Cisco Secure Cloud Analytics

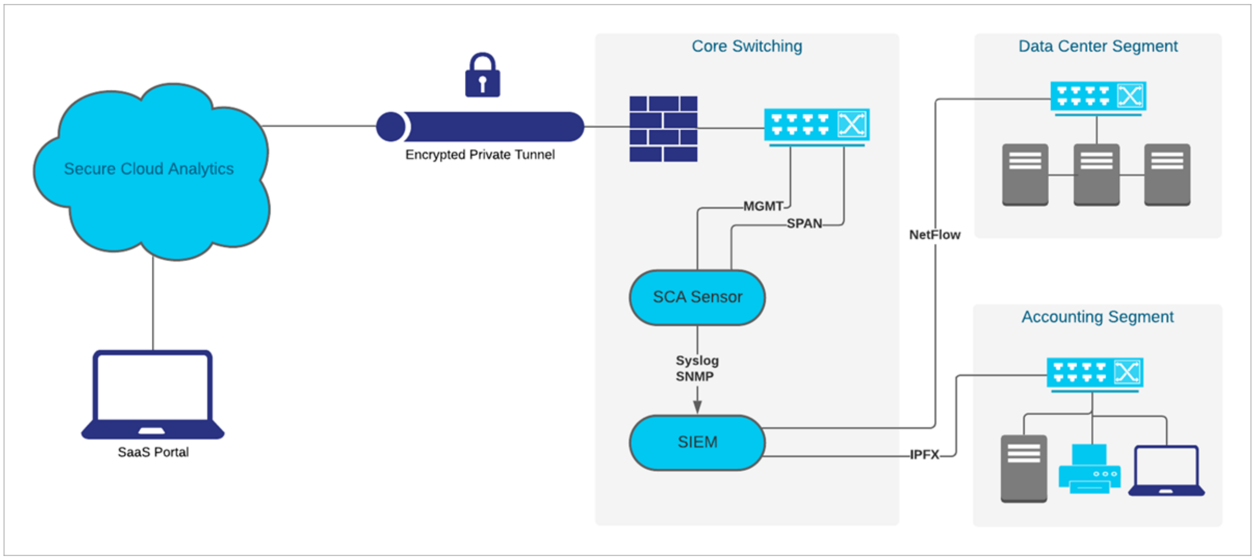
Sensor Advanced Configuration Guide

Table of Contents

About Private Network Monitor Sensor

Cisco Secure Cloud Analytics provides visibility and advanced threat detection for on-premises and cloud networks. For on-premises networks, a Cisco Secure private network monitoring virtual appliance is needed to collect network flow data and send it to the cloud. The virtual appliance is available as an ISO, which contains the necessary Secure Cloud Analytics packages as part of an Ubuntu Linux image. The virtual appliance software is included in the Secure Cloud Analytics service; users can download the sensor ISO directly from their customer portal. This Secure Cloud Analytics reference guide covers additional options for installing and configuring the virtual appliance.

The sensor collects local network data telemetry, such as NetFlow, and sends it securely to the cloud.



Due to the wide variety of network topologies deployed, additional configuration may be necessary to ensure a successful virtual appliance deployment. This guide covers advanced configuration and troubleshooting not addressed by the installation guide.

Checking Your Sensor Version

To ensure you have the most recent sensor deployed on your network, you can check an existing sensor's version from the command line.

Procedure

1. SSH into a deployed sensor.
2. At the prompt, enter `cat /opt/obsrvbl-ona/version` and press **Enter**. If the console does not display 5.1.1, your sensor is out of date.
   If you need to upgrade your sensor, refer to **Appendix D - Upgrading the Sensor** for instructions.

Manually Installing the Package for Linux Operating Systems

In addition to the provided ISO, the Virtual Appliance can be deployed on the following operating systems:

- Ubuntu Linux version 18.04 (32- and 64-bit)
- Ubuntu Linux versions 20.04 and later (32- and 64-bit)
- Red Hat Enterprise Linux (RHEL) version 7 and compatible, including CentOS version 7 (64-bit)
- Red Hat Enterprise Linux (RHEL) version 8 and compatible, including CentOS version 8 (64-bit)
- Raspberry Pi 2 Model B with Raspberry Pi OS (32-bit armhf)
- Docker, tested with CoreOS (64-bit)

Install on Ubuntu with NetFlow collection

Before You Begin

- Log into the Ubuntu system as an administrator.

Procedure

In the command-line interface:

1. Enter `wget https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_UbuntuXenial_amd64.deb` to download the Secure Cloud Analytics package.
2. Enter `sudo apt-get install -y net-tools tcpdump` to install dependencies.
3. Enter `sudo apt-get update && sudo apt-get install -y libglib2.0-0 liblzo2-2 libltdl7` to install updates and additional packages.
4. Enter `wget https://assets-production.obsrvbl.com/ona-packages/netsa/v0.1.27/netsa-pkg.deb` to download the package manager file.
5. Enter `sudo apt install ./ona-service_UbuntuXenial_amd64.deb ./netsa-pkg.deb` to install the package manager file.
6. Enter `sudo reboot` to reboot Linux.
7. Confirm services are running. See **Appendix C - Services** for Secure Cloud Analytics services.

Install on Ubuntu without NetFlow collection

Before You Begin

- Log into the Ubuntu system as an administrator.

Procedure

In the command-line interface:

1. Enter `wget https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_UbuntuXenial_amd64.deb` to download the Secure Cloud Analytics package.
2. Enter `sudo apt-get install -y net-tools tcpdump` to install dependencies.
3. Enter `sudo apt-get –f install` to verify dependencies installed properly.
4. Enter `sudo apt install ./ona-service_UbuntuXenial_amd64.deb ./netsa-pkg.deb` to install the Secure Cloud Analytics service.
5. Confirm services are running. See **Appendix C - Services** for Secure Cloud Analytics services.

Install on RHEL

RHEL 8

Before You Begin

- Log into the RHEL 8 system as an administrator.

Procedure

In the command-line interface:

1. Enter `curl -L -O https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_RHEL_8_x86_64.rpm` to download the Secure Cloud Analytics package.
2. Enter `sudo yum install -y net-tools tcpdump` to install dependencies.
3. Run the following commands to install updates and additional packages:

   a. Enter `sudo yum updateinfo`

   b. Enter `yum install -y libpcap libtool-ltdl lzo`

4. Enter `curl -L -O https://assets-production.obsrvbl.com/ona-packages/netsa/v0.1.27/netsa-pkg.rpm` to download the package manager file.

⚠ Make sure that you enter the complete command.

5. Enter `sudo rpm -i netsa-pkg.rpm` to install the package manager file.
6. Enter `sudo rpm -i ona-service_RHEL_8_x86_64.rpm` to install the Secure Cloud Analytics service.
7. Confirm services are running. See **Appendix C - Services** for Secure Cloud Analytics services.

RHEL 7

Before You Begin

- Log into the RHEL 7 system as an administrator.

Procedure

In the command-line interface:

1. Enter `curl -L -O https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_RHEL_7_x86_64.rpm` to download the Secure Cloud Analytics package.
2. Enter `sudo yum install -y net-tools tcpdump` to install dependencies.
3. Run the following commands to install updates and additional packages:
   a. Enter `sudo yum updateinfo`
   b. Enter `yum install -y libpcap libtool-ltdl lzo`
4. Enter `curl -L -O https://assets-production.obsrvbl.com/ona-packages/netsa/v0.1.27/netsa-pkg.rpm` to download the package manager file.

⚠ Make sure that you enter the complete command.

5. Enter `sudo rpm -i netsa-pkg.rpm` to install the package manager file.
6. Enter `sudo rpm -i ona-service_RHEL_7_x86_64.rpm` to install the Secure Cloud Analytics service.
7. Confirm services are running. See **Appendix C - Services** for Secure Cloud Analytics services.

Attaching Sensors to the Web Portal

Once a sensor is installed, it will need to be linked with your portal. This is done by identifying the sensor's public IP address and entering it into the web portal. If you cannot determine the sensor's public IP address, you can manually link the sensor to your portal using its unique service key.

The sensor can connect to the following portals:

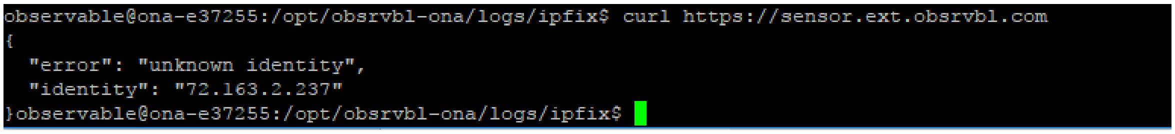
- https://sensor.ext.obsrvbl.com (US)
- https://sensor.eu-prod.obsrvbl.com (EU)
- https://sensor.anz-prod.obsrvbl.com (Australia)

> ⓘ If multiple sensors are staged in a central location, such as an MSSP, and they are intended for different customers, the public IP should be removed after each new customer is configured. If a public IP address of the staging environment is used for multiple sensors, a sensor could be incorrectly attached to the wrong portal

> ⓘ If you are using proxy server, complete the steps in the **Configuring Proxy** section to enable communication between the sensor and the Secure Cloud Analytics web portal.

Finding and Adding a Sensor's Public IP Address to a Portal

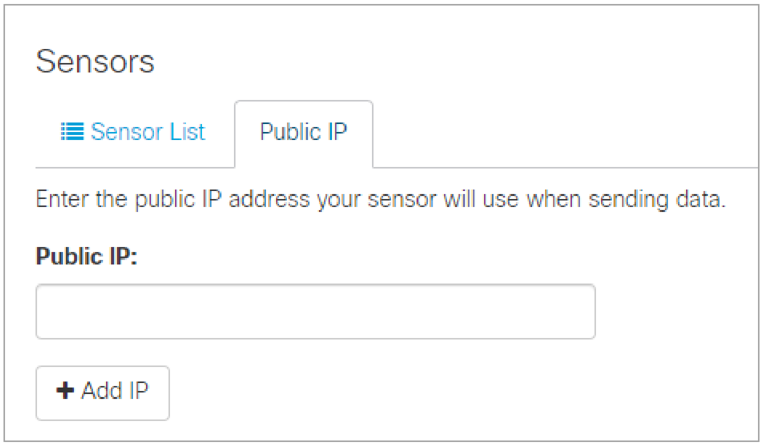
1. SSH into the sensor and login as an administrator.
2. At the command prompt, enter `curl https://sensor.ext.obsrvbl.com` and press **Enter**. The `error` value of `unknown identity` means that the sensor is not associated with a portal. See the following image for an example.



```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ curl https://sensor.ext.obsrvbl.com
{
  "error": "unknown identity",
  "identity": "72.163.2.237"
}observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
```

3. Copy the `identity` IP address.
4. Log out of the sensor.
5. Log into the web portal as a site administrator.
6. Select the **sensor (☁) icon > Public IP**.

7. Enter the `identity` IP address in the Public IP field. See the following image for an example.



Sensors

☰ Sensor List | Public IP

Enter the public IP address your sensor will use when sending data.

Public IP:

+ Add IP

8. Click **Add IP**. After the portal and sensor exchange keys, they establish future connections using the keys, not the public IP address.

> It can take up to 10 minutes before a new sensor is reflected in the portal.

Manually Add a Portal’s Service Key to a Sensor

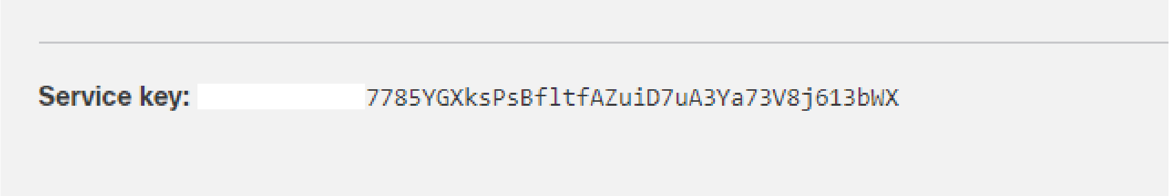
> This procedure is **not** required if you already added a sensor's public IP address to the web portal. We recommend you try that before trying this procedure. Manually adding a portal's service key to a sensor is intended primarily for older sensors that you deployed before ISO version
> `ona-18.04.1-server-amd64.iso`
> available as of December 2018. You can also redeploy older sensors using the current version of the sensor ISO, available in the web portal.

If you cannot add a sensor's public IP address to the web portal, or you are an MSSP managing multiple web portals, edit a sensor’s `config.local` configuration file to manually add a portal’s service key to associate the sensor with the portal.

> This key exchange is done automatically when using the public IP address in the previous section.

1. Log into the portal web UI as an administrator.

2. Select **Settings** > **Sensors**.
3. Navigate to the end of the sensor list and copy the **Service key**. See the following image for an example.

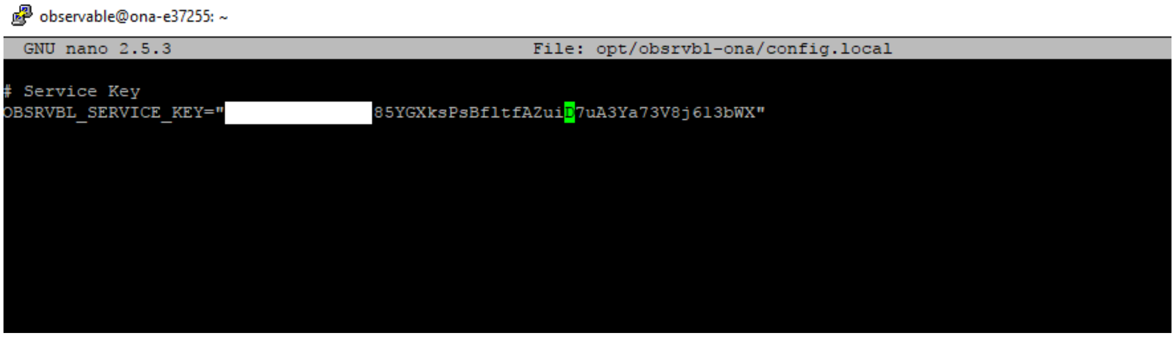


Service key: [redacted]7785YGXksPsBfltfAZuiD7uA3Ya73V8j613bWX

4. SSH login to the sensor as an administrator.
5. At the command prompt, enter this command: `sudo nano opt/obsrvbl-ona/config.local` and press **Enter** to edit the configuration file.
6. Beneath the line `# Service Key`, add the following line, replacing *<service-key>* with the following portal's service key:

   `OBSRVBL_SERVICE_KEY="`*<service-key>*`"`

   See the following for an example.



```
observable@ona-e37255: ~
  GNU nano 2.5.3                              File: opt/obsrvbl-ona/config.local

# Service Key
OBSRVBL_SERVICE_KEY="[redacted]85YGXksPsBfltfAZuiD7uA3Ya73V8j613bWX"
```

7. Press Ctrl + 0 to save the changes.
8. Press Ctrl + x to exit.
9. At the command prompt, enter `sudo service obsrvbl-ona restart` to restart the Secure Cloud Analytics service.

Configuring Proxy

If you are using proxy server, complete the following steps to enable communication between the sensor and the web portal.

1. SSH into the sensor and login as an administrator.

2. At the command prompt, enter this command:
   `sudo nano opt/obsrvbl-ona/config.local` and press **Enter** to edit the configuration file.
3. Add the following line, replacing `proxy.name.com` with your proxy server's hostname or IP address and `Port` with your proxy server's port number:
   `HTTPS_PROXY="proxy.name.com:Port"`

> HTTP may be supported in certain situations. Contact Support for more information.

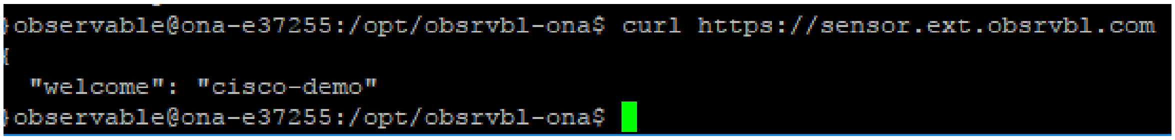
4. Press Ctrl + 0 to save the changes.
5. Press Ctrl + x to exit.
6. At the command prompt, enter `sudo service obsrvbl-ona restart` to restart the Secure Cloud Analytics service.

Confirm a Sensor’s Portal Connection

After a sensor is added to the portal, confirm the connection.

> If you manually linked a sensor to the web portal by updating the `config.local` configuration file using a service key, using the `curl` command to confirm the connection from the sensor may not return the web portal name.

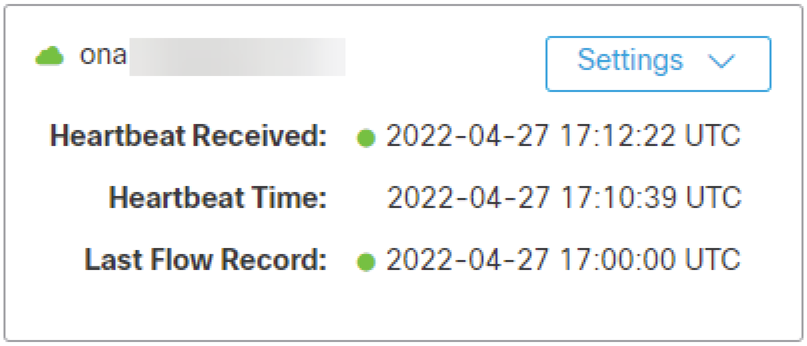
1. SSH into the sensor as an administrator.
2. At the command prompt, enter `curl https://sensor.ext.obsrvbl.com` and press **Enter**. The sensor returns the portal name. See the following image for an example.



```
observable@ona-e37255:/opt/obsrvbl-ona$ curl https://sensor.ext.obsrvbl.com
{
  "welcome": "cisco-demo"
observable@ona-e37255:/opt/obsrvbl-ona$
```

3. Log out of the sensor.
4. Log into the portal web UI.

5. Select **Settings > Sensors.** The sensor appears in the list.



ona [redacted]

Heartbeat Received: ● 2022-04-27 17:12:22 UTC

Heartbeat Time: 2022-04-27 17:10:39 UTC

Last Flow Record: ● 2022-04-27 17:00:00 UTC

Configuring a Sensor to Collect Flow Data

A sensor creates flow records from the traffic on its Ethernet interfaces by default. This default configuration assumes that the sensor is attached to a SPAN or mirror Ethernet port. If other devices on your network can generate flow records, you can configure the sensor in the web portal UI to collect flow records from these sources and send them to the cloud.

If the network devices generate different types of flows it is recommended to configure the sensor to collect each type over a different UDP port. This also makes troubleshooting easier. By default, the local sensor firewall (`iptables`) has ports 2055/UDP, 4739/UDP, and 9995/UDP open. You must open additional UDP ports in the web portal UI if you want to use them.

You can configure collection of the following flow types, with the following ports:

- NetFlow v5 - Port 2055/UDP (open by default)
- NetFlow v9 - Port 9995/UDP (open by default)
- IPFIX - Port 9996/UDP
- sFlow - Port 6343/UDP

Certain network appliances must be selected in the web portal UI before they will work properly:

- Cisco Meraki - Port 9998/UDP
- Cisco ASA - Port 9997/UDP
- SonicWALL - Port 9999/UDP

Configuring Sensors for Flow Collection

Before You Begin

- Log into the portal web UI as an administrator.

Procedure

1. Select **Settings > Sensors**.
2. Click **Change settings** for the sensor you added.
3. Select **NetFlow/IPFIX**.

> ℹ This option requires an up-to-date sensor version. If you do not see this option, select **Help (?) > On-Prem Sensor Install** to download a current version of the sensor ISO.

4. Click **Add New Probe**.
5. Select a flow type from the **Probe Type** drop-down list.
6. Enter a **Port** number.

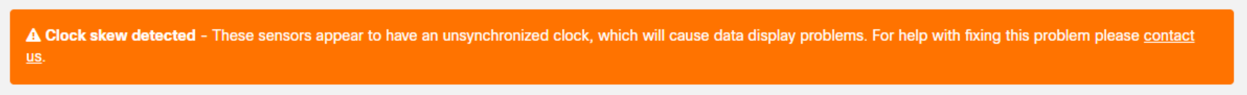
> ℹ If you want to pass Enhanced NetFlow to your sensor, ensure that the UDP port you configure is not one that is also configured for Flexible NetFlow or IPFIX in your sensor configuration. For example, configure port 2055/UDP for Enhanced NetFlow, and port 9995/UDP for Flexible NetFlow. See the Configuration Guide for Enhanced NetFlow for more information.

7. Select a **Protocol**.
8. Select a **Source device** from the drop-down list.
9. Click **Save**.

Appendix A - Troubleshooting

Resolve Time Drift and Synchronizing NTP

By default, a sensor is configured to use `pool.ntp.org` for NTP time synchronization, and to ensure data displays properly in the portal. If outbound NTP is not permitted, you may need to update the NTP settings. If the sensor time is not properly synchronized, the portal displays a warning. See the following image for an example.



⚠ **Clock skew detected** - These sensors appear to have an unsynchronized clock, which will cause data display problems. For help with fixing this problem please contact us.

Before You Begin

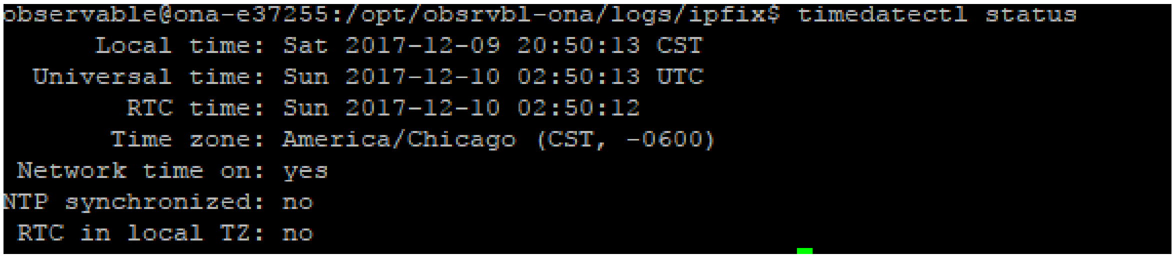
- SSH into the sensor as an administrator.

Summary Steps

1. `timedatectl status` and press **Enter** to verify if NTP is synchronizedJuli.
2. `sudo apt-get update && sudo apt-get install -y ntpdate ntp`
3. `sudo service ntp stop`
4. `sudo ntpdate pool.ntp.org`
5. If outbound NTP is not allowed, specify an internal IP address instead of `pool.ntp.org`
6. `sudo service ntp start`

Procedure

1. At the command prompt, enter `timedatectl status` and press **Enter** to verify if NTP is synchronized. See the following image for an example of a sensor that is not properly synchronized with NTP:



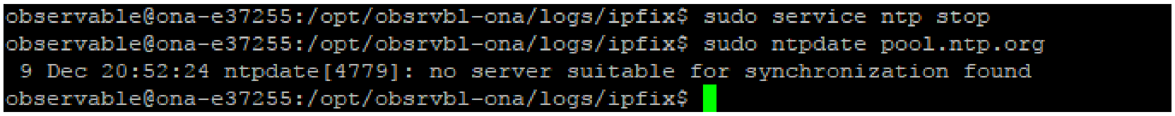
```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ timedatectl status
      Local time: Sat 2017-12-09 20:50:13 CST
  Universal time: Sun 2017-12-10 02:50:13 UTC
        RTC time: Sun 2017-12-10 02:50:12
       Time zone: America/Chicago (CST, -0600)
 Network time on: yes
NTP synchronized: no
 RTC in local TZ: no
```

2. Enter the following command and press **Enter** to ensure that the correct NTP packages are installed and up-to-date:

```
sudo apt-get update && sudo apt-get install -y ntpdate ntp
```

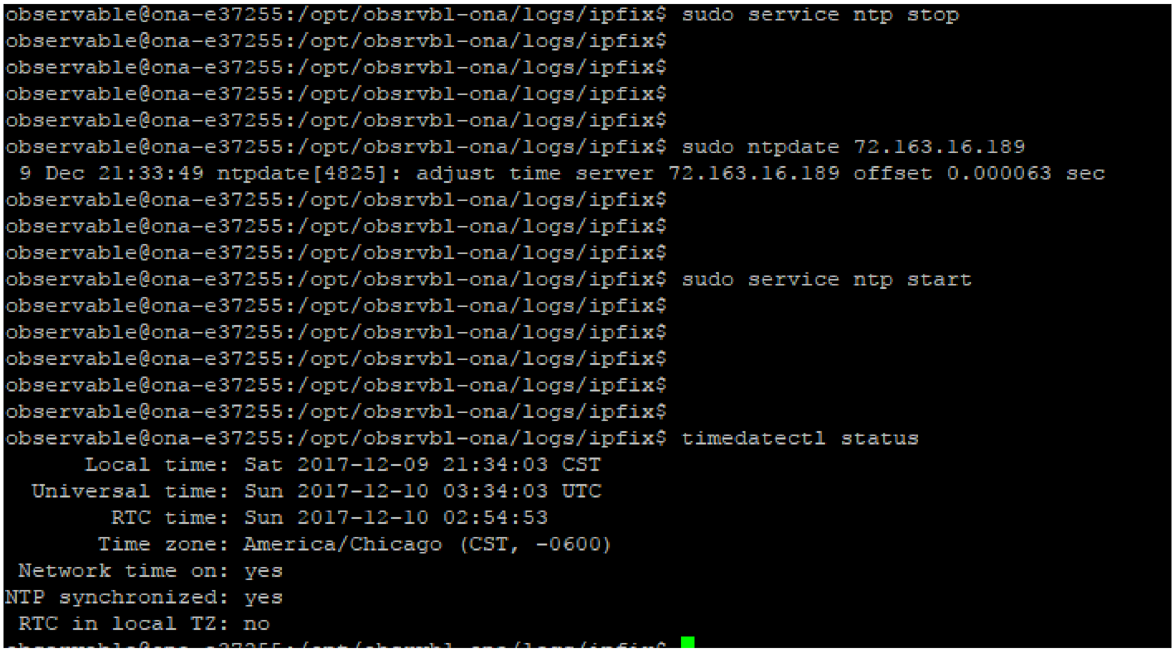
3. Enter `sudo service ntp stop` and press **Enter** to stop the NTP service.
4. Enter `sudo ntpdate pool.ntp.org` and press enter to set the NTP server to synchronize against.

   If outbound NTP is not allowed, the system displays an error message stating that it cannot find the server. See the following image for an example.



```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ sudo service ntp stop
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ sudo ntpdate pool.ntp.org
 9 Dec 20:52:24 ntpdate[4779]: no server suitable for synchronization found
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
```

5. If outbound NTP is not allowed, specify an internal IP address instead of `pool.ntp.org`. See the following image for an example.



```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ sudo service ntp stop
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ sudo ntpdate 72.163.16.189
 9 Dec 21:33:49 ntpdate[4825]: adjust time server 72.163.16.189 offset 0.000063 sec
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ sudo service ntp start
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ timedatectl status
      Local time: Sat 2017-12-09 21:34:03 CST
  Universal time: Sun 2017-12-10 03:34:03 UTC
        RTC time: Sun 2017-12-10 02:54:53
       Time zone: America/Chicago (CST, -0600)
 Network time on: yes
NTP synchronized: yes
 RTC in local TZ: no
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
```

6. Enter `sudo service ntp start` and press **Enter** to start the NTP service.

Resolve Unidirectional Traffic Errors

The Secure Cloud Analytics service detects when a sensor is not seeing bidirectional flows. For example, a large number of hosts with only outbound or inbound TCP traffic indicates some of the data feed is missing. This could be an issue with an improperly configured mirror port, missing VLAN, or an improperly configured firewall that is not sending flow data on all its interfaces. You can search for traffic passing through the mirror port and determine whether it is unidirectional or bidirectional.

Before You Begin

- SSH into the sensor as an administrator.

Summary Steps

1. Enter `ifconfig -a`
2. Enter this command:

   ```
   sudo tcpdump -i <mirror-interface-name> -n -c 100 "tcp"
   ```

   and press **Enter** to capture traffic passing through the mirror interface, to ensure it is seeing TCP traffic, not just broadcast traffic.

3. Enter this command:

   ```
   sudo tcpdump -i <mirror-interface-name> -n -c 100 "port 9996"
   ```

   and press Enter to capture traffic that matches port 9996/TCP.

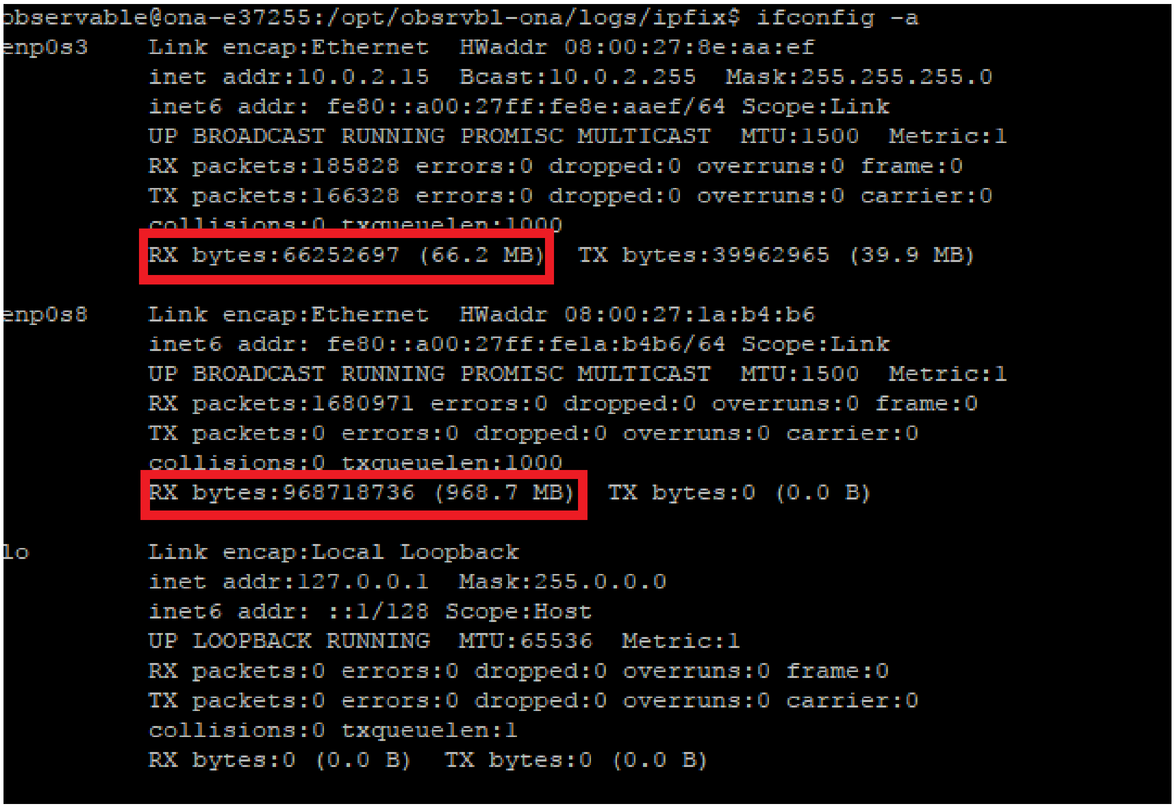
4. Enter this command:

   ```
   sudo tcpdump -i <mirror-interface-name> -n -c 100 "src 10.99.102.180"
   ```

   and press **Enter** to capture traffic that matches a source IP address of 10.99.102.180.

Procedure

1. At the command prompt, enter `ifconfig -a` and press **Enter** to view the list of interfaces. The mirror port interface typically has no associated IP address, and much larger packet and byte counts than the other interfaces. See the following image for an example; the `enp0s8` interface sees much more traffic, which is indicative of a mirror port.



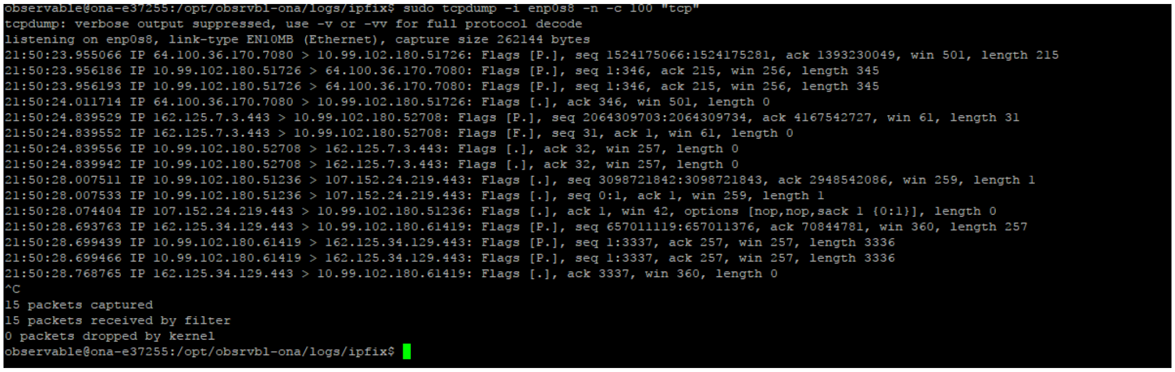
```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ ifconfig -a
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:8e:aa:ef
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8e:aaef/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:185828 errors:0 dropped:0 overruns:0 frame:0
          TX packets:166328 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:66252697 (66.2 MB)  TX bytes:39962965 (39.9 MB)

enp0s8    Link encap:Ethernet  HWaddr 08:00:27:1a:b4:b6
          inet6 addr: fe80::a00:27ff:fe1a:b4b6/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:1680971 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:968718736 (968.7 MB)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

2. Enter the following command:

   `sudo tcpdump -i <mirror-interface-name> -n -c 100 "tcp"`

   (replace `<mirror-interface-name>` with an interface name, such as `eth0`).

   Press **Enter** to capture traffic passing through the mirror interface, to ensure it is seeing TCP traffic, not just broadcast traffic. See the following image for an example.

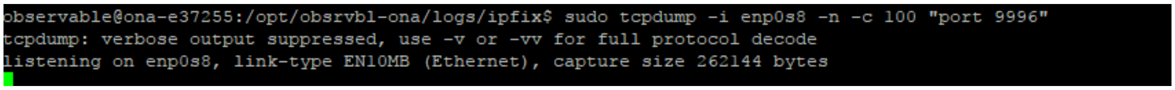


```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ sudo tcpdump -i enp0s8 -n -c 100 "tcp"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), capture size 262144 bytes
21:50:23.955066 IP 64.100.36.170.7080 > 10.99.102.180.51726: Flags [P.], seq 1524175066:1524175281, ack 1393230049, win 501, length 215
21:50:23.956186 IP 10.99.102.180.51726 > 64.100.36.170.7080: Flags [P.], seq 1:346, ack 215, win 256, length 345
21:50:23.956193 IP 10.99.102.180.51726 > 64.100.36.170.7080: Flags [P.], seq 1:346, ack 215, win 256, length 345
21:50:24.011714 IP 64.100.36.170.7080 > 10.99.102.180.51726: Flags [.], ack 346, win 501, length 0
21:50:24.839529 IP 162.125.7.3.443 > 10.99.102.180.52708: Flags [P.], seq 2064309703:2064309734, ack 4167542727, win 61, length 31
21:50:24.839552 IP 162.125.7.3.443 > 10.99.102.180.52708: Flags [F.], seq 31, ack 1, win 61, length 0
21:50:24.839556 IP 10.99.102.180.52708 > 162.125.7.3.443: Flags [.], ack 32, win 257, length 0
21:50:24.839942 IP 10.99.102.180.52708 > 162.125.7.3.443: Flags [.], ack 32, win 257, length 0
21:50:28.007511 IP 10.99.102.180.51236 > 107.152.24.219.443: Flags [.], seq 3098721842:3098721843, ack 2948542086, win 259, length 1
21:50:28.007533 IP 10.99.102.180.51236 > 107.152.24.219.443: Flags [.], seq 0:1, ack 1, win 259, length 1
21:50:28.074404 IP 107.152.24.219.443 > 10.99.102.180.51236: Flags [.], ack 1, win 42, options [nop,nop,sack 1 {0:1}], length 0
21:50:28.693763 IP 162.125.34.129.443 > 10.99.102.180.61419: Flags [P.], seq 657011119:657011376, ack 70844781, win 360, length 257
21:50:28.699439 IP 10.99.102.180.61419 > 162.125.34.129.443: Flags [P.], seq 1:3337, ack 257, win 257, length 3336
21:50:28.699466 IP 10.99.102.180.61419 > 162.125.34.129.443: Flags [P.], seq 1:3337, ack 257, win 257, length 3336
21:50:28.768765 IP 162.125.34.129.443 > 10.99.102.180.61419: Flags [.], ack 3337, win 360, length 0
^C
15 packets captured
15 packets received by filter
0 packets dropped by kernel
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
```

3. Enter the following command:

   `sudo tcpdump -i <mirror-interface-name> -n -c 100 "port 9996"` (replace `<mirror-interface-name>` with an interface name, such as `eth0`).

Press **Enter** to capture traffic that matches port 9996/TCP. You can configure the command as necessary to look for specific traffic. See the following image for an example.



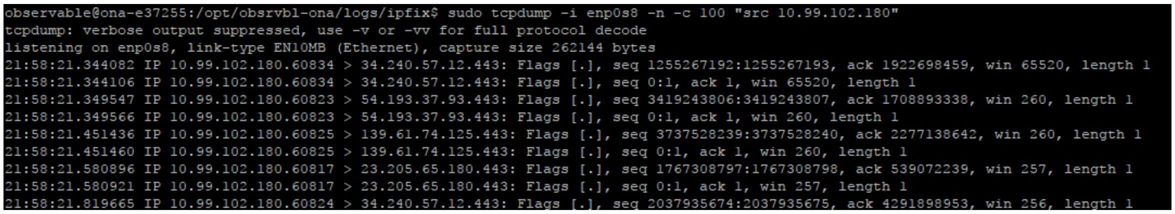
```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ sudo tcpdump -i enp0s8 -n -c 100 "port 9996"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), capture size 262144 bytes
```

4. Enter the following command:

   ```
   sudo tcpdump -i <mirror-interface-name> -n -c 100 "src 10.99.102.180"
   ```

   (replace `<mirror-interface-name>` with an interface name, such as `eth0`).

   Press **Enter** to capture traffic that matches a source IP address of `10.99.102.180`. See the following image for an example.



```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ sudo tcpdump -i enp0s8 -n -c 100 "src 10.99.102.180"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), capture size 262144 bytes
21:58:21.344082 IP 10.99.102.180.60834 > 34.240.57.12.443: Flags [.], seq 1255267192:1255267193, ack 1922698459, win 65520, length 1
21:58:21.344106 IP 10.99.102.180.60834 > 34.240.57.12.443: Flags [.], seq 0:1, ack 1, win 65520, length 1
21:58:21.349547 IP 10.99.102.180.60823 > 54.193.37.93.443: Flags [.], seq 3419243806:3419243807, ack 1708893338, win 260, length 1
21:58:21.349566 IP 10.99.102.180.60823 > 54.193.37.93.443: Flags [.], seq 0:1, ack 1, win 260, length 1
21:58:21.451436 IP 10.99.102.180.60825 > 139.61.74.125.443: Flags [.], seq 3737528239:3737528240, ack 2277138642, win 260, length 1
21:58:21.451460 IP 10.99.102.180.60825 > 139.61.74.125.443: Flags [.], seq 0:1, ack 1, win 260, length 1
21:58:21.580896 IP 10.99.102.180.60817 > 23.205.65.180.443: Flags [.], seq 1767308797:1767308798, ack 539072239, win 257, length 1
21:58:21.580921 IP 10.99.102.180.60817 > 23.205.65.180.443: Flags [.], seq 0:1, ack 1, win 257, length 1
21:58:21.819665 IP 10.99.102.180.60824 > 34.240.57.12.443: Flags [.], seq 2037935674:2037935675, ack 4291898953, win 256, length 1
```

Appendix B - Reference Information

Secure Cloud Analytics Documentation

The following describes Secure Cloud Analytics documentation that you can use to deploy sensors.

Resource	Description
Sensor Installation Guide	This guide contains installation instructions for the sensor on a VM or bare-metal server and best practices information on where and how to deploy the on-premises sensor. It also contains the IP addresses that the Secure Cloud Analytics service uses, in case a customer has to adjust firewall rules.
Public Cloud Monitoring for Amazon Web Services Quick Start Guide	This guide contains the process to enable an AWS account to be monitored by Secure Cloud Analytics.

Secure Cloud Analytics Files and Directories

The following private network monitoring Linux directories and file paths contain advanced sensor configuration.

- `/opt/obsrvbl-ona` – This directory contains the Secure Cloud Analytics configuration files (`config`, `config.auto`, `config.local`) and various sub-directories created during the sensor installation, including log file directories.
- `/opt/obsrvbl-ona/config` – This text file, created during the sensor installation, contains default sensor configuration. Cisco recommends that this file is not directly edited, changes should be made in `config.local`. If you want to edit this file, create a backup first. You can reference this file when updating the `config.local` file. Configuration settings in the `config.local` file overrides the default `config` file configuration.

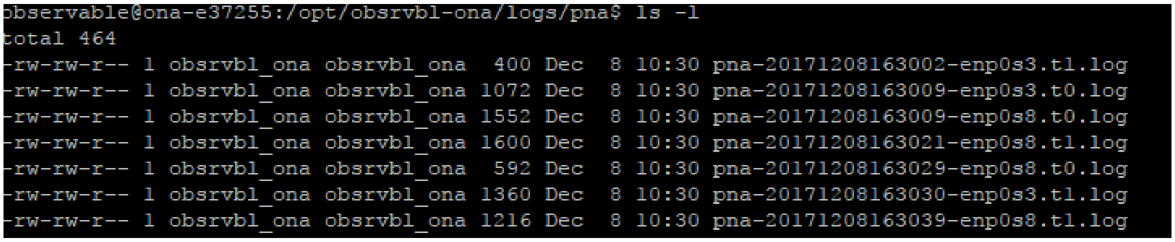
> The most recent version of the config configuration file is located on the Secure Cloud Analytics GitHub site at https://github.com/obsrvbl-oss/ona/blob/master/packaging/root/opt/obsrvbl-ona/config.

- /opt/obsrvbl-ona/config.auto – This text file contains sensor configuration changes users make from the web portal. For example, if you enable a sensor's logging to syslog or SNMP from the web portal, the web portal updates this file to include these configuration updates. Cisco recommends that you do **NOT** edit this file directly.
- /opt/obsrvbl-ona/config.local – This text file contains custom configuration for this sensor. Configuration updates to this file override configuration settings in the config configuration file. Examples of local configuration include, but are not limited to, enabling flow collection, setting flow collection types (e.g. NetFlow v5, IPFIX, etc.), and enabling 3rd party integration with programs like Suricata.

> Updating the config.local file to configure flow collection is intended primarily for older sensors that you deployed before ISO version ona-18.04.1-server-amd64.iso, available as of December 2018. You can redeploy older sensors using the current version of the sensor ISO, available in the web portal.

- /opt/obsrvbl-ona/logs/PNA – This directory contains log files related to flows created by the sensor's Ethernet ports. The sensor periodically uploads these files to the cloud, and empties the directory after it does so. You can monitor this directory to ensure that a mirror port is working properly, as the log files increment in byte count and quantity, relative to the size of the data entering the Ethernet ports.

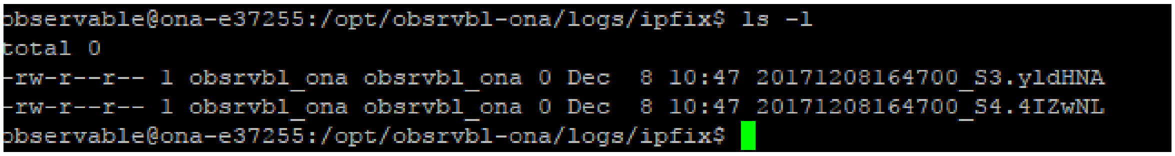
  In the following image, the log files are very small, indicating very little Ethernet port traffic. However, the service is running, and actively generating log files.



```
bservable@ona-e37255:/opt/obsrvbl-ona/logs/pna$ ls -l
total 464
-rw-rw-r-- 1 obsrvbl_ona obsrvbl_ona  400 Dec  8 10:30 pna-20171208163002-enp0s3.t1.log
-rw-rw-r-- 1 obsrvbl_ona obsrvbl_ona 1072 Dec  8 10:30 pna-20171208163009-enp0s3.t0.log
-rw-rw-r-- 1 obsrvbl_ona obsrvbl_ona 1552 Dec  8 10:30 pna-20171208163009-enp0s8.t0.log
-rw-rw-r-- 1 obsrvbl_ona obsrvbl_ona 1600 Dec  8 10:30 pna-20171208163021-enp0s8.t1.log
-rw-rw-r-- 1 obsrvbl_ona obsrvbl_ona  592 Dec  8 10:30 pna-20171208163029-enp0s8.t0.log
-rw-rw-r-- 1 obsrvbl_ona obsrvbl_ona 1360 Dec  8 10:30 pna-20171208163030-enp0s3.t1.log
-rw-rw-r-- 1 obsrvbl_ona obsrvbl_ona 1216 Dec  8 10:30 pna-20171208163039-enp0s8.t1.log
```

- /opt/obsrvbl-ona/logs/ipfix – This directory contains log files collected by the flow data feeds, such as NetFlow and IPFIX. If this directory exists, then flow collection is properly enabled and being received. If this directory does not exist, flow collection is probably not enabled.

  In the following image, the log files are not incrementing and are empty. The sensor is not receiving flow data.



```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ ls -l
total 0
-rw-r--r-- 1 obsrvbl_ona obsrvbl_ona 0 Dec  8 10:47 20171208164700_S3.yldHNA
-rw-r--r-- 1 obsrvbl_ona obsrvbl_ona 0 Dec  8 10:47 20171208164700_S4.4IZwNL
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ 
```

- `/etc/iptables` – This directory contains the `iptables` firewall configuration files for the sensor.

Appendix C - Services

Secure Cloud Analytics utilizes the following Linux services:

Service	Enabled by default?	Description
`obsrvbl-ona`	yes	Monitors for configuration changes and handles automatic updates. Starting this service also starts the other configured services.
`log-watcher`	yes	Tracks the sensor's authentication logs.
`pdns-capturer`	yes	Collects passive DNS queries.
`pna-monitor`	yes	Collects IP traffic metadata.
`pna-pusher`	yes	Sends IP traffic metadata to the cloud.
`hostname-resolver`	yes	Resolves active IP addresses to local hostnames.
`netflow-monitor`	no	Listens for NetFlow data sent by routers and switches.
`netflow-pusher`	no	Sends NetFlow data to the cloud.
`notification-publisher`	no	Relays observations and alerts over syslog or SNMP.
`ossec-alert-watcher`	no	Monitors OSSEC alerts, if installed.
`suricata-alert-watcher`	no	Monitors Suricata alerts, if installed.

Verify Running Services

You can verify that the various services are running from the sensor command line.

Before You Begin

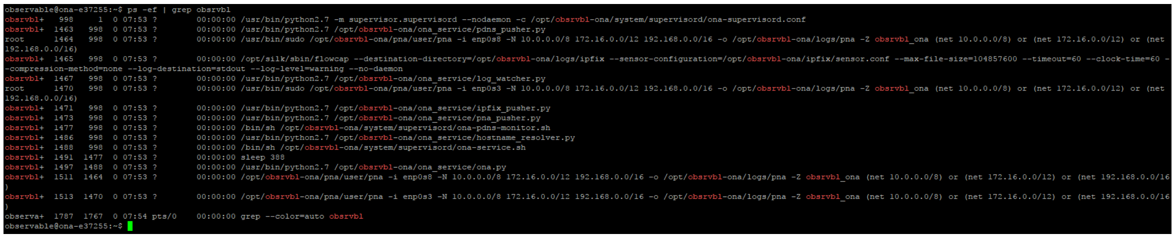
- SSH into the sensor and login as an administrator.

Summary Steps

```
ps -ef | grep obsrvbl
```

Procedure

1. At the command prompt, enter `ps -ef | grep obsrvbl` and press **Enter**. See the following image for an example.



```
observable@ona-e37255:~$ ps -ef | grep obsrvbl
obsrvbl+   998     1  0 07:53 ?        00:00:00 /usr/bin/python2.7 -m supervisor.supervisord --nodaemon -c /opt/obsrvbl-ona/system/supervisord/ona-supervisord.conf
obsrvbl+  1463   998  0 07:53 ?        00:00:00 /usr/bin/python2.7 /opt/obsrvbl-ona/ona_service/pdns_pusher.py
root      1464   998  0 07:53 ?        00:00:00 /usr/bin/sudo /opt/obsrvbl-ona/pna/user/pna -i enp0s8 -N 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 -o /opt/obsrvbl-ona/logs/pna -Z obsrvbl_ona (net 10.0.0.0/8) or (net 172.16.0.0/12) or (net
192.168.0.0/16)
obsrvbl+  1465   998  0 07:53 ?        00:00:00 /opt/silk/sbin/flowcap --destination-directory=/opt/obsrvbl-ona/logs/ipfix --sensor-configuration=/opt/obsrvbl-ona/ipfix/sensor.conf --max-file-size=104857600 --timeout=60 --clock-time=60 -
-compression-method=none --log-destination=stdout --log-level=warning --no-daemon
obsrvbl+  1467   998  0 07:53 ?        00:00:00 /usr/bin/python2.7 /opt/obsrvbl-ona/ona_service/log_watcher.py
root      1470   998  0 07:53 ?        00:00:00 /usr/bin/sudo /opt/obsrvbl-ona/pna/user/pna -i enp0s3 -N 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 -o /opt/obsrvbl-ona/logs/pna -Z obsrvbl_ona (net 10.0.0.0/8) or (net 172.16.0.0/12) or (net
192.168.0.0/16)
obsrvbl+  1471   998  0 07:53 ?        00:00:00 /usr/bin/python2.7 /opt/obsrvbl-ona/ona_service/ipfix_pusher.py
obsrvbl+  1473   998  0 07:53 ?        00:00:00 /usr/bin/python2.7 /opt/obsrvbl-ona/ona_service/pna_pusher.py
obsrvbl+  1477   998  0 07:53 ?        00:00:00 /bin/sh /opt/obsrvbl-ona/system/supervisord/ona-pdns-monitor.sh
obsrvbl+  1486   998  0 07:53 ?        00:00:00 /usr/bin/python2.7 /opt/obsrvbl-ona/ona_service/hostname_resolver.py
obsrvbl+  1488   998  0 07:53 ?        00:00:00 /bin/sh /opt/obsrvbl-ona/system/supervisord/ona-service.sh
obsrvbl+  1491  1477  0 07:53 ?        00:00:00 sleep 388
obsrvbl+  1497  1488  0 07:53 ?        00:00:00 /usr/bin/python2.7 /opt/obsrvbl-ona/ona_service/ona.py
obsrvbl+  1511  1464  0 07:53 ?        00:00:00 /opt/obsrvbl-ona/pna/user/pna -i enp0s8 -N 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 -o /opt/obsrvbl-ona/logs/pna -Z obsrvbl_ona (net 10.0.0.0/8) or (net 172.16.0.0/12) or (net 192.168.0.0/16
)
obsrvbl+  1513  1470  0 07:53 ?        00:00:00 /opt/obsrvbl-ona/pna/user/pna -i enp0s3 -N 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 -o /opt/obsrvbl-ona/logs/pna -Z obsrvbl_ona (net 10.0.0.0/8) or (net 172.16.0.0/12) or (net 192.168.0.0/16
)
observa+  1787  1767  0 07:54 pts/0    00:00:00 grep --color=auto obsrvbl
observable@ona-e37255:~$
```

Appendix D – Upgrading the Sensor

If your sensor is working properly, it is not necessary to upgrade it. However, if you find that it is missing a new feature (such as the ability to integrate with an external service), use one of the following procedures to upgrade it:

- **Upgrade with Ubuntu** If you downloaded the sensor image (ISO) from our web portal UI, use these instructions. This is the most common scenario.
- **Upgrade with Red Hat Enterprise Linux-Based Operating System**

Upgrade with Ubuntu

If you downloaded the sensor image (ISO) from our our web portal UI, use Ubuntu to upgrade your sensor.

Before You Begin

- Follow the instructions in **Checking Your Sensor Version** to review the current sensor version.
- Log in to the Ubuntu system as an administrator.

Summary Steps

1.
   ```
   sudo systemctl stop obsrvbl-ona.service
   ```

2.
   ```
   sudo cp /opt/obsrvbl-ona/config.auto ~/config.auto
   ```

3.
   ```
   sudo cp /opt/obsrvbl-ona/config.local ~/config.local
   ```

4.
   ```
   rm -f ona-service_UbuntuXenial_amd64.deb
   ```

5.
   ```
   wget https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_UbuntuXenial_amd64.deb
   ```

6.
   ```
   sudo apt remove --purge ona-service_UbuntuXenial_amd64.deb
   ```

7.
   ```
   sudo apt install ./ona-service_UbuntuXenial_amd64.deb
   ```

8.
   ```
   sudo cp ~/config.auto /opt/obsrvbl-ona/config.auto
   ```

9.
   ```
   sudo cp ~/config.local /opt/obsrvbl-ona/config.local
   ```

10.
    ```
    sudo chown obsrvbl_ona:obsrvbl_ona /opt/obsrvbl-ona/config.auto /opt/obsrvbl-ona/config.local
    ```

11.
    ```
    sudo systemctl restart obsrvbl-ona.service
    ```

Procedure

Run the commands in each section to complete the procedure for upgrading the sensor.

Stop the service and back up the existing configuration:

1. At the command prompt, enter this command:

   `sudo systemctl stop obsrvbl-ona.service`
   and press **Enter** to stop the service.

2. Enter `sudo cp /opt/obsrvbl-ona/config.auto ~/config.auto` and press **Enter**.

3. Enter `sudo cp /opt/obsrvbl-ona/config.local ~/config.local` and press **Enter**.

Download the new package:

4. Enter `rm -f ona-service_UbuntuXenial_amd64.deb` and press **Enter**.

5. Enter `wget https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_UbuntuXenial_amd64.deb` and press **Enter**.

Remove the old package and install the new one:

6. Enter `sudo apt remove --purge ona-service_UbuntuXenial_amd64.deb` and press **Enter**.

7. Enter `sudo apt install ./ona-service_UbuntuXenial_amd64.deb` and press **Enter**.

Restore your backup configuration:

8. Enter `sudo cp ~/config.auto /opt/obsrvbl-ona/config.auto` and press **Enter**.

9. Enter `sudo cp ~/config.local /opt/obsrvbl-ona/config.local` and press **Enter**.

10. Enter `sudo chown obsrvbl_ona:obsrvbl_ona /opt/obsrvbl-ona/config.auto /opt/obsrvbl-ona/config.local` and press **Enter**.

Restart the system:

11. Enter `sudo systemctl restart obsrvbl-ona.service` and press **Enter**.

Verify the update:

12. Follow the instructions in **Confirm a Sensor's Portal Connection** and confirm the sensor is shown in the list and receiving data.

13. Follow the instructions in **Checking Your Sensor Version** to confirm that the sensor version is updated.

Upgrade with Red Hat Enterprise Linux-Based Operating System

If you have a Red Hat Enterprise Linux-based operating system, such as CentOS, use the following instructions to upgrade your sensor.

Before You Begin

- Follow the instructions in **Checking Your Sensor Version** to review the current sensor version.
- SSH into the sensor and log in as an administrator.

Summary Steps

1. `sudo systemctl stop obsrvbl-ona.service`
2. `sudo cp /opt/obsrvbl-ona/config.auto ~/config.auto`
3. `sudo cp /opt/obsrvbl-ona/config.local ~/config.local`
4. `rm -f ona-service_RHEL_7_x86_64.rpm`
5. `curl -L -O https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_RHEL_8_x86_64.rpm`
6. `sudo yum remove ona-service`
7. `sudo yum install ./ona-service_RHEL_8_x86_64.rpm`
8. `sudo cp ~/config.auto /opt/obsrvbl-ona/config.auto`
9. `sudo cp ~/config.local /opt/obsrvbl-ona/config.local`
10. `sudo chown obsrvbl_ona:obsrvbl_ona /opt/obsrvbl-ona/config.auto /opt/obsrvbl-ona/config.local`
11. `sudo systemctl restart obsrvbl-ona.service`

Procedure

Run the commands in each section to complete the procedure for upgrading the sensor.

Stop the service and back up the existing configuration:

1. At the command prompt, enter this command:

   ```
   sudo systemctl stop obsrvbl-ona.service
   ```

   and press **Enter** to stop the service.
2. Enter `sudo cp /opt/obsrvbl-ona/config.auto ~/config.auto` and press **Enter**.

3. Enter `sudo cp /opt/obsrvbl-ona/config.local ~/config.local` and press **Enter**.

Download the new package:

4. Enter `rm -f ona-service_RHEL_7_x86_64.rpm` and press **Enter**.
5. Enter `curl -L -O https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_RHEL_8_x86_64.rpm` and press **Enter**.

Remove the old package and install the new one:

6. Enter `sudo yum remove ona-service` and press **Enter**.
7. Enter `sudo yum install ./ona-service_RHEL_8_x86_64.rpm` and press **Enter**.

Restore your backup configuration:

8. Enter `sudo cp ~/config.auto /opt/obsrvbl-ona/config.auto` and press **Enter**.
9. Enter `sudo cp ~/config.local /opt/obsrvbl-ona/config.local` and press **Enter**.
10. Enter `sudo chown obsrvbl_ona:obsrvbl_ona /opt/obsrvbl-ona/config.auto /opt/obsrvbl-ona/config.local` and press **Enter**.

Restart the system:

11. Enter `sudo systemctl restart obsrvbl-ona.service` and press **Enter**.

Verify the update:

12. Follow the instructions in **Confirm a Sensor's Portal Connection** and confirm the sensor is shown in the list and receiving data.
13. Follow the instructions in **Checking Your Sensor Version** to confirm that the sensor version is updated.

Additional Resources

For more information about Secure Cloud Analytics, refer to the following:

- https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html for a general overview
- https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html to sign up for a 60-day Free Trial
- https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html for documentation resources
- https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html for installation and configuration guides, including the Secure Cloud Analytics Initial Deployment Guide

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html
- For Secure Cloud Analytics Free Trial customers, open a case by email: swatchc-support@cisco.com

Change History

Revision	Revision Date	Description
1_0		Initial version.
1_5	February 8, 2018	Incorporates additional changes and updates to the installation process, and minor fixes to the text.
1_6	March 26, 2018	Added instructions for enabling NetFlow collection on manual Ubuntu Linux installations.
1_7	May 24, 2018	Fixed issue with NetFlow configuration.
1_8	May 25, 2018	Added IPFIX configuration reminder to appendix.
1_9	May 29, 2018	Fixed syntax issues with copying from document directly into Ubuntu.
1_10	June 19, 2018	Changed rendering format.
1_11	August 8, 2018	Corrected variable.
1_12	November 26, 2018	Updated sensor flow configuration.
1_13	January 22, 2019	Updated sensor flow collection configuration and corrected miscellaneous errors.
1_14	18 April 18, 2019	Updated deprecated terms.

1_15	September 4, 2020	Updated UI directions.
1_16	October 16, 2020	Updated based on UI updates.
1_17	August 03, 2021	Updated the "Manually Installing the Package for Linux Operating Systems" section. Updated the "Checking your Sensor Version" section. Updated branded terms. Added "Appendix D - Upgrading the Sensor."
2_0	February 10, 2022	Updated portal URLs. Added RHEL 8 information. Added Ubuntu 20.04 information.
2_1	June 8, 2022	Updated sensor download URLs. Updated sensor installation steps. Updated reference documentation.
3_0	August 1, 2022	Added Contacting Support and Additional Resources. Updated document title.
3_1	January 17, 2023	Updated GitHub repository link.
4_0	March 29,2023	Updated Manually Installing the Package for Linux

		Operating Systems section • RHEL 7 • RHEL 8
4_1	July 24, 2023	Fixed a typo.

Copyright Information