Fehlerbehebung ONA Sensor Offline Status

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie mehrere mögliche Ursachen untersuchen können, warum ein Secure Cloud Analytics (SCA)-Sensor als offline angezeigt wird.

Hintergrundinformationen

Secure Cloud Analytics (SCA) wurde früher als Stealthwatch Cloud (SWC) bezeichnet und kann hier synonym verwendet werden.

Der SCA Sensor ist der Private Network Monitor und kann als ONA, ONA Sensor oder einfach nur als Sensor bezeichnet werden.

Die Befehle in diesem Artikel basieren auf der ona-20.04.1-server-amd64.iso-Debian-Installation.

Mögliche Ursachen von Offline-Sensoren

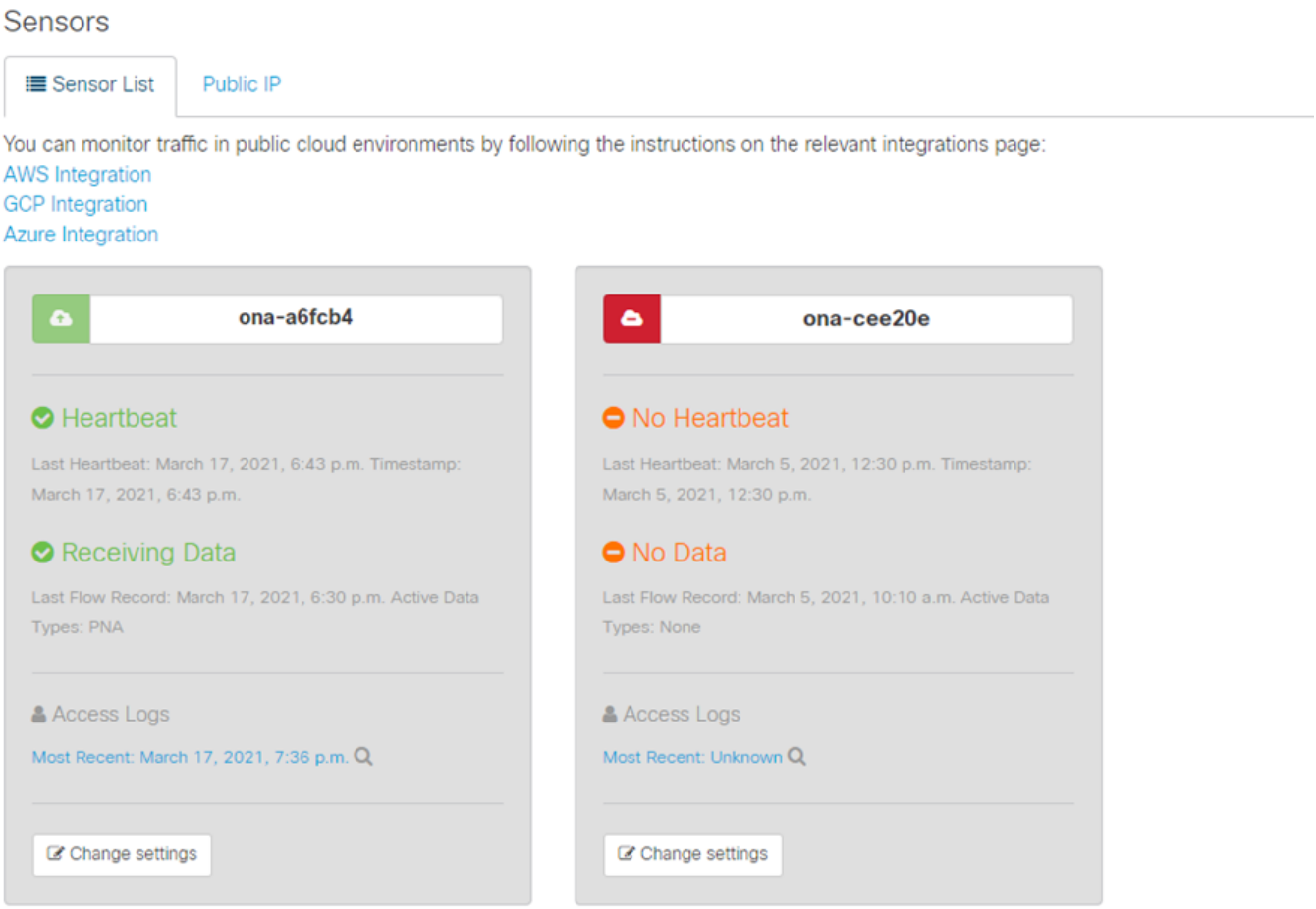
Es gibt viele mögliche Faktoren, die dazu führen können, dass ein Sensor einen Offline-Status anzeigt.

Zwei Beispiele für diese Faktoren sind Netzwerkprobleme, und das lokale Dateisystem verfügt über eine volle Festplatte.

Identifizieren eines Offline-Sensors

Das SCA Portal enthält eine Liste der konfigurierten Sensoren. Um auf diese Seite zuzugreifen, navigieren Sie zu Settings > Sensors.

Der Offline-Sensor in diesem Bild ist rot dargestellt und zeigt keinen aktuellen Heartbeat und keine neuen Daten an.



Überprüfen eines Offlinesensors

Netzwerkprobleme

Der ONA-Host kann den Internetzugriff verlieren, sodass der Sensor als offline aufgeführt wird.

Testen Sie, ob der ONA-Host in der Lage ist, einen Ping an eine bekannte aktive IP-Adresse zu senden, z. B. an einen der Google DNS-Server unter 8.8.8.8.

Melden Sie sich beim ONA-Sensor an, und führen Sie den Befehl **ping -c4 8.8.8.8 aus**.

<#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:~#
```

Wenn der Sensor einen Ping an eine bekannte aktive IP-Adresse nicht senden kann, prüfen Sie das genauer.

Bestimmen Sie mit dem Befehl das Standard-route -nGateway.

Prüfen Sie mit dem **arp -an** Befehl, ob ein gültiger ARP-Eintrag (Address Resolution Protocol) für das Standardgateway vorhanden ist.

Wenn der Sensor einen Ping an eine bekannte IP-Adresse senden kann, testen Sie die Auflösung des DNS-Hostnamens und die Fähigkeit des Sensors, eine Verbindung zur Cloud herzustellen.

Melden Sie sich beim Sensor an, und führen Sie den sudo curl https://sensor.ext.obsrvbl.com Befehl aus.

Die Ausgabe des curl-Befehls zeigt an, dass die DNS-Auflösung für sensor.ext.obsrvbl.com fehlgeschlagen ist und eine Untersuchung des DNS gerechtfertigt ist.

<#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:~#
```

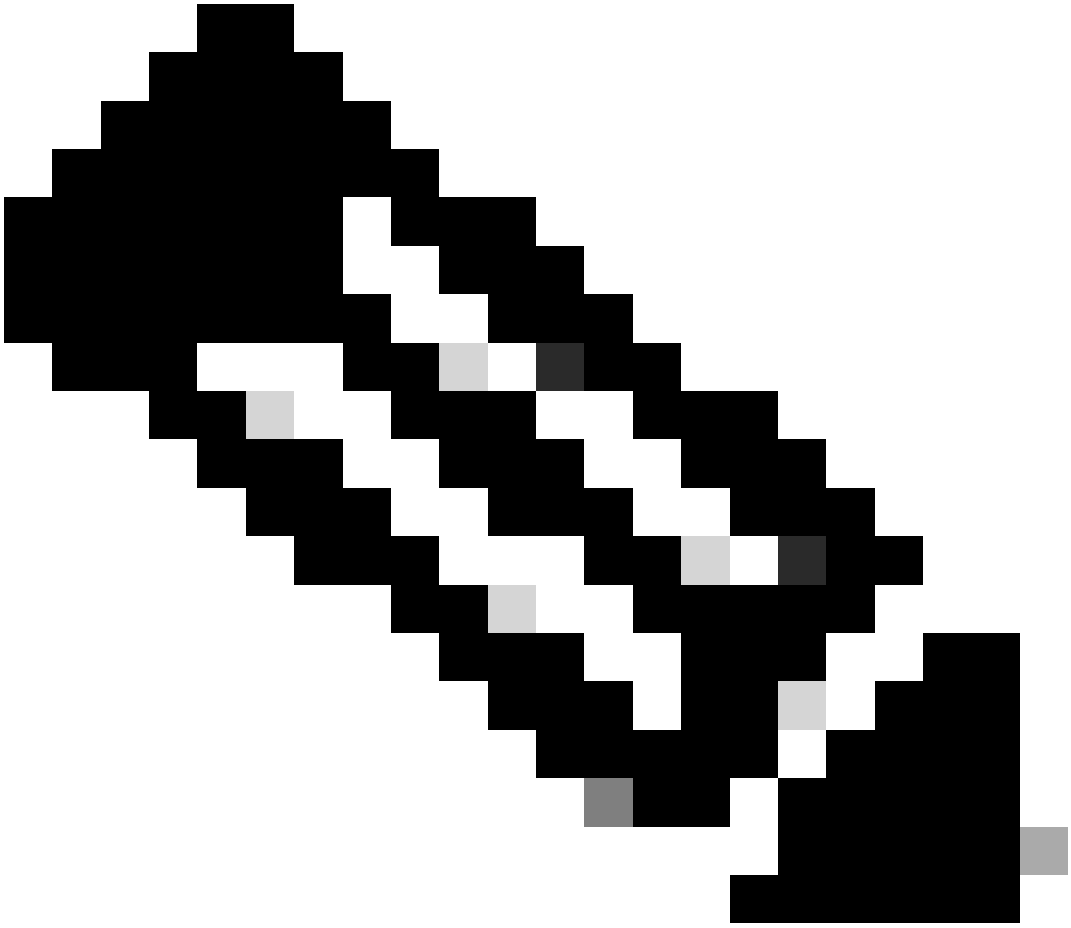
Diese Art von Antwort weist auf eine gute Verbindung hin und darauf, dass das Cloud-Portal den Sensor erkennt.

<#root>

user@example-ona:~#

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

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



Hinweis: Der Befehl curl kann geändert werden, um die entsprechende Region USA zu verwenden: https://sensor.ext.obsrvbl.com Europa: https://sensor.eu-prod.obsrvbl.com Australien: https://sensor.anz-prod.obsrvbl.com

Diese Art von Antwort weist auf eine gute Verbindung hin, aber der Sensor wurde keiner bestimmten Domäne zugeordnet.

```
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-Probleme

Wenn der Sensor Hostnamen nicht mit DNS auflösen kann, überprüfen Sie die DNS-Einstellungen mit dem cat /etc/netplan/01-netcfg.yaml Befehl.

Informationen, ob DNS-Einstellungen geändert werden müssen, finden Sie im Abschnitt "DNS-Konfiguration aktualisieren".

Nachdem die DNS-Einstellungen validiert wurden, führen Sie den sudo systemctl restart systemd-resolved.service Befehl aus.

Mit diesem Befehl wird keine Ausgabe erwartet.

<#root>

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

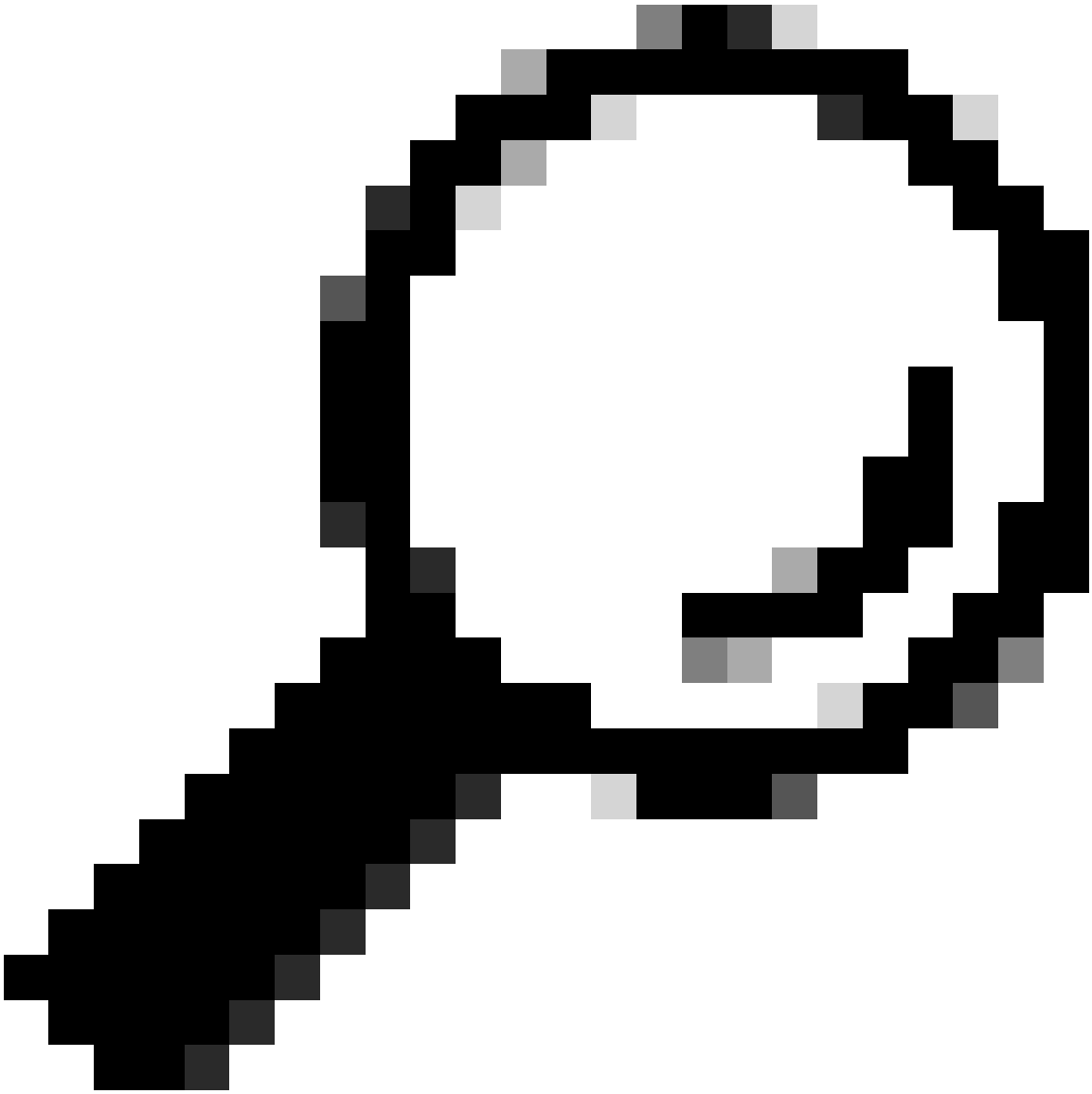
sudo systemctl restart systemd-resolved.service

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

Aktualisieren der DNS-Konfiguration

Um DNS-Server in Netplan zu aktualisieren, können Sie die Netplan-Konfigurationsdatei für Ihre Netzwerkschnittstelle ändern.

Netplan-Konfigurationsdateien werden im Verzeichnis **/etc/netplan** gespeichert.



Tipp: In diesem Verzeichnis befinden sich eine oder zwei YAML-Dateien. Die erwarteten Dateinamen sind 01-netcfg.yaml und/oder 50-cloud-init.yaml.

Öffnen Sie die NetPlan-Konfigurationsdatei mit dem sudo vi /etc/netplan/01-netcfg.yaml Befehl.

Suchen Sie in der Netplan-Konfigurationsdatei den Schlüssel "nameservers" unter der Netzwerkschnittstelle.

Sie können mehrere DNS-Server-IP-Adressen durch Kommas getrennt angeben.

Wenden Sie die Änderungen mit dem **sudo netplan apply** Befehl auf die NetPlan-Konfiguration an.

NetPlan generiert die Konfigurationsdateien für den systemaufgelösten Dienst.

Führen Sie den Befehl aus, um zu überprüfen, ob die neuen DNS-Resolver festgelegt sindresolvectl 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:~#
```

Lokales Dateisystem voll

Eine häufige Fehlermeldung kann in der Konsole des Sensors angezeigt werden: "Fehler beim Erstellen des neuen Systemjournals: Auf dem Gerät ist kein Speicherplatz mehr vorhanden."

Dies zeigt an, dass der Datenträger voll ist und im /root-Dateisystem kein Speicherplatz mehr verbleibt.

Führen Sie den df -ah / Befehl aus, und bestimmen Sie, wie viel Speicherplatz verfügbar ist.

<#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:~#
```

Löschen Sie alte Journalprotokolle, um mit dem Befehl Speicherplatz freizugebenjournalctl --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:~#
```

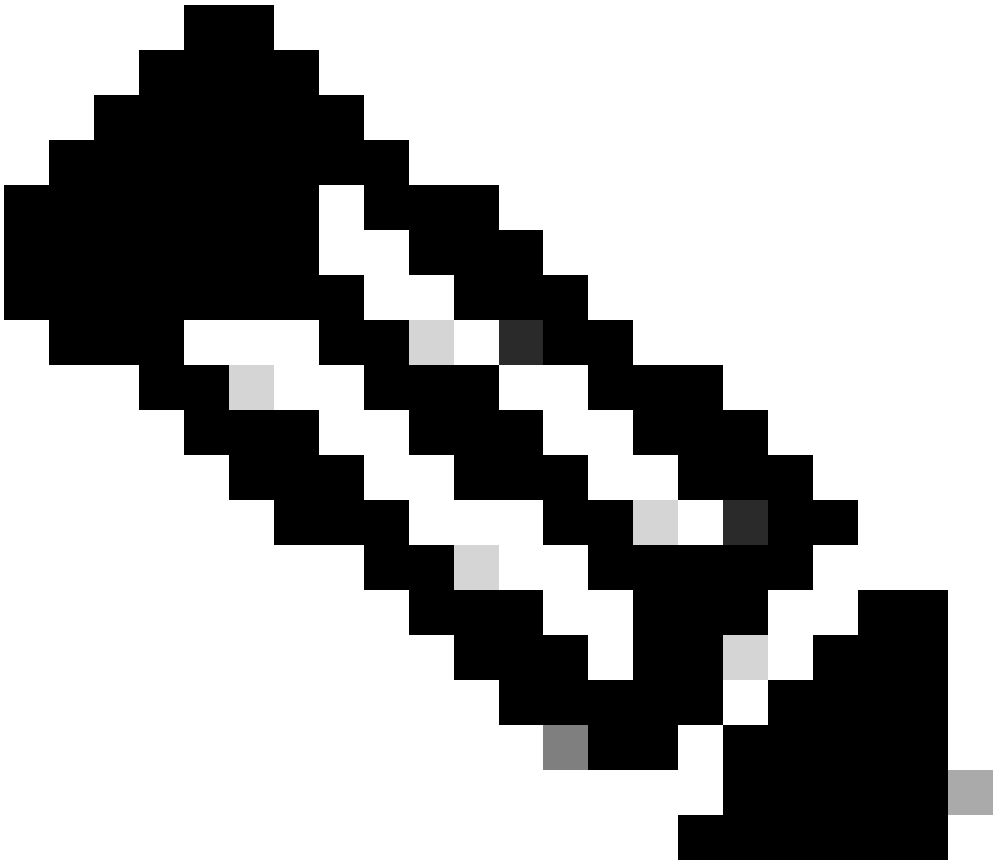
Stellen Sie sicher, dass Ihr Speicherplatz die im Leitfaden zur Erstbereitstellung beschriebenen Mindestsystemanforderungen erfüllt.

Der Leitfaden kann von der Support-Seite für Cisco Secure Cloud Analytics (StealthWatch Cloud) abgerufen werden: https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/series.html

Überwachungskonfiguration

Ein Sensor mit einer guten Netzwerkverbindung zur Cloud und gültigen DNS-Einstellungen kann weiterhin einen Offline-Status anzeigen.

Ein Offline-Status ist möglich, wenn die Optionen für die Sensorüberwachung deaktiviert sind oder der Sensor keine Heartbeats sendet.



Hinweis: Dieser Abschnitt dient zur Standardinstallation des ONA-Sensors ohne Anpassungen und empfängt aktiv NetFlow- und/oder IPFIX-Daten.

Führen Sie den grep PNA_SERVICE /opt/obsrvbl-ona/config Befehl aus, um den Status zu ermitteln.

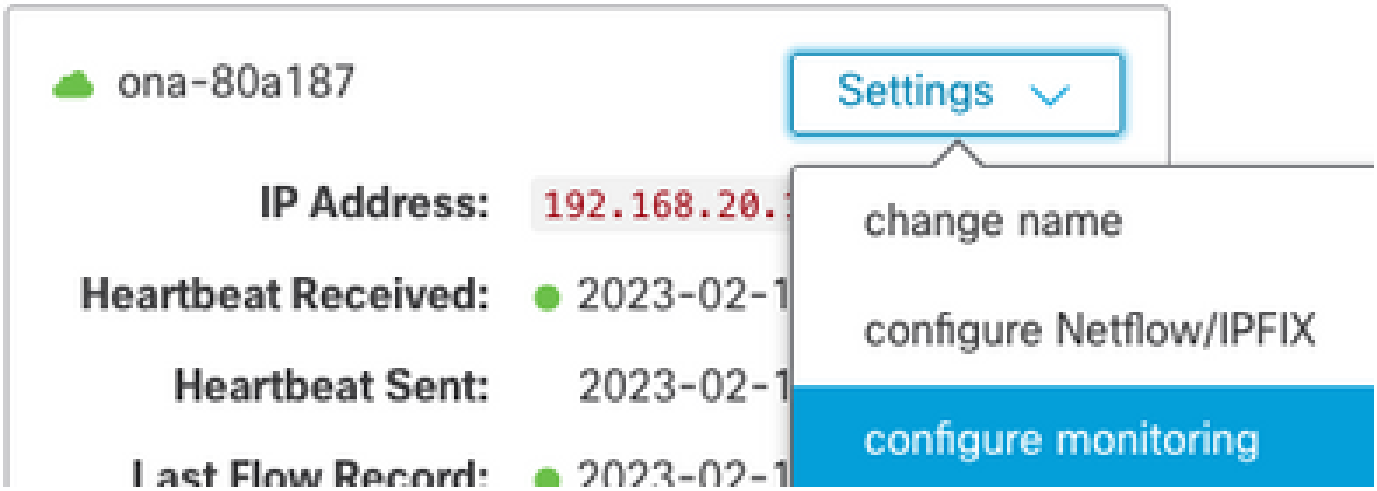
```
<#root>

user@example-ona:~#

grep PNA_SERVICE /opt/obsrvbl-ona/config

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

Wenn der Service auf "false" gesetzt ist, überprüfen Sie, ob die gewünschten Netzwerke Settings > configure monitoring für Ihren Sensor im SCA-Portal aufgeführt sind.



Führen Sie den ps -fu obsrvbl_ona | grep pna Befehl und den Hinweis aus, wenn der Dienst angezeigt wird und die erwarteten überwachten Netzwerkbereiche aufgeführt sind.

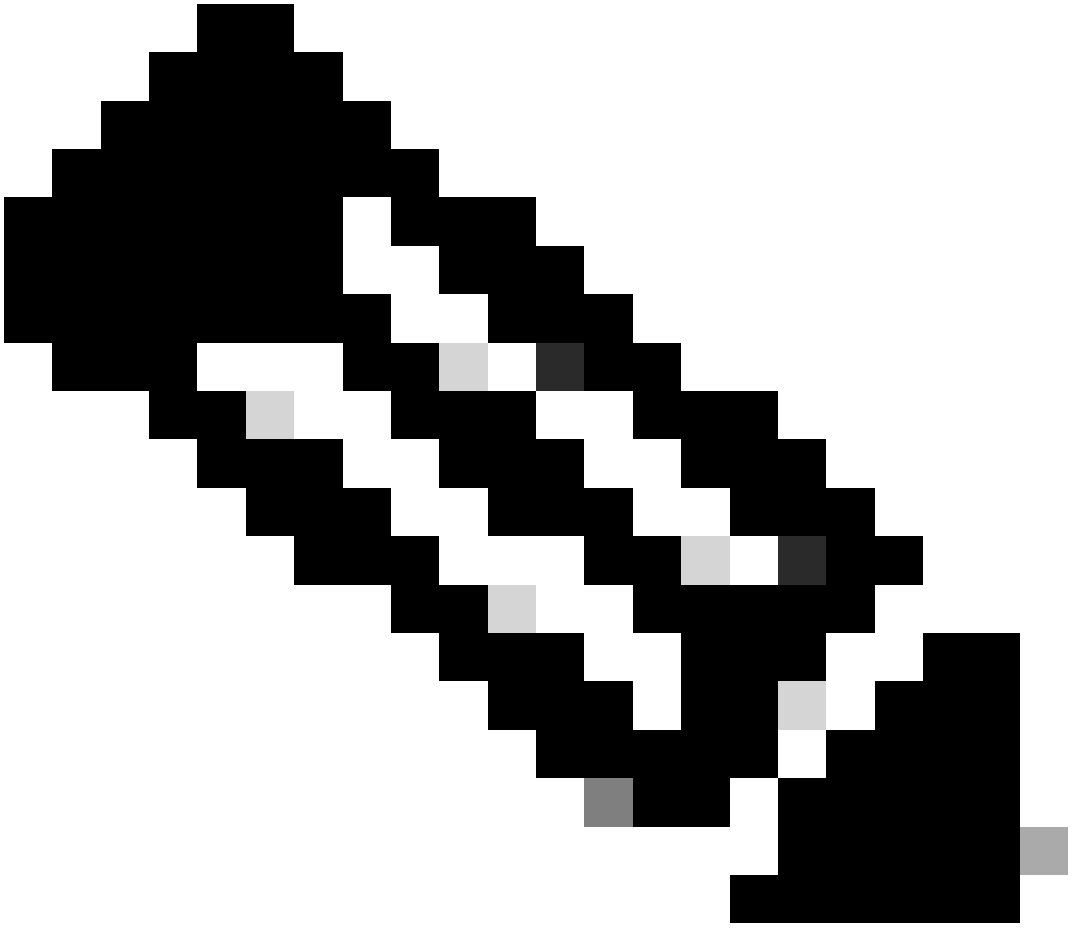
<#root>

```
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:~#
```

Die Ausgabe des Befehls zeigt, dass der PNA-Dienst die Prozess-ID 956 und 957 hat und dass die privaten Adressbereiche 10.0.0.0/8, 172.16.0.0/12 und 192.168.0.0/16 an den ens192- und ens224-Schnittstellen überwacht werden.



Hinweis: Die Adressbereiche und Schnittstellennamen können sich je nach Konfiguration und Bereitstellung des Sensors unterscheiden.

SSL-Fehler

Überprüfen Sie die Datei /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log mit dem Befehl auf SSL-Fehlerless /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log.

Es wird ein Beispielfehler angegeben.

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

Führen Sie den wget https://s3.amazonaws.com Befehl aus, und überprüfen Sie die Ausgabe, um festzustellen, ob eine HTTPS-Überprüfung möglich ist.

Wenn eine HTTPS-Überprüfung stattfindet, stellen Sie sicher, dass der Sensor aus jeder Überprüfung entfernt oder in eine Liste zulässiger Prüfungen aufgenommen wird.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.