أستكشاف أخطاء مستشعر ONA غير المتصل وإصلاحها

المحتويات

المقدمة

يوضح هذا المستند كيفية التحقيق في الأسباب المتعددة المحتملة لظهور مستشعر تحليلات سحابة آمنة (SCA) دون اتصال.

معلومات أساسية

كانت Secure Cloud Analytics (SCA) تسمى سابقا Stealthwatch Cloud (SWC) ويمكن إستخدام هذه المصطلحات بشكل متبادل.

مستشعر SCA هو شاشة الشبكة الخاصة ويمكن الإشارة إليه كمستشعر ONA أو ONA أو ببساطة كمستشعر.

تستند الأوامر الواردة في هذه المقالة إلى تثبيت ONA-20.04.1-server-AMD64.iso debian.

الأسباب المحتملة لأجهزة الاستشعار غير المتصلة

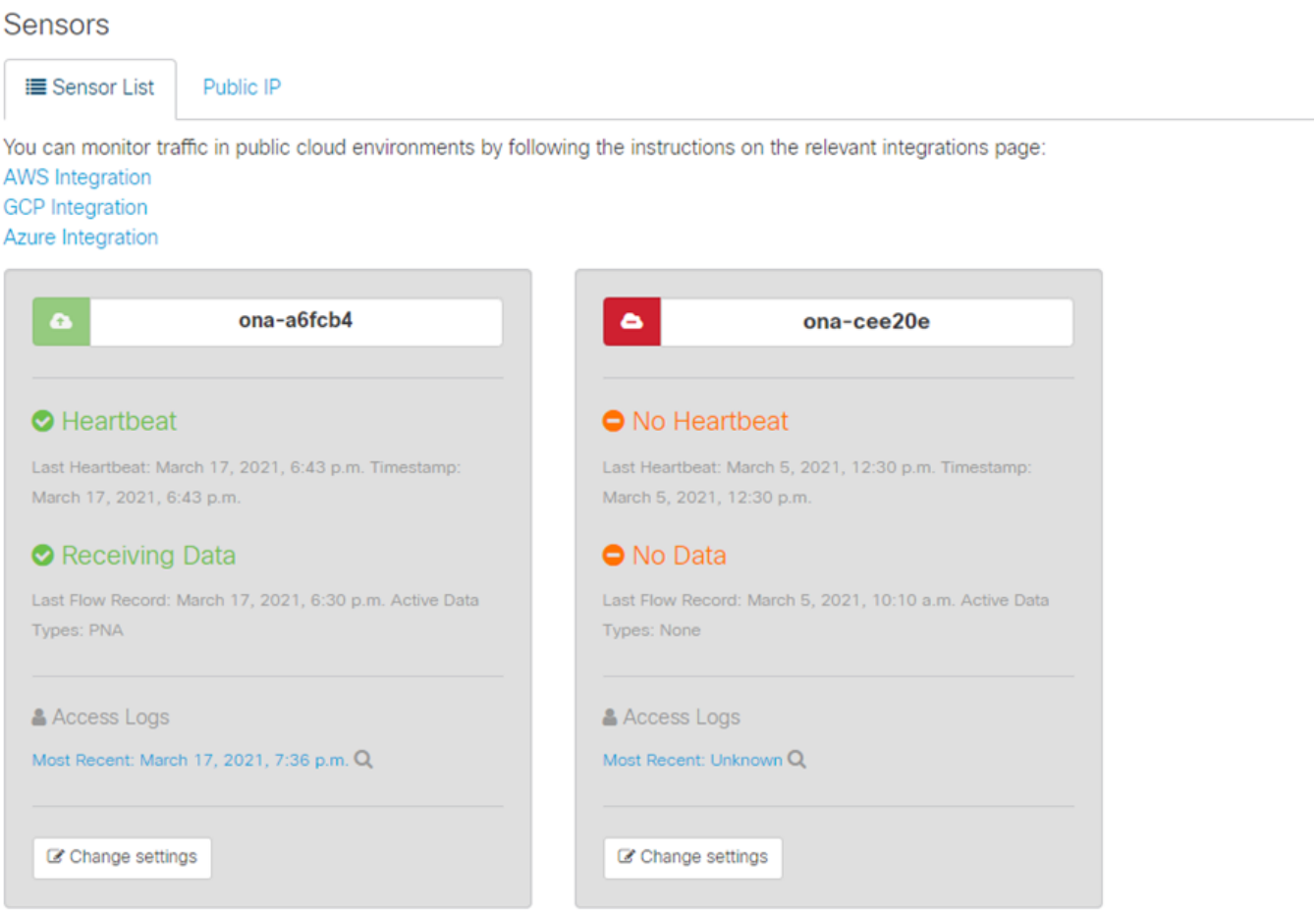
هناك العديد من العوامل المحتملة التي يمكن أن تؤدي إلى قيام المستشعر بتقديم حالة عدم الاتصال.

من بين الأمثلة على هذه العوامل المشاكل المتعلقة بالشبكة، ويحتوي نظام الملفات المحلي على قرص كامل.

التعرف على مستشعر دون اتصال

تحتوي بوابة SCA على قائمة بأجهزة الاستشعار التي تم تكوينها. للوصول إلى هذه الصفحة انتقل إلى Settings > Sensors.

المستشعر غير المتصل في هذه الصورة تم تمثيله باألحمر والى يعرض بيانات ونبضات قلبية حديثة.



التحقيق في مستشعر دون اتصال

مشاكل الشبكة

يمكن أن يفقد مضيف ONA الوصول إلى الإنترنت، مما يؤدي إلى إزاحة المستشعر في قائمة غير متصل.

قم بإجراء اختبار ما إذا كان مضيف ONA قادرا على اختبار اتصال عنوان IP معروف بشكل حي مثل أحد خوادم Google DNS على 8.8.8.8.

قم بتسجيل الدخول إلى مستشعر ONA وقم بتشغيل الأمر **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:~#
```

إذا لم يتمكن المستشعر من إختبار اتصال عنوان IP معروف على قيد الحياة، فتحقق بعد ذلك.

حدد البوابة الافتراضية باستخدام route -n الأمر.

حدد ما إذا كان هناك إدخال صالح لبروتوكول تحليل العنوان (ARP) تمت مشاهدته للعبارة الافتراضية باستخدام **arp -an** الأمر.

إذا كان المستشعر قادرا على إختبار اتصال عنوان IP معروف، اختبر دقة اسم مضيف DNS وقدرة المستشعر على الاتصال بالسحابة.

قم بتسجيل الدخول إلى المستشعر، ثم قم بتشغيل sudo curl https://sensor.ext.obsrvbl.com الأمر.

يظهر إخراج الأمر curl أن تحليل DNS ل sensor.ext.obsrvbl.com فشل والتحقيق في DNS له ما يبرره.

<#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:~#
```

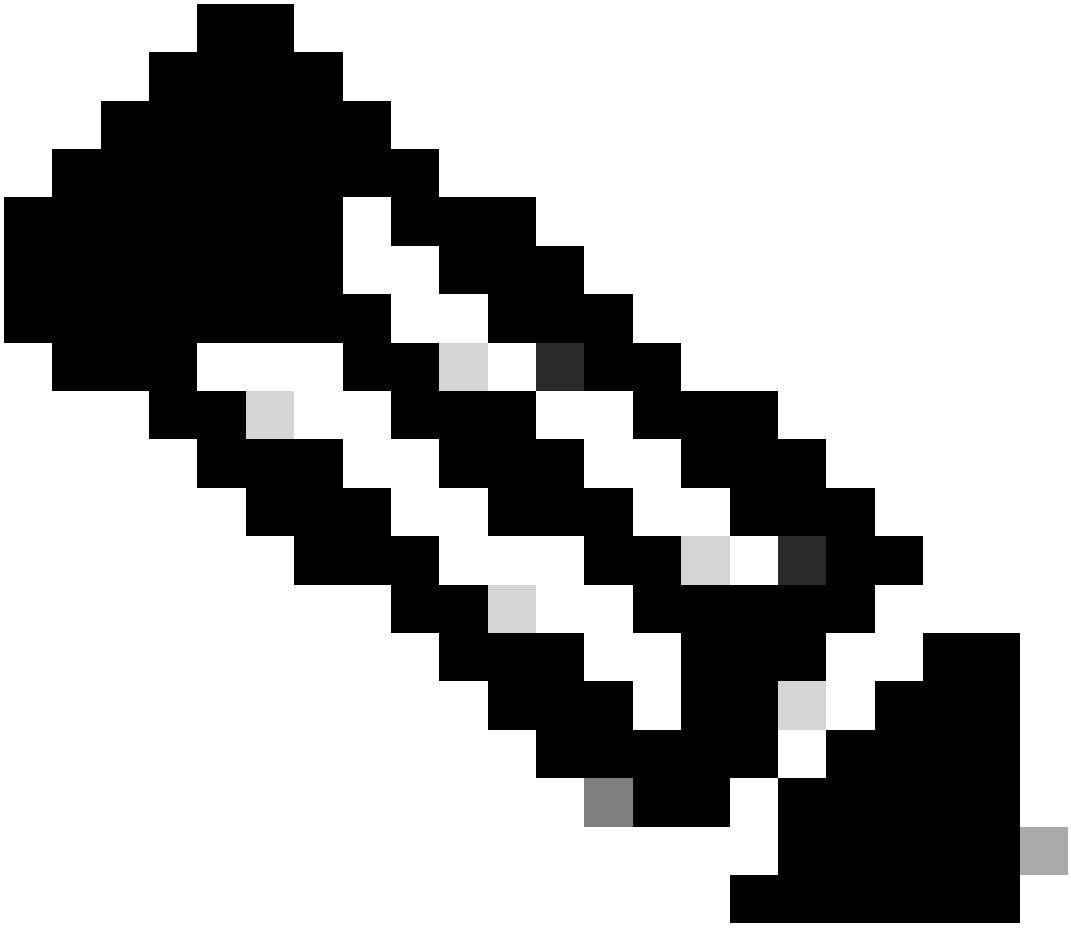
يشير هذا النوع من الاستجابة إلى وجود اتصال جيد وكذلك إلى أن بوابة السحابة تتعرف على المستشعر.

<**#root**>

user@example-ona:~#

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

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



ملاحظة: يمكن تعديل الأمر curl لاستخدام المنطقة المناسبة في الولايات المتحدة: https://sensor.ext.obsrvbl.com أوروبا: https://sensor.eu-prod.obsrvbl.com أستراليا: https://sensor.anz-prod.obsrvbl.com

يشير هذا النوع من الاستجابة إلى وجود اتصال جيد ولكن المستشعر لم يتم ربطه بمجال معين.

```
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:~#
```

مشاكل DNS

إذا لم يكن المستشعر قادرا على حل أسماء المضيف باستخدام DNS، فتحقق من إعدادات DNS باستخدام cat /etc/netplan/01-netcfg.yaml الأمر.

إذا كانت إعدادات DNS تتطلب تغييرات ارجع إلى قسم تحديث تكوين DNS.

بمجرد التحقق من صحة إعدادات DNS، قم بتشغيل sudo systemctl restart systemd-resolved.service الأمر.

الذي يتوقع إخراج مع هذا الأمر.

<#root>

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

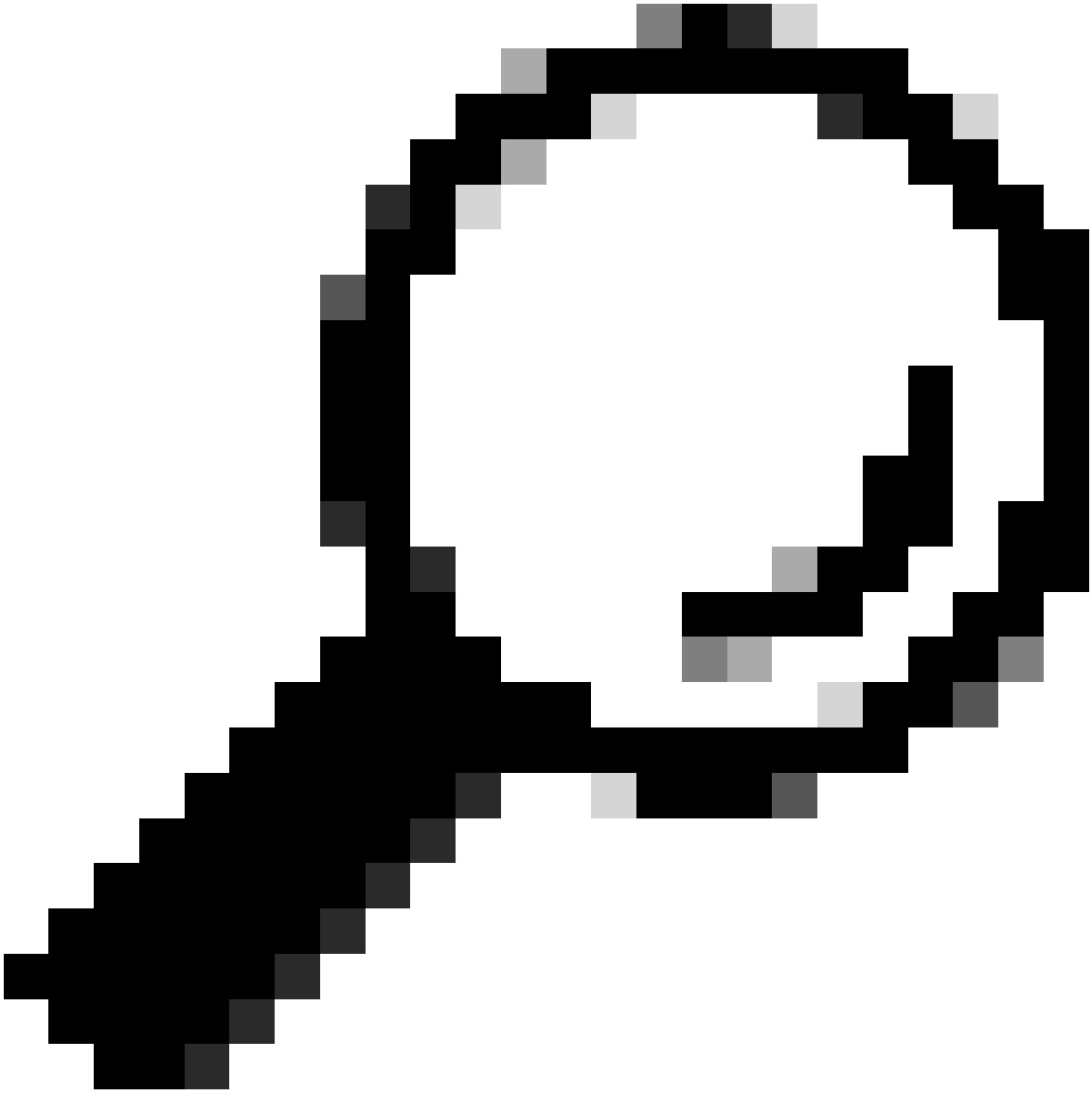
sudo systemctl restart systemd-resolved.service

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

تحديث تكوين DNS

لتحديث خوادم DNS في Netplan، يمكنك تعديل ملف تكوين Netplan لواجهة الشبكة.

يتم تخزين ملفات تكوين NetPlan في دليل **/etc/netplan**.



تلميح: يمكن العثور على ملف YAML واحد أو ملفين في هذا الدليل. أسماء الملفات المتوقعة هي 01-netcfg.yaml و/أو 50-cloud-init.yaml.

افتح ملف تكوين NetPlan باستخدام sudo vi /etc/netplan/01-netcfg.yaml الأمر.

في ملف تكوين NetPlan، حدد موقع المفاتيح "nameservers" أسفل واجهة الشبكة.

يمكنك تحديد عناوين IP متعددة لخادم DNS مفصولة بفاصلة.

تطبيق التغييرات على تكوين NetPlan باستخدام **sudo netplan apply** الأمر.

تقوم NetPlan بإنشاء ملفات التكوين للخدمة التي تم حلها بواسطة النظام.

للتحقق من تعيين تحليلات DNS الجديدة، قم بتشغيل resolvectl status | grep -A2 'DNS Servers' الأمر.

<#root>

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

resolvectl status | grep -A2 'DNS Servers'

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

user@example-ona:~#
```

نظام الملفات المحلي ممتلئ

يمكن أن تظهر رسالة خطأ شائعة على وحدة التحكم الخاصة بالمستشعر: "فشل إنشاء دفتر يومية نظام جديد: لم يتم ترك مساحة على الجهاز."

وهذا يشير إلى أن القرص ممتلئ، ولم تعد هناك مساحة في نظام الملفات الجذر.

قم بتشغيل df -ah / الأمر وحدد مقدار المساحة المتوفرة.

<#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:~#

مسح سجلات دفتر اليوميّة القديمة لتحرير مساحة على القرص باستخدام journalctl --vacuum-time 1d الأمر.

<#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:~#

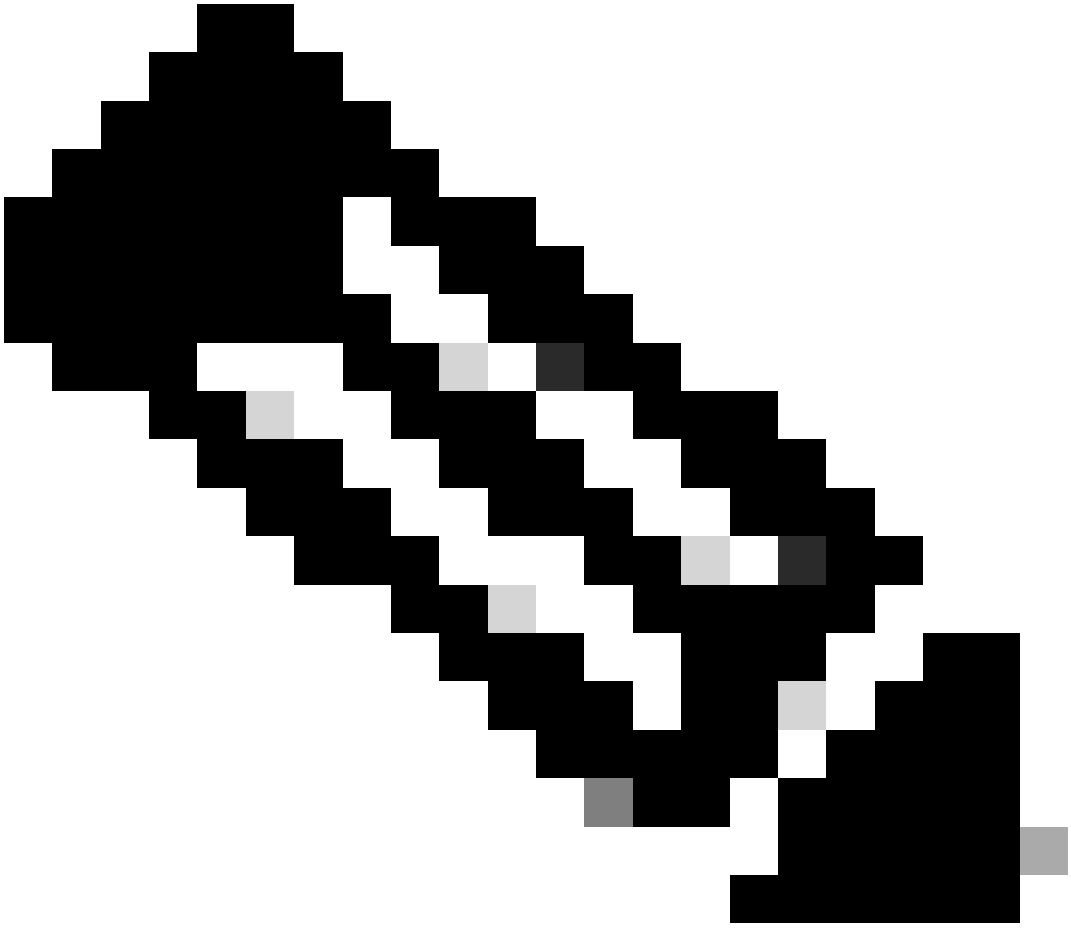
تأكد من أن مساحة التخزين لديك تفي بالحد الأدنى لمتطلبات النظام المحددة في دليل النشر الأولي.

يمكن إستدراد الدليل من صفحة دعم منتجات تحليلات سحابة Cisco الآمنة (سحابة Stealthwatch):
https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/series.html

مراقبة التكوين

ال يزال بإمكان "المستشعر" الذي لديه اتصال شبكة جيد بالسحابة وإعدادات DNS الصحيحة تقديم حالة عدم اتصال.

حالة عدم الاتصال ممكنة إذا كانت خيارات مراقبة المستشعر معطلة أو إذا لم يرسل المستشعر ضربات القلب.



ملاحظة: مخصص هذا القسم للتثبيت الافتراضي لمستشعر ONA بدون تخصيصات ويستلم بنشاط بيانات NetFlow و/أو IPFIX.

قم بتشغيل grep PNA_SERVICE /opt/obsrvbl-ona/config الأمر لتحديد الحالة.

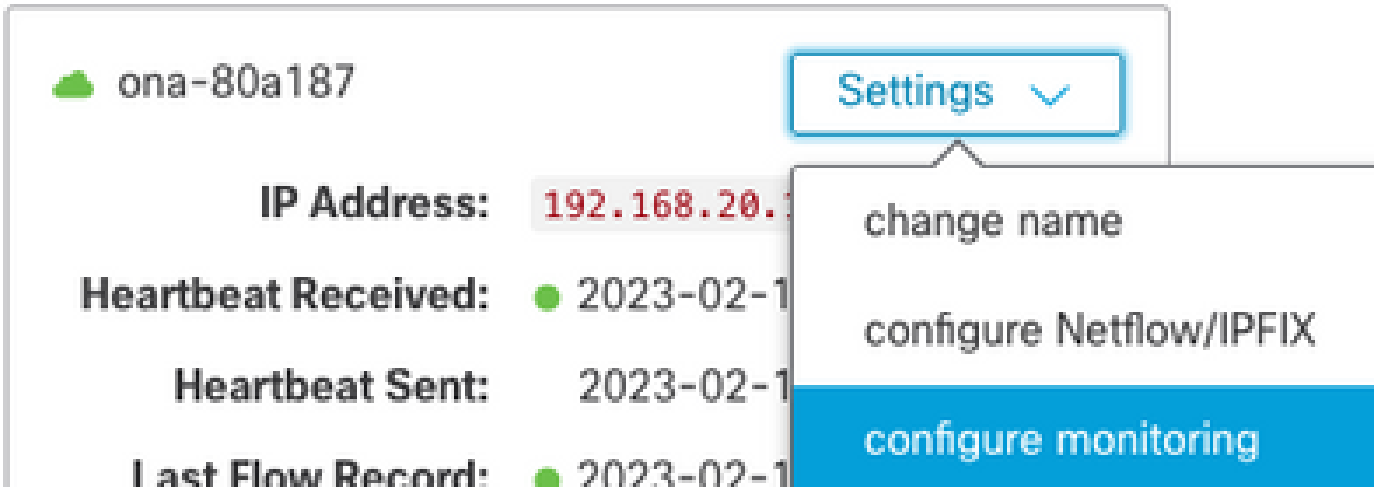
<#root>

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

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

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

إذا تم تعيين الخدمة على خطأ، فتحقق من سرد الشبكات المطلوبة Settings > configure monitoring في "جهاز الاستشعار" في بوابة SCA.



قم بتشغيل ps -fu obsrvbl_ona | grep pna الأمر والملاحظة إذا كانت الخدمة مرئية وإذا كانت نطاقات الشبكة المراقبة المتوقعة مدرجة.

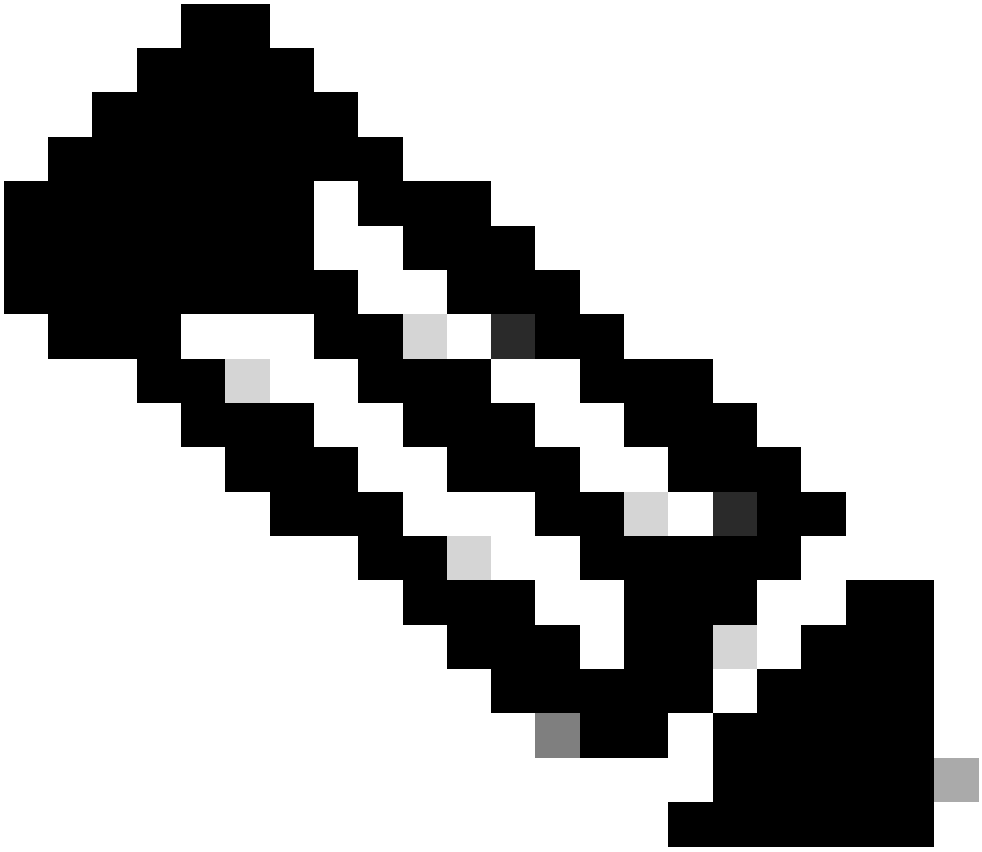
<#root>

```
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:~#
```

يوضح إخراج الأمر أن خدمة PNA بها معرف العملية 956 و957، ويتم مراقبة نطاقات العناوين الخاصة 10.0.0.0/8 و172.16.0.0/12 على الواجهات ENS192 و ENS224.



ملاحظة: يمكن أن تختلف نطاقات العناوين وأسماء الواجهة استنادا إلى تكوين جهاز الاستشعار ونشره.

أخطاء SSL

راجع ملف /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log للتعرف على أخطاء SSL باستخدام less /opt/obsrvbl-ona/logs/ona_service/ona-pna-pusher.log الأرم.

تم توفير مثال للخطأ.

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

قم بتشغيل wget https://s3.amazonaws.com الأرم ومراجعة الإخراج لمعرفة ما إذا كان هناك أي فحص HTTPS محتمل.

في حالة وجود فحص HTTPS، تأكد من إزالة المستشعر من أي فحص أو وضعه في قائمة مسموح بها.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).