Dépannage de l'état hors connexion du capteur ONA

Table des matières

Introduction

Ce document décrit comment étudier plusieurs causes possibles de l'apparition d'un capteur Secure Cloud Analytics (SCA) hors ligne.

Informations générales

Secure Cloud Analytics (SCA) s'appelait auparavant StealthWatch Cloud (SWC) et ces termes peuvent être utilisés indifféremment.

Le capteur SCA est le moniteur de réseau privé et peut être référencé en tant que capteur ONA, ONA ou simplement en tant que capteur.

Les commandes de cet article sont basées sur l'installation debian ona-20.04.1-server-amd64.iso.

Causes possibles des capteurs hors connexion

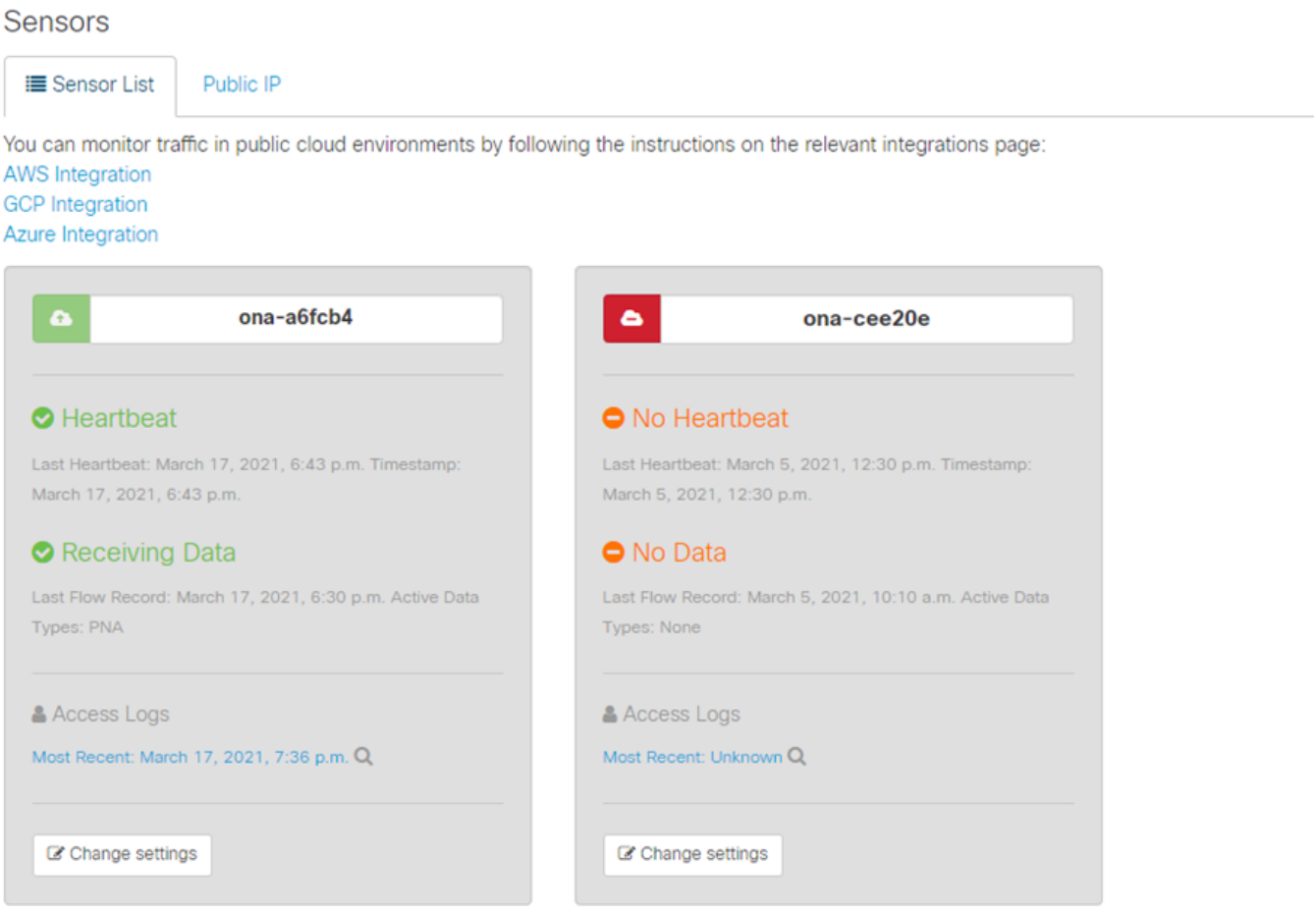
Il existe de nombreux facteurs qui peuvent amener un capteur à présenter un état hors ligne.

Deux exemples de ces facteurs sont les problèmes liés au réseau, et le système de fichiers local a un disque plein.

Identifier un capteur hors ligne

Le portail SCA contient une liste de capteurs configurés. Pour accéder à cette page, accédez à Settings > Sensors.

Le capteur hors ligne de cette image est représenté en rouge et n'affiche pas de pulsation et de données récentes.



Examiner un capteur hors connexion

Problèmes réseau

L'hôte ONA peut perdre l'accès à Internet, ce qui a pour conséquence que le capteur est répertorié comme étant hors connexion.

Testez si l'hôte ONA peut envoyer une requête ping à une adresse IP active connue, telle que l'un des serveurs DNS Google à l'adresse 8.8.8.8.

Connectez-vous au capteur ONA et exécutez la commande **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 le capteur ne parvient pas à envoyer une requête ping à une adresse IP active connue, examinez-la plus en détail.

Déterminez la passerelle par défaut à l’aide de la commanderoute -n.

Déterminez si une entrée ARP (Address Resolution Protocol) valide a été vue pour la passerelle par défaut à l'aide de la **arp -an** commande.

Si le capteur peut envoyer une requête ping à une adresse IP connue, testez la résolution du nom d'hôte DNS et la capacité du capteur à se connecter au cloud.

Connectez-vous au capteur et exécutez la commandesudo curl https://sensor.ext.obsrvbl.com.

Le résultat de la commande curl montre que la résolution DNS pour sensor.ext.obsrvbl.com a échoué et qu'une enquête sur DNS est justifiée.

<#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:~#
```

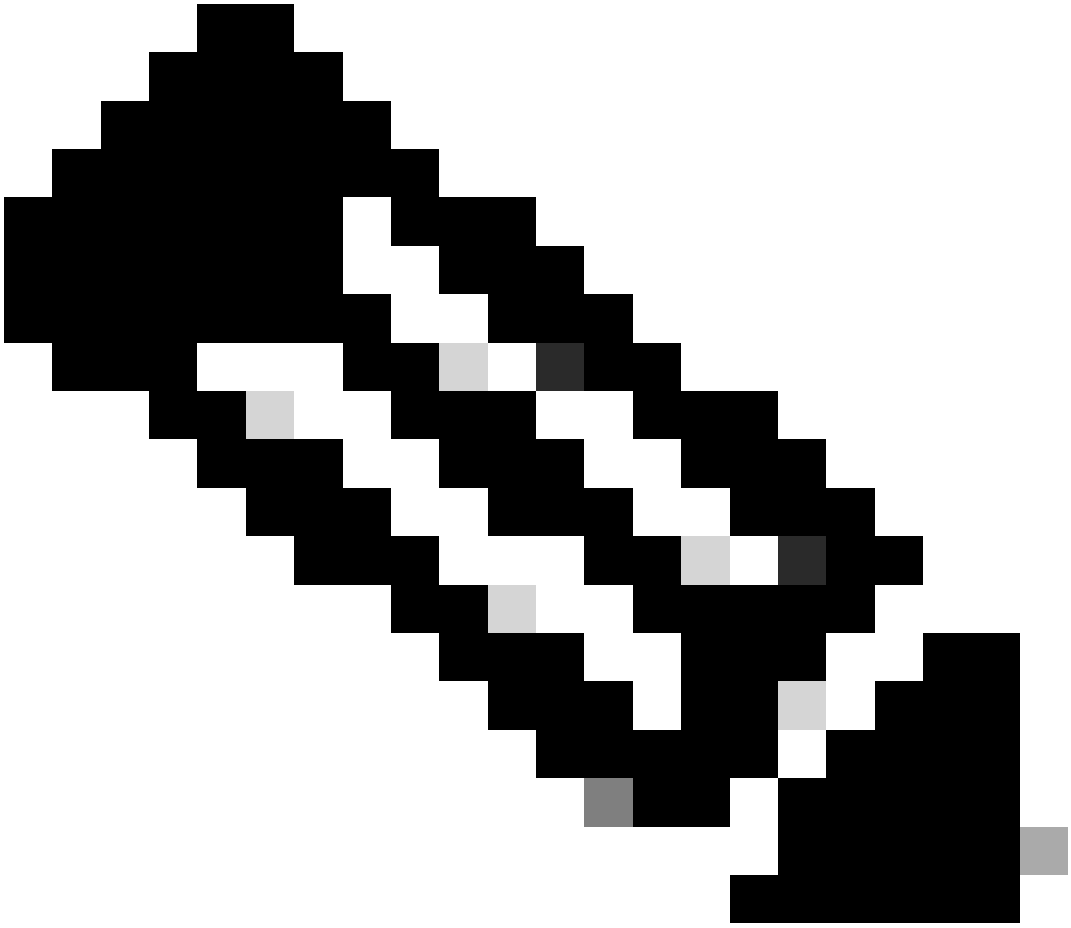
Ce type de réponse indique une bonne connexion et également que le portail cloud reconnaît le capteur.

<#root>

user@example-ona:~#

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

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



Remarque : la commande curl peut être modifiée pour utiliser la région appropriée US : https://sensor.ext.obsrvbl.com Europe : https://sensor.eu-prod.obsrvbl.com Australie : https://sensor.anz-prod.obsrvbl.com

Ce type de réponse indique une connexion correcte, mais le capteur n'a pas été associé à un domaine particulier.

```
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:~#
```

Problèmes DNS

Si Sensor ne parvient pas à résoudre les noms d'hôte avec DNS, vérifiez les paramètres DNS à l'aide de la commandecat /etc/netplan/01-netcfg.yaml .

Si les paramètres DNS nécessitent des modifications, reportez-vous à la section Mettre à jour la configuration DNS.

Une fois les paramètres DNS validés, exécutez la commandesudo systemctl restart systemd-resolved.service.

Aucune sortie n'est attendue avec cette commande.

<#root>

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

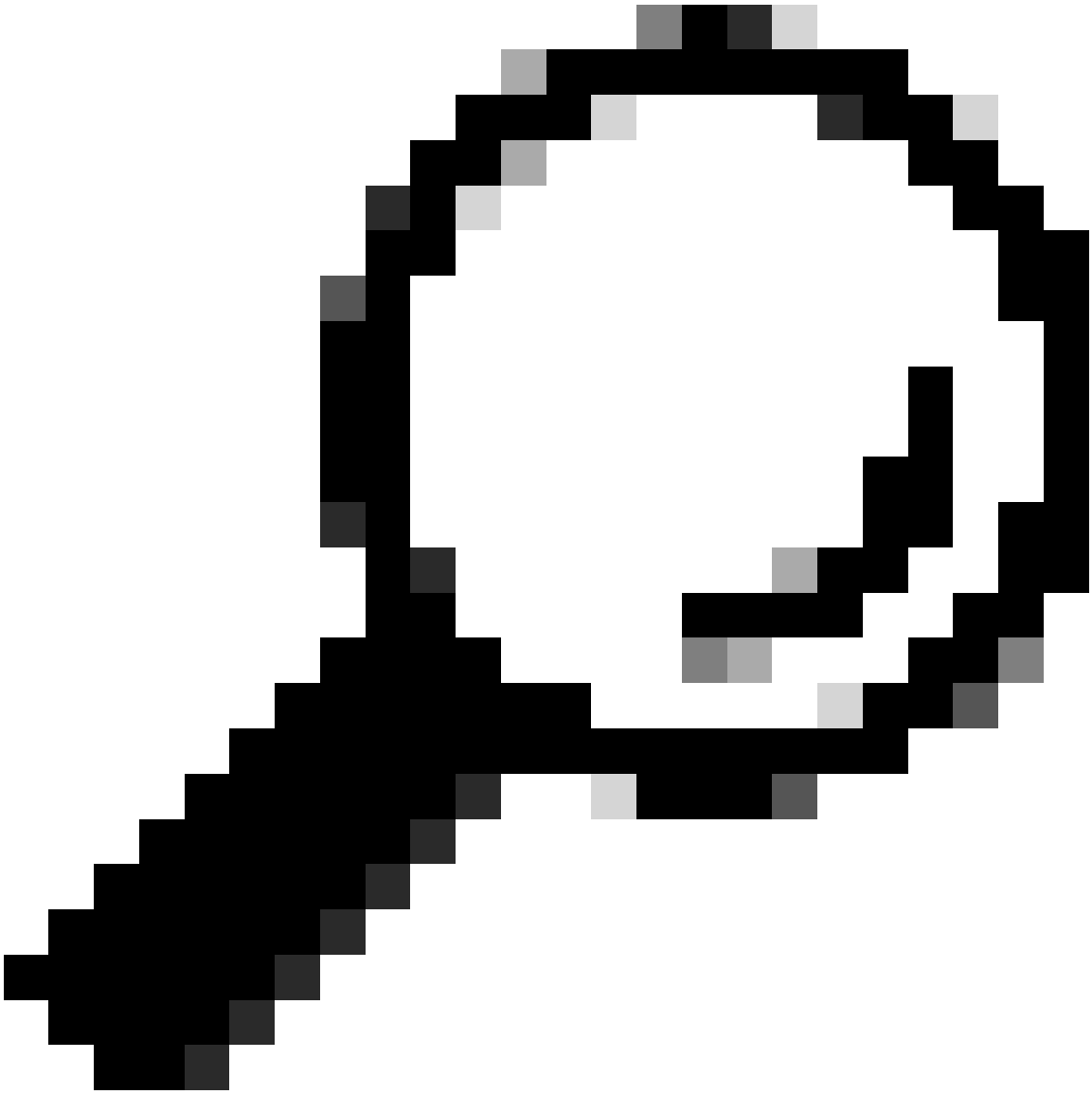
sudo systemctl restart systemd-resolved.service

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

Mettre à jour la configuration DNS

Pour mettre à jour les serveurs DNS dans Netplan, vous pouvez modifier le fichier de configuration Netplan de votre interface réseau.

Les fichiers de configuration Netplan sont stockés dans le répertoire **/etc/netplan**.



Conseil : un ou deux fichiers YAML se trouvent dans ce répertoire. Les noms de fichiers attendus sont 01-netcfg.yaml et/ou 50-cloud-init.yaml.

Ouvrez le fichier de configuration Netplan à l’aide de la commandesudo vi /etc/netplan/01-netcfg.yaml .

Dans le fichier de configuration Netplan, localisez la clé « nameservers » sous l’interface réseau.

Vous pouvez spécifier plusieurs adresses IP de serveur DNS séparées par des virgules.

Appliquez les modifications apportées à la configuration Netplan à l’aide de la **sudo netplan apply** commande.

Netplan génère les fichiers de configuration pour le service résolu par le système.

Pour vérifier que les nouveaux résolveurs DNS sont définis, exécutez la commanderesolvectl 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:~#
```

Système de fichiers local plein

Un message d'erreur courant peut apparaître sur la console du capteur : « Failed to create new system journal: No space left on device ».

Cela indique que le disque est plein et qu'il ne reste plus d'espace dans le système de fichiers / racine.

Exécutez la commandedf -ah / et déterminez l'espace 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:~#
```

Effacez les anciens journaux pour libérer de l'espace disque à l'aide de la commandejournalctl --vacuum-time 1d.

<#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:~#
```

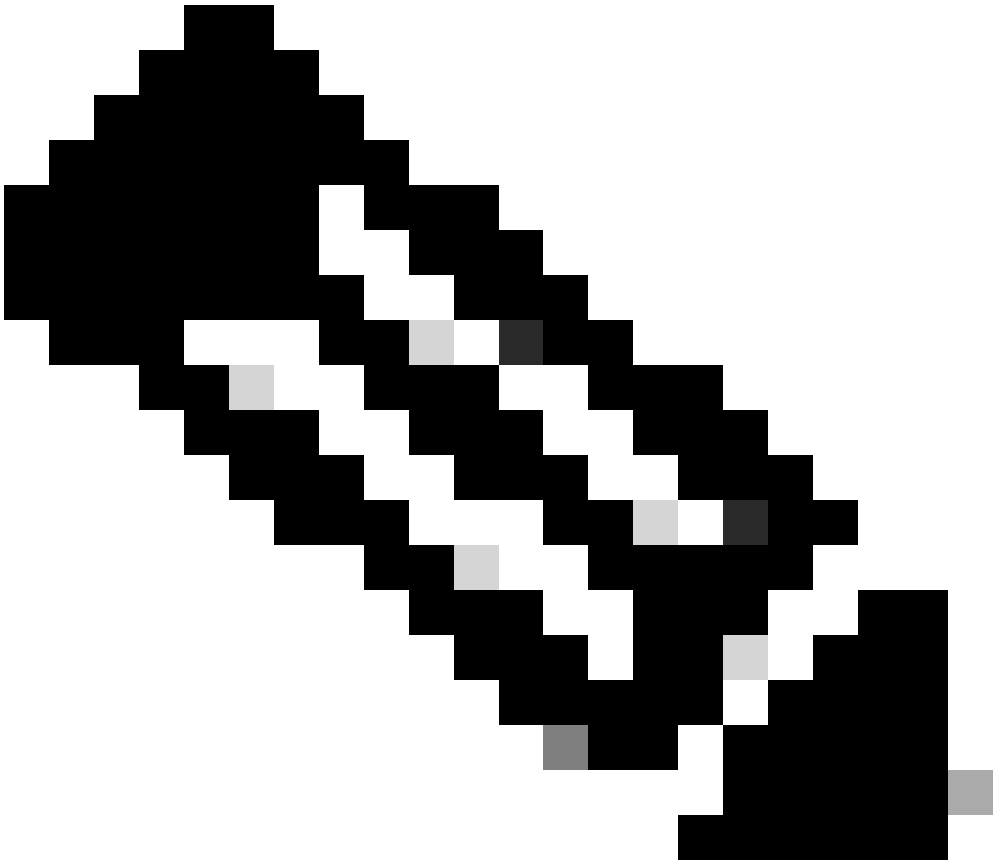
Assurez-vous que votre espace de stockage répond à la configuration système minimale requise décrite dans le guide de déploiement initial.

Ce guide est disponible sur la page d'assistance produit de Cisco Secure Cloud Analytics (StealthWatch Cloud) : https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/series.html

Configuration de surveillance

Un capteur disposant d'une bonne connectivité réseau au cloud et de paramètres DNS valides peut toujours présenter un état hors connexion.

Un état hors connexion est possible si les options de surveillance du capteur sont désactivées ou si le capteur n'envoie pas de pulsations.



Remarque : cette section concerne une installation par défaut du capteur ONA sans personnalisation et reçoit activement les données Netflow et/ou IPFIX.

Exécutez la commandegrep PNA_SERVICE /opt/obsrvbl-ona/config pour déterminer l'état.

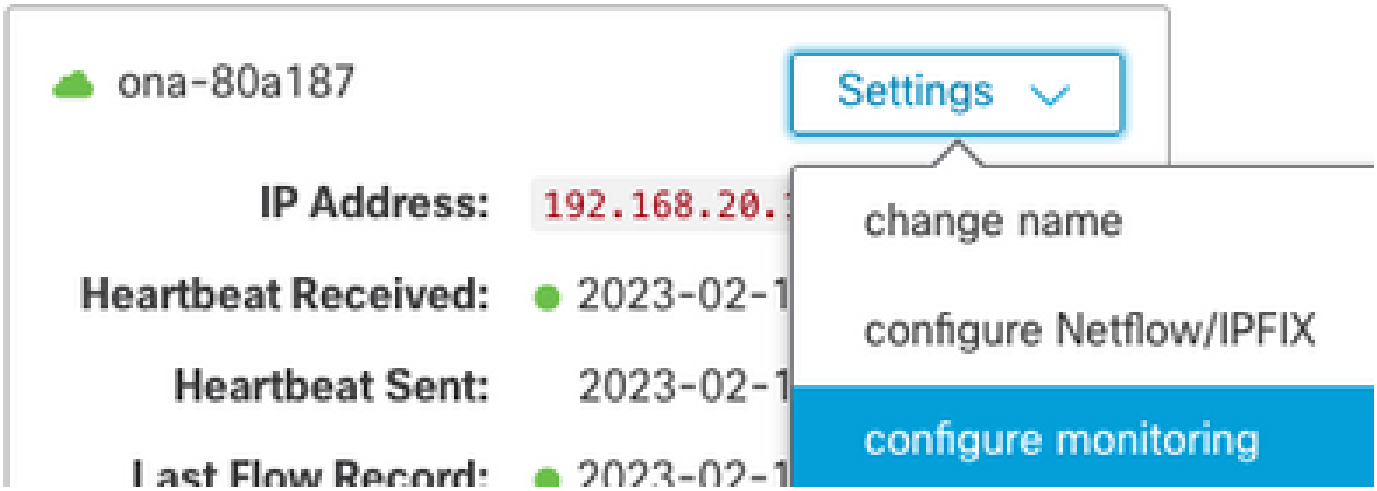
<#root>

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

grep PNA_SERVICE /opt/obsrvbl-ona/config

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

Si le service est défini sur false, vérifiez que les réseaux souhaités sont répertoriés dans Settings > configure monitoring pour votre capteur dans le portail SCA.



Exécutez la commandeps -fu obsrvbl_ona | grep pna et notez si le service est détecté et si les plages réseau surveillées attendues sont répertoriées.

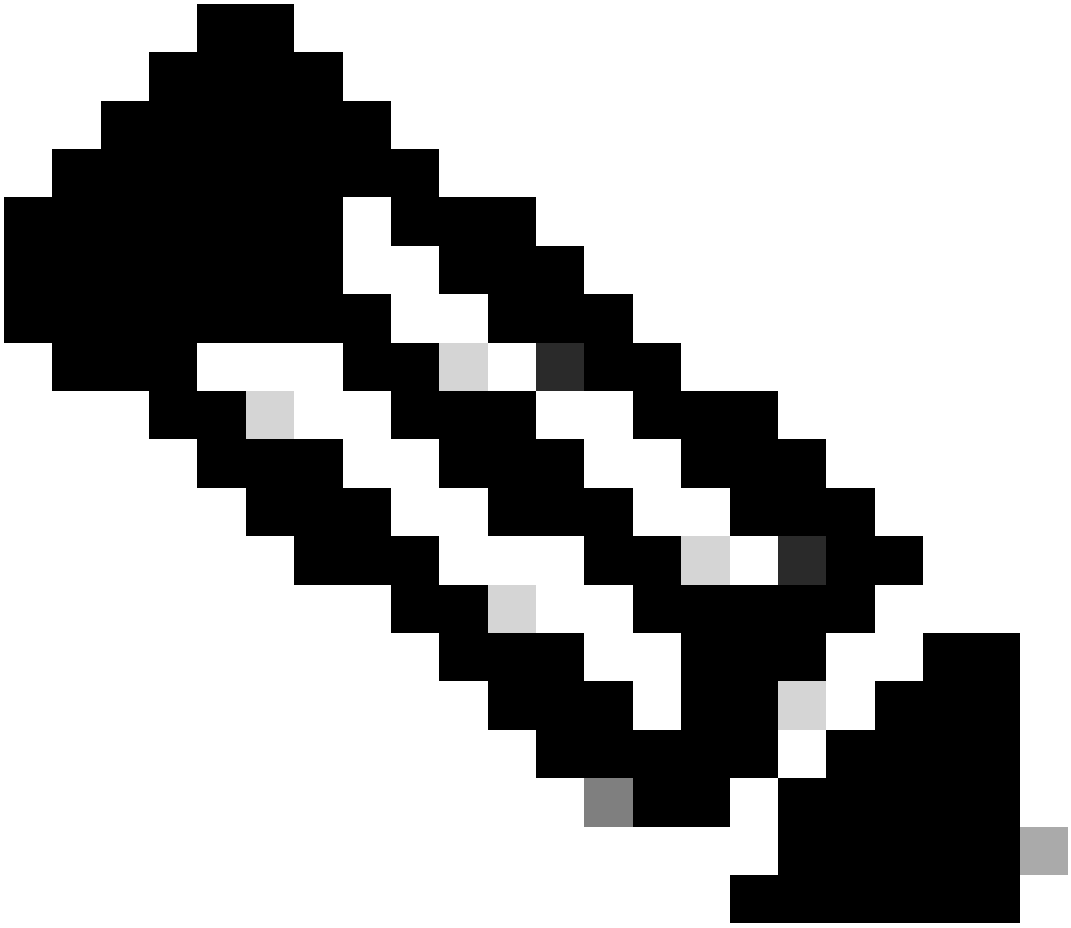
<#root>

```
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:~#
```

Le résultat de la commande montre que le service PNA a les ID de processus 956 et 957, et que les plages d'adresses privées 10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16 sont surveillées sur les interfaces ens192 et ens224.



Remarque : les plages d'adresses et les noms d'interface peuvent varier en fonction de la configuration et du déploiement du capteur

Erreurs SSL

Recherchez les erreurs SSL dans le fichier /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log à l'aide de la commandeless /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log.

Un exemple d'erreur est fourni.

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

Exécutez la commandewget https://s3.amazonaws.com et examinez le résultat pour voir s'il y a une inspection HTTPS possible.

En cas d'inspection HTTPS, assurez-vous que le capteur est retiré de toute inspection ou placé sur une liste autorisée.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.