

Cisco Secure Cloud Analytics

センサー インストール ガイド



目次

はじめに	3
センサー導入の考慮事項	3
センサーの前提条件	3
物理アプライアンスの追加要件	4
仮想マシンの追加要件	4
VMWare Hypervisor	4
VirtualBox	5
センサーの展開についての提案	5
センサーのバージョンの確認	5
センサーのアクセス要件	6
ネットワーク デバイス設定	6
フロー設定	7
Cisco Defense Orchestrator およびセンサーの展開	8
センサーメディアのインストールと設定	9
ブートメディアの作成	9
センサー ISO ファイルのダウンロード	9
ブート可能な光学ディスクの作成	9
ブート可能な USB フラッシュドライブの作成	10
センサーのインストール	10
Web ポータルへのセンサーの接続	13
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	13
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	14
センサーのポータル接続の確認	15
フローデータを収集するセンサーの設定	16
フロー収集用のセンサーの設定	17
トラブルシューティング	18
センサーからのパケットのキャプチャ	18
Wireshark でのパケットキャプチャの分析	18
関連リソース	19
変更履歴	20

はじめに

Cisco Secure Cloud Analytics (旧 Stealthwatch Cloud) は、オンプレミスとクラウド内の両方の IT 環境で脅威を検出して対応する SaaS ベースのセキュリティサービスです。このガイドでは、エンタープライズ ネットワーク、プライベートデータセンター、分散拠点、およびその他のオンプレミス環境で使用するために、プライベートネットワークのモニタリング サービスの一環として Secure Cloud Analytics センサーを展開する方法について説明します。



Amazon Web Services、Microsoft Azure、Google Cloud Platform などのパブリッククラウド環境のみで Secure Cloud Analytics を使用する場合は、センサーをインストールする必要はありません。詳細については、[パブリッククラウドのモニタリング ガイド](#)にアクセスしてください。

センサー導入の考慮事項

NetFlow などのフローデータを収集するように、またはネットワーク上のルータやスイッチからミラー化されるネットワークトラフィックを取得するようにセンサーを導入できます。フローデータの収集とミラー化されたネットワークトラフィックの取得の両方を行うようにセンサーを設定することもできます。導入するセンサーの数に制限はありません。

フローデータを収集するようにセンサーを設定する場合、詳細については、「[フローデータを収集するセンサーの設定](#)」を参照してください。

ミラーまたは SPAN ポートからのトラフィックを取得するようにセンサーを設定する場合、トラフィックをミラー化するためのネットワークデバイスの設定の詳細については、「[ネットワークデバイス設定](#)」を参照してください。



センサー バージョン 4.0 以降では、拡張 NetFlow テレメトリを収集できます。これにより、Secure Cloud Analytics では新しいタイプの観測内容とアラートを生成できます。詳細については、『[Secure Cloud Analytics Configuration Guide for Enhanced NetFlow](#)』[英語]を参照してください。

センサーの前提条件

次の要件が満たされている場合に、センサーを物理アプライアンスまたは仮想マシンにインストールできます。

コンポーネント	最小要件
ネットワークインターフェイス	Secure Cloud Analytics サービスに情報を渡すための、制御インターフェイスとして指定された、1 つ以上のネットワーク インターフェイス <div data-bbox="378 1667 422 1713" data-label="Image"> </div> 任意で、ミラーポートを経由するネットワークトラフィックを複製するネットワークデバイスからのトラフィックを取得するようにセンサーを設定する場合は、ミラーインターフェイスとして指定された 1 つ以上のネットワークインターフェイスが必要です。


RAM	2 GB
CPU	2 つ以上のコア
記憶領域	32 GB
インターネットアクセス	インストールプロセス用のパッケージをダウンロードするために必要

パフォーマンスの評価指標と推奨事項については、この[ホワイトペーパー](#)を参照してください。

指定されたミラー インターフェイスについては、次の点に注意してください。

- ミラー インターフェイスは、宛先へのすべてのインバウンドおよびアウトバウンド送信元トラフィックのコピーを受信します。ピークトラフィックがセンサーのミラー インターフェイス リンクの容量より小さいことを確認してください。
- 多くのスイッチでは、ミラー ポートの宛先に過剰なトラフィックが設定されている場合、送信元インターフェイスからのパケットがドロップされます。

物理アプライアンスの追加要件

コンポーネント	最小要件
インストールファイルのアップロード	<p>インストール .iso ファイルをアップロードするには次のいずれかが必要です。</p> <ul style="list-style-type: none"> • 1 つの USB ポートと、USB フラッシュドライブ • 1 つの光学ディスクドライブと、書き込み可能な光学ディスク (CD-R ディスクなど) <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <p> 仮想マシンは、追加の要件なしで .iso ファイルから直接起動できます。</p> </div>

仮想マシンの追加要件

センサーが仮想マシンとして展開されている場合、ミラーポートまたは SPAN ポートからのトラフィックを取得する予定のときは、2 つ目のネットワークインターフェイスで仮想ホストとネットワークが無差別モードに設定されていることを確認してください。

VMWare Hypervisor

VMWare Hypervisor で仮想マシンを実行している場合は、無差別モード用に仮想スイッチを設定します。

1. インベントリでホストを選択します。
2. [設定 (Configuration)] タブを選択します。
3. [ネットワーキング (Networking)] をクリックします。
4. 仮想スイッチの [プロパティ (Properties)] をクリックします。
5. 仮想スイッチを選択し、[編集 (Edit)] をクリックします。
6. [セキュリティ (Security)] タブを選択します。
7. [無差別モード (Promiscuous Mode)] ドロップダウンから [許可 (Accept)] を選択します。

無差別モードの詳細については、VMware ナレッジベースを参照してください。VLAN ID を 4095 に設定することが必要になる場合があります。

VirtualBox

VirtualBox で仮想マシンを実行している場合は、アダプタを無差別モードに設定します。

1. [ネットワーク設定 (Network Settings)] からミラーインターフェイス用のアダプタを選択します。
2. [詳細オプション (Advanced Options)] で無差別モードを [許可 (Allow)] に設定します。

詳細については、仮想ネットワークに関する VirtualBox のドキュメントを参照してください。

センサーの展開についての提案

ネットワークトポロジは大きく異なる可能性があるため、センサーを展開するときは、次の一般的なガイドラインに注意してください。

1. 次の目的のためにセンサーを展開するかどうかを決定します。
 - フロー データを収集する
 - ミラー化されたネットワークトラフィックを取得する
 - 一部のセンサーにフロー データを収集させ、その他のセンサーにミラー化されたネットワークトラフィックを取得させる
 - 両方のセンサーにフロー データを収集させるとともにミラー化されたネットワークトラフィックを取得させる
2. フローデータを収集する場合は、ネットワークデバイスがエクスポートできる形式 (NetFlow v5、NetFlow v9、IPFIX、sFlow など) を決定します。



[Cisco ASA ファイアウォール](#) や [Cisco Meraki MX アプライアンス](#) などの多数のファイアウォールが NetFlow をサポートしています。製造元のサポートドキュメントを参照して、ファイアウォールが NetFlow もサポートしているかどうかを確認してください。

3. センサーのネットワークポートがミラーポート容量をサポートできることを確認します。

ネットワークに複数のセンサーを展開する際に支援が必要な場合は、support@obsrvbl.com にお問い合わせください。

センサーのバージョンの確認

最新のセンサー (バージョン 5.1.1) 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。アップグレードする必要がある場合は、センサーを再インストールしてください。

手順

1. 展開されているセンサーに SSH でログインします。
2. プロンプトで、「`cat /opt/obsrvbl-ona/version`」と入力して Enter キーを押します。コンソールに 5.1.1 と表示されない場合は、旧規格のセンサーです。Web ポータル UI から最新のセンサー ISO をダウンロードしてください。

センサーのアクセス要件

物理アプライアンスまたは仮想マシンは、インターネットを介して特定のサービスにアクセスできる必要があります。センサーと外部インターネットの間の次のトラフィックを許可するようにファイアウォールを設定します。

トラフィックのタイプ	必須	IP アドレスまたはドメインとポート
センサーの制御インターフェイスから Amazon Web Services でホストされている Secure Cloud Analytics サービスへのアウトバウンド HTTPS トラフィック	○	<ul style="list-style-type: none"> • 可変
Linux OS および関連する更新をダウンロードするための、センサーの制御インターフェイスから Ubuntu Linux サーバーへのアウトバウンドトラフィック	○	<ul style="list-style-type: none"> • us.archive.ubuntu.com:443/TCP • us.archive.ubuntu.com:80/TCP
ホスト名解決のための、センサーの制御インターフェイスから DNS サーバーへのアウトバウンドトラフィック	○	<ul style="list-style-type: none"> • [local DNS server]:53/UDP
リモートトラブルシューティング アプライアンスからのインバウンドトラフィック センサー	不可	<ul style="list-style-type: none"> • 54.83.42.41:22/TCP

i プロキシサービスを使用する場合は、センサー制御インターフェイスの IP アドレスのプロキシ例外を作成します。

ネットワーク デバイス設定

トラフィックのコピーをミラー化してセンサーに渡すようにネットワークスイッチまたはルーターを設定できます。

i センサーは通常のトラフィックフローの外側にあるため、トラフィックに直接影響する可能性はありません。Web ポータルの UI で行った設定変更は、トラフィックフローのあり方ではなくアラートの生成に影響します。アラートに基づいてトラフィックを許可またはブロックするには、ファイアウォール設定を更新します。

ネットワークスイッチの製造元と、ミラー化トラフィックを設定するためのリソースについては、次の資料を参照してください。

製造元	ミラー化トラフィック名	設定例
Cisco	スイッチ ポートアナライザ (SPAN)	『Configuration Examples and TechNotes』
Juniper	ポート ミラー	EX シリーズ スイッチで従業員のリソース使用をローカルでモニターリングするためのポートミラーリングの設定例については、Juniper の TechLibrary ドキュメントを参照してください。
NETGEAR	ポート ミラー	ポートミラーリングの例と、マネージドスイッチでの動作については、Netgear のナレッジベースのドキュメントを参照してください。
ZyXEL	ポート ミラー	ZyXEL スイッチでミラーリングを使用する方法については、ZyXEL のナレッジベースのドキュメントを参照してください。
その他	モニター ポート、アナライザ ポート、タップ ポート	複数のメーカーのスイッチリファレンスについては、Wireshark の wiki ドキュメントを参照してください。

ネットワークテストアクセスポイント(タップ)デバイスを展開してトラフィックのコピーをセンサーに渡すこともできます。ネットワークタップの製造元と、ネットワークタップを設定するためのリソースについては、次の資料を参照してください。

製造元	デバイス名	資料
NetOptics	ネットワークタップ	ドキュメントおよびその他の情報については、Ixia の技術情報ページを参照してください。
Gigamon	ネットワークタップ	ドキュメントおよびその他の情報については、Gigamon のリソースページおよびナレッジページを参照してください。

フロー設定

NetFlow データを渡すようにネットワークデバイスを設定する必要があります。シスコネットワークデバイスでの NetFlow の設定の詳細については、<https://configurenetflow.info/> または https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco_NetFlow_Configuration.pdf を参照してください。

Cisco Defense Orchestrator およびセンサーの展開

Cisco Defense Orchestrator (CDO) を使用して Firepower アプライアンスをネットワークに展開する場合は、シスコのセキュリティ分析とロギング (SaaS) ライセンス (**Firewall Analytics and Monitoring** または **Total Network Analytics and Monitoring**) を購入し、Firepower イベントデータに Secure Cloud Analytics の動的エンティティモデリングを適用できます。詳細については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging を参照してください。

Firewall Analytics and Monitoring または Total Network Analytics and Monitoring のライセンスを使用すると、既存の Secure Cloud Analytics ポータルを CDO の展開に関連付けるか、シスコに新しい Secure Cloud Analytics ポータルをプロビジョニングさせることができます。シスコのセキュリティ分析とロギング (SaaS) を設定すると、Firepower イベントデータ専用の connection-events という名前のセンサーが自動的にプロビジョニングされます。詳細については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging/0201_Request_a_Stealthwatch_Cloud_Portal を参照してください。

Firewall Analytics and Monitoring ライセンスは動的エンティティモデリングを Firepower イベントデータにのみ適用するため、このライセンスのネットワークに追加のセンサーを展開する必要はありません。これに対して、**Total Network Analytics and Monitoring** ライセンスは、Firepower イベントデータとオンプレミス ネットワークトラフィックの両方に動的エンティティモデリングを適用するため、ライセンス機能を最大限に活用するには、追加のセンサーをネットワークに展開します。



CDO の設定を完了しても、Secure Cloud Analytics ポータルに connection-events センサーが表示されない場合は、support@obsrvbl.com にお問い合わせください。

センサーメディアのインストールと設定

センサーを物理アプライアンスにインストールする場合は、.iso ファイルを使用してブート可能メディアを作成し、アプライアンスを再起動してそのメディアから起動する必要があります。

センサーを仮想マシンにインストールする場合は、.iso ファイルから直接起動できます。



インストールプロセスでは、センサーのインストール前に、センサーがインストールされるディスクのデータが消去されます。センサーをインストールする物理アプライアンスや仮想マシン上に、保存が必要なデータがないことを確認してください。

ブートメディアの作成

センサーを物理アプライアンスに展開する場合は、Ubuntu Linux をベースとするセンサーをインストールする .iso ファイルを展開します。

CD や DVD などの光学ディスクに .iso ファイルを書き込む場合は、光学ディスクドライブ内の光学ディスクを使用して物理アプライアンスを再起動し、その光学ディスクから起動することを選択できます。

.iso ファイルと Rufus ユーティリティを使用して USB フラッシュドライブを作成した場合は、物理アプライアンスを再起動し、USB フラッシュドライブを USB ポートに挿入して、USB フラッシュドライブから起動することを選択できます。



ISO を使用せずにセンサーを展開する場合は、トラフィックを許可するようにローカルアプライアンスのファイアウォール設定を更新する必要がある場合があります。提供されている ISO を使用してセンサーを展開することを強くお勧めします。



ブート可能な USB フラッシュドライブを作成すると、フラッシュドライブ上のすべての情報が削除されます。フラッシュドライブに他の情報がないことを確認してください。

センサー ISO ファイルのダウンロード

最新バージョンのセンサー ISO を Web ポータルからダウンロードしてください。これを使用してインストール(新しいセンサーの場合)または再インストール(既存のセンサーをアップグレードする場合)します。

手順

1. Web ポータル UI に管理者アカウントでログインします。
2. [ヘルプ(?) (Help (?))] > [センサーのインストール (Install)] を選択します。
3. .iso のボタンをクリックして最新バージョンの ISO をダウンロードします。

ブート可能な光学ディスクの作成

手順

- 製造元の指示に従って、.iso ファイルを光学ディスクにコピーしてください。

ブート可能な USB フラッシュドライブの作成

はじめる前に

- ブート可能な USB フラッシュドライブを作成するために使用するアプライアンスの USB ポートに空の USB フラッシュドライブを挿入してください。
- ワークステーションにログインしてください。

手順

1. Web ブラウザで、Rufus ユーティリティの Web サイトに移動します。
2. 最新バージョンの Rufus ユーティリティをダウンロードします。
3. Rufus ユーティリティを開きます。
4. [デバイス(Device)] ドロップダウンで USB フラッシュドライブを選択します。
5. [ブートの選択(Boot selection)] ドロップダウンから [ディスクまたは ISO イメージ(Disk or ISO image)] を選択します。
6. [選択(SELECT)] をクリックし、センサー ISO ファイルを選択します。
7. [開始(START)] をクリックします。



ブート可能な USB フラッシュドライブを作成すると、フラッシュドライブ上のすべての情報が削除されます。フラッシュドライブに他の情報がないことを確認してください。

センサーのインストール

はじめる前に

- 物理アプライアンスにインストールする場合は、ブート可能メディアを挿入してアプライアンスを再起動し、ブート可能メディアから起動してください。
- 仮想マシンにインストールする場合は、.iso ファイルから起動してください。

手順

1. 最初のプロンプトで [観測可能なネットワーク アプライアンスのインストール(Install Observable Network Appliance)] を選択し、Enter キーを押します。
2. 矢印キーを使用して言語のリストから **言語を選択**し、Enter キーを押します。
3. 矢印キーを使用して国のリストから **使用場所を選択**し、Enter キーを押します。
4. 次の選択肢があります。
 - 矢印キーを使用して [はい(Yes)] を選択することによって **キーボードを設定**し、Enter キーを押して、**キーボードレイアウト**を選択してから Enter キーを押します。
 - 標準の米国英語キーボードを使用している場合は、[いいえ(No)] を選択してデフォルトを受け入れ、Enter キーを押します。
5. 矢印キーを使用して **キーボードの製造国**を選択し、Enter キーを押します。
6. 矢印キーを使用して **キーボードレイアウト**を選択し、Enter キーを押します。

7. ネットワークを設定し、矢印キーを使用して、制御インターフェイス(センサーを管理し、ネットワークデバイスからフローデータを収集する)として使用するプライマリ ネットワーク インターフェイスを選択し、Enter キーを押します。

i 他のすべてのネットワーク インターフェイスは、自動的にミラー インターフェイスとして設定されます。

8. インストールプロセスによってアプライアンスのコンポーネントが検出されるのを待ち、追加の設定を行います。インストール プロセスでは、DHCP を使用して、選択したプライマリ ネットワーク インターフェイスが制御インターフェイスとして設定されます。ネットワークで DHCP が使用されていない場合は、次の手順を実行します。

ネットワークが DHCP を使用していない場合、またはシステムが「ネットワークの自動設定に失敗しました (Network auto configuration failed)」というメッセージを表示した場合は、次の手順を実行します。

[ネットワークの手動設定 (Configure network manually)] を選択し、Enter キーを押します。

アプライアンスの IP アドレスを入力し、矢印キーを使用して [続行 (Continue)] を選択して、Enter キーを押します。

ネットマスクを入力し、矢印キーを使用して [続行 (Continue)] を選択して、Enter キーを押します。

ゲートウェイルータ IP アドレスを入力し、矢印キーを使用して [続行 (Continue)] を選択して、Enter キーを押します。

最大 3 つのドメイン ネーム サーバー アドレスを入力し、矢印キーを使用して [続行 (Continue)] を選択して、Enter キーを押します。

i デフォルトでは、インストールでは自動的に DHCP が使用され、インストールを続行します。DHCP IP アドレスを上書きするには、インストールの完了後にインターフェイスを手動で編集する必要があります。

i ローカル権威ネームサーバーがネットワークに展開されている場合は、そのアドレスを入力することをお勧めします。

9. 管理者以外の権限用に root 以外のアカウントに関連付けられる新しいユーザーのフルネームを入力し、矢印キーを使用して [続行 (Continue)] を選択して、Enter キーを押します。
10. 管理者以外の権限を持つ root 以外のアカウントである自分のアカウントのユーザー名を入力し、矢印キーを使用して [続行 (Continue)] を選択して、Enter キーを押します。
11. 新しいユーザーのパスワードを選択し、矢印キーを使用して [続行 (Continue)] を選択して、Enter キーを押します。
12. 確認のためにパスワードを再入力し、矢印キーを使用して [続行 (Continue)] を選択して、Enter キーを押します。
同じパスワードを 2 回入力しなかった場合は、やりなおしてください。
13. 矢印キーを使用して [はい (Yes)] を選択してホーム ディレクトリを暗号化し、Enter キーを押します。
14. 矢印キーを使用してタイムゾーンを選択し、Enter キーを押します。

i セットアップ中に作成したアカウントは、仮想マシンへのアクセスに使用できる唯一のアカウントです。このインストールでは、個別の Secure Cloud Analytics ポータルアカウントは作成されません。

15. [ガイド付き – ディスク全体を使用してディスクドライブをパーティション分割 (Guided – use entire disk to partition the disk drive)] を選択し、Enter キーを押します。ディスクの詳細設定を実行する場合は、他のオプションを選択してください。
16. **パーティション分割するディスクを選択し**、Enter キーを押します。
17. 矢印を使用して [パーティション分割を終了して変更をディスクに書き込む (Finish partitioning and write changes to disk)] を選択し、Enter キーを押します。
18. [はい (Yes)] を選択してアクションを確認し、Enter キーを押します。

! このアクションにより、ドライブ上のすべてのデータが削除されます。続行する前にドライブが空であることを確認してください。

インストーラが必要なファイルをインストールするまで数分待ちます。

19. **HTTP プロキシ情報**を入力するか (HTTP プロキシを使用する場合) フィールドを空白のままにして (HTTP プロキシを使用しない場合)、矢印キーを使用して [続行 (Continue)] を選択し、Enter キーを押します。

インストーラが設定を実行するまで待ちます。

20. 矢印キーを使用してリストから更新ポリシーを選択し、Enter キーを押します。[セキュリティ更新の自動インストール (Install security updates automatically)] を選択することをお勧めします。

インストーラが設定を実行し、追加のパッケージをインストールするまで待ちます。

21. **GRUB ブートローダーをマスターブートレコードにインストール**するために矢印キーを使用して [はい (Yes)] を選択し、Enter キーを押します。

インストーラが GRUB ブートローダーをインストールするまで待ち、設定を完了します。

22. インストーラによって「**Installation Complete**」と表示されたら、矢印キーを使用して [続行 (Continue)] を選択し、Enter キーを押してブートメディアを削除してから、設定を完了し、アプライアンスを再起動します。
23. アプライアンスが再起動したら、作成したアカウントでログインし、クレデンシャルが正しいことを確認します。

次の作業

- センサーを使用してネットワークフロートラフィック (NetFlow など) を収集している場合、センサーの設定の詳細については、「[フローデータを収集するセンサーの設定](#)」を参照してください。
- センサーを使用し、SPAN ポートまたはミラーポートに接続して、ミラートラフィックを収集している場合、Secure Cloud Analytics Web ポータルでのセンサー追加の詳細については、「[Web ポータルへのセンサーの接続](#)」を参照してください。
- 拡張 NetFlow テレメトリを送るようにセンサーを設定する場合は、『[Cisco Secure Cloud Analytics Configuration Guide for Enhanced NetFlow](#)』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、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。

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

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

1. 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$
```

2. `identity` IP アドレスをコピーします。
3. センサー からログアウトします。
4. サイト管理者として Web ポータルにログインします。
5. センサー (🌿) アイコン > [パブリック IP (Public IP)] を選択します。
6. [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。

7. [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。

i 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

i 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、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` 設定ファイルを編集し、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。

i 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。

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. 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。

```
Service key: [redacted] 7785YGXksPsBfltfAZuiD7uA3Ya73V8j613bWX
```

3. 管理者としてセンサーに SSH ログインします。
4. 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。

5. # Service Key の下に次の行を追加します。

<service-key> は次のポータル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。

```
observable@ona-e37255: ~
GNU nano 2.5.3 File: opt/obsrvbl-ona/config.local
# Service Key
OBSRVBL_SERVICE_KEY="[redacted]85YGXksPsBfltfAZuiD7uA3Ya73V8j613bWX"
```

6. Ctrl+O を押して変更を保存します。
7. Ctrl+X を押して終了します。
8. 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。

はじめる前に

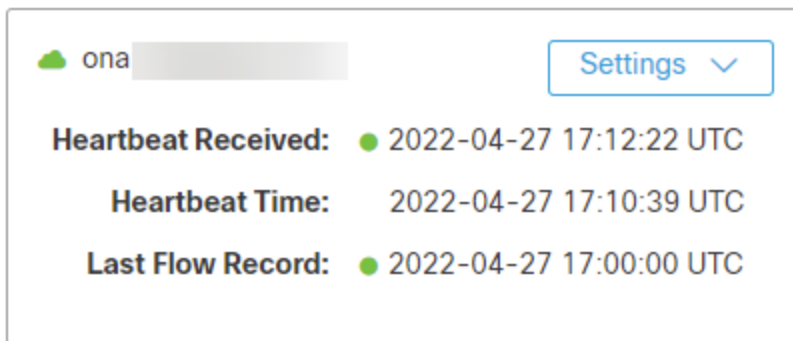
- 管理者としてセンサーに SSH 接続します。

手順

1. 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$
```

2. センサー からログアウトします。
3. ポータル Web UI にログインします。
4. [設定 (Settings)] > [センサー (Sensors)] を選択します。センサーがプロフィールリストに表示されます。



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



Meraki ファームウェアバージョン 14.50 では、Meraki ログエクスポート形式が NetFlow 形式に準拠しています。Meraki デバイスがファームウェアバージョン 14.50 以降を実行している場合は、NetFlow v9 のプローブタイプと Meraki MX のソース (バージョン 14.50+) でセンサーを設定します。Meraki デバイスがファームウェアバージョン 14.50 より前のバージョンを実行している場合は、NetFlow v9 のプローブタイプと Meraki MX のソース (バージョン 14.50 より前) でセンサーを設定します。

フロー収集用のセンサーの設定

はじめる前に

- ポータルの Web UI に管理者アカウントでログインします。

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 (?))] > [センサーのインストール (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 Flexible 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。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。

次の作業

- Cisco Defense Orchestrator (CDO) の **Total Network Analytics and Monitoring** ライセンスを購入し、CDO を Secure Cloud Analytics と統合している場合については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging を参照してください。

トラブルシューティング

センサーからのパケットのキャプチャ

シスコサポートが、センサーに受信されているフローデータを確認することが必要な場合があります。フローのパケットキャプチャを生成して、データを確認することをお勧めします。Wireshark でパケットキャプチャを開いてデータを確認することもできます。

1. センサーに SSH ログインします。
2. プロンプトで「`ifconfig -a`」と入力して Enter キーを押し、インターフェイスのリストを表示します。センサーの制御インターフェイスの名前に注意してください。
3. プロンプトで「`sudo tcpdump -i <control_interface> -n -c 100 "port <port_number>" -w <pcap_name>`」と入力し、<control_interface> を制御インターフェイス名に置き換え、<port_number> を設定済みのフローデータに対応するポート番号に置き換え、<pcap_name> を生成された pcap ファイルの名前と置き換えてから、Enter キーを押します。システムは、指定されたポートを介して、該当するインターフェイスのトラフィックに対して指定された名前を持つ pcap ファイルを生成します。
4. センサーからログアウトします。
5. PuTTY SFTP (PSFTP) または WinSCP などの SFTP プログラムを使用して、センサーにログインします。
6. プロンプトで「`get <pcap_name>`」と入力します。<pcap_name> を生成された pcap ファイル名に置き換えてから Enter キーを押し、ファイルをローカルワークステーションに転送します。

Wireshark でのパケットキャプチャの分析

1. Wireshark をダウンロードしインストールしてから、Wireshark を開きます。
2. [ファイル (File)] > [開く (Open)] を選択してから、pcap ファイルを選択します。
3. [分析 (Analyze)] > [復元方法 (Decode As)] を選択します。
4. [+] をクリックして新しいルールを追加します。
5. [最新 (Current)] ドロップダウンから [CFLOW] を選択して、[OK] をクリックします。UI が更新され、NetFlow、IPFIX、または sFlow に関連したパケットのみが表示されるようになります。結果が表示されない場合は、pcap に NetFlow 関連のパケットが含まれておらず、フローデータ収集がセンサーで正しく設定されていません。

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> 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> 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> を参照してください。
- Secure Cloud Analytics 無料トライアルのガイドなど、インストールおよび設定ガイドについては、<https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html> を参照してください。

変更履歴

リビジョン	改訂日	説明
1.0	2022 年 4 月 27 日	初版

著作権情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、URL: <https://www.cisco.com/go/trademarks> をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1721R)