ONA 센서 오프라인 상태 문제 해결

목차

소개

이 문서에서는 SCA(Secure Cloud Analytics) 센서가 오프라인으로 표시되는 여러 가지 가능한 원인을 조사하는 방법에 대해 설명합니다.

배경 정보

SCA(Secure Cloud Analytics)는 이전에 SWC(Stealthwatch Cloud)로 불리었으며 이러한 용어는 혼용할 수 있습니다.

SCA 센서는 사설 네트워크 모니터이며 ONA, ONA 센서 또는 단순히 센서로 참조될 수 있습니다.

이 문서의 명령은 ona-20.04.1-server-amd64.iso 데비안 설치를 기반으로 합니다.

오프라인 센서의 가능한 원인

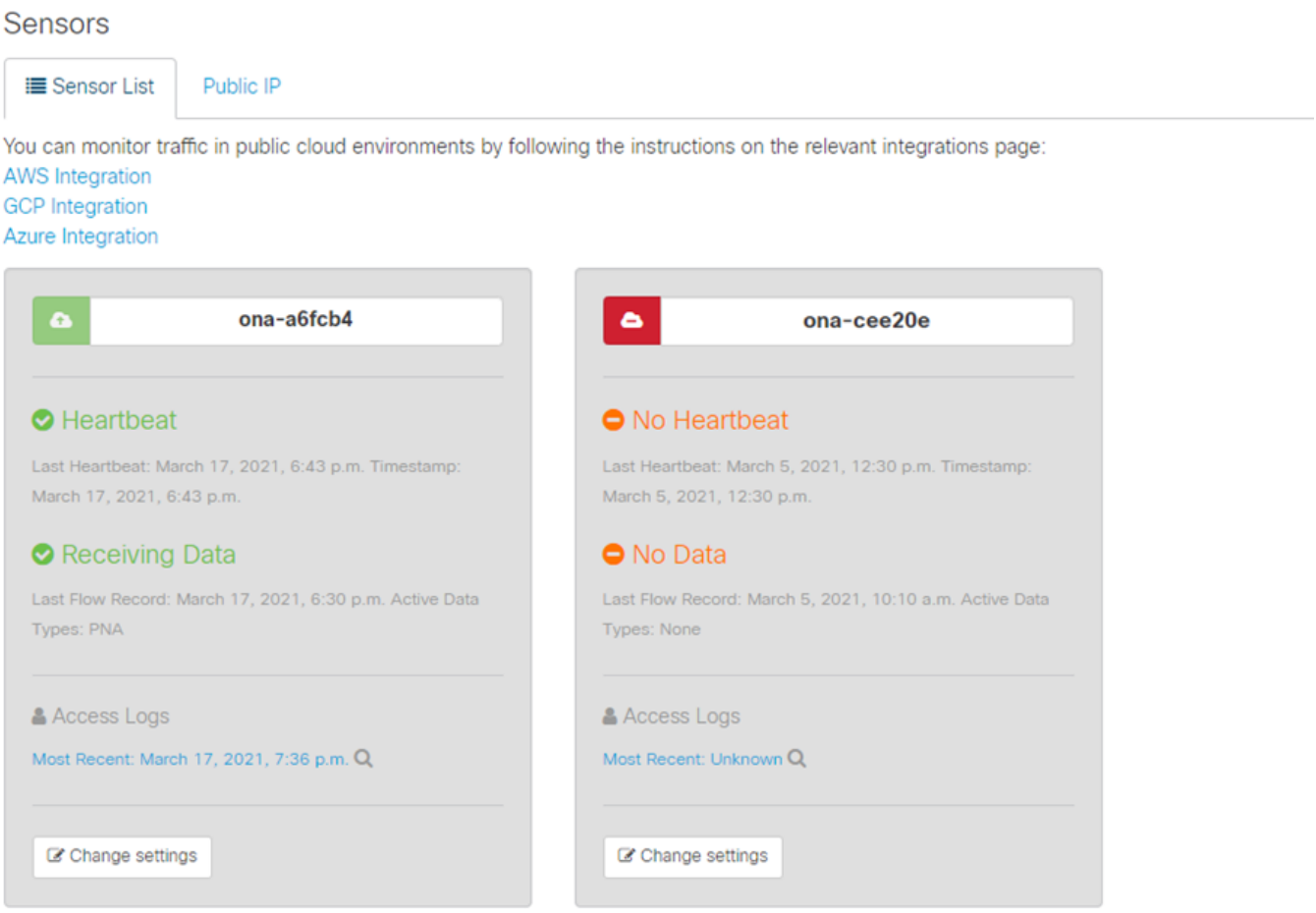
센서가 오프라인 상태를 제시하게 할 수 있는 많은 가능한 요소들이 있다.

이러한 요인의 두 가지 예는 네트워크 관련 문제이며 로컬 파일 시스템에 전체 디스크가 있습니다.

오프라인 센서 식별

SCA 포털에는 구성된 센서 목록이 포함되어 있습니다. 이 페이지에 액세스하려면 Settings > Sensors.

이 이미지의 오프라인 센서는 빨간색으로 표시되며 최근 하트비트 및 데이터를 표시하지 않습니다.



오프라인 센서 조사

네트워크 문제

ONA 호스트에서 인터넷에 액세스할 수 없게 되면 센서가 오프라인으로 나열됩니다.

ONA 호스트가 8.8.8.8에서 Google DNS 서버 중 하나와 같은 알려진 활성 IP 주소를 ping할 수 있는지 테스트합니다.

ONA 센서에 로그인하고 **ping -c4 8.8.8.8 명령을** 실행합니다.

<#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:~#
```

센서가 알려진 활성 IP 주소를 ping할 수 없는 경우 자세히 알아보십시오.

명령을 사용하여 기본 게이트웨이를 route -n 결정합니다.

명령을 통해 기본 게이트웨이에 대해 유효한 ARP(Address Resolution Protocol) 항목이 표시되는지 **arp -an** 확인합니다.

센서가 알려진 IP 주소를 ping할 수 있는 경우 DNS 호스트 이름 확인 및 클라우드에 연결하기 위한 센서 기능을 테스트합니다.

센서에 로그인하고 명령을 sudo curl https://sensor.ext.obsrvbl.com 실행합니다.

curl 명령 출력에서는 sensor.ext.obsrvbl.com에 대한 DNS 확인이 실패했으며 DNS에 대한 조사가 보장됨을 보여 줍니다.

<#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:~#
```

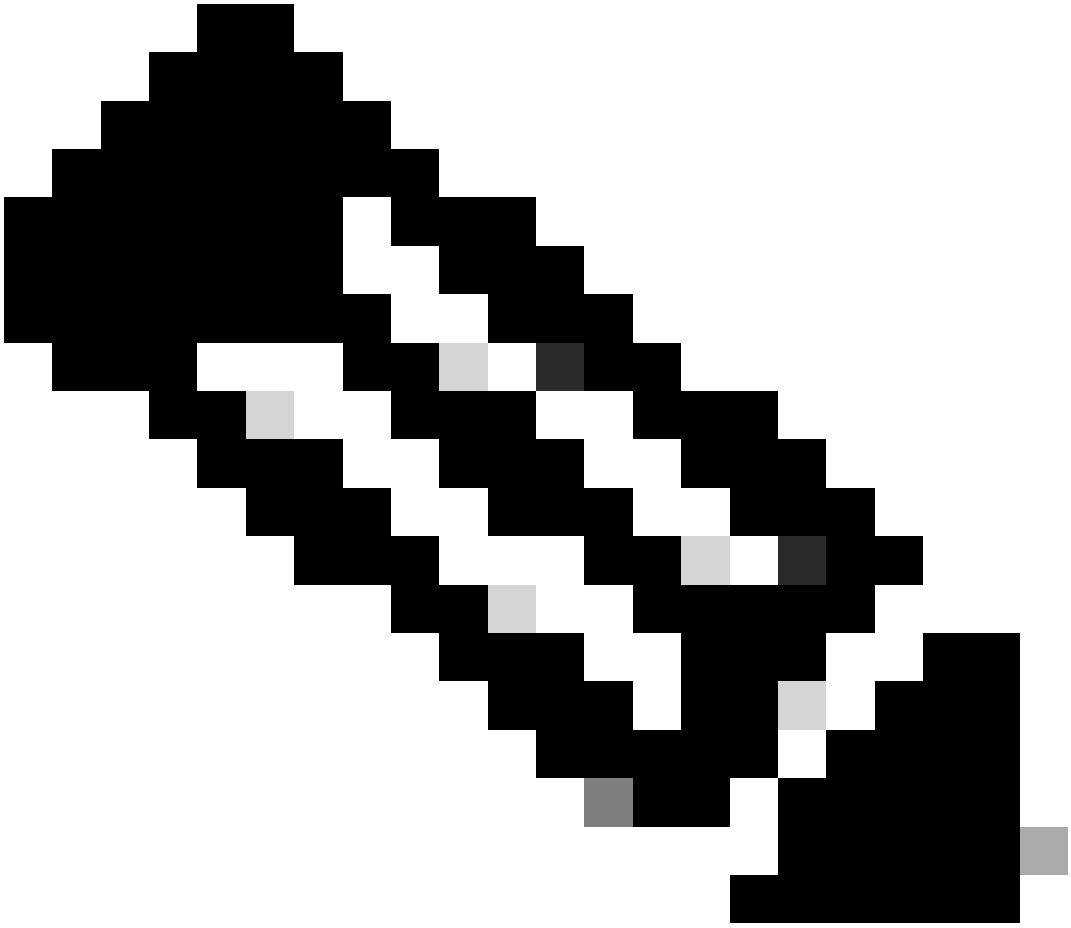
이 응답 유형은 연결이 양호하며 클라우드 포털에서 센서를 인식한다는 것을 나타냅니다.

<#root>

user@example-ona:~#

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

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



참고: curl 명령은 해당 지역(미국: https://sensor.ext.obsrvbl.com 유럽: https://sensor.eu-prod.obsrvbl.com 호주: https://sensor.anz-prod.obsrvbl.com)을 사용하도록 수정할 수 있습니다.

이 응답 유형은 연결이 양호하지만 센서가 특정 도메인과 연결되지 않았음을 나타냅니다.

```
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 문제

센서가 DNS로 호스트 이름을 확인할 수 없는 경우 명령을 사용하여 DNS 설정을 cat /etc/netplan/01-netcfg.yaml 확인합니다.

dns 설정을 변경해야 하는 경우 Update the DNS Configuration 섹션을 참조하십시오.

DNS 설정이 확인되면 명령을 sudo systemctl restart systemd-resolved.service 실행합니다.

이 명령에는 출력이 필요하지 않습니다.

<#root>

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

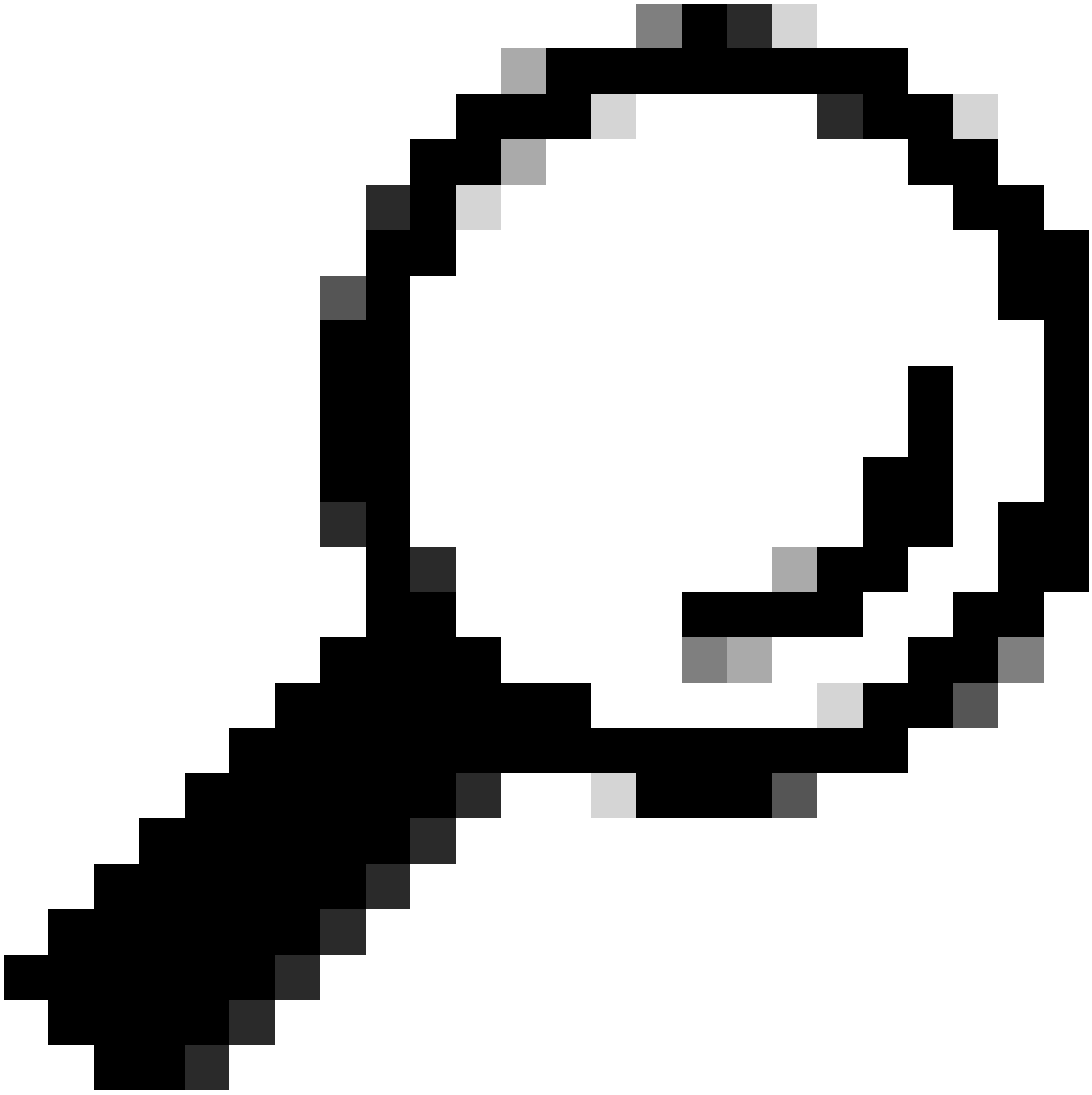
sudo systemctl restart systemd-resolved.service

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

DNS 컨피그레이션 업데이트

Netplan에서 DNS 서버를 업데이트하려면 네트워크 인터페이스에 대한 Netplan 컨피그레이션 파일을 수정할 수 있습니다.

Netplan 컨피그레이션 파일은 **/etc/netplan 디렉토리에** 저장됩니다.



팁: 이 디렉토리에서 YAML 파일을 한두 개 찾을 수 있습니다. 필요한 파일 이름은 01-netcfg.yaml 및/또는 50-cloud-init.yaml 입니다.

명령을 사용하여 Netplan 컨피그레이션 파일을 sudo vi /etc/netplan/01-netcfg.yaml 엽니다.

Netplan 컨피그레이션 파일의 네트워크 인터페이스 아래에서 "nameservers" 키를 찾습니다.

쉼표로 구분하여 여러 DNS 서버 IP 주소를 지정할 수 있습니다.

명령을 사용하여 Netplan 컨피그레이션에 변경 사항을 **sudo netplan apply** 적용합니다.

Netplan은 시스템에서 해결된 서비스에 대한 컨피그레이션 파일을 생성합니다.

새 DNS 확인기가 설정되었는지 확인하려면 명령을 resolvectl status | grep -A2 'DNS Servers' 실행합니다.

<#root>

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

resolvectl status | grep -A2 'DNS Servers'

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

user@example-ona:~#
```

로컬 파일 시스템 가득 참

센서의 콘솔에 "새 시스템 저널을 만들지 못했습니다. 장치에 공간이 없습니다."라는 일반적인 오류 메시지가 나타날 수 있습니다.

이는 디스크가 꽉 찼으며 / 루트 파일 시스템에 더 이상 공간이 없음을 나타냅니다.

명령을 df -ah / 실행하고 사용 가능한 공간을 확인합니다.

<#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:~#
```

이전 저널 로그를 지워 이 명령으로 디스크 공간을 journalctl --vacuum-time 1d 확보합니다.

<#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:~#
```

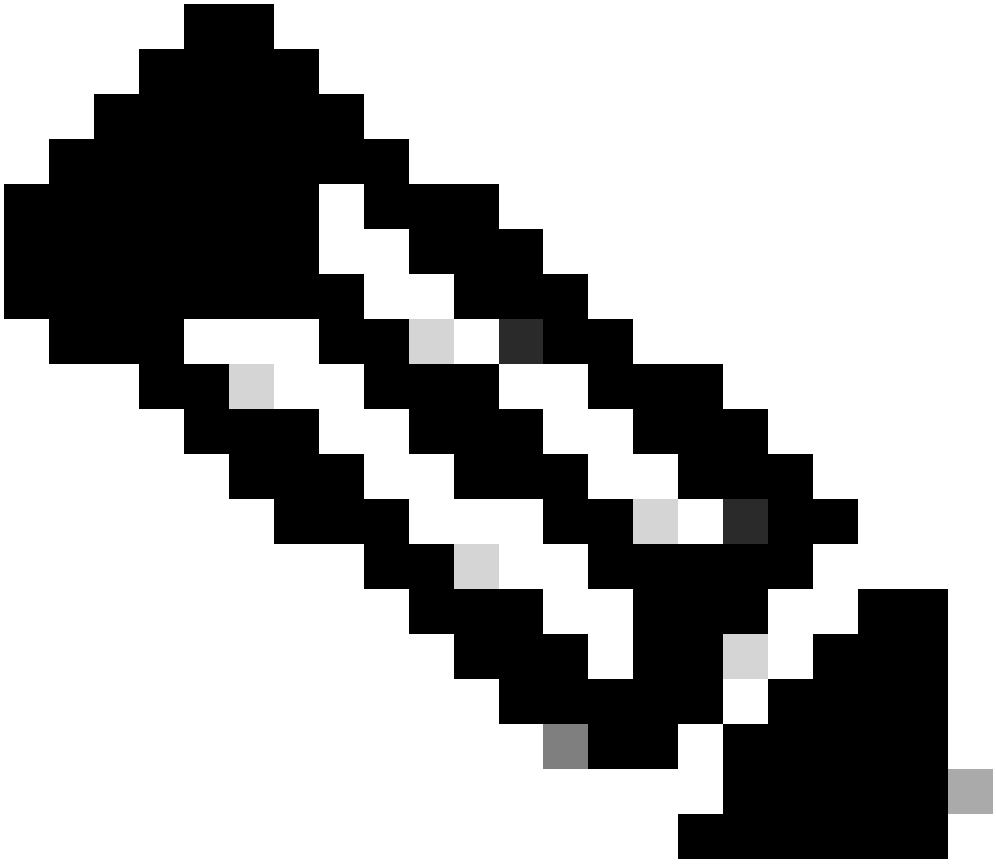
스토리지 공간이 초기 구축 가이드에 요약된 최소 시스템 요구 사항을 충족하는지 확인합니다.

이 가이드는 Cisco Secure Cloud Analytics(Stealthwatch Cloud) 제품 지원 페이지 (https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/series.html)에서 검색할 수 있습니다.

컨피그레이션 모니터링

클라우드에 대한 네트워크 연결이 양호하고 유효한 DNS 설정이 있는 센서는 여전히 오프라인 상태를 나타낼 수 있습니다.

Sensor 모니터링 옵션이 비활성화되었거나 Sensor에서 하트비트를 전송하지 않으면 오프라인 상태가 가능합니다.



참고: 이 섹션은 사용자 지정 없이 ONA 센서를 기본 설치하고 netflow 및/또는 IPFIX 데이터를 능동적으로 수신하기 위한 것입니다.

상태를 grep PNA_SERVICE /opt/obsrvbl-ona/config 확인하려면 명령을 실행합니다.

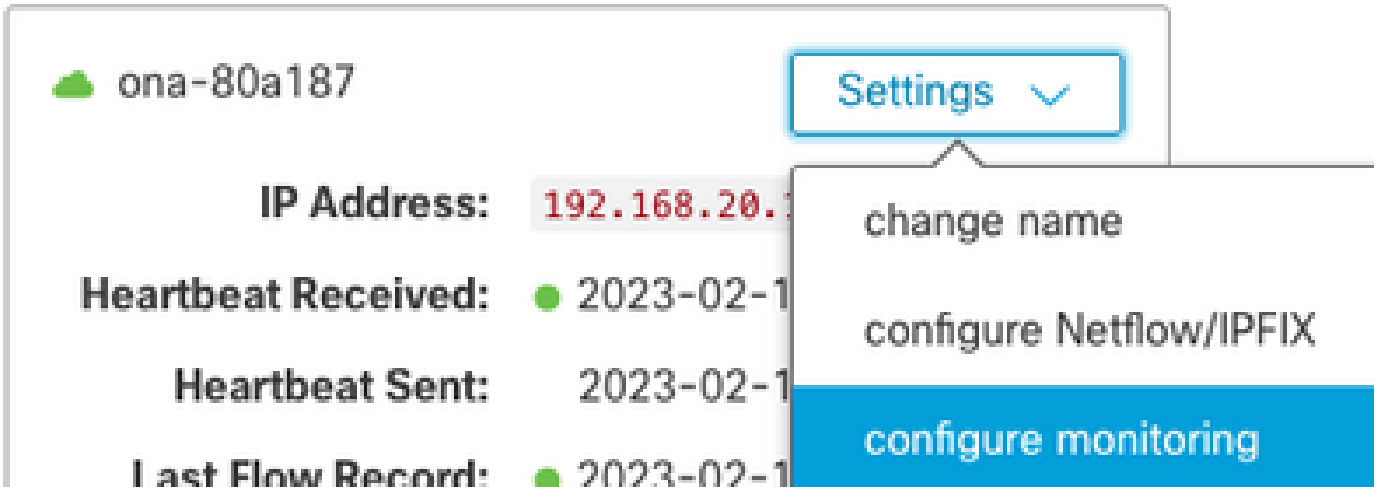
<#root>

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

grep PNA_SERVICE /opt/obsrvbl-ona/config

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

서비스가 false로 설정된 경우 원하는 네트워크가 SCA 포털의 센서 Settings > configure monitoring 에 대해 나열되어 있는지 확인합니다.



서비스가 ps -fu obsrvbl_ona | grep pna 표시되고 예상되는 모니터링되는 네트워크 범위가 나열되면 명령과 메모를 실행합니다.

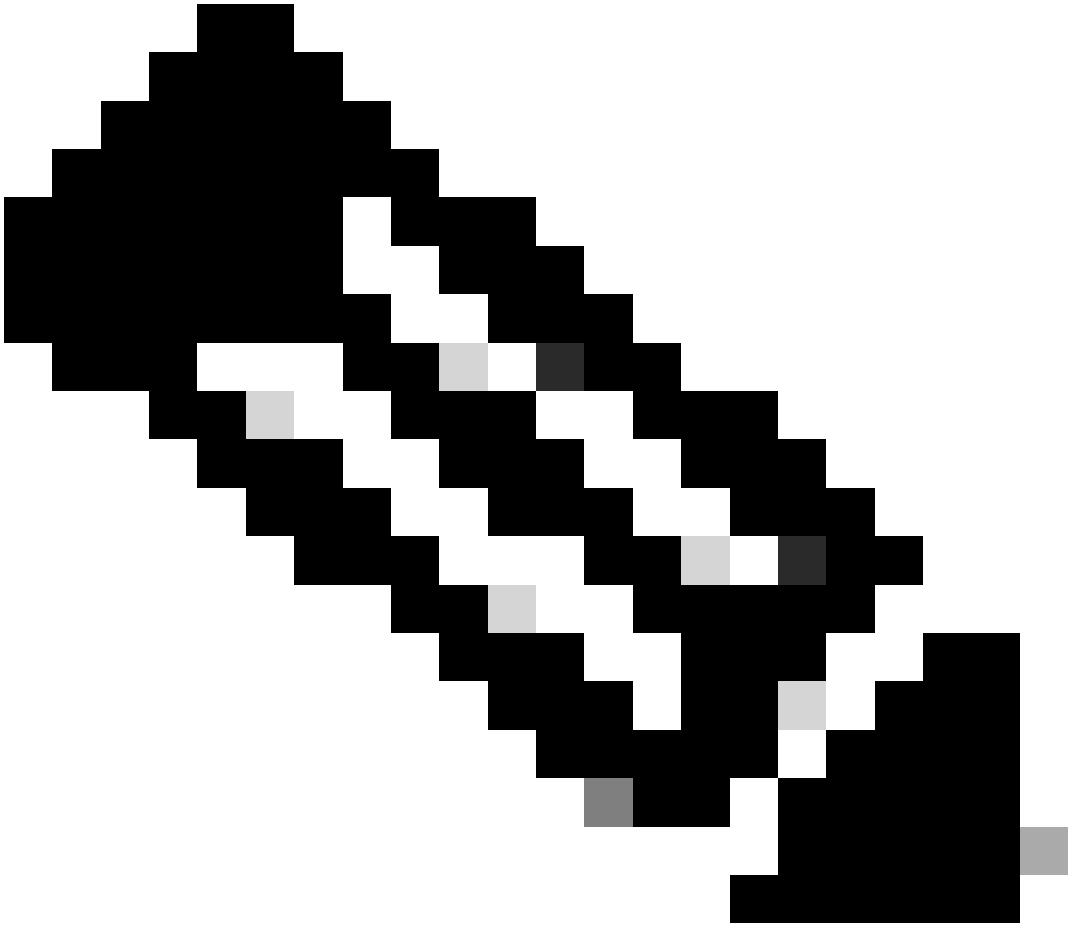
<#root>

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:~#

명령의 출력에서는 PNA 서비스에 프로세스 ID가 956 및 957이며, 개인 주소 범위 10.0.0.0/8, 172.16.0.0/12 및 192.168.0.0/16이 ens192 및 ens224 인터페이스에서 모니터링됨을 보여 줍니다.



참고: 주소 범위 및 인터페이스 이름은 센서의 컨피그레이션 및 구축에 따라 다를 수 있습니다

SSL 오류

이 명령을 사용하여 /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log 파일에서 SSL 오류를 less /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log 검토합니다.

예제 오류가 제공됩니다.

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

명령을 wget https://s3.amazonaws.com 실행하고 출력을 검토하여 가능한 HTTPS 검사가 있는지 확인합니다.

HTTPS 검사가 있는 경우 센서가 검사에서 제거되거나 허용된 목록에 있는지 확인합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.