Risoluzione dei problemi relativi allo stato offline del sensore ONA

Sommario

Introduzione

Premesse

- Possibili cause dei sensori offline
- Identificazione di un sensore non in linea

Esaminare un sensore non in linea

- Problemi di rete
- Problemi DNS
- Aggiorna la configurazione DNS
- File system locale pieno
- Configurazione di monitoraggio

Introduzione

In questo documento viene descritto come analizzare diverse possibili cause per cui un sensore SCA (Secure Cloud Analytics) viene visualizzato come offline.

Premesse

Secure Cloud Analytics (SCA) in precedenza si chiamava Stealthwatch Cloud (SWC) e questi termini possono essere utilizzati in modo intercambiabile.

Il sensore SCA è il monitor di rete privato e può essere denominato ONA, ONA Sensor o semplicemente Sensor.

I comandi di questo articolo si basano sull'installazione debian ona-20.04.1-server-amd64.iso.

Possibili cause dei sensori offline

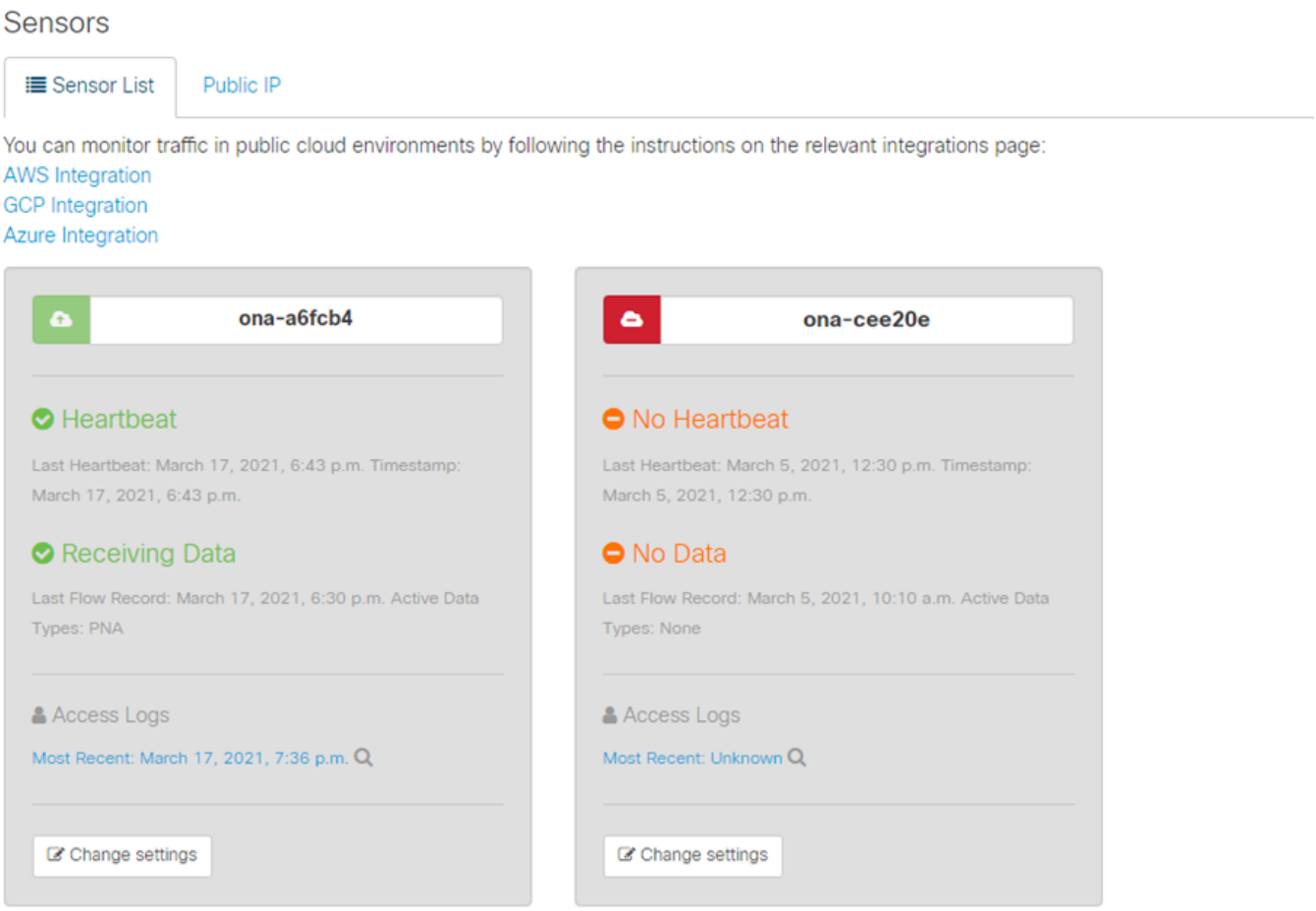
Sono molti i possibili fattori che possono determinare la presenza di uno stato non in linea da parte di un sensore.

Due esempi di questi fattori sono i problemi relativi alla rete e il file system locale dispone di un disco completo.

Identificazione di un sensore non in linea

Il portale SCA contiene un elenco di sensori configurati. Per accedere a questa pagina, passare a Settings > Sensors.

Il sensore offline in questa immagine è rappresentato in rosso e non mostra alcun heartbeat e dati recenti.



Esaminare un sensore non in linea

Problemi di rete

L'host ONA può perdere l'accesso a Internet e di conseguenza il sensore può essere elencato come non in linea.

Verificare se l'host ONA è in grado di eseguire il ping di un indirizzo IP noto come attivo, ad esempio uno dei server DNS Google, alla posizione 8.8.8.8.

Accedere al sensore ONA ed eseguire il 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 il sensore non è in grado di eseguire il ping di un indirizzo IP attivo noto, eseguire ulteriori ricerche.

Determinare il gateway predefinito con il route -n comando.

Verificare la presenza di una voce ARP (Address Resolution Protocol) valida rilevata per il gateway predefinito con il **arp -an** comando.

Se il sensore è in grado di eseguire il ping di un indirizzo IP noto, verificare la risoluzione dei nomi host DNS e la capacità del sensore di connettersi al cloud.

Accedere al sensore ed eseguire il sudo curl https://sensor.ext.obsrvbl.com comando.

L'output del comando curl mostra che la risoluzione DNS per sensor.ext.obsrvbl.com non è riuscita e che è garantita l'analisi del DNS.

<#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:~#
```

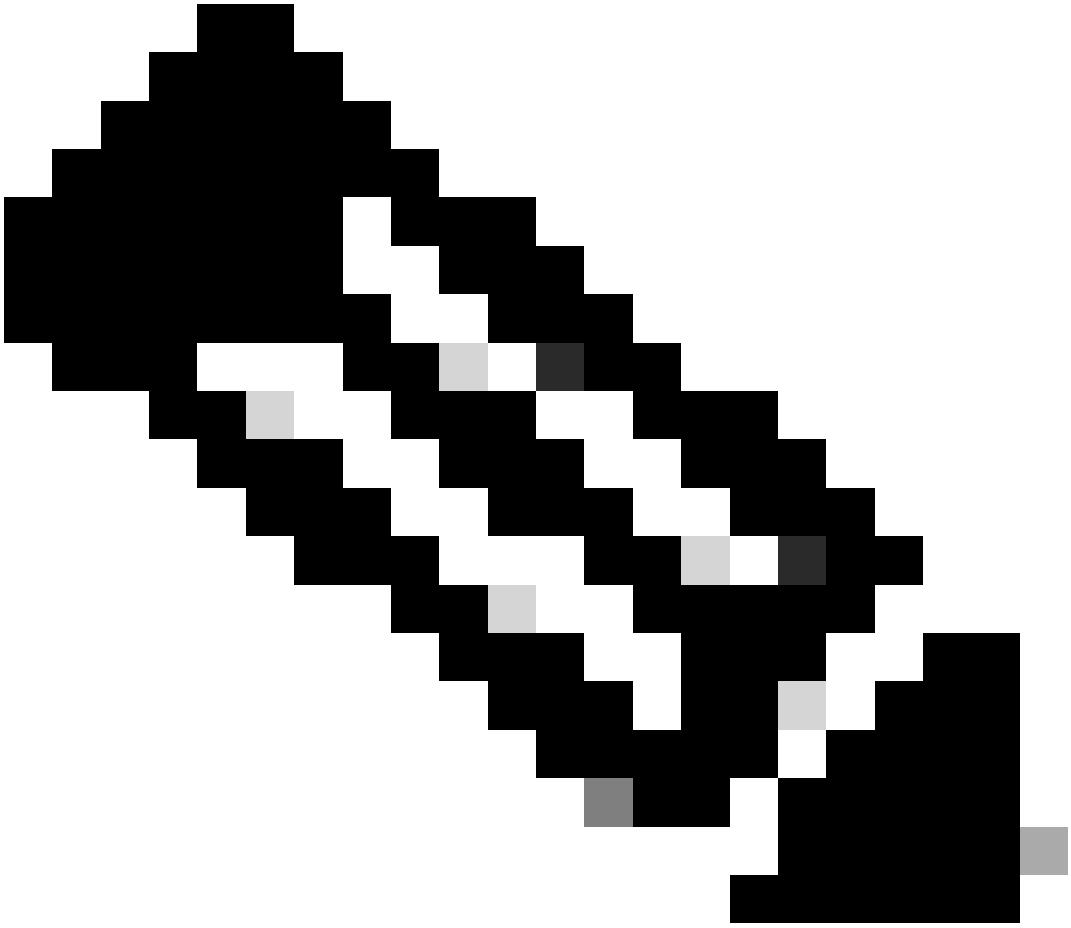
Questo tipo di risposta indica una buona connessione e anche che il portale del cloud riconosce il sensore.

<#root>

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

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

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



Nota: il comando curl può essere modificato in modo da utilizzare la regione appropriata US: https://sensor.ext.obsrvbl.com Europe: https://sensor.eu-prod.obsrvbl.com Australia: https://sensor.anz-prod.obsrvbl.com

---

Questo tipo di risposta indica una connessione valida, ma il sensore non è stato associato a un particolare dominio.

```
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:~#
```

Problemi DNS

Se Sensor non è in grado di risolvere i nomi host con DNS, verificare le impostazioni DNS con il cat /etc/netplan/01-netcfg.yaml comando.

se le impostazioni DNS richiedono modifiche, fare riferimento alla sezione Aggiornamento della configurazione DNS.

Una volta convalidate le impostazioni DNS, eseguire il sudo systemctl restart systemd-resolved.service comando.

Non è previsto alcun output con questo comando.

<#root>

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

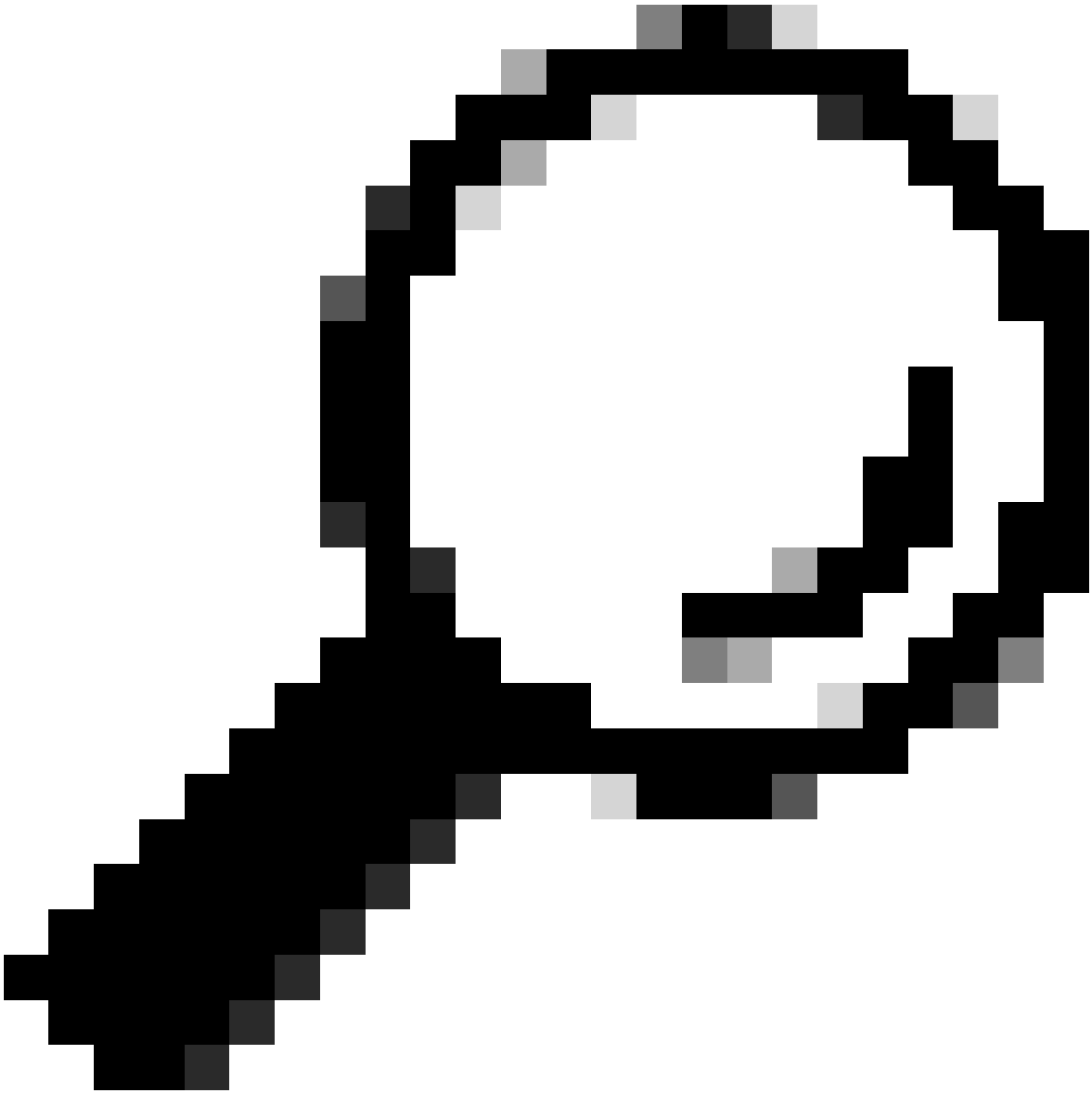
sudo systemctl restart systemd-resolved.service

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

Aggiorna la configurazione DNS

Per aggiornare i server DNS in Netplan, è possibile modificare il file di configurazione di Netplan per l'interfaccia di rete.

I file di configurazione Netplan sono memorizzati nella directory **/etc/netplan**.



Suggerimento: in questa directory è possibile trovare uno o due file YAML. I nomi file previsti sono 01-netcfg.yaml e/o 50-cloud-init.yaml.

Aprire il file di configurazione Netplan con il sudo vi /etc/netplan/01-netcfg.yaml comando.

Nel file di configurazione Netplan, individuare la chiave "nameservers" nell'interfaccia di rete.

È possibile specificare più indirizzi IP dei server DNS separati da virgole.

Applicare le modifiche alla configurazione Netplan con il **sudo netplan apply** comando.

Netplan genera i file di configurazione per il servizio risolto dal sistema.

Per verificare che i nuovi resolver DNS siano impostati, eseguire il resolvectl status | grep -A2 'DNS Servers' comando.

<#root>

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

resolvectl status | grep -A2 'DNS Servers'

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

user@example-ona:~#
```

File system locale pieno

Sulla console del sensore può essere visualizzato un messaggio di errore comune: "Impossibile creare il nuovo journal di sistema: spazio esaurito sul dispositivo".

Ciò indica che il disco è pieno e non vi è più spazio nel file system radice.

Eseguire il comandodf -ah / e determinare lo spazio disponibile.

<#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:~#
```

Per liberare spazio su disco con il comando,journalctl --vacuum-time 1d cancellare i registri di journal meno recenti.

<#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:~#
```

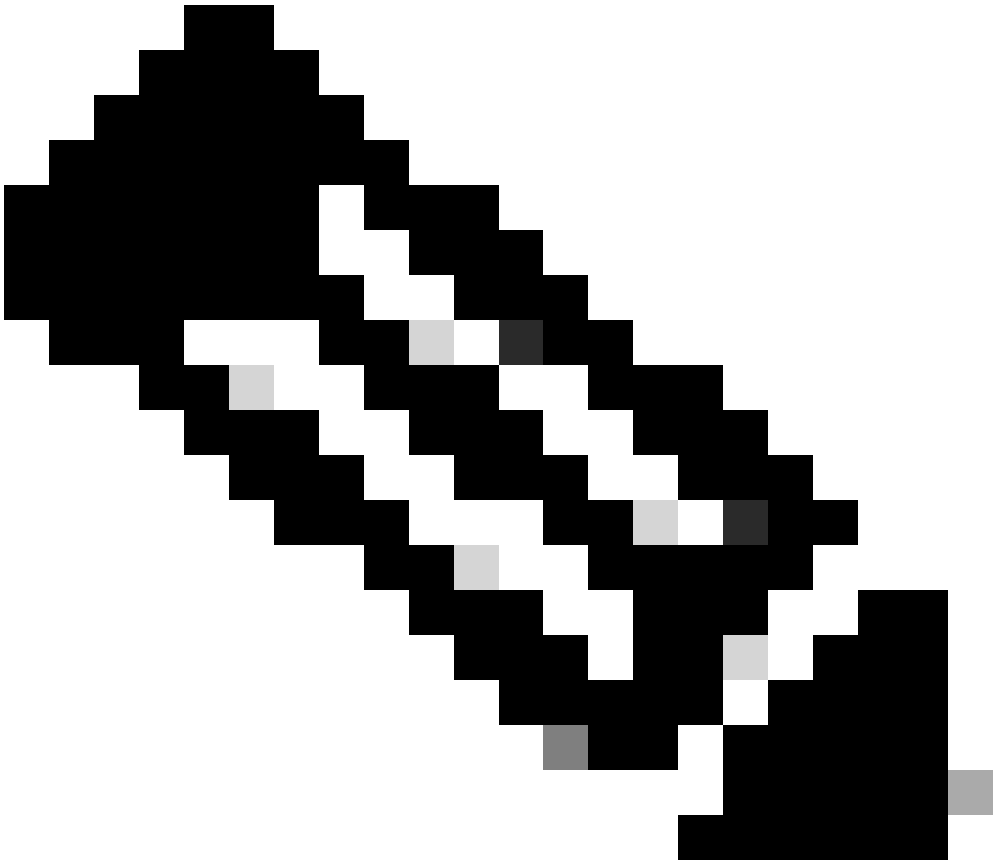
Verificare che lo spazio di storage in uso soddisfi i requisiti minimi di sistema descritti nella Guida alla distribuzione iniziale.

La guida può essere recuperata dalla pagina di supporto dei prodotti Cisco Secure Cloud Analytics (Stealthwatch Cloud): https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/series.html

Configurazione di monitoraggio

Un sensore con una buona connettività di rete al cloud e impostazioni DNS valide può comunque presentare uno stato offline.

Lo stato offline è possibile se le opzioni di monitoraggio del sensore sono disabilitate o se il sensore non invia heartbeat.



Nota: questa sezione è destinata all'installazione predefinita del sensore ONA senza personalizzazioni e riceve attivamente i dati netflow e/o IPFIX.

Eseguire il comandogrep PNA_SERVICE /opt/obsrvbl-ona/config per determinare lo stato.

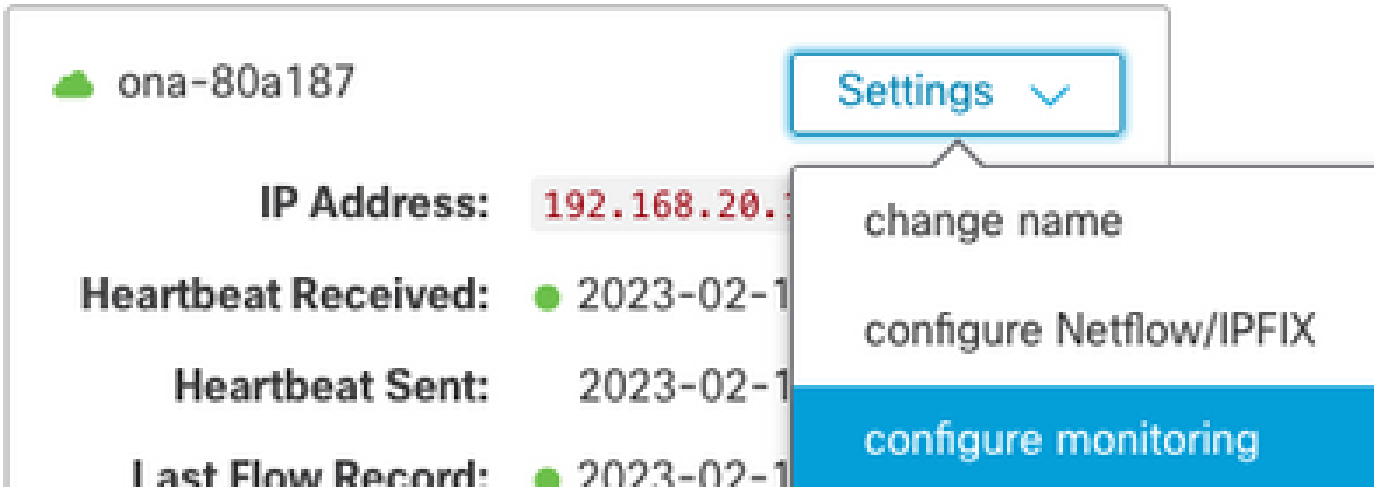
<#root>

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

grep PNA_SERVICE /opt/obsrvbl-ona/config

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

Se il servizio è impostato su false, verificare che le reti desiderate siano elencate in Settings > configure monitoring per il sensore nel portale SCA.



Eseguire il comando e la nota se il servizio è visibile e se sono elencati gli intervalli di rete monitorati previstips -fu obsrvbl_ona | grep pna.

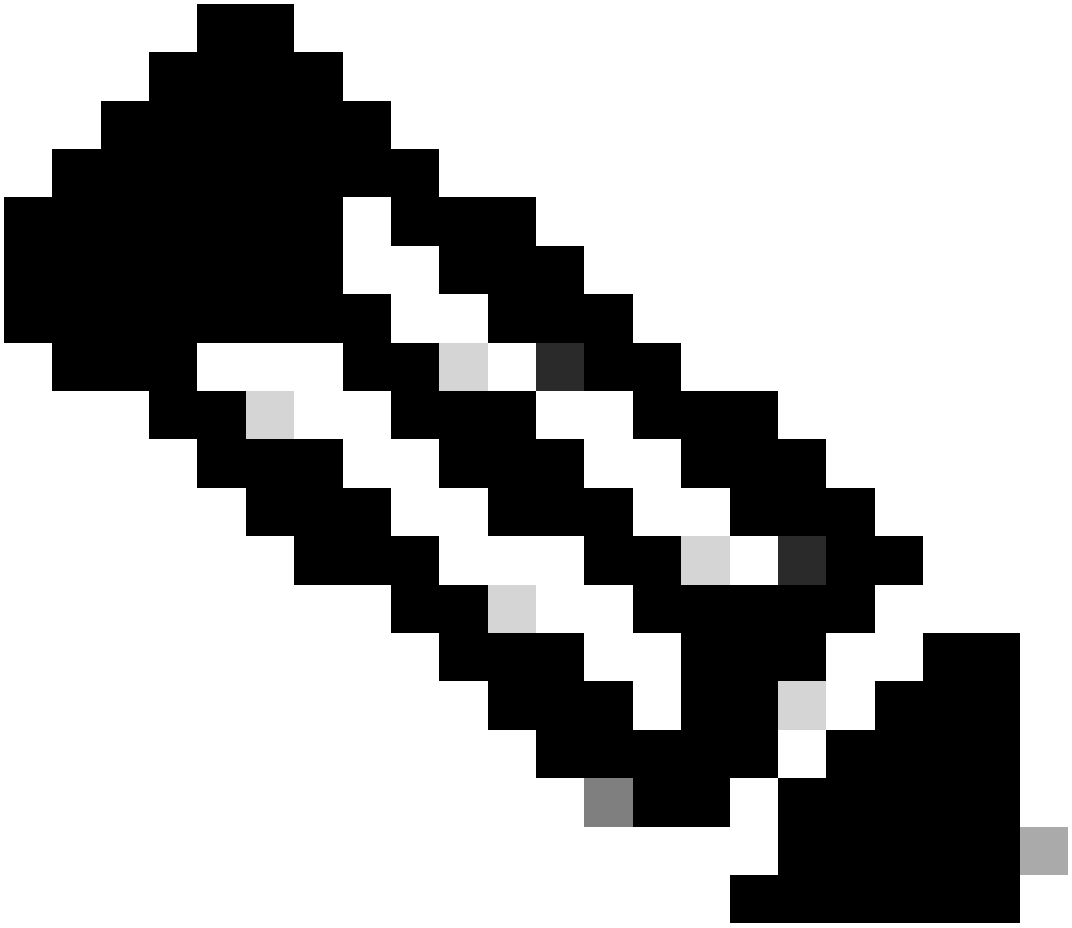
<#root>

```
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:~#
```

L'output del comando mostra che il servizio PNA ha gli ID di processo 956 e 957 e che gli intervalli di indirizzi privati 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16 sono monitorati sulle interfacce ens192 e ens224.



Nota: gli intervalli di indirizzi e i nomi delle interfacce possono variare in base alla configurazione e alla distribuzione del sensore

Errori SSL

Esaminare il file /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log per individuare eventuali errori SSL con il less /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log comando.

Viene fornito un esempio di errore.

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

Eseguire il comandowget https://s3.amazonaws.com e rivedere l'output per verificare se è possibile eseguire l'ispezione HTTPS.

In caso di ispezione HTTPS, assicurarsi che il sensore sia rimosso da qualsiasi ispezione o inserito in un elenco consentito.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).