ONA感測器離線狀態故障排除

目錄

簡介

本文檔介紹如何調查Secure Cloud Analytics (SCA)感測器顯示為離線狀態的多種可能原因。

背景資訊

安全雲分析(SCA)以前稱為Stealthwatch雲(SWC)，這些術語可以互換使用。

SCA感測器是專用網路監控器，可以作為ONA、ONA感測器或僅作為感測器來引用。

本文中的命令基於ona-20.04.1-server-amd64.iso debian安裝。

離線感測器的可能原因

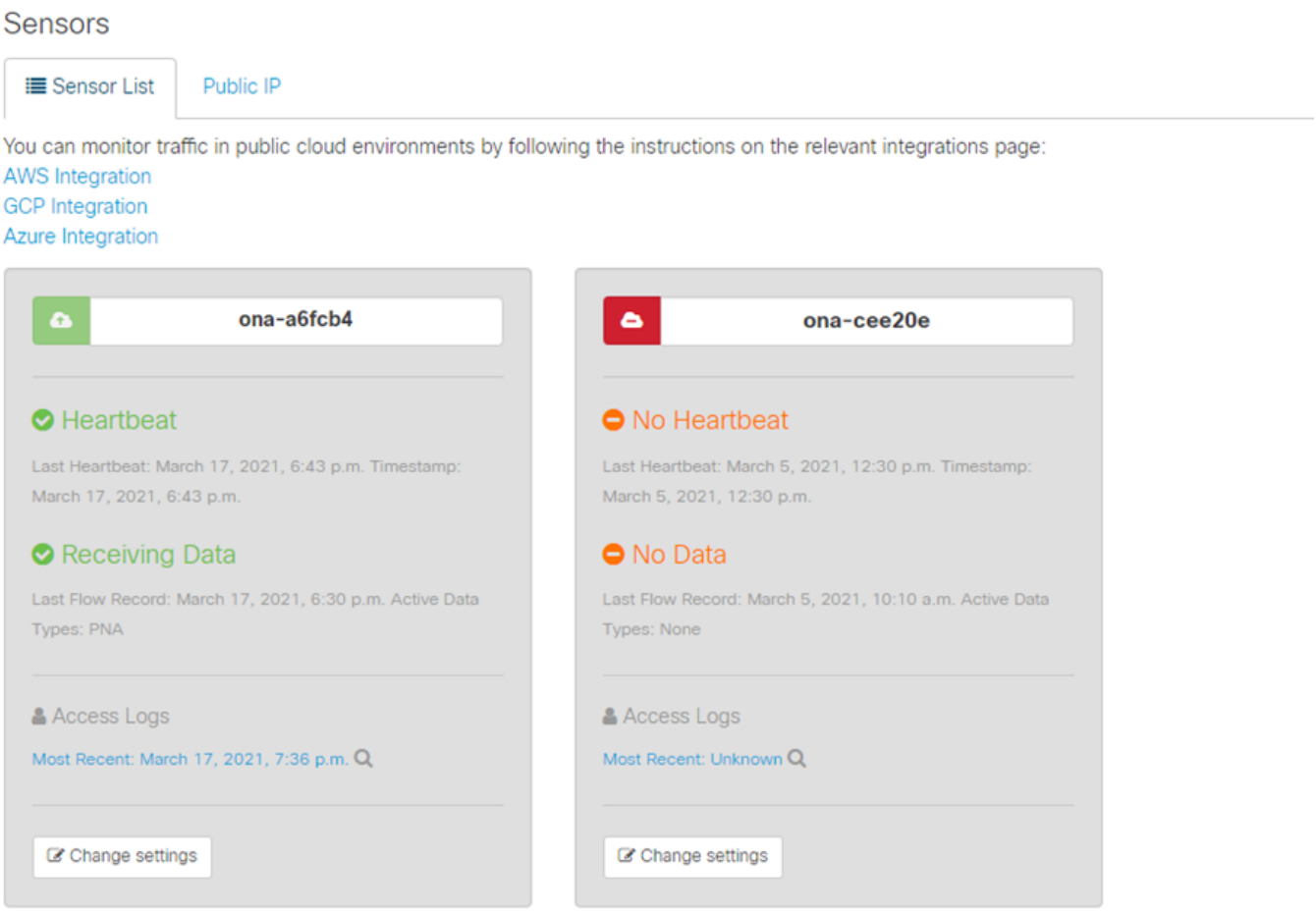
有許多可能的因素會導致感測器處於離線狀態。

這些因素的兩個示例是與網路相關的問題，並且本地檔案系統有一個全磁碟。

辨識離線感測器

SCA門戶包含已配置的感測器清單。若要存取此頁面，請瀏覽至 Settings > Sensors.

此映像中的離線感測器以紅色表示，並且未顯示最近的心跳和資料。



檢查離線感測器

網路問題

ONA主機可能丟失網際網路訪問，從而導致感測器被列為離線。

測試ONA主機是否能ping通已知的活動IP地址，例如8.8.8.8的Google DNS伺服器之一。

登入ONA感測器並運行**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:~#
```

如果感測器無法ping通已知的有效的IP地址，請進一步檢查。

使用route -n命令確定預設網關。

使用 **arp -an** 命令確定在預設網關中是否存在有效地址解析協定(ARP)條目。

如果感測器能夠ping通已知的IP地址，則測試DNS主機名解析以及感測器連線到雲的能力。

登入感測器並運行sudo curl https://sensor.ext.obsrvbl.com命令。

curl命令輸出顯示，sensor.ext.obsrvbl.com的DNS解析失敗且保證對DNS進行調查。

<#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:~#
```

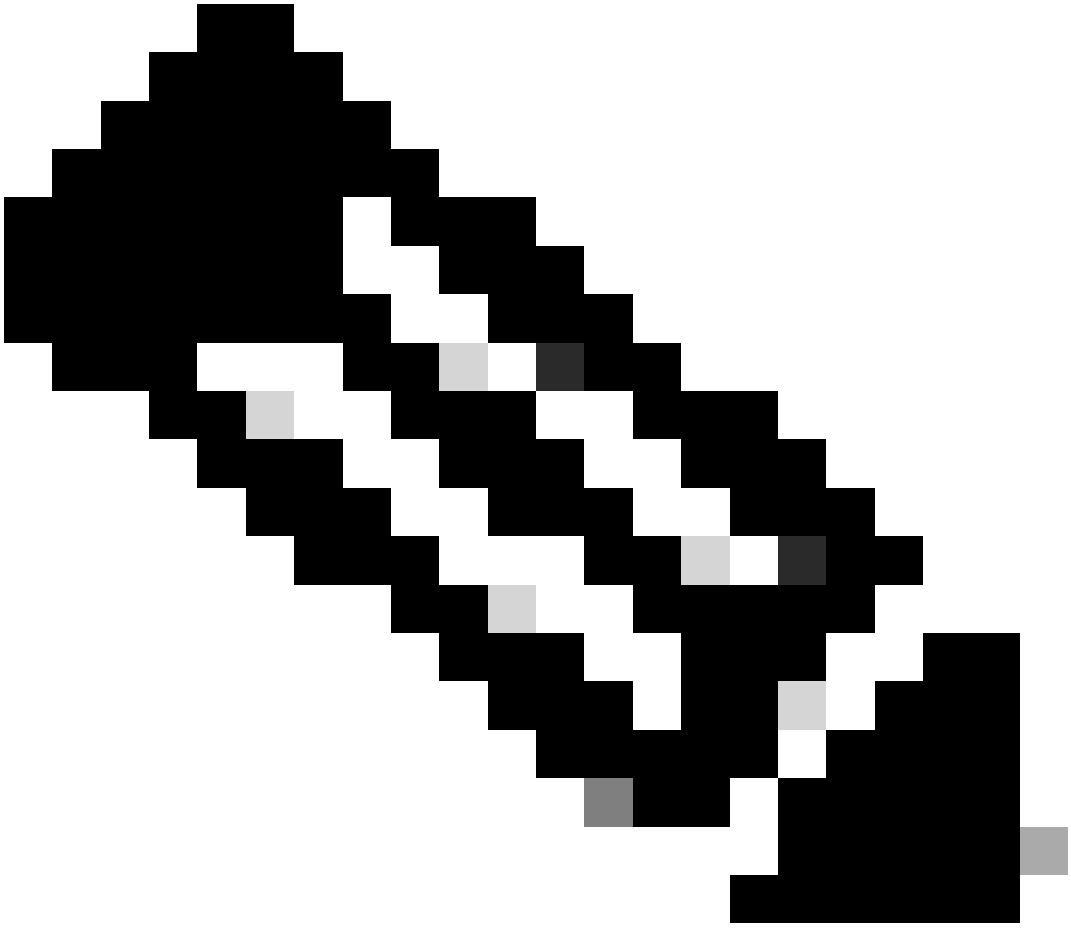
此類響應表示連線良好，並且雲門戶可辨識感測器。

<#root>

user@example-ona:~#

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

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



註：可以修改curl命令以使用相應的區域US：https://sensor.ext.obsrvbl.com Europe：https://sensor.eu-prod.obsrvbl.com Australia：https://sensor.anz-prod.obsrvbl.com

這種型別的響應表示連線良好，但感測器尚未與特定域關聯。

```
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問題

如果感測器無法使用DNS解析主機名，則使用cat /etc/netplan/01-netcfg.yaml命令驗證DNS設定。

如果DNS設定需要更改，請參閱更新DNS配置部分。

驗證DNS設定後，運行sudo systemctl restart systemd-resolved.service命令。

此命令不需要任何輸出。

<#root>

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

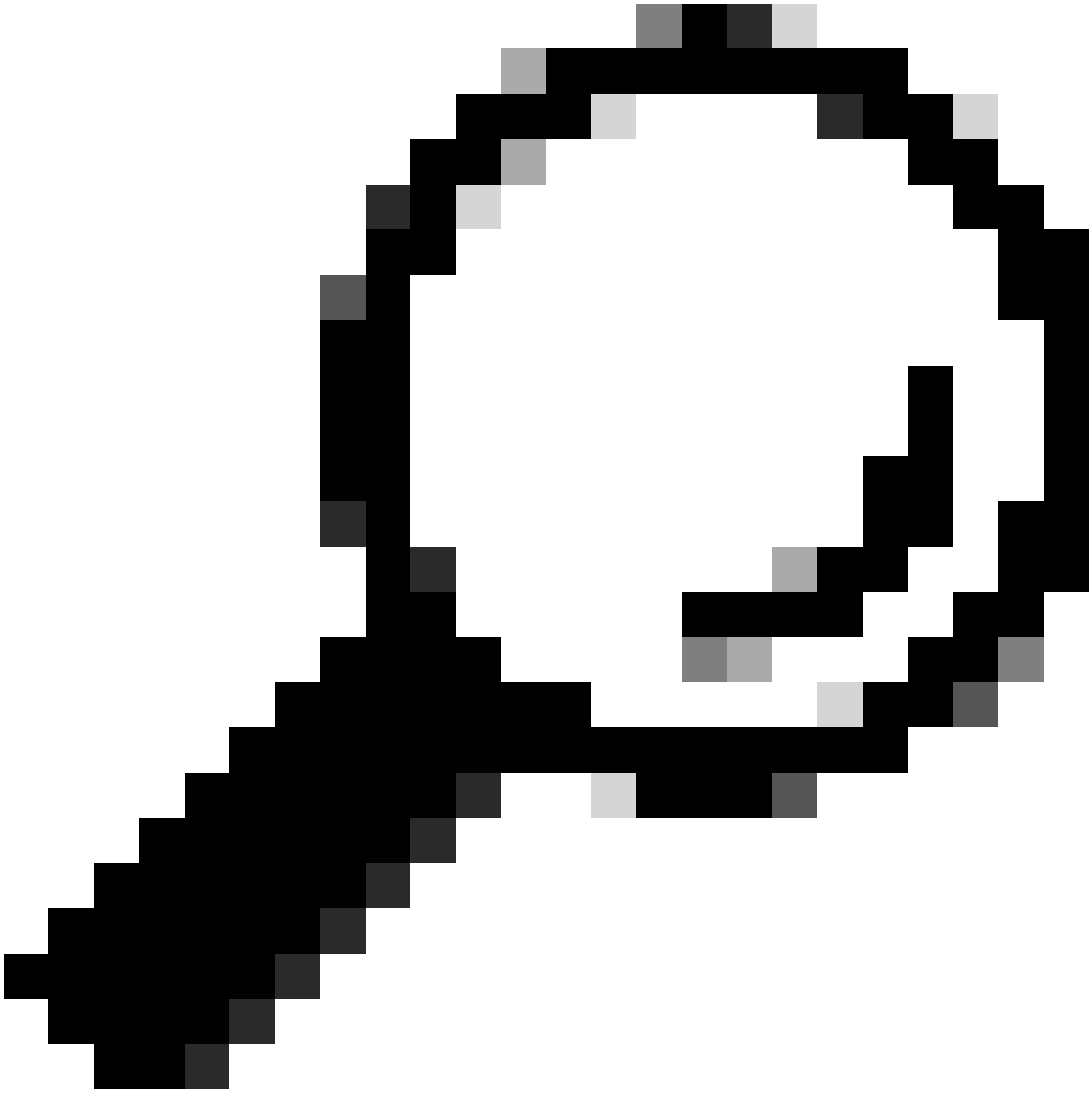
sudo systemctl restart systemd-resolved.service

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

更新DNS配置

要更新Netplan中的DNS伺服器，可以修改網路介面的Netplan配置檔案。

Netplan**配置檔案儲存在/etc/netplan**目錄中。



提示：在此目錄中找到一個或兩個YAML檔案。預期的檔名為01-netcfg.yaml和/或50-cloud-init.yaml。

使用sudo vi /etc/netplan/01-netcfg.yaml命令打開Netplan配置檔案。

在Netplan配置檔案中，在網路介面下找到「nameservers」金鑰。

您可以指定多個DNS伺服器IP地址（用逗號分隔）。

使用 **sudo netplan apply** 命令將更改應用於Netplan配置。

Netplan為系統解析的服務生成配置檔案。

要驗證新的DNS解析器是否已設定，請運行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:~#
```

本機檔案系統已滿

感測器控制檯上可能會出現一條常見的錯誤消息：「Failed to create new system journal： No space left on device」（無法建立新系統日誌：裝置上沒有剩餘空間）。

這表示磁碟已滿，且/根檔案系統中已沒有剩餘空間。

運行df -ah /命令，並確定有多少空間可用。

<#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命令清除舊的日誌以釋放磁碟空間。

<#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:~#

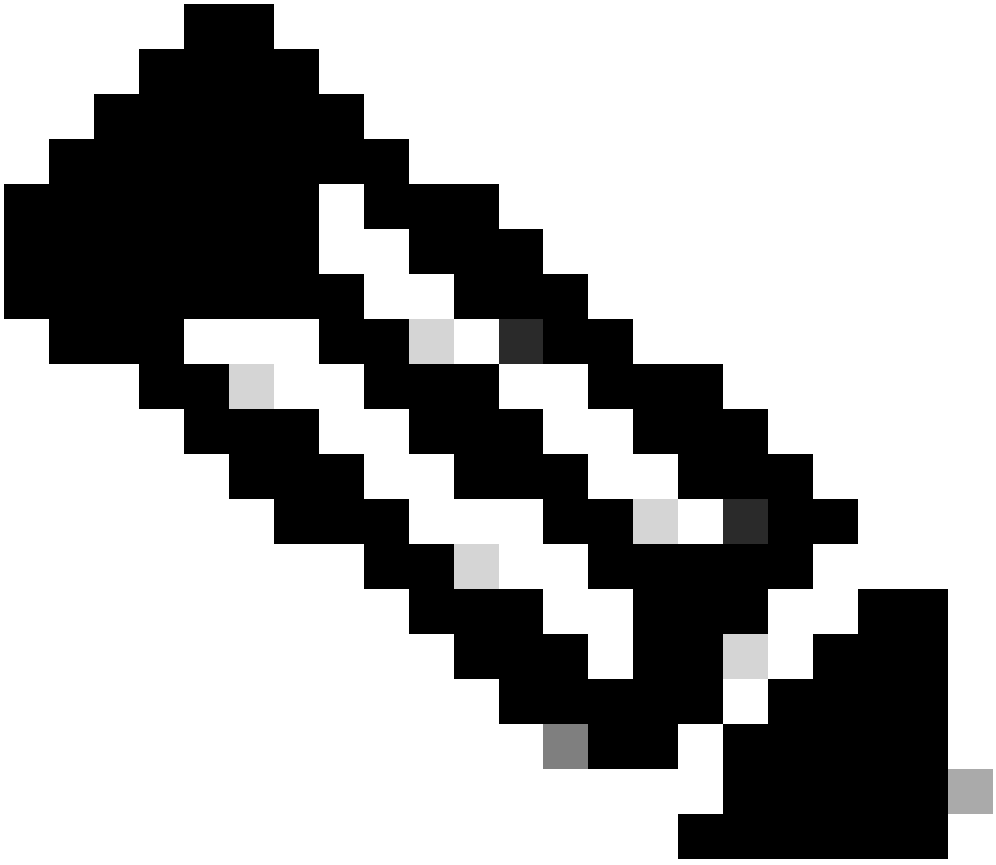
確保您的儲存空間滿足初始部署指南中列出的最低系統要求。

您可以從Cisco Secure Cloud Analytics (Stealthwatch Cloud)產品支援頁面獲取該指南：https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/series.html

監視配置

如果感測器與雲的網路連線良好，並且有效的DNS設定仍然可以呈現離線狀態。

如果感測器監視選項被停用，或者感測器不傳送心跳，則可能處於離線狀態。



註：本部分介紹不帶自定義設定的ONA感測器的預設安裝，用於主動接收netflow和/或IPFIX資料。

運行grep PNA_SERVICE /opt/obsrvbl-ona/config命令確定狀態。

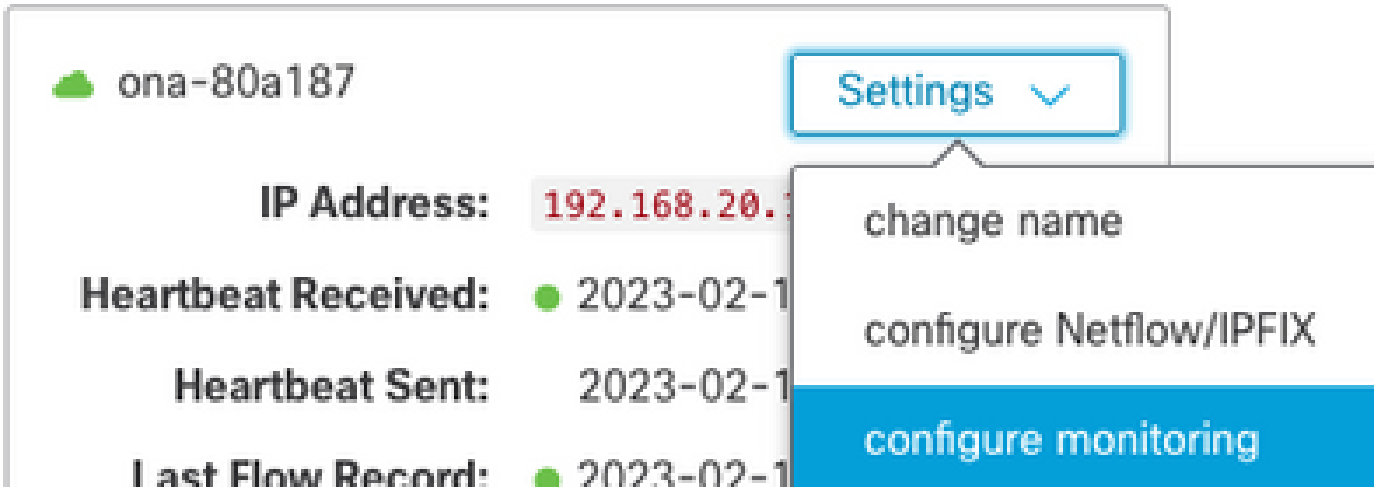
```
<#root>

user@example-ona:~#

grep PNA_SERVICE /opt/obsrvbl-ona/config

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

如果服務設定為false，請驗證在SCA門戶中的感測器 Settings > configure monitoring 中是否列出了所需的網路。



運行ps -fu obsrvbl_ona | grep pna命令，並注意是否看到服務，以及是否列出了預期的監控網路範圍。

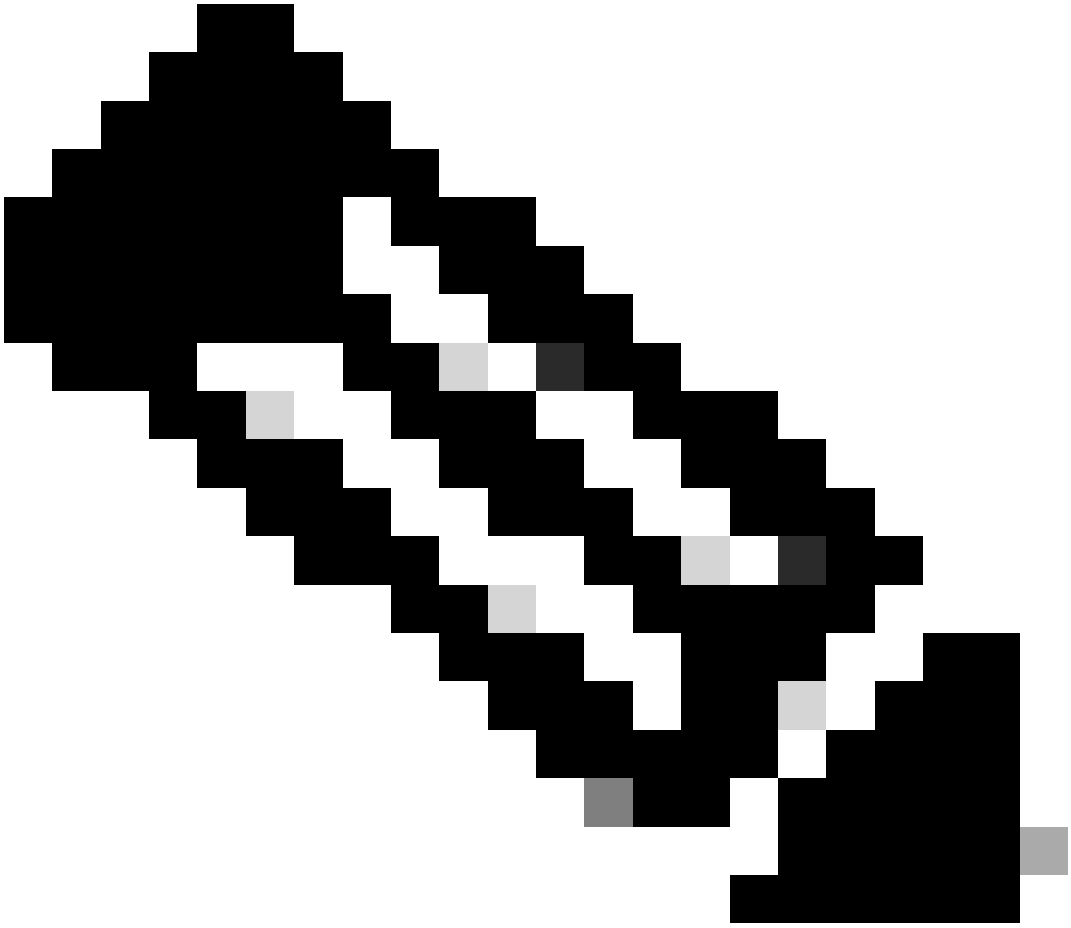
<#root>

```
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:~#
```

該命令的輸出顯示，PNA服務的進程ID為956和957，在ens192和ens224介面上監控私有地址範圍10.0.0.0/8、172.16.0.0/12和192.168.0.0/16。



註：地址範圍和介面名稱可能因感測器的配置和部署而異

SSL錯誤

使用less /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log命令檢查/opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log檔案中是否存在SSL錯誤。

提供了錯誤示例。

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

運行wget https://s3.amazonaws.com命令並檢視輸出，以檢視是否有任何可能的HTTPS檢查。

如果存在HTTPS檢測，請確保從任何檢測中移除感測器或將其置於允許清單中。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。