Cisco Telemetry Broker

Cisco Telemetry Broker v2.0.1 ユーザーガイド

目次

はじめに

このガイドでは、Cisco Telemetry Broker マネージャの Web インターフェイスのリファレンスを提供します。

Cisco Telemetry Broker（このドキュメントでは CTB と呼ぶこともある）では、多くの入力からネットワークテレメトリを取得し、テレメトリ形式を変換して、それらのテレメトリを 1 つまたは複数の宛先に転送できます。

対象読者

このガイドは、ネットワーク テレメトリ フローの維持とネットワークテレメトリのモニタリングを担当する担当者を対象としています。

ユーザー補助機能の設定

利用可能な Web サイトユーザー補助機能を設定するためのアクセス権を持つには、Cisco Telemetry Broker マネージャの Web インターフェイスを使用するときにブラウザとして Chrome を使用する必要があります。次に、Chrome 以外のブラウザを使用している場合に設定できないユーザー補助機能の例を示します（これらがすべてではありません）。

次のことを実行する機能：

- Web ページの各項目を強調表示する
- コンパクトタブバーに色を表示する
- 特定のフォントサイズを使用しないように指定する

略語

このガイドでは、次の略語が使用されます。

省略形	説明
DMZ	非武装地帯（境界ネットワーク）
DNS	ドメイン ネーム サーバ
FC	Flow Collector
FS	Flow Sensor
FTP	ファイル転送プロトコル
Gbps	ギガビット/秒
GB	ギガバイト
HTTPS	Hypertext Transfer Protocol（Secure）

省略形	説明
ISE	Identity Services Engine
Mbps	メガビット/秒
NAT	ネットワーク アドレス変換
NIC	ネットワーク インターフェイス カード
NTP	ネットワーク タイム プロトコル
PCIe	Peripheral Component Interconnect Express; ペリフェラル コンポーネント インターコネクト エクスプレス
SNMP	Simple Network Management Protocol（簡易ネットワーク管理プロトコル）
SPAN	スイッチ ポート アナライザ
SSH	セキュア シェル
TAP	テスト アクセス ポート
UDPD	UDP Director
UPS	無停電電源
URL	ユニバーサル リソース ロケータ
USB	Universal Serial Bus
VLAN	仮想ローカル エリア ネットワーク
VM	仮想マシン

共通用語

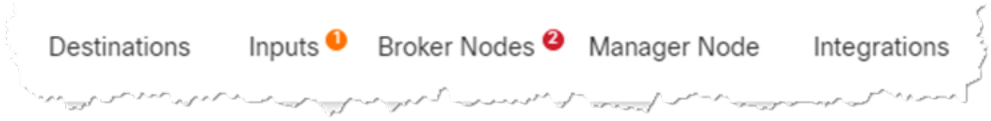
このガイドでは、次の用語が使用されます。

省略形	説明
宛先	Cisco Telemetry Broker がテレメトリを転送する場所。Cisco Telemetry Broker は、複数のタイプの宛先をサポートしています。
エクスポータ	Cisco Telemetry Broker の入力にトラフィックを転送する、お客様のネットワーク上のデバイス。エクスポータは、通常、IP アドレスによって定義されます。

省略形	説明
入力	Cisco Telemetry Broker がお客様のネットワークからテレメトリを収集または受信する方法。Cisco Telemetry Broker は、複数のタイプの入力をサポートしています。
ルール	単一の入力から単一の宛先にテレメトリを転送する方法を Cisco Telemetry Broker に指示するユーザー定義のロジック。
テレメトリ	分析のために役立つ、お客様によって生成されるあらゆるタイプのデータ。UDP パケット、IPFIX、syslog、JSON などがあります。

アラート

エンティティ（設定済みの宛先、入力、またはブローカーノード）に対して 1 つ以上のアラートが存在する場合、関連付けられたメインメニューの見出しの横に、番号とともにステータスインジケータが表示されます。



この数は、アラートがあるエンティティカテゴリ内のエンティティの数を反映しています。[入力（Inputs）] ページのステータスインジケータは、入力の 3 つのサブページ（[UDP入力（UDP Inputs）]、[仮想プライベートクラウド（VPC）フローログ（Virtual Private Cloud（VPC）Flow Logs）]、および [Microsoftネットワーク セキュリティ グループ（NSG）フローログ（Microsoft Network Security Group（NSG）Flow Logs）]）ごとにさらに分類されます。これらの各ページには、問題のあるエンティティごとにステータスインジケータが表示されます。

エンティティに複数の問題がある場合（たとえば、宛先に同時に到達できず、ルールがない場合や、入力に宛先がなく、非アクティブになっている場合など）、Cisco Telemetry Broker ではこの 1 つの問題が考慮されます。既存の問題の個々の数に基づいて問題の数を計算することはありません。したがって、たとえば、1 つのエンティティに 5 つの異なる問題がある場合、Cisco Telemetry Broker はこれを 5 つの問題ではなく 1 つの問題と見なします。

概要

このページには、Cisco Telemetry Broker システムの構成設定、システムの状態、主要なメトリック、およびライセンス情報のスナップショットが表示されます。

[概要(Overview)] ページへのアクセス

Cisco Telemetry Broker メインメニューから [概要(Overview)] を選択するか、Cisco ロゴ(ページの左上隅)をクリックします。

各種コンポーネントの表示

[入力(Inputs)]

このコンポーネントは、次の情報の過去 24 時間のテレメトリを表示します。

- Cisco Telemetry Broker で設定されている入力の数。
- すべての入力から受信したテレメトリの量。
- この平均値は、過去 30 日間のテレメトリから計算されます。
- ルールが設定されていない入力の数。この数は、[宛先なし(No Destination)] フィールドの数で表されます。
- ドーナツグラフの各セグメントには、各入力から受信したテレメトリの量が表示されます。このグラフのセグメントにカーソルを合わせると、次の情報を表示できます。
    - 入力名
    - 過去 24 時間に特定の入力から受信したテレメトリの量

[宛先(Destinations)]

このコンポーネントは、次の情報の過去 24 時間のテレメトリを表示します。

- Cisco Telemetry Broker で設定されている宛先の数。
- すべての宛先に送信されたテレメトリの量。
- すべての宛先に送信されたテレメトリの 1 日あたりの平均レート。この平均値は、過去 30 日間のテレメトリから計算されます。
- 送信されるテレメトリを受け入れない宛先の数([到達不能(Unreachable)] フィールドの数で表されます)。この番号をクリックすると、[宛先(Destinations)] ページが開きます。到達できない宛先は、ここにリストされています。
- ドーナツグラフの各セグメントには、各宛先に送信されたテレメトリの量が表示されます。このグラフのセグメントにカーソルを合わせると、次の情報を表示できます。
    - 宛先名
    - 過去 24 時間にこの特定の宛先に送信されたテレメトリの量

ブローカーノード

このセクションは、関連付けられたクラスタ名の下でクラスタごとにグループ化されます。高可用性クラスタが存在しない場合、すべてのブローカノードは「クラスタなし」のサブ見出しの下にグループ化されます。

- 各弧は、ノードの理論上の容量に対するブローカノードの受信レートの割合を示します。弧は、該当する色でマークされています。弧の色の説明については、次の表を参照してください。

色	定義
赤（重大）	ブローカノードで到達した容量の割合は 100% です。
オレンジ（警告）	ブローカノードで到達した容量の割合は 80% から 99.99% です。
青（情報）	ブローカノードで到達した容量の割合は 80% 未満です。

- ブローカノードのページにアクセスするには、ノードの名前をクリックします。
- ブローカノードにアラートがある場合は、ノードの下に表示されます。それらは、赤い背景に白い X でマークされ、簡単な説明が付いています。

アラート

アラートコンポーネントには、発生して、アクティブなアラート、または解決済みのアラートの最新の 10 個が一覧表示されます。赤色のアラートはまだアクティブで、灰色のアラートは解決済みです。リストは、一番上にある最新のアラートが先頭で、一番下にある最も古いアラートが最後です。追加のアラートを表示するには、リストの下部にある [もっと見る...（See more...）] リンクをクリックします。

- このコンポーネントの右上隅には、Cisco Telemetry Broker の未解決アラートの数とすべてのアラートの数が表示されます。
- デフォルトでは、すべての未解決アラートのリストが表示されます。すべてのアラートのリストを表示するには、このコンポーネントの右上隅にある [すべて（All）] フィルタオプションをクリックします。
- 各アラートの下には、関連付けられたエンティティ（ブローカノードや宛先など）に関する情報と、アラートが発生した時刻が表示されます。
- アラートが無効になった（解決された）場合、アラートは次のように表示されます。
    - グレー表示されます
    - チェックマークが付きます
    - 解決した時期が記されます
- 各アラート名の下に表示されるリンクをクリックすると、アラートタイプに応じて、関連付けられている [ブローカノード（Broker Node）] ページまたは [宛先（Destinations）] ページが開きます。

CPU

マネージャノードと各ブローカノードの両方について、このコンポーネントは次の情報の過去 30 日間のテレメトリを表示します。

- 使用可能な CPU の数。
- 使用可能な CPU の使用率（バーの色で表されます）。

- 各ブローカーノードの使用可能な CPU の番号ごとに、1 分間の負荷平均（このデータを表示するには、ブローカーノード名にカーソルを合わせます）。

各バーに表示される色の説明については、次の表を参照してください。

色	定義
赤（重大）	ノードで到達した最大 CPU 負荷の割合は 100% です。
オレンジ（警告）	ノードで到達した最大 CPU 負荷の割合は 80% から 99.99% です。
青（情報）	ノードで到達した最大 CPU 負荷の割合は 80% 未満です。

ライセンス

このコンポーネントは、過去 14 日間のテレメトリを表示します。

- 青い点線は、過去 7 日間の 1 日あたりの平均 GB を示しています。この数値を表示するには、点線にカーソルを合わせます。この番号は、ライセンス料を計算するためにスマート ソフトウェア ライセンシングに送信される資格番号であり、[Telemetry Brokerスマートライセンシング（Telemetry Broker Smart Licensing）] ページに表示される値と一致します。
- グラフの各棒は、異なる日を表します。グラフの右端にあるバーは前日を表し、さらに左に移動するごとに 1 日ずつさかのぼります。
- 特定の日に受信した正確な GB 数を表示するには、対応するバーの上にカーソルを置きます。このバーに関連付けられた日付も表示されます。
- 製品がまだ登録されていない場合、右上隅に警告が表示され、トライアルライセンスの期限が切れるまでの日数が示されます。

テレメトリフロー

このコンポーネントは、過去 24 時間のテレメトリを表示します。

- すべての入力（グラフの左側のテレメトリで表示）によって受信され、すべての宛先（右側のテレメトリで表示）に送信されたさまざまなタイプのテレメトリ。
- フローの正確な値を表示するには、フローにカーソルを合わせてツールチップを開きます。
- SCA 宛先の場合、ここに表示されるテレメトリ統計は、SCA に送信された非圧縮データを表します。したがって、これらの統計は、送信される実際のテレメトリ（宛先コンポーネントで表される）と釣り合わない可能性があります。

メトリック

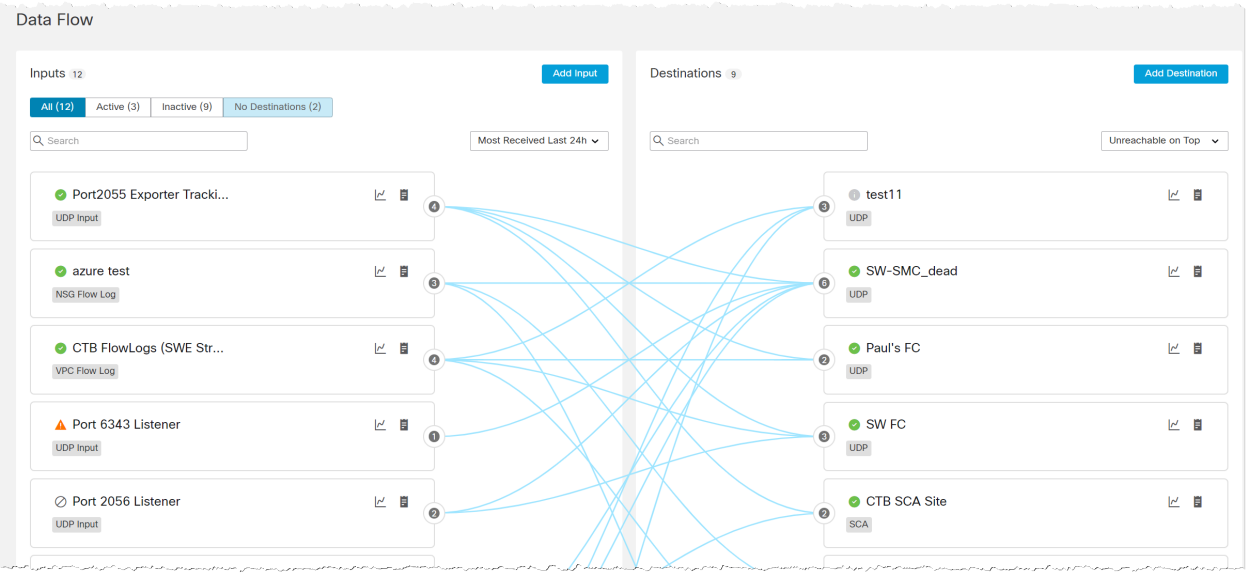
このコンポーネントのテーブルには、次の情報の過去 24 時間のデータが表示されます。

[合計受信レート（Total Received Rate）] すべての入力から受信したテレメトリの合計量。

[合計送信レート（Total Sent Rate）] すべての宛先に送信されたテレメトリの合計量。

[データフロー（Data Flow）]

このページを使用して、どの入力がどの宛先に割り当てられているか簡単に確認できます。1 つの入力に複数の宛先を割り当てることができ、1 つの宛先を複数の入力に割り当てることができる点に注意してください。このページでは、設定した入力と宛先に関連するアラート、データフロー情報、およびその他の詳細も確認できます。



データフローの表示

さまざまな入力と宛先をつなぐラインは、それらの入力と宛先の間に存在するルールを表しています。ルールの追加については、「**宛先**」の章の「宛先のルールの追加」を参照してください。

特定の入力または宛先のカードをクリックするか、それにカーソルを合わせると、入力または宛先のデータフローが表示されます。

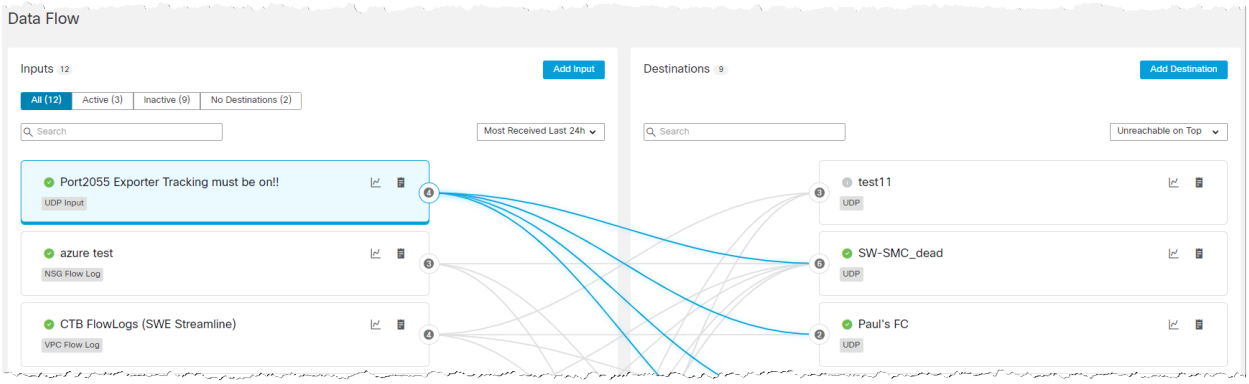
> カードの選択を解除するには、カードをもう一度クリックするか、カードの外側の任意の場所をクリック（別のカードのクリックも含む）します。

カードをクリックしたときとマウスオーバーしたときの視覚的な変化について、次の表を参照してください。これらの視覚的な変化により、選択したカードに関連する情報をより簡単に確認できます。

クリックとマウスオーバーの比較

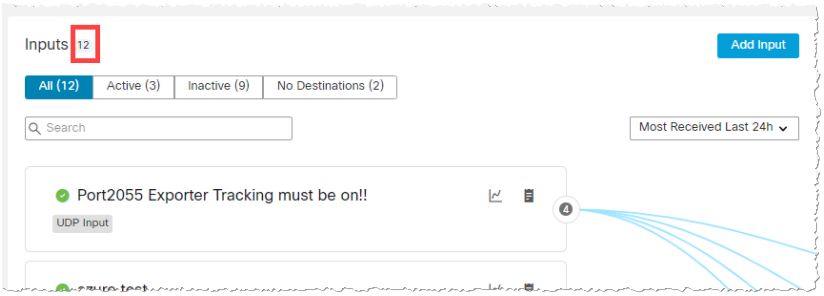
実行する操作	結果
カードをクリックする	• カードの縁が濃い青に変わります。 • カード内が明るい青に変わります。 • 入力または宛先のデータフローラインが濃い青に変わります。[データフロー(Data Flow)] ページの他のすべてのラインがグレーに変わります。
カードをマウスオーバーする	• カードの縁が濃い青に変わります。 • カード内は白のままです。 • 入力または宛先のデータフローラインが濃い青に変わります。[データフロー(Data Flow)] ページの他のすべてのラインは明るい青のままです。
カードをクリックしてから、別のカードをマウスオーバーする	• カードの縁が濃い青に変わります。 • カード内は白のままです。 • 入力または宛先のデータフローラインが濃い青に変わります。[データフロー(Data Flow)] ページの他のすべてのラインはグレーのままです。 • クリックしたカードは、選択された状態を保持します。

例: 下の画像では、ユーザーが [入力(Inputs)] リストの最初の入力カードをクリックしています。

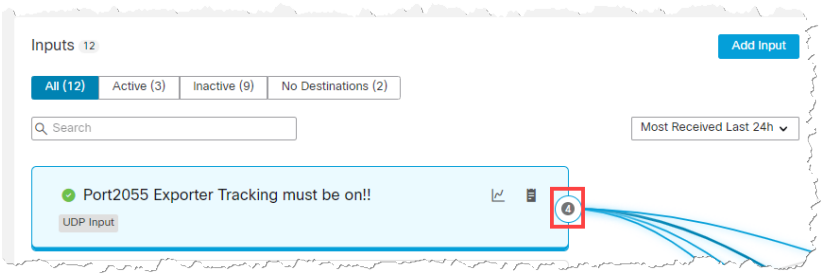


スナップショット情報の表示

設定済み入力と宛先の総数

設定済み総数を表示する対象	丸で囲まれた番号が表示される場所
入力	[入力(Inputs)]リストの上部にある[入力(Inputs)]タイトルの横。 
宛先	[宛先(Destinations)]リストの上部にある[宛先(Destinations)]タイトルの横。 

割り当済み入力と宛先の合計

総数を表示する対象	丸で囲まれた番号が表示される関連項目
特定の入力に割り当てられた宛先	入力カード。 
特定の宛先に割り当てられた入力	宛先カード。 

データフローレート

入力または宛先に関する以下の情報を表示するには、カーソルを (グラフ)アイコンの上に置きます。次の情報が表示されます。

- 過去 24 時間にこの入力から受信したすべてのテレメトリの受信レート。
- 過去 24 時間にこの宛先に送信されたすべてのテレメトリの送信レート。

[詳細(Details)]

入力または宛先の詳細情報を表示するには、 (詳細)アイコンをクリックします。

詳細アイコンをクリックする項目

- 入力カード。その入力の [入力(Inputs)] ページが開きます。
- 宛先カード。その宛先の [宛先(Destinations)] ページが開きます。

アラートとステータスインジケータ

特定の入力または宛先の既存のアラートまたはステータスインジケータの説明を表示するには、関連するアイコンの上にカーソルを置きます。Cisco Telemetry Broker アラートのリストについては、「**付録 B:サポートされるアラート**」を参照してください。

入力または宛先の検索

次のエンティティのいずれかを使用して、検索結果をフィルタリングできます。

[フィルタ（Filter）] ボタン

[All（すべて）]、[アクティブ（Active）]、[非アクティブ（Inactive）]、および [宛先なし（No Destination）]（どの宛先にも割り当てられていない入力）のいずれかのフィルタを使用して、検索をフィルタ処理できます。フィルタを選択するには、[Inputs（入力）] リストの上部にある関連のボタンをクリックします。

> 1 つ以上のフィルタを使用する場合は、すべてのフィルタの論理積がとられるため、返される結果はすべて、すべてのフィルタの検索条件と一致する必要があります。

検索フィールド

検索フィールドに、（使用しているリストに応じて）検索する入力または宛先の名前を入力します。エントリの入力を開始すると、フィールドが動的にフィルタ処理され、入力した文字を含むエントリの一覧が表示されます。

同じ名前の複数の入力を作成でき、複数の宛先mo使用できることに注意してください。ブローカーノード間でポート番号を重複することもできます。したがって、同じ名前が複数ある入力または宛先を検索したり、2 つ以上のブローカーノードで重複しているポート番号を検索すると、検索の処理の終了後に、一致するすべてのエントリが [データフロー（Data Flow）] ページに表示されます。

フィルタのクリア

- 1 つ以上の結果が表示されても、検索している項目が表示されない場合は、設定されているフィルタの数が多すぎる可能性があります。この場合は、一度に 1 つずつフィルタを削除して、意図した結果が表示されるかどうかを確認することをお勧めします。
- 結果が表示されない場合は、[フィルタのクリア（Clear Filter）] をクリックして、検索条件を再設定します。

ソートオプション

これらのドロップダウンリストを使用して、[Inputs（入力）] リストと [宛先（duplicated）] リストの両方でデータをソートできます。

Inputs（入力）] リスト [Inputs（入力）] リスト内で、[最も多く受信した過去24時間（Most Received Last 24h）] ドロップダウンリストのオプションを変更します。他のオプションは、次のとおりです。

- 最も直近で観察された
- 最も宛先が多い
- 最も高い受信レート

[宛先（duplicated）] リスト [宛先（duplicated）] リスト内で、[上位の到達不能（Unreachable on Top）] ドロップダウンリストのオプションを変更します。他のオプションは、次のとおりです。

- [最高送信レート（Highest Sent Rate）]
- [最も多く送信した過去 24 時間（Most Sent Last 24h）]
- [最も新しく追加（Most Recently Added）]

入力の追加

入力を追加するには、[入力(Inputs)]リストの右上隅にある[入力の追加(Add Input)]をクリックします。

入力を追加する方法については、以下にリストされている(追加する入力のタイプに応じて)該当するトピックを参照してください。

- UDP 入力
- VPC フローログ
- NSG フローログ

宛先の追加

宛先を追加するには、[宛先(Destinations)]リストで、ページの右上隅にある[宛先の追加(Add Destination)]をクリックします。

宛先を追加する方法については、「宛先」を参照してください。

宛先

Cisco Telemetry Broker は、次のタイプの宛先へのテレメトリの送信をサポートしています。

- **UDP 宛先**：特定の IP アドレスおよびポートで UDP データを受信する宛先。
- **SCA 宛先**：お客様が所有する Secure Cloud Analytics アカウントにデータを送信する宛先。

  SCA 宛先を設定すると、（アップロードされた FPS に関して）システムのパフォーマンスが制限される可能性があります。この要因として考えられるのは、フローレコードのサイズ、それらのフロー レコードで達成可能な圧縮、およびブローカーノードから Secure Cloud Analytics にテレメトリを送信するために使用可能な帯域幅です。

  ほとんどの状況で（フローレコードあたり 100 バイト未満と想定）、Cisco Telemetry Broker は次の情報を送信できます。

  - 仮想展開の場合、ブローカノードあたり 40K FPS の送信が可能です（ブローカノードあたり 8 つのコアが存在すると想定）。
  - ハードウェア展開（M6）の場合、ブローカノードあたり 300K FPS の送信が可能です。

Cisco Telemetry Broker は、テレメトリを宛先に送信します。ルールは、宛先が特定のテレメトリストリームから受信するテレメトリを記述します。

[Cisco Telemetry Broker 宛先（Cisco Telemetry Broker Destinations）] ページには、すべての宛先のグラフが表示されます。宛先ごとに、次の情報を確認できます。

- 宛先名
- IP アドレスとポート（UDP 宛先のみ）
- 過去 1 日に受信したテレメトリ
- 宛先がアクティブにテレメトリを受信しており、マネージャノードにより到達可能であるかどうか
- テレメトリを宛先に送信する入力およびエクスポータ

このページから宛先を追加できます。また、変更や更新も可能です。宛先ごとに、ルールを追加し、異なるテレメトリ入力からテレメトリを受信できます。宛先ごとに複数のルール（ルールごとに 1 つのテレメトリ入力）を設定できます。

到達可能性チェック

到達可能性チェック機能は、到達不能または応答不能な宛先についてユーザーに警告し、存在しない宛先へのテレメトリの転送によって引き起こされるネットワークのダメージを軽減します。

この機能は、長さゼロの UDP パケットを作成し、宛先の設定済み UDP ポートに送信します。次に、ブローカーノードは ICMP Host Unreachable または Port Unreachable 応答をリッスンして、宛先が到達不能かどうかを判断します。応答がない場合は、宛先がテレメトリを受信している可能性が高いことを示します。

到達可能性チェック機能は、Secure Cloud Analytics ではない宛先に対してのみ使用できます。この機能は、宛先ごとに無効に設定できます。宛先の設定やファイアウォールルールの設定によって誤検出アラートが発生する場合は、この機能を無効にします。

この設定の方法については、「**宛先の詳細**」の「UDP 宛先の追加」または「到達可能性チェックの設定」のトピックを参照してください。

テレメトリ入力を Cisco Telemetry Broker が非アクティブとしてマークするまでの時間を設定する方法については、「**全般**」を参照してください。

宛先の追加

UDP 宛先の追加

1. ページの右上隅で、[宛先の追加（Add Destination）] > [UDP宛先（UDP Destination）] をクリックします。
2. 宛先の [名前（Name）] を入力します。
3. この宛先の [宛先IPアドレス（Destination IP Address）] と [宛先UDPポート（Destination UDP Port）] を入力します。
4. 到達不能または応答不能な宛先のアラートを受け取るには、  （[到達可能性チェック（Reachability Check）]）アイコンを有効にします（有効にするとバーが青色になります）。到達可能性チェック機能の詳細については、次を参照してください。

> - 到達可能性チェック機能は、Secure Cloud Analytics ではない宛先に対してのみ使用できます。
> - 宛先の設定やファイアウォールルールの設定によって誤検出アラートが発生する場合は、この機能を無効にします。

5. [保存（Save）] をクリックします。

Secure Cloud Analytics（SCA）宛先の追加

> - Cisco Telemetry Broker では、システムごとに 1 つの SCA 宛先のみを追加できます。
> - Cisco Telemetry Broker は、NetFlow V5、NetFlow V9、および IPFIX パケットからフローデータを抽出し、このデータを Secure Cloud Analytics に送信します。
> - Cisco Telemetry Broker 環境にテレメトリが少ない場合は、SCA 宛先を追加してからテレメトリが [宛先（Destinations）] ページに表示されるまでに最大 20 分かかることがあります。

SCA 宛先を追加する前に、SCA サービスキーと SCA ホスト URL を取得する必要があります。Secure Cloud Analytics がこのキーを使用して Cisco Telemetry Broker を認証し、Cisco Telemetry Broker が URL を使用してテレメトリを Secure Cloud Analytics に送信します。

キーと URL の確認

1. Cisco Secure Cloud Analytics にログインします。
2. メインメニューから [設定（Settings）] > [センサー（Sensor）] をクリックします。
3. ページの下部にあるサービスキーとサービスホストを見つけてコピーします。

SCA 宛先の追加

1. Cisco Telemetry Broker にログインします。
2. 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。
3. 宛先の [名前（Name）] を入力します。
4. [SCAサービスキー（SCA Service Key）] を入力します。キー全体を貼り付けてください。
5. [SCAホストURL（SCA Host URL）] を入力します。URL 全体を貼り付けてください。
6. [保存（Save）] をクリックします。

Cisco Telemetry Broker 宛先として Secure Cloud Analytics を設定すると、30 分以内に Secure Cloud Analytics イベントビューアで Cisco Telemetry Broker からのテレメトリを確認できるようになります。そうならない場合は、ポータル URL を使用して swatchc-support@cisco.com に連絡して支援を受けてください。

宛先の編集

1. 該当する宛先を含む行で、  （[編集（Edit）]）アイコンをクリックします。
2. 開いた [デバイスの編集（Edit Device）] ダイアログボックスで、次のフィールドを更新します。
   - UDP 宛先の場合：[宛先名（Destination Name）] および [宛先のアベイラビリティの確認（Check Destination Availability）] トグルスイッチ。[宛先IPアドレス（Destination IP Address）] フィールドと [宛先UDPポート（Destination UDP Port）] フィールドは編集できません。
   - SCA 宛先の場合：[宛先名（Destination Name）]、[SCA APIキー（SCA API Key）]、および [SCA URL]。
3. [保存（Save）] をクリックします。

宛先の削除

宛先を削除した場合でも、その宛先は引き続きメトリックグラフで選択できますが、その宛先に関連付けられている名前は、「Destination」という用語の後に宛先 ID と「deleted」という語句が続きます。たとえば、Destination (ID 10) deleted となります。削除された宛先のデータが存在する限り、グラフには削除された宛先のデータが引き続き含まれます。データの期限が切れると、関連付けられた宛先は、[宛先ごと（Per Destination ）] ドロップダウンリスト（[ブローカノード（Broker Nodes）] ページ）では選択できなくなります。

宛先を削除するには、次の手順を実行します。

1. 該当する宛先を含む行で、  （[削除（Remove）]）アイコンをクリックします。
2. 開いた [宛先の削除（Remove Destination）] ダイアログで、[削除（Remove）] をクリックします。

宛先のルールの追加

> ルールは、常に、1 つの入力と 1 つの宛先だけで構成されます。ただし、入力は複数の特定の宛先にデータを送信できることに注意してください。これは、別のルールを作成するだけで実現できます。

1. 該当する宛先を含む行で、左下隅にある [+ルールの追加（+ Add Rule）] をクリックします。
2. [入力の選択（Select Input）] ドロップダウンリストで、目的の入力名を選択します。
3. （条件付き）UDP 入力を選択すると、[これらのサブネットに対して受信したデータを追跡する（Track data received against these subnets）] フィールドが開きます。このフィールドは、宛先に送信されるトラフィックを決定するためのフィルタメカニズムとして機能します。指定されたサブネット内のエクスポータ IP からのトラフィックのみが転送されます。この宛先が該当するテレメトリを受信するサブネットを入力します。エントリはカンマで区切ります。

   [これらのサブネットに対して受信したデータを追跡する（Track data received against these subnets）] フィールドを空のままにすると、デフォルトで、すべてのトラフィックを含む単一のサブネットに設定されます。

   - IPv4 IP サブネットの場合、CIDR IP アドレス範囲は 0.0.0.0/0 になります。
   - IPv6 IP サブネットの場合、CIDR IP アドレス範囲は ::/0 になります。

4. [Add Rule] をクリックします。

宛先の詳細の表示

特定の宛先に関する詳細情報を表示できます。これを実行するには、行の左上隅にある目的の宛先名をクリックします。このページの詳細については、次のセクション「**宛先の詳細**」を参照してください。

宛先の詳細

このページで、特定の宛先に関する詳細情報を表示できます。宛先の詳細を表示するには、次の手順を実行します。

- [宛先（Destinations）] タブで、行の左上隅にある目的の宛先名をクリックします。

  その宛先の [宛先の詳細（Destination Details）] ページが開きます。

このページでは次の情報を確認できます。

- テレメトリの受信に使用する宛先名、IP アドレス、およびポート（UDP 宛先のみ）。
- 宛先のタイプ（SCA 宛先のみ）。
- 宛先のステータスと最後にテレメトリを受信した時刻。
- この宛先がテレメトリを受信しているテレメトリ入力の数。
- Cisco Telemetry Broker から受信したバイト数と受信レート（ビット/秒）。
- この宛先に設定されたルールと、各ルールの詳細（単一ノードまたは複数ノードのいずれかで設定されている、特定の入力にデータを送信するように設定されたエクスポータの数など）（この数は、[ルール（Rules）] テーブルの [エクスポータ（Exporters）] 列に表示されます）。

  この数は、[入力の詳細（Input Details）] ページに表示される数（[エクスポータ（Exporters）] セクションの左上隅にあるタイトル [エクスポータ（Exporters）] に続くカッコ内）に表示される数とは必ずしも一致しないことに注意してください。こちらも、特定の入力にデータを送信するように設定された一意のエクスポータの数です。これらの数が一致するかどうかを判断するには、以下を参照してください。

- 同じ入力で設定されている単一のノードにデータを送信するように単一のエクスポータが設定されている場合、これらの数は一致します。
- 同じ入力で設定されている 2 つのノードにデータを送信するように単一のエクスポータが設定されている場合、[宛先の詳細(Destinations Details)] ページに表示される数は、[入力の詳細(Input Details)] ページに表示される数の 2 倍になります。
- 同じ入力で設定されている 3 つのノードにデータを送信するように単一のエクスポータが設定されている場合、[宛先の詳細(Destinations Details)] ページに表示される数は、[入力の詳細(Input Details)] ページに表示される数の 3 倍になります(以下同様)。

> これらの数が一致しない状況はほとんど発生しません。この問題を回避するため、1 つのブローカノードまたは 1 つのクラスタのみで入力を設定することをお勧めします。あるいは、同じ UDP ポートでリッスンするものの、異なるブローカノードまたはクラスタに割り当てられる 2 つの別個の UDP 入力を作成することもできます。

メトリック:送信レート

[メトリック(Metrics)] セクションに、[送信レート(Sent Rate)] テーブルが表示されます。このテーブルには、テレメトリをフィルタ処理するために使用できる次のフィルタごとに、入力が一定期間にわたってこの宛先に送信したテレメトリが示されます(各ドロップダウンリストから複数のオプションを選択できます)。

> SCA 宛先の場合は、ブローカーノードごとか総受信量ごとにのみ、このテーブルのテレメトリをフィルタ処理できます。

- テレメトリタイプごと
- 入力ごと
- エクスポータごと
- ブローカーノードごと
- 総量

[メトリック(Metrics)] テーブルの右上隅にある次の時間枠から目的のものをクリックすると、その時間枠でこれらのメトリックを表示できます。

- 過去 1 時間
- 過去 4 日間
- 過去 1 日
- 過去 1 週間
- 過去 1 ヵ月

到達可能性チェック

到達不能または応答不能な宛先のアラートを受け取るには、ページの右上隅にある  ([到達可能性チェック(Reachability Check)])アイコンを有効にします(有効にするとバーが青色になります)。到達可能性チェック機能の詳細については、「**宛先**」の「到達可能性チェック」のセクションを参照してください。

- 到達可能性チェック機能は、Secure Cloud Analytics ではない宛先に対してのみ使用できます。
- 宛先の設定やファイアウォールルールの設定によって誤検出アラートが発生する場合は、この機能を無効にします。

宛先の編集

1. ページの右上隅で、  （[宛先の編集（Edit Destination）]）をクリックします。
2. 開いた [デバイスの編集（Edit Device）] ダイアログボックスで、次のフィールドを更新します。
   - UDP 宛先の場合：[宛先名（Destination Name）] および [宛先のアベイラビリティの確認（Check Destination Availability）] トグルスイッチ。[宛先IPアドレス（Destination IP Address）] フィールドと [宛先UDPポート（Destination UDP Port）] フィールドは編集できません。
   - SCA 宛先の場合：[宛先名（Destination Name）]、[SCA APIキー（SCA API Key）]、および [SCA URL]。
3. [保存（Save）] をクリックします。

宛先の削除

宛先を削除した場合でも、その宛先は引き続きメトリックグラフで選択できますが、その宛先に関連付けられている名前は、「Destination」という用語の後に宛先 ID と「deleted」という語句が続きます。たとえば、Destination (ID 10) deleted となります。削除された宛先のデータが存在する限り、グラフには削除された宛先のデータが引き続き含まれます。データの期限が切れると、関連付けられた宛先は、[宛先ごと（Per Destination ）] ドロップダウンリスト（[ブローカノード（Broker Nodes）] ページ）では選択できなくなります。

宛先を削除するには、次の手順を実行します。

1. ページの右上隅で、  （[宛先の削除（Remove Destination）]）アイコンをクリックします。
2. 開いた [宛先の削除（Remove Destination）] ダイアログで、[削除（Remove）] をクリックします。

宛先のルールの追加

ルールは、常に、1 つの入力と 1 つの宛先だけで構成されます。ただし、入力は複数の特定の宛先にデータを送信できることに注意してください。これは、別のルールを作成するだけで実現できます。

1. [ルール（Rules）] セクションで、[+ルールの追加（+ Add Rule）] をクリックします。
2. [入力の選択（Select Input）] ドロップダウンリストで、目的の入力名を選択します。
3. （条件付き）UDP 入力を選択すると、[これらのサブネットに対して受信したデータを追跡する（Track data received against these subnets）] フィールドが開きます。このフィールドは、宛先に送信されるトラフィックを決定するためのフィルタメカニズムとして機能します。指定されたサブネット内のエクスポータ IP からのトラフィックのみが転送されます。この宛先が該当するテレメトリを受信するサブネットを入力します。エントリはカンマで区切ります。

[これらのサブネットに対して受信したデータを追跡する（Track data received against these subnets）] フィールドを空のままにすると、デフォルトで、すべてのトラフィックを含む単一のサブネットに設定されます。

- IPv4 IP サブネットの場合、CIDR IP アドレス範囲は 0.0.0.0/0 になります。
- IPv6 IP サブネットの場合、CIDR IP アドレス範囲は ::/0 になります。

4. [Add Rule] をクリックします。

入力

Cisco Telemetry Broker は、次のタイプの入力からのテレメトリの送信をサポートしています。

- **UDP 入力**：UDP テレメトリを消費し、それを宛先に送信する入力。
- **VPC フローログ**：s3 バケットから Amazon Web Services（AWS）PVC フローログを消費し、それらを IPFIX に変換して、その IPFIX を宛先に送信する入力。
- **NSG フローログ**：Azure ストレージアカウントから Azure NSG フローログを消費し、それらを IPFIX に変換して、その IPFIX を宛先に送信する入力。

各種の入力のタブにアクセスするには、Cisco Telemetry Broker メインメニューから［入力（Inputs）］を選択します。

> ⚠ テレメトリの収集を開始するには、まず Cisco Telemetry Broker 内に 1 つ以上の入力を作成する必要があります。

Cisco Telemetry Broker で処理するテレメトリのタイプに基づいて入力を設定する必要があります。たとえば、すべてのブローカーノードのポート 2055 で UDP パケットを収集する場合は、ポート 2055 でリッスンするように設定された UDP 入力を作成する必要があります。また、VPC フローログテレメトリのみを処理する場合は、VPC フローログ入力を作成する必要があります。

入力の表示

1. Cisco Telemetry Broker メインメニューから［入力（Inputs）］を選択します。
2. 該当するタブをクリックして、次のいずれかを表示します。
   - UDP 入力
   - VPC フローログ
   - NSG フローログ

UDP 入力

Cisco Telemetry Broker では、着信 UDP テレメトリを特定の UDP ポートでリッスンするように UDP 入力を設定できます。［入力（Input）］タブには次の情報が表示されます。

- 入力名、入力ポート、および受信したテレメトリのタイプ
- 入力のステータスと最後にテレメトリを受信した時刻
- 割り当てられているブローカーノードおよびクラスタ
- この入力に関して設定されている宛先の数
- 過去 24 時間の受信バイト数およびレート（バイト/秒）

このテレメトリは、さまざまな条件でフィルタリングできます。ページ上部のドロップダウンメニューから、次の条件タイプのいずれかを選択します。

- 最も多く受信した過去 24 時間
- 最も直近で観察された
- 最も宛先が多い
- 最も高い受信レート

[検索(Search)]フィールドのプレースホルダテキストは、検索を実行できる列を示します。エントリの入力を開始すると、テーブルが動的にフィルタ処理され、入力した文字を含むエントリのリストが表示されます。

UDP 入力の追加

1. [入力(Inputs)]タブで、[UDP入力(UDP Inputs)]タブをクリックします。
2. ページの右上隅で、[UDP入力の追加(Add UDP Input)]をクリックします。

   [UDP入力の追加(ADD UDP Input)]ダイアログが開きます。
3. [UDPポート(UDP Port)]フィールドに、UDP テレメトリをリッスンする UDP ポートを入力します。
4. [UDP入力名(UDP Input name)]に、この入力の名前を入力します。
5. Cisco Telemetry Broker は、テレメトリを UDP 入力に送信するすべてのエクスポータを追跡します。ただし、単一の UDP 入力にテレメトリを送信する多数の一意のエクスポータがあるときは、システムのパフォーマンスの問題が発生しないように、エクスポータの追跡を無効にする必要がある場合があります。

   エクスポータの追跡を無効にするには、[UDP入力の追加(Add UDP Input)]ダイアログ(手順 2 で開くダイアログ)で [エクスポータの追跡を無効にする(Disable Exporters Tracking)]チェックボックスをオンにします。エクスポータの追跡を無効にすると、エクスポータごとのメトリックが計算されなくなります。それでも、UDP 入力によってまだ処理されている集約メトリックを表示することはできます。ただし、システムには下記の制限が生じます。

   - **[入力の詳細(Input Details)]ページ** [エクスポータ(Exporters)]セクションには、エクスポータごとのデータメトリックが表示されなくなります(このページは、[UDP入力(UDP Inputs)]タブで入力名をクリックすると開きます)。ただし、関連付けられた入力に関して設定された各ブローカノードで確認されたエクスポータの数は表示されます。
   - **[ブローカーノードの詳細(Broker Nodes Details)]ページ**:[受信レート(Received Rate)]グラフの [エクスポータごと(Per Exporter)]ドロップダウンリストには、エクスポータの追跡が無効になっている UDP 入力からのエクスポータが含まれなくなります(このページは、[ブローカーノード(Broker Nodes)]タブでブローカーノード名をクリックすると開きます)。

> エクスポータの追跡の詳細については、「**UDP 入力の詳細**」の「エクスポータ」のセクションを参照してください。

5. [HAクラスタの割り当て(Assign HA Clusters)]セクションで、この入力を追加する HA クラスタについて、該当するチェックボックスをオンにします。
6. [ブローカーノードの割り当て(Assign Broker Nodes)]セクションで、この入力を追加するノードについて、該当するチェックボックスをオンにします。

> このダイアログの [HAクラスタの割り当て(Assign HA Cluster)]セクションで [HAクラスタ(HA Cluster)]オプションにノードが含まれている場合、そのノードは [ブローカーノードの割り当て(Assign Broker Nodes)]セクションには表示されず、その逆も同様です。

7. [保存(Save)]をクリックします。

UDP 入力の編集

1. 該当する UDP 入力を含む行で、  （[編集（Edit）]）アイコンをクリックします。
2. 開いた [UDP入力の編集（Edit UDP Input）] ダイアログで編集を行い、[保存（Save）] をクリックします。

UDP 入力の削除

入力を削除すると、Cisco Telemetry Broker は、指定されたポートでのテレメトリの受信を停止し、この入力に関連付けられたすべてのルールを削除します。

その入力は引き続きメトリックグラフで選択できますが、その入力に関連付けられている名前は、「Input」という用語の後に入力 ID と「deleted 」という語句が続きます。たとえば、Input（ID 10）deleted などです。削除された入力のデータが存在する限り、グラフには削除された入力のデータが引き続き含まれます。データの期限が切れると、関連付けられた入力は、[入力ごと（Per Input）] ドロップダウンリスト（[宛先（Destinations）] ページと [ブローカノード（Broker Nodes）] ページ）では選択できなくなります。

UDP 入力を削除するには、次の手順を実行します。

1. 該当する UDP 入力を含む行で、  （[削除（Remove）]）アイコンをクリックします。
2. [UDP入力の削除（Remove UDP Input）] ダイアログで、[削除（Remove）] をクリックします。

UDP 入力の詳細の表示

特定の UDP 入力に関する詳細情報を表示できます。これを行うには、該当する UDP 入力を含む行で、入力名をクリックします。このページの詳細については、次のセクション「**UDP 入力の詳細**」を参照してください。

UDP 入力の詳細

このページでは、UDP 入力に関する詳細情報を表示できます。UDP 入力の詳細を表示するには、次の手順を実行します。

- [UDP入力（UDP Inputs）] タブの該当する UDP 入力を含む行で、入力名をクリックします。

  その入力の [UDP入力の詳細（UDP Input Details）] ページが開きます。

このページでは次の情報を確認できます。

全般

- UDP 入力の表示名、受信する UDP ポート、および割り当てられているブローカノードとクラスタ
- UDP 入力のステータス（これは、この UDP 入力のポートが現在テレメトリを受信しているかどうかを示します）
- UDP 入力に割り当てられている宛先の数
- 過去 24 時間の Cisco Telemetry Broker からの受信バイト数およびレート（バイト/秒）

ルール（Rules）

この UDP 入力に割り当てられているルールのリスト（各ルールの宛先の IP アドレスとポートを含む）。SCA 宛先に関連付けられているルールについては IP アドレスがリストされていないことに注意してください。

[エクスポータ(Exporters)]

特定のポートに割り当てられている個別のエクスポータに関する次の情報を表示できます。

- 特定の入力にデータを送信するように設定された一意のエクスポータの数。この数は、[エクスポータ(Exporters)] セクションの左上隅にあるタイトル [エクスポータ(Exporters)] に続くカッコ内に表示されます。
- エクスポータ名。
- 受信したテレメトリのタイプ。
- エクスポータのステータス(これは、この UDP 入力のポートが現在このエクスポータからテレメトリを受信しているかどうかを示します)。
- エクスポータに割り当てられている宛先の数。
- 過去 24 時間の受信バイト数およびレート(バイト/秒)。

[検索(Search)] フィールドのプレースホルダテキストは、検索を実行できるエンティティを示します。エントリの入力を開始すると、テーブルが動的にフィルタ処理され、入力した文字を含むエントリのリストが表示されます。

Cisco Telemetry Broker は、テレメトリを UDP 入力に送信するすべてのエクスポータを追跡します。ただし、単一の UDP 入力にデータを送信する多数の一意のエクスポータがあるときは、システムのパフォーマンスの問題が発生しないように、エクスポータの追跡を無効にする必要がある場合があります。

エクスポータの追跡を無効にするには、[エクスポータの追跡を無効にする(Disable Exporters Tracking)] チェックボックスをオンにします。

エクスポータの追跡を無効にすると、エクスポータごとのメトリックが計算されなくなります。それでも、UDP 入力によってまだ処理されている集約メトリックを表示することはできます。ただし、システムには制限が生じます。これらの制限の詳細については、「**UDP 入力**」の「UDP 入力の追加」のセクションを参照してください。

エクスポータごとにメトリックスが計算されなくなっても、そのエクスポータのデータは、[保持間隔(Retention Interval)] で設定された期間データが存在する限り表示されます。

例: [保持間隔(Retention Interval)] は 8 日です。エクスポータは 8 月 10 日にデータの送信を停止しましたが、8 月 10 日から 18 日までのデータを保持しています。今日は 8 月 20 日です。

- 7 日間または 30 日間のチャートをフィルタリングすると、8 月 10 ～ 18 日が 7 ～ 30 日前に含まれるため、グラフには引き続きそのエクスポータのデータが表示されます。
- 4 時間または 24 時間のチャートをフィルタリングすると、8 月 10 日から 18 日が過去 48 時間の範囲外になるため、そのエクスポータのデータはチャートに表示されなくなります。

指標: 受信率

[メトリック(Metrics)] セクションに、[受信レート(Received Rate)] テーブルが表示されます。このテーブルには、テレメトリをフィルタ処理するために使用できる次のフィルタごとに、宛先がこの UDP 入力から一定期間にわたって受信したテレメトリが表示されます。各ドロップダウンリストから複数のオプションを選択できます。

- エクスポータごと
- ブローカーノードごと

[メトリック(Metrics)] テーブルの右上隅にある次の時間枠から目的のものをクリックすると、その時間枠でこれらのメトリックを表示できます。

- 過去 1 時間
- 過去 4 日間
- 過去 1 日
- 過去 1 週間
- 過去 1 ヵ月

UDP 入力の編集

1. ページの右上隅で、  ([UDP入力の編集(Edit UDP Input)]) アイコンをクリックします。
2. 開いた [UDP入力の編集(Edit UDP Input)] ダイアログで編集を行い、[保存(Save)] をクリックします。

> UDP ポートは編集できません。

UDP 入力の削除

入力を削除すると、Cisco Telemetry Broker は、指定されたポートでのテレメトリの受信を停止し、この入力に関連付けられたすべてのルールを削除します。

その入力は引き続きメトリックグラフで選択できますが、その入力に関連付けられている名前は、「Input」という用語の後に入力 ID と「deleted 」という語句が続きます。たとえば、Input (ID 10) deleted などです。削除された入力のデータが存在する限り、グラフには削除された入力のデータが引き続き含まれます。データの期限が切れると、関連付けられた入力は、[入力ごと(Per Input)] ドロップダウンリスト([宛先(Destinations)] ページと [ブローカノード(Broker Nodes)] ページ) では選択できなくなります。

UDP 入力を削除するには、次の手順を実行します。

1. ページの右上隅で、  ([UDP入力の削除(Remove UDP Input)]) アイコンをクリックします。
2. 開いた [UDP入力の削除(Remove UDP Input)] ダイアログで、[削除(Remove)] をクリックします。

VPC フローログ

Cisco Telemetry Broker では、S3 バケットから AWS VPC フローログを消費し、IPFIX に変換し、IPFIX を宛先に送信するように、VPC フローログ入力を設定できます。これらの入力は、[VPCフローログ(VPC Flow Logs)] タブのテーブルから管理できます。このタブでは、システムの既存の各入力と次のような関連情報を表示できます

- 名前、IPv4 または IPv6 アドレス、および S3 バケット名
- 入力のステータスと最後にテレメトリを受信した時刻
- 割り当てられているブローカーノードおよびクラスタ
- この入力に関して設定されている宛先の数
- 過去 24 時間の受信バイト数およびレート(バイト/秒)

このテレメトリは、次の期間について表示できます。いずれかのオプションを、ページの右上にあるドロップダウン メニューから選択します。

- 最も多く受信した過去 24 時間
- 最も直近で観察された
- 最も宛先が多い
- 最も高い受信レート

[検索（Search）] フィールドのプレースホルダテキストは、検索を実行できる列を示します。エントリの入力を開始すると、テーブルが動的にフィルタ処理され、入力した文字を含むエントリのリストが表示されます。

VPC フローログの追加および編集

VPC フローログを追加および編集する方法については、「**統合**」セクションを参照してください。

VPC フローログの編集

1. 該当する VPC フローログを含む行で、  （[編集（Edit）]）アイコンをクリックします。
2. 開いた [VPCフローログの編集（Edit VPC Flow Log）] ダイアログで編集を行い、[保存（Save）] をクリックします。

VPC フローログの削除

1. 該当する VPC フローログを含む行で、  （[削除（Remove）]）アイコンをクリックします。
2. [VPCフローログの削除（Remove VPC Flow Log）] ダイアログで、[削除（Remove）] をクリックします。

VPC フローログの詳細の表示

特定の VPC フローログに関する詳細情報を表示できます。これを行うには、該当する VPC フローログを含む行で、フローログ名をクリックします。このページの詳細については、次のセクション「**VPC フローログの詳細**」を参照してください。

VPC フローログの詳細

このページでは、VPC フローログに関する詳細情報を表示できます。VPC フローログの詳細を表示するには、次の手順を実行します。

- [VPCフローログ（VPC Flow Logs）] タブの該当する VPC フローログを含む行で、入力名をクリックします。

  そのフローの [VPCフローログの詳細（VPC Flow Log Details）] ページが開きます。

このページでは次の情報を確認できます。

全般

次の情報が表示されます。

- 入力名、S3 バケット、リージョン、および該当する場合は、テレメトリの受信に使用される割り当て済みのブローカーノード
- 入力のステータスと最後にテレメトリを受信した時刻

- この入力に関して設定されている宛先の数
- 過去 24 時間の受信バイト数およびレート（バイト/秒）

ルール（Rules）

この VPC フローログに割り当てられているルールのリスト（各ルールの宛先の IP アドレスとポートを含む）。SCA 宛先に関連付けられているルールについては IP アドレスがリストされていないことに注意してください。

メトリック：受信レート

[メトリック（Metrics）] セクションに、[受信レート（Received Rate）] テーブルが表示されます。このテーブルには、テレメトリをフィルタ処理するために使用できる次のフィルタごとに、宛先がこの VPC フローログから一定期間にわたって受信したテレメトリが表示されます。各ドロップダウンリストから複数のオプションを選択できます。

- ブローカーノードごと
- 次の異なる時間枠での受信レート：
  - 過去 1 時間
  - 過去 4 日間
  - 過去 1 日
  - 過去 1 週間
  - 過去 1 ヵ月

VPC フローログの編集

1. ページの右上隅で、  （[VPCフローログ（Edit VPC Flow Log）]）アイコンをクリックします。
2. 開いた [VPCフローログの編集（Edit VPC Flow Log）] ダイアログで編集を行い、[保存（Save）] をクリックします。

VPC フローログの削除

1. ページの右上隅で、  （[VPCフローログの削除（Remove Edit VPC Flow Log）]）アイコンをクリックします。
2. 開いた [VPCフローログの削除（Remove VPC Flow Log）] ダイアログで、[削除（Remove）] をクリックします。

NSG フローログ

Cisco Telemetry Broker では、Azure ストレージアカウントから Azure NSG フローログを消費し、IPFIX に変換し、IPFIX を宛先に送信するように、NSG フローログ入力を設定できます。これらの入力は、[NSGフローログ（NSG Flow Logs）] タブのテーブルから管理できます。このタブでは、システムの既存の各入力と次のような関連情報を表示できます。

- 入力名、IPv4 または IPv6 アドレス、および BLOB サービス SAS URL
- 入力のステータスと最後にテレメトリを受信した時刻
- 割り当てられているブローカーノードおよびクラスタ

- この入力に関して設定されている宛先の数
- 過去 24 時間の受信バイト数およびレート（バイト/秒）

このテレメトリは、次の期間について表示できます。いずれかのオプションを、ページの右上にあるドロップダウン メニューから選択します。

- 最も多く受信した過去 24 時間
- 最も直近で観察された
- 最も宛先が多い
- 最も高い受信レート

[検索（Search）] フィールドのプレースホルダテキストは、検索を実行できる列を示します。エントリの入力を開始すると、テーブルが動的にフィルタ処理され、入力した文字を含むエントリのリストが表示されます。

NSG フローログの追加

> ⚠ このセクションでは、NSG フローログを有効にするように Azure アカウントを設定していることを前提としています。Azure アカウントの設定手順については、「**Azure の設定**」を参照してください。

1. [入力（Inputs）] ページで、[NSGフローログ（NSG Flow Logs）] タブをクリックします。
2. ページの右上隅で、[NSGフローログの追加（Add NSG Flow Log）] をクリックします。
3. [BLOBサービスSAS URL（Blob Service SAS URL）] フィールドに、Azure アカウントの NSG フローログを設定したときに取得した Azure sas_url を入力します。
4. [入力名（Input Name）] フィールドに、入力 IP アドレス名を入力します。
5. [入力IPアドレス（Input IP Address）] フィールドに、このフローログに割り当てる入力 IP アドレスを入力します。Cisco Telemetry Broker は、NSG フローログから生成された IPFIX を送信するときに、この IP アドレスを入力アドレスとして使用します。これは内部 IP アドレスである必要があり、ネットワーク上の他の IP アドレスと競合しないようにする必要があります。

   Cisco Telemetry Broker では、パケットの適切なブローカーリングを保証するために、入力 IP アドレス値に次の制約があります。次のいずれかの条件が満たされていない場合は、Cisco Telemetry Broker に次のエラーメッセージが表示されます。

   - 入力 IP アドレスは、[割り当て済みノード（Assigned Node）] のテレメトリインターフェイスのサブネットと重複してはいけません。
   - 入力 IP アドレスは、システム内の既存の入力 IP アドレスと競合してはいけません。
   - 入力 IP アドレスは、システム内の宛先 IP アドレスと競合してはいけません。
6. [割り当て済みブローカーノード（Assigned Broker Node）] ドロップダウンリストから、割り当て済みブローカーノードを選択します。このブローカーノードは、ストレージアカウントからのすべてのフローログテレメトリを処理します。
7. フローログテレメトリを取り込む 1 つ以上の宛先を選択します。Cisco Telemetry Broker は、NSG フローログを IPFIX に変換することに注意してください。
8. [保存（Save）] をクリックします。

NSG フローログの編集

該当する NSG フローログを含む行で、  （[編集（Edit）]）アイコンをクリックします。
開いた [NSGフローログの編集（Edit NSG Flow Log）] ダイアログで編集を行い、[保存（Save）] をクリックします。

NSG フローログの削除

該当する NSG フローログを含む行で、  （[削除（Remove）]）アイコンをクリックします。
[NSGフローログの削除（Remove NSG Flow Log）] ダイアログで、[削除（Remove）] をクリックします。

NSG フローログの詳細の表示

特定の NSG フローログに関する詳細情報を表示できます。これを行うには、該当する NSG フローログを含む行で、フローログ名をクリックします。このページの詳細については、次のセクション「**NSG フローログの詳細**」を参照してください。

NSG フローログの詳細

このページでは、NSG フローログに関する詳細情報を表示できます。NSG フローログの詳細を表示するには、次の手順を実行します。

- [NSGフローログ（NSG Flow Logs）] タブの該当する NSG フローログを含む行で、入力名をクリックします。

  そのフローログの [NSGフローログの詳細（NSG Flow Log Details）] ページが開きます。

このページでは次の情報を確認できます。

全般

次の情報が表示されます。

- 入力名、BLOB サービス SAS URL、URL の有効期限、および該当する場合は、テレメトリの受信に使用される割り当て済みのブローカーノード
- 入力のステータスと最後にテレメトリを受信した時刻
- この入力に関して設定されている宛先の数
- 過去 24 時間の受信バイト数およびレート（バイト/秒）

ルール（Rules）

この NSG フローログに割り当てられているルールのリスト（各ルールの宛先の IP アドレスとポートを含む）。SCA 宛先に関連付けられているルールについては IP アドレスがリストされていないことに注意してください。

メトリック：受信レート

[メトリック（Metrics）] セクションに、[受信レート（Received Rate）] テーブルが表示されます。このテーブルには、テレメトリをフィルタ処理するために使用できる次のフィルタごとに、宛先がこの NSG フローログから一定期間にわたって受信したテレメトリが表示されます。各ドロップダウンリストから複数のオプションを選択できます。

- ブローカーノードごと

- 次の異なる時間枠での受信レート:
  - 過去 1 時間
  - 過去 4 日間
  - 過去 1 日
  - 過去 1 週間
  - 過去 1 ヵ月

NSG フローログの編集

1. ページの右上隅で、  （[NSGフローログ（Edit NSG Flow Log）]）アイコンをクリックします。
2. 開いた [NSGフローログの編集（Edit NSG Flow Log）] ダイアログで編集を行い、[保存（Save）] をクリックします。

NSG フロー ログの削除

1. ページの右上隅で、  （**[NSGフローログの削除（Remove NSG Flow Log）]**）アイコンをクリックします。
2. 開いた [NSGフローログの削除（Remove NSG Flow Log）] ダイアログで、[削除（Remove）] をクリックします。

ブローカーノード

[Cisco Telemetry Broker ノードの概要（Cisco Telemetry Broker Nodes Overview）] には、以下を含むすべてのブローカーノードの詳細が表示されます。

- ブローカーノード名
- 管理インターフェース（管理ネットワーク）IPv4/IPv6 アドレス
- テレメトリインターフェイス IPv4/IPv6 アドレス
- ブローカーノードの容量
- ブローカーノードが所属するハイ アベイラビリティ クラスタ（存在する場合）
- 受信および送信レート（bps）
- ブローカーノードのステータスと、マネージャノードがブローカーノードと最後に通信した時刻

このテレメトリは、次の条件でフィルタリングできます。ページ上部のドロップダウンメニューから、次の条件タイプのいずれかを選択します。

- 最も高い受信レート
- 最も直近で観察された

[検索（Search）] フィールドのプレースホルダテキストは、検索を実行できる列を示します。エントリの入力を開始すると、テーブルが動的にフィルタ処理され、入力した文字を含むエントリのリストが表示されます。

クラスタの追加

クラスタ関連の情報とタスクについては、「**ハイ アベイラビリティ クラスタ**」と「**クラスタのタスク**」を参照してください。

ブローカーノードの詳細の表示

特定のブローカノードに関する詳細情報を表示できます。これを行うには、該当する行で、[ブローカノード名（Broker Node Name）] 列の目的のブローカノード名をクリックします。このページの詳細については、次のセクション「**ブローカノードの詳細**」を参照してください。

ブローカノードの詳細

ブローカーノードの詳細を表示するには、次の手順を実行します。

- [ブローカーノード（Broker Nodes）] ページの [ブローカーノード（Broker Nodes）] テーブルにある [ブローカーノード名（Broker Node Name）] 列で、該当するブローカーノード名をクリックします。

[一般情報（General）] セクションでは、次の情報を確認できます。

- ホスト名と管理ネットワーク IP アドレス
- 入力のステータスと最後にテレメトリを受信した時刻
- 過去 24 時間の受信レート（バイト/秒）
- 過去 24 時間の送信レート（バイト/秒）

[テレメトリインターフェイス（Telemetry Interface）] セクションには、次の情報が含まれています。

- インターフェイス インデックス
- Interface name
- [MACアドレス(MAC Address)]
- PCI アドレス
- 容量(bps)
- IPv4 アドレス/マスク
- IPv4 ゲートウェイアドレス
- IPv6 アドレス/マスク
- IPv6 ゲートウェイ/アドレス
- インターフェイス MTU(バイト)

ブローカノードの編集

ブローカノードを編集するには、次の手順を実行します。

1. [テレメトリインターフェイス(Telemetry Interface)] セクションの ([編集(Edit)]) アイコンをクリックして、必要な変更を行います。
2. [保存(Save)] をクリックします。

ブローカーノードの削除

マネージャノードからブローカーノードを削除すると、そのブローカーノードはデータベースから削除され、以前に割り当てられた入力および宛先のいずれにも割り当てられなくなります。そのブローカーノードは引き続きメトリックグラフで選択できますが、そのノードに関連付けられた名前は変更されて、「Broker Node」という用語の後に入力 ID と「deleted」という語句が続きます。たとえば、Broker Node (ID 10) deleted となります。

削除されたブローカーノードのデータが存在する限り、グラフには削除されたブローカーノードのデータが引き続き含まれます。データの期限が切れると、関連付けられたブローカーノードは、[ブローカーノードごと(Per Broker Node)] ドロップダウンリスト([宛先(Destinations)] ページと [入力(Inputs)] ページ)では選択できなくなります。

ブローカー ノードの削除について次のルールがあります。

- 設定情報が確実に削除されるようにするには、`ctb-manage` を実行して、[非アクティブ化(deactivate)] を選択する必要があります。
- 前の箇条書きで説明されているアクションを実行しない場合、ブローカーノードは以前保存された設定で引き続き実行され、マネージャーノードに統計は送信されません。
- 以前削除したブローカーノードを同じマネージャーノードにもう一度追加する場合は、このノードを新しいアプライアンスとして設定する必要があります(テレメトリ IP アドレスの割り当て、入力の割り当てなど)。

ブローカノードを削除するには、次の手順を実行します。

1. 右上隅にある ([ブローカノードの削除(Remove Broker Node)]) アイコンをクリックします。
2. [削除(Remove)] ダイアログで、[削除(Remove)] をクリックします。

メトリック

ここでは、メトリック情報について詳しく説明します。[メトリック(Metrics)] セクションには、このブローカーノードが受信する一定期間のテレメトリが、入力ごとと宛先ごとの両方で表示されます。

[受信レート(Received Rate)] テーブル

このテーブルには、テレメトリをフィルタ処理するために使用できる次のフィルタごとに、このブローカーノードが一定期間にわたって受信したテレメトリが表示されます。各ドロップダウンリストから複数のオプションを選択できます。

- 入力ごと
- エクスポータごと

- [キャパシティとの比較(Compare to Capacity)]トグルアイコンが無効になっている場合( )、該当する入力から受信されたテレメトリの現在の受信レート値(1 分間隔)を表示できます。(最初に、テーブルの右上隅にある時間枠オプションバーから [過去 1 時間(Last 1h)] をクリックする必要があります)。x 軸(時間を表す水平線)の上にカーソルを合わせると、時刻の特定の分を確認できます。

- [キャパシティとの比較(Compare to Capacity)]トグルアイコンが有効になっている場合( )、しきい値と比較した受信レート値を表示できます。しきい値の 90% を超えるレートは調査の必要があります。これらは懸念される状況であるためです。

テーブルの右上隅にある次の時間枠から目的のものをクリックすると、その時間枠でこれらのメトリックを表示できます。

- 過去 1 時間
- 過去 4 日間
- 過去 1 日
- 過去 1 週間
- 過去 1 ヵ月

[送信レート(Sent Rate)] テーブル

このテーブルには、このブローカーノードが [宛先単位(Per Destination)] ドロップダウンリストで選択した宛先に一定期間にわたって送信したテレメトリが表示されます。

- [キャパシティとの比較(Compare to Capacity)]トグルアイコンが無効になっている場合( )、該当する宛先に送信されたテレメトリの現在の送信レート値(1 分間隔)を表示できます。(最初に、テーブルの右上隅にある時間枠オプションバーから [過去 1 時間(Last 1h)] をクリックする必要があります)。x 軸(時間を表す水平線)の上にカーソルを合わせると、時刻の特定の分を確認できます。
- [キャパシティとの比較(Compare to Capacity)]トグルアイコンが有効になっている場合( )、しきい値と比較した送信レート値を表示できます。しきい値の 90% を超えるレートは調査の必要があります。これらは懸念される状況であるためです。

> 受信レートまたは送信レートがしきい値を超えている場合は、ブローカーノードを追加してキャパシティを増やします。

テーブルの右上隅にある次の時間枠から目的のものをクリックすると、その時間枠でこれらのメトリックを表示できます。

- 過去 1 時間
- 過去 4 日間
- 過去 1 日
- 過去 1 週間
- 過去 1 ヵ月

1 分間の負荷平均のテーブル

1 分間隔で計測した、選択したブローカーノードの CPU 負荷平均（最初に、テーブルの右上隅にある時間枠オプションバーから [過去 1 時間（Last 1h）] をクリックする必要があります）。x 軸（時間を表す水平線）の上にカーソルを合わせると、時刻の特定の分を確認できます。CPU 数に設定されたしきい値（y 軸で表される値）を負荷平均が超えると、ネットワークテレメトリのフローレートが低下します。

メモリ使用率のテーブル

3 分間隔で計測した、メモリ使用量と使用可能な合計メモリ（最初に、テーブルの右上隅にある時間枠オプションバーから [過去 1 時間（Last 1h）] をクリックする必要があります）。x 軸（時間を表す水平線）の上にカーソルを合わせると、時刻の特定の 3 分間隔を確認できます。しきい値の 80% を超えるレートは調査の必要があります。これらは懸念される状況であるためです。

ディスクストレージのテーブル

3 分間隔で計測した、ディスクストレージ使用量と使用可能なストレージ容量の合計（最初に、テーブルの右上隅にある時間枠オプションバーから [過去 1 時間（Last 1h）] をクリックする必要があります）。x 軸（時間を表す水平線）の上にカーソルを合わせると、時刻の特定の 3 分間隔を確認できます。しきい値の 80% を超えるレートは調査の必要があります。これらは懸念される状況であるためです。

> 負荷平均、メモリ使用率、またはディスクストレージが、関連するしきい値を超えている場合は、VM のリソース割り当てを拡張します。

ハイ アベイラビリティ クラスタ

Cisco Telemetry Broker ハイアベイラビリティにより、高い可用性を持つ IPv4 および IPv6 仮想 IP アドレスが入力のターゲットとして提供され、入力から宛先への信頼性の高いテレメトリ配信が保証されます。

ハイ アベイラビリティ クラスタを複数作成し、それぞれのクラスタに複数のブローカノードを割り当てることで、ブローカノードの高可用性を確立することができます。各クラスタでは、1 つのブローカノードがアクティブに指定されます。これは、テレメトリを受け渡し、メトリックを Cisco Telemetry Broker に提供することを意味します。残りのノードは、パッシブに指定されます。これは、現時点でテレメトリを渡さず、メトリックを提供しないことを意味します。アクティブなブローカーノードがテレメトリの受け渡しを停止するか、Cisco Telemetry Broker との接続を失うと、いずれかのパッシブブローカノードがアクティブなブローカーノードに昇格し、テレメトリの受け渡しを開始します。

クラスタについては、次の点に注意してください。

- 各ブローカノードは、同時に 1 つのクラスタのみに属することができます。
- クラスタを作成するには、そのクラスタに 1 つ以上のブローカノードを割り当てる必要があります。
- ブローカノードを 1 つのみ含むクラスタを作成し、このブローカノードに障害が発生した場合、アクティブなブローカノードに昇格できる他のブローカノードがないことに注意してください。同様に、クラスタ内のすべてのブローカノードに障害が発生した場合は、アクティブなブローカノードに昇格できるブローカノードはありません。ブローカノードに障害が発生した場合は、できるだけ早くオンラインに復帰させてください。
- 特定のクラスタでどのブローカノードがアクティブであるかを選択することはできません。
- 特定の仮想 IP アドレスのアクティブブローカノードに障害が発生すると、同じクラスタ内のパッシブブローカノードの 1 つがその仮想 IP アドレスのアクティブブローカノードになります。障害が発生したブローカノードが復帰すると、パッシブブローカノードの状態を維持します。そのノードを再度アクティブにする場合は、提供されているコマンドを使用して手動で操作する必要があります。（これらのコマンドを表示するには、『Cisco Telemetry BrokerVirtual Appliance Deployment and Configuration Guide』の、VIP の特定のノードへの移動に関する項を参照してください）。
- 仮想 IPv4 または仮想 IPv6 アドレスのいずれか、または両方をクラスタに割り当てることができます。Cisco Telemetry Broker は、この仮想 IP アドレスを使用してクラスタと通信し、アクティブなブローカーノードと Cisco Telemetry Broker の接続が失われた場合にパッシブのブローカーノードをアクティブなブローカーノードに昇格させます。

Cisco Telemetry Broker ソフトウェア アップデート プロセス中に HA クラスタがどのようにアップデートされるかについては、「**ソフトウェア更新**」を参照してください。

クラスタのタスク

クラスタの詳細の表示

[ブローカノード(Broker Nodes)] ページの [高可用性クラスタ(High Availability Clusters)] セクションでは、次のデータを表示できます。

- 設定済みのすべてのクラスタ
- 各クラスタの IPv4 アドレスと IPv6 アドレス
- 各クラスタに属するブローカノード

クラスタの追加

1. Cisco Telemetry Broker メインメニューから [ブローカーノード(Broker Nodes)] を選択します。
2. ページの右側で、[+クラスタの追加(+ Add Cluster)] をクリックします。
3. わかりやすいクラスタ名を入力します。
4. クラスタに含める 1 つ以上のブローカーノードを選択します。
5. クラスタ仮想 IPv4 アドレス、IPv6 アドレス、またはその両方を入力します。
6. [クラスタの追加(Add Cluster)] をクリックします。

> - 構成が伝播され、VIP アドレスがネットワークで使用可能になるまでに最大 3 分かかります。
> - クラスタに割り当てることができるブローカーノードがない場合、[+クラスタの追加(+Add Cluster)] ボタンは無効になります。

クラスタの構成の変更

1. Cisco Telemetry Broker メインメニューから [ブローカーノード(Broker Nodes)] を選択します。
2. [ハイアベイラビリティクラスタ(High Availability Clusters)] セクションで、編集するクラスタの  ([編集(Edit)]) アイコンをクリックします。
3. 開いた [編集(Edit)] ダイアログで編集を行い、[保存(Save)] をクリックします。

クラスタの削除

1. Cisco Telemetry Broker メインメニューから [ブローカーノード(Broker Nodes)] を選択します。
2. [高可用性クラスタ(High Availability Clusters)] セクションで、削除するクラスタの  ([削除(Remove)]) アイコンをクリックします。
3. 開いた [削除(Remove)] ダイアログで、[削除(Remove)] をクリックします。

クラスタの管理については、『Cisco Telemetry Broker Virtual Deployment Guide』のハイ アベイラビリティ クラスタの管理に関する項を参照してください。

マネージャノード

[Cisco Telemetry Broker マネージャ（Cisco Telemetry Broker Manager）] ビューには、Cisco Telemetry Broker マネージャのメトリックが表示されます。次の情報が表示されます。

- ホスト名と管理インターフェース（管理ネットワーク）IPv4/IPv6 アドレス
- 現在のメモリ使用量と使用可能な合計メモリ
- 現在のディスクストレージ使用量と使用可能なディスクストレージ容量の合計

1 分間の負荷平均のテーブル

1 分間隔で計測した、選択したブローカーノードの CPU 負荷平均（最初に、テーブルの右上隅にある時間枠オプションバーから [過去 1 時間（Last 1h）] をクリックする必要があります）。x 軸（時間を表す水平線）の上にカーソルを合わせると、時刻の特定の分を確認できます。CPU 数に設定されたしきい値（y 軸で表される値）を負荷平均が超えると、ネットワークテレメトリのフローレートが低下します。

メモリ使用率のテーブル

1 分間隔で計測した、メモリ使用量と使用可能な合計メモリ（最初に、テーブルの右上隅にある時間枠オプションバーから [過去 1 時間（Last 1h）] をクリックする必要があります）。x 軸（時間を表す水平線）の上にカーソルを合わせると、時刻の特定の 3 分間隔を確認できます。しきい値の 80% を超えるレートは調査の必要があります。これらは懸念される状況であるためです。

ディスクストレージのテーブル

3 分間隔で計測した、ディスクストレージ使用量と使用可能なストレージ容量の合計（最初に、テーブルの右上隅にある時間枠オプションバーから [過去 1 時間（Last 1h）] をクリックする必要があります）。x 軸（時間を表す水平線）の上にカーソルを合わせると、時刻の特定の 3 分間隔を確認できます。しきい値の 80% を超えるレートは調査の必要があります。これらは懸念される状況であるためです。

> 負荷平均、メモリ使用率、またはディスクストレージが、関連するしきい値を超えている場合は、VM のリソース割り当てを拡張します。

[メトリック（Metrics）] テーブルの右上隅にある次の時間枠から目的のものをクリックすると、その時間枠でこれらのメトリックを表示できます。

- 過去 1 時間
- 過去 4 日間
- 過去 1 日
- 過去 1 週間
- 過去 1 ヵ月

統合

Cisco Telemetry Broker 統合には、VPC フローログに関する情報が表示されます。VPC フローログを Cisco Telemetry Broker にエクスポートするように AWS 展開を設定し、VPC フローログを IPFIX に変換して宛先が取り込めるように Cisco Telemetry Broker を設定できます。

統合情報の表示

Cisco Telemetry Broker メインメニューから、[統合（Integrations）] を選択します。

AWS の構成

AWS の構成 – パート1

フローロギングの有効化

1 つ以上の VPC のフローロギングを有効にし、フローログを S3 バケットに送信するには、次の手順を実行します。

1. AWS の VPC メインメニューから [使用するVPC（Your VPCs）] を選択します。
2. VPC を右クリックして、[フローログの作成（Create Flow Log）] を選択します。
3. [フィルタ（Filter）] ドロップダウンから、[すべて（All）] を選択して承認されたテレメトリと拒否されたテレメトリをログに記録するか、[承認（Accept）] を選択して承認されたテレメトリのみをログに記録します。
4. [S3バケット宛先に送信（Send to an S3 bucket destination）] を選択します。
5. フローログテレメトリを保存する S3 バケット ARN を入力します。
6. [作成（Create）] をクリックします。

IAM ユーザーの作成

S3 バケットにアクセスできる IAM ユーザーを作成し、アクセスキー ID とシークレットアクセスキーを記録するには、次の手順を実行します。

1. AWS の IAM メインメニューから、[ユーザー（Users）] > [ユーザーの追加（Add user）] の順に選択します。
2. [ユーザー名（User Name）] に入力します。
3. [プログラムによるアクセス（Programmatic access）] を選択します。
4. [次へ：権限（Next: Permissions）] をクリックします。
5. [次へ：タグ（Next: Tag）] をクリックします。
6. [次へ：レビュー（Next: Review）] をクリックします。
7. [Create User] をクリックします。
8. アクセスキー ID とシークレットアクセスキーの両方について、[表示（Show）] をクリックします。
9. アクセスキー ID とシークレットアクセスキーを記録するか、[ダウンロード（Download）] をクリックしてキーを安全な場所に保存します。

Cisco Telemetry Broker構成 – パート 1

AWS アクセスのアップロード

AWS アクセスキーとシークレットアクセスキーを Cisco Telemetry Broker にアップロードするには、次の手順を実行します。

1. Cisco Telemetry Broker メインメニューから、[統合(Integrations)] を選択します。

   [AWS] タブが開きます。

2. [AWSログイン情報の追加(Add AWS Credentials)] をクリックします(右上隅の AWS ログイン情報テーブルの上にあります)。
3. [ログイン情報名(Credentials Name)] に解りやすい名前を入力します。
4. [AWSアクセスキーID(AWS Access Key ID)] と [AWSシークレットアクセスキー(AWS Secret Access Key)] を入力します。
5. [保存(Save)] をクリックします。
6. 追加の S3 ログイン情報がある場合は、手順 1 ～ 5 を繰り返します。

VPC フローログ入力の設定

VPC フローログ入力を設定し、バケットポリシーを AWS にアップロードするには、次の手順を実行します。

1. Cisco Telemetry Broker メインメニューから、[入力(Inputs)] > [VPCフローログ(VPC Flow Logs)] タブを選択します。
2. [VPCフローログの追加(Add VPC Flow Log)] をクリックします(右上隅の [入力(Inputs)] テーブルの上にあります)。

   [VPCフローログの追加(Add VPC Flow Log)] ダイアログが開きます。

3. [S3バケットパス(S3 Bucket Path)] フィールドに、S3 バケット名とパスを入力します。次に例を示します。

   ```
   [bucket-name]/[path]
   ```

4. [リージョンコード(Region Code)] フィールドに、S3 バケットを作成した AWS リージョンを入力します。
5. [ログイン情報(Credentials)] で、アップロードしたアクセスキーとシークレットアクセスキーに基づいてログイン情報を選択します。
6. 次のフィールドの矢印をクリックして、ペインを展開します。このペインから、S3 バケットポリシーをコピーし、AWS の S3 バケット設定に使用します。
7. このダイアログを開いたままにして、次の「AWS の構成 – パート 2」に進みます。

AWS の構成 – パート 2

S3 バケットポリシーの作成

1. AWS の IAM メインメニューから、[ポリシー(Policies)] を選択します。
2. [ポリシーの作成(Create Policy)] をクリックします。
3. [JSON] タブを選択します。
4. Cisco Telemetry Broker からコピーしたポリシーを JSON エディタに貼り付けます。

5. [ポリシーの確認（Review policy）] をクリックします。
6. [名前（Name）] フィールドに、ポリシーを識別する一意の名前を入力します（例：**ctb_policy**）。
7. 説明を入力します（例：VPC フローログへのアクセスを Cisco Telemetry Broker に許可するポリシー）。
8. [ポリシーの作成（Create Policy）] をクリックします。

ユーザ グループの作成

ユーザーグループを作成し、ポリシーを IAM グループに割り当て、IAM ユーザーを IAM グループに追加するには、次の手順を実行します。

1. AWS の IAM メインメニューから、[グループ（Groups）] > [新しいグループの作成（Create New Group）] の順に選択します。
2. グループ名を入力します。
3. [次のステップ（Next Step）] をクリックします。
4. 作成した Cisco Telemetry Broker ポリシーを選択します。
5. [次のステップ（Next Step）] をクリックします。
6. [グループの作成（Create Group）] をクリックします。
7. IAM コンソールで [グループ（Groups）] を選択し、グループ名を選択します。
8. [ユーザー（Users）] タブをクリックします。
9. [ユーザーをグループに追加（Add Users to Group）] をクリックし、**Cisco Telemetry Broker ユーザー**を選択します。
10. [ユーザを追加（Add Users）] をクリックします。

Cisco Telemetry Broker の構成 – パート 2

Cisco Telemetry Broker での AWS フローログの登録

VPC フローログテレメトリを処理して IPFIX に変換するように Cisco Telemetry Broker を設定するには、次の手順を実行します。

1. 「Cisco Telemetry Broker の構成 – パート 1」で部分的に完了したダイアログに戻ります（「**VPC フローログ入力の設定**」セクションを参照）。
2. [入力名（Input Name）] フィールドに、入力 IP アドレス名を入力します。
3. [入力IPアドレス（Input IP Address）] フィールドに、このフローログに割り当てる入力 IP アドレスを入力します。Cisco Telemetry Broker は、VPC フローログから生成された IPFIX を送信するときに、この IP アドレスを入力アドレスとして使用します。これは内部 IP アドレスである必要があり、ネットワーク上の他の IP アドレスと競合しないようにする必要があります。

   Cisco Telemetry Broker では、パケットの適切なブローカーリングを保証するために、入力 IP 値に次の制限が設定されています。次のいずれかの条件が満たされていない場合は、Cisco Telemetry Broker にエラーメッセージが表示されます。

   - 入力 IP は、[割り当て済みノード（Assigned Node）] のテレメトリインターフェイスのサブネットと重複してはいけません。
   - 入力 IP は、システム内の既存の入力 IP と競合してはいけません。

- 入力 IP は、システム内の宛先 IP と競合してはいけません。

4. [割り当て済みブローカーノード(Assigned Broker Node)]ドロップダウンリストから、割り当て済みブローカーノードを選択します。このブローカーノードは、S3 バケットからのすべてのフローログテレメトリを処理します。
5. フローログテレメトリを取り込む 1 つ以上の宛先を選択します。Cisco Telemetry Broker は、VPC フローログを IPFIX に変換することに注意してください。
6. [VPCフローログを追加(Add VPC Flow Log)]をクリックします。
7. 設定する VPC フローログが複数ある場合は、設定する VPC フローログごとに次の手順を実行します。
    a. 「**VPC フローログ入力の設定**」のすべての手順を繰り返します。
    b. 「**S3 バケットポリシーの作成**」のすべての手順を繰り返します。
    c. 「**ユーザ グループの作成**」のすべての手順を繰り返します。
    d. この項のステップ 1 ～ 5 を繰り返します。
8. [保存(Save)]をクリックします。

> VPC フローログを正常に設定するには、AWS S3 バケットにフローログが存在する(すでに書き込まれている)ことを確認します。存在しない場合、AWS VPC フローログの設定は失敗します。

Azure の設定

次の手順では、Azure 環境から分析用のテレメトリを収集するモニタリング アプリケーションをセットアップする方法について詳しく説明します。モニタリングが必要なすべてのサブスクリプションのグローバル管理者 AD ロールおよび所有者ロールを割り当てられたユーザーとして、次の手順に従うことをお勧めします。

これが不可能な場合は、Azure AD 管理者に問い合わせて、モニタ対象の各サブスクリプションについて、ユーザーが Azure リソース(認証、ネットワーク、ストレージアカウント、モニタリング)にアクセスできるようにしてください。これを行うには、ユーザーにユーザーアクセス管理者ロールとコントリビュータロールを割り当てる必要があります。

前提条件

NSGフローログを構成する前に、次の手順を実行します。

1. **Azureに接続する** Azure ポータルにアクセスし、指示に従ってサインインします。コマンドラインアクセスの場合は、検索バーの横にあるコンソールアイコンを使用して bash コンソールを起動します。
2. **Network Watcher をセットアップする** モニタリング対象のリソースグループが存在するリージョンの Network Watcher サービスをセットアップします。
    a. メインメニューから、[Network Watcher] > [概要(Overview)]を選択します。
    b. ••• (省略記号)アイコンをクリックし、サブスクリプションレベルまたはターゲットリージョンで [Network Watcher の有効化(Enable Network Watcher)]を選択します。

3. **ストレージアカウントを作成する** NSG フローログを保存するには、ターゲットリソースグループと同じ場所（米国東部など）にストレージアカウントが必要です。ターゲットロケーションにまだストレージアカウントがない場合は、BLOB ストレージ機能（StorageV2 または BlobStorage）を使用してアカウントをいくつか作成する必要があります。

NSG フローログの有効化

モニタする NSG について、次の手順を実行してフローロギングを有効にする必要があります。

1. メインメニューから [Network Watcher] > [NSGフローログ（NSG Flow Logs）] の順に選択します。ネットワーク セキュリティ グループのリストが表示されます。
2. フローログの設定画面を表示するには、メインメニューから NSG を選択します。
3. 次の設定を入力して、フォームを完成します。
   - **[状態（Status）]**：オン
   - **[フローログのバージョン（Flow Logs version）]**：バージョン 2
   - **[ストレージアカウント（Storage account）]**：以前に作成したストレージアカウントを選択します。
   - **[リテンション期間（Retention）]**：現在、Microsoft には、フローログの保持に関する既知の問題があります。詳細については、Microsoft ドキュメントの「Enable NSG Flow Log」セクションのステップ 11 の注記を参照してください。
   - **[トラフィック分析（Traffic Analytics）] ステータス**：オフ（オプションで、これを有効にすることができます）
4. [保存（Save）] をクリックし、NSG ごとにフローログのセットアップを繰り返します。

> モニタするリソースグループを新しく作成するごとに、NSG フローログを有効にする必要があります。

5. Azure ポータルで、メインメニューから [ストレージアカウント（Storage Accounts）] > アカウントを選択 > [コンテナ（Containers）] の順に選択します。[コンテナ（Containers）] のリストに insights-logs-networksecuritygroupflowevent エントリが表示されていることを確認します。表示されるまで数分かかることがあります。

BLOB サービス SAS URL の取得

Cisco Telemetry Broker で必要な BLOB サービス SAS URL を生成するには、次の手順を実行します。

1. Azure ポータル のメインメニューから、[ストレージアカウント（Storage Accounts）] > アカウントを選択 > [共有アクセス署名（Shared Access Signature）] の順に選択します。開いたフォームには、次のエントリが含まれています。
   - **[使用できるサービス（Allowed Services）]**：[Blob]
   - **[使用できるリソースタイプ（Allowed Resource Type）]**：[サービス（Service）]、[コンテナ（Container）]、[オブジェクト（Object）]
   - **[許可される権限（Allowed Permissions）]**：[読み取り（Read）]、[リスト（List）]

- **[開始および失効日時(Start and Expiry Times)]**: Cisco Telemetry Broker にアクセスを許可する間隔に設定します

2. [SASを生成(Generate SAS)] を選択して接続文字列を選択します。
3. BLOB サービス SAS URL をコピーします。

> NSG フローログを Cisco Telemetry Broker に追加するときの BLOB サービス SAS URL を指定します。

次での Azure フローログの登録: Cisco Telemetry Broker

NSG フローログテレメトリを処理して IPFIX に変換するように Cisco Telemetry Broker を設定するには、次の手順を実行します

1. Cisco Telemetry Broker に戻ります。
2. Cisco Telemetry Broker メインメニューから、[入力(Inputs)] > [NSGフローログ(NSG Flow Logs)] タブをクリックします。
3. [NSGフローログの追加(Add NSG Flow Log)] をクリックします(右上隅の [入力(Inputs)] テーブルの上にあります)。

   [NSGフローログの追加(Add NSG Flow Log)] ダイアログが開きます。
4. [入力名(Input Name)] フィールドに、入力 IP アドレス名を入力します。
5. [入力IPアドレス(Input IP Address)] フィールドに、このフローログに割り当てる入力 IP アドレスを入力します。Cisco Telemetry Broker は、NSG フローログから生成された IPFIX を送信するときに、この IP アドレスを入力アドレスとして使用します。これは内部 IP アドレスである必要があり、ネットワーク上の他の IP アドレスと競合しないようにする必要があります。

   Cisco Telemetry Broker では、パケットの適切なブローカーリングを保証するために、入力 IP 値に次の制限が設定されています。次のいずれかの条件が満たされていない場合は、Cisco Telemetry Broker にエラーメッセージが表示されます。

   - 入力 IP は、[割り当て済みノード(Assigned Node)] のテレメトリインターフェイスのサブネットと重複してはいけません。
   - 入力 IP は、システム内の既存の入力 IP と競合してはいけません。
   - 入力 IP は、システム内の宛先 IP と競合してはいけません。
6. [割り当て済みブローカーノード(Assigned Broker Node)] ドロップダウンリストから、割り当て済みブローカーノードを選択します。このブローカーノードは、S3 バケットからのすべてのフローログテレメトリを処理します。
7. フローログテレメトリを取り込む 1 つ以上の宛先を選択します。Cisco Telemetry Broker は、NSG フローログを IPFIX に変換することに注意してください。
8. [NSGフローログの追加(Add NSG Flow Log)] をクリックします。
9. 設定する NSG フローログが複数ある場合は、設定する NSG フローログごとに、次の手順を順番に実行します。

a. この「Azure の設定」トピックの先行する各セクションのすべての手順を繰り返します。
b. このセクションのステップ 1 ～ 7 を繰り返します。

10. ［保存（Save）］をクリックします。

アプリケーションの設定

アプリケーション設定により、Cisco Telemetry Broker の展開を制御します。以下の設定を使用できます。

全般

ソフトウェア更新

スマート ライセンス

TLS 証明書

ユーザ管理

全般

1. ⚙（設定）アイコンをクリックします。

   [アプリケーション設定（Application Settings）] ページが開きます。

2. [全般（General）] タブをクリックします。

非アクティブ間隔の設定

テレメトリ入力の設定では、Cisco Telemetry Broker がテレメトリ入力を非アクティブとしてマークするまでの時間を設定できます。

1. [入力（Inputs）] セクションで、[非アクティブ間隔（Inactivity Interval）] ドロップダウンリストから非アクティブ間隔を分単位で選択します。
2. [保存（Save）] をクリックします。

HTTPS プロキシの設定

HTTPS プロキシ設定を使用すると、Cisco Telemetry Broker が HTTPS プロキシを使用してインターネットに接続する場合に HTTPS プロキシサーバー設定を構成できます。

> Cisco Telemetry Broker は、HTTP プロキシサーバーの使用をサポートしていません。

1. [HTTPSプロキシ（HTTPS Proxy）]セクションで、[HTTPSプロキシを使用（Use HTTPS proxy）] を有効にします。
2. [IPアドレス（IP Address）] と [ポート（Port）] を入力します。
3. [保存（Save）] をクリックします。

ソフトウェア更新

[ソフトウェアアップデート（Software Update）] ページには、マネージャノードとブローカーノードの現在の Cisco Telemetry Broker バージョンが表示され、最新のリリースバージョンにアップグレードできます。

この更新により、マネージャとすべての管理対象ブローカーノードが最新バージョンにアップグレードされます。更新を実行する前に、Cisco Telemetry Broker VM の VM スナップショットを作成することをお勧めします。このスナップショットを使用して、予期しないエラーが発生した場合に現在の状態に戻すことができます。

更新プロセス中はシステムが応答しません。まずマネージャを更新し、次にブローカーノードを更新します。マネージャの更新中は、Cisco Telemetry Broker の展開の状態が正しく表示されない場合があります。ブローカーノードの更新中は、送信されたテレメトリを宛先に正しく渡すことができません。

Cisco Telemetry Broker HA クラスタは、アップグレード中にダウンタイムが発生しないように設計されています。したがって、HA クラスタでは、マネージャは常に一度に 1 つのノードのみを更新します。HA クラスタを更新する場合、マネージャノードはそのクラスタ内のノードを作成順に更新します。ノードが更新を開始すると、まずそれ自体がスタンバイモードになります。これがアクティブノードの場合、Cisco Telemetry Broker 機能は代替ノードに転送されます。これは、それまでアクティブだったノードがテレメトリの処理を停止する前に発生します。これにより、アップグレード中のテレメトリ損失を最小限に抑えることができます。

Cisco Telemetry Broker 展開のアップグレード

更新ファイルのダウンロード

1. Cisco Software Central に移動します。
2. [ダウンロードとアップグレード（Download and Upgrade）] セクションで、[ダウンロードにアクセス（Access Download）] を選択します。
3. 検索フィールドに「Cisco Telemetry Broker」と入力します。
4. [マネージャ ノード ソフトウェア（Manager Node Software）] を選択します。
5. CTB 更新バンドルファイルをダウンロードします。

更新ファイルのアップロード

1. Cisco Telemetry Broker マネージャで、⚙（設定）アイコンをクリックします。

   [アプリケーション設定（Application Settings）] ページが開きます。
2. [ソフトウェアの更新（Software Update）] タブをクリックします。
3. ページの右上隅にある [更新ファイルのアップロード（Upload an Update File）] をクリックします。
4. ダウンロードしたファイルを選択します。

   表示される推定時間に基づき、アップロードが完了するまで数分かかる場合があります。ファイルがアップロードされると、ソフトウェアアップデートが利用可能になったことを通知するメッセージが表示されます。
5. **[Cisco Telemetry Broker の更新（Update Cisco Telemetry Broker）]** をクリックします。

   マネージャノードが最新バージョンに更新されている間は、Cisco Telemetry Broker 内を移動できません。更新プロセスには約 10 分かかります。
6. 更新が完了すると、再度 Cisco Telemetry Broker にログインするように求められます。

   更新中の各ブローカーノードの横にロードインジケータが表示されます。

スマート ライセンス

[スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページに、Cisco Telemetry Broker スマートライセンスの状態が表示されます。

Cisco Telemetry Broker ライセンスは、ブローカーノードが 1 日に取り込む GB に基づきます。

1. ☼（設定）アイコンをクリックします。
   [アプリケーション設定（Application Settings）] ページが開きます。
2. [スマートライセンシング（Smart Licensing）] タブをクリックします。

ユーザ管理

1. （設定）アイコンをクリックします。
   [アプリケーション設定（Application Settings）] ページが開きます。
2. [ユーザー管理（User Management）] タブをクリックします。

ユーザの追加

1. [ユーザの追加（Add User）] をクリックします。
2. ユーザーの [名（First Name）] と [姓（Last Name）] を入力します。
3. [ユーザー名（Username）] を入力します。管理者もユーザーも、このユーザー名は作成後は変更できません。
4. [新しいパスワード（New Password）] フィールドに新しいパスワードを入力し、[パスワードの確認（Confirm Password）] フィールドにもう一度入力します。必ずパスワードのガイドラインに従ってください。
5. [+ユーザーの追加（+ Add User）] をクリックします。

ユーザの編集

1. 編集するユーザーを含む行で、••• （アクション）アイコンをクリックし、[プロファイルの編集（Edit Profile）] をクリックします。
2. 編集を完了します。
3. [保存（Save）] をクリックします。

ユーザーの削除

1. 編集するユーザーを含む行で、**アクション**アイコンをクリックし、[ユーザーの削除（Remove User）] をクリックします。
2. [削除（Remove）] をクリックします。

ユーザーのパスワードを変更する

1. パスワードを変更するユーザーを含む行で**アクション**アイコンをクリックし、[パスワードの変更（Change Password）] をクリックします。
2. [パスワード（Password）] フィールドに新しいパスワードを入力し、[パスワードの確認（Confirm Password）] フィールドにもう一度入力します
3. [パスワードの変更（Change Password）] をクリックします。

TLS 証明書

このページでは次の情報を確認できます。

- ホストネーム
- 証明書の有効期限日時
- サブジェクト名と発行者名（[証明書の詳細（Certificate details）]）

> ⚠ 証明書と秘密キーは PEM でエンコードされている必要があります。

> ⚠ 秘密キーファイルはパスワードで保護できません。

TLS 証明書のアップロード

1. ⚙（設定）アイコンをクリックします。

   [アプリケーション設定（Application Settings）] ページが開きます。

2. [TLS 証明書（TLS Certificates）] タブをクリックします。
3. 証明書の詳細を表示するには、[証明書の詳細（Certificate details）] ドロップダウン矢印をクリックします。このセクションでは、サブジェクト名、発行者名、サブジェクト代替名を表示できます。
4. ページの右上隅にある [TLS証明書のアップロード（Upload TLS Certificate）] をクリックします。
5. 表示される [TLS証明書のアップロード（Upload TLS certificate）] ダイアログで、アップロードする各証明書と各秘密キーの [ファイルの選択（Choose File）] をクリックします。

   関連するファイルの下に証明書の詳細が表示されるため、すべての関連情報が正しいことを確認できます。

6. [アップロード（Upload）] をクリックします。

ブローカーノードの再登録

適切な TLS 証明書をアップロードした後、各ブローカーノードを再登録して、マネージャノードとブローカノード間の接続を有効にする必要があります。

1. SSH または VM サーバーコンソールを使用して、**admin** としてアプライアンスにログインします。
2. 次のコマンドを入力します。

   ```
   sudo ctb-manage
   ```

   マネージャ設定がすでに存在することが通知されます。

3. **オプション C「Re-fetch the manager's certificate but keep other other」**を選択します。

Syslog 通知

1. ⚙（設定）アイコンをクリックします。

   [アプリケーション設定（Application Settings）] ページが開きます。

2. [通知（Notifications）] タブをクリックします。

サポートされているアラートのリストを表示するには、ページの上部にある［サポートされているアラート（Supported Alerts）］ドロップダウン矢印をクリックします。アラートが生成されたときに syslog 通知を送信するように、Cisco Telemetry Broker に指示できます。これらのアラートのリストについては、「**付録 B：サポートされるアラート**」を参照してください。

> 現在、カスタムアラートタイプは設定できません。

Syslog サーバーの設定

最初に、Syslog サーバーを設定する必要があります。

1. ［Syslogサーバーのアドレス（Syslog Server Address）］フィールドで、［設定（Configure）］をクリックします。
2. 該当する Syslog サーバーアドレス（IPv4 アドレス、IPv6 アドレス、または DNS 名）とポート番号を入力します。
3. ［保存（Save）］をクリックします。

Syslog サーバーで通知を受信できるようにする

次に、次の手順を実行します。

- ［Syslog通知の送信（Send Syslog Notifications）］トグル（  ）を有効にします。

Syslog サーバーを設定した後は、このトグルを有効にする必要があります。そうしないと、Syslog サーバーは通知を受信しません。このトグルを有効にすると、Cisco Telemetry Broker がアラートをトリガーするとすぐに syslog 通知が Syslog サーバーに送信されます。

テスト Syslog 通知を送信する

必要に応じて、Syslog サーバーにテスト syslog 通知を手動で送信できます。このテスト通知は、Syslog サーバーが syslog メッセージを正常に受信していることを確認します。

テスト syslog 通知を送信するたびに、メッセージのコピーが［送信されたテスト（Sent Test）］ボタンの下に表示されます。これにより、送信されたメッセージと Syslog サーバーが受信したメッセージを比較できます。

Cisco Telemetry Broker からログアウトした場合、再度ログインするとメッセージは表示されなくなります。

> Syslog サーバーを手動でチェックして、テスト通知が受信されたことを確認する必要があります。

テスト syslog 通知を送信するには、次の手順を実行します。

1. ［Syslog通知の送信（Send Syslog Notifications）］トグル（  ）を有効にします。
2. ［テストを送信（Send Test）］をクリックします。
3. 確認ダイアログで、［送信（Send）］をクリックします。

重大度とファシリティ値

テレメトリブローカーは、重大度の値を warning に、ファシリティの値を local0 にハードコードします。

電子メールの通知

1. ⚙(設定)アイコンをクリックします。

   [アプリケーション設定(Application Settings)] ページが開きます。

2. [通知(Notifications)] タブをクリックします。

アラートが生成されたときに電子メール通知を送信するように、Cisco Telemetry Broker に指示できます。これらのアラートのリストについては、「**付録 B:サポートされるアラート**」を参照してください。

> ℹ 現在、カスタムアラートタイプは設定できません。

SMTP サーバーの設定

まず、SMTP サーバーの設定を構成する必要があります。

1. [SMTPサーバー(SMTP Server)] フィールドで、[設定(Configure)] をクリックします。
2. 該当する SMTP サーバーアドレス(IPv4 アドレス、IPv6 アドレスまたは DNS 名)、ポート番号、およびアラートの送信元の電子メールアドレスを入力します。
3. 認証を要求するかどうかを指定します。要求する場合は、SMTP サーバーのユーザー名とパスワードを関連するフィールドに入力します。
4. 暗号化タイプを選択します。
5. [保存(Save)] をクリックします。

ユーザーが電子メール通知を受信できるようにする

SMTP サーバーを構成した後、Cisco Telemetry Broker による電子メール通知の送信を有効にする必要があります。そうしないと、指定されたユーザーは通知を受信しません。

1. [電子メールでの通知の送信(Send Email Notifications)] トグル(⬭)を有効にします。
2. [受信者(Recipients)] フィールドで、[編集(Edit)] をクリックします。
3. 開いた [受信者の編集(Edit recipients)] ダイアログで、電子メール通知を受信できるようにするすべてのユーザーを選択します。

   現在のユーザーの名前がリストの一番上に表示されます。プロファイルに電子メールアドレスがないユーザーのユーザー名は、リストの下部にグレー表示されます。

4. [保存(Save)] をクリックします。

テスト電子メール通知の送信

必要に応じて、すべてのアラートに関するテスト電子メール通知を手動で送信できます。このテスト電子メール通知は、SMTP サーバーが正しく構成されていること、およびすべての適切なユーザーが発生した(自分に割り当てられている)アラートに関する電子メール通知を正常に受信することを確認します。

1. [電子メールでの通知の送信(Send Email Notifications)] トグル(⬭)を有効にします。
2. [テストを送信(Send Test)] をクリックします。

3. このテスト電子メール通知を受信するユーザーのリストを編集する必要がある場合は、開いた[テストを送信(Send Test)]ダイアログで、[選択(Choose)]をクリックして編集を行います。

   現在のユーザーの名前がリストの一番上に表示されます。プロファイルに電子メールアドレスがないユーザーのユーザー名は、リストの下部にグレー表示されます。

4. [送信(Send)]をクリックします。

プロファイル設定

個人情報の編集

1. ([ユーザ(User)])アイコン をクリックします。
   [プロファイル設定(Profile Settings)] ページが開きます。
2. [個人情報(Personal Information)] セクションで、(編集)アイコンをクリックします。
3. 編集を完了します。
4. [保存(Save)] をクリックします。

パスワードの変更

1. **(ユーザー)** アイコンをクリックします。
   [プロファイル設定(Profile Settings)] ページが開きます。
2. [パスワード(Password)] セクションで、[パスワードの変更(Change Password)] をクリックします。
3. [パスワード(Password)] フィールドに新しいパスワードを入力し、[パスワードの確認(Confirm Password)] フィールドにもう一度入力します
4. [パスワードの変更(Change Password)] をクリックします。

Cisco Telemetry Broker Manager およびブローカノードのディスクサイズの拡張

Cisco Telemetry Broker を使用すると、マネージャと任意のブローカーノードの両方のディスクサイズを拡張できます。

1. パーティションテーブル情報のバックアップ

アプライアンスにログインし、次のコマンドを実行します。

```
admin@ctb-nfik72TO:~$ sudo sgdisk -p /dev/sda > partition_table_
$(date +'%Y_%m_%d_%H_%M_%S').txt
```

これにより、次の内容と同様な partition_table_2021_07_09_15_51_04.txt ファイルと同様のファイルが作成されます。

```
Disk /dev/sda: 81920000 sectors, 39.1 GiB
Model: Virtual disk
Sector size (logical/physical): 512/512 bytes
Disk identifier (GUID): B078BED8-2BD0-4EEA-9149-BA93FC8A299D
Partition table holds up to 128 entries
Main partition table begins at sector 2 and ends at sector 33
First usable sector is 34, last usable sector is 81919966
Partitions will be aligned on 2048-sector boundaries
Total free space is 4029 sectors (2.0 MiB)

Number Start (sector) End (sector) Size Code Name
 1 2048 4095 1024.0 KiB EF02
 2 4096 491519 238.0 MiB 8300
 3 491520 3844095 1.6 GiB 8200
 4 3844096 33767423 14.3 GiB 8300
 5 33767424 63690751 14.3 GiB 8300
 6 63690752 81917951 8.7 GiB 8300
```

ディスクの合計サイズ（/dev/ada）は 39.1 GB で、Cisco Telemetry Broker アプリケーションパーティションのサイズ（/dev/sda6）は 8.7 GB です。

2. アプライアンスの既存のすべての VM スナップショットの削除

スナップショットが存在する場合、ESXi VM ディスクのサイズを変更することはできません。ディスクサイズを増やすには、既存のスナップショットをすべて削除する必要があります。

1. ESXi コンソール（vSphere または Web クライアント）にログインします。
2. VM を右クリックして、[スナップショット（Snapshots）] > [スナップショットの管理（Manage Snapshots）] > [すべて削除（Delete All）] を選択します。

3. アプライアンスのディスクサイズの増加

1. ESXi コンソール（vSphere または Web クライアント）にログインします。
2. 左パネルの VM のリストから、アプライアンスを選択します。
3. ページ上部のツールバーで、  （編集）アイコンをクリックします。
4. [ハード ディスク1（Hard Disk 1）] 行で、必要なサイズまで増やします。
5. VM を再起動します。
6. ログインし、次のコマンドを実行して新しいサイズが適用されたことを確認します。

```
$ sudo sgdisk -p /dev/sda
Disk /dev/sda: 125829120 sectors, 60.0 GiB
Model: Virtual disk
Sector size (logical/physical): 512/512 bytes
Disk identifier (GUID): B078BED8-2BD0-4EEA-9149-BA93FC8A299D
Partition table holds up to 128 entries
Main partition table begins at sector 2 and ends at sector 33
First usable sector is 34, last usable sector is 81919966
Partitions will be aligned on 2048-sector boundaries
Total free space is 4029 sectors (2.0 MiB)

Number Start (sector) End (sector) Size Code Name
 1 2048 4095 1024.0 KiB EF02
 2 4096 491519 238.0 MiB 8300
 3 491520 3844095 1.6 GiB 8200
 4 3844096 33767423 14.3 GiB 8300
 5 33767424 63690751 14.3 GiB 8300
 6 63690752 81917951 8.7 GiB 8300
```

4. ctb-part-resize.sh スクリプトの実行

1. VM のスナップショットを作成します。
2. 次のコマンドを実行します。

```
$ sudo /opt/titan/bin/ctb-part-resize.sh

WARNING

This program will update /dev/sda6 to use the full remaining free space
available on /dev/sda.

It is HIGHLY RECOMMENDED that you take a backup of any important data/configuration
before proceeding.

Do you wish to proceed?y
<134>Mar 8 15:35:30 ctb-disk-resize: Moving the partition table header to the end of the
disk(/dev/sda)
Warning: The kernel is still using the old partition table.
The new table will be used at the next reboot or after you
run partprobe(8) or kpartx(8)
```

```
The operation has completed successfully.
<134>Mar 8 15:35:31 ctb-disk-resize: Deleting CTB application partition (/dev/sda6)
Warning: The kernel is still using the old partition table.
The new table will be used at the next reboot or after you
run partprobe(8) or kpartx(8)
The operation has completed successfully.
<134>Mar 8 15:35:32 ctb-disk-resize: Creating the CTB application partition (/dev/sda6)
Warning: The kernel is still using the old partition table.
The new table will be used at the next reboot or after you
run partprobe(8) or kpartx(8)
The operation has completed successfully.
<134>Mar 8 15:35:33 ctb-disk-resize: Updating kernel partition tables
<134>Mar 8 15:35:34 ctb-disk-resize: Resizing /dev/sda6
resize2fs 1.44.5 (15-Dec-2018)
Filesystem at /dev/sda6 is mounted on /var/lib/titan; on-line resizing required
old_desc_blocks = 2, new_desc_blocks = 2
The filesystem on /dev/sda6 is now 2412283 (4k) blocks long.
```

5. スペースが割り当てられていることの確認

次のコマンドを実行します。

```
$ df -h /dev/sda
Filesystem Size Used Avail Use% Mounted on
/dev/sda4 14G 5.6G 7.7G 42% /
/dev/sda2 227M 80M 132M 38% /boot
/dev/sda5 14G 41M 14G 1% /mnt/alt_root
/dev/sda6 8.5G 172M 7.9G 3% /var/lib/titan
```

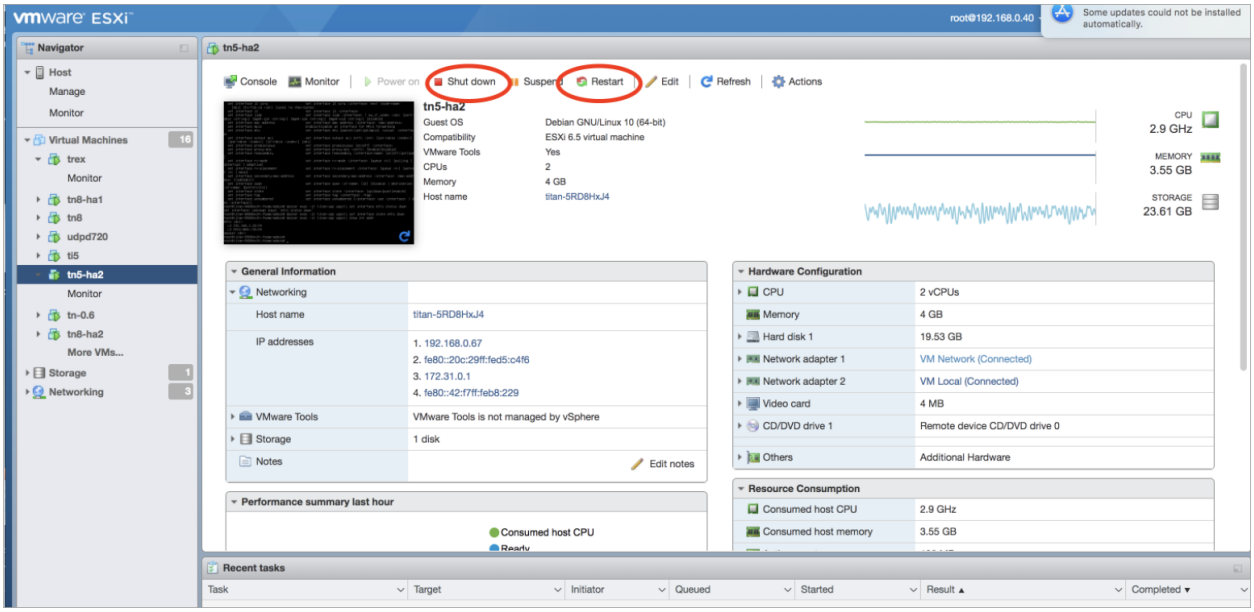
Cisco Telemetry Broker のシャットダウンまたはリブート

ある時点で Cisco Telemetry Broker のシャットダウンまたはリブートが必要な場合は、次の手順を実行します。

1. ユーザー名 **admin** を使用して、ssh またはコンソールから CTB マネージャまたは CTB ブローカーノードにログインします。
   - シャットダウンするには、`sudo shutdown now` と入力します。
   - リブートするには、`sudo shutdown -r now` と入力します。
2. VMWare コンソールにログインし、VM がシャットダウンまたはリブートを正常に完了したことを確認します。

オプションで、VMWare を使用してシャットダウンまたはリブートを実行できます。これを行うには、次の手順を実行します。

1. VMWare コンソールにログインし、該当する VM を選択します。
2. シャットダウンするかリブートするかに応じて、ページの上部に表示される次のオプションのいずれかをクリックします。



付録 A：Cisco Telemetry Broker でサポートされる IPFIX フィールド

この付録の表には、Cisco Telemetry Broker がサポートする IPFIX フィールドのリストが含まれています。

Cisco Telemetry Broker は、NetFlow メッセージ内の情報要素から数値 ID（各数値 ID は要素 ID と PEN を含む）を抽出し、それらをそれぞれ関連する記述名にマッピングします。

> Cisco Telemetry Broker が情報要素の数値 ID を認識しない場合でも、要素情報は Cisco Secure Cloud Analytics に送信されますが、Cisco Telemetry Broker は次の形式を使用して名前を割り当てます。
> `unknownID_<ElementID>_<PEN>`

要素 ID の説明を表示する場合は、『Cisco Secure Network Analytics Information Elements Guide』を参照してください。

ElementID	PEN	[名前（Name）]
1	0	octetDeltaCount
2	0	packetDeltaCount
3	0	deltaFlowCount
4	0	protocolIdentifier
5	0	ipClassOfService
6	0	tcpControlBits
7	0	sourceTransportPort
8	0	sourceIPv4Address
9	0	sourceIPv4PrefixLength
10	0	ingressInterface
11	0	destinationTransportPort
12	0	destinationIPv4Address
13	0	destinationIPv4PrefixLength
18	0	egressInterface

ElementID	PEN	[名前（Name）]
15	0	ipNextHopIPv4Address
16	0	bgpSourceAsNumber
17	0	bgpDestinationAsNumber
18	0	bgpNextHopIPv4Address
19	0	postMCastPacketDeltaCount
20	0	postMCastOctetDeltaCount
21	0	flowEndSysUpTime
22	0	flowStartSysUpTime
23	0	postOctetDeltaCount
24	0	postPacketDeltaCount
25	0	minimumIpTotalLength
26	0	maximumIpTotalLength
27	0	sourceIPv6Address
36	0	destinationIPv6Address
29	0	sourceIPv6PrefixLength
30	0	destinationIPv6PrefixLength
31	0	flowLabelIPv6
32	0	icmpTypeCodeIPv4
33	0	igmpType
34	0	samplingInterval
35	0	samplingAlgorithm
36	0	flowActiveTimeout

ElementID	PEN	[名前（Name）]
37	0	flowIdleTimeout
38	0	engineType
39	0	engineId
40	0	exportedOctetTotalCount
41	0	exportedMessageTotalCount
54	0	exportedFlowRecordTotalCount
43	0	ipv4RouterSc
44	0	sourceIPv4Prefix
45	0	destinationIPv4Prefix
46	0	mplsTopLabelType
47	0	mplsTopLabelIPv4Address
48	0	samplerId
49	0	samplerMode
50	0	samplerRandomInterval
51	0	classId
52	0	minimumTTL
53	0	maximumTTL
54	0	fragmentIdentification
55	0	postIpClassOfService
72	0	sourceMacAddress
57	0	postDestinationMacAddress
58	0	vlanId

ElementID	PEN	[名前（Name）]
59	0	postVlanId
60	0	ipVersion
61	0	flowDirection
62	0	ipNextHopIPv6Address
63	0	bgpNextHopIPv6Address
64	0	ipv6ExtensionHeaders
70	0	mplsTopLabelStackSection
71	0	mplsLabelStackSection2
72	0	mplsLabelStackSection3
73	0	mplsLabelStackSection4
74	0	mplsLabelStackSection5
75	0	mplsLabelStackSection6
76	0	mplsLabelStackSection7
77	0	mplsLabelStackSection8
78	0	mplsLabelStackSection9
79	0	mplsLabelStackSection10
80	0	destinationMacAddress
81	0	postSourceMacAddress
82	0	interfaceName
83	0	interfaceDescription
84	0	samplerName
85	0	octetTotalCount

ElementID	PEN	[名前（Name）]
86	0	packetTotalCount
87	0	flagsAndSamplerId
88	0	fragmentOffset
89	0	forwardingStatus
90	0	mplsVpnRouteDistinguisher
91	0	mplsTopLabelPrefixLength
92	0	srcTrafficIndex
93	0	dstTrafficIndex
94	0	applicationDescription
95	0	applicationId
96	0	applicationName
98	0	postIpDiffServCodePoint
99	0	multicastReplicationFactor
100	0	className
101	0	classificationEngineId
102	0	layer2packetSectionOffset
103	0	layer2packetSectionSize
104	0	layer2packetSectionData
128	0	bgpNextAdjacentAsNumber
129	0	bgpPrevAdjacentAsNumber
130	0	exporterIPv4Address
131	0	exporterIPv6Address

ElementID	PEN	[名前（Name）]
132	0	droppedOctetDeltaCount
133	0	droppedPacketDeltaCount
134	0	droppedOctetTotalCount
135	0	droppedPacketTotalCount
136	0	flowEndReason
137	0	commonPropertiesId
138	0	observationPointId
139	0	icmpTypeCodeIPv6
140	0	mplsTopLabelIPv6Address
141	0	lineCardId
142	0	portId
143	0	meteringProcessId
144	0	exportingProcessId
145	0	templateId
146	0	wlanChannelId
147	0	wlanSSID
148	0	flowId
149	0	observationDomainId
150	0	flowStartSeconds
151	0	flowEndSeconds
152	0	flowStartMilliseconds
153	0	flowEndMilliseconds

ElementID	PEN	[名前（Name）]
154	0	flowStartMicroseconds
155	0	flowEndMicroseconds
156	0	flowStartNanoseconds
157	0	flowEndNanoseconds
158	0	flowStartDeltaMicroseconds
159	0	flowEndDeltaMicroseconds
160	0	systemInitTimeMilliseconds
161	0	flowDurationMilliseconds
162	0	flowDurationMicroseconds
163	0	observedFlowTotalCount
164	0	ignoredPacketTotalCount
165	0	ignoredOctetTotalCount
166	0	notSentFlowTotalCount
167	0	notSentPacketTotalCount
168	0	notSentOctetTotalCount
169	0	destinationIPv6Prefix
170	0	sourceIPv6Prefix
171	0	postOctetTotalCount
172	0	postPacketTotalCount
173	0	flowKeyIndicator
174	0	postMCastPacketTotalCount
175	0	postMCastOctetTotalCount

ElementID	PEN	[名前（Name）]
176	0	icmpTypeIPv4
177	0	icmpCodeIPv4
178	0	icmpTypeIPv6
179	0	icmpCodeIPv6
180	0	udpSourcePort
181	0	udpDestinationPort
182	0	tcpSourcePort
183	0	tcpDestinationPort
184	0	tcpSequenceNumber
185	0	tcpAcknowledgementNumber
186	0	tcpWindowSize
187	0	tcpUrgentPointer
188	0	tcpHeaderLength
189	0	ipHeaderLength
190	0	totalLengthIPv4
191	0	payloadLengthIPv6
192	0	ipTTL
193	0	nextHeaderIPv6
194	0	mplsPayloadLength
195	0	ipDiffServCodePoint
196	0	ipPrecedence
197	0	fragmentFlags

ElementID	PEN	[名前（Name）]
198	0	octetDeltaSumOfSquares
199	0	octetTotalSumOfSquares
200	0	mplsTopLabelTTL
201	0	mplsLabelStackLength
202	0	mplsLabelStackDepth
203	0	mplsTopLabelExp
204	0	ipPayloadLength
205	0	udpMessageLength
206	0	isMulticast
207	0	ipv4IHL
208	0	ipv4Options
209	0	tcp-options
210	0	paddingOctets
211	0	collectorIPv4Address
212	0	collectorIPv6Address
213	0	exportInterface
214	0	exportProtocolVersion
215	0	exportTransportProtocol
216	0	collectorTransportPort
217	0	exporterTransportPort
218	0	tcpSynTotalCount
219	0	tcpFinTotalCount

ElementID	PEN	[名前（Name）]
220	0	tcpRstTotalCount
221	0	tcpPshTotalCount
222	0	tcpAckTotalCount
223	0	tcpUrgTotalCount
224	0	ipTotalLength
225	0	postNATSourceIPv4Address
226	0	postNATDestinationIPv4Address
227	0	postNAPTSourceTransportPort
228	0	postNAPTDestinationTransportPort
229	0	natOriginatingAddressRealm
230	0	natEvent
231	0	initiatorOctets
232	0	responderOctets
233	0	firewallEvent
234	0	ingressVRFID
235	0	egressVRFID
236	0	VRFname
237	0	postMplsTopLabelExp
238	0	tcpWindowScale
239	0	biflowDirection
240	0	ethernetHeaderLength
241	0	ethernetPayloadLength

ElementID	PEN	[名前（Name）]
242	0	ethernetTotalLength
243	0	dot1qVlanId
244	0	dot1qPriority
245	0	dot1qCustomerVlanId
246	0	dot1qCustomerPriority
247	0	metroEvcId
248	0	metroEvcType
249	0	pseudoWireId
250	0	pseudoWireType
251	0	pseudoWireControlWord
252	0	ingressPhysicalInterface
253	0	egressPhysicalInterface
254	0	postDot1qVlanId
255	0	postDot1qCustomerVlanId
256	0	ethernetType
257	0	postIpPrecedence
258	0	collectionTimeMilliseconds
259	0	exportSctpStreamId
260	0	maxExportSeconds
261	0	maxFlowEndSeconds
262	0	messageMD5Checksum
263	0	messageScope

ElementID	PEN	[名前（Name）]
264	0	minExportSeconds
265	0	minFlowStartSeconds
266	0	opaqueOctets
267	0	sessionScope
268	0	maxFlowEndMicroseconds
269	0	maxFlowEndMilliseconds
270	0	maxFlowEndNanoseconds
271	0	minFlowStartMicroseconds
272	0	minFlowStartMilliseconds
273	0	minFlowStartNanoseconds
274	0	collectorCertificate
275	0	exporterCertificate
276	0	dataRecordsReliability
277	0	observationPointType
278	0	newConnectionDeltaCount
279	0	connectionSumDurationSeconds
280	0	connectionTransactionId
281	0	postNATSourceIPv6Address
282	0	postNATDestinationIPv6Address
283	0	natPoolId
284	0	natPoolName
285	0	anonymizationFlags

ElementID	PEN	[名前（Name）]
286	0	anonymizationTechnique
287	0	informationElementIndex
288	0	p2pTechnology
289	0	tunnelTechnology
290	0	encryptedTechnology
291	0	basicList
292	0	subTemplateList
293	0	subTemplateMultiList
294	0	bgpValidityState
295	0	IPSecSPI
296	0	greKey
297	0	natType
298	0	initiatorPackets
299	0	responderPackets
300	0	observationDomainName
301	0	selectionSequenceId
302	0	selectorId
303	0	informationElementId
304	0	selectorAlgorithm
305	0	samplingPacketInterval
306	0	samplingPacketSpace
307	0	samplingTimeInterval

ElementID	PEN	[名前（Name）]
308	0	samplingTimeSpace
309	0	samplingSize
310	0	samplingPopulation
311	0	samplingProbability
312	0	dataLinkFrameSize
313	0	ipHeaderPacketSection
314	0	ipPayloadPacketSection
315	0	dataLinkFrameSection
316	0	mplsLabelStackSection
317	0	mplsPayloadPacketSection
318	0	selectorIdTotalPktsObserved
319	0	selectorIdTotalPktsSelected
320	0	absoluteError
321	0	relativeError
322	0	observationTimeSeconds
323	0	observationTimeMilliseconds
324	0	observationTimeMicroseconds
325	0	observationTimeNanoseconds
326	0	digestHashValue
327	0	hashIPPayloadOffset
328	0	hashIPPayloadSize
329	0	hashOutputRangeMin

ElementID	PEN	[名前（Name）]
330	0	hashOutputRangeMax
331	0	hashSelectedRangeMin
332	0	hashSelectedRangeMax
333	0	hashDigestOutput
334	0	hashInitialiserValue
335	0	selectorName
336	0	upperCILimit
337	0	lowerCILimit
338	0	confidenceLevel
339	0	informationElementDataType
340	0	informationElementDescription
341	0	informationElementName
342	0	informationElementRangeBegin
343	0	informationElementRangeEnd
344	0	informationElementSemantics
345	0	informationElementUnits
346	0	privateEnterpriseNumber
347	0	virtualStationInterfaceId
348	0	virtualStationInterfaceName
349	0	virtualStationUUID
350	0	virtualStationName
351	0	layer2SegmentId

ElementID	PEN	[名前（Name）]
352	0	layer2OctetDeltaCount
353	0	layer2OctetTotalCount
354	0	ingressUnicastPacketTotalCount
355	0	ingressMulticastPacketTotalCount
356	0	ingressBroadcastPacketTotalCount
357	0	egressUnicastPacketTotalCount
358	0	egressBroadcastPacketTotalCount
359	0	monitoringIntervalStartMilliSeconds
360	[0]	monitoringIntervalEndMilliSeconds
361	0	portRangeStart
362	0	portRangeEnd
363	0	portRangeStepSize
364	0	portRangeNumPorts
365	0	staMacAddress
366	0	staIPv4Address
367	0	wtpMacAddress
368	0	ingressInterfaceType
369	0	egressInterfaceType
370	0	rtpSequenceNumber
371	0	userName
372	0	applicationCategoryName
373	0	applicationSubCategoryName

ElementID	PEN	[名前（Name）]
374	0	applicationGroupName
375	0	originalFlowsPresent
376	0	originalFlowsInitiated
377	0	originalFlowsCompleted
378	0	distinctCountOfSourceIPAddress
379	0	distinctCountOfDestinationIPAddress
380	0	distinctCountOfSourceIPv4Address
381	0	distinctCountOfDestinationIPv4Address
382	0	distinctCountOfSourceIPv6Address
383	0	distinctCountOfDestinationIPv6Address
384	0	valueDistributionMethod
385	0	rfc3550JitterMilliseconds
386	0	rfc3550JitterMicroseconds
387	0	rfc3550JitterNanoseconds
388	0	dot1qDEI
389	0	dot1qCustomerDEI
390	0	flowSelectorAlgorithm
391	0	flowSelectedOctetDeltaCount
392	0	flowSelectedPacketDeltaCount
393	0	flowSelectedFlowDeltaCount
394	0	selectorIDTotalFlowsObserved
395	0	selectorIDTotalFlowsSelected

ElementID	PEN	[名前（Name）]
396	0	samplingFlowInterval
397	0	samplingFlowSpacing
398	0	flowSamplingTimeInterval
399	0	flowSamplingTimeSpacing
400	0	hashFlowDomain
401	0	transportOctetDeltaCount
402	0	transportPacketDeltaCount
403	0	originalExporterIPv4Address
404	0	originalExporterIPv6Address
405	0	originalObservationDomainId
406	0	intermediateProcessId
407	0	ignoredDataRecordTotalCount
408	0	dataLinkFrameType
409	0	sectionOffset
410	0	sectionExportedOctets
411	0	dot1qServiceInstanceTag
412	0	dot1qServiceInstanceId
413	0	dot1qServiceInstancePriority
414	0	dot1qCustomerSourceMacAddress
415	0	dot1qCustomerDestinationMacAddress
417	0	postLayer2OctetDeltaCount
418	0	postMCastLayer2OctetDeltaCount

ElementID	PEN	[名前（Name）]
420	0	layer2OctetTotalCount
421	0	postMCastLayer2OctetTotalCount
422	0	minimumLayer2TotalLength
423	0	maximumLayer2TotalLength
424	0	droppedLayer2OctetDeltaCount
425	0	droppedLayer2OctetTotalCount
426	0	ignoredLayer2OctetTotalCount
427	0	notSentLayer2OctetTotalCount
428	0	layer2OctetDeltaSumOfSquares
429	0	layer2OctetTotalSumOfSquares
430	0	layer2FrameDeltaCount
431	0	layer2FrameTotalCount
432	0	pseudoWireDestinationIPv4Address
433	0	ignoredLayer2FrameTotalCount
434	0	mibObjectValueInteger
435	0	mibObjectValueOctetString
436	0	mibObjectValueOID
437	0	mibObjectValueBits
438	0	mibObjectValueIPAddress
439	0	mibObjectValueCounter
440	0	mibObjectValueGauge
441	0	mibObjectValueTimeTicks

ElementID	PEN	[名前（Name）]
442	0	mibObjectValueUnsigned
443	0	mibObjectValueTable
444	0	mibObjectValueRow
445	0	mibObjectIdentifier
446	0	mibSubIdentifier
447	0	mibIndexIndicator
448	0	mibCaptureTimeSemantics
449	0	mibContextEngineID
450	0	mibContextName
451	0	mibObjectName
452	0	mibObjectDescription
453	0	mibObjectSyntax
454	0	mibModuleName
455	0	mobileIMSI
456	0	mobileMSISDN
457	0	httpStatusCode
458	0	sourceTransportPortsLimit
459	0	httpRequestMethod
460	0	httpRequestHost
461	0	httpRequestTarget
462	0	httpMessageVersion
463	0	natInstanceID

ElementID	PEN	[名前（Name）]
464	0	internalAddressRealm
465	0	externalAddressRealm
466	0	natQuotaExceededEvent
467	0	natThresholdEvent
468	0	httpUserAgent
469	0	httpContentType
470	0	httpReasonPhrase
471	0	maxSessionEntries
472	0	maxBIBEntries
473	0	maxEntriesPerUser
474	0	maxSubscribers
475	0	maxFragmentsPendingReassembly
476	0	addressPoolHighThreshold
477	0	addressPoolLowThreshold
478	0	addressPortMappingHighThreshold
479	0	addressPortMappingLowThreshold
480	0	addressPortMappingPerUserHighThreshold
481	0	globalAddressMappingHighThreshold
482	0	vpnIdentifier
483	0	bgpCommunity
484	0	bgpSourceCommunityList
485	0	bgpDestinationCommunityList

ElementID	PEN	[名前（Name）]
486	0	bgpExtendedCommunity
487	0	bgpSourceExtendedCommunityList
488	0	bgpDestinationExtendedCommunityList
489	0	bgpLargeCommunity
490	0	bgpSourceLargeCommunityList
491	0	bgpDestinationLargeCommunityList
33002	0	ASAFirewallExtendedEvent
34000	0	TrustSecSourceIdentifier
34001	0	TrustSecDestinationIdentifier
34002	0	TrustSecSourceName
34003	0	TrustSecDestinationName
1232	9	SGTSourceId_9
1233	9	SGTDestinationId_9
9292	9	AVCRespsCountDelta_9
9303	9	AVCSumRespTime_9
9306	9	AVCSumServerRespTime_9
12172	9	ETAInitialDataPacket
12173	9	ETASequenceOfPacketLengthsAndTimes_9
12184	9	ETASequenceOfPacketLengths_9
12185	9	ETASequenceOfPacketTimes_9
12235	9	AVCSubApplicationValueIPFIX_9
12332	9	NVMUdid_9

ElementID	PEN	[名前（Name）]
12333	9	NVMLoggedInUser_9
12334	9	NVMOsName_9
12335	9	NVMOsVersion_9
12336	9	NVMSystemManufacturer_9
12337	9	NVMSystemType_9
12338	9	NVMProcessAccount_9
12339	9	NVMParentProcessAccount_9
12340	9	NVMProcessName_9
12341	9	NVMProcessHash_9
12342	9	NVMParentProcessName_9
12343	9	NVMParentProcessHash_9
12344	9	NVMDnsSuffix_9
12345	9	NVMDestinationHostname_9
12346	9	NVML4ByteCountIn_9
12347	9	NVML4ByteCountOut_9
12351	9	NVMOsEdition_9
12352	9	NVMModuleNameList_9
12353	9	NVMModuleHashList_9
12355	9	NVMInterfaceInfoUid_9
12356	9	NVMInterfaceIndex_9
12357	9	NVMInterfaceType_9
12358	9	NVMInterfaceName_9

ElementID	PEN	[名前（Name）]
12359	9	NVMInterfaceDetailsList_9
12360	9	NVMInterfaceMacAddress_9
12361	9	NVMUserAccountType_9
12362	9	NVMProcessAccountType_9
12363	9	NVMParentProcessAccountType_9
12364	9	NVMAgentVersion_9
12365	9	NVMProcessId_9
12366	9	NVMParentProcessId_9
12367	9	NVMProcessPath_9
12368	9	NVMParentProcessPath_9
12369	9	NVMProcessArgs_9
12370	9	NVMParentProcessArgs_9
12371	9	NVMFlowStartMsec_9
12372	9	NVMFlowEndMsec_9
12172	8712	FlowSensorEtaInitialDataPacket_8712
12173	8712	FlowSensorEtaSequenceOfPacketLengthsAndTimes_8712
29794	8712	FlowSensorInitiator_8712
29795	8712	FlowSensorTcpSynAckTotalCount_8712
29796	8712	FlowSensorTcpSrsTotalCount_8712
29797	8712	FlowSensorRoundTripTime_8712
29798	8712	FlowSensorServerResponseTime_8712
29799	8712	FlowSensorRetransmits_8712

ElementID	PEN	[名前（Name）]
29800	8712	FlowSensorTcpBadTotalCount_8712
29801	8712	FlowSensorTcpFragTotalCount_8712
29802	8712	FlowSensorSourceEmailIn_8712
29803	8712	FlowSensorSourceEmailOut_8712
29804	8712	FlowSensorSourceEmailInMess_8712
29805	8712	FlowSensorSourceEmailOut_8712
29806	8712	FlowSensorSourceEmailInTrys_8712
29807	8712	FlowSensorSourceEmailOutTrys_8712
29808	8712	FlowSensorDestinationEmailIn_8712
29809	8712	FlowSensorDestinationEmailOut_8712
29810	8712	FlowSensorDestinationEmailInMess_8712
29811	8712	FlowSensorDestinationEmailOutMess_8712
29812	8712	FlowSensorDestinationEmailInTrys_8712
29813	8712	FlowSensorDestinationEmailOutTrys_8712
29814	8712	FlowSensorTraces_8712
29817	8712	FlowSensorEmbIcmpProtocol_8712
29818	8712	FlowSensorEmbIcmpType_8712
29819	8712	FlowSensorEmbIcmpCode_8712
29820	8712	FlowSensorApplicationIdentifier_8712
29821	8712	FlowSensorBadFlagXmas_8712
29822	8712	FlowSensorBadFlagSynFin_8712
29823	8712	FlowSensorBadFlagBadRst_8712

ElementID	PEN	[名前（Name）]
29824	8712	FlowSensorBadFlagNoAck_8712
29825	8712	FlowSensorBadFlagUrg_8712
29826	8712	FlowSensorBadFlagNoflag_8712
29828	8712	FlowSensorShortFragAttack_8712
29829	8712	FlowSensorFragPktTooShort_8712
29830	8712	FlowSensorFragPktTooLong_8712
29831	8712	FlowSensorFragDifferentSizes_8712
29832	8712	FlowSensorApplicationDetails_8712
29833	8712	FlowSensorSrcSgt_8712
56701	25461	PaloAltoApplicationIdentifier_25461
56702	25461	PaloAltoUserIdentifier_25461

付録 B：サポートされるアラート

次の表に、Cisco Telemetry Broker アラートのリストを示します。

アラート	説明
アプライアンスのディスク容量が致命的に低下（Appliance Disk Space Critically Low）	アプライアンスのディスクの空き容量が 1G 未満です。システムの動作が低下しています。
アプライアンスディスクの容量が低下（Appliance Low Disk Space）	アプライアンスのディスクが容量の 80% に達しました。
ブローカーノードのパケットドロップ（Broker Node Dropping Packets）	このノードはパケットをドロップしています。ブローカーノードが過負荷になっていないか、または設定が間違っていないが確認してください。
ブローカーノードが非表示（Broker Node Not Seen）	このノードは [x] 分間マネージャーと通信していません。
宛先到達不能	宛先が「destination unreachable」ICMP メッセージを送信しました。
不十分な CPU 割り当て（Insufficient CPU Allocated）	このアプライアンスには、推奨される数の CPU が割り当てられていません。
不十分なメモリ割り当て（Insufficient Memory Allocated）	このアプライアンスには、推奨されるメモリ量が割り当てられていません。
有効期限が近い TLS 証明書（TLS Certificate Close to Expiration）	マネージャの TLS 証明書の有効期限が近づいています。新しい証明書をインストールしてください。
期限切れの TLS 証明書（TLS Certificate Expired）	マネージャの TLS 証明書の有効期限が切れています。新しい証明書をインストールしてください。

サポートに連絡

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 Cisco Telemetry Broker パートナーにご連絡ください。
- Cisco Telemetry Broker サポートにご連絡ください。
- 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

マニュアルのバージョン	公開日	説明
1_0	2023 年 4 月	最初のバージョン。
1_1	2023 年 6 月	「Azure の設定」セクションでいくつかの編集を行いました。

著作権情報