Probleemoplossing voor ONA Sensor offline status

Inhoud

Inleiding

Achtergrondinformatie

- Mogelijke oorzaken van offline sensoren
- Identificeer een offline sensor

Een offline sensor onderzoeken

- Netwerkproblemen
- DNS-problemen
- De DNS-configuratie bijwerken
- Lokaal bestandssysteem - volledig
- Configuratie van bewaking

Inleiding

Dit document beschrijft hoe u meerdere mogelijke oorzaken van een Secure Cloud Analytics (SCA)-sensor kunt onderzoeken om als offline te verschijnen.

Achtergrondinformatie

Secure Cloud Analytics (SCA) werd voorheen Stealthwatch Cloud (SWC) genoemd en deze termen kunnen onderling worden gebruikt.

De SCA Sensor is de Private Network Monitor en kan worden aangeduid als ONA, ONA Sensor of gewoon als Sensor.

De commando's in dit artikel zijn gebaseerd op de ona-20.04.1-server-amd64.iso debian installatie.

Mogelijke oorzaken van offline sensoren

Er zijn vele mogelijke factoren die kunnen resulteren in een sensor om een offline status weer te geven.

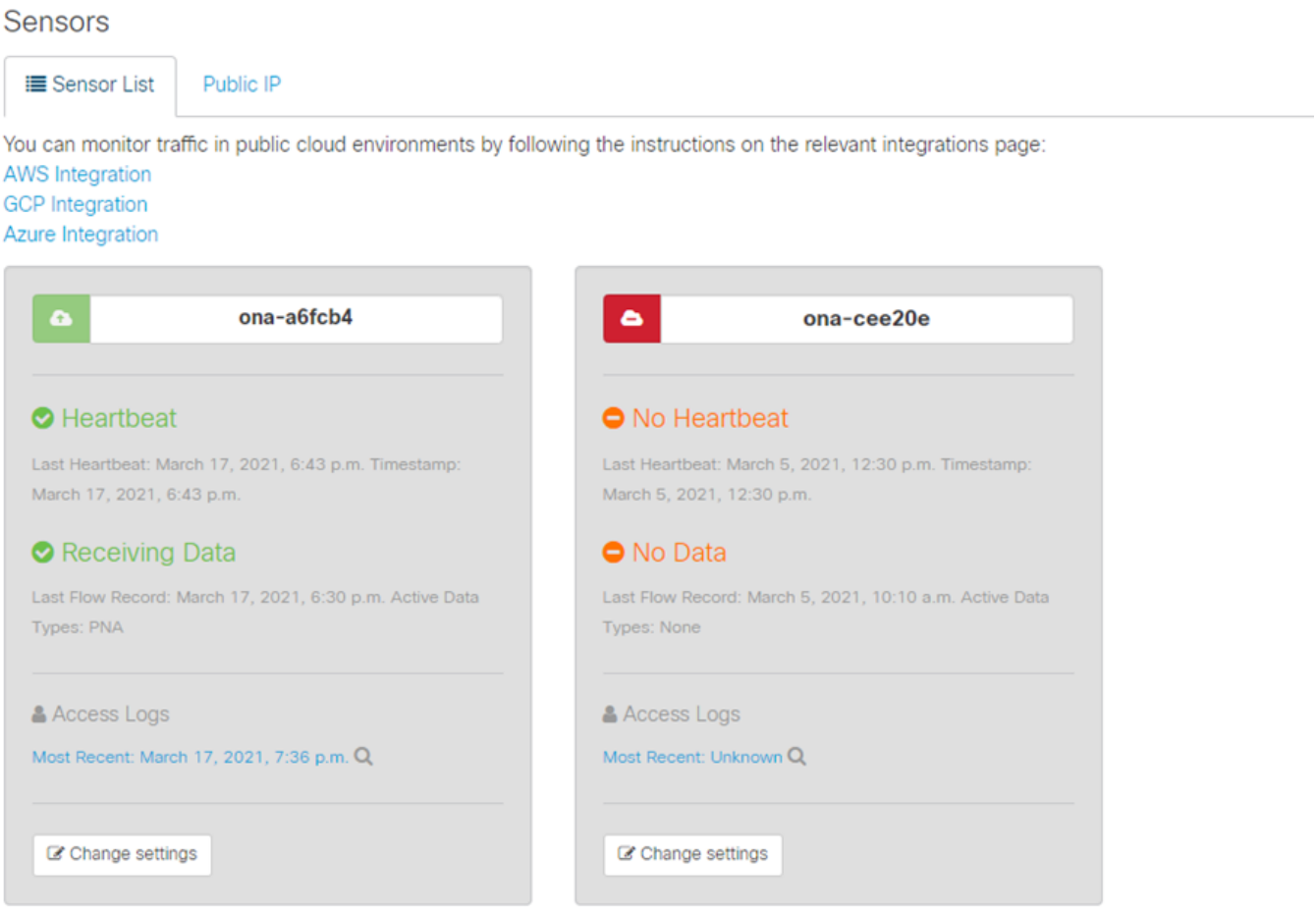
Twee voorbeelden van deze factoren zijn Netwerkgerelateerde problemen, en het lokale bestandssysteem heeft een volledige schijf.

Identificeer een offline sensor

Het SCA-portal bevat een lijst met geconfigureerde sensoren. Voor toegang tot deze pagina

navigeer je naar Settings > Sensors.

De offline sensor in dit beeld wordt weergegeven in rood en toont geen recente hartslag en data.



Een offline sensor onderzoeken

Netwerkproblemen

De ONA host kan internettoegang verliezen, wat resulteert in de Sensor om te worden vermeld als offline.

Test of de ONA Host in staat is om een bekend levend IP-adres, zoals een van de Google DNS-servers, te pingen op 8.8.8.8.

Log in op de ONA sensor en voer de opdracht **ping -c4 8.8.8.8 uit**.

<#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:~#
```

Als de Sensor niet in staat is om een bekend levend IP-adres te pingen, onderzoek dan verder.

Bepaal de standaardgateway met het route -n bevel.

Bepaal of er een geldige ARP-ingang (Address Resolution Protocol) is voor de standaardgateway die met de **arp -an** opdracht wordt weergegeven.

Als de Sensor een bekend IP-adres kan pingen, test dan de resolutie van de DNS-hostnaam en de mogelijkheid om van de sensor verbinding te maken met de cloud.

Log in op de Sensor en voer de opdrachtsudo curl https://sensor.ext.obsrvbl.com uit.

De curl opdrachtoutput laat zien dat DNS-resolutie voor sensor.ext.obsrvbl.com is mislukt en onderzoek naar DNS is gerechtvaardigd.

<#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:~#
```

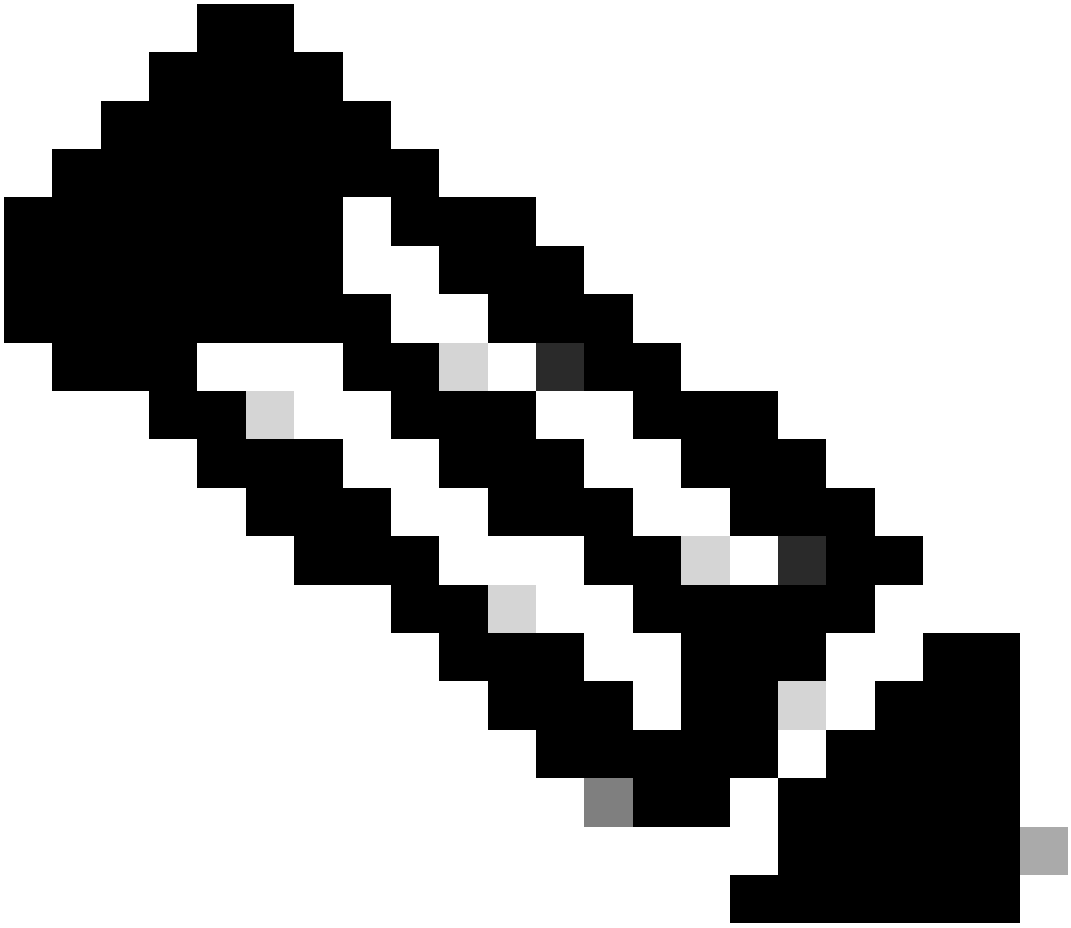
Dit type van een reactie duidt op een goede verbinding en ook dat de cloud portal de sensor herkent.

<**#root**>

user@example-ona:~#

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

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



Opmerking: De curl commando kan worden aangepast om de juiste regio te gebruiken: https://sensor.ext.obsrvbl.com Europa: https://sensor.eu-prod.obsrvbl.com Australië: https://sensor.anz-prod.obsrvbl.com

Dit type respons geeft een goede verbinding aan, maar de sensor is niet gekoppeld aan een bepaald domein.

```
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-problemen

Als Sensor niet in staat is om hostnamen met DNS op te lossen, verifieert u de DNS-instellingen met de opdrachtcat /etc/netplan/01-netcfg.yaml.

Als DNS-instellingen wijzigingen vereisen, raadpleegt u de sectie DNS Configuration bijwerken.

Zodra de DNS-instellingen zijn gevalideerd, voert u de opdracht uitsudo systemctl restart systemd-resolved.service.

Er wordt geen uitvoer verwacht met deze opdracht.

<#root>

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

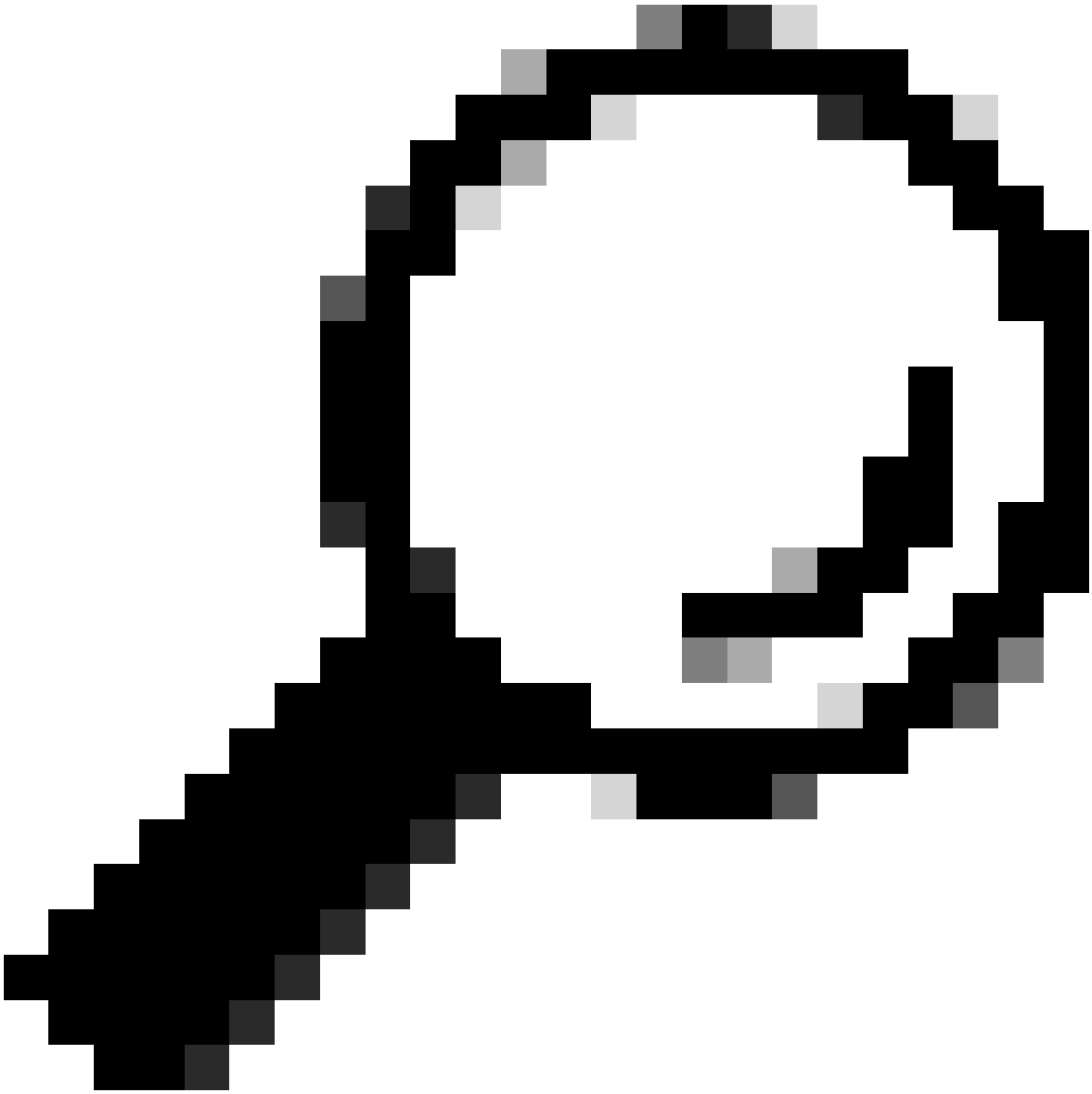
sudo systemctl restart systemd-resolved.service

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

De DNS-configuratie bijwerken

Als u DNS-servers in Netplan wilt bijwerken, kunt u het Netplan-configuratiebestand voor uw netwerkinterface wijzigen.

Netplan-configuratiebestanden worden opgeslagen in de **/etc/netplan** directory.



Tip: Een of twee YAML-bestanden kunnen in deze map worden gevonden. De verwachte bestandsnamen zijn 01-netcfg.yaml en/of 50-cloud-init.yaml.

Open het NetPlan-configuratiebestand met de opdrachtsudo vi /etc/netplan/01-netcfg.yaml.

Zoek in het Netplan-configuratiebestand de "nameservers"-toets onder de netwerkinterface.

U kunt meerdere IP-adressen van DNS-server opgeven, gescheiden door komma's.

Pas de wijzigingen toe op de NetPlan configuratie met de **sudo netplan apply** opdracht.

NetPlan genereert de configuratiebestanden voor de systeemopgeloste service.

Om te verifiëren dat de nieuwe DNS resolvers worden ingesteld, voert u de opdrachtresolvectl status | grep -A2 'DNS Servers' uit.

<#root>

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

resolvectl status | grep -A2 'DNS Servers'

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

user@example-ona:~#
```

Lokaal bestandssysteem - volledig

Een veel voorkomende foutmelding kan verschijnen op de console van de Sensor: "Mislukt om een nieuw systeemdagboek te maken: Geen ruimte over op apparaat."

Dit geeft aan dat de schijf vol is en dat er geen ruimte meer over is in het systeem met / hoofdbestanden.

df -ah /

Voer de opdracht uit en bepaal hoeveel ruimte er beschikbaar is.

<#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:~#
```

Oude tijdschriftenlogboeken wissen om schijfruimte vrij te maken met de opdrachtjournalctl --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:~#
```

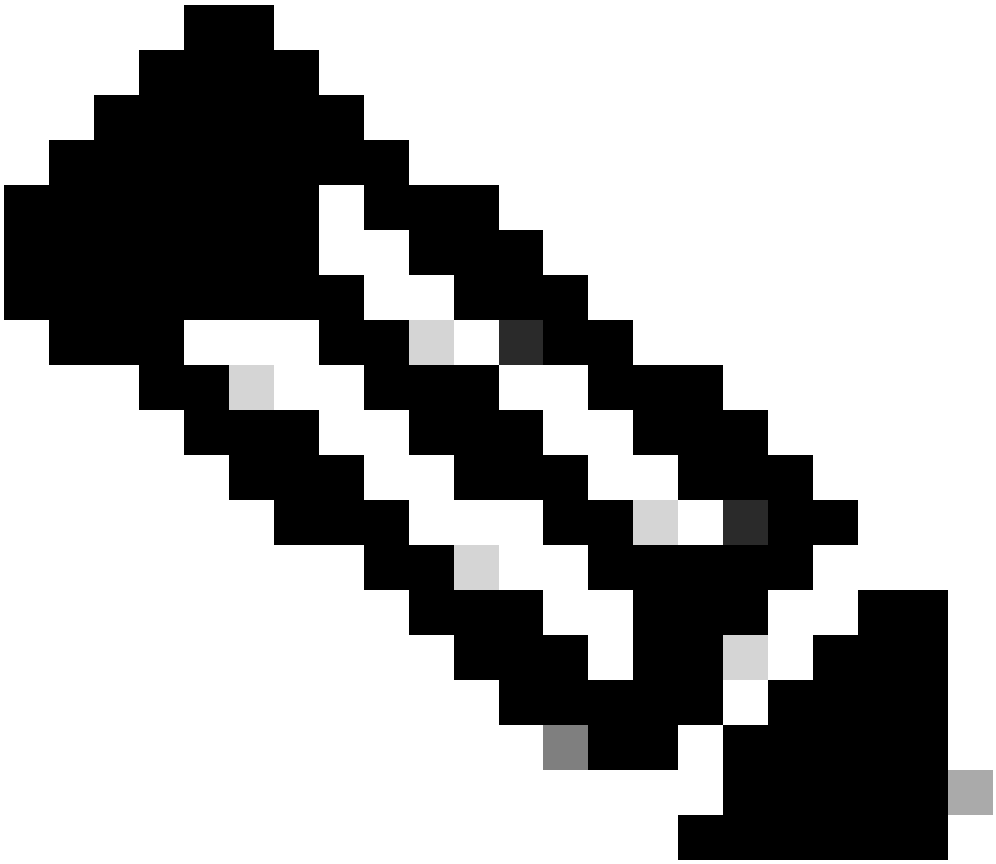
Zorg ervoor dat uw opslagruimte voldoet aan de minimale systeemvereisten die in de handleiding voor eerste implementatie zijn beschreven.

De handleiding kan worden opgehaald op de pagina voor productondersteuning van Cisco Secure Cloud Analytics (Stealthwatch Cloud): https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/series.html

Configuratie van bewaking

Een sensor die een goede netwerkverbinding met de cloud heeft en geldige DNS-instellingen kan nog steeds een offline status weergeven.

Een offline status is mogelijk als de Sensor controleopties zijn uitgeschakeld of als de Sensor geen hartslagen verstuurt.



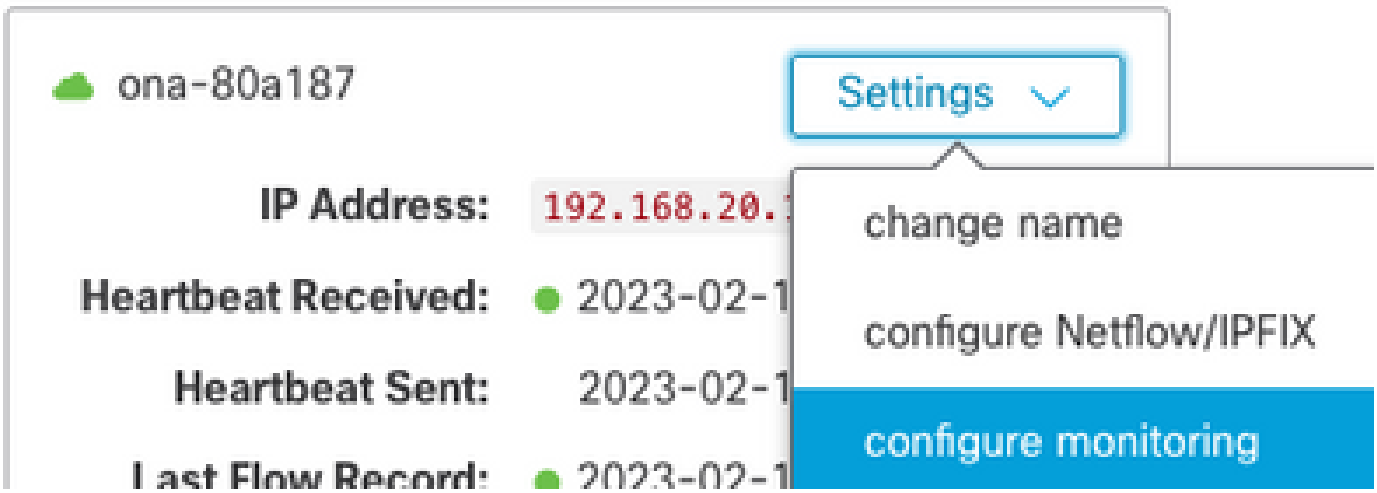
Opmerking: dit gedeelte is bedoeld voor een standaardinstallatie van de ONA Sensor zonder aanpassingen en ontvangt actief netflow- en/of IPFIX-gegevens.

Voer de opdrachtgrep PNA_SERVICE /opt/obsrvbl-ona/config uit om de status te bepalen.

```
<#root>

user@example-ona:~#

grep PNA_SERVICE /opt/obsrvbl-ona/config

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

Als de service op false is ingesteld, controleert u of de gewenste netwerken in Settings > configure monitoring voor uw sensor in het SCA-portal zijn vermeld.

ps -fu obsrvbl_ona | grep pna



Voer de opdracht en de opmerking uit als de service wordt gezien en als het verwachte bewaakte netwerkbereik wordt weergegeven.

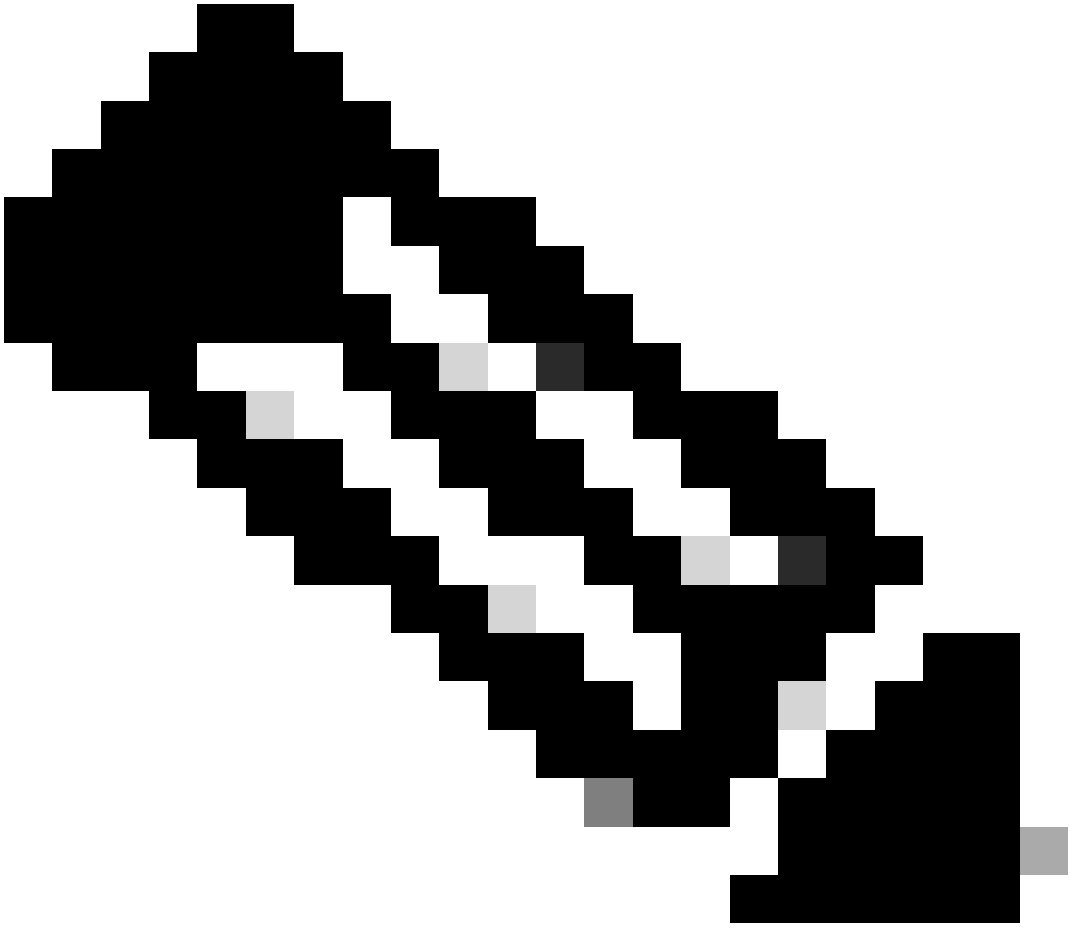
<#root>

```
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:~#
```

De output van het bevel toont aan dat de dienst PNA proces-ID 956 en 957 heeft, en de privé adresbereiken 10.0.0.0/8, 172.16.0.0/12, en 192.168.0.0/16 worden gecontroleerd op de interfaces ens192 en ens224.



Opmerking: het adresbereik en de interfacenamen kunnen verschillen op basis van de configuratie en de implementatie van de sensor

SSL-fouten

Controleer het /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log bestand op SSL-fouten met de opdrachtless /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log.

Er is een voorbeeldfout opgegeven.

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

Voer de opdrachtwget https://s3.amazonaws.com uit en controleer de uitvoer om te zien of er een mogelijke HTTPS-inspectie is.

Als er een HTTPS-inspectie is, zorg er dan voor dat de Sensor wordt verwijderd uit elke inspectie of wordt geplaatst op een toegestane lijst.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.