Cisco Stealthwatch Cloud

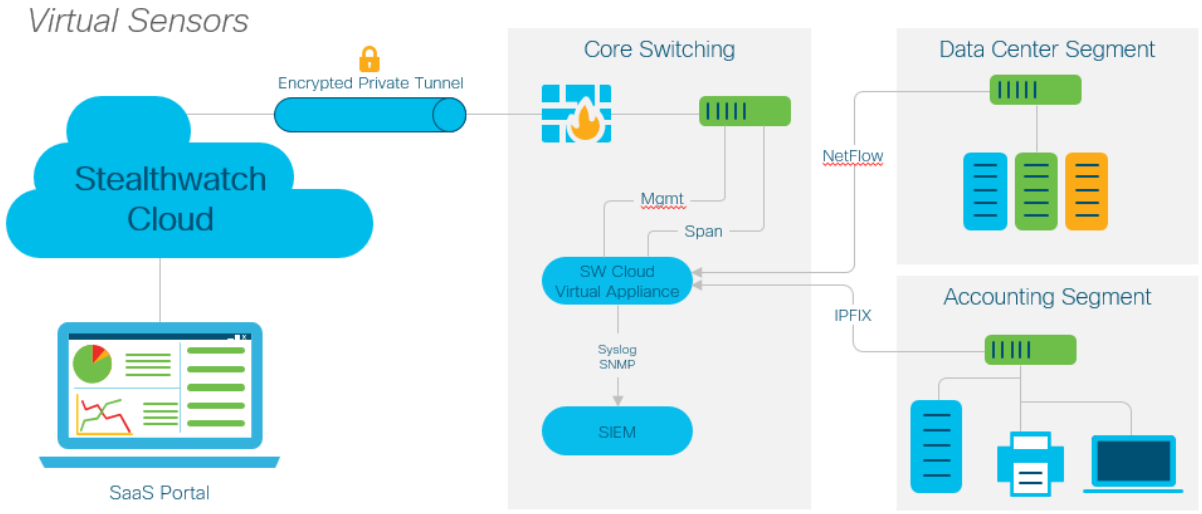
Private Network Monitoring Advanced Configuration Guide

TOC

About Stealthwatch Cloud Private Network Monitor Sensor

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

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 VA 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 (version 4.0), you can check an existing sensor's version from the command line. If you need to upgrade, reinstall the sensor.

Check your sensor version:

Procedure

1. SSH log into a deployed sensor.
2. At the prompt, enter `cat /opt/obsrvbl-ona/version` and press Enter. If the console does not display 4.0.0, your sensor is out of date. Download the most recent sensor ISO from the web portal UI.

Manually Installing the Package for Linux Operating Systems

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

- Ubuntu Linux version 14.04 (32- and 64-bit)
- Ubuntu Linux versions 16.04 and later (32- and 64-bit)
- Red Hat Enterprise Linux (RHEL) version 6 and compatible, including CentOS version 6* and Amazon Linux for EC2 (32- and 64-bit)
- Red Hat Enterprise Linux (RHEL) version 7 and compatible, including CentOS version 7 (64-bit)
- Raspberry Pi 2 Model B with Raspbian (32-bit armhf)
- Docker, tested with CoreOS (64-bit)

Install on RHEL 7

Before You Begin

- Log into the RHEL 7 system as an administrator.

Summary Steps

1. `curl -L -O https://s3.amazonaws.com/onstatic/ona-service/master/ona-service_RHEL_7_x86_64.rpm`
2. `sudo yum install -y net-tools tcpdump`
3. `sudo yum updateinfo && yum install -y libpcap libtool-ltdl lzo`
4. `curl -L -O https://github.com/bbayles/netsa-pkg/releases/download/v0.1.15/netsa-pkg.rpm`
5. `sudo rpm -i netsa-pkg.rpm`
6. `sudo rpm -i ona-service_RHEL_7_x86_64.rpm`

Procedure

1. At the command prompt, enter `curl -L -O https://s3.amazonaws.com/onstatic/ona-service/master/ona-service_RHEL_7_x86_64.rpm` and press Enter to download the Stealthwatch Cloud package.

2. Enter `sudo yum install -y net-tools tcpdump` and press Enter to install dependencies.

3. Enter `sudo yum updateinfo && yum install -y libpcap libtool-ltdl lzo` and press Enter to install updates and additional packages.

4. Enter `curl -L -O https://github.com/bbayles/netsa-pkg/releases/download/v0.1.15/netsa-pkg.rpm` and press Enter to download the `netsa-pkg.rpm` package manager file.

5. Enter `sudo rpm -i netsa-pkg.rpm` and press Enter to install the `netsa-pkg.rpm` package manager file.

6. Enter `sudo rpm -i ona-service_RHEL_7_x86_64.rpm` and press Enter to install the Stealthwatch Cloud service.

Install on RHEL 6

RHEL 6 does not include Python 2.7. Additional repositories must be added to install Python.

Before You Begin

- Log into the RHEL 6 system as an administrator.

Summary Steps

1. `curl -L -O https://s3.amazonaws.com/onstatic/ona-service/master/ona-service_RHEL_6_x86_64.rpm`
2. `curl -L -O https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm`
3. You have the following options:
    - `curl -L -O https://rhel6.iuscommunity.org/ius-release.rpm` for RHEL
    - `curl -L -O https://centos6.iuscommunity.org/ius-release.rpm` for CentOS
4. You have the following options:
    - `sudo rpm -i epel-release-latest-6.noarch.rpm` for RHEL
    - `sudo rpm -i ius-release.rpm` for CentOS
5. `sudo yum install python27 tcpdump`

6. `sudo yum updateinfo && yum install -y libpcap libtool-ltdl lzo`
7. `curl -L -O https://github.com/bbayles/netsa-pkg/releases/download/v0.1.15/netsa-pkg.rpm`
8. `sudo rpm -i netsa-pkg.rpm`
9. `sudo rpm -i ona-service_RHEL_6_x86_64.rpm`

Procedure

1. At the command prompt, enter `curl -L -O https://s3.amazon-aws.com/onstatic/ona-service/master/ona-service_RHEL_6_x86_64.rpm` and press Enter to download the Stealthwatch Cloud package.
2. Enter `curl -L -O https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm` and press Enter to download the EPEL repository package.
3. You have the following options:
   - Enter `curl -L -O https://rhel6.iuscommunity.org/ius-release.rpm` and press Enter to download the IUS repository package for RHEL.
   - Enter `curl -L -O https://centos6.iuscommunity.org/ius-release.rpm` and press Enter to download the IUS repository package for CentOS.
4. You have the following options:
   - Enter `sudo rpm -i epel-release-latest-6.noarch.rpm` to install the IUS repository package for RHEL.
   - Enter `sudo rpm -i ius-release.rpm` to install the IUS repository package for CentOS.
5. Enter `sudo yum install python27 tcpdump` and press Enter to install Python 2.7.
6. Enter `sudo yum updateinfo && yum install -y libpcap libtool-ltdl lzo` and press Enter to install updates and additional packages.
7. Enter `curl -L -O https://github.com/bbayles/netsa-pkg/releases/download/v0.1.15/netsa-pkg.rpm` and press Enter to download the `netsa-pkg.rpm` package manager file.
8. Enter `sudo rpm -i netsa-pkg.rpm` and press Enter to install the `netsa-pkg.rpm` package manager file.

9. Enter `sudo rpm -i ona-service_RHEL_6_x86_64.rpm` and press Enter to install the Stealthwatch Cloud service.

Install on Ubuntu with NetFlow collection

Before You Begin

- Log into the Ubuntu system as an administrator.

Summary Steps

1. `curl -L -O https://s3.amazonaws.com/onstatic/ona-service/master/ona-service_UbuntuXenial_amd64.deb`
2. `sudo apt-get install -y net-tools tcpdump`
3. `sudo apt-get update && sudo apt-get install -y libglib2.0-0 liblzo2-2 libltdl7`
4. `curl -L -O https://github.com/bbayles/netsa-pkg/releases/download/v0.1.15/netsa-pkg.deb`
5. `sudo dpkg -i netsa-pkg.deb`
6. `sudo apt-get -f install`
7. `sudo dpkg -i ona-service_UbuntuXenial_amd64.deb`
8. `sudo reboot`
9. Confirm services are running, see Appendix C for Stealthwatch Cloud services.

Procedure

1. At the command prompt, enter `curl -L -O https://s3.amazonaws.com/onstatic/ona-service/master/ona-service_UbuntuXenial_amd64.deb` and press Enter to download the Stealthwatch Cloud package.
2. Enter `sudo apt-get install -y net-tools tcpdump` and press Enter to install dependencies.
3. Enter `sudo apt-get update && sudo apt-get install -y libglib2.0-0 liblzo2-2 libltdl7` and press Enter to install updates and additional packages.
4. Enter `curl -L -O https://github.com/bbayles/netsa-pkg/releases/download/v0.1.15/netsa-pkg.deb` and press Enter to download the `netsa-pkg.rpm` package manager file.
5. Enter `sudo dpkg -i netsa-pkg.deb` and press Enter to install the `netsa-pkg.rpm` package manager file.

6. Enter `sudo apt-get -f install` to verify dependencies installed properly.
7. Enter `sudo dpkg -i ona-service_UbuntuXenial_amd64.deb` and press Enter to install the Stealthwatch Cloud service.
8. Enter `sudo reboot` and press Enter to reboot Linux.
9. Confirm services are running. See **Appendix C - Stealthwatch Cloud Services** for Stealthwatch Cloud services.

Install on Ubuntu without NetFlow collection

Before You Begin

- Log into the Ubuntu system as an administrator.

Summary Steps

1. `curl -L -O https://s3.amazonaws.com/onstatic/ona-service/master/ona-service_UbuntuXenial_amd64.deb`
2. `sudo apt-get install -y net-tools tcpdump`
3. `sudo apt-get -f install`
4. `sudo dpkg -i ona-service_UbuntuXenial_amd64.deb`

Procedure

1. At the command prompt, enter `curl -L -O https://s3.amazonaws.com/onstatic/ona-service/master/ona-service_UbuntuXenial_amd64.deb` and press Enter to download the Stealthwatch Cloud package.
2. Enter `sudo apt-get install -y net-tools tcpdump` and press Enter to install dependencies.
3. Enter `sudo apt-get -f install` to verify dependencies installed properly.
4. Enter `sudo dpkg -i ona-service_UbuntuXenial_amd64.deb` and press Enter to install the Stealthwatch Cloud service.

Attaching Sensors to the Stealthwatch Cloud Portal

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

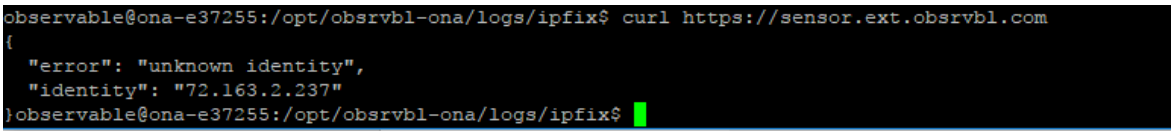
> If multiple sensors are staged in a central location, such as an MSSP, and they are intended for different customers, the public IP should be removed after each new customer is configured. If a public IP address of the staging environment is used for multiple sensors, a sensor could be incorrectly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

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

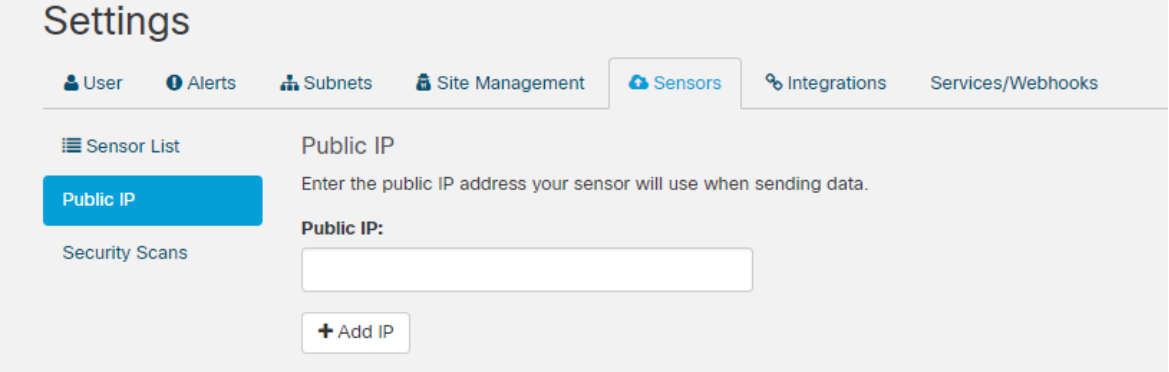
Before You Begin

- SSH into the sensor and login as an administrator.

1. 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 screenshot for an example.



2. Copy the `identity` IP address.
3. Log out of the sensor.
4. Log into the web portal as a site administrator.
5. Select the **sensors (☁) icon > Public IP**.
6. Enter the `identity` IP address in the Public IP field. See the following screenshot for an example.



7. 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. Cisco recommends 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.

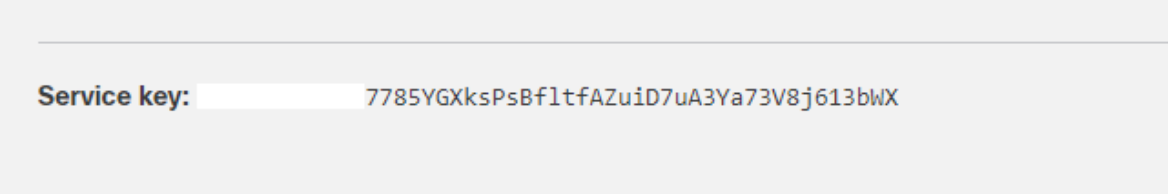
If you cannot add a sensor's public IP address to the web portal, or you are an MSSP managing multiple web portals, edit a sensor's `config.local` configuration file on the VA to manually add a portal's service key to associate the sensor with the portal.

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

Before You Begin

Log into the portal web UI as an administrator.

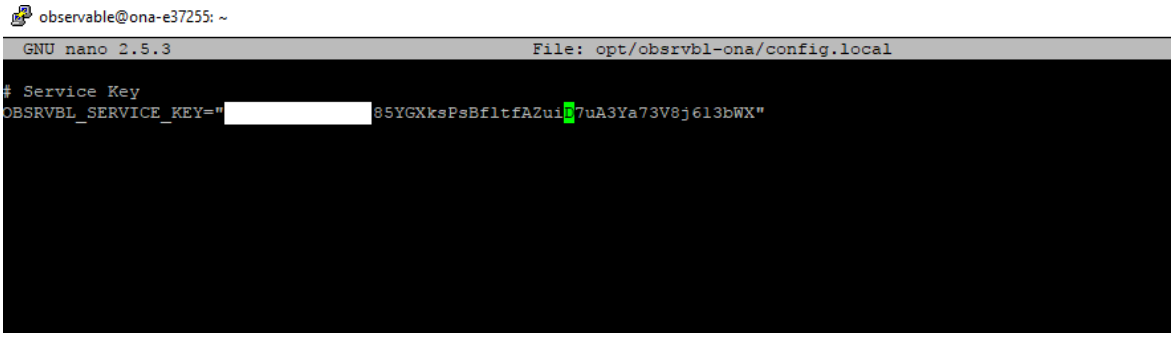
1. Select **Settings > Sensors**.
2. Navigate to the end of the sensor list and copy the **Service key**. See the following screenshot for an example.



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

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

   See the following for an example.



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

Confirm a Sensor's Portal Connection

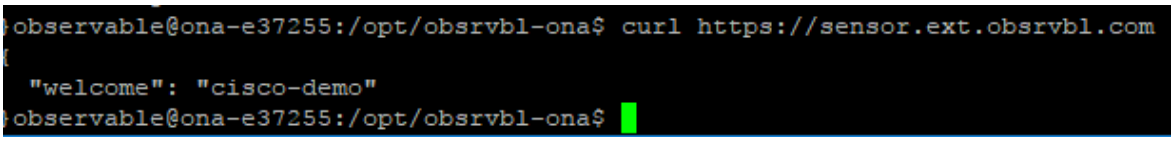
After a sensor is added to the portal, confirm the connection.

> 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.

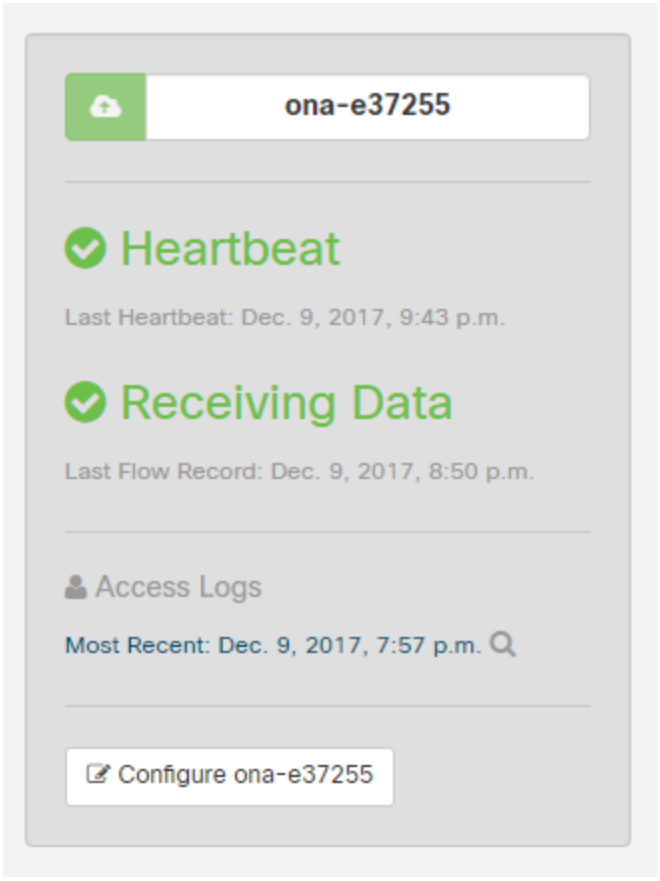
Before You Begin

SSH log into the sensor as an administrator.

1. At the command prompt, enter `curl https://sensor.ext.obsrvbl.com` and press Enter. The sensor returns the portal name. See the following screenshot for an example.



2. Log out of the sensor.
3. Log into the portal web UI.
4. Select **Settings > Sensors**. The sensor appears in the list. See the following screenshot for an example.



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**.

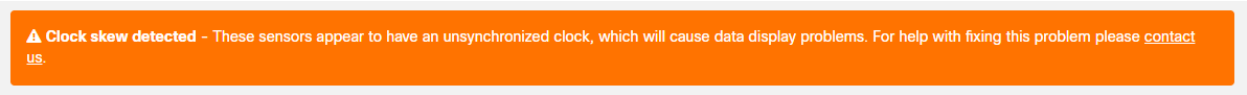
> This option requires an up-to-date sensor version. If you do not see this option, select **Help (?) > On-Prem Sensor Install** to download a current version of the sensor ISO.

4. Click **Add New Probe**.
5. Select a flow type from the **Probe Type** drop-down.
6. Enter a **Port** number.
7. Select a **Protocol**.
8. Select a **Source device** from the drop-down.
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 screenshot for an example.



Before You Begin

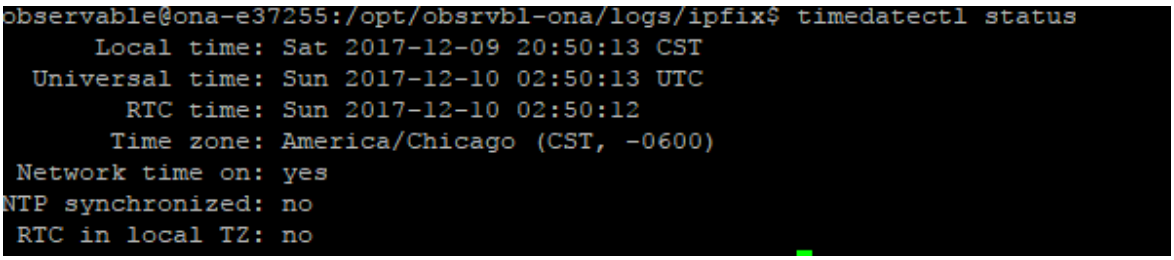
- SSH log into the sensor as an administrator.

Summary Steps

1. `timedatectl status` and press Enter to verify if NTP is synchronized.
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 screenshot for an example of a sensor that is not properly synchronized with NTP:



2. Enter `sudo apt-get update && sudo apt-get install -y ntpdate ntp` and press Enter to ensure that the correct NTP packages are installed and up-to-date.
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 screenshot 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 screenshot 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
```

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

Resolve Unidirectional Traffic Errors

The Stealthwatch Cloud 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 log into the sensor as an administrator.

Summary Steps

1. `ifconfig –a`
2. `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. `sudo tcpdump –i <mirror-interface-name> -n –c 100 "port 9996"` and press Enter to capture traffic that matches port 9996/TCP.
4. `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 screenshot for an example; the `enp0s8` interface sees much more traffic, which is indicative of a mirror port.

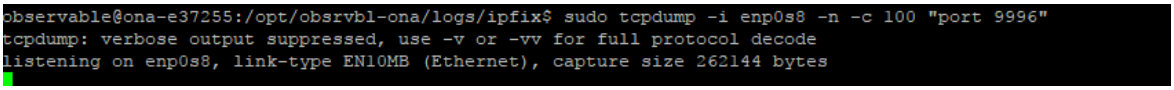
```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ ifconfig -a
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:8e:aa:ef
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8e:aaef/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  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 `sudo tcpdump -i <mirror-interface-name> -n -c 100 "tcp"`, replace `<mirror-interface-name>` with an interface name, such as `eth0`, and press Enter to capture traffic passing through the mirror interface, to ensure it is seeing TCP traffic, not just broadcast traffic. See the following screenshot for an example.

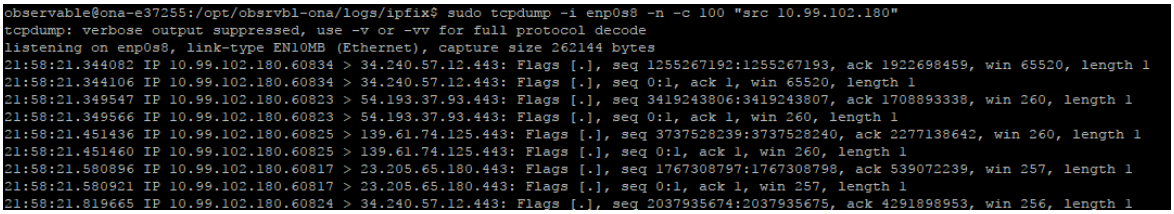
```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ sudo tcpdump -i enp0s8 -n -c 100 "tcp"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), capture size 262144 bytes
21:50:23.955066 IP 64.100.36.170.7080 > 10.99.102.180.51726: 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 `sudo tcpdump -i <mirror-interface-name> -n -c 100 "port 9996"`, replace `<mirror-interface-name>` with an interface name, such as `eth0`, and 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 screenshot for an example.



4. Enter `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`, and press Enter to capture traffic that matches a source IP address of `10.99.102.180`. See the following screenshot for an example.



Appendix B - Stealthwatch Cloud Reference Information

Stealthwatch Cloud Documentation

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

Resource	Description	Link
Sensor Installation Guide	This guide contains installation instructions for the PNM on a VM or bare-metal server. It also contains the IP addresses that the Stealthwatch Cloud service uses, in case a customer has to adjust firewall rules.	https://s3.amazonaws.com/onstatic/iso-install-guide.pdf
Network Considerations Guide	This guide contains best practices information on where and how to deploy the on-premises sensor.	https://s3.amazonaws.com/onstatic/network-setup-considerations.pdf
AWS Configuration Guide	This guide contains the process to enable an AWS account to be monitored by Stealthwatch Cloud.	https://s3.amazonaws.com/onstatic/vpc-flow-logs.pdf

Stealthwatch Cloud Files and Directories

The following PNM Linux directories and file paths contain advanced sensor configuration.

- `/opt/obsrvbl-ona` – This directory contains the Stealthwatch Cloud 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 Stealthwatch Cloud GitHub site at https://github.com/obsrvbl/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 screenshot, the log files are very small, indicating very little Ethernet port traffic. However, the service is running, and actively generating log files.

```
observable@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.tl.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.tl.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.tl.log
-rw-rw-r-- 1 obsrvbl_ona obsrvbl_ona 1216 Dec  8 10:30 pna-20171208163039-enp0s8.tl.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 screenshot, 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 - Stealthwatch Cloud Services

Stealthwatch Cloud 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 Stealthwatch Cloud services are running from the sensor command line.

Before You Begin

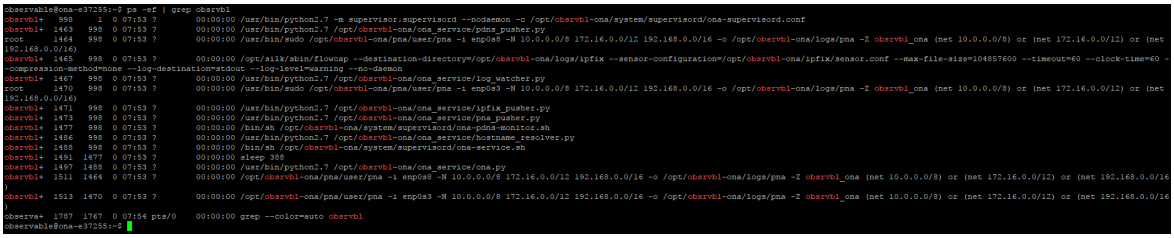
- SSH into the sensor and login as an administrator.

Summary Steps

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

Procedure

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



Change History

Revision	Revision Date	Description
1.0		Initial version.
1.5	8 February 2018	Incorporates additional changes and updates to the installation process, and minor fixes to the text.
1.6	26 March 2018	Added instructions for enabling NetFlow collection on manual Ubuntu Linux installations.
1.7	24 May 2018	Fixed issue with NetFlow configuration.
1.8	25 May 2018	Added IPFIX configuration reminder to appendix.
1.9	29 May 2018	Fixed syntax issues with copying from document directly into Ubuntu.
1.10	19 June 2018	Changed rendering format.
1.11	8 August 2018	Corrected variable.
1.12	26 November 2018	Updated sensor flow configuration.
1.13	22 January 2019	Updated sensor flow collection configuration and corrected miscellaneous errors.
1.14	18 April 2019	Updated deprecated terms.
1.15	4 September 2020	Updated UI directions.
1.16	16 October 2020	Updated based on UI updates.

Copyright Information