



Cisco Cloud Network Controller 統計情報

- [Google クラウド 統計について \(1 ページ\)](#)
- [統計情報フィルタについて \(2 ページ\)](#)
- [Google クラウド統計情報の構成に関する注意事項と制限事項 \(4 ページ\)](#)
- [ルータ統計情報の表示 \(5 ページ\)](#)
- [フロー ログ統計を有効化 \(7 ページ\)](#)
- [GUI を使用した統計情報フィルタの定義 \(8 ページ\)](#)
- [フロー ログ統計の表示 \(10 ページ\)](#)
- [REST API を使用した VPC フロー ログの有効化 \(12 ページ\)](#)
- [REST API を使用した統計情報フィルタの定義 \(13 ページ\)](#)

Google クラウド 統計について

Google クラウドフローログの処理によって取得された統計情報を表示できます。さらに、Cisco Catalyst 8000V ルータから収集された統計情報を表示できます。

Cisco クラウド ネットワーク コントローラ リリース 25.1 (1) 以降では、Google クラウド フローログから取得された統計にフィルタを適用することもできます。

ルータ統計

Cisco クラウド ネットワーク コントローラを使用すると、テナント内の個々のクラウド コンテキスト プロファイルのルータ統計情報を表示できます。クラウド コンテキスト プロファイル内の Cisco Catalyst 8000V ルータの統計情報が表示されます。

各ルータインスタンスは、物理インターフェイスとトンネルインターフェイスごとに、入力および出力バイトとパケットの統計情報をキャプチャして保存します。Cisco クラウド ネットワーク コントローラは、これらの統計についてルータにクエリを実行し、応答を Cisco クラウド ネットワーク コントローラの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。Cisco クラウド ネットワーク コントローラ GUI には、ルータについて収集された統計情報が表示されます。

フロー統計情報

Cisco クラウド ネットワーク コントローラを使用すると、テナント内の個々のクラウド コンテキスト プロファイルのフロー ログ統計を有効にすることができます。クラウド コンテキスト プロファイルの統計情報が有効になっている場合、対応する VPC 内のすべての IP アドレスの統計情報が収集されます。使用可能な統計情報には、VPC、リージョン、およびエンドポイントの内部および外部の入力バイトと出力バイトとパケットが含まれます。

収集された統計情報は、次の階層で集約されます。

- IP 統計情報は、エンドポイント統計情報を決定するために集約されます。
- エンドポイント統計情報は、ゾーン統計情報を決定するために集約されます。
- ゾーンの統計情報は、サブネットの統計情報を決定するために集約されます。
- サブネット統計情報は、リージョン統計情報を決定するために集約されます。
- リージョン統計情報は、VPC 統計情報を決定するために集約されます。

Cisco クラウド ネットワーク コントローラ GUI には、VPC、リージョン、およびエンドポイントの収集された統計が表示されます。

Google クラウド フロー ログの詳細については、Google クラウド ウェブサイトで「VPC フロー ログ」を参照します。

統計情報フィルタについて

Cisco クラウド ネットワーク コントローラ リリース 25.1 (1) 以降では、Google Cloud フロー ログから取得された統計にフィルタを適用できます。

フィルタ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、IP アドレスのペアと特定のポートまたはプロトコル間のフローに関する情報をキャプチャできます。

統計フィルタには、次の3つの属性があります。

1. [ピアIP (Peer IP)]: フィルタ処理する IPv4 アドレス。
2. プロトコル: リッスンするプロトコル番号
3. PeerPort: リッスンするポート番号

GCP フロー ログレコードはドロップされたトラフィックに関する情報を提供しないため、各エンドポイントについて収集された統計情報には、フィルタ処理後に次のフィールドのみが含まれます。

1. 送信パケット数
2. 送信バイト数
3. 受信パケット数

4. 受信されたバイト数



(注) 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。

統計情報フィルタの集約

Google Cloud は、次の各レベルでフィルタ処理された統計情報の集約をサポートしています。

1. エンドポイント
2. リージョン
3. VPC

フィルタ処理された統計情報は 15 分ごとに自動的に集約され、表形式で表示されます。次の表に、統計フィルタ処理集約を各レベルで表示できる形式を示します。

収集されたフィルタ処理された統計情報は、フローログ統計情報と同じ階層に従うように集約されます。

	エンドポイント	リージョン (Region)	VPC
Dn format	Ep Dn/sf- (フィルタ処理)	Rg Dn/sf- (フィルタ処理)	VPC Dn/sf- (フィルタ処理)
例	uni/tn-t1/vpc-vpc-3/ rg-us-west1/sn-[20.20.10.0/24]/ zne-us-west1-b/ep-[instance-2/nic0]/ sf-sfpeerip-34.0.0.0:8- sfpeerport-22-sfprotocol-6	uni/tn-t1/vpc-vpc-3/ rg-us-west1/sf-sfpeerip-34.83.229.0:24- sfpeerport-22-sfprotocol-6	uni/tn-t1/vpc-vpc-3/ sf-sfpeerip-34.83.229.0:24- sfpeerport-22-sfproto

統計フィルタ処理による VPC 間統計

Google Cloud 統計フィルタ処理は、特定のネットワーク、プロトコル、およびポートの統計を収集する機能を提供します。これにより、特定のネットワークでフィルタ処理を定義することで、VPC の特定のペアの VPC 間統計情報を提供できます。

また、特定のプロトコルとポートをフィルタ処理に追加することで、VPC ペア間の特定のタイプのトラフィックの統計情報を提供することもできます。

VPC 間統計情報オブジェクトは、各 VPC で定義されたフィルタ処理の数に基づいて、各 VPC の下に表示されます。各 VPC で最大 8 つのフィルタ処理を定義できます。

VPC 間統計情報を表示できる例を次に示します。

インフラ VPC に接続されている 3 つの VPC があり、VPC1 は VPC2 および VPC3 と通信しています。

VPC1 の IP フィールドに VPC2 のネットワークで定義されたフィルタ処理がある場合、VPC1 の観点から VPC1 と VPC2 間のトラフィック フローを示す VPC 間統計オブジェクトが VPC1 の下に作成されます。

VPC3 に、IP フィールドに VPC1 のネットワーク、ポート フィールドに SSH を使用して定義されたフィルタ処理がある場合、VPC3 の観点から VPC1 と VPC3 間の SSH トラフィック フローを表す VPC 間統計オブジェクトが VPC3 の下に作成されます。

GCP フローログレコードはドロップされたトラフィックに関する情報を提供しないため、各エンドポイントのフィルタ処理後、統計オブジェクトには次のフィールドのみが含まれます。

1. 送信パケット数
2. 送信バイト数
3. 受信パケット数
4. 受信されたバイト数

フィルタ処理統計情報は、各 NIC レベルで収集されます。NIC レベルのフィルタ処理統計情報は、VPC レベルの特定のフィルタ処理に一致する統計情報を取得するために、VPC の下の特定のフィルタ処理に対してすべて集約されます。特定の VPC のネットワークに一致するように定義されたフィルタ処理は、その VPC へのすべてのトラフィック フローを提供しますが、特定のプロトコルとポートを使用して特定の VPC のネットワークに一致するように定義されたフィルタ処理は、その VPC への特定のタイプのトラフィック フローを提供します。

Google クラウド統計情報の構成に関する注意事項と制限事項

Google クラウド統計を収集するために Cisco クラウド ネットワーク コントローラ を構成する場合のガイドラインと制限事項は次のとおりです。

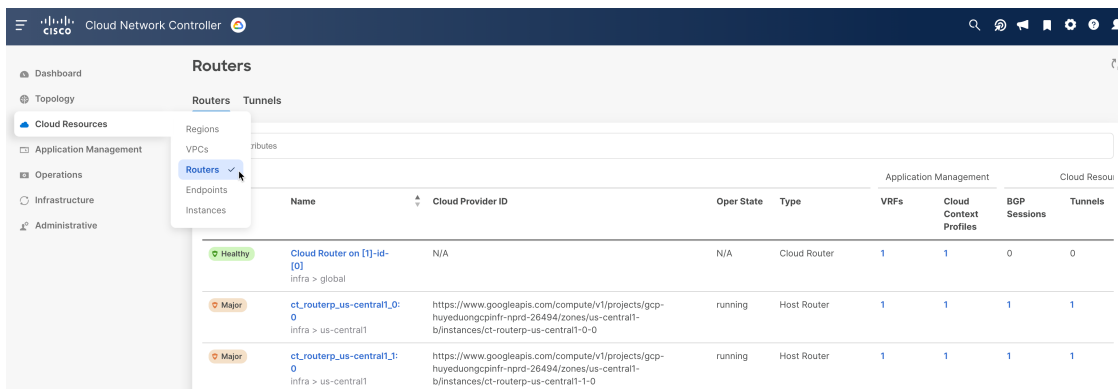
- Cisco Catalyst 8000V ルータが Cisco クラウド ネットワーク コントローラ で起動すると、ルータ統計情報がデフォルトで有効になります。
- フロー ログ統計機能は、デフォルトではイネーブルになっていません。
- フロー ログ統計情報は、テナント内の個々のコンテキストプロファイルに対して有効にできます。この場合、フロー ログは、対応する VPC に属するすべてのサブネットでも有効になります。
- フロー ログは 1 分間隔で集約されます。集約間隔とサンプル レートは構成できません。
- ドロップされたトラフィックの統計は、フロー ログではサポートされていません。
- 統計フィルタ処理は、ドロップ/拒否されたパケットまたはバイトには提供されません。
- ザーンとサブネットの統計情報は表示されません。

ルータ統計情報の表示

Cisco クラウド ネットワーク コントローラ GUI では、Cisco Catalyst 8000V ルータの統計情報をグラフで表示できます。各ルータで使用可能な統計情報には、入力および出力のバイト数とパケット数が含まれます。各カウンタのピーク値は、ピーク値がいつ発生したかを示すタイムスタンプとともに表示されます。

この手順の例では、Cisco クラウド ネットワーク コントローラ GUI でルータの統計情報を表示する方法を示します。

ステップ 1 統計情報を表示する Cisco Catalyst 8000V ルータを選択します。



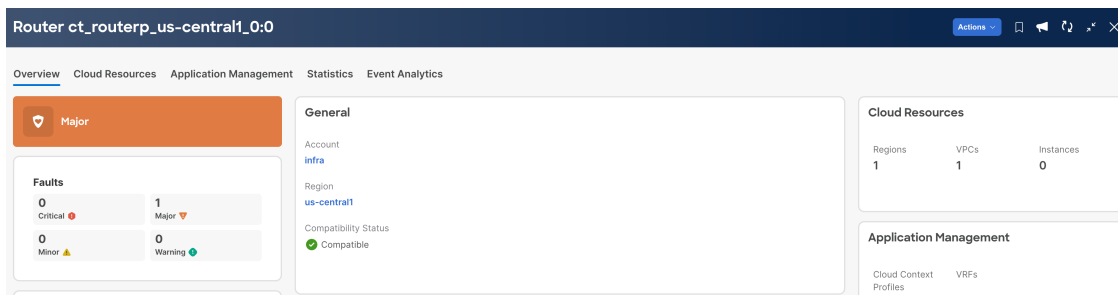
- a) ナビゲーションメニューから [クラウド情報技術 (Cloud Resources)] > [ルータ (Routers)] を選択します。

作業ウィンドウに [ルータ (Routers)] サマリーテーブルが表示されます。

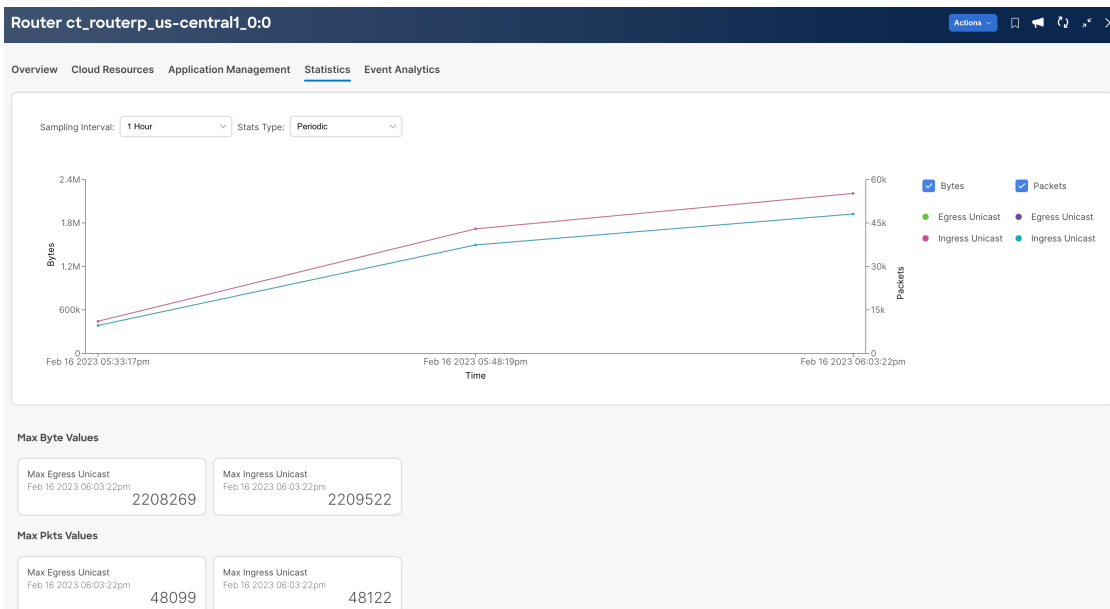
- b) サマリーテーブルで、ルータの名前をダブルクリックします。

ルータ ダイアログボックスが [仕事 (Work)] ペインの上に表示されます。ルータ ダイアログボックスは、[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)] タブを表示します。

ステップ 2 [Statistics] タブをクリックします。



ルータ統計情報のグラフィカルビューが、最大値のテーブルとともに表示されます。



ステップ3 統計情報の表示を構成します。

表示される統計情報のパラメータを構成するには、次の設定を変更します：

【プロパティ (Properties)】	説明
サンプリング間隔	間隔を選択します： <ul style="list-style-type: none"> • 1 時間 • 12時間 • 1日 • 週 1 回 • 1ヵ月
統計情報タイプ	表示タイプを選択します。 <ul style="list-style-type: none"> • 期間：この間隔のカウンタの値（「1 時間」間隔など） • 累積：最初からのカウンタの合計値 • [傾向 (Trend)]：前の間隔をこの間隔と比較し、傾向が増加しているか減少しているかを判断します。 • レート：定期的な値/間隔
バイト	バイトカウンタ グラフを表示するには、このチェックボックスを選択します。グラフの左側の縦軸は、バイト数を示します。

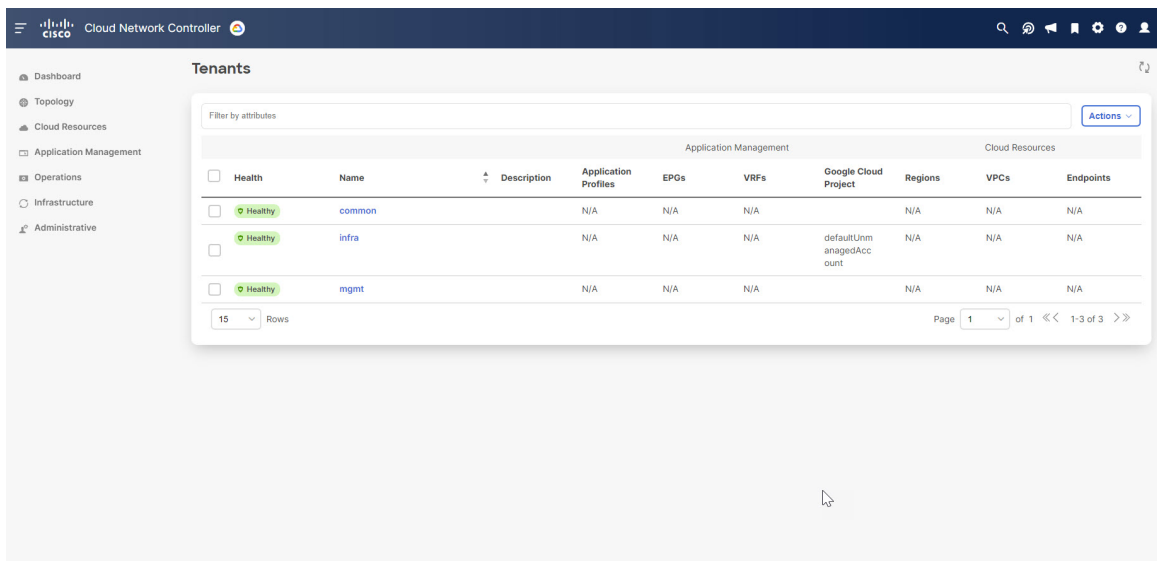
[プロパティ (Properties)]	説明
Packets	パケット カウンタ グラフを表示するには、このチェックボックスを選択します。グラフの右側の縦軸は、パケット数を示します。

フロー ログ統計を有効化

テナント内の個々のコンテキストプロファイルの Google Cloud フロー ログ統計の収集を有効にできます。その後、それぞれのクラウド情報技術 GUI メニューで VPC、リージョン、およびエンドポイントの統計情報を表示できます。

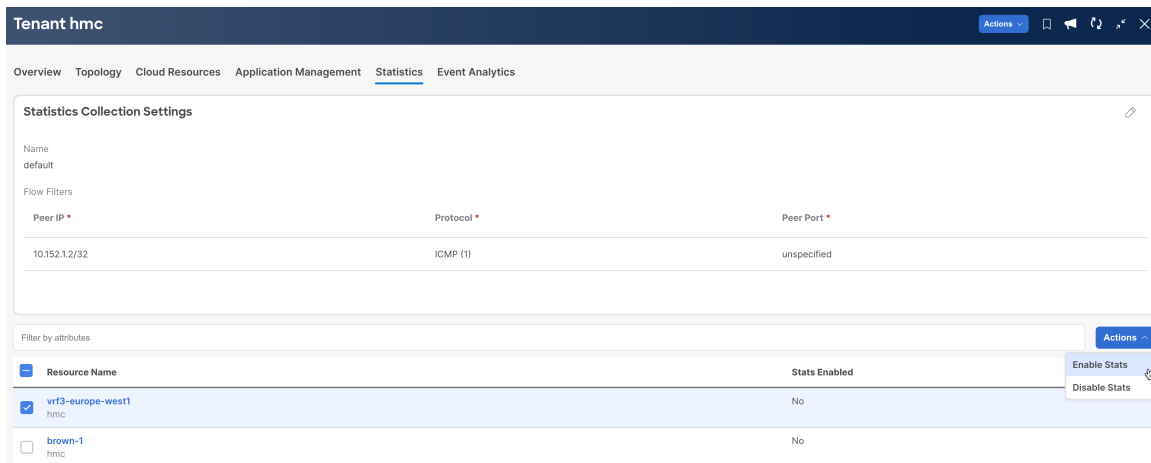
Cisco クラウド ネットワーク コントローラ GUI を使用したフロー ログ統計の有効化

ステップ 1 フローログ統計を有効にする情報技術を含むテナントを選択します。



- ナビゲーションメニューから、[アプリケーション管理 (Application Management)] >> [テナント (Tenants)] を選択します。
作業ウィンドウに [テナント (Tenants)] サマリ テーブルが表示されます。
- サマリ テーブルで、テナントの名前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 [仕事 (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)]、[トポロジ (Topology)]、[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 2 目的の情報技術でフロー ログ統計情報収集を有効にします。



- a) テナントのダイアログ ボックスで、**[統計 (Statistics)]** タブを選択します。
[情報技術名 (Resource Name)] テーブルが表示され、コンテキストプロファイルがテーブルの行としてリストされます。**[統計有効 (Stats Enabled)]** 列は、各情報技術に対してフローログ統計が有効になっているかどうかを示します。
- b) 該当する製品情報技術の横にあるチェックボックスをオンにします。
- c) テナントダイアログ ボックスの右上で、**[アクション (Actions)]** メニューをクリックし、**[統計の有効化 (Enable Stats)]** を選択します。

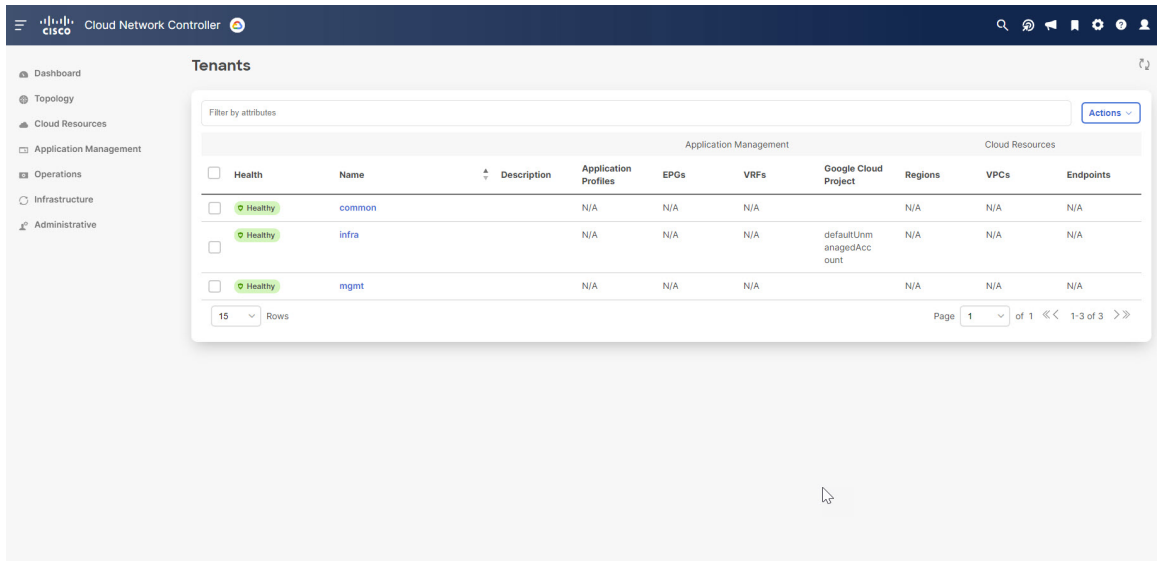
GUI を使用した統計情報フィルタの定義

テナントの Google クラウドフロー ログから取得された統計情報にフィルタを適用できます。作成すると、VPC、リージョン、およびエンドポイントのフィルタ処理された統計をそれぞれの **[クラウド情報技術 (Cloud Resources)]** GUI メニューで表示できます。

始める前に

[フロー ログ統計を有効化 \(7 ページ\)](#) の手順を使用して、目的のクラウドコンテキストプロファイルの Google Cloud フローログ統計を有効にします。

ステップ 1 フローログ統計が有効になっている情報技術を含むテナントを選択します。



- a) ナビゲーションメニューから、[アプリケーション管理（Application Management）]>>[テナント（Tenants）]を選択します。
- 作業ウィンドウに[テナント（Tenants）]サマリテーブルが表示されます。
- b) サマリテーブルで、テナントの名前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[仕事（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）]、[トポロジ（Topology）]、[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。
- [統計（Statistics）]タブを選択して、作業ペインで開きます。

ステップ2 [統計の収集の設定（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（鉛筆）（edit (pencil)）]アイコンが表示されます。

ステップ3 [編集（鉛筆）（edit (pencil)）]アイコンをクリックします。

[統計収集設定（Statistics Collection Settings）]ダイアログボックスが表示されます。

ステップ4 [フローフィルタの追加]ダイアログボックスの[統計収集設定（Statistics Collection Settings）]をクリックします。

[フローフィルタの追加]ボタンをクリックすると、塗りつぶされる必要がある次の属性の新しいフィルタが作成されるのが表示されます。

- a) （注） フィルタ処理がテナントに適用されるように、[現用系（Active）]チェックボックスがオンになっていることを確認します。[現用系（Active）]チェックボックスを選択せずにフィルタ処理を作成した場合、フィルタ処理は適用されず、フィルタ処理された統計を表示できません。

[現用系（Active）]フィールドで、チェックボックスをオンにしてフィルタ処理を適用します。

- 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。

- c) [**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。
- d) [**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。

ステップ 5 チェック アイコンをクリックして[**保存 (Save)**] をクリックします。

フロー ログ統計の表示

Cisco クラウド ネットワーク コントローラ GUI では、VPC、リージョン、およびエンドポイントの統計をグラフで表示できます。それぞれで使用可能な統計情報には、入力および出力のバイト数とパケット数が含まれます。VPC とリージョンの場合、統計情報はさらに次のカテゴリに分類されます：

- 統計：フロー ログ レコードから抽出されたすべてのトラフィック カウンタ。
- リージョン間統計：特定のリージョンについて、VPC 内の他のリージョンとの間で送受信されるすべての入力および出力トラフィック。
- 外部統計：送信元または宛先が VPC の外部にあるすべての入力および出力トラフィック。
- ゾーン間統計：特定のゾーンについて、同じリージョンおよび VPC 内の他のゾーンとの間で送受信されるすべての入力および出力トラフィック。これらの集約された統計情報は、[**リージョン (region)**] ページと VPC ページで確認できます。

各カウンタのピーク値は、ピーク値がいつ発生したかを示すタイムスタンプとともに表示されます。

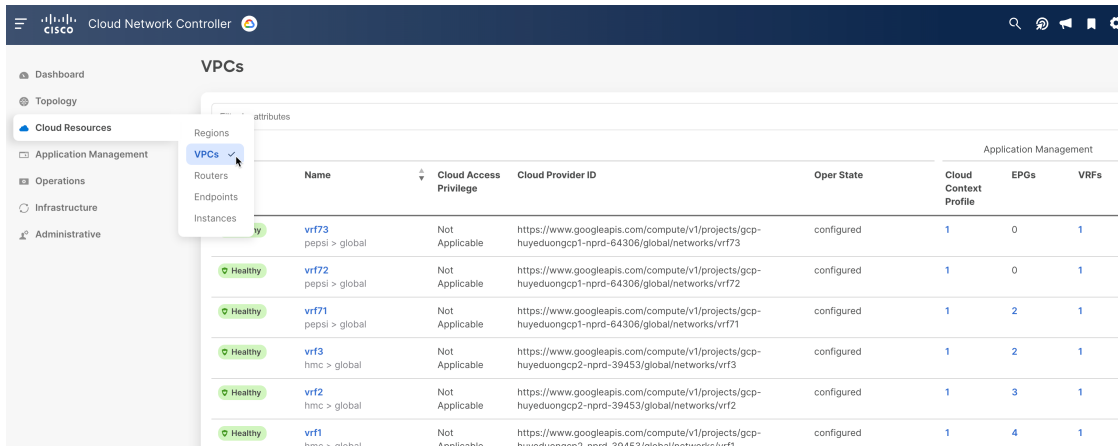
Cisco クラウド ネットワーク コントローラ リリース 25.1 (1) 以降では、VPC、リージョン、およびエンドポイントのフィルタリングされた統計と統計フィルタリングされた集約を表示できます。

この手順の例では、Cisco クラウド ネットワーク コントローラ GUI で VPC のフロー ログ統計を表示する方法を示します。次の手順で VPC の代わりに [**リージョン (Regions)**] または [**エンドポイント (Endpoints)**] を選択することで、同じ方法でリージョンまたはエンドポイントの統計情報を表示することもできます。

始める前に

[フロー ログ統計を有効化 \(7 ページ\)](#) の手順を使用して、目的のクラウド コンテキスト プロファイルの Google Cloud フロー ログ統計を有効にします。

ステップ 1 統計情報を表示する情報技術を選択します。

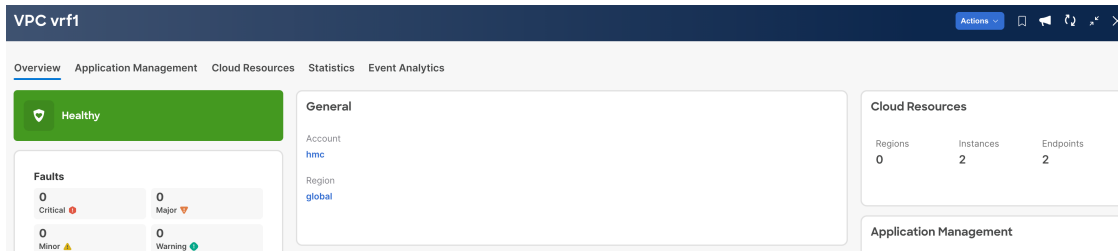


a) ナビゲーションメニューから [クラウド情報技術 (Cloud Resources)] > VPCs を選択します。作業ウィンドウに VPC サマリーテーブルが表示されます。

b) サマリーテーブルで、VPC の名前をダブルクリックします。

VPC ダイアログボックスが [仕事 (Work)] ペインの上に表示されます。VPC ダイアログボックスは、**Overview**, [アプリケーション管理 (Application Management)], [クラウド情報技術 (Cloud Resources)], [統計 (Statistics)] と [イベント分析 (Event Analytics)] タブを表示します。

ステップ 2 [Statistics] タブをクリックします。



VPC 統計のグラフィカルビューが、集約されたフィルタ処理された統計のテーブルとともに表示されます。

ステップ 3 統計情報の表示を構成します。

表示される統計情報のパラメータを構成するには、次の設定を変更します：

[プロパティ (Properties)]	説明
サンプリング間隔	間隔を選択します : <ul style="list-style-type: none"> • 1 時間 • 12時間 • 1日 • 週 1 回 • 1ヵ月
統計情報タイプ	表示タイプを選択します。 <ul style="list-style-type: none"> • 期間 : この間隔のカウンタの値 (「1 時間」間隔など) • 累積 : 最初からのカウンタの合計値 • [傾向 (Trend)] : 前の間隔をこの間隔と比較し、傾向が増加しているか減少しているかを判断します。 • レート : 定期的な値/間隔
バイト	バイト カウンタ グラフを表示するには、このチェックボックスをオンにします。グラフの左側の縦軸は、バイト数を示します。
Packets	パケット カウンタ グラフを表示するには、このチェックボックスをオンにします。グラフの右側の縦軸は、パケット数を示します。
フロー フィルター	フローログ統計情報に適用するために作成されたフィルタのいずれかを選択します。フィルタが適用されると、フィルタ処理された統計情報が自動的に集約されます。

REST API を使用した VPC フロー ログの有効化

Google Cloud フローログ統計は、テナント内の個々のコンテキストプロファイルに対して有効にできます。

ステップ 1 テナントでフロー ログ ポリシー (`c1oudGcpFlowLogPol`) を定義します。

名前以外の構成設定は必要ありません。

(注) フロー ログ ポリシーの名前については、次の制約事項に注意してください。

- 正規表現の一致:

```
[az]([-a-z0-9] * [a-z0-9])?
```

このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。

- この名前には 14 文字以下を使用することを推奨します。

例 :

```
<polUni>
  <fvTenant name="tenant1" status="">
    <cloudGcpFlowLogPol name="myFlowLogPol1" status="">
    </cloudGcpFlowLogPol>
    <cloudCtxProfile name="ctxProfile2" status="" vpcGroup="vpc-4">
    .
    .
    .
```

ステップ 2 クラウド コンテキスト プロファイル内で、フロー ログ ポリシーへの参照を追加します。

クラウド コンテキスト プロファイルのフロー ログ統計は、参照オブジェクト (`cloudRsCtxToGcpFlowLog`) の存在によって有効になります。クラウド コンテキスト プロファイルのフロー ログ統計情報を無効にするには、参照オブジェクトを削除します。

例 :

```
.
.
.
  <cloudRsCtxToGcpFlowLog tnCloudGcpFlowLogPolName="myFlowLogPol1" status=""/>
</cloudCtxProfile>
</fvTenant>
</polUni>
```

REST API を使用した統計情報フィルタの定義

このセクションは、REST API を使用して GCP 統計フィルタ ポリシーを定義する方法を表示します。

始める前に

[REST API を使用した VPC フロー ログの有効化 \(12 ページ\)](#) の手順を使用して、目的のクラウド コンテキスト プロファイルの Google Cloud フロー ログ統計を有効にします。

```
<polUni>
  <fvTenant name="t1" status="">
    <cloudGcpFlowLogPol name="f11" status="">
      <cloudRsToGcpStatsFilter tDn="uni/tn-t1/gcpip-[11.11.1.2/24]-gcpport-22-gcpprotocol-1"
status=""/>
      <cloudRsToGcpStatsFilter tDn="uni/tn-t1/gcpip-[11.11.3.2/24]-gcpport-https-gcpprotocol-6"
status=""/>
    </cloudGcpFlowLogPol>

    <cloudGcpStatsFilter peerIP="11.11.1.2/24" peerPort="22" protocol="1" status="">
    </cloudGcpStatsFilter>
    <cloudGcpStatsFilter peerIP="11.11.3.2/24" peerPort="https" protocol="6" status="">
    </cloudGcpStatsFilter>
  </fvTenant>
</polUni>
```

翻訳について

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。