Solucionar problemas do status off-line do sensor ONA

Contents

Introdução

Este documento descreve como investigar várias causas possíveis de um sensor Secure Cloud Analytics (SCA) aparecer como off-line.

Informações de Apoio

O Secure Cloud Analytics (SCA) era anteriormente chamado Stealthwatch Cloud (SWC) e esses termos podem ser usados de forma intercambiável.

O sensor SCA é o Private Network Monitor e pode ser referenciado como ONA, ONA Sensor ou simplesmente como Sensor.

Os comandos neste artigo são baseados na instalação de ona-20.04.1-server-amd64.iso debian.

Possíveis causas de sensores off-line

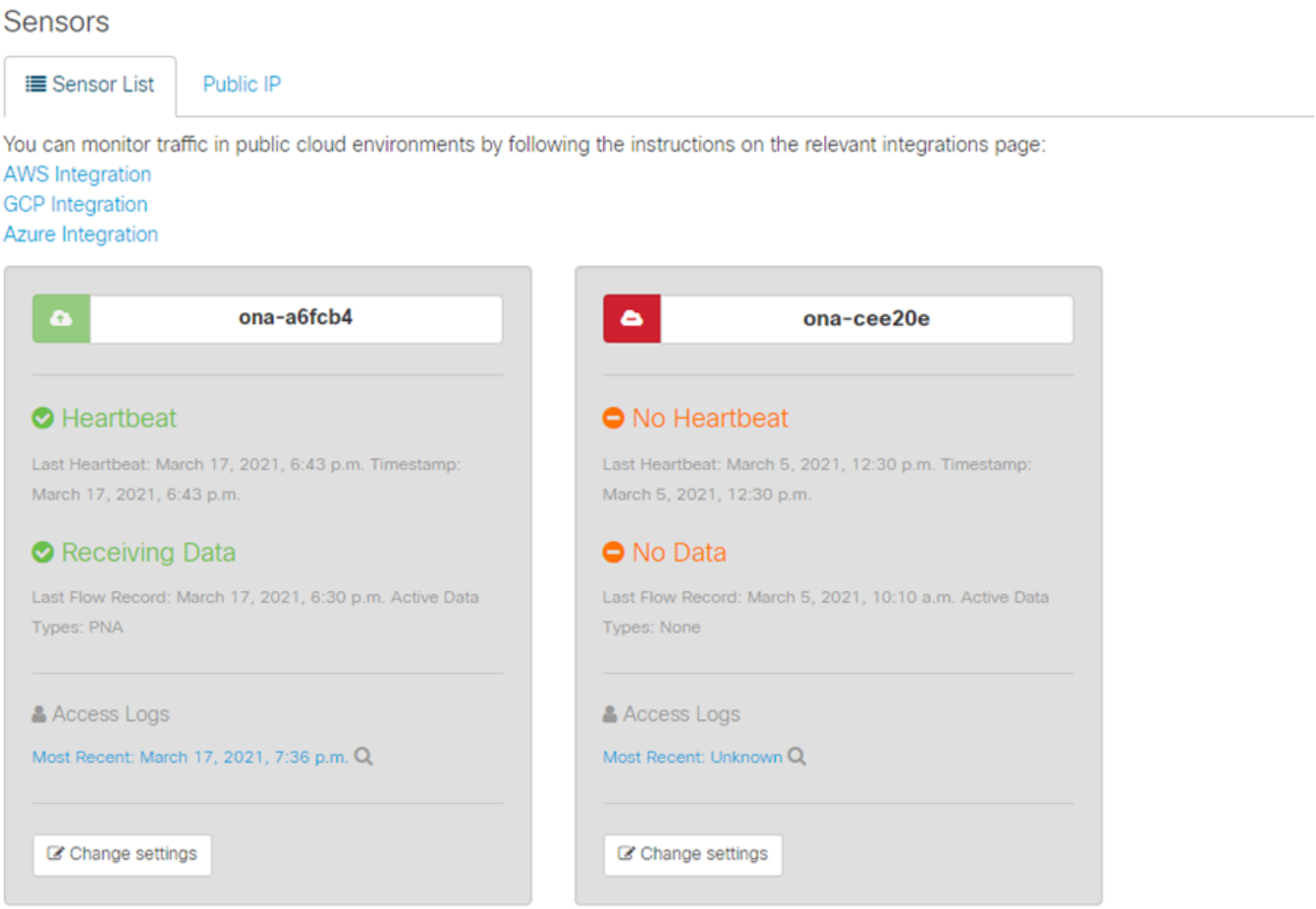
Há muitos fatores possíveis que podem fazer com que um sensor apresente um status off-line.

Dois exemplos desses fatores são problemas relacionados à rede, e o sistema de arquivos local tem um disco cheio.

Identificar um sensor offline

O SCA Portal contém uma lista de sensores configurados. Para acessar esta página, navegue até Settings > Sensors.

O sensor offline nesta imagem é representado em vermelho e não mostra Pulsação e Dados recentes.



Investigar um sensor off-line

Problemas de rede

O host ONA pode perder acesso à Internet, o que faz com que o Sensor seja listado como off-line.

Teste se o ONA Host pode fazer ping em um endereço IP ativo conhecido, como um dos servidores DNS do Google em 8.8.8.8.

Faça login no sensor ONA e execute o 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:~#
```

Se o Sensor não conseguir fazer ping em um endereço IP ativo conhecido, investigue mais.

Determine o gateway padrão com o route -n comando.

Determine se há uma entrada ARP (Address Resolution Protocol) válida vista para o gateway padrão com o **arp -an** comando.

Se o sensor puder fazer ping em um endereço IP conhecido, teste a resolução de nome de host DNS e a capacidade de recuperação do sensor de se conectar à nuvem.

Efetue login no Sensor e execute o comandosudo curl https://sensor.ext.obsrvbl.com.

A saída do comando curl mostra que a resolução DNS para sensor.ext.obsrvbl.com falhou e a investigação sobre DNS é garantida.

<#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:~#
```

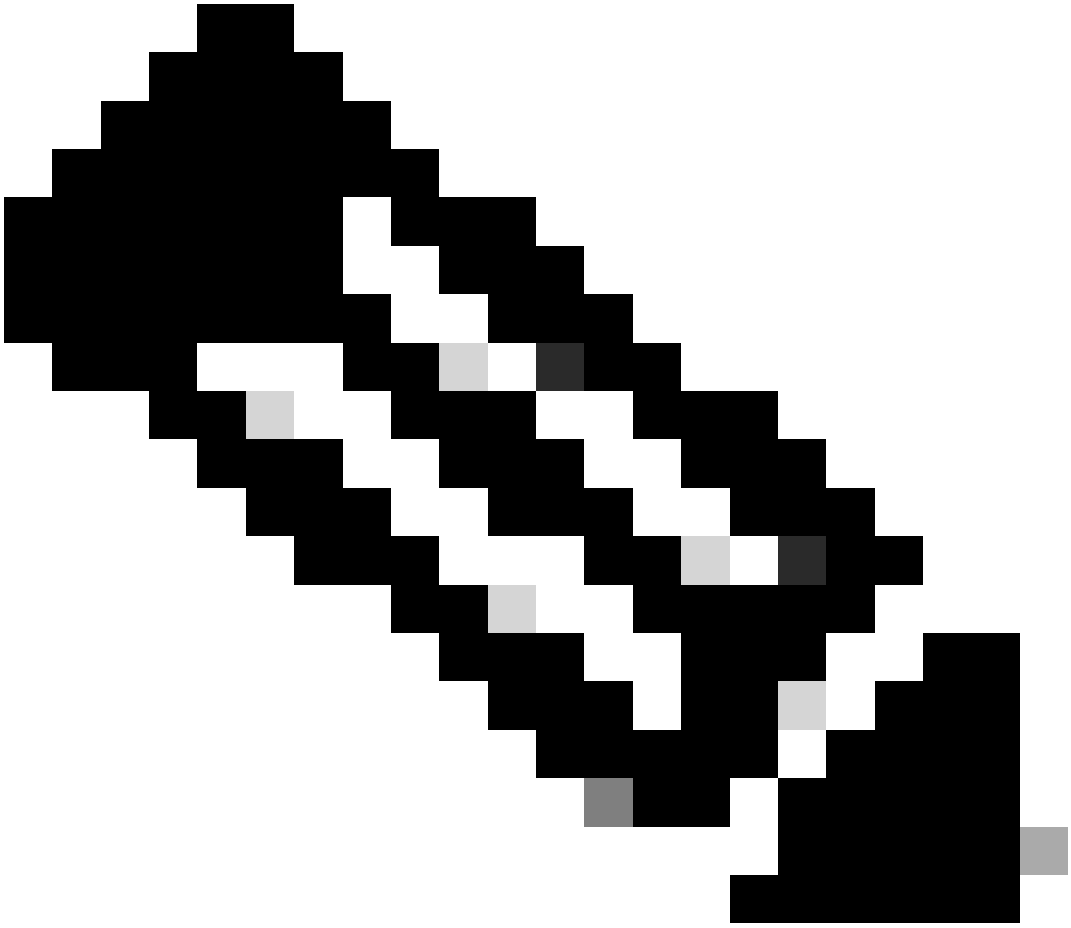
Esse tipo de resposta indica uma boa conexão e também que o portal de nuvem reconhece o sensor.

<#root>

user@example-ona:~#

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

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



Observação: o comando curl pode ser modificado para usar a região apropriada US: https://sensor.ext.obsrvbl.com Europa: https://sensor.eu-prod.obsrvbl.com Austrália: **https://sensor.anz-prod.obsrvbl.com**

Esse tipo de resposta indica uma boa conexão, mas o sensor não foi associado a um domínio específico.

```
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

Se o Sensor não puder resolver nomes de host com DNS, verifique as configurações DNS com o comandocat /etc/netplan/01-netcfg.yaml.

se as configurações de DNS exigirem alterações, consulte a seção Atualizar a configuração de DNS.

Depois que as configurações DNS forem validadas, execute o comandosudo systemctl restart systemd-resolved.service.

Nenhuma saída é esperada com este comando.

<#root>

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

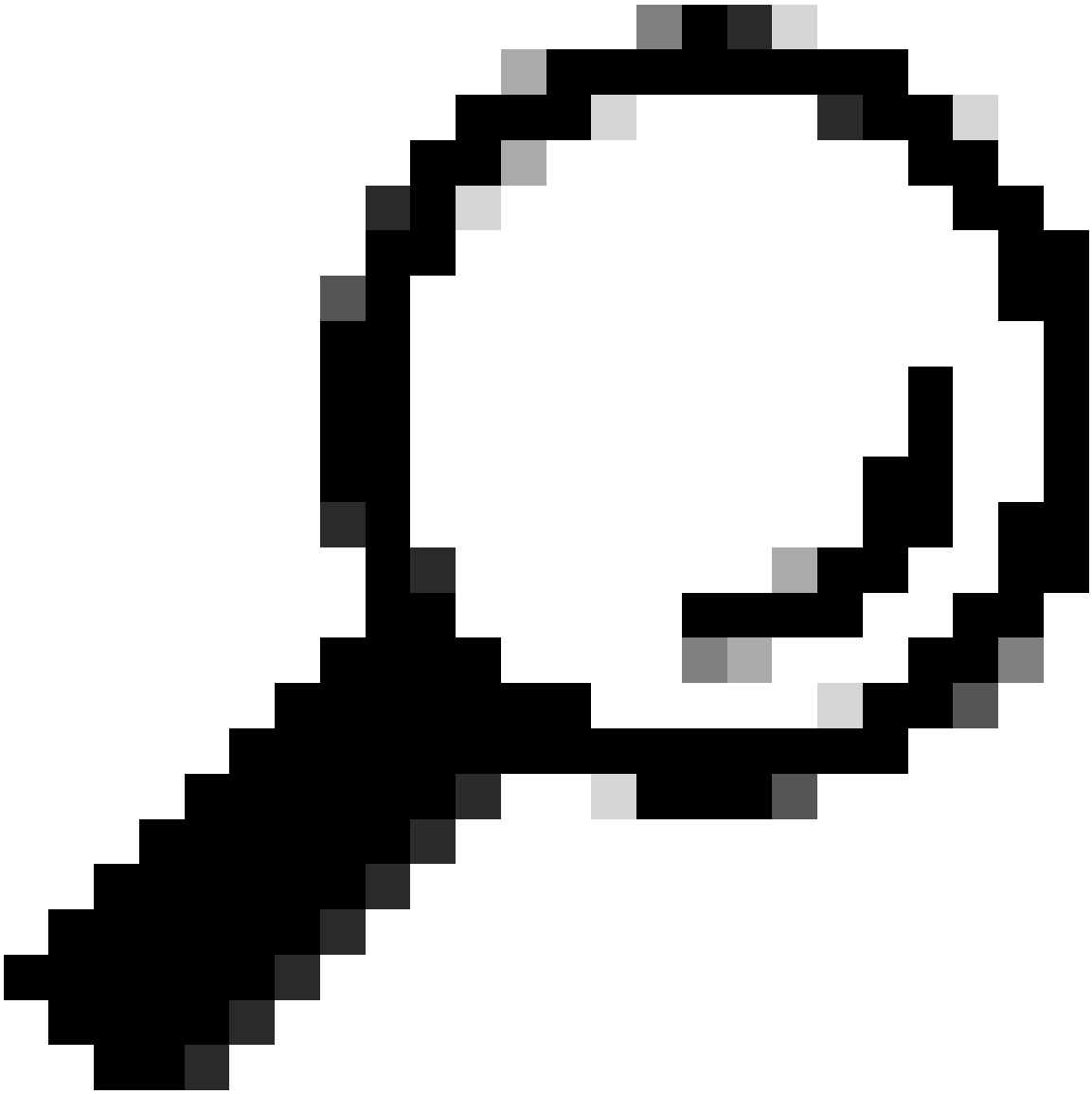
sudo systemctl restart systemd-resolved.service

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

Atualizar a configuração DNS

Para atualizar servidores DNS no Netplan, você pode modificar o arquivo de configuração do Netplan para sua interface de rede.

Os arquivos de configuração do Netplan são armazenados no diretório **/etc/netplan**.



Dica: um ou dois arquivos YAML podem ser encontrados neste diretório. Os nomes de arquivo esperados são 01-netcfg.yaml e/ou 50-cloud-init.yaml.

Abra o arquivo de configuração do Netplan com o comandosudo vi /etc/netplan/01-netcfg.yaml .

No arquivo de configuração do Netplan, localize a chave "nameservers" na interface de rede.

Você pode especificar vários endereços IP de servidor DNS separados por vírgulas.

Aplique as alterações à configuração do Netplan com o **sudo netplan apply** comando.

O Netplan gera os arquivos de configuração para o serviço resolvido pelo systemd.

Para verificar se os novos resolvedores DNS estão definidos, execute o comandoresolvectl status | grep -A2 'DNS Servers' .

<#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 Arquivos Local Cheio

Uma mensagem de erro comum pode aparecer no console do sensor: "Falha ao criar novo diário do sistema: Não há espaço disponível no dispositivo."

Isso indica que o disco está cheio e que não há mais espaço no sistema de arquivos raiz /.

Execute o comandodf -ah / e determine quanto espaço está disponível.

<#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:~#

Limpe os logs de diário antigos para liberar espaço em disco com o 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:~#

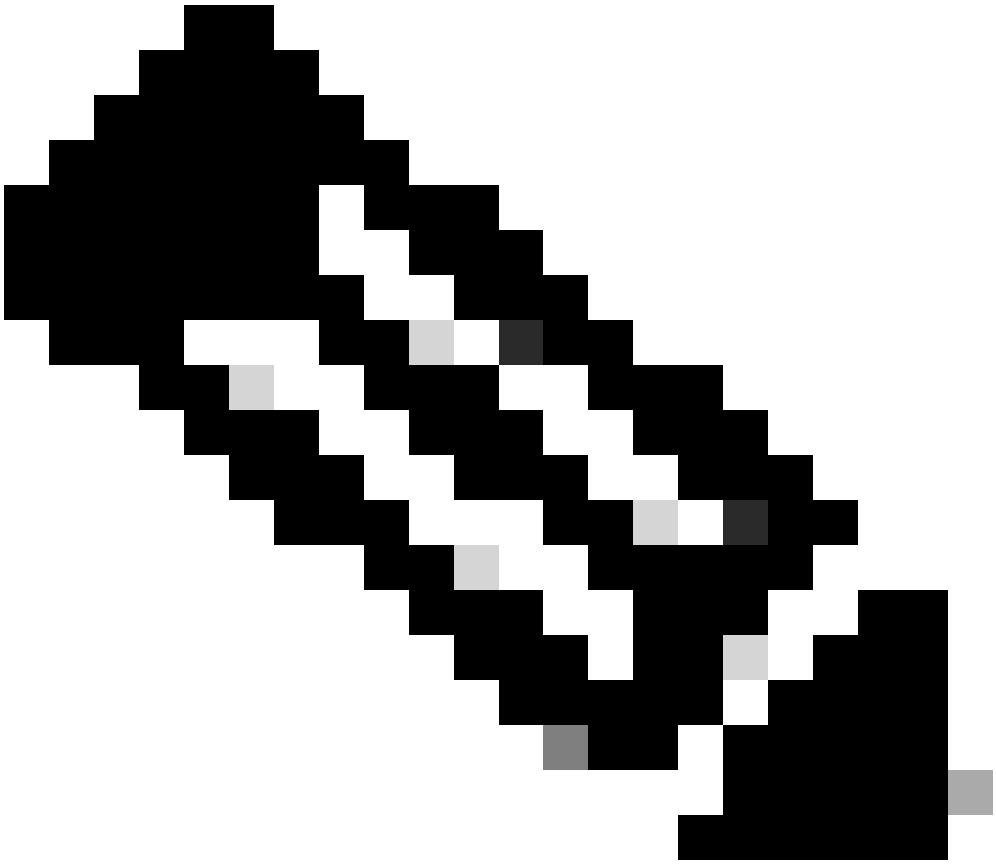
Certifique-se de que seu espaço de armazenamento atenda aos requisitos mínimos do sistema descritos no guia de implantação inicial.

O guia pode ser acessado na página de suporte do produto Cisco Secure Cloud Analytics (Stealthwatch Cloud): https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/series.html

Configuração de monitoramento

Um sensor que tenha boa conectividade de rede com a nuvem e configurações de DNS válidas ainda pode apresentar um status offline.

Um status offline será possível se as opções de monitoramento do Sensor estiverem desabilitadas ou se o Sensor não enviar pulsações.



Observação: esta seção é para uma instalação padrão do ONA Sensor sem personalizações e recebe ativamente dados de netflow e/ou IPFIX.

Execute o comandogrep PNA_SERVICE /opt/obsrvbl-ona/config para determinar o status.

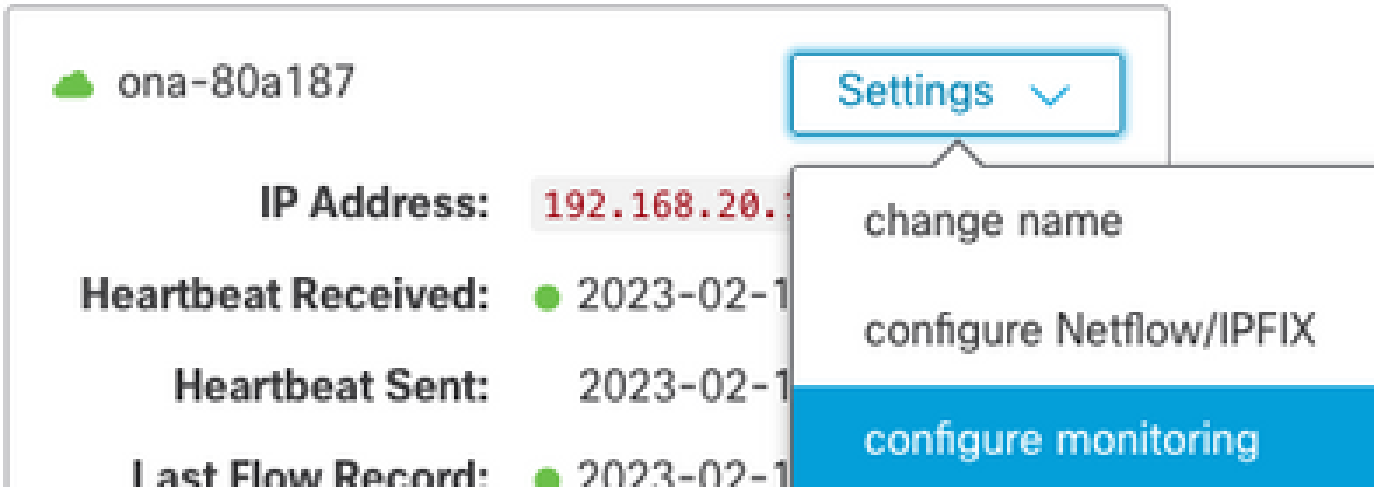
```
<#root>

user@example-ona:~#

grep PNA_SERVICE /opt/obsrvbl-ona/config

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

Se o serviço estiver definido como falso, verifique se as redes desejadas estão listadas no Settings > configure monitoring para seu sensor no SCA Portal.



Execute o comandops -fu obsrvbl_ona | grep pna e a observação se o serviço for visto e se os intervalos de rede monitorados esperados forem listados.

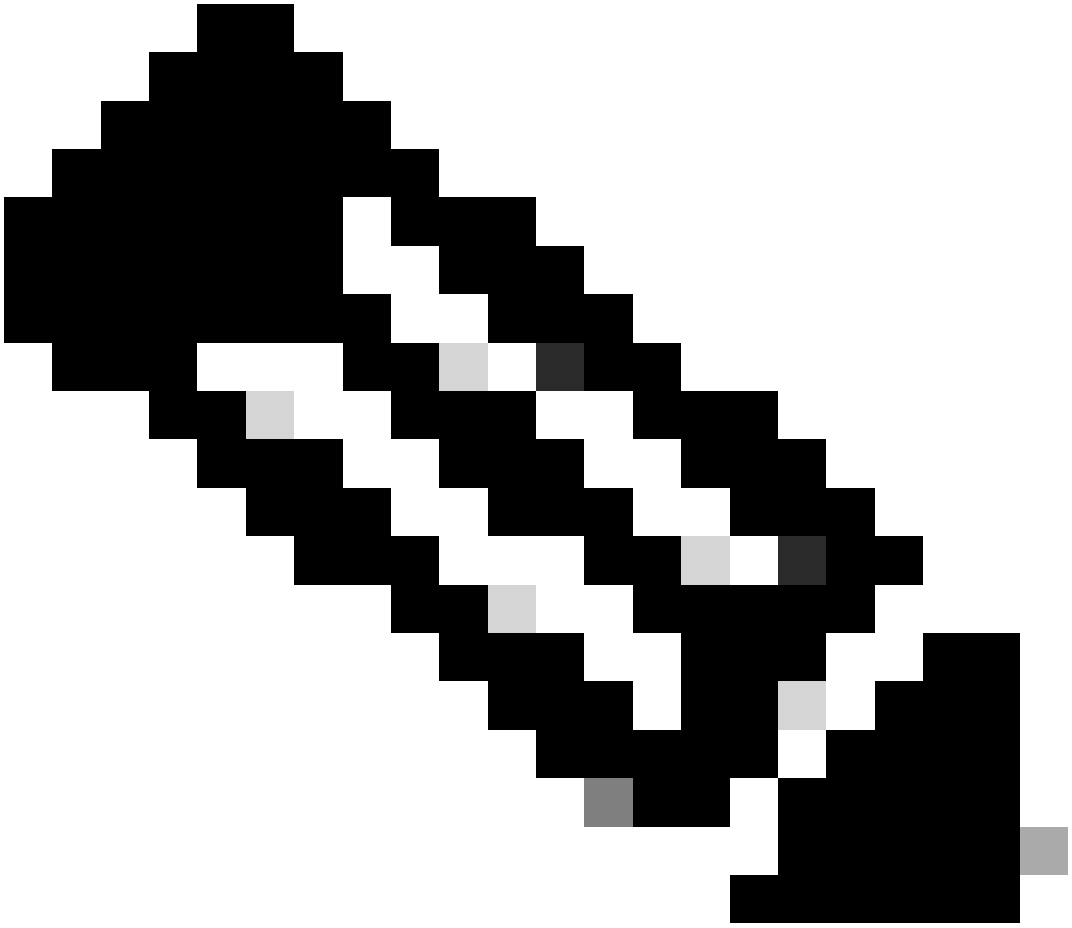
<#root>

```
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:~#
```

A saída do comando mostra que o serviço PNA tem os ID de processo 956 e 957, e os intervalos de endereço privado 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16 são monitorados nas interfaces ens192 e ens224.



Observação: os intervalos de endereços e os nomes de interface podem diferir com base na configuração e implantação do Sensor

Erros SSL

Verifique se há erros SSL no arquivo /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log com o less /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log comando.

Um exemplo de erro é fornecido.

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

Execute o wget https://s3.amazonaws.com comando e examine a saída para ver se há alguma inspeção HTTPS possível.

Se houver inspeção de HTTPS, verifique se o sensor foi removido de qualquer inspeção ou colocado em uma lista de permissão.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.