ONA传感器脱机状态故障排除

目录

简介

本文档介绍如何调查安全云分析(SCA)传感器显示为脱机状态的多种可能原因。

背景信息

安全云分析(SCA)以前称为Stealthwatch云(SWC)，这些术语可以互换使用。

SCA传感器是专用网络监视器，可以作为ONA、ONA传感器或仅作为传感器来引用。

本文中的命令基于ona-20.04.1-server-amd64.iso debian安装。

脱机传感器的可能原因

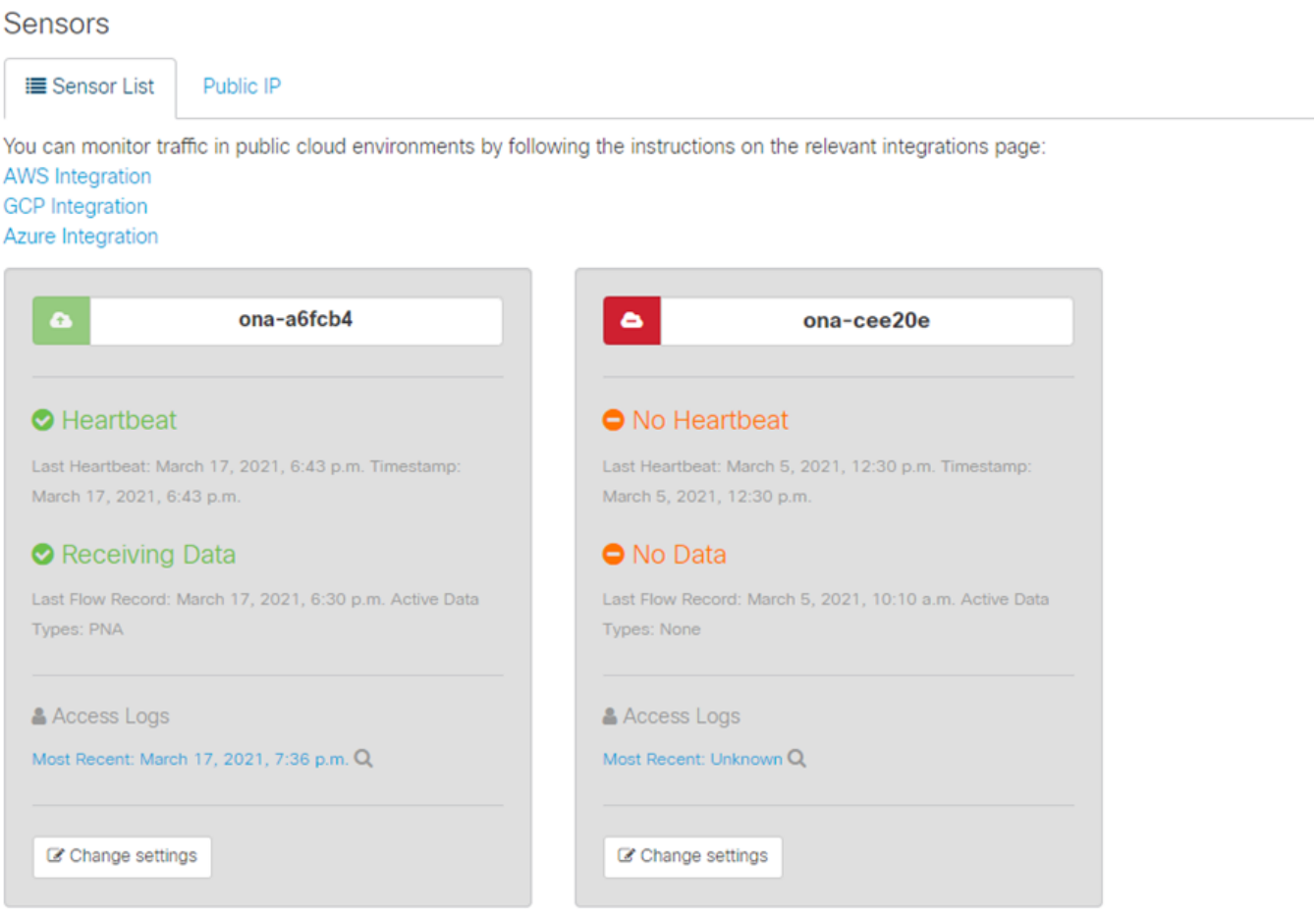
有许多可能因素会导致传感器呈现脱机状态。

这些因素的两个示例是与网络相关的问题，并且本地文件系统具有完整的磁盘。

识别脱机传感器

SCA门户包含配置的传感器列表。要访问此页面，请导航至 Settings > Sensors.

此映像中的脱机传感器以红色表示，并且不显示最近的检测信号和数据信息。



检查脱机传感器

网络问题

ONA主机可能失去Internet访问权限，从而导致传感器被列为离线。

测试ONA主机是否能ping通已知的活动IP地址，例如在8.8.8.8的一个Google DNS服务器。

登录ONA传感器并运行**ping -c4 8.8.8.8** 命令。

<#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:~#
```

如果传感器无法ping通已知的活动IP地址，请进一步检查。

使用route -n命令确定默认网关。

使用 **arp -an** 命令确定对于默认网关是否显示有效的地址解析协议(ARP)条目。

如果传感器能够ping通已知的IP地址，则测试DNS主机名解析以及传感器连接到云的能力。

登录传感器并运行sudo curl https://sensor.ext.obsrvbl.com命令。

curl命令输出显示，对sensor.ext.obsrvbl.com的DNS解析失败，并且需要调查DNS。

<#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:~#
```

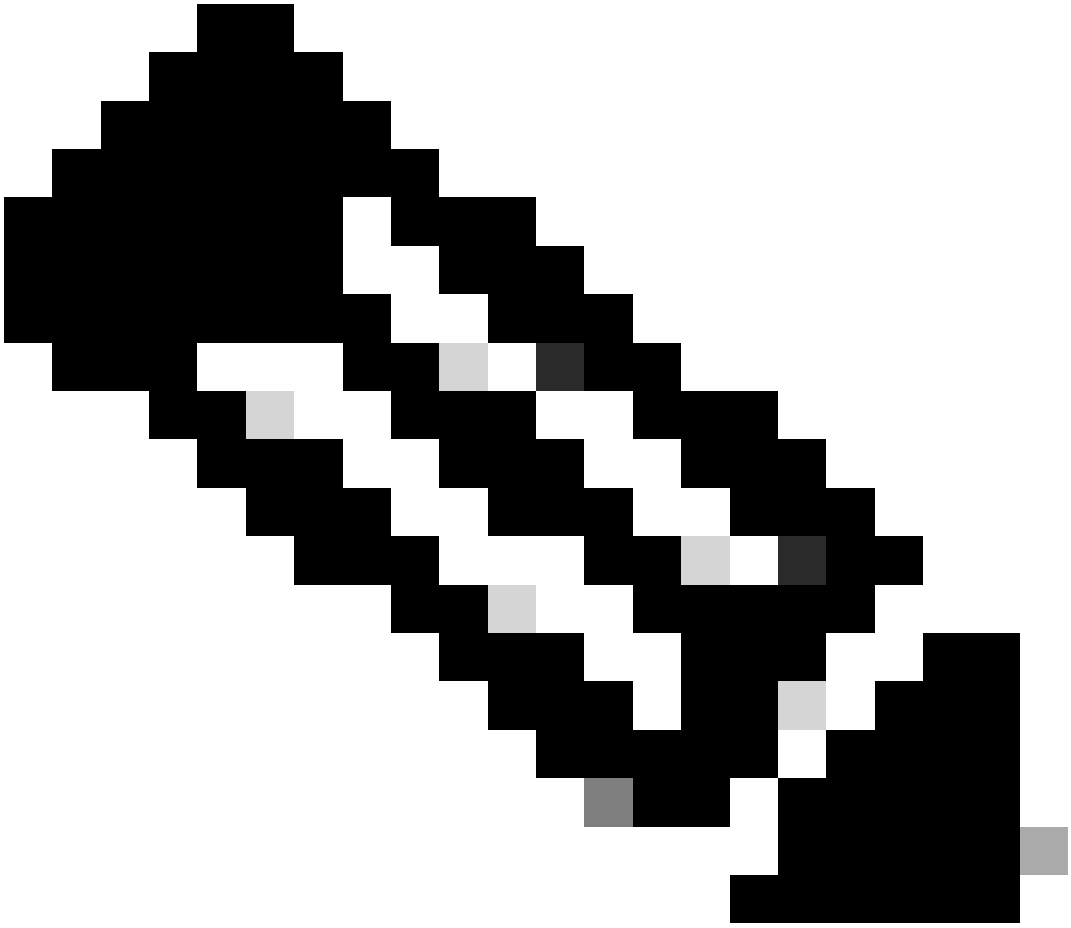
此类响应表示连接正常，并且云门户可识别传感器。

<#root>

user@example-ona:~#

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

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



注意：可以修改curl命令以使用相应的区域US：https://sensor.ext.obsrvbl.com欧洲：https://sensor.eu-prod.obsrvbl.com澳大利亚：https://sensor.anz-prod.obsrvbl.com

此类型的响应表示连接正常，但传感器尚未与特定域关联。

```
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:~#
```

DNS问题

如果传感器无法通过DNS解析主机名，请使用cat /etc/netplan/01-netcfg.yaml命令验证DNS设置。

如果DNS设置需要更改，请参阅更新DNS配置部分。

验证DNS设置后，运行sudo systemctl restart systemd-resolved.service命令。

此命令不需要任何输出。

<#root>

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

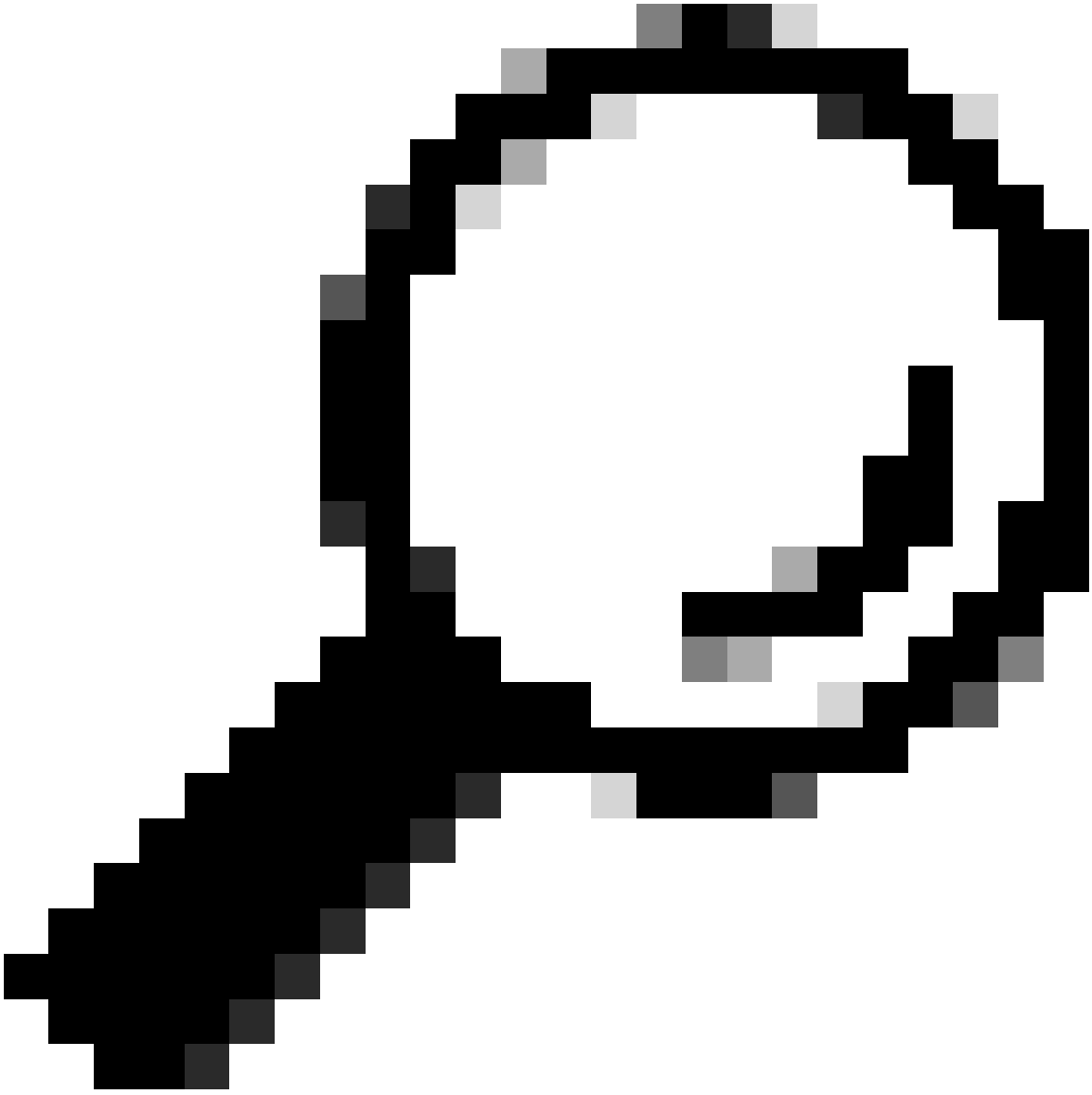
sudo systemctl restart systemd-resolved.service

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

更新DNS配置

要更新Netplan中的DNS服务器，可以修改网络接口的Netplan配置文件。

Netplan**配置文件存储在/etc/netplan**目录中。



提示：在此目录中找到一个或两个YAML文件。预期文件名是01-netcfg.yaml和/或50-cloud-init.yaml。

使用sudo vi /etc/netplan/01-netcfg.yaml命令打开Netplan**配置文件**。

在Netplan配置文件中，在网络接口下找到“nameservers”密钥。

可以指定多个DNS服务器IP地址，用逗号分隔。

使用 **sudo netplan apply** 命令将更改应用于Netplan配置。

Netplan为systemd解析的服务生成配置文件。

要检验新的DNS解析器是否已设置，请运行resolvectl status | grep -A2 'DNS Servers'命令。

<#root>

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

resolvectl status | grep -A2 'DNS Servers'

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

user@example-ona:~#
```

本地文件系统已满

传感器控制台上可能会出现一条常见的错误消息：“Failed to create new system journal： No space left on device”（创建新系统日志失败：设备上没有剩余空间）。

这表示磁盘已满，并且/root文件系统中没有剩余空间。

运行df -ah /命令，并确定有多少空间可用。

<#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:~#

使用journalctl --vacuum-time 1d命令清除旧日志日志以释放磁盘空间。

<#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:~#

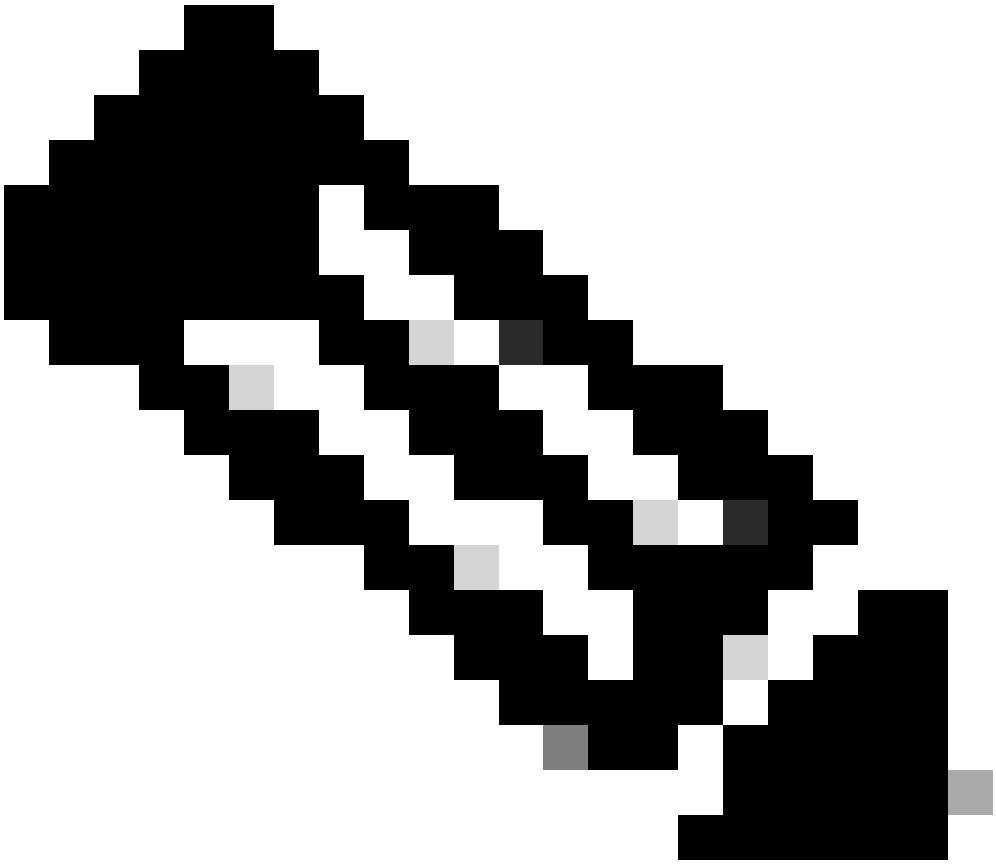
确保您的存储空间满足初始部署指南中列出的最低系统要求。

可从思科安全云分析（Stealthwatch云）产品支持页面检索该指南：https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/series.html

监控配置

与云的网络连接良好且有效的DNS设置的传感器仍可呈现脱机状态。

如果传感器监视选项被禁用或传感器不发送心跳，则可能会出现脱机状态。



注意：此部分用于默认安装的ONA传感器，没有自定义配置并主动接收netflow和/或IPFIX数据。

运行grep PNA_SERVICE /opt/obsrvbl-ona/config命令以确定状态。

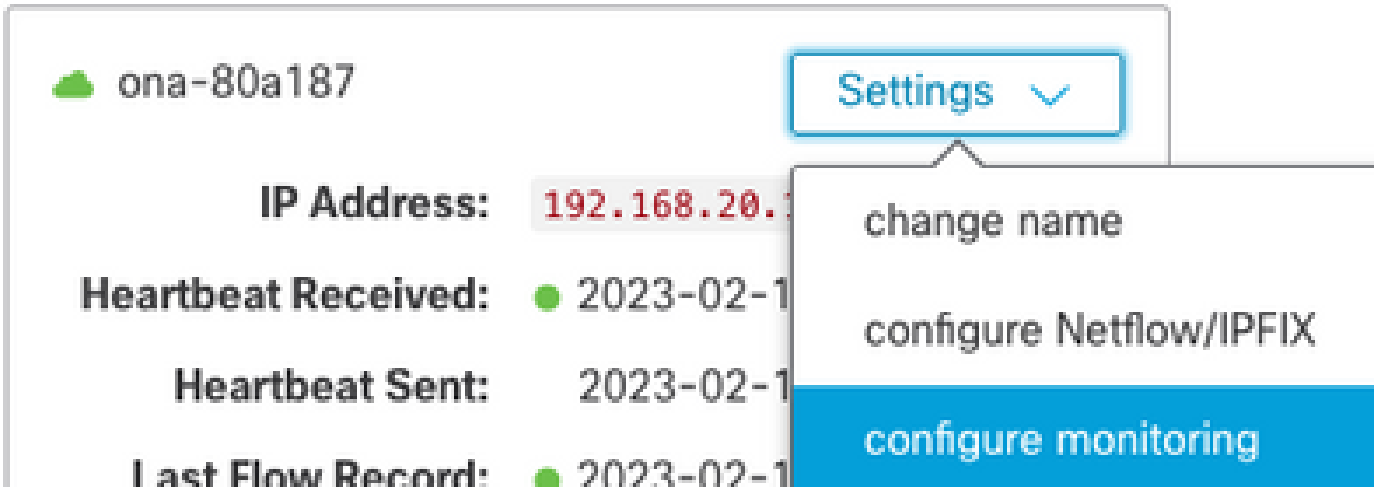
```
<#root>

user@example-ona:~#

grep PNA_SERVICE /opt/obsrvbl-ona/config

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

如果服务设置为false，请验证在SCA门户中是否为传感器列出了 Settings > configure monitoring 所需的网络。



运行ps -fu obsrvbl_ona | grep pna命令，并注意是否显示服务，以及是否列出预期的监控网络范围。

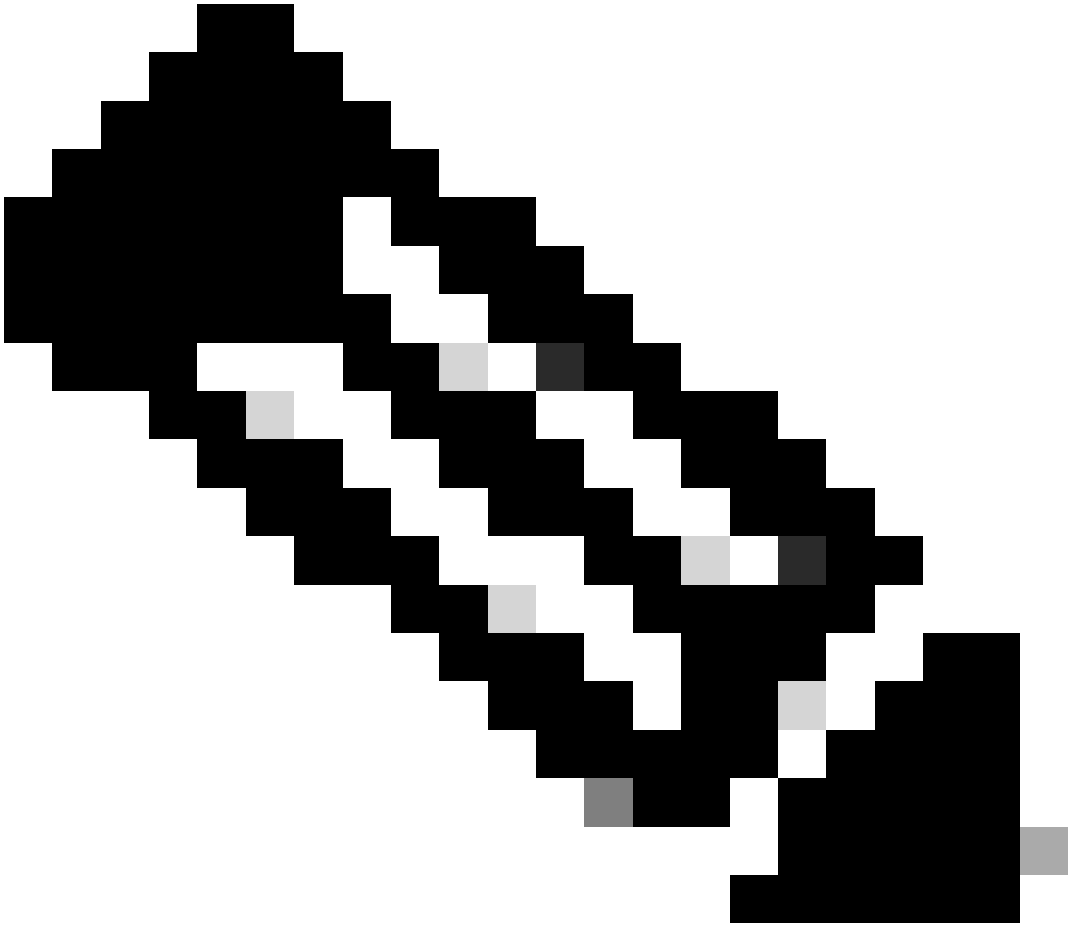
<#root>

```
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:~#
```

该命令的输出显示，PNA服务的进程ID为956和957，并且在ens192和ens224接口上监控私有地址范围10.0.0.0/8、172.16.0.0/12和192.168.0.0/16。



注意：地址范围和接口名称可能因传感器的配置和部署而异

SSL错误

使用less /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log命令检查/opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log文件中是否存在SSL错误。

此处提供了一个错误示例。

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

运行wget https://s3.amazonaws.com命令并查看输出，看是否有任何可能的HTTPS检查。

如果存在HTTPS检查，请确保从任何检查中删除传感器或将其置于允许列表中。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。