Solucionar problemas de estado sin conexión del sensor ONA

Contenido

Introducción

En este documento se describe cómo investigar varias causas posibles de que un sensor de Secure Cloud Analytics (SCA) aparezca como desconectado.

Antecedentes

Secure Cloud Analytics (SCA) se denominaba anteriormente StealthWatch Cloud (SWC) y estos términos pueden utilizarse indistintamente.

El sensor SCA es el monitor de red privada y se puede hacer referencia como ONA, sensor ONA o simplemente como sensor.

Los comandos de este artículo se basan en la instalación de ona-20.04.1-server-amd64.iso debian.

Posibles causas de los sensores sin conexión

Hay muchos factores posibles que pueden hacer que un sensor presente un estado fuera de línea.

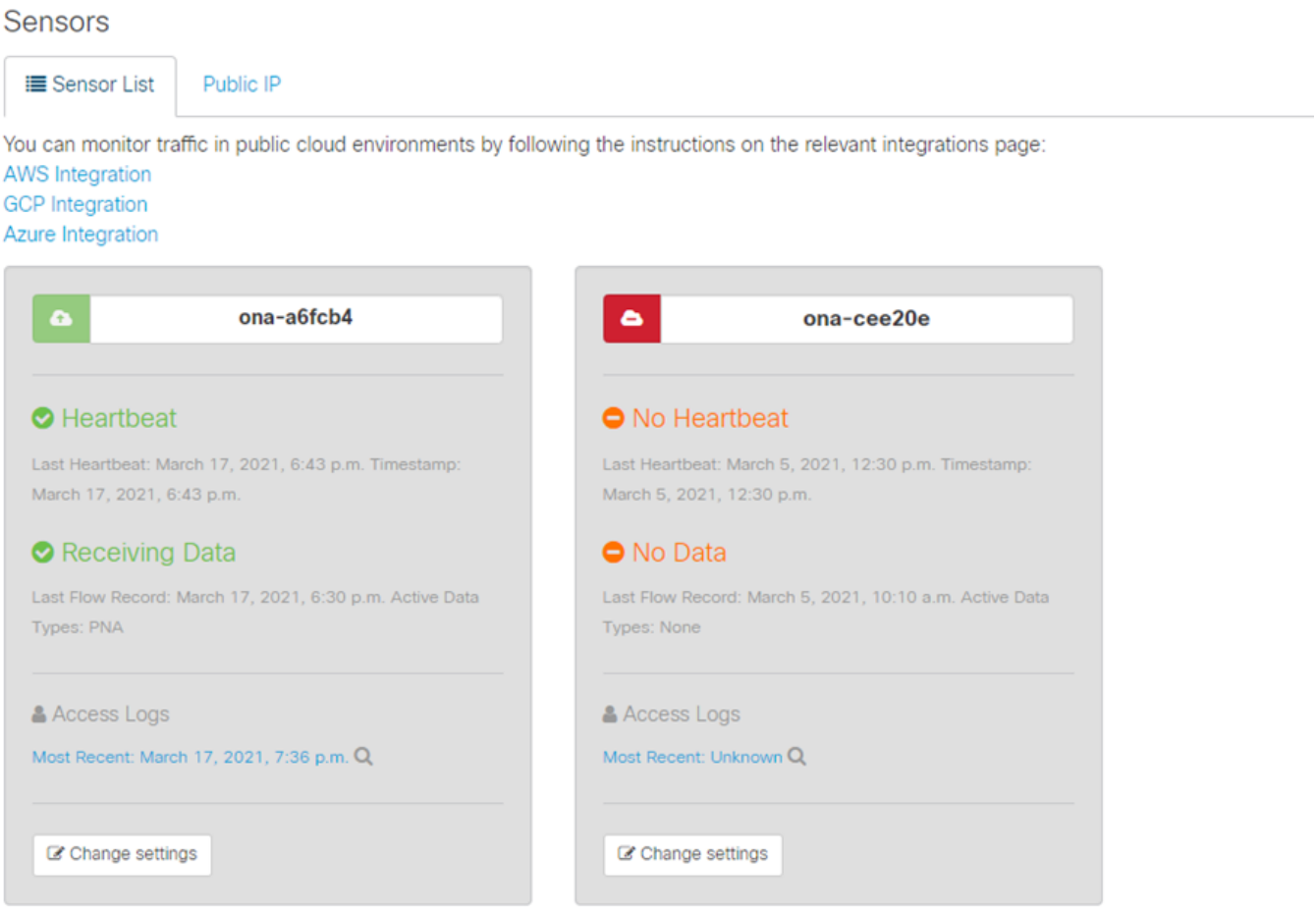
Dos ejemplos de estos factores son los problemas relacionados con la red y el sistema de archivos local tiene un disco completo.

Identificar un sensor fuera de línea

El portal de SCA contiene una lista de sensores configurados. Para acceder a esta página, vaya a

Settings > Sensors.

El sensor fuera de línea de esta imagen se representa en rojo y no muestra ningún latido y datos recientes.



Investigar un sensor fuera de línea

Problemas de red

El host ONA puede perder el acceso a Internet, lo que hace que el sensor aparezca como desconectado.

Pruebe si el host ONA puede hacer ping a una dirección IP activa conocida, como uno de los servidores DNS de Google en 8.8.8.8.

Inicie sesión en el sensor ONA y ejecute el comando **ping -c4 8.8.8.8**.

<#root>

```
user@example-ona:~#
```

ping -c4 8.8.8.8

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 10.10.10.11 icmp_seq=1 Destination Host Unreachable
From 10.10.10.11 icmp_seq=2 Destination Host Unreachable
From 10.10.10.11 icmp_seq=3 Destination Host Unreachable
From 10.10.10.11 icmp_seq=4 Destination Host Unreachable

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3065ms
user@example-ona:~#
```

Si el sensor no puede hacer ping a una dirección IP activa conocida, siga investigando.

Determine la gateway predeterminada con el route -n comando.

Determine si existe una entrada válida del Protocolo de resolución de direcciones (ARP) para la puerta de enlace predeterminada con el **arp -an** comando.

Si el sensor es capaz de hacer ping a una dirección IP conocida, pruebe la resolución del nombre de host DNS y la capacidad del sensor para conectarse a la nube.

Inicie sesión en el Sensor y ejecute el sudo curl https://sensor.ext.obsrvbl.com comando.

El resultado del comando curl muestra que la resolución de DNS para sensor.ext.obsrvbl.com falló y la investigación de DNS está garantizada.

<#root>

```
user@example-ona:~#
```

sudo curl https://sensor.ext.obsrvbl.com

```
[sudo] password for user:
curl: (6) Could not resolve host: sensor.ext.obsrvbl.com
user@example-ona:~#
```

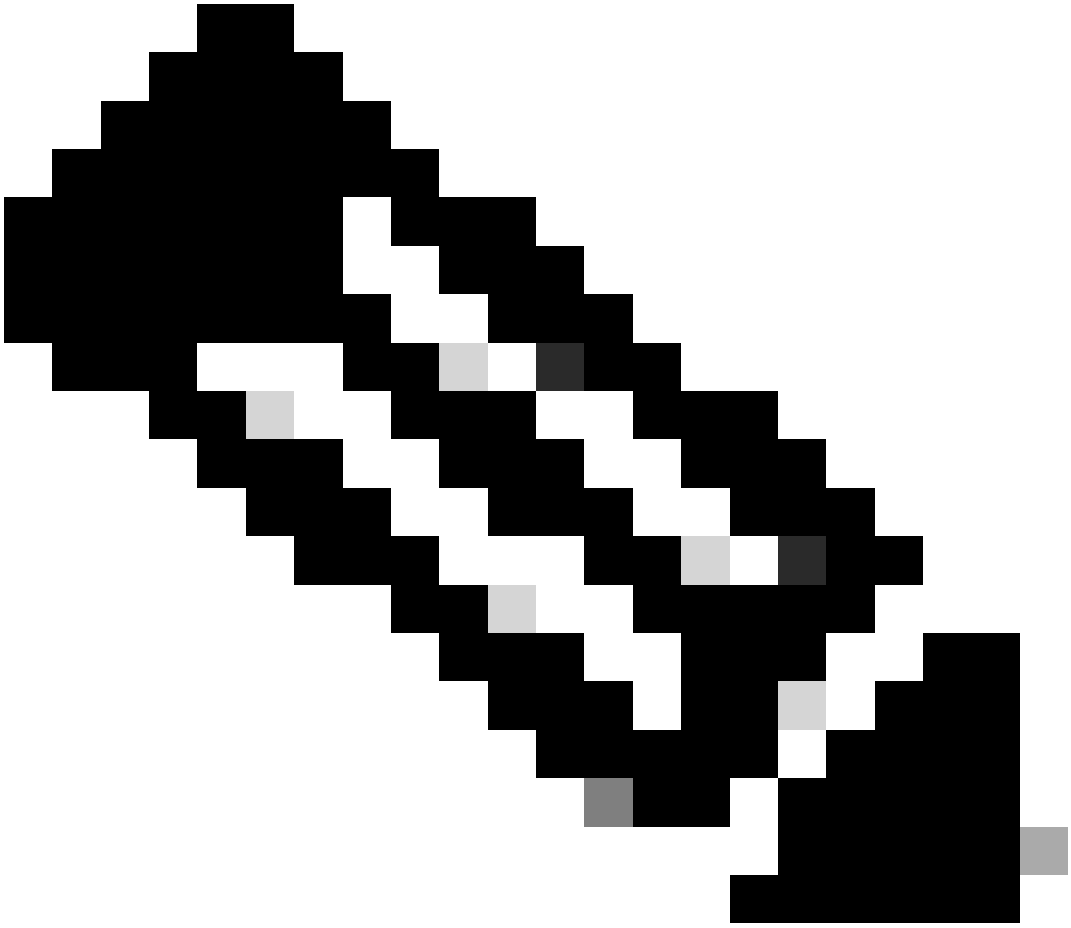
Este tipo de respuesta indica una buena conexión y también que el portal de la nube reconoce el sensor.

<#root>

user@example-ona:~#

sudo curl https://sensor.ext.obsrvbl.com

[sudo] password for user:
{"welcome":"example-domain"}
user@example-ona:~#



Nota: El comando curl se puede modificar para utilizar la región adecuada US: https://sensor.ext.obsrvbl.com Europe: https://sensor.eu-prod.obsrvbl.com Australia: https://sensor.anz-prod.obsrvbl.com

Este tipo de respuesta indica una buena conexión, pero el sensor no se ha asociado a un dominio concreto.

```
user@example-ona:~# sudo curl https://sensor.anz-prod.obsrvbl.com
[sudo] password for user:
{"error":"unknown identity","identity":"240.0.0.0"}
user@example-ona:~#
```

Problemas de DNS

Si Sensor no puede resolver los nombres de host con DNS, verifique la configuración de DNS con el cat /etc/netplan/01-netcfg.yaml comando.

si la configuración de DNS requiere cambios, consulte la sección Actualización de la configuración de DNS.

Una vez validados los parámetros de DNS, ejecute el sudo systemctl restart systemd-resolved.service comando.

No se espera ningún resultado con este comando.

<#root>

```
user@example-ona:~#
```

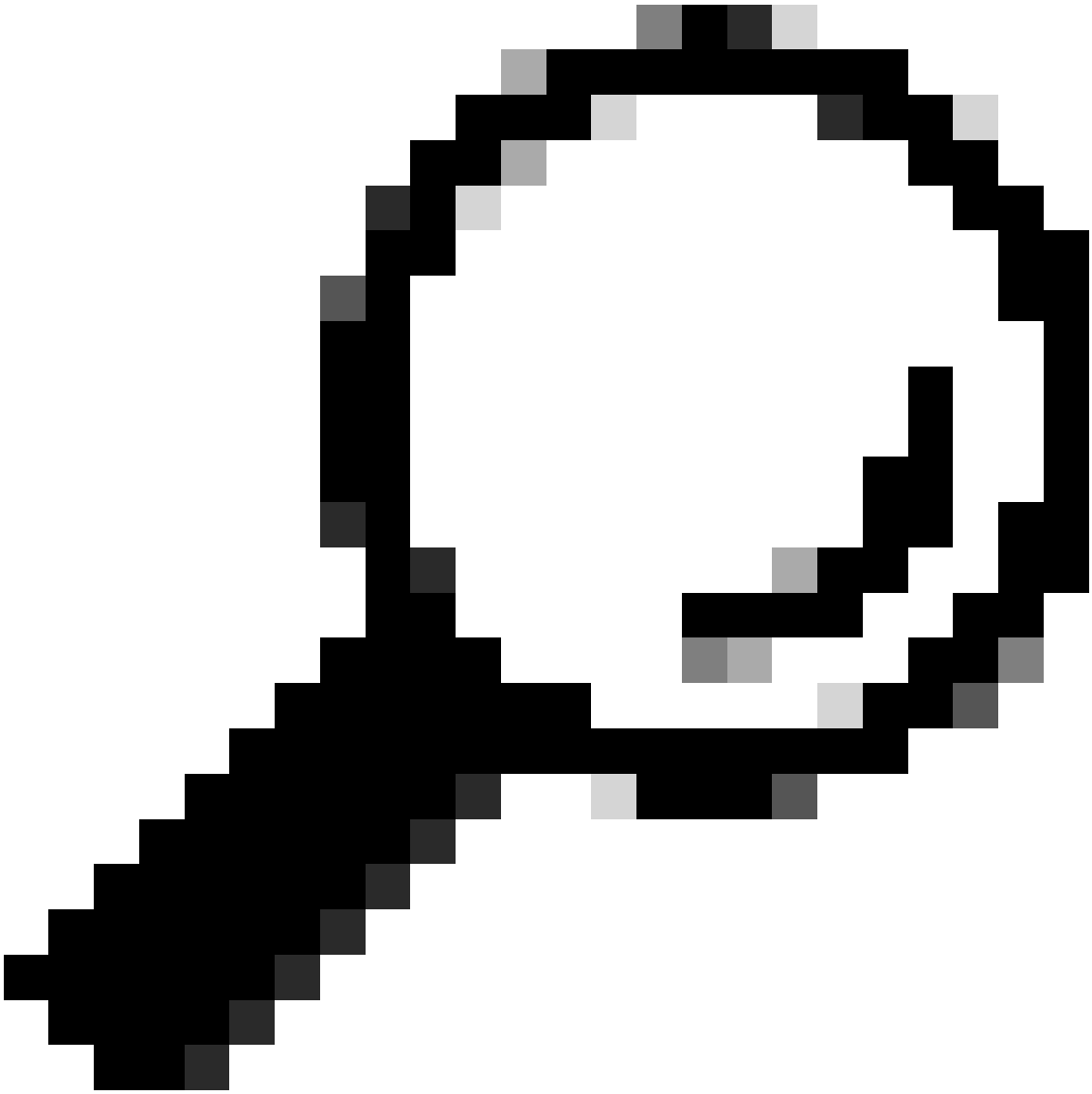
sudo systemctl restart systemd-resolved.service

```
[sudo] password for user:
user@example-ona:~#
```

Actualizar la configuración DNS

Para actualizar los servidores DNS en Netplan, puede modificar el archivo de configuración de Netplan para la interfaz de red.

Los archivos de configuración de Netplan se almacenan en el directorio **/etc/netplan**.



Sugerencia: Se pueden encontrar uno o dos archivos YAML en este directorio. Los nombres de archivo esperados son 01-netcfg.yaml o 50-cloud-init.yaml.

Abra el archivo de configuración de Netplan con el sudo vi /etc/netplan/01-netcfg.yaml comando.

En el archivo de configuración de Netplan, localice la clave "nameservers" en la interfaz de red.

Puede especificar varias direcciones IP de servidor DNS separadas por comas.

Aplique los cambios a la configuración de Netplan con el **sudo netplan apply** comando.

Netplan genera los archivos de configuración para el servicio resuelto por el sistema.

Para verificar que los nuevos resolvers DNS están configurados, ejecute el resolvectl status | grep -A2 'DNS Servers' comando.

<#root>

```
user@example-ona:~#
```

resolvectl status | grep -A2 'DNS Servers'

```
 DNS Servers: 10.122.147.56
 DNS Domain: example.org

user@example-ona:~#
```

Sistema de archivos local completo

Un mensaje de error común puede aparecer en la consola del Sensor: "Error al crear el nuevo diario del sistema: No queda espacio en el dispositivo."

Esto indica que el disco está lleno y no queda más espacio en el sistema de archivos / root.

Ejecute el df -ah / comando y determine cuánto espacio está disponible.

<#root>

```
user@example-ona:~#
```

df -ah /

```
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/vgona--default-root 30G 30G 0G 100% /
user@example-ona:~#
```

Borre los antiguos registros del diario para liberar espacio en disco con el journalctl --vacuum-time 1d comando.

<#root>

```
user@example-ona:~#
```

journalctl --vacuum-time 1d

```
Vacuuming done, freed 0B of archived journals from /var/log/journal.
{Removed for brevity}
Vacuuming done, freed 2.9G of archived journals from /var/log/journal/315bfec86e0947b2a3a23da2a672e577.
Vacuuming done, freed 0B of archived journals from /run/log/journal.
user@example-ona:~#
```

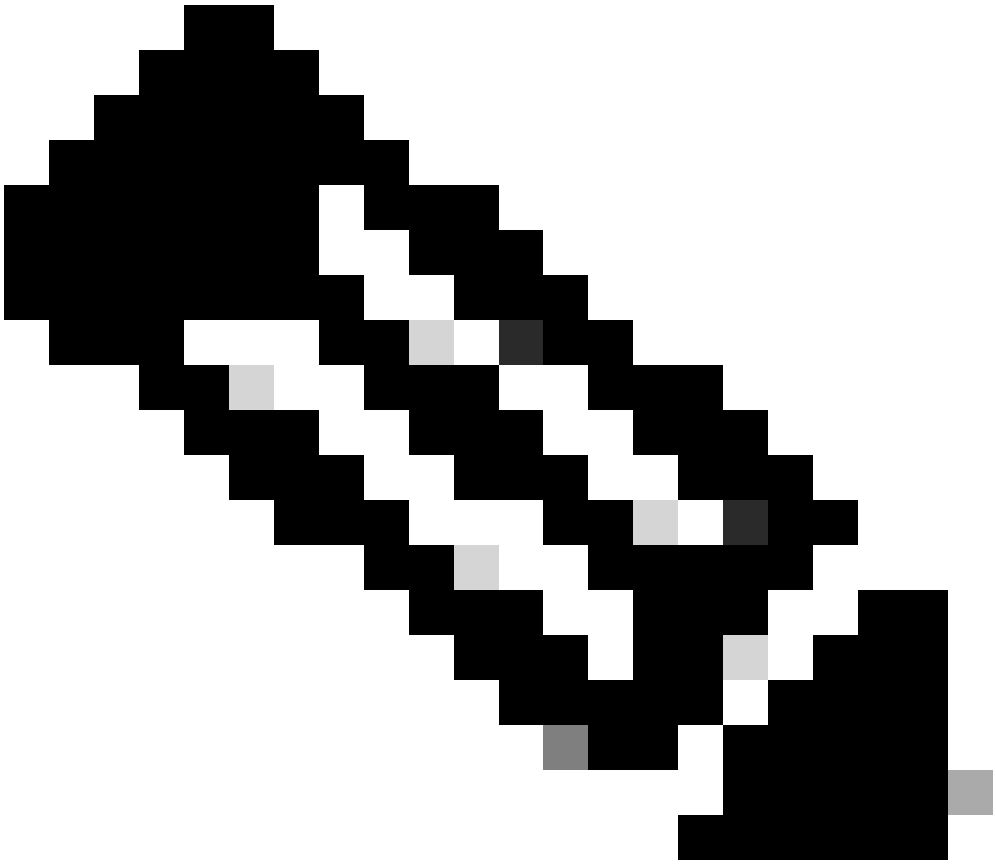
Asegúrese de que el espacio de almacenamiento cumple los requisitos mínimos del sistema descritos en la guía de implementación inicial.

La guía se puede recuperar en la página de soporte de productos de Cisco Secure Cloud Analytics (Stealthwatch Cloud): https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/series.html

Configuración de supervisión

Un sensor que tenga buena conectividad de red con la nube y una configuración de DNS válida puede seguir presentando un estado sin conexión.

Un estado fuera de línea es posible si las opciones de monitoreo del sensor están inhabilitadas o el sensor no envía latidos.



Nota: Esta sección es para una instalación predeterminada del sensor ONA sin personalizaciones y recibe activamente datos de NetFlow y/o IPFIX.

Ejecute el grep PNA_SERVICE /opt/obsrvbl-ona/config comando para determinar el estado.

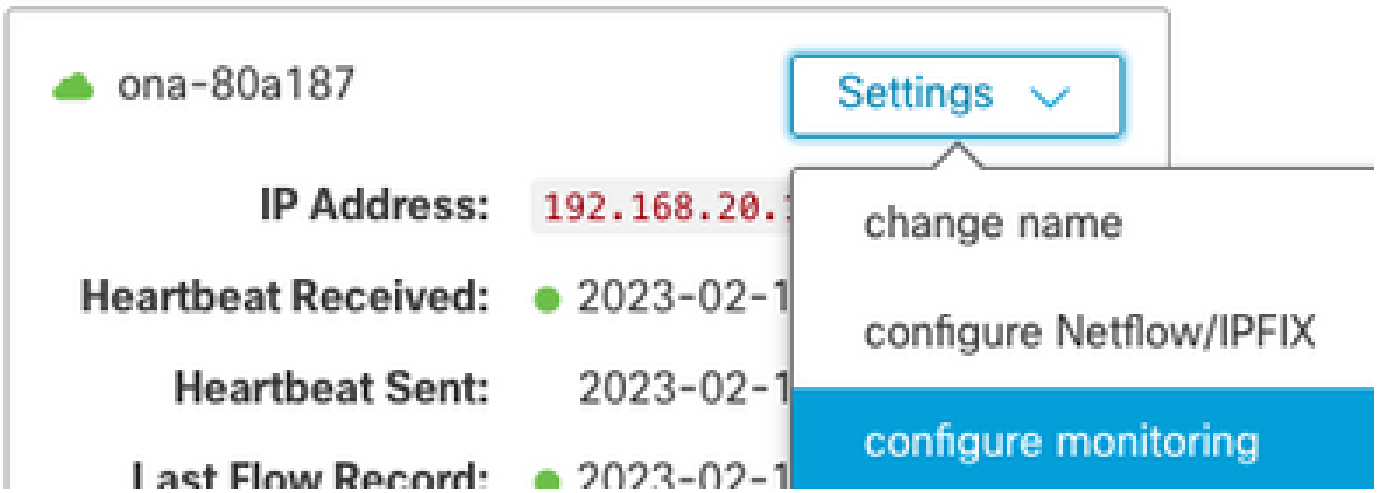
```
<#root>

user@example-ona:~#

grep PNA_SERVICE /opt/obsrvbl-ona/config

OBSRVBL_PNA_SERVICE="false"
user@example-ona:~#
```

Si el servicio se establece en false, compruebe que las redes deseadas aparezcan en Settings > configure monitoring para el sensor en el portal de SCA.



Ejecute el ps -fu obsrvbl_ona | grep pna comando y observe si se ve el servicio y si se enumeran los rangos de red monitoreados esperados.

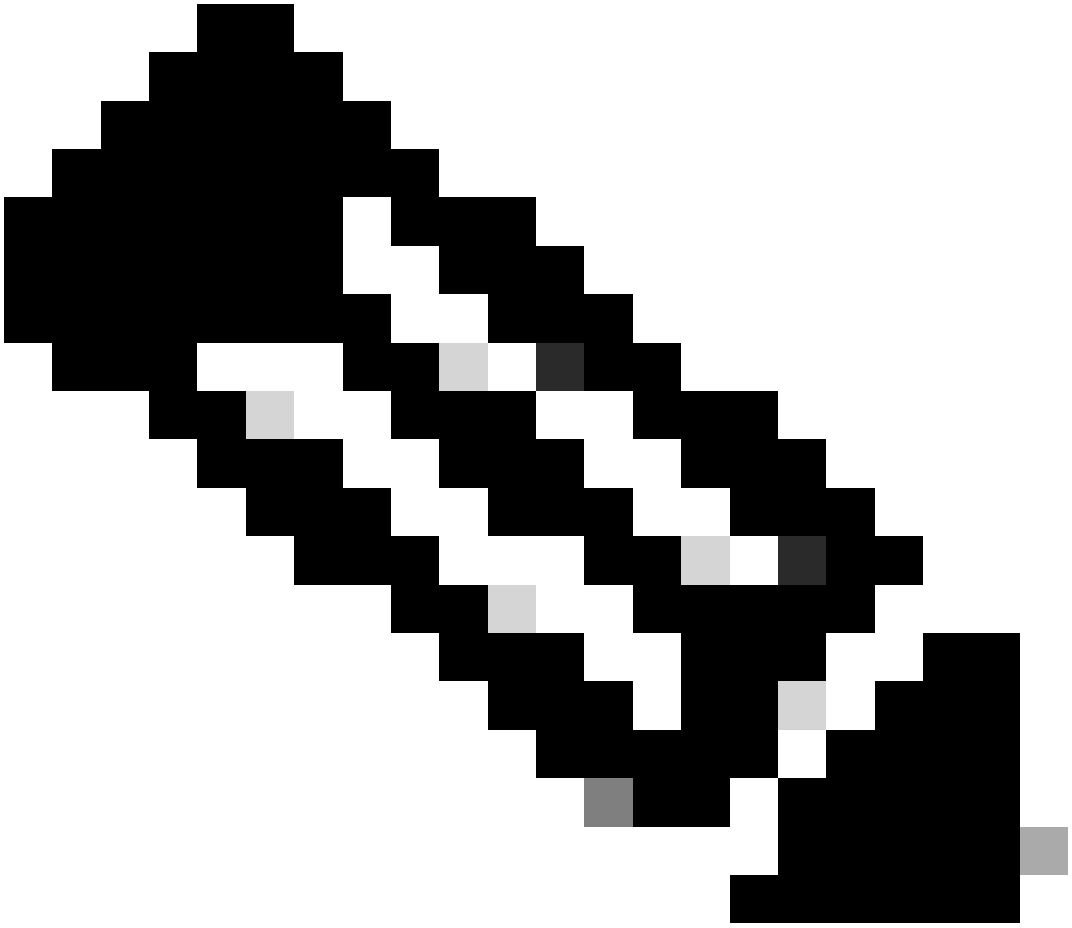
<#root>

```
user@example-ona:~#
```

ps -fu obsrvbl_ona | grep pna

```
obsrvbl+ 925 763 0 Feb09 ? 00:29:04 /usr/bin/python3 /opt/obsrvbl-ona/ona_service/pna_pusher.py
obsrvbl+ 956 920 0 Feb09 ? 00:24:00 /opt/obsrvbl-ona/pna/user/pna -i ens192 -N 10.0.0.0/8 172.16.0.0/12
obsrvbl+ 957 921 0 Feb09 ? 00:00:00 /opt/obsrvbl-ona/pna/user/pna -i ens224 -N 10.0.0.0/8 172.16.0.0/12
user@example-ona:~#
```

La salida del comando muestra que el servicio PNA tiene el ID de proceso 956 y 957, y los rangos de direcciones privadas 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16 se monitorean en las interfaces ens192 y ens224.



Nota: Los rangos de direcciones y los nombres de interfaz pueden variar según la configuración y el despliegue del sensor

Errores SSL

Revise el archivo /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log para ver si hay errores SSL con el less /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log comando.

Se proporciona un ejemplo de error.

```
(Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify fa
```

Ejecute el wget https://s3.amazonaws.com comando y revise el resultado para ver si hay alguna inspección de HTTPS posible.

Si hay inspección HTTPS, asegúrese de que el sensor se haya eliminado de cualquier inspección o se haya colocado en una lista de permitidos.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).