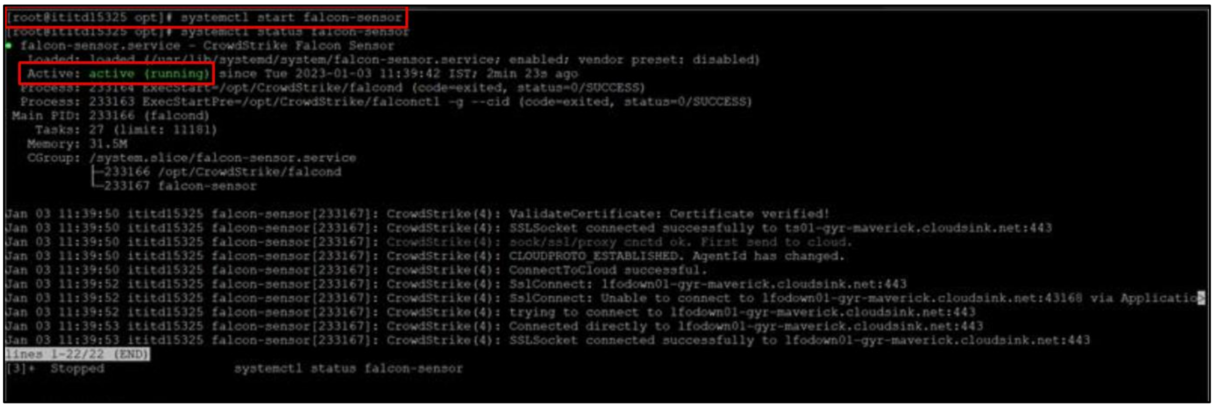
After the sensor is installed, the host connects to the Falcon console. You can confirm a sensor installation by reviewing your hosts.

To view a complete list of newly installed sensors, use the Sensor Report in the Falcon console.

Host

To validate that the Falcon sensor for Linux is running on a host, run this command at a terminal:

ps -e | grep falcon-sensor



```
[root@ititd15325 opt]# systemctl start falcon-sensor
[root@ititd15325 opt]# systemctl status falcon-sensor
● falcon-sensor.service - CrowdStrike Falcon Sensor
   Loaded: loaded (/usr/lib/systemd/system/falcon-sensor.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-01-03 11:39:42 IST; 2min 23s ago
  Process: 233164 ExecStart=/opt/CrowdStrike/falcond (code=exited, status=0/SUCCESS)
  Process: 233163 ExecStartPre=/opt/CrowdStrike/falconctl -g --cid (code=exited, status=0/SUCCESS)
 Main PID: 233166 (falcond)
    Tasks: 27 (limit: 11181)
   Memory: 31.5M
   CGroup: /system.slice/falcon-sensor.service
           ├─233166 /opt/CrowdStrike/falcond
           └─233167 falcon-sensor

Jan 03 11:39:50 ititd15325 falcon-sensor[233167]: CrowdStrike(4): ValidateCertificate: Certificate verified!
Jan 03 11:39:50 ititd15325 falcon-sensor[233167]: CrowdStrike(4): SSLSocket connected successfully to ts01-gyr-maverick.cloudsink.net:443
Jan 03 11:39:50 ititd15325 falcon-sensor[233167]: CrowdStrike(4): sock/ssl/proxy cnctd ok. First send to cloud.
Jan 03 11:39:50 ititd15325 falcon-sensor[233167]: CrowdStrike(4): CLOUDPROTO_ESTABLISHED. AgentId has changed.
Jan 03 11:39:50 ititd15325 falcon-sensor[233167]: CrowdStrike(4): ConnectToCloud successful.
Jan 03 11:39:52 ititd15325 falcon-sensor[233167]: CrowdStrike(4): SslConnect: lfodown01-gyr-maverick.cloudsink.net:443
Jan 03 11:39:52 ititd15325 falcon-sensor[233167]: CrowdStrike(4): SslConnect: Unable to connect to lfodown01-gyr-maverick.cloudsink.net:43168 via Applicatio>
Jan 03 11:39:52 ititd15325 falcon-sensor[233167]: CrowdStrike(4): trying to connect to lfodown01-gyr-maverick.cloudsink.net:443
Jan 03 11:39:53 ititd15325 falcon-sensor[233167]: CrowdStrike(4): Connected directly to lfodown01-gyr-maverick.cloudsink.net:443
Jan 03 11:39:53 ititd15325 falcon-sensor[233167]: CrowdStrike(4): SSLSocket connected successfully to lfodown01-gyr-maverick.cloudsink.net:443
lines 1-22/22 (END)
[3]+  Stopped                 systemctl status falcon-sensor
```

Installing Dependencies

While Installing CrowdStrike Sensor in RHEL 8, if you are getting any error on libnl dependencies. Then download and install the dependencies using the below command.
wget http://mirror.centos.org/centos/7/os/x86_64/Packages/libnl-1.1.4-3.el7.x86_64.rpm

CROWDSTRIKE FALCON SENSOR AGENT INSTALLATION ON CENTOS

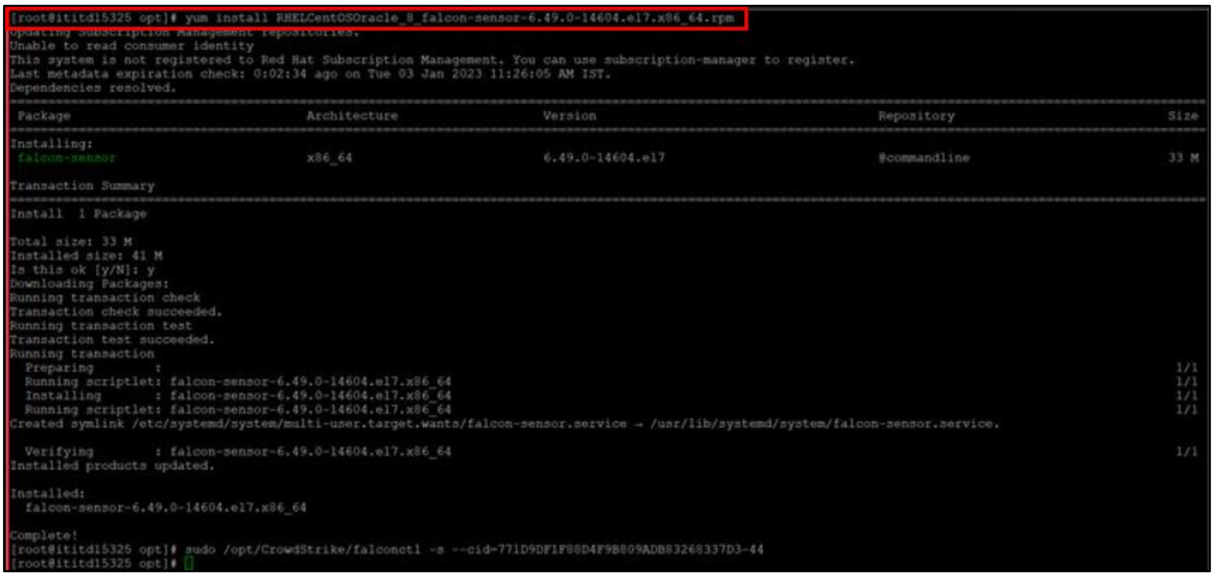
To install the Falcon sensor on the nodes, perform these procedures:

- Installing the Falcon sensor.
- Verifying the installation.

Installing the Falcon sensor

1. Download or copy the package from below Central path to the Linux host
   [CrowdStrike Agent Setup]

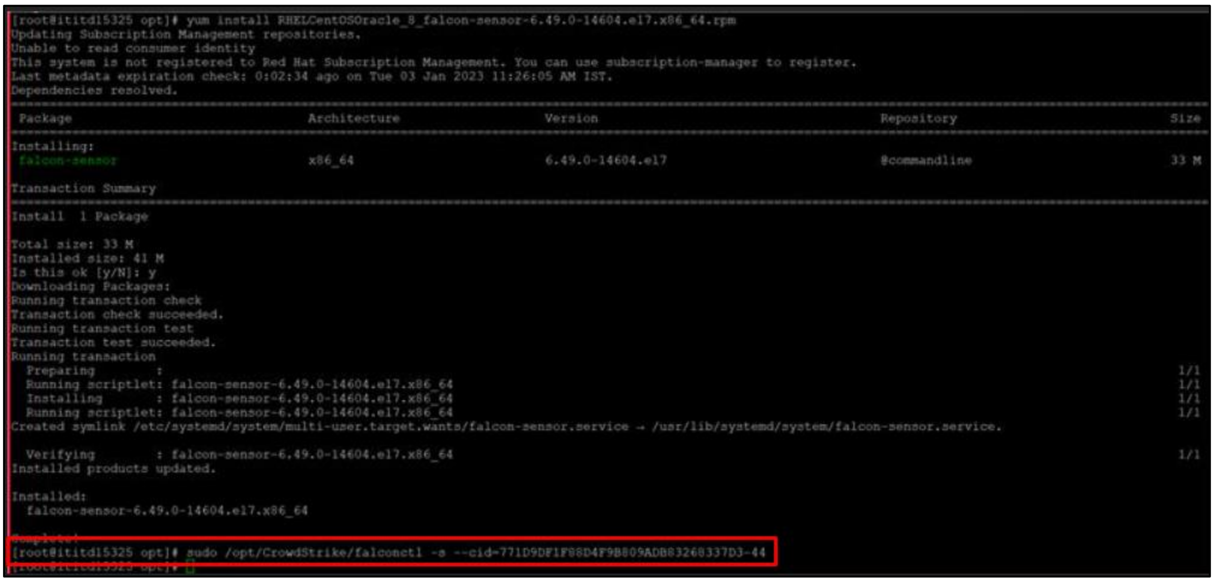
2. Run the installer, substituting **RHELCentOSOracle 8 falcon-sensor-6.49.0-14604.el7.x86_64.rpm** with your installer's file name.
   - RHEL, CentOS, Amazon Linux: **sudo yum install RHELCentOSOracle 8 falcon-sensor-6.49.0-14604.el7.x86_64.rpm**



```
[root@ititd15325 opt]# yum install RHELCentOSOracle_8_falcon-sensor-6.49.0-14604.el7.x86_64.rpm
Updating Subscription Management repositories.
Unable to read consumer identity
This system is not registered to Red Hat Subscription Management. You can use subscription-manager to register.
Last metadata expiration check: 0:02:34 ago on Tue 03 Jan 2023 11:26:05 AM IST.
Dependencies resolved.
=====================================================================================================================
 Package                       Architecture               Version                       Repository             Size
=====================================================================================================================
Installing:
 falcon-sensor                 x86_64                     6.49.0-14604.el7              @commandline           33 M

Transaction Summary
=====================================================================================================================
Install  1 Package

Total size: 33 M
Installed size: 41 M
Is this ok [y/N]: y
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                                                              1/1
  Running scriptlet: falcon-sensor-6.49.0-14604.el7.x86_64                                                        1/1
  Installing       : falcon-sensor-6.49.0-14604.el7.x86_64                                                        1/1
  Running scriptlet: falcon-sensor-6.49.0-14604.el7.x86_64                                                        1/1
Created symlink /etc/systemd/system/multi-user.target.wants/falcon-sensor.service → /usr/lib/systemd/system/falcon-sensor.service.

  Verifying        : falcon-sensor-6.49.0-14604.el7.x86_64                                                        1/1
Installed products updated.

Installed:
  falcon-sensor-6.49.0-14604.el7.x86_64

Complete!
[root@ititd15325 opt]# sudo /opt/CrowdStrike/falconctl -s --cid=771D9DF1F88D4F9B809ADB83268337D3-44
[root@ititd15325 opt]# 
```

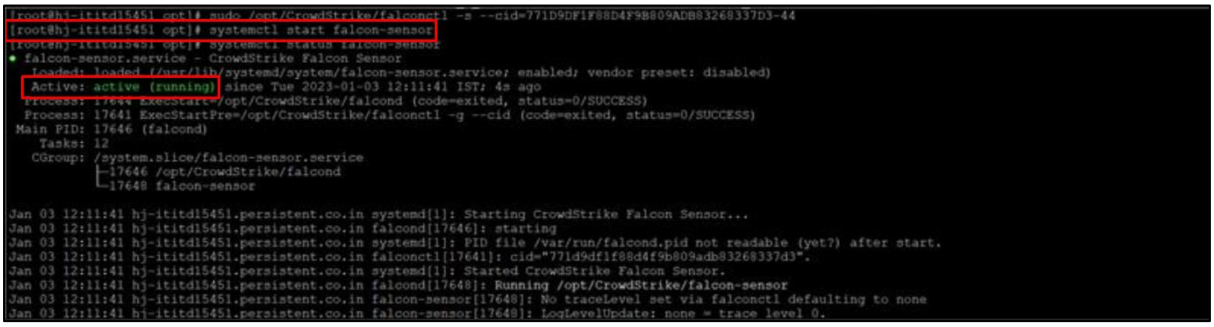
3. After Installing the sensor Activate using below command:

sudo /opt/CrowdStrike/falconctl -s -cid=771D9DF1F88D4F9B809ADB83268337D3-44



```
[root@ititd15325 opt]# yum install RHELCentOSOracle_8_falcon-sensor-6.49.0-14604.el7.x86_64.rpm
Updating Subscription Management repositories.
Unable to read consumer identity
This system is not registered to Red Hat Subscription Management. You can use subscription-manager to register.
Last metadata expiration check: 0:02:34 ago on Tue 03 Jan 2023 11:26:05 AM IST.
Dependencies resolved.
================================================================================================================================
 Package                          Architecture                Version                               Repository               Size
================================================================================================================================
Installing:
 falcon-sensor                    x86_64                      6.49.0-14604.el7                      @commandline             33 M

Transaction Summary
================================================================================================================================
Install  1 Package

Total size: 33 M
Installed size: 41 M
Is this ok [y/N]: y
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                                                                       1/1
  Running scriptlet: falcon-sensor-6.49.0-14604.el7.x86_64                                                                 1/1
  Installing       : falcon-sensor-6.49.0-14604.el7.x86_64                                                                 1/1
  Running scriptlet: falcon-sensor-6.49.0-14604.el7.x86_64                                                                 1/1
Created symlink /etc/systemd/system/multi-user.target.wants/falcon-sensor.service → /usr/lib/systemd/system/falcon-sensor.service.

  Verifying        : falcon-sensor-6.49.0-14604.el7.x86_64                                                                 1/1
Installed products updated.

Installed:
  falcon-sensor-6.49.0-14604.el7.x86_64

Complete!
[root@ititd15325 opt]# sudo /opt/CrowdStrike/falconctl -s --cid=771D9DF1F88D4F9B809ADB83268337D3-44
[root@ititd15325 opt]# 
```

4. Start the sensor manually. This step is not required for versions 4.0 and earlier.
    - Hosts with SysVinit: **sudo service falcon-sensor start**
    - Hosts with Systemd: **sudo systemctl start falcon-sensor**



```
[root@hj-ititd15451 opt]# sudo /opt/CrowdStrike/falconctl -s --cid=771D9DF1F88D4F9B809ADB83268337D3-44
[root@hj-ititd15451 opt]# systemctl start falcon-sensor
[root@hj-ititd15451 opt]# systemctl status falcon-sensor
● falcon-sensor.service - CrowdStrike Falcon Sensor
   Loaded: loaded (/usr/lib/systemd/system/falcon-sensor.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-01-03 12:11:41 IST; 4s ago
  Process: 17644 ExecStart=/opt/CrowdStrike/falcond (code=exited, status=0/SUCCESS)
  Process: 17641 ExecStartPre=/opt/CrowdStrike/falconctl -g --cid (code=exited, status=0/SUCCESS)
 Main PID: 17646 (falcond)
    Tasks: 12
   CGroup: /system.slice/falcon-sensor.service
           ├─17646 /opt/CrowdStrike/falcond
           └─17648 falcon-sensor

Jan 03 12:11:41 hj-ititd15451.persistent.co.in systemd[1]: Starting CrowdStrike Falcon Sensor...
Jan 03 12:11:41 hj-ititd15451.persistent.co.in falcond[17646]: starting
Jan 03 12:11:41 hj-ititd15451.persistent.co.in systemd[1]: PID file /var/run/falcond.pid not readable (yet?) after start.
Jan 03 12:11:41 hj-ititd15451.persistent.co.in falconctl[17641]: cid="771d9df1f88d4f9b809adb83268337d3".
Jan 03 12:11:41 hj-ititd15451.persistent.co.in systemd[1]: Started CrowdStrike Falcon Sensor.
Jan 03 12:11:41 hj-ititd15451.persistent.co.in falcond[17648]: Running /opt/CrowdStrike/falcon-sensor
Jan 03 12:11:41 hj-ititd15451.persistent.co.in falcon-sensor[17648]: No traceLevel set via falconctl defaulting to none
Jan 03 12:11:41 hj-ititd15451.persistent.co.in falcon-sensor[17648]: LogLevelUpdate: none = trace level 0.
```

TROUBLESHOOTING AND INSTALLATION ON NODES

Installation fails:
Issue: Your sensor installation fails.

Solution
Verify that the SHA-256 checksum of the installer file you downloaded matches the SHA-256 checksum shown in Host setup and management > **Deploy** > **Sensor Downloads**.

Ubuntu installation fails: "Dependent Packages are not Installed"
Issue: Your Ubuntu installation fails with an error that "dependent packages are not installed."

Solution
Use this command to install the dependent packages:

```
$ apt-get -f install
```

SLES installation fails: "Nothing Provides Openssl"
Issue: Your SLES installation fails with an error that nothing provides openssl1 >= 1.0.1. This is most caused by a SLES version that doesn't include a modern OpenSSL implementation.

Solution

- Enable the SLES 11 security module: $ sudo zypper mr --enable SLE11-Security-Module
- Run the sensor installer again.

Verifying those dependencies are Installed
Issue: Your installation fails with an error message about missing dependencies of libssl, libc, or libcrypto.

```
--> Missing Dependency: libssl.so.10()(64bit) is needed by package falcon-sensor-1.0.3-1.e16x86_64 (/falcon-sensor-1.0.3-1.e16.x86_64) Error Missing Dependency: libc.so.6(GLIBC_2.7)(64bit) is needed by package falcon-sensor-1.0.3-1.e16x86_64 (/falcon-sensor-1.0.3-1.e16.x86_64) Error Missing Dependency: libcrypto.so.10()(64bit) is needed by package falcon-sensor-1.0.3-1.e16x86_64 (/falcon-sensor-1.0.3-1.e16.x86_64)
```

Solution
Install a supported version of OpenSSL.

TROUBLESHOOTING GENERAL ISSUE

Verifying that the sensor is running

1. Check running processes to verify the Falcon sensor is running: ps -e | grep -e falcon-sensor
2. Check kernel modules to verify the Falcon sensor's kernel modules are running: lsmod | grep falcon
3. Check the Falcon sensor's configurable options: sudo /opt/CrowdStrike/falconctl -g

   Optional parameters:
   --aid: the sensor's agent ID
   --cid: your Customer ID
   --apd: the sensor's proxy status (enabled or disabled)
   --aph: the sensor's proxy host
   --app: the sensor's proxy port
   --version: the sensor's version number

The sensor requires these runtime services:

- network
- systemd
  - local-fs
  - sysinit
  - multi-user
  - shutdown

Verifying the sensor files on disk

If the sensor is not running, verify that the sensor's application files exist on your host:
$ sudo ls -al /opt/CrowdStrike /opt/CrowdStrike/falcon-sensor
This should be a symlink to either:

- the original sensor installation at /opt/CrowdStrike/falcon-sensor
- a sensor update package with a release build number, such as /opt/CrowdStrike/falcon-sensor3000

Verifying the sensor is connected to the CrowdStrike cloud

You can verify that the host is connected to the CrowdStrike cloud by using the Falcon console or a command line on the host.

Falcon console

Search for the host in Host setup and management > Manage endpoints > Host management.
To view a complete list of newly installed sensors, use the Sensor Report.

Host

Check network statistics using the command line:

```
sudo netstat -tapn | grep falcon
```

If the Falcon sensor is communicating with the cloud, you'll see output like this:

```
tcp        0      0    192.0.2.176:35382       ec2-54-148-96-12:443
 ESTABLISHED 3228/falcon-sensor
```

Providing troubleshooting info to Support

When you need help from Support with a sensor, collect data using the falcon-diagnostic script. To download this script, see Troubleshooting Linux Sensors.

Logs

Logs are stored within your host's syslog. The syslog locations vary but are specified in /etc/syslog.conf or rsyslog.conf, with these being the most common:

- /var/log/messages
- var/log/syslog
- /var/log/rsyslog
- /var/log/daemon

grep for the string falcon for sensor logs, similar to this example:

```
sudo grep falcon /var/log/messages | tail -n 100
```

Logs are kept according to your host's log rotation settings.