ONAセンサーのオフラインステータスのトラブルシューティング

内容

はじめに

背景説明

- オフラインセンサーの考えられる原因
- オフラインセンサーの識別

オフラインセンサーの調査

- ネットワークの問題
- DNSの問題
- DNS設定の更新
- ローカルファイルシステムがいっぱいです
- モニタリング設定

はじめに

このドキュメントでは、Secure Cloud Analytics(SCA)Sensorがオフラインとして表示される複数の原因を調査する方法について説明します。

背景説明

Secure Cloud Analytics(SCA)は、以前はStealthwatch Cloud(SWC)と呼ばれていましたが、これらの用語は同じ意味で使用できます。

SCAセンサーはプライベートネットワーク監視であり、ONA、ONAセンサー、または単にセンサーと呼ぶことができます。

この記事のコマンドは、ona-20.04.1-server-amd64.iso debianインストールに基づいています。

オフラインセンサーの考えられる原因

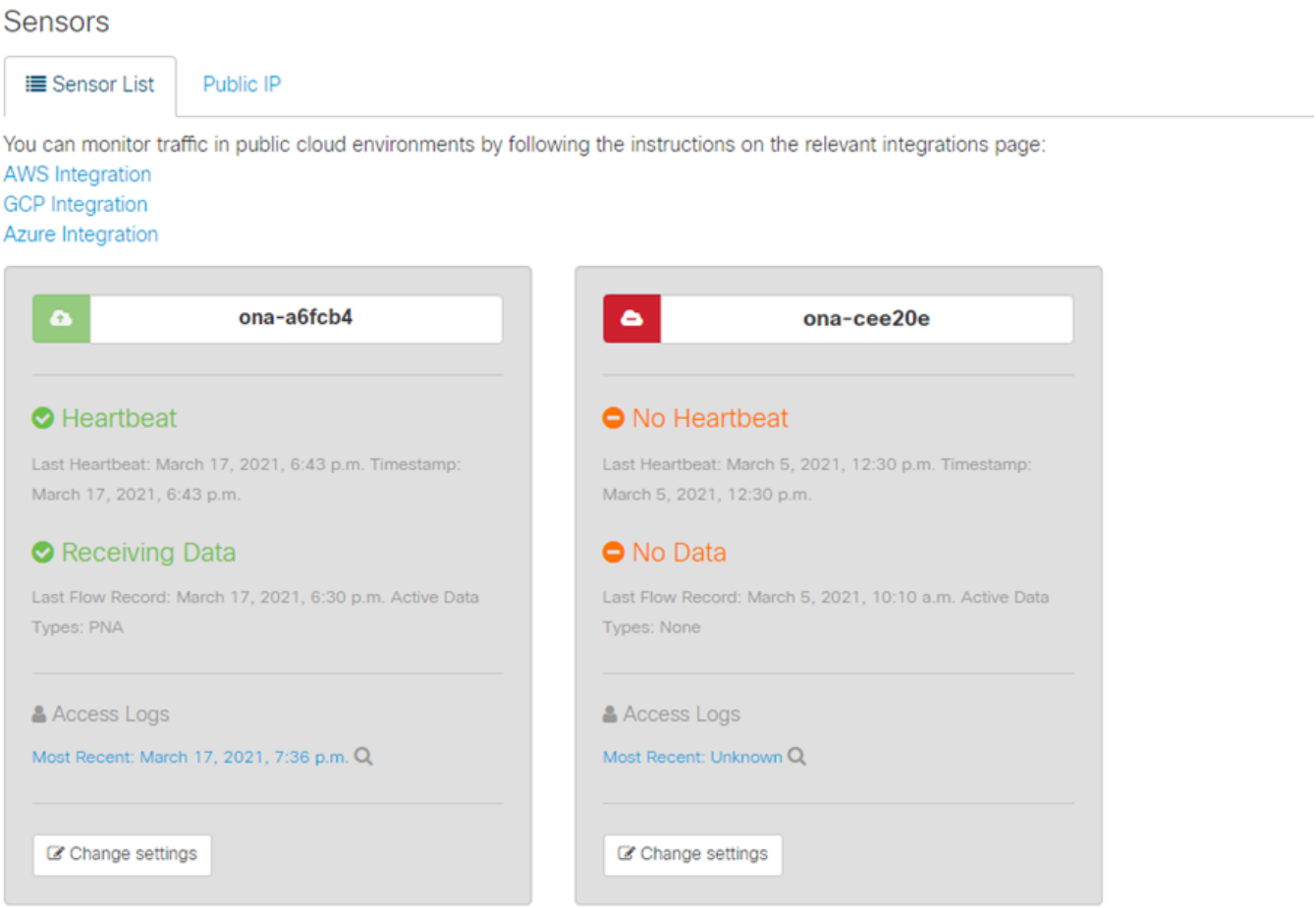
センサーがオフライン状態を示す原因として、さまざまな要因が考えられます。

これらの要因の2つの例はネットワーク関連の問題であり、ローカルファイルシステムにはフルディスクがあります。

オフラインセンサーの識別

SCAポータルには、設定済みセンサーのリストが含まれています。このページにアクセスするには、 Settings > Sensors.

このイメージのオフラインセンサーは赤で表示され、最近のハートビートとデータは表示されません。



オフラインセンサーの調査

ネットワークの問題

ONAホストがインターネットアクセスを失い、センサーがオフラインとしてリストされる可能性があります。

ONAホストが、8.8.8.8のGoogle DNSサーバの1つなど、既知の有効なIPアドレスにpingできるかどうかをテストします。

ONAセンサーにログインし、**ping -c4 8.8.8.8**コマンドを実行します。

<#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:~#
```

センサーが既知の有効なIPアドレスにpingできない場合は、さらに調査します。

route -n

コマンドを使用してデフォルトゲートウェイを確認します。

arp -an

コマンドを使用して、有効なAddress Resolution Protocol（ARP；アドレス解決プロトコル）エントリがデフォルトゲートウェイに表示されているかどうかを確認します。

センサーが既知のIPアドレスにpingできる場合は、DNSホストの名前解決と、センサーがクラウドに接続できるかどうかをテストします。

センサーにログインし、sudo curl https://sensor.ext.obsrvbl.comコマンドを実行します。

curlコマンドの出力は、sensor.ext.obsrvbl.comのDNS解決が失敗し、DNSの調査が必要であることを示しています。

<#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:~#
```

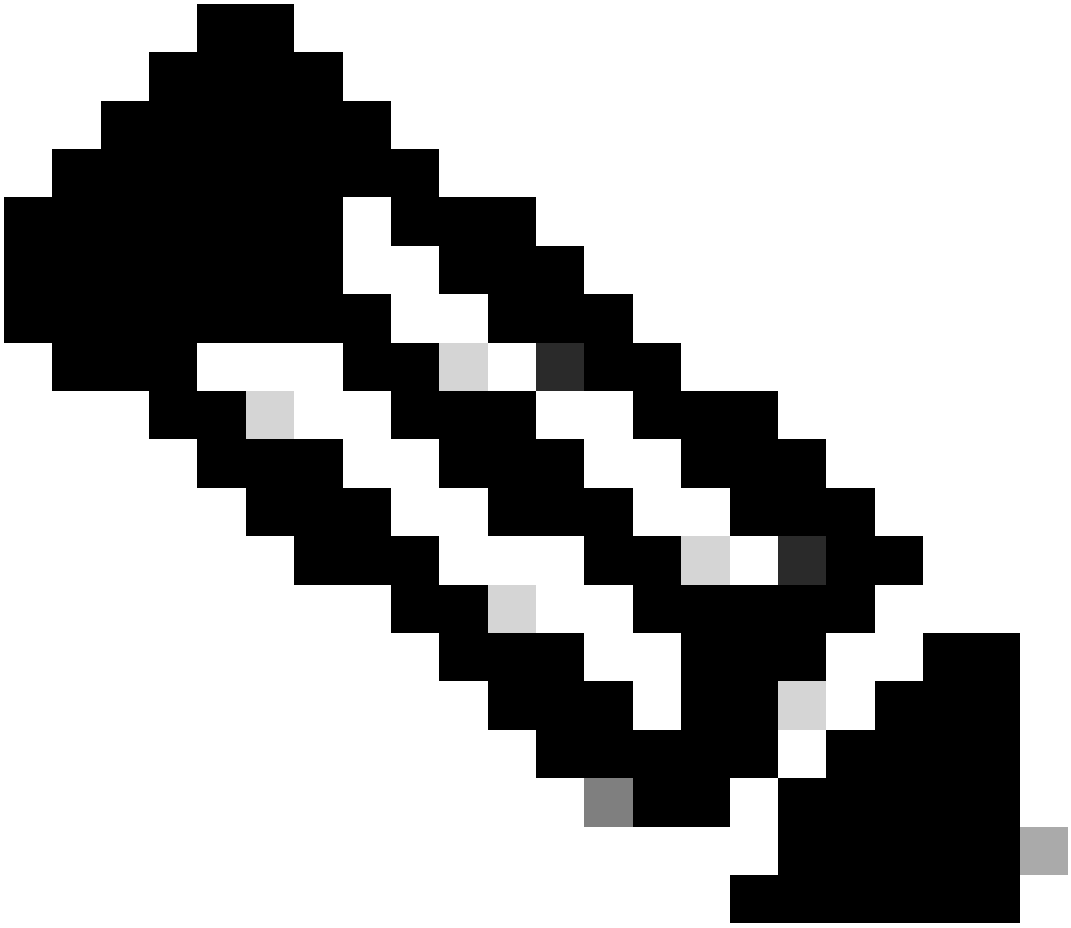
このタイプの応答は、接続が良好であること、およびクラウドポータルがセンサーを認識していることを示します。

<#root>

user@example-ona:~#

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

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



注:curlコマンドは、次の適切な地域を使用するように変更できます。米国：https://sensor.ext.obsrvbl.comヨーロッパ：https://sensor.eu-prod.obsrvbl.comオーストラリア：https://sensor.anz-prod.obsrvbl.com

---

このタイプの応答は、良好な接続を示していますが、センサーが特定のドメインに関連付けられていません。

```
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の問題

センサーがDNSでホスト名を解決できない場合は、cat /etc/netplan/01-netcfg.yamlコマンドでDNS設定を確認します。

dns設定を変更する必要がある場合は、「DNS設定の更新」セクションを参照してください。

DNS設定を検証したら、sudo systemctl restart systemd-resolved.serviceコマンドを実行します。

このコマンドでは、何も出力されないはずです。

<#root>

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

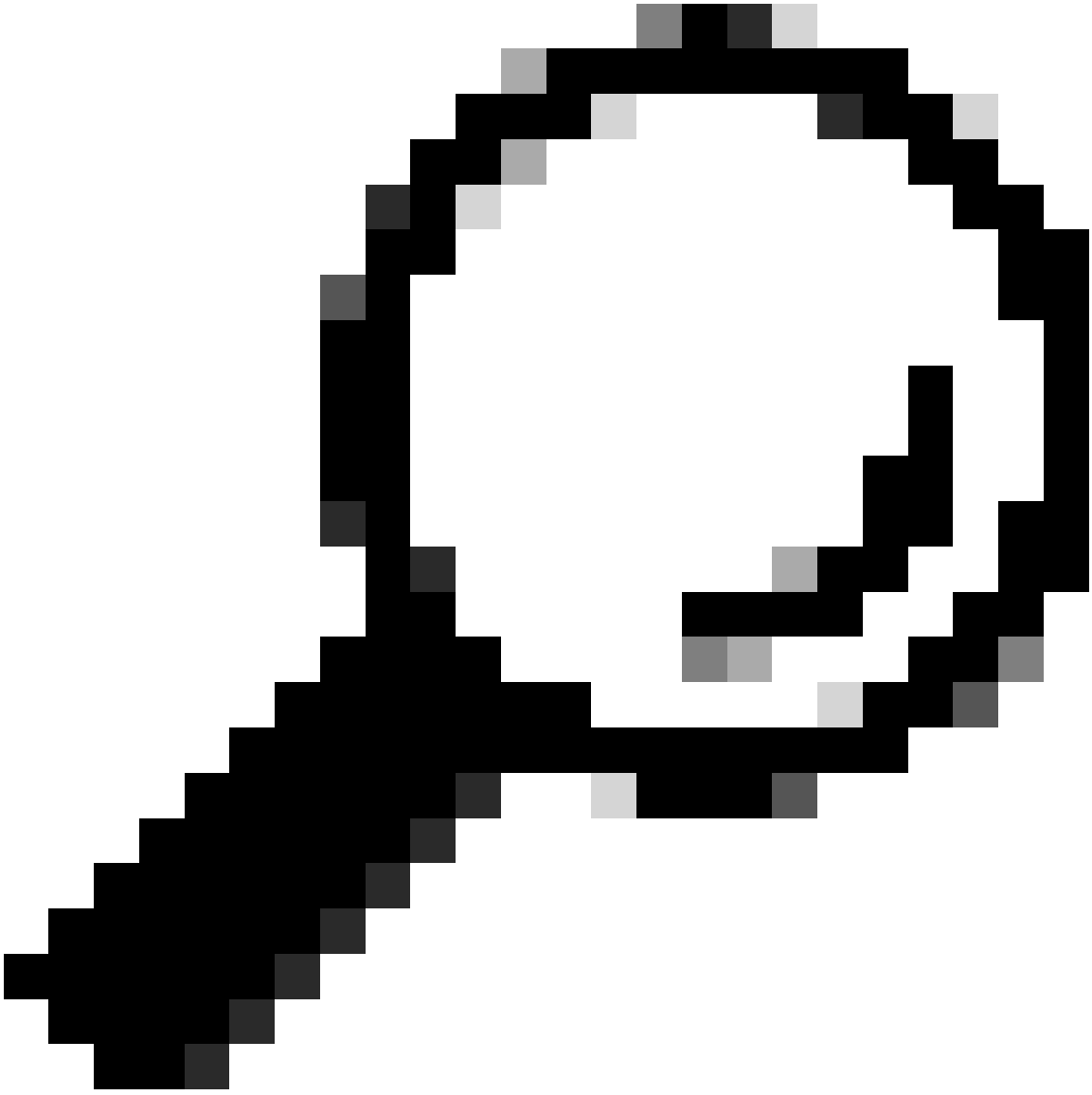
sudo systemctl restart systemd-resolved.service

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

DNS設定の更新

NetplanのDNSサーバを更新するには、ネットワークインターフェイスのNetplan設定ファイルを変更します。

Netplanの設定ファイルは、**/etc/netplan**ディレクトリに保存されます。



ヒント：このディレクトリには1つまたは2つのYAMLファイルがあります。必要なファイル名は01-netcfg.yamlまたは50-cloud-init.yaml、あるいはその両方です。

```
sudo vi /etc/netplan/01-netcfg.yaml
```

コマンドを使用してNetplanコンフィギュレーションファイルを開きます。

Netplan設定ファイルで、ネットワークインターフェイスの下にある「nameservers」キーを探します。

複数のDNSサーバIPアドレスをカンマで区切って指定できます。

sudo netplan apply

コマンドを使用して、Netplan設定に変更を適用します。

Netplanは、systemdが解決したサービスのコンフィギュレーションファイルを生成します。

新しいDNSリゾルバが設定されていることを確認するには、resolvectl status | grep -A2 'DNS Servers'コマンドを実行します。

<#root>

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

resolvectl status | grep -A2 'DNS Servers'

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

user@example-ona:~#
```

ローカルファイルシステムがいっぱいです

センサーのコンソールに、「Failed to create new system journal: No space left on device」という一般的なエラーメッセージが表示される場合があります。

これは、ディスクがいっぱいであり、 / ルートファイルシステムに空き領域がないことを示します。

df -ah /

コマンドを実行して、使用可能なスペースの量を確認します。

journalctl --vacuum-time 1d

<#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:~#

コマンドを使用して、古いジャーナルログをクリアし、ディスク領域を解放します。

<#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:~#

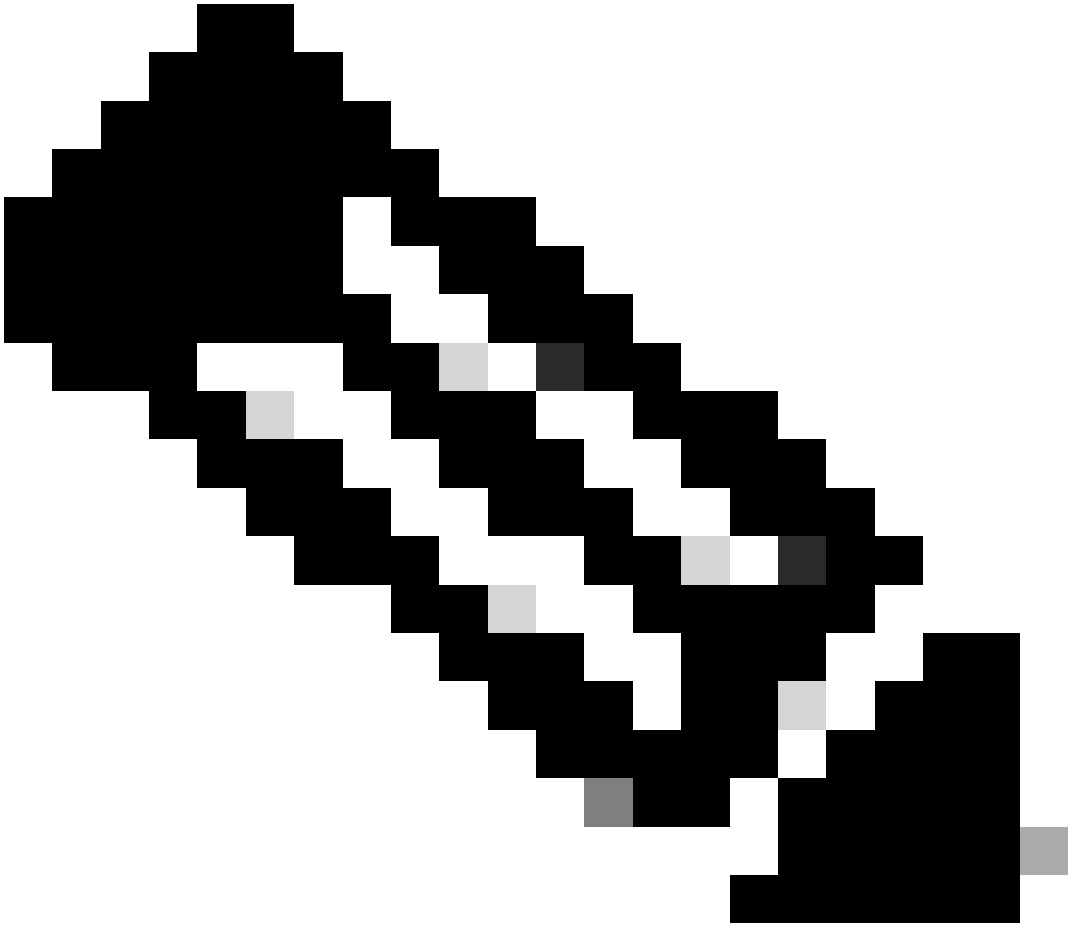
ストレージスペースが、『初期導入ガイド』に記載されている最小システム要件を満たしていることを確認します。

このガイドは、Cisco Secure Cloud Analytics(Stealthwatch Cloud)製品サポートページ (https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/series.html)から入手できます。

モニタリング設定

クラウドへのネットワーク接続が良好で、有効なDNS設定を持つセンサーは、引き続きオフライン状態を示す可能性があります。

センサーの監視オプションが無効になっているか、センサーがハートビートを送信しない場合は、オフラインステータスになる可能性があります。



注：このセクションは、カスタマイズされていないONAセンサーのデフォルトインストール用で、netflowやIPFIXのデータをアクティブに受信します。

```
grep PNA_SERVICE /opt/obsrvbl-ona/config
```

コマンドを実行してステータスを確認します。

```
<#root>
```

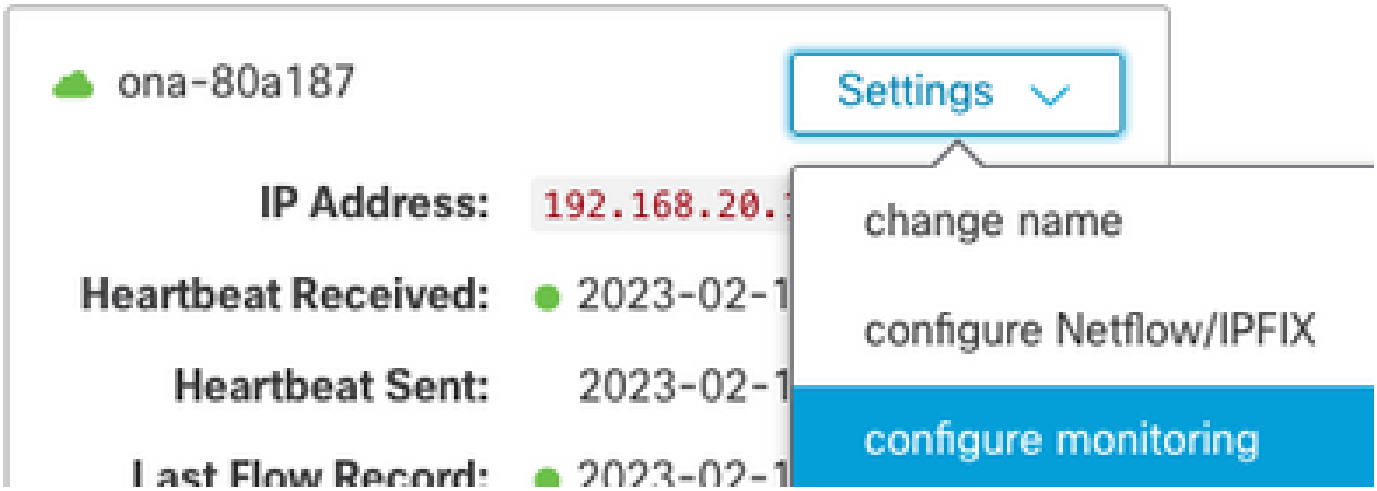
```
user@example-ona:~#
```

```
grep PNA_SERVICE /opt/obsrvbl-ona/config
```

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

このサービスがfalseに設定されている場合は、使用しているセンサーに対する Settings > configure monitoring の目的のネットワークがSCAポータルにリストされていることを確認します。

ps -fu obsrvbl_ona | grep pna



コマンドを実行し、サービスが表示されるかどうか、およびモニタ対象の予期されるネットワーク範囲がリストされているかどうかを確認します。

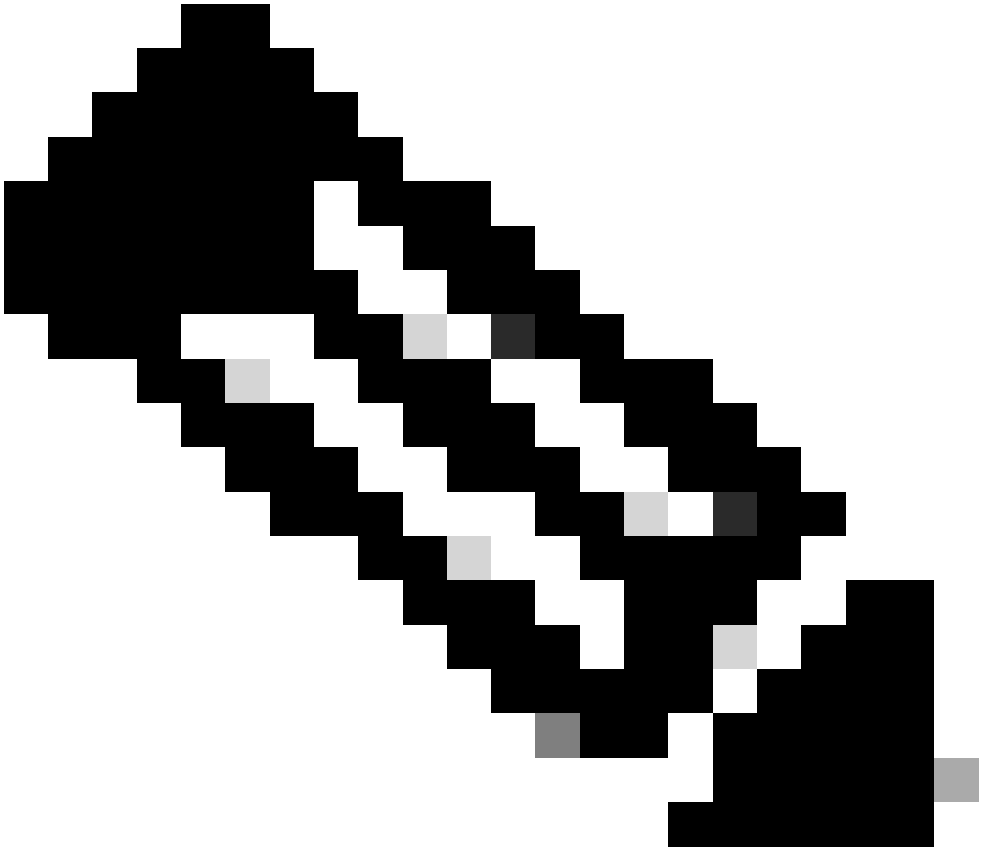
<#root>

```
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:~#
```

コマンドの出力に、PNAサービスのプロセスIDが956と957で、プライベートアドレス範囲が10.0.0.0/8、172.16.0.0/12、および192.168.0.0/16がens192とens224インターフェイスでモニタされていることが示されます。



注：アドレス範囲とインターフェイス名は、センサーの設定と導入によって異なる場合があります

SSLエラー

less /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log

コマンドで/opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.logファイルを調べ、SSLエラーがないか確認します。

エラーの例を示します。

wget https://s3.amazonaws.com

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

コマンドを実行し、出力を確認して、HTTPSインスペクションが行われているかどうかを確認します。

HTTPSインスペクションが行われる場合は、すべてのインスペクションからセンサーが削除されているか、許可リストにセンサーが配置されていることを確認します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。