Cisco Cloud APIC 統計

Cisco Cloud APIC 統計の概要

Cisco Cloud Application Policy Infrastructure Controller (APIC) は、クラウド ルータから収集される統計をサポートします。さらに、Amazon Web Services (AWS) フロー ログを処理することによって得られる統計をサポートします。AWS フロー ログは無料のサービスではないため、Cisco Cloud APIC によりこの機能を制御できるポリシーが提供されています。この機能は、デフォルトでイネーブルではありません。

CloudWatch とフロー ログの詳細については、AWS ウェブサイトの Amazon Virtual Private Cloud の「VPC フロー ログ」を参照してください。

Cisco Cloud APIC リリース 5.0(1) 以降、次のことを実行できます。

- フィルターを使用して、AWS フロー ログから特定の情報を表示できます。特定のフロー ログ ポリシー (または VPC) に対して同時に最大 8 つのフィルターを定義できます。送信元または宛先の IP アドレス、ポート、およびプロトコルの組み合わせでフィルタリングできます。詳細については、「Cisco Cloud APIC 統計フィルタ （3 ページ）」を参照してください。
- AWS Transit Gateway との間のトラフィックの統計を収集できます。このガイドのAWS Transit Gateway Statistics （3 ページ）セクションを参照してください。

AWS ネットワーク インターフェイス統計コレクション

AWS は、フロー ログを通じてネットワーク インターフェイスごとの非リアルタイム IP トラフィック情報を提供します。Cisco Cloud APIC は、`cloudCtxProfile` ごとにフロー ログを有効にするためのポリシーを提供します。`cloudCtxProfile` は AWS の VPC にマッピングされるため、`cloudCtxProfile` または VPC ごとにフロー ログを有効にするということは、その VPC に属する各インターフェイスのフロー ログを有効にすることを意味します。フロー ログが有効になると、フロー レコードは定期的に AWS Cloudwatch にプッシュされます。次に、Cisco Cloud APIC はこれらのフロー レコードについて AWS CloudWatch を定期的にポーリングし、これらのレコードを解析して統計を抽出します。フロー レコードを CloudWatch に発行するのに最大 15 分かかることがあるため、Cisco Cloud APIC は CloudWatch へのフロー ログのクエリも 15 分遅らせます。これは、CloudWatch に存在するフロー ログと、Cisco Cloud APIC に表示される対応する統計との間にラグがあることを意味します。Cisco Cloud APIC は、CloudWatch への発行に 15 分以上かかるフロー レコードを処理しません。

Cisco Cloud APIC エンドポイントと cloudEPg 統計処理

Cisco Cloud APIC は、CloudWatch にフロー ログが存在する AWS ネットワーキング エンドポイントごとに、次の統計を抽出します。

- 送信されたバイト数またはパケット数（送信側）
- 受信したバイト数またはパケット数（受信側）
- 拒否されたバイト数またはパケット数（送信側ドロップ）
- ドロップされたバイト数またはパケット数 (受信側ドロップ)

これらの統計は、`cloudEpInfoHolder` オブザーバブルに関連付けられています。

また、Cisco Cloud APIC は、フロー ログ レコードをリージョンごとに 1 つ以上の `cloudEPg` オブジェクトにマッピングします。これは、`cloudEPg` が複数のリージョンに存在する可能性があるためです。これらの統計は、`cloudRgInfoHolder` オブザーバブルに関連付けられています。このオブザーバブルは `cloudEPg` の子であり、cloudRgInfoHolder の子の統計を蓄積すると、`cloudEPg` の統計になります。`cloudEPg` は、次の統計をサポートしています。

- 送信されたバイト数またはパケット数（送信側）
- 受信したバイト数またはパケット数（受信側）
- 拒否されたバイト数またはパケット数（送信側ドロップ）
- ドロップされたバイト数またはパケット数 (受信側ドロップ)

`cloudEPg` 統計は、`fvApp` まで集計され、次に `fvTenant` まで集計されます。

Cisco Cloud APIC 統計フィルタ

Cisco Cloud Application Policy Infrastructure Controller リリース 5.0(1) 以降、フィルタを使用して、Amazon Web Services (AWS) フロー ログから特定の情報を表示できます。

フィルターが展開されているエンドポイントごとに統計が収集されます。フィルタを使用すると、送信元または送信先の IP アドレス、ポート、およびプロトコルの組み合わせによってフィルタリングされたフローに関する情報を表示できます。特定の AWS ログ グループに対して同時に最大 8 つのフィルタを定義できます。

統計フィルタには、次の 3 つの属性があります。

- **PeerIP:** フィルタリングする IPv4 アドレス
- **PeerPort:** リッスンするポート番号
- **プロトコル:** リッスンするプロトコル番号

（注） Cisco Cloud APIC GUI を使用して統計フィルタを構成することをお勧めします。代わりに REST API を使用することもできます。ただし、そうしてから GUI に切り替えると、機能が不完全に見えます。選択した方法に固執する必要があります。

統計フィルタの使用は、Virtual Private Cloud (VPC) フロー ログの有効化に依存します。統計フィルタを構成する前に、ログを有効にする必要があります。

AWS CloudWatch に保存されるフロー ログは、フロー ログ レコードで構成されます。Cisco Cloud Application Policy Infrastructure Controller (APIC) は、フロー ログ レコードを解析して統計を抽出します。

特定のフロー レコードが発生してから AWS CloudWatch に存在するまで、最大 15 分かかることがあります。Cisco Cloud APIC は過去 15 分以上に発生したフロー レコードをポーリングします。AWS CloudWatch に表示されるまでに 15 分以上かかるフロー レコードは処理しません。

AWS Transit Gateway Statistics

You can collect statistics for traffic going through Amazon Web Services (AWS) Transit Gateways on both the infra tenant and the user tenant. Statistics reported for user tenant represent the traffic of an attachment between an user VPC and an AWS Transit Gateway. Statistics reported from infra tenant represents the traffic of an attachment between an infra VPC and a Transit Gateway.

The following statistics are collected for AWS Transit Gateway:

- Ingress packets
- Ingress packet bytes
- Ingress packet drops

- Ingress packet drop bytes
- Egress packets
- Egress packet bytes
- Egress packet drops
- Egress packet drop bytes

You can enable infra tenant Transit Gateway statistics collection from the Cisco Cloud Application Policy Infrastructure Controller **Setup - Region Management** page. See the section "Set Up the Cloud Site to Use AWS Transit Gateway" in *Increasing Bandwidth Between VPCs by Using AWS Transit Gateway*.

You can enable user tenant Transit Gateway statistics collection by enabling flow logs on the user VPC. See the sections VPC フロー ログの有効化, on page 4 and Cisco Cloud APIC GUI を使用した VPC フロー ログの有効化, on page 4 in this guide.

To view AWS Transit Gateway statistics, in the Cisco Cloud APIC GUI, click the **Statistics** tab and then click **AWS Transit Gateway** in the left navigation pane. The central pane displays the information.

VPC フロー ログの有効化

VPC フロー ログを有効にする手順:

1. ログ グループ ポリシーを定義します。
2. フロー ログ ポリシーを定義し、最初の手順で定義したログ グループを関連付けます。
3. フロー ログ ポリシーを 1 つ以上の `cloudCtxProfile` に関連付けます。

ログ グループ プロパティ:

- **name**：フロー ログが送信される CloudWatch 内の場所。

（注） AWS でプログラムされている実際のログ グループ名は、`<tenant name><cloudCtxProfile name><log group name>` です。

- **retention**：CloudWatch にログを保存する期間の長さ。デフォルトは 5 日です。

フロー ログのプロパティ:

- **trafficType**：収集するトラフィックのタイプ。サポートされているタイプは、**all**、**accept only**、**reject only** です。デフォルトは、**all** です。

Cisco Cloud APIC GUI を使用した VPC フロー ログの有効化

このセクションでは、Cisco Cloud APIC GUI を使用した VRF フロー ログを有効にする方法について説明します。

（注） フィルタを使用して AWS フロー ログから特定の情報を表示する場合は、この手順のオプションのステップを実行します。

ステップ 1 **[ナビゲーション（Navigation）] メニュー** > **[アプリケーション管理（Application Management）]** > **[テナント（Tenants）]**の順にクリックします。

[テナント（Tenant）] ウィンドウが表示され、テナントがサマリー テーブルの行としてリストされます。

ステップ 2 テナントをダブルクリックします。

テナント ダイアログ ボックスが [Work] ペインの上に表示されます。テナント ダイアログ ボックスには、**[概要（Overview）]**、**[クラウド リソース（Cloud Resources）]**、**[アプリケーション管理（Application Management）]**、**[統計（Statistics）]**、および **[イベント分析（Event Analytics）]** タブが表示されます。

ステップ 3 [Statistics] タブをクリックします。

The **EPGs**, **CCRs**, and **Flow Log Collection** subtabs appear.

ステップ 4 **[フローログの収集（Flow Log Collection）]** をクリックします。

[フローログの収集の設定（Flow Log Collection Setting）]情報がダイアログ ボックスの上部に表示され、右上隅に**編集**アイコンが表示されます。

ステップ 5 [Edit] アイコンをクリックします。

[フロー ログ収集設定] ダイアログ ボックスが表示されます。

ステップ 6 次の *[フロー ログ収集設定（Flow Log Collection Settings）]* ダイアログボックスのフィールドの表に示されているように、各フィールドに適切な値を入力し、続行します。

表 *1:* フローログ収集設定ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
ログに記録するトラフィックのタイプ	**[ログに記録するトラフィックのタイプ]** ドロップダウン リストをクリックし、次のオプションを選択します。 • デフォルトによる**すべてのトラフィック** • **許可されたトラフィックのみ** • **拒否されたトラフィックのみ**
Destination	**[接続先（Destination）]** ドロップダウン リストをクリックし、**[CloudWatch (デフォルト)]** を選択します。

[プロパティ（Properties）]	説明
保持	**[冗長性（Retention）]** ドロップダウンリストをクリックし、次のオプションを選択します。 • **1日** • **3日** • **5 日** (デフォルト) • **1 ヵ月** • **13 ヵ月** • **18 ヵ月** • **2ヵ月** • **3 か月** • **4 ヵ月** • **5 ヵ月** • **6 ヵ月** • **1 週間** • **2 週間** • **1 年** • **10 年** • **2 年** • **5 年**

ステップ 7 (オプション) 次のタスクを実行して、フロー フィルタを追加して、送信元と送信先の IP アドレス、ポート、またはプロトコルに関する情報を取得します。

統計フィルターの詳細については、セクション Cisco Cloud APIC 統計フィルタ （3 ページ） を参照してください。

a) **[フロー フィルタの追加]** ダイアログ ボックスの下部にある **[フロー ログ収集設定（Flow Log Collection Settings）]** をクリックします。

フィルタ属性のフィールドが表示されます。

[フロー フィルタの追加] ボタンをクリックすると、新しいフィルタが作成されていることがわかります。属性を入力します。

b) **[ピア IP（Peer IP）]** フィールドで、ピアの IPv4 IP アドレスを入力します。

アドレスは x.x.x.x/x の形式である必要があります。どのネットワークを監視するかをフィルタに指示します。0.0.0.0/0 のアドレスはすべてに一致します。

c) （オプション）**[プロトコル（Protocol）]** ドロップダウン リストから、プロトコルを選択します。

選択肢は 0 ～ 255 の整数です。255 を入力すると、どのプロトコルにも一致します。よく知られたプロトコルは、テキスト形式が指定されている場合に翻訳されます。

• "icmp": 1	• "igp": 9	• "eigrp": 88
• "igmp": 2	• "l2tp": 115	• "ospfigp": 89
• "tcp": 6	• "udp": 17	• "pim": 103
• egp(8)	• "icmpv6": 58	

d) (オプション) **[ピア ポート]** フィールドに、リッスンするポート番号を入力します。

この番号は、0 ～ 65535 の整数、または既知のポート番号のテキスト入力である必要があります。0 を入力すると、すべてのポートに一致します。よく知られたプロトコルは、テキスト形式が指定されている場合に翻訳されます。

• "dns": 53	• "http": 80	• "rtsp": 554
• "ftpData": 20	• "https": 443	• "pop3": 110
• "smtp": 25		

e) (オプション) **[アクティブ]** チェックボックスをオンにして、チェック アイコンをクリックします。

ステップ 8 [保存（Save）] をクリックします。

REST API を使用した VPC フロー ログの有効化

このセクションでは、REST API を使用して VPC フロー ログを有効にする方法を示します。

ステップ 1 ログ グループの作成:

```
<cloudAwsLogGroup name="lg1" retention="days-3" status="">
    </cloudAwsLogGroup>
```

ステップ 2 フロー ログ ポリシーの作成:

```
<cloudAwsFlowLogPol name="flowLog1" trafficType="ALL" status="">
        <cloudRsToLogGrp tDn="uni/tn-t20/loggrp-lg1" status=""/>
    </cloudAwsFlowLogPol>
```

ステップ 3 CtxProfile からフロー ログ ポリシーへの関係を作成します。

```
    <cloudCtxProfile name=" vrf1" status="">
```

```
  <cloudRsCtxToFlowLog tnCloudAwsFlowLogPolName="flowLog1" status=""/>
</cloudCtxProfile>
```

クラウド ルータ統計

これらの統計は、クラウド ルータで利用できます。

- 受信側パケット
- 送信側パケット
- 受信側バイト
- 送信側バイト

Cisco Cloud Application Policy Infrastructure Controller(APIC) は、次の粒度でクラウド ルータの統計情報を収集して保存します。

- 15分
- 1 時間
- 1ヶ月
- 1 年

収集メカニズム

各クラウド ルータ インスタンスは、物理インターフェイスおよびトンネル インターフェイスごとに前述の 4-stat 値をキャプチャして保存します。

Cisco Cloud Application Policy Infrastructure Controller(APIC) は、これらの統計についてクラウド ルータにクエリを実行し、応答を Cisco Cloud APIC のクラウド ルータ統計にマッピングします。統計クエリは、トンネルが稼働している限り、5 分ごとに繰り返されます。

RAW 統計情報

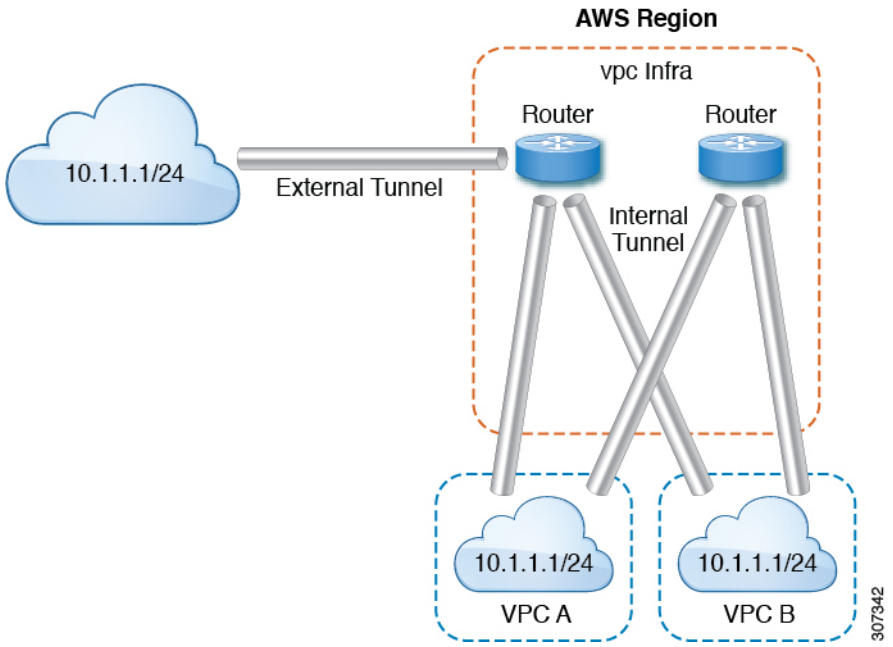
生の統計は 2 Dns の下に保存されます。

- `uni/tn-<infraTenant>/ctx-<infraCtx>/region-<infraRegion>/router-<csrname>/to-<ip or user-region>/tunn-<tunnel-id>`
- `uni/tn-<userTenant>/ctx-<userCtx>/region-<userRegion>/region-<infraRegion>/router-<csrname>/tunn-<tunnel-id>`

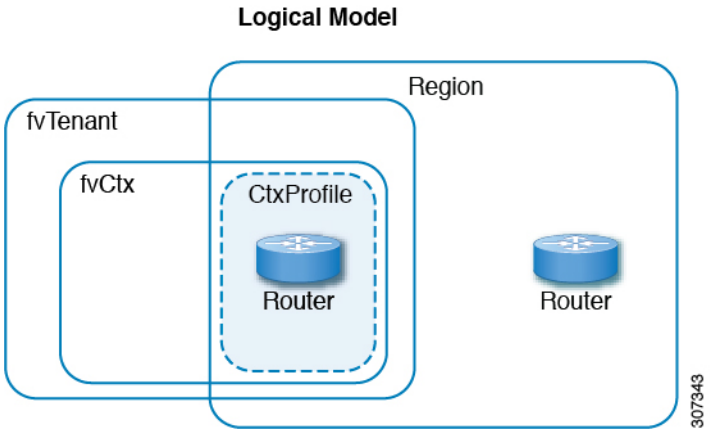
（注）

- 2 番目の Dn ホルダーは、クラウド ルータに接続されているユーザー エンドポイントから見た統計です。These statistics are hence flipped (Ingress on the CCR becomes egress on the user region)
- すべてのトンネルに対応するユーザー dn があるわけではありません。これは、内部トンネルにのみ適用されます。外部トンネルの統計は、1 番目の Dn でのみ使用できます。

次の図では、内部トンネルはユーザー VPC とインフラ VPC の間にあります。The infra VPC contains the CCR router. The user VPC can contain the CCR or VGW router. Cisco Cloud APIC creates these tunnels. その結果、インフラ側とユーザー側の両方で統計を利用できます。外部トンネルは、インフラ VPC と外部 IP アドレスの間にあります。統計はインフラ側 (Dn-1) でのみ使用できます。



論理モデル図では、テナントはインフラまたはユーザー テナントです。VRF (または `fvCtx`) をテナント内 (テナントごと) に設定します。VRF は、1 つのリージョン内にある場合もあれば、複数のリージョンにまたがる場合もあります。



集計された統計

統計は、DN の各親レベルで集計されます。前述のケースでは、トンネルの統計、統計は宛先 IP、クラウド ルータ、リージョン、vrf (`ctx`)、およびテナントに集約されます。

たとえば、インフラ クラウド ルータからユーザー リージョンへのエグレス パケットを見つけたい場合は、
`uni/tn-<infraTenant>/ctx-<infraCtx>/region-<infraRegion>/router-<csrname>/to-<ip or user-region>/` で利用できます。

ユーザー region1 と infra region2 の間のすべてのパケットを取得する場合は、
`uni/tn-<userTenant>/ctx-<userCtx>/region-<userRegion>/region-<infraRegion>/` で使用できます。

また、`cloudCtxProfile` ごとの統計を検索する場合は、
`uni/tn-<userTenant>/ctx-<userCtx>/region-<userRegion>/` または
`uni/tn-<infraTenant>/ctx-<infraCtx>/region-<infraRegion>/` で利用できます。

クラウド ルータ GUI 統計

Cisco Cloud APIC GUI では、テナント、VRF、インフラ リージョン、およびクラウド コンテキスト プロファイルの下で使用可能な統計が表示されます。

Amazon Web Services (AWS) Transit Gateway の統計の場合は、**[クラウド コンテキスト プロファイル]** 作業ペインで、**[AWS Transit Gateway]** をクリックします。他のすべての統計の場合は、**[クラウド コンテキスト プロファイル]** 作業ペインで、**[エンドポイント]** をクリックします。