Cisco Secure Cloud Analytics

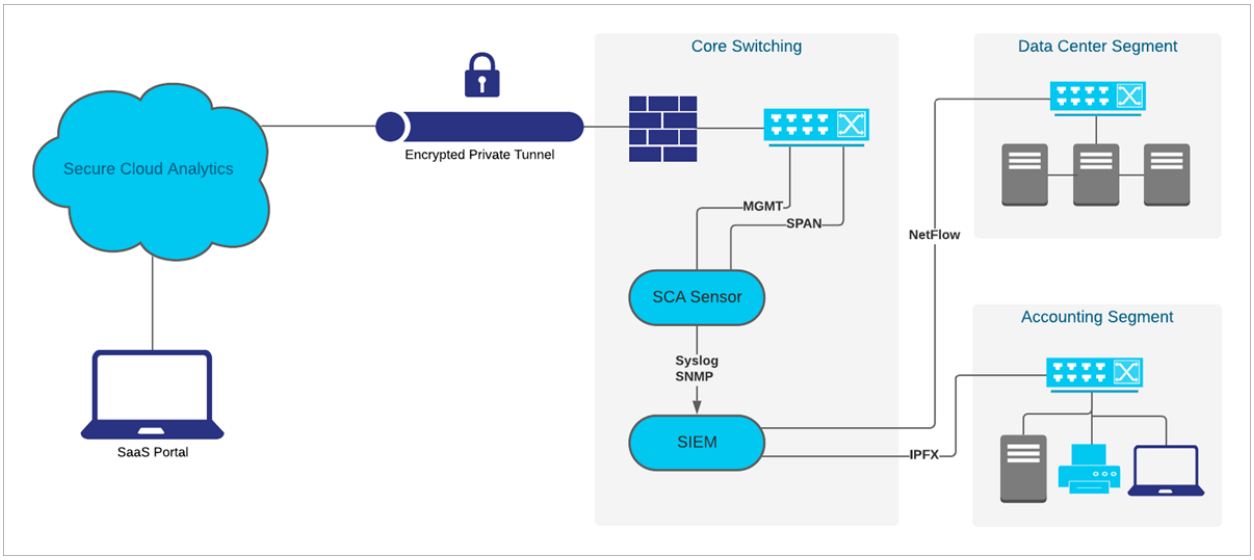
センサー詳細コンフィギュレーション ガイド

目次

プライベート ネットワーク モニター センサーについて

Cisco Secure Cloud Analytics は、オンプレミスおよびクラウドネットワークの可視性と拡張脅威検出を実現します。オンプレミスネットワークの場合、ネットワークフローデータを収集してクラウドに送信するために Cisco Secure プライベートネットワークのモニタリング 仮想アプライアンスが必要です。仮想アプライアンスは、Ubuntu Linux イメージの一部として必要な Secure Cloud Analytics パッケージを含む ISO として使用できます。仮想アプライアンスソフトウェアは Secure Cloud Analytics サービスに含まれており、ユーザーは顧客ポータルから直接センサー ISO をダウンロードできます。この Secure Cloud Analytics リファレンスガイドでは、仮想アプライアンスのインストールおよび設定に関する追加オプションについて説明します。

センサーは NetFlow などのローカル ネットワーク データのテレメトリを収集し、クラウドに安全に送信します。



さまざまなネットワークトポロジが展開されているため、仮想アプライアンスの導入を成功させるには追加設定が必要な場合があります。このガイドでは、インストール ガイドで扱われていない詳細設定とトラブルシューティングについて説明します。

センサーのバージョンの確認

最新のセンサーがネットワーク上に展開されていることを確認するには、コマンドラインから既存のセンサーのバージョンを調べます。

手順

1. 展開されているセンサーへ SSH で接続します。
2. プロンプトで、`cat /opt/obsrvbl-ona/version`と入力して Enter を押します。コンソールに 5.1.1 と表示されない場合、センサーは古くなっています。
   センサーをアップグレードする必要がある場合は、「**付録 D – センサーのアップグレード**」を参照してください。

Linux オペレーティング システム用パッケージの手動インストール

指定の ISO に加えて、次のオペレーティングシステムで仮想アプライアンスを展開することができます。

- Ubuntu Linux バージョン 18.04（32 ビットおよび 64 ビット）
- Ubuntu Linux バージョン 20.04 以降（32 ビットおよび 64 ビット）
- Red Hat Enterprise Linux（RHEL）バージョン 7、および互換性のある CentOS バージョン 7（64 ビット）
- Red Hat Enterprise Linux（RHEL）バージョン 8、および互換性のある CentOS バージョン 8（64 ビット）
- Raspberry Pi OS 搭載の Raspberry Pi 2 Model B（32 ビット armhf）
- CoreOS でテスト済みの Docker（64 ビット）

NetFlow 収集を実行する Ubuntu へのインストール

はじめる前に

- 管理者として Ubuntu システムにログインします。

手順

コマンドライン インターフェイスで次の手順を実行します。

1. `wget https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_UbuntuXenial_amd64.deb` と入力して Secure Cloud Analytics パッケージをダウンロードします。
2. `sudo apt-get install -y net-tools tcpdump` と入力して依存関係をインストールします。
3. `sudo apt-get update && sudo apt-get install -y libglib2.0-0 liblzo2-2 libltdl7` と入力してアップデートおよび追加パッケージをインストールします。
4. Enter `wget https://assets-production.obsrvbl.com/ona-packages/netsa/v0.1.27/netsa-pkg.deb` と入力してパッケージ マネージャ ファイルをダウンロードします。
5. `sudo apt install ./ona-service_UbuntuXenial_amd64.deb ./netsa-pkg.deb` と入力してパッケージ マネージャ ファイルをインストールします。
6. `sudo reboot`と入力して Linux を再起動します。
7. サービスが実行されていることを確認します。サービスについては、「**付録 C – サービス**」を参照してください。

NetFlow 収集を実行しない Ubuntu へのインストール

はじめる前に

- 管理者として Ubuntu システムにログインします。

手順

コマンドライン インターフェイスで次の手順を実行します。

1. `wget https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_UbuntuXenial_amd64.deb` と入力して Secure Cloud Analytics パッケージをダウンロードします。
2. `sudo apt-get install -y net-tools tcpdump` と入力して依存関係をインストールします。
3. `sudo apt-get -f install` と入力して依存関係が正しくインストールされていることを確認します。
4. `sudo apt install ./ona-service_UbuntuXenial_amd64.deb ./netsa-pkg.deb` と入力して Secure Cloud Analytics サービスをインストールします。
5. サービスが実行されていることを確認します。サービスについては、「付録 C – サービス」を参照してください。

RHEL へのインストール

RHEL 8

はじめる前に

- 管理者として RHEL 8 システムにログインします。

手順

コマンドライン インターフェイスで次の手順を実行します。

1. `curl -L -O https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_RHEL_8_x86_64.rpm` と入力して Secure Cloud Analytics パッケージをダウンロードします。
2. `sudo yum install -y net-tools tcpdump` と入力して依存関係をインストールします。
3. 次のコマンドを実行して、更新プログラムと追加パッケージをインストールします。
    a. `sudo yum updateinfo` と入力します
    b. `yum install -y libpcap libtool-ltdl lzo` と入力します
4. `curl -L -O https://assets-production.obsrvbl.com/ona-packages/netsa/v0.1.27/netsa-pkg.rpm` と入力してパッケージ マネージャ ファイルをダウンロードします。

    > ⚠ 完全なコマンドを入力してください。

5. `sudo rpm -i netsa-pkg.rpm` と入力してパッケージ マネージャ ファイルをインストールします。

6. `sudo rpm -i ona-service_RHEL_8_x86_64.rpm` と入力して Secure Cloud Analytics サービスをインストールします。
7. サービスが実行されていることを確認します。サービスについては、「付録 C – サービス」を参照してください。

RHEL 7

はじめる前に

- 管理者として RHEL 7 システムにログインします。

手順

コマンドライン インターフェイスで次の手順を実行します。

1. `curl -L -O https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_RHEL_7_x86_64.rpm` と入力して Secure Cloud Analytics パッケージをダウンロードします。
2. `sudo yum install -y net-tools tcpdump` と入力して依存関係をインストールします。
3. 次のコマンドを実行して、更新プログラムと追加パッケージをインストールします。
   a. `sudo yum updateinfo` と入力します
   b. `yum install -y libpcap libtool-ltdl lzo` と入力します
4. `curl -L -O https://assets-production.obsrvbl.com/ona-packages/netsa/v0.1.27/netsa-pkg.rpm` と入力してパッケージ マネージャ ファイルをダウンロードします。

   > ⚠ 完全なコマンドを入力してください。

5. `sudo rpm -i netsa-pkg.rpm` と入力してパッケージ マネージャ ファイルをインストールします。
6. `sudo rpm -i ona-service_RHEL_7_x86_64.rpm` と入力して Secure Cloud Analytics サービスをインストールします。
7. サービスが実行されていることを確認します。サービスについては、「付録 C – サービス」を参照してください。

Web ポータルへのセンサーの接続

センサーのインストールが完了したら、そのセンサーをポータルにリンクさせる必要があります。そのためには、センサーのパブリック IP アドレスを特定して Web ポータルに入力します。センサーのパブリック IP アドレスを特定できない場合は、一意のサービスキーを使用して手動でセンサーをポータルにリンクさせることができます。

センサーは、次のポータルに接続できます。

- https://sensor.ext.obsrvbl.com（米国）
- https://sensor.eu-prod.obsrvbl.com（EU）
- https://sensor.anz-prod.obsrvbl.com（オーストラリア）

> 複数のセンサーが MSSP などの中央ロケーションにステージングされ、複数のお客様が対象になっている場合は、新規のお客様を設定するたびにパブリック IP を削除する必要があります。ステージング環境のパブリック IP アドレスを複数のセンサーに使用すると、センサーが誤ったポータルに不適切に接続される可能性があります。

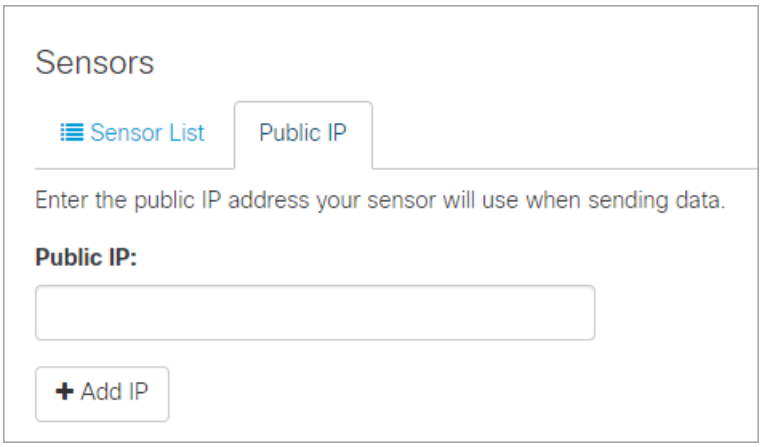
> プロキシサーバーを使用している場合は、「**プロキシの設定** Web ポータル間の通信を有効にします。

センサーのパブリック IP アドレスの検索とポータルへの追加

1. センサーに SSH で接続し、管理者としてログインします。
2. コマンドプロンプトで「`curl https://sensor.ext.obsrvbl.com`」と入力し、Enter を押します。`error` 値の `unknown identity` は、センサーがポータルに関連付けられていないことを意味します。次のスクリーンショットで例を参照してください。

```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ curl https://sensor.ext.obsrvbl.com
{
  "error": "unknown identity",
  "identity": "72.163.2.237"
}observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
```

3. `identity` IP アドレスをコピーします。
4. センサーからログアウトします。
5. サイト管理者として Web ポータルにログインします。
6. センサー（☁）アイコン > [パブリック IP（Public IP）] を選択します。
7. [パブリックIP（Public IP）] フィールドに `identity` IP アドレスを入力します。次のスクリーンショットで例を参照してください。



8. [IPの追加(Add IP)]をクリックします。ポータルとセンサーがキーを交換した後は、パブリック IP アドレスではなくキーを使用して以降の接続が確立されます。

> 新しいセンサーがポータルで反映されるまでに、最大 10 分かかる場合があります。

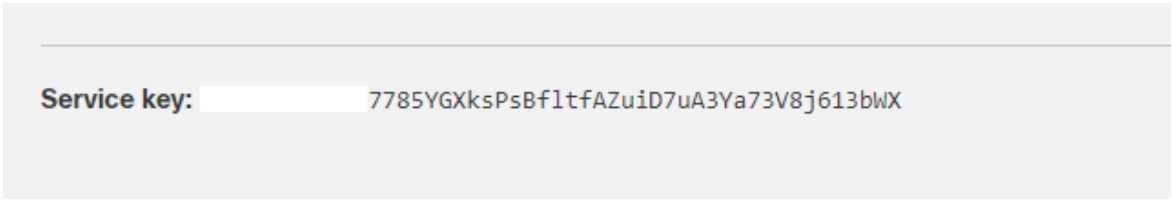
ポータルのサービス キーのセンサーへの手動による追加

> この手順は、センサーのパブリック IP アドレスが Web ポータルにすでに追加されている場合は必要**ありません**。この手順を試行する前に追加することを推奨します。ポータルのサービスキーのセンサーへの手動追加は、主に、2018 年 12 月時点で使用可能な ISO バージョン `ona-18.04.1-server-amd64.iso` より前に展開した古いセンサーを対象としています。また、Web ポータルで使用可能な現在のバージョンのセンサー ISO を使用して、古いセンサーを再展開することもできます。

センサーのパブリック IP アドレスを Web ポータルに追加できない場合か、または MSSP で複数の Web ポータルを管理している場合は、センサーの `config.local` 構成ファイルを編集し、ポータルのサービスキーを手動で追加してセンサーをポータルに関連付けます。

> 前の項のパブリック IP アドレスを使用すると、このキー交換が自動的に行われます。

1. 管理者としてポータル Web UI にログインします。
2. [設定(Settings)]>[センサー(Sensors)]を選択します。
3. センサーリストの末尾に移動して[サービスキー(Service key)]をコピーします。次のスクリーンショットで例を参照してください。



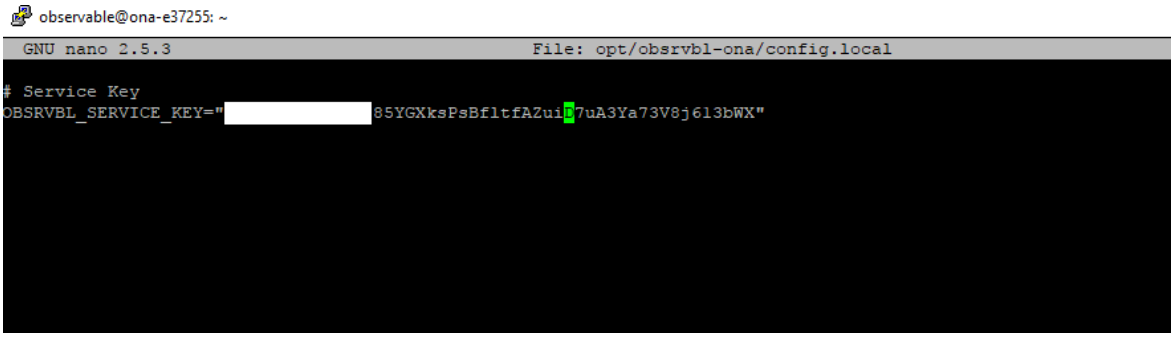
4. 管理者としてセンサーに SSH ログインします。

5. コマンドプロンプトで、このコマンドを入力し、`sudo nano opt/obsrvbl-ona/config.local` を入力し、Enter を押して設定ファイルを編集します。
6. `# Service Key` の下に次の行を追加します。

   <service-key> は次のポータルのサービスキーに置き換えてください。

   `OBSRVBL_SERVICE_KEY="<service-key>"`

   次に例を示します。



7. Ctrl+0 を押して変更を保存します。
8. Ctrl+X を押して終了します。
9. コマンド プロンプトで「`sudo service obsrvbl-ona restart`」を入力し、Secure Cloud Analytics サービスを再起動します。

プロキシの設定

プロキシサーバーを使用している場合は、次の手順を実行して、センサーと Web ポータル間の通信を有効にします。

1. センサーに SSH で接続し、管理者としてログインします。
2. コマンドプロンプトで、このコマンドを入力し、`sudo nano opt/obsrvbl-ona/config.local` を入力し、Enter を押して設定ファイルを編集します。
3. 次の行を追加し、`proxy.name.com` をプロキシサーバーのホスト名または IP アドレスに置き換え、`Port` をプロキシサーバーのポート番号に置き換えます。
   `HTTPS_PROXY="proxy.name.com:Port"`

> HTTP は特定の状況でサポートされる場合があります。詳細については、サポートまでお問い合わせください。

4. Ctrl+0 を押して変更を保存します。
5. Ctrl+X を押して終了します。
6. コマンド プロンプトで「`sudo service obsrvbl-ona restart`」を入力し、Secure Cloud Analytics サービスを再起動します。

センサーのポータル接続の確認

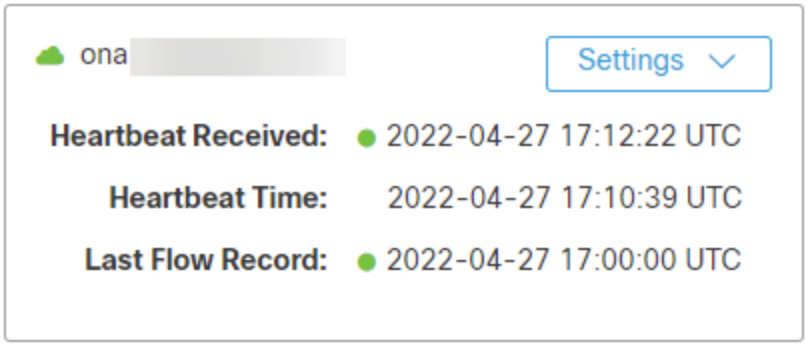
センサーをポータルに追加したら、接続を確認します。

> サービスキーを使用して `config.local` 設定ファイルを更新し、手動でセンサーを Web ポータルにリンクさせた場合は、`curl` コマンドを使用してセンサーからの接続を確認しても Web ポータルの名前が返されないことがあります。

1. 管理者としてセンサーに SSH で接続します。
2. コマンドプロンプトで「`curl https://sensor.ext.obsrvbl.com`」と入力し、Enter を押します。センサーは、ポータルの名前を返します。次のスクリーンショットで例を参照してください。

```
observable@ona-e37255:/opt/obsrvbl-ona$ curl https://sensor.ext.obsrvbl.com
{
  "welcome": "cisco-demo"
observable@ona-e37255:/opt/obsrvbl-ona$
```

3. センサーからログアウトします。
4. ポータル Web UI にログインします。
5. [設定（Settings）] > [センサー（Sensors）] を選択します。リストにセンサーが表示されます。



フロー データを収集するセンサーの設定

センサーは、デフォルトでイーサネット インターフェイス上のトラフィックからフロー レコードを作成します。このデフォルト設定は、センサーが SPAN またはミラー イーサネット ポートに接続されていることを前提としています。ネットワーク上の他のデバイスでフローレコードを生成できる場合、これらのソースからフローレコードを収集してクラウドに送信するように、Web ポータル UI でセンサーを設定できます。

ネットワーク デバイスでさまざまなタイプのフローが生成される場合は、タイプごとに異なる UDP ポートで収集するようにセンサーを設定することをお勧めします。これにより、トラブルシューティングも容易になります。デフォルトでは、ローカル センサー ファイアウォール（`iptables`）のポート 2055/UDP、4739/UDP、および 9995/UDP が開いています。追加の UDP ポートを使用するには、Web ポータル UI でそれらのポートを開く必要があります。

次のポートを使用した、次のフロータイプの収集を設定できます。

- NetFlow v5：ポート 2055/UDP（デフォルトで開いている）
- NetFlow v9：ポート 9995/UDP（デフォルトで開いている）
- IPFIX：ポート 9996/UDP
- sFlow：ポート 6343/UDP

一部のネットワーク アプライアンスは、正しく機能させるために Web ポータル UI で選択する必要があります。

- Cisco Meraki：ポート 9998/UDP
- Cisco ASA：ポート 9997/UDP
- SonicWALL：9999/UDP

フロー収集のためのセンサーの設定

はじめる前に

- 管理者としてポータル Web UI にログインします。

手順

1. [設定（Settings）] > [センサー（Sensors）] を選択します。
2. 追加したセンサーについて、[設定の変更（Change settings）] をクリックします。
3. [NetFlow/IPFIX] を選択します。

   > このオプションには最新バージョンのセンサーが必要です。このオプションが表示されない場合は、[ヘルプ（？）（Help (?)）] > [オンプレミスセンサーのインストール（On-Prem Sensor Install）] を選択して、最新バージョンのセンサー ISO をダウンロードしてください。

4. [新しいプローブの追加（Add New Probe）] をクリックします。
5. [プローブタイプ（Probe Type）] ドロップダウンリストからフロータイプを選択します。
6. **ポート**番号を入力します。

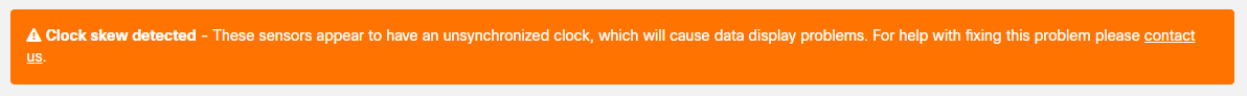
> センサーに拡張 NetFlow を渡す場合は、設定する UDP ポートが、センサーの設定で Flexible NetFlow や IPFIX 用に設定されていないことを確認してください。たとえば、拡張 NetFlow にはポート 2055/UDP を設定し、Flexible NetFlow にはポート 9995/UDP を設定します。詳細については、『Configuration Guide for Enhanced NetFlow』を参照してください。

7. [プロトコル（Protocol）] を選択します。
8. ドロップダウンリストから [送信元デバイス（Source device）] を選択します。
9. [保存（Save）] をクリックします。

付録 A – トラブルシューティング

時刻のずれの解決と NTP の同期

デフォルトでは、センサーは NTP 時刻同期に `pool.ntp.org` を使用し、ポータルで適切にデータが表示されるように設定されています。アウトバウンド NTP が許可されていない場合は、NTP の設定を更新する必要が生じることがあります。センサーの時刻が正しく同期されていない場合は、ポータルに警告が表示されます。次のスクリーンショットで例を参照してください。



はじめる前に

- 管理者としてセンサーに SSH で接続します。

手順の概要

1. `timedatectl status` と入力して **Enter** を押し、NTP が同期されているかどうかを確認します。
2. `sudo apt-get update && sudo apt-get install -y ntpdate ntp`
3. `sudo service ntp stop`
4. `sudo ntpdate pool.ntp.org`
5. アウトバウンド NTP が許可されていない場合は、`pool.ntp.org` の代わりに内部 IP アドレスを指定します。
6. `sudo service ntp start`

手順

1. コマンドプロンプトで `timedatectl status` と入力して Enter を押し、NTP が同期されているかどうかを確認します。正しく NTP と同期されていないセンサーの例については、次のスクリーンショットを参照してください。

```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ timedatectl status
      Local time: Sat 2017-12-09 20:50:13 CST
  Universal time: Sun 2017-12-10 02:50:13 UTC
        RTC time: Sun 2017-12-10 02:50:12
       Time zone: America/Chicago (CST, -0600)
 Network time on: yes
NTP synchronized: no
 RTC in local TZ: no
```

2. 次のコマンドを入力してEnter を押し、正しい NTP パッケージがインストールされ、最新の状態であることを確認します。

   `sudo apt-get update && sudo apt-get install -y ntpdate ntp`

3. `sudo service ntp stop` と入力して Enter を押し、NTP サービスを停止します。
4. `sudo ntpdate pool.ntp.org` と入力して Enter を押し、同期に使用する NTP サーバを設定します。

   アウトバウンド NTP が許可されていない場合は、サーバが見つからないことを示すエラーメッセージが表示されます。次のスクリーンショットで例を参照してください。

```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ sudo service ntp stop
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ sudo ntpdate pool.ntp.org
 9 Dec 20:52:24 ntpdate[4779]: no server suitable for synchronization found
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
```

5. アウトバウンド NTP が許可されていない場合は、`pool.ntp.org` の代わりに内部 IP アドレスを指定します。次のスクリーンショットで例を参照してください。

```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ sudo service ntp stop
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ sudo ntpdate 72.163.16.189
 9 Dec 21:33:49 ntpdate[4825]: adjust time server 72.163.16.189 offset 0.000063 sec
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ sudo service ntp start
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ timedatectl status
      Local time: Sat 2017-12-09 21:34:03 CST
  Universal time: Sun 2017-12-10 03:34:03 UTC
        RTC time: Sun 2017-12-10 02:54:53
       Time zone: America/Chicago (CST, -0600)
 Network time on: yes
NTP synchronized: yes
 RTC in local TZ: no
```

6. `sudo service ntp start` と入力して Enter を押し、NTP サービスを開始します。

単方向トラフィックのエラーの解決

Secure Cloud Analytics サービスは、センサーが双方向フローを認識していない場合にそのことを検出します。たとえば、発信または着信 TCP トラフィックのみのホストが多数存在する場合は、データ フィードの一部が欠落することを意味します。その場合は、適切に設定されていないミラー ポート、見つからない VLAN、または設定が正しくないファイアウォールの影響ですべてのインターフェイス上ではフロー データが送信されないなどの問題が想定されます。ミラー ポートを通過するトラフィックを検索し、単方向か双方向かを特定できます。

はじめる前に

- 管理者としてセンサーに SSH で接続します。

手順の概要

1. `ifconfig -a` と入力します。
2. 次のコマンドを入力します。

   `sudo tcpdump -i <mirror-interface-name> -n -c 100 "tcp"`

   Enter を押してミラーインターフェイスを通過するトラフィックをキャプチャし、ブロードキャストトラフィックだけでなく TCP トラフィックが検出されることを確認します。
3. 次のコマンドを入力します。

   `sudo tcpdump -i <mirror-interface-name> -n -c 100 "port 9996"`

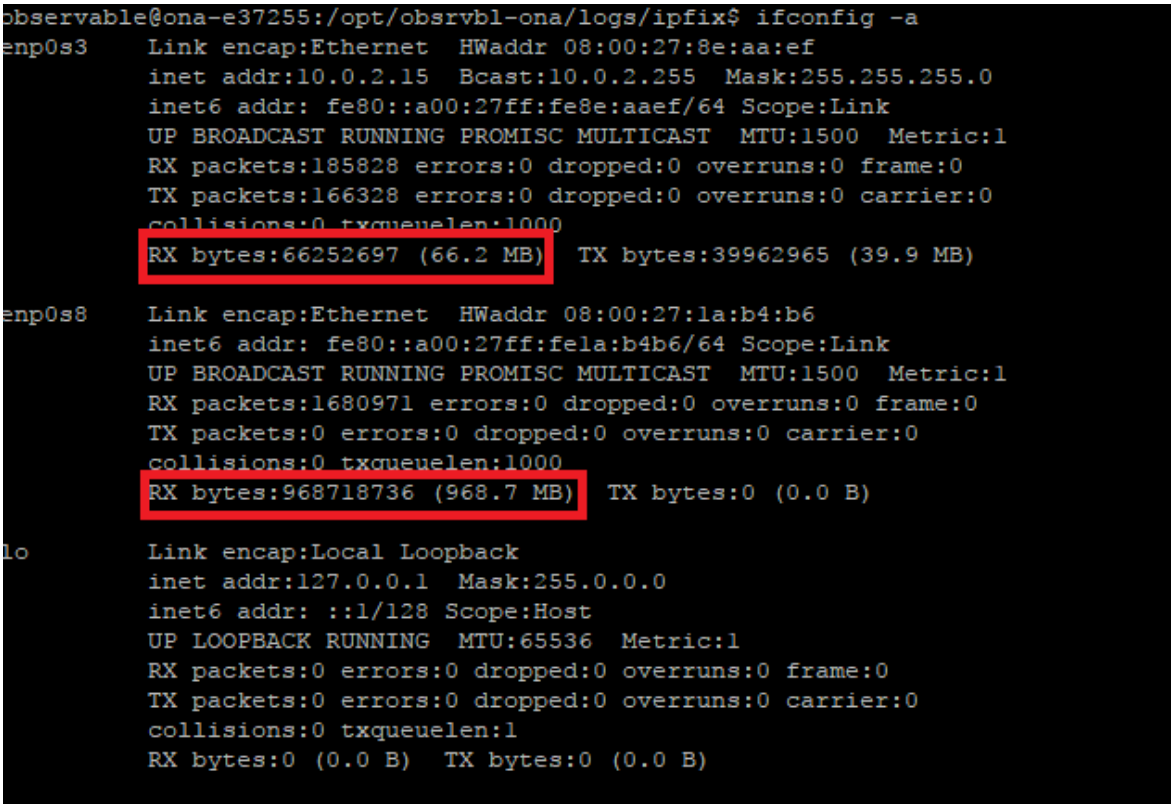
   Enter を押して、ポート 9996/TCP に一致するトラフィックをキャプチャします。
4. 次のコマンドを入力します。

   `sudo tcpdump -i <mirror-interface-name> -n -c 100 "src 10.99.102.180"`

   Enter を押して、送信元 IP アドレス 10.99.102.180 に一致するトラフィックをキャプチャします。

手順

1. コマンド プロンプトで `ifconfig -a` と入力して Enter を押し、インターフェイスのリストを表示します。通常、ミラー ポート インターフェイスには関連付けられた IP アドレスがなく、パケット数とバイト数は他のインターフェイスよりも多くなっています。次のスクリーンショットの例では、`enp0s8` インターフェイスのトラフィックが非常に多く、ミラーポートであることを示しています。

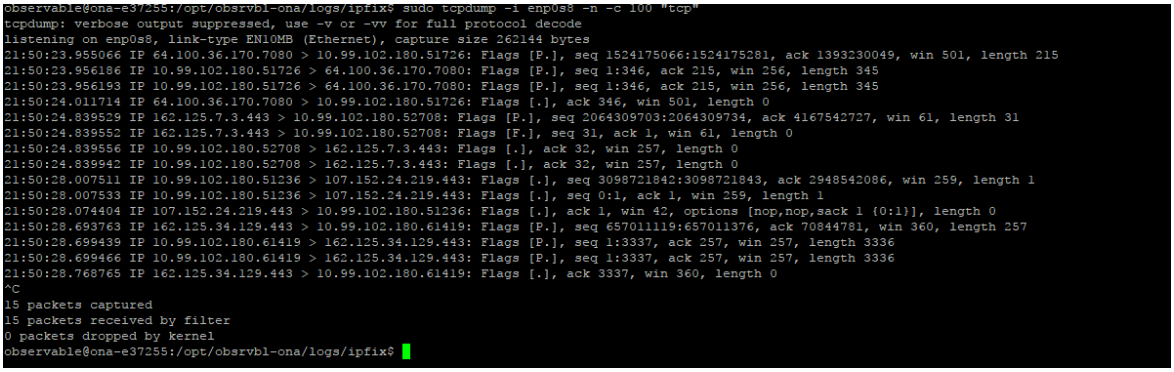


2. 次のコマンドを入力します。

   `sudo tcpdump –i <mirror-interface-name> -n –c 100 "tcp"`

   (`<mirror-interface-name>` は、`eth0` などのインターフェイス名と置き換えてください)

   Enter を押してミラーインターフェイスを通過するトラフィックをキャプチャし、ブロードキャストトラフィックだけでなく TCP トラフィックが検出されることを確認します。次のスクリーンショットで例を参照してください。

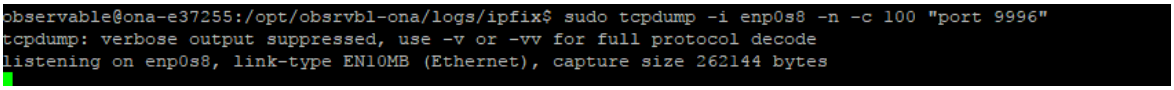


3. 次のコマンドを入力します。

   `sudo tcpdump –i <mirror-interface-name> -n –c 100 "port 9996"`

   (`<mirror-interface-name>` は、`eth0` などのインターフェイス名と置き換えてください)

   Enter を押して、ポート 9996/TCP に一致するトラフィックをキャプチャします。必要に応じて、特定のトラフィックを検索するようにコマンドを設定できます。次のスクリーンショットで例を参照してください。

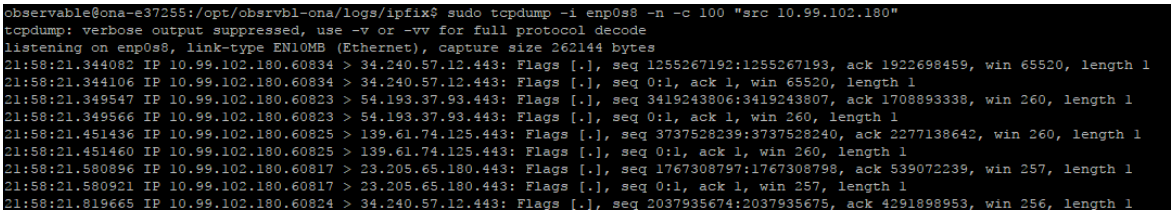


4. 次のコマンドを入力します。

   `sudo tcpdump –i <mirror-interface-name> -n –c 100 "src 10.99.102.180"`

   (`<mirror-interface-name>` は、`eth0` などのインターフェイス名と置き換えてください)

   Enter を押して、送信元 IP アドレス `10.99.102.180` に一致するトラフィックをキャプチャします。次のスクリーンショットで例を参照してください。



付録 B – 参考情報

Secure Cloud Analytics 資料

次に、センサーの導入に使用できる Secure Cloud Analytics ドキュメンテーションについて説明します。

リソース	説明
センサーインストールガイド	このガイドには、VM またはベアメタルサーバーでのセンサーのインストール手順と、オンプレミスセンサーを展開する場所および方法に関するベストプラクティス情報が含まれています。 顧客がファイアウォールルールを調整する必要がある場合に備えて、Secure Cloud Analytics サービスで使用する IP アドレスも記載されています。
Amazon Web Services 向けパブリック クラウド モニターリング クイック スタート ガイド	このガイドでは、Secure Cloud Analytics によってモニタされる AWS アカウントを有効にするプロセスについて説明しています。

Secure Cloud Analytics ファイルとディレクトリ

次の プライベートネットワークのモニタリング Linux ディレクトリおよびファイルパスには、高度なセンサー設定が含まれています。

- `/opt/obsrvbl-ona`:このディレクトリには、Secure Cloud Analytics の設定ファイル(`config`、`config.auto`、`config.local`)、およびセンサーのインストール時に作成されるさまざまなサブディレクトリ(ログファイルディレクトリなど)が含まれています。
- `/opt/obsrvbl-ona/config`:センサーのインストール時に作成されるこのテキストファイルには、デフォルトのセンサー設定が含まれています。このファイルを直接編集することはお勧めしません。変更は `config.local` で行う必要があります。このファイルを編集する場合は、最初にバックアップを作成してください。このファイルは、`config.local` ファイルを更新する際に参照できます。`config.local` ファイルの設定内容によって、デフォルトの `config` ファイル設定が上書きされます。

  > config 設定ファイルの最新バージョンは、Secure Cloud Analytics GitHub サイト(https://github.com/obsrvbl-oss/ona/blob/master/packaging/root/opt/obsrvbl-ona/config)にあります。

- `/opt/obsrvbl-ona/config.auto`:このテキストファイルには、ユーザが Web ポータルから行ったセンサー設定の変更内容が含まれています。たとえば、センサーによる Web ポータルから syslog または SNMP へのロギングを有効にすると、Web ポータルはこのファイルを更新し、これらの設定の更新を追加します。このファイルを直接編集**しない**ことを推奨します。
- `/opt/obsrvbl-ona/config.local`:このテキストファイルには、このセンサーのカスタム設定が含まれています。このファイルの設定の更新によって、`config` 設定ファイルの設定内容が上書きされます。ローカル設定の例には、フロー収集の有効化、フロー収集タイプ

の設定（NetFlow v5、IPFIX など）、Suricata などのプログラムとのサードパーティ統合の有効化が含まれますが、これに限定されるわけではありません。

> フロー収集の設定に使用する config.local ファイルの更新は、主に 2018 年 12 月時点で使用可能な ISO バージョン `ona-18.04.1-server-amd64.iso` より前に展開した古いセンサーを対象としています。Web ポータルで使用可能な現在のバージョンのセンサー ISO を使用して、古いセンサーを再展開できます。

- `/opt/obsrvbl-ona/logs/PNA`:このディレクトリには、センサーのイーサネットポートで作成されたフローに関連するログファイルが含まれています。センサーは定期的にこれらのファイルをクラウドにアップロードして、ディレクトリを空にします。イーサーネット ポートに入るデータのサイズに関連して、ログ ファイルのバイト数と数量が増えるので、ミラー ポートが適切に機能するようにこのディレクトリをモニタできます。

  次のスクリーンショットでは、ログファイルが非常に小さく、イーサネットポートのトラフィックがかなり少ないことがわかります。ただし、サービスは実行中であり、アクティブにログ ファイルを生成しています。

```
observable@ona-e37255:/opt/obsrvbl-ona/logs/pna$ ls -l
total 464
-rw-rw-r-- 1 obsrvbl_ona obsrvbl_ona  400 Dec  8 10:30 pna-20171208163002-enp0s3.tl.log
-rw-rw-r-- 1 obsrvbl_ona obsrvbl_ona 1072 Dec  8 10:30 pna-20171208163009-enp0s3.t0.log
-rw-rw-r-- 1 obsrvbl_ona obsrvbl_ona 1552 Dec  8 10:30 pna-20171208163009-enp0s8.t0.log
-rw-rw-r-- 1 obsrvbl_ona obsrvbl_ona 1600 Dec  8 10:30 pna-20171208163021-enp0s8.tl.log
-rw-rw-r-- 1 obsrvbl_ona obsrvbl_ona  592 Dec  8 10:30 pna-20171208163029-enp0s8.t0.log
-rw-rw-r-- 1 obsrvbl_ona obsrvbl_ona 1360 Dec  8 10:30 pna-20171208163030-enp0s3.tl.log
-rw-rw-r-- 1 obsrvbl_ona obsrvbl_ona 1216 Dec  8 10:30 pna-20171208163039-enp0s8.tl.log
```

- `/opt/obsrvbl-ona/logs/ipfix`:このディレクトリには、NetFlow や IPFIX などのフローデータフィードによって収集されたログファイルが含まれています。このディレクトリが存在する場合、フロー収集は正常に有効化されて受信されています。このディレクトリが存在しない場合は、フロー収集が有効になっていない可能性があります。

  次のスクリーンショットでは、ログファイルが増加せずに空の状態です。センサーは、フローデータを受信していません。

```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ ls -l
total 0
-rw-r--r-- 1 obsrvbl_ona obsrvbl_ona 0 Dec  8 10:47 20171208164700_S3.yldHNA
-rw-r--r-- 1 obsrvbl_ona obsrvbl_ona 0 Dec  8 10:47 20171208164700_S4.4IZwNL
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
```

- `/etc/iptables`:このディレクトリには、センサーの `iptables` ファイアウォール設定ファイルが含まれています。

付録 C – サービス

Secure Cloud Analytics は次の Linux サービスを利用します。

サービス	デフォルトでイネーブルかどうか	説明
obsrvbl-ona	はい	設定の変更をモニタし、自動更新を処理します。このサービスを開始すると、設定されている他のサービスも開始されます。
log-watcher	はい	センサーの認証ログを追跡します。
pdns-capturer	はい	パッシブ DNS クエリを収集します。
pna-monitor	はい	IP トラフィックのメタデータを収集します。
pna-pusher	はい	クラウドに IP トラフィックのメタデータを送信します。
hostname-resolver	はい	アクティブ IP アドレスをローカル ホスト名に解決します。
netflow-monitor	いいえ	ルータおよびスイッチによって送信される NetFlow データをリッスンします。
netflow-pusher	いいえ	NetFlow データをクラウドに送信します。
notification-publisher	いいえ	Syslog または SNMP を介して監視結果とアラートをリレーします。
ossec-alert-watcher	いいえ	OSSEC アラートをモニタします（インストールされている場合）。
suricata-alert-watcher	いいえ	Suricata アラートをモニタします（インストールされている場合）。

実行中のサービスの確認

センサーのコマンドラインから、さまざまなサービスが実行されていることを確認できます。

はじめる前に

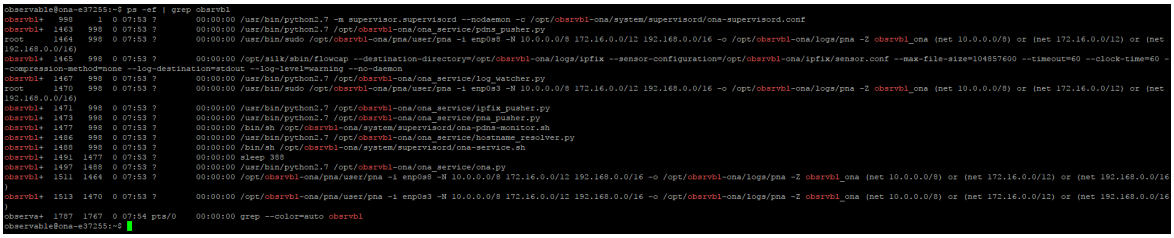
- センサーに SSH で接続し、管理者としてログインします。

手順の概要

`ps -ef | grep obsrvbl`

手順

1. コマンドプロンプトで `ps -ef |grep obsrvbl` と入力して Enter を押します。次のスクリーンショットで例を参照してください。



付録 D – センサーのアップグレード

センサーが正常に動作している場合は、アップグレードする必要はありません。ただし、新しい機能（外部サービスとの統合など）が不足している場合は、次のいずれかの手順を使用してアップグレードします。

- **Ubuntuでのアップグレード**シスコの Web ポータル UI からセンサーイメージ（ISO）をダウンロードした場合は、次の手順を参照してください。これが最も一般的なシナリオです。
- **Red Hat Enterprise Linux ベースのオペレーティングシステムでのアップグレード**

Ubuntuでのアップグレード

シスコの Web ポータル UI からセンサーイメージ（ISO）をダウンロードした場合は、Ubuntu を使用してセンサーをアップグレードします。

はじめる前に

- 「**センサーのバージョンの確認**」の手順に従って、現在のセンサーのバージョンを確認します。
- 管理者として Ubuntu システムにログインします。

手順の概要

1. `sudo systemctl stop obsrvbl-ona.service`
2. `sudo cp /opt/obsrvbl-ona/config.auto ~/config.auto`
3. `sudo cp /opt/obsrvbl-ona/config.local ~/config.local`
4. `rm -f ona-service_UbuntuXenial_amd64.deb`
5. `wget https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_UbuntuXenial_amd64.deb`
6. `sudo apt remove --purge ona-service_UbuntuXenial_amd64.deb`
7. `sudo apt install ./ona-service_UbuntuXenial_amd64.deb`
8. `sudo cp ~/config.auto /opt/obsrvbl-ona/config.auto`
9. `sudo cp ~/config.local /opt/obsrvbl-ona/config.local`
10. `sudo chown obsrvbl_ona:obsrvbl_ona /opt/obsrvbl-ona/config.auto /opt/obsrvbl-ona/config.local`
11. `sudo systemctl restart obsrvbl-ona.service`

手順

各セクションでコマンドを実行して、センサーをアップグレードする手順を完了します。

サービスを停止し、既存の設定をバックアップします。

1. コマンドプロンプトで、このコマンドを入力し、

   `sudo systemctl stop obsrvbl-ona.service`

   と入力し、Enter を押してサービスを停止します。

2. `sudo cp /opt/obsrvbl-ona/config.auto ~/config.auto` と入力し、Enter を押します。
3. `sudo cp /opt/obsrvbl-ona/config.local ~/config.local` と入力し、Enter を押します。

新しいパッケージのダウンロード

4. `rm -f ona-service_UbuntuXenial_amd64.deb` と入力し、Enter を押します。
5. `wget https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_UbuntuXenial_amd64.deb` と入力し、Enter を押します。

古いパッケージを削除し、新しいパッケージをインストールします。

6. `sudo apt remove --purge ona-service_UbuntuXenial_amd64.deb` と入力し、Enter を押します。
7. `sudo apt install ./ona-service_UbuntuXenial_amd64.deb` と入力し、Enter を押します。

バックアップ設定の復元

8. `sudo cp ~/config.auto /opt/obsrvbl-ona/config.auto` と入力し、Enter を押します。
9. `sudo cp ~/config.local /opt/obsrvbl-ona/config.local` と入力し、Enter を押します。
10. `sudo chown obsrvbl_ona:obsrvbl_ona /opt/obsrvbl-ona/config.auto /opt/obsrvbl-ona/config.local` と入力し、Enter を押します。

システムの再起動:

11. `sudo systemctl restart obsrvbl-ona.service` と入力し、Enter を押します。

更新の確認:

12. 「**センサーのポータル接続の確認**」の手順に従って、センサーがリストに表示され、データを受信していることを確認します。
13. 「**センサーのバージョンの確認**」の手順に従って、センサーのバージョンが更新されていることを確認します。

Red Hat Enterprise Linux ベースのオペレーティングシステムでのアップグレード

CentOS などの Red Hat Enterprise Linux ベースのオペレーティングシステムを使用している場合は、次の手順に従ってセンサーをアップグレードします。

はじめる前に

- 「**センサーのバージョンの確認**」の手順に従って、現在のセンサーのバージョンを確認します。
- センサーに SSH で接続し、管理者としてログインします。

手順の概要

1. `sudo systemctl stop obsrvbl-ona.service`
2. `sudo cp /opt/obsrvbl-ona/config.auto ~/config.auto`
3. `sudo cp /opt/obsrvbl-ona/config.local ~/config.local`
4. `rm -f ona-service_RHEL_7_x86_64.rpm`
5. `curl -L -O https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_RHEL_8_x86_64.rpm`
6. `sudo yum remove ona-service`
7. `sudo yum install ./ona-service_RHEL_8_x86_64.rpm`
8. `sudo cp ~/config.auto /opt/obsrvbl-ona/config.auto`
9. `sudo cp ~/config.local /opt/obsrvbl-ona/config.local`
10. `sudo chown obsrvbl_ona:obsrvbl_ona /opt/obsrvbl-ona/config.auto /opt/obsrvbl-ona/config.local`
11. `sudo systemctl restart obsrvbl-ona.service`

手順

各セクションでコマンドを実行して、センサーをアップグレードする手順を完了します。

サービスを停止し、既存の設定をバックアップします。

1. コマンドプロンプトで、このコマンドを入力し、

   `sudo systemctl stop obsrvbl-ona.service`
   と入力し、Enter を押してサービスを停止します。
2. `sudo cp /opt/obsrvbl-ona/config.auto ~/config.auto` と入力し、Enter を押します。
3. `sudo cp /opt/obsrvbl-ona/config.local ~/config.local` と入力し、Enter を押します。

新しいパッケージのダウンロード:

4. `rm -f ona-service_RHEL_7_x86_64.rpm` と入力し、Enter を押します。
5. `curl -L -O https://assets-production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-service_RHEL_8_x86_64.rpm` と入力し、Enter を押します。

古いパッケージを削除し、新しいパッケージをインストールします。

6. `sudo yum remove ona-service` と入力し、Enter を押します。
7. `sudo yum install ./ona-service_RHEL_8_x86_64.rpm` と入力し、Enter を押します。

バックアップ設定の復元

8. `sudo cp ~/config.auto /opt/obsrvbl-ona/config.auto` と入力し、Enter を押します。
9. `sudo cp ~/config.local /opt/obsrvbl-ona/config.local` と入力し、Enter を押します。
10. `sudo chown obsrvbl_ona:obsrvbl_ona /opt/obsrvbl-ona/config.auto /opt/obsrvbl-ona/config.local` と入力し、Enter を押します。

システムの再起動:

11. `sudo systemctl restart obsrvbl-ona.service` と入力し、Enter を押します。

更新の確認:

12. 「**センサーのポータル接続の確認**」の手順に従って、センサーがリストに表示され、データを受信していることを確認します。
13. 「**センサーのバージョンの確認**」の手順に従って、センサーのバージョンが更新されていることを確認します。

関連リソース

Secure Cloud Analytics の詳細については、次を参照してください。

- 概要については、https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html [英語] を参照してください。
- 60 日間の無料トライアルに登録するには、https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html [英語] にアクセスしてください。
- ドキュメントリソースについては、https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html [英語] を参照してください。
- Secure Cloud Analytics 初期導入ガイドなど、インストールおよびコンフィギュレーション ガイドについては、https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html [英語] を参照してください。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html
- Secure Cloud Analytics 無料トライアルの試用時に電子メールでケースを開く場合：
  swatchc-support@cisco.com

変更履歴

リビジョン	改訂日	説明
1_0		最初のバージョン
1_5	2018 年 2 月 8 日	インストール プロセスに対する変更と更新、テキストのマイナー修正が行われました。
1_6	2018 年 3 月 26 日	Ubuntu Linux の手動インストールで NetFlow 収集を有効にする手順を追加しました。
1_7	2018 年 5 月 24 日	NetFlow 設定の問題を修正しました。
1_8	2018 年 5 月 25 日	付録に IPFIX 設定のリマインダを追加しました。
1_9	2018 年 5 月 29 日	ドキュメントから Ubuntu に直接コピーする構文の問題を修正しました。
1_10	2018 年 6 月 19 日	レンダリング形式を変更しました。
1_11	2018 年 8 月 8 日	変数を訂正しました。
1_12	2018 年 11 月 26 日	センサーフロー収集の設定を更新しました。
1_13	2019 年 1 月 22 日	センサーフロー収集の設定が更新され、その他のエラーが修正されました。
1_14	2019 年 4 月 18 日	廃止された用語を更新。
1_15	2020 年 9 月 4 日	UI の指示を更新しました。
1_16	2020 年 10 月 16 日	UI の更新を基に更新しました。
1_17	2021 年 8 月 3 日	「Linux オペレーティングシステム用パッケージの手動インストール」のセクションを更新しました。 「センサーのバージョンの確認」のセクションを更新しました。 ブランド用語を更新。 「付録D – センサーのアップグレード」を追加しました。
2_0	2022 年 2 月 10 日	ポータルの URL を更新しました。 RHEL 8 の情報を追加しました。 Ubuntu 20.04 の情報を追加しました。

2_1	2022 年 6 月 8 日	センサーのダウンロード URL を更新しました。 センサーのインストール手順を更新しました。 参照ドキュメントを更新しました。
3_0	2022 年 8 月 1 日	「サポートへの問い合わせ」と「関連リソース」を追加しました。 ドキュメントのタイトルを更新しました。
3_1	2023 年 1 月 17 日	GitHub リポジトリのリンクを更新。
4_0	2023 年 3 月 29 日	「Linux オペレーティングシステム用パッケージの手動インストール」のセクションを更新しました。 • RHEL 7 • RHEL 8
4_1	2023 年 7 月 24 日	タイプミスを修正しました。

著作権情報