Cisco Telemetry Broker 1.2

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 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 では、多くのソースからネットワークテレメトリを取得し、データ形式を変換して、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トラフィックのモニタリングを担当する担当者を対象としています。

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
HTTPS	Hypertext Transfer Protocol（Secure）
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）

省略形	説明
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

ステータス インジケータ

エンティティ（構成済みの宛先、ソース、またはブローカノード）に対して 1 つ以上のアラートまたは警告が存在する場合、関連付けられたメインメニューの見出しの横に、番号と共に赤いインジケータが表示されます。この数は、アラートまたは警告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。[ソース（Source）] ページのステータスインジケータは、ソースの 3 つのサブページ（UDP ソース、VPC フローログ、および NSG フローログ）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、ソースに宛先がなく、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 つの問題がある場合、これは 5 つの問題ではなく 1 つの問題としてカウントされます。

ステータスインジケータの重大度レベル

各重大度レベルの定義については、次の表を参照してください。

重大度	説明
赤（重大）	Cisco Telemetry Broker が重大アラートを割り当てるイベントは、次のイベントのみです。 • 宛先到達不能 • ブローカーノードデータなし（Broker Node No Data） • ブローカーノードのパケットドロップ（Broker Node Dropping Packets）
オレンジ（警告）	Cisco Telemetry Broker が警告を出す必要があると判断したその他すべてのイベント。

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。

次のコンポーネントの表示

ソース

このコンポーネントは、次の情報の過去 24 時間のデータを表示します。

- すべてのソースから受信したデータの量。
- すべてのソースから受信したデータの平均レート。平均値は、過去 30 日間のデータから計算されます。
- アクティブなソースの数。この数値は、ドーナツグラフの中央に表示されます。
- 過去 24 時間にデータを宛先に送信していないソースの数([宛先なし(No Destination)] フィールドの数で表されます)。
- ドーナツグラフには、すべてのソースから受け取ったデータのタイプが表示されます。このグラフのツールチップにカーソルを合わせると、次の情報を表示できます。
    - 過去 24 時間に特定のテレメトリタイプで受信したデータの量
    - テレメトリタイプ名
    - このテレメトリタイプを送信するソースの数

宛先

このコンポーネントは、次の情報の過去 24 時間のデータを表示します。

- すべての宛先に送信されたデータの量。
- すべての宛先に送信されたデータの平均レート。平均値は、過去 30 日間のデータから計算されます。
- 送信されるデータ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。
- ドーナツグラフには、すべての宛先に送信されたデータのタイプが表示されます。このグラフのツールチップにカーソルを合わせると、次の情報を表示できます。
    - 過去 24 時間に特定の宛先に送信されたデータの量
    - 宛先の名前

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。

- 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。
- 未解決のアラートのリストを表示するには、コンポーネントの上部にある [未解決（Unresolved）] フィルタオプションをクリックします。未解決のアラートの数は、フィルタの見出しに表示されます。

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 日間のデータを表示します。

- 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）。
- 使用可能な CPU の数ごとの 1 分間の負荷平均。

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 日間のデータを表示します。

- 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 時間のデータを表示します。

- すべてのソース（グラフの左側のデータで表示）によって受信され、すべての宛先（右側のデータで表示）に送信されたさまざまなタイプのデータ。
- 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。

メトリック

このコンポーネントは、過去 4 時間のデータ（GB 単位）を表示します。

- グラフの上にあるフィルタオプションから、次のフィルタタイプを選択できます。
    - データを表示する測定単位
    - 目的のデータを検索する期間
- 各グラフのドロップダウンメニューから、表示するデータの種類と、データを表示する特定の宛先を選択できます。グラフの上にあるパーセンテージボタンをフィルタとして選択した場合、特定のテレメトリタイプまたは宛先を指定することはできないことに注意してください。

宛先

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。各宛先について、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しているデータソース

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、異なるデータソース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 つのデータソース）を設定できます。

宛先を選択すると、次のような詳細情報を表示できます。

- 宛先名
- Cisco Telemetry Broker を受信するのに使用する IP アドレスとポート（UDP 宛先のみ）
- 宛先のタイプ（SCA 宛先のみ）
- 現在の宛先のステータス
- データソースに対するルールの数
- この宛先が受信しているデータソースの数 Cisco Telemetry Broker
- 宛先に送信されたデータ量の現在の日次合計

この宛先に関連する次のメトリックも表示できます。

- この宛先に設定されているルール

これらのメトリックを次の複数の時間枠で表示できます。

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

宛先の表示

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

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. ブローカーノードと宛先の間に非アクティブ間隔を確立する場合は、[宛先の可用性の確認（Check Destination Availability）] を有効にします。これにより、宛先が応答していない場合、またはテレメトリを受信していない場合にそれを識別できます。詳細については、「**全般**」を参照してください。

> 宛先の可用性の確認機能は、非セキュア Cloud Analytics の宛先でのみ使用できます。

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 IPFIX パケットのみを Secure Cloud Analytics に送信します。
- Cisco Telemetry Broker デプロイメントにトラフィックが少ない場合、SCA 宛先を追加した後、データが [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 を使用してデータを Secure Cloud Analytics に送信します。

キーと URL を見つけるには、次の手順を実行します。

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。

これで、SCA 宛先を追加する準備ができました。

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 からのトラフィック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. 宛先の設定を編集するには、[宛先(Destinations)]タブで宛先の  (編集)アイコンをクリックします。
2. 次のフィールドを更新します。
   - UDP 宛先の場合:[名前(Name)]、[IPアドレス(IP Address)]、[ポート(Address)]、および[宛先の可用性の確認(Check Destination Availability)]トグルスイッチ。
   - SCA 宛先の場合:[名前(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。

宛先のルールの追加

> ⚠ テレメトリを受信するには、少なくとも 1 つのルールを宛先に追加する必要があります。宛先ごとに、最大 1000 のルールを追加できます。

1. [宛先(Destinations)]タブで、該当する宛先サマリーの左下隅にある[+ルールの追加(+ Add Rule)]をクリックします。
2. [受信UDPポート(Receiving UDP Port)]を入力します。
3. この宛先が特定のトラフィックを受信するサブネットを指定する場合は、[サブネット(Subnets)]を 1 つ以上追加します。

> ℹ SCA 宛先のルールを追加するときに、IPv6 サブネットを追加することはできません。

4. [保存(Save)]をクリックします。

ルールの編集

1. [宛先(Destinations)]タブで、宛先をクリックして詳細を表示します。
2. [編集]アイコンをクリックします。
3. [受信UDP ポート(Receiving UDP Port)]と[サブネット(Subnets)]を変更します。
4. [保存(Save)]をクリックします。

ルールの削除

1. [宛先(Destinations)]タブで、宛先をクリックして詳細を表示します。
2. ルールを削除するには、[宛先の削除(Remove Destination)]  をクリックします

UDP Director 設定のインポートとエクスポート

UDP Director、または UDP Director を管理するマネージャから、現在の UDP Director 宛先とルールの設定を XML ファイルとしてエクスポートして、これを Cisco Telemetry Broker にインポートできます。

> ⚠ UDP Director 設定をインポートすると、現在設定されているすべての宛先とルールを含む、現在の Cisco Telemetry Broker 設定が上書きされます。

UDP Director からの UDP Director 設定のエクスポート

UDP Director から UDP Director 設定をエクスポートするには、次の手順を実行します。

1. UDP Director コンソールに **admin** としてログインします。
2. [設定（Configuration）] タブをクリックします。
3. [転送ルール（Forwarding Rules）] をクリックします。
4. [エクスポート（コンフィグレーション ファイルをローカルシステムにエクスポート）（Export (Export the configuration file to local system)）] を選択します。
5. ファイルをワークステーションに保存します。

マネージャからの UDP Director 設定のエクスポート

マネージャから UDP Director 設定をエクスポートするには、次の手順を実行します。

1. Web アプリケーションに **sysadmin** としてログインします。
2. ⚙（[グローバル設定（Global Settings）]）アイコンをクリックします。
3. ドロップダウンメニューから、[UDP Directorの設定（UDP Director Configuration）] を選択します。
4. [アクション（Actions）] メニューをクリックします。
5. [転送ルールのエクスポート（Export Forwarding Rules）] を選択します。
6. [保存（Save）] をクリックします。

Cisco Telemetry Broker への UDP Director 設定のインポート

保存した UDP Director 設定を Cisco Telemetry Broker にインポートするには、次の手順を実行します。

1. Cisco Telemetry Broker マネージャノードにログインします。
2. [グローバル設定（Global Settings）] アイコンをクリックします。
3. [設定（Configuration）] タブをクリックします。
4. [設定のインポート（Import Configuration）] をクリックします。
5. [アップロード（Upload）] をクリックして、保存した XML 設定をアップロードします。プレビューを確認して、このファイルに必要な設定が含まれていることを確認します。
6. チェックボックスをオンにして、続行することを確認します。
7. [インポート（Import）] をクリックします。

到達不能宛先の検出

到達不能宛先検出は、宛先の到達不能をオペレータに警告する Cisco Telemetry Broker の機能で、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。

この機能は、宛先ごとに無効に設定できます。

ソース

Cisco Telemetry Broker メインメニューから [ソース(Sources)] を選択します。

テレメトリ用に特定の UDP ポートをリッスンするようにブローカーノードを明示的に設定する必要はありません。Cisco Telemetry Broker は、送信元に対する有効な宛先ルールが存在する限り、すべてのポートでリッスンし、固有の送信元を記録します(つまり、宛先ルールは受信テレメトリの送信元 IP、および受信 UDP ポートと一致する必要があります)。

したがって、UDP テレメトリを任意のブローカーノード上のテレメトリ ネットワーク インターフェイスのアドレスに送信するように送信元を簡単に設定できます。[ソース(Sources)] タブでは、これらの送信元のリストと、これら送信元が送信するテレメトリを確認できます。送信元が 15 分以上 Cisco Telemetry Broker へのテレメトリの送信に失敗すると、「データなし」警告が表示されます。

Cisco Telemetry Broker は、UDP ソース、VPC フローログ、NSG フローログなど、さまざまなソースタイプをサポートしています。

データソースの表示

1. Cisco Telemetry Broker メインメニューから [ソース(Sources)] 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 ソース
    - VPC フローログ
    - NSG フローログ

UDP ソース

このタブでは、各ソースに設定されているルールの数を表示できます。次を含む、テレメトリ UDP ソースのフローログソースに関する情報が表示されます。

- テレメトリを に送信するために使用される IP アドレスとポート Cisco Telemetry Broker
- ステータス、および最後にテレメトリを送信した時刻(テレメトリを一定期間送信していない場合)
- 宛先に対するルールの数
- Cisco Telemetry Broker への送信バイト数とレート(バイト/秒)

このデータは、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

VPC フローログ

Cisco Telemetry Broker では、s3 バケットから AWS PVC フローログを消費し、IPFIX に変換し、この IPFIX を宛先に送信するように、VPC フローログソースを設定できます。これらのソースは、[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、システム内の次のような既存の各ソースを表示できます。

- テレメトリを に送信するために使用される IP アドレスとポート Cisco Telemetry Broker
- ステータス、および最後にテレメトリを送信した時刻(テレメトリを一定期間送信していない場合)
- 宛先に対するルールの数
- Cisco Telemetry Broker への送信バイト数とレート(バイト/秒)

このデータは、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

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 フローログの削除

1. [ソース(Sources)] ページで、[VPCフローログ(VPC Flow Logs)] タブをクリックします。
2. テーブルにリストされている該当するフローログに対し、編集アイコンをクリックして、フローログの設定を編集します。

VPC フローログの詳細の表示

1. [ソース(Sources)] ページで、[VPCフローログ(VPC Flow Logs)] タブをクリックします。
2. テーブルで、該当するフローログ名をクリックします。

次の情報が表示されます。

- フローログの表示名、S3 バケット名、リージョン、および割り当てられたブローカーノード
- 現在のステータス
- このフローログの送信先の数
- 送信されたデータ量の現在の日次合計
- 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

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 フローログソースを設定できます。これらのソースは、[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、システム内の次のような既存の各ソースを表示できます。

- テレメトリを に送信するために使用される IP アドレスとポート Cisco Telemetry Broker
- ステータス、および最後にテレメトリを送信した時刻（テレメトリを一定期間送信していない場合）
- 宛先に対するルールの数
- Cisco Telemetry Broker への送信バイト数とレート（バイト/秒）

このデータは、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

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. [ソース（Sources）] 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）] 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. [ソース名（Source Name）] フィールドに、ソース IP アドレス名を入力します。
5. [送信元IPアドレス（Source IP Address）] フィールドに、このフローログに割り当てる送信元 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 データを送信するときに、この IP アドレスを送信元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、送信元 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。

   - 送信元 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。
   - 送信元 IP アドレスは、システム内の既存の送信元 IP アドレスと競合してはいけません。
   - 送信元 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データを処理します。
7. フローログデータを取り込む 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。

NSG フローログの編集

1. [ソース(Sources)] ページで、[NSGフローログ(NSG Flow Logs)] タブをクリックします。
2. テーブルにリストされている該当するフローログに対し、  (編集)アイコンをクリックしてフローログの設定を編集します。

NSG フローログの削除

1. [ソース(Sources)] ページで、[NSGフローログ(NSG Flow Logs)] タブをクリックします。
2. テーブルにリストされている該当するフローログに対し、編集アイコンをクリックして、フローログの設定を編集します。

NSG フローログの詳細の表示

1. [ソース(Sources)] ページで、[NSGフローログ(NSG Flow Logs)] タブをクリックします。
2. テーブルで、該当するフローログ名をクリックします。

次の情報が表示されます。

- フローログの表示名、Azure sas_url、および割り当て済みブローカーノード
- 現在のステータス
- このフローログの送信先の数
- 送信されたデータ量の現在の日次合計
- 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

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と IP アドレス
- テレメトリインターフェイスの IP アドレス、速度、および送受信トラフィック
- ブローカーノードのステータス、およびマネージャが最後に通信した時刻
- 所属する高可用性クラスタ(存在する場合)

ここでは、ブローカーノードの追加、ブローカーノードの削除、クラスタの設定、およびブローカーノードのテレメトリインターフェイスの設定を行うことができます。

ブローカーノードを選択して、次のような詳細情報を表示することもできます。

> しきい値は変更できません。

- **[受信レート(Received Rate)]**:[送信元単位(Per Source)] ドロップダウンリストで選択した送信元ごとの、このブローカーノードが経時的に受信するトラフィック。
  - [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( )、該当する送信元から送信されたトラフィックの現在の受信レート値(1 分間隔)を表示できます。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。
- **[送信レート(Sent Rate)]**:このブローカーノードから [宛先単位(Per Destination)] ドロップダウンリストで選択した宛先に経時的に送信されるトラフィック。
  - [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トラフィックの現在の送信レート値(1 分間隔)を表示できます。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。

- **[負荷平均(Load Average)]**: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。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(Memory Usage)]**:メモリの消費量および使用可能合計メモリ。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(Disk Storage)]**:使用されているディスクストレージおよび合計使用可能ストレージ。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。

ページの右上隅にある目的の時間枠をクリックすると、次の複数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

ブローカーノードのメトリックの表示

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. メトリックを表示するブローカーノードをクリックします。
3. 次のいずれかの値を選択して、その期間内のメトリックを表示します。
    - 過去 1 時間(Last Hour)
    - 過去 4 時間(Last 4 Hours)
    - 過去 24 時間(Last 24 Hours)
    - 過去 7 日間(Last 7 Days)
    - 過去 30 日間(Last 30 Days)

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 アドレスが送信元のターゲットとして提供され、送信元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。
- 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)。
- ブローカノードを 1 つのみ持つクラスタを作成できますが、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ブローカノード内のクラスタがありません。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。
- ブローカーノードを持たないクラスタを作成し、後でブローカーノードを追加できます。
- 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. [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. [ブローカーノード名（Broker Node Name）] 列で、該当するブローカノードをクリックします。
3. クラスタの **（編集）**アイコンをクリックします。

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. [ブローカーノード名（Broker Node Name）] 列で、該当するブローカノードをクリックします。
3. クラスタの **（削除）**アイコンをクリックし、選択を確認します。

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。

- マネージャ名、ホスト名、および IP アドレス
- マネージャの現在のステータス
- 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

マネージャに関連するメトリックを表示することもできます。

> しきい値は変更できません。

- **[負荷平均(Load Average)]**:1 分間の CPU 負荷平均。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(Memory Usage)]**:メモリの消費量および使用可能合計メモリ。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(Disk Storage)]**:使用されているディスクストレージおよび合計使用可能ストレージ。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。

> これらのメトリックのいずれか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)] セクションの右上隅にある目的の時間枠をクリックすると、次の複数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

マネージャ情報とメトリックの表示

1. Cisco Telemetry Broker メインメニューから [マネージャノード（Manager Nodes）] を選択します。
2. 次のいずれかの値を選択して、その期間内のメトリックを表示します。
    - 過去 1 時間（Last Hour）
    - 過去 4 時間（Last 4 Hours）
    - 過去 24 時間（Last 24 Hours）
    - 過去 7 日間（Last 7 Days）
    - 過去 30 日間（Last 30 Days）

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。仮想プライベートクラウド（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トラフィックと拒否されたトラフィックをログに記録するか、[承認（Accept）] を選択して承認されたトラフィック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. フローログデータを保存する 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 フローログ送信元の設定

VPC フローログ送信元を設定し、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、[ソース(Sources)] > [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(右上隅のソース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。S 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. [使用するポリシー(Policy to use)] をクリックして、ペインを展開します。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。

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。

ユーザーグループの作成

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 構成 – パート 2

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

VPC フローログデータを処理して 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[VPCフローログの追加(Add VPC Flow Log)]ダイアログ(「VPC フローログソースの設定」のステップ 2 を参照)で、[ソース名(Source Name)]を入力します。
2. [送信元IPアドレス(Source IP Address)]を入力します。Cisco Telemetry Broker は、VPC フローログから生成された IPFIX データを送信するときに、この IP アドレスを送信元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、送信元 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。

   - 送信元 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。
   - 送信元 IP は、システム内の既存の送信元 IP と競合してはいけません。
   - 送信元 IP は、システム内の宛先 IP と競合してはいけません。

1. ドロップダウンメニューから [割り当て済みノード(Assigned Node)] 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データを処理します。
2. フローログデータを取り込む 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。
3. [VPCフローログを追加(Add VPC Flow Log)] をクリックします。
4. 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 フローログ送信元の設定**」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. 「**ユーザーグループの作成**」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。

Azure の設定

次の手順では、Azure 環境から分析用のデータ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。

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

データソースの設定では、Cisco Telemetry Broker がデータソース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. [ソース(Sources)] 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、送信されたトラフィック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データ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データ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. [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

⚠ 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. 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。
4. 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。

5. [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。

次のいずれかの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。

アラート	説明
ブローカーノードデータなし（Broker Node No Data）	関連付けられたノードは、最後の [x] 分間データを転送していません。
ブローカーノードのパケットドロップ（Broker Node Dropping Packets）	受信レートがキャパシティを超えています。
宛先到達不能	宛先が「destination unreachable」ICMP メッセージを送信しました。
アプライアンスのディスクが満杯	アプライアンスのディスクが容量に達しました。

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 サーバーのアドレス（IP 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。

次のいずれかの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。

アラート	説明
ブローカーノードデータなし（Broker Node No Data）	関連付けられたノードは、最後の [x] 分間データを転送していません。
ブローカーノードのパケットドロップ（Broker Node Dropping Packets）	受信レートがキャパシティを超えています。
宛先到達不能	過去 [x] 分間、受信先がハートビートに応答していません。
アプライアンスのディスクが満杯	アプライアンスのディスクが容量に達しました。

ⓘ 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（IP 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
```

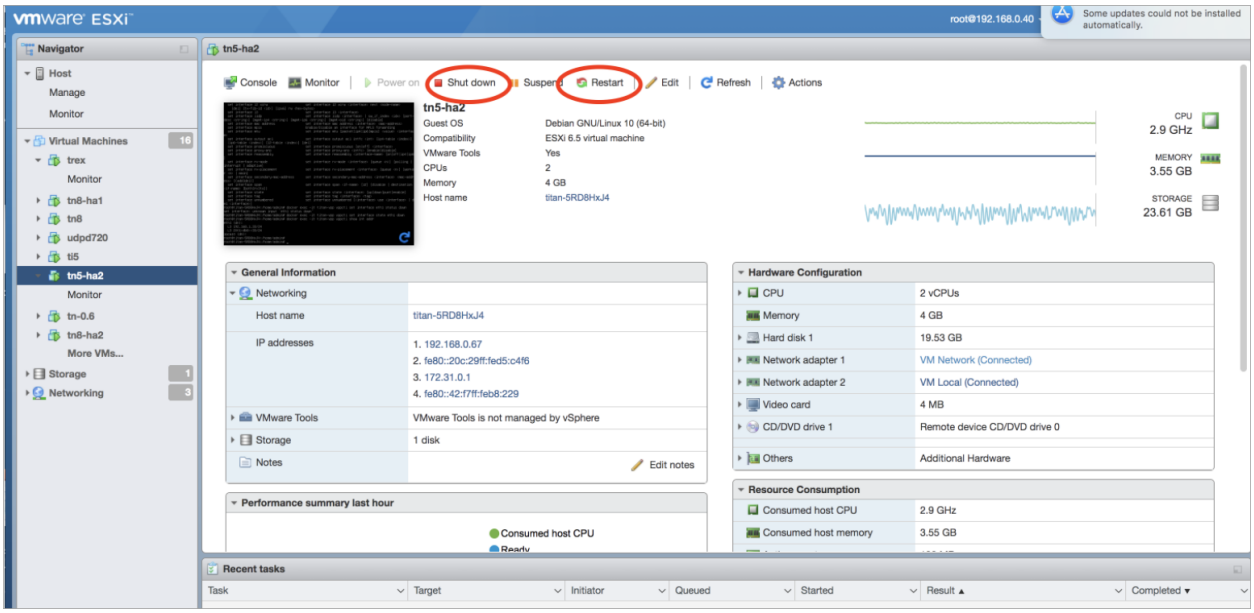
Cisco Telemetry Broker のシャットダウンまたはリブート

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 コンソールから、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. マネージャノードから、VMWare vCenter が提供する仮想マシンにログインします（ユーザー名は **install**）。
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。



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：1-800-553-2447（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

著作権情報

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。