

Cisco Secure Cloud Analytics

Cisco Telemetry Broker または Cisco Secure Network Analytics から Cisco Secure Cloud Analytics へのオンプレミスフロー送信構成ガイド



目次

はじめに	3
サポートされているフローデータのタイプ	3
Cisco Telemetry Broker 設定	4
前提条件	4
Cisco Telemetry Broker の設定	4
Flow Collector 設定	6
前提条件	6
リソース要件	6
Flow Collector の設定	6
プロキシの構成	7
検証	9
サポートへの問い合わせ	10
変更履歴	11

はじめに

このガイドでは、オンプレミスフローデータが Cisco Telemetry Broker または Secure Network Analytics (以前の Stealthwatch) から Cisco Secure Cloud Analytics (以前の Stealthwatch Cloud) に送信されるように構成する方法について説明します。

i オンプレミスフローデータを Secure Cloud Analytics に送信するには、Cisco Telemetry Broker を使用することをお勧めします。または、フローデータを直接 Secure Cloud Analytics に送信するようにフローコレクタを構成できます。詳細については、「[フローコレクタのリソース要件](#)」を参照してください。

サポートされているフローデータのタイプ

Cisco Telemetry Broker または Flow Collector を使用して Secure Network Analytics から Secure Cloud Analytics に送信されるフローデータのタイプは次のとおりです。

- IPFIX パケット
- NetFlow v5 (Cisco Telemetry Broker v1.3 以降)
- NetFlow v9 (Cisco Telemetry Broker v1.3 以降)


i Network Visibility Module (NVM) のデータは Secure Cloud Analytics ではサポートされていません。Secure Network Analytics の展開で NVM データを取り込む場合は、専用のフローベースのテレメトリ Flow Collector を使用してオンプレミスフローデータを送信し、別の Flow Collector を使用して NVM データを取り込むことをお勧めします。

Cisco Telemetry Broker 設定

次の手順を使用して、オンプレミスフローデータを Secure Cloud Analytics に送信するように Cisco Telemetry Broker を構成します。1 秒あたりのフロー数 (FPS) が 50,000 を超える環境では、この方法を使用することをお勧めします。

前提条件

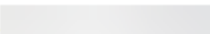
- Secure Cloud Analytics アカウント
- Cisco Telemetry Broker v1.2 以降

 Cisco Telemetry Broker を展開するには、『[Cisco Telemetry Broker Virtual Appliance Deployment and Configuration Guide](#)』[英語] の手順に従います。

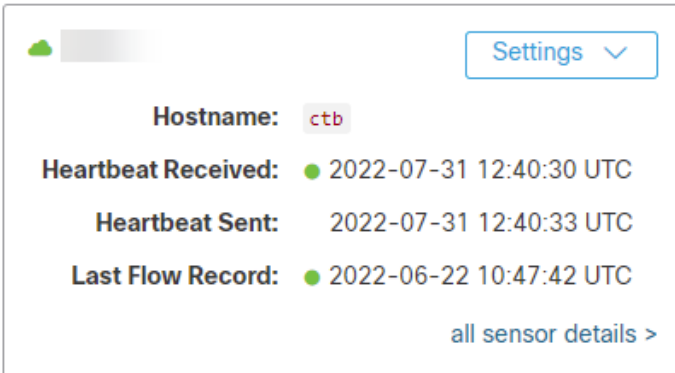
Cisco Telemetry Broker の設定

1. Secure Cloud Analytics Web ポータルにログインします。
2. [設定 (Settings)] > [センサー (Sensors)] をクリックします。
3. ページの一番下までスクロールし、サービスキーとサービスホストの情報を保存します。

Service key: 

Service host: https://  .obsrvbl.com

4. Cisco Telemetry Broker にログインします。
5. ページの右上隅で、[宛先の追加 (Add Destination)] > [SCA宛先 (SCA Destination)] をクリックします。
6. 宛先の [名前 (Name)] を入力します。
7. [SCAサービスキー (SCA Service Key)] を入力します。必ずキー全体を貼り付けてください。
8. [SCAホストURL (SCA Host URL)] を入力します。必ず URL 全体を貼り付けてください。
9. [保存 (Save)] をクリックします。
10. Secure Cloud Analytics ポータルの [センサー (Sensors)] ページに戻ります。センサーリストに含まれている Telemetry Broker のホスト名と情報が表示されます。



Settings ▾

Hostname: `ctb`

Heartbeat Received: ● 2022-07-31 12:40:30 UTC

Heartbeat Sent: ● 2022-07-31 12:40:33 UTC

Last Flow Record: ● 2022-06-22 10:47:42 UTC

[all sensor details >](#)



宛先の構成の詳細については、『[Cisco Telemetry Broker User Guide](#)』[英語]を参照してください。

Flow Collector 設定

次の手順を使用して、オンプレミスフロー データを Secure Cloud Analytics に送信するように Flow Collector を構成します。

! オンプレミスフローデータを送信するように Cisco Telemetry Broker を構成している場合は、Flow Collector を構成する必要はありません。ネットワークのエリアごとにフローデータを Secure Cloud Analytics にエクスポートする必要があるのは 1 回だけです。

前提条件

- Secure Cloud Analytics アカウント
- Secure Network Analytics Flow Collector v7.4.1

リソース要件

オンプレミスフローデータを Flow Collector から Secure Cloud Analytics に直接送信する場合は、Flow Collector に次のリソースを割り当てておくことをお勧めします。

1 秒あたりのフロー数 (FPS)	必須予約済みメモリ	必須予約済み CPU	必須最小データストレージ
最大 50,000	70 GB	8	200 GB

i 50,000 FPS を超える環境では、オンプレミスフローデータを送信するように [Cisco Telemetry Broker](#) を構成することをお勧めします。



Flow Collector の設定

1. Secure Cloud Analytics Web ポータルにログインします。
2. [設定 (Settings)] > [センサー (Sensors)] をクリックします。
3. ページの一番下までスクロールし、サービスキーとサービスホストの情報を保存します。

Service key: _____

Service host: https:// _____ .obsrvbl.com


4. SSH で Flow Collector に root としてログインします。
5. センサーの構成フォルダまで移動するには、次のコマンドを入力します。
`cd /lancope/var/containers/sna-sca-sensor/config/`
6. `sna-sca-sensor.conf` ファイルを開きます。
7. 手順 3 で保存したサービスキーとサービスホストをコピーして貼り付けます。
`sca_key = 「サービスキー」`
`sca_url = 「サービスホスト」`

 インターネットプロキシの構成方法については、 ([ユーザ (User)]) アイコン をクリックし、[ヘルプ (Help)] > [インターネットプロキシ (Internet Proxy)] をクリックします。IP アドレス、ポート、およびプロキシログイン情報は、ネットワークに固有です。サポートが必要な場合は、ネットワーク管理者にご連絡ください。


Appliance Configuration - Flow Collector

Appliance **Network Services** General

Internet Proxy **Modification Requires Reboot**

 Confirm your DNS server is configured.

Proxy Setup

Enable 

IP Address *

Port *

Proxy Login Credentials (if applicable)

User Name

Password

Authentication Type

basic

ntlm

Domain

6. [設定の適用 (Apply settings)] をクリックします。
7. 画面に表示される指示に従って操作します。アプライアンスが自動的に再起動します。

検証

次の手順を使用して、Secure Cloud Analytics がオンプレミスフローデータを受信していることを確認します。

i 構成後、30 分以内に Cisco Telemetry Broker または Flow Collector からのフローレコードが Secure Cloud Analytics に表示されるようになります。表示されない場合は、[シスコサポート](#)までご連絡ください。

1. Secure Cloud Analytics Web ポータルにログインします。
2. [調査 (Investigate)] > [イベントビューア (Event Viewer)] に移動します。
3. [セッションの詳細 (Session Details)] をクリックします。

Secure Cloud Analytics Monitor Investigate Report Settings

Event Viewer

Session Traffic Rejected Traffic Cloud Posture Azure Activity Logs AWS CloudTrail ISE **Session Details** Passive DNS

2022-07-08 22:41:55 GMT+5:30 | 2022-07-08 23:41:55 GMT+5:30 Q switch to query-mode above to enable

Timestamp	Start Time	sourceIPv4Address	destinationIPv4Address	sourceTransportPort
▶ 2022-03-11 14:26:44 EST	2020-03-17 14:07:12 UTC	↔ [redacted]	[redacted]	56254
▶ 2022-03-11 14:26:44 EST	2020-03-17 14:07:12 UTC	↔ [redacted]	[redacted]	51808
▶ 2022-03-11 14:26:44 EST	2020-03-17 14:07:12 UTC	🇨🇦 [redacted]	[redacted]	53 (domain)

4. Cisco Telemetry Broker または Flow Collector からのフローレコードが表示されます。

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>

変更履歴

リビジョン	改訂日	説明
1.0	2022年3月31日	初版
2.0	2022年8月8日	Cisco Telemetry Broker 構成を追加。
2.1	2022年11月3日	ドキュメントのタイトルと概要セクションを更新。

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)