Cisco Cloud Network Controller Statistics

About Google Cloud Statistics

You can view statistics that are derived by processing Google Cloud flow logs. In addition, you can view statistics that are collected from the Cisco Catalyst 8000V routers.

Beginning with Cisco Cloud Network Controller Release 25.1(1), you can also apply filters to the statistics that are derived from the Google Cloud flow logs.

Router Statistics

Cisco Cloud Network Controller allows you to view router statistics for individual cloud context profiles within a tenant. Statistics are displayed for Cisco Catalyst 8000V routers within the cloud context profile.

Each router instance captures and stores the ingress and egress byte and packet statistics for each physical and tunnel interface. The Cisco Cloud Network Controller queries the routers for these statistics and maps the response to router statistics on the Cisco Cloud Network Controller. The statistics query repeats every 5 minutes for as long as the tunnel is up and operational. The Cisco Cloud Network Controller GUI displays the collected statistics for the routers.

Flow Log Statistics

Cisco Cloud Network Controller allows you to enable flow log statistics for individual cloud context profiles within a tenant. When statistics are enabled for a cloud context profile, statistics are collected for every IP address within the corresponding VPCs. Available statistics include ingress and egress bytes and packets, internal and external, for VPCs, regions, and endpoints.

The collected statistics are aggregated through the following hierarchy:

- IP statistics are aggregated to determine endpoint statistics.
- Endpoint statistics are aggregated to determine zone statistics.
- Zone statistics are aggregated to determine subnet statistics.
- Subnet statistics are aggregated to determine region statistics.
- Region statistics are aggregated to determine VPC statistics.

The Cisco Cloud Network Controller GUI displays the collected statistics for VPCs, regions, and endpoints.

For more information about Google Cloud flow logs, see "VPC Flow Logs" on the Google Cloud website.

About Statistics Filter

Beginning with Cisco Cloud Network Controller Release 25.1(1), you can apply filters to the statistics that are derived from the Google Cloud flow logs.

Statistics are collected for each endpoint on which the filter is deployed. The filters allow you to capture information about flows between a pair of IP addresses and a certain port or protocol.

A statistics filter has the following three attributes:

1. Peer IP: The IPv4 address to filter.
2. Protocol: The protocol number to listen to
3. PeerPort: The port number to listen to

As the GCP flow log records do not provide any information about dropped traffic, the statistics collected for each endpoint will only have the following fields after filtering:

1. Number of packets sent
2. Number of bytes sent
3. Number of packets received
4. Number of bytes received

Note Use of statistics filters depend on enabling Virtual Private Cloud (VPC) flow log; you must enable the logs before you configure the statistics filters.

Statistics Filter Aggregation

Google Cloud supports aggregation of filtered statistics on each of the following levels:

1. The endpoint
2. The region
3. The VPC

The filtered statistics are automatically aggregated every 15 minutes and will be displayed to you in the form of a table. The following table highlights the format in which the statistics filter aggregation can be viewed by you on each level.

The collected filtered statistics are aggregated to follow the same hierarchy as the flow log statistics.

	End point	**Region**	**VPC**
Dn format	Ep Dn/sf-(filter)	Rg Dn/ sf-(filter)	VPC Dn/sf-(filter)
Example	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-sfprotocol-6

Inter-VPC Statistics via Statistics Filter

Google Cloud statistics filter provides the capability of collecting statistics for a given network, protocol, and port. With that we can provide inter-VPC statistics for a given pair of VPCs by defining filters with specific networks.

We can also provide statistics for a given type of traffic between a VPC pair by adding specific protocol and port to the filters.

The inter-VPC statistics objects will be shown under each VPC, based on number of filters defined under each VPC. You can define up to eight filters under each VPC.

An example where inter-VPC statistics can be viewed is mentioned below.

We have 3 VPCs connected to an Infra VPC, and VPC1 is talking to VPC2 and VPC3.

If VPC1 has a filter defined with VPC2's network in its IP field, this will create an inter-VPC stats object under VPC1 indicating the traffic flow between VPC1 and VPC2 from VPC1's perspective.

If VPC3 has a filter defined with VPC1's network in its IP field and SSH in its port field, this will create an inter-VPC stats object under VPC3 representing the SSH traffic flow between VPC1 and VPC3 from VPC3's perspective.

Since GCP flow log record does not provide any information about dropped traffic, the statistics object will only have the following fields after filtering for each endpoint:

1. Number of packets sent
2. Number of bytes sent
3. Number of packets received
4. Number of bytes received

The filter statistics are collected on each NIC level. The NIC level filter statistics are all aggregated for a given filter under a VPC to derive the statistics matching a certain filter on a VPC level. A filter defined to match a given VPC's network will give us all the traffic flow to that VPC, whereas, a filter defined to match a given VPC's network using certain protocol and port will give us a specific type of traffic flow to that VPC.

Guidelines and Limitations For Configuring Google Cloud Statistics

Following are the guidelines and limitations when configuring Cisco Cloud Network Controller to collect Google Cloud statistics:

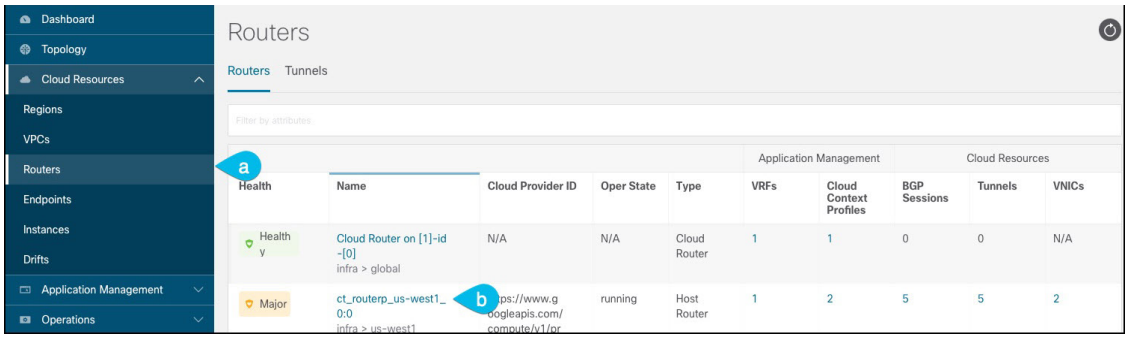
- Router statistics are enabled by default when Cisco Catalyst 8000V routers are brought up in the Cisco Cloud Network Controller.
- The flow log statistics feature is not enabled by default.
- Flow log statistics can be enabled for individual context profiles within a tenant. In this case, flow logs are enabled on all subnets belonging to the corresponding VPC.
- Flow logs are aggregated at one minute intervals. The aggregation interval and sample rate are not configurable.
- Statistics for dropped traffic are not supported by flow logs.
- Statistics filtering is not provided for dropped/ rejected packets or bytes.
- Zone and subnet statistics are not displayed.

Viewing Router Statistics

In the Cisco Cloud Network Controller GUI, you can view graphed statistics for Cisco Catalyst 8000V routers. Available statistics for each router include ingress and egress bytes and packets. Peak values for each counter are displayed with a timestamp that shows when the peak value occurred.

This example procedure shows you how to view the statistics for a router in the Cisco Cloud Network Controller GUI.

Step 1 Select the Cisco Catalyst 8000V router whose statistics you would like to view.



a) From the navigation menu, select **Cloud Resources** > **Routers**.

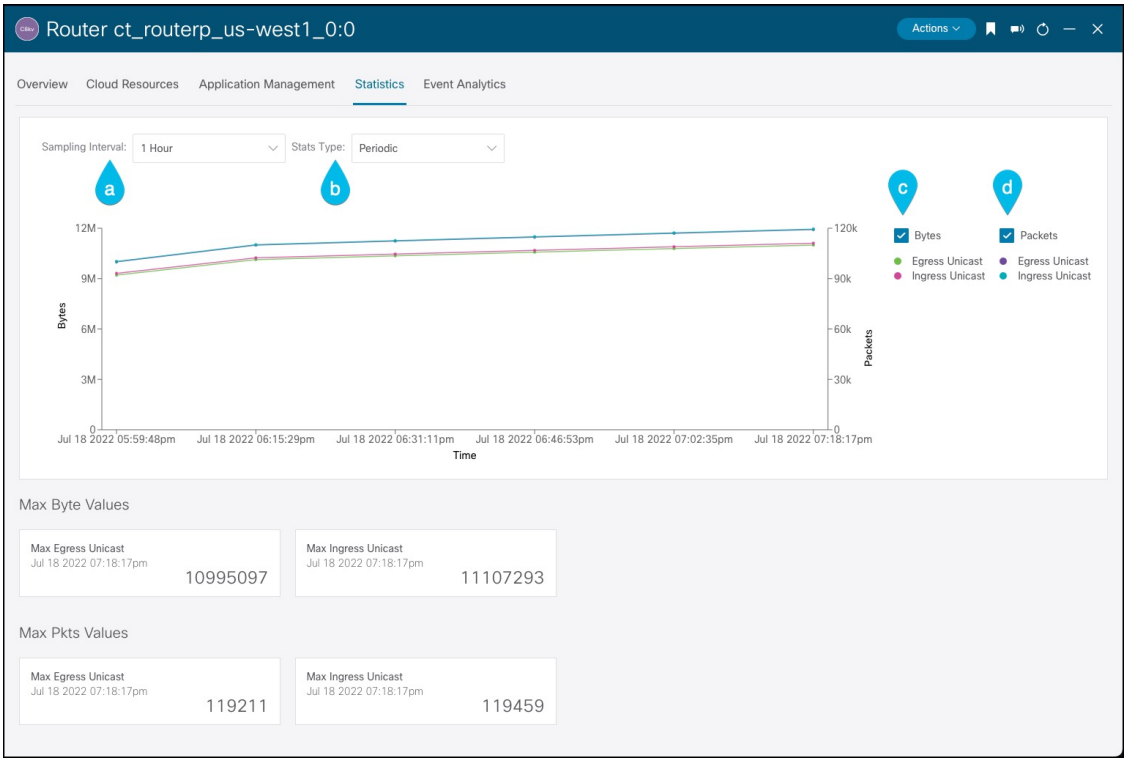
A **Routers** summary table appears in the work pane.

b) In the summary table, double-click the name of the router.

The router dialog box appears over the work pane. The router dialog box displays the **Overview**, **Cloud Resources**, **Application Management**, **Statistics**, and **Event Analytics** tabs.

Step 2 Click the **Statistics** tab.

A graphical view of the router statistics appears along with a table of maximum values.



Step 3 Configure the display of the statistics.

To configure the parameters of the displayed statistics, you can modify the following settings:

Properties	Description
Sampling Interval	Choose the interval: • 1 hour • 12 Hours • 1 Day • 1 Week • 1 Month

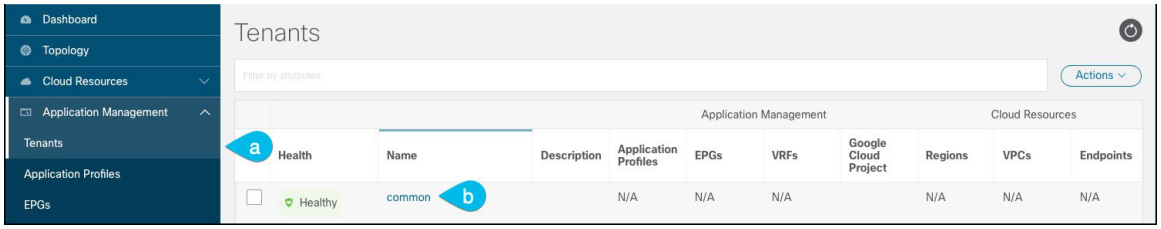
Properties	Description
Stats Type	Choose the display type: • Periodic- the value of the counter for this interval – for example '1 hour' interval • Cumulative- the total value of the counter from the beginning • Trend- compares the prior interval to this interval and determines if the trend is increasing or decreasing • Rate- periodic value/interval
Bytes	Select the checkbox to display the byte counter graph. The vertical axis on the left side of the graph indicates the byte count.
Packets	Select the checkbox to display the packet counter graph. The vertical axis on the right side of the graph indicates the packet count.

Enabling Flow Log Statistics

You can enable the collection of Google Cloud flow log statistics for individual context profiles within a tenant. Statistics can then be viewed for VPCs, regions, and endpoints in their respective **Cloud Resources** GUI menus.

To enable flow log statistics using the Cisco Cloud Network Controller GUI:

Step 1 Select the tenant containing the resource for which flow log statistics will be enabled.



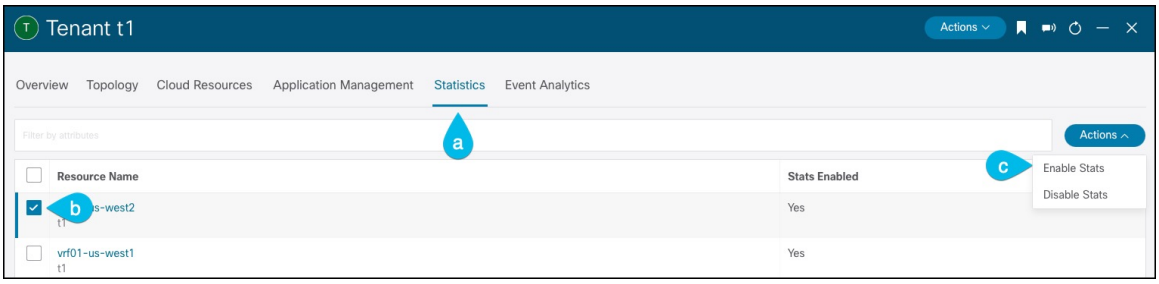
a) From the navigation menu, select **Application Management** > **Tenants**.

A **Tenants** summary table appears in the work pane.

b) In the summary table, double-click the name of the tenant.

The tenant dialog box appears over the work pane. The tenant dialog box displays the **Overview**, **Topology**, **Cloud Resources**, **Application Management**, **Statistics**, and **Event Analytics** tabs.

Step 2 Enable flow log statistics collection on the desired resource.



a) In the tenant dialog box, select the **Statistics** tab.

A **Resource Name** table appears with context profiles listed as rows in the table. The **Stats Enabled** column indicates whether flow log statistics are enabled for each resource.

b) Check the checkbox next to the desired resource.

c) In the top right of the tenant dialog box, click the **Actions** menu and select **Enable Stats**.

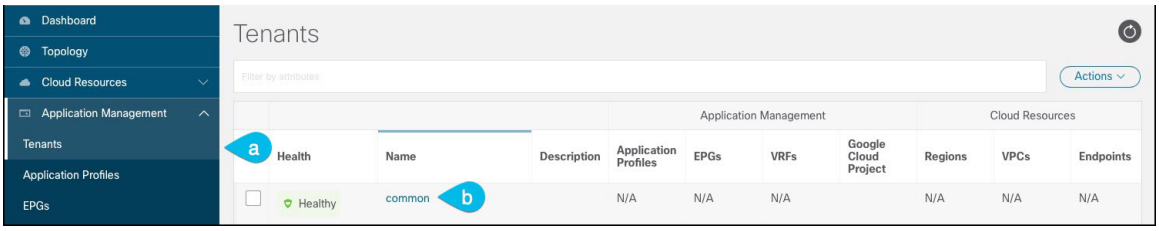
Defining Statistics Filter using GUI

You can apply filters to the statistics that are derived from the Google Cloud flow logs for a tenant. Once created, filtered statistics can be viewed for VPCs, regions, and endpoints in their respective **Cloud Resources** GUI menus.

Before you begin

Enable Google Cloud flow log statistics for the desired cloud context profile using the procedure in Enabling Flow Log Statistics, on page 6.

Step 1 Select the tenant containing the resource for which flow log statistics is enabled.



a) From the navigation menu, select **Application Management** > **Tenants**.

A **Tenants** summary table appears in the work pane.

b) In the summary table, double-click the name of the tenant.

The tenant dialog box appears over the work pane. The tenant dialog box displays the **Overview**, **Topology**, **Cloud Resources**, **Application Management**, **Statistics**, and **Event Analytics** tabs.

Select the **Statistics** tab to open it in the work pane.

Step 2 The **Statistics Collection Settings** information appears at the top of the dialog box with the **edit (pencil)** icon in the top-right corner.

Step 3 Click the **edit (pencil)** icon.

The **Statistics Collection Settings** dialog box appears.

Step 4 Click **Add Flow Filters** in the **Statistics Collection Settings** dialog box.

After you click on the **Add Flow Filters** button, you will see a new filter being created for which the following attributes are to be filled.

a) **Note** Make sure that the **Active** checkbox is selected to ensure that the filter is applied to the tenant. If a filter is created without selecting the **Active**checkbox, it will not be applied and you cannot view the filtered statistics.

In the **Active** field, check in the box to apply the filter.

b) In the **Peer IP** field, enter the IPv4 IP address of the peer.

The address needs to be in the format x.x.x.x/x. It tells the filter which network to monitor.

c) From the **Protocol** drop-down list, choose a protocol to listen to.

d) In the **Peer Port** field, enter the port number to listen to.

Step 5 Click the check icon and click **Save**.

Viewing Flow Log Statistics

In the Cisco Cloud Network Controller GUI, you can view graphed statistics for VPCs, regions, and endpoints. Available statistics for each include ingress and egress bytes and packets. For VPCs and regions, the statistics are further separated into the following categories:

- Statistics: All traffic counters extracted from the flow logs records.
- Inter-Region Statistics: For a particular region, all ingress and egress traffic to or from other regions within the VPC.
- External Statistics: All ingress and egress traffic with a source or destination outside of the VPC.
- Inter-Zone Statistics: For a particular zone, all ingress and egress traffic to or from other zones within the same region and VPC. These aggregated statistics are available on the region page and on the VPC page.

Peak values for each counter are displayed with a timestamp that shows when the peak value occurred.

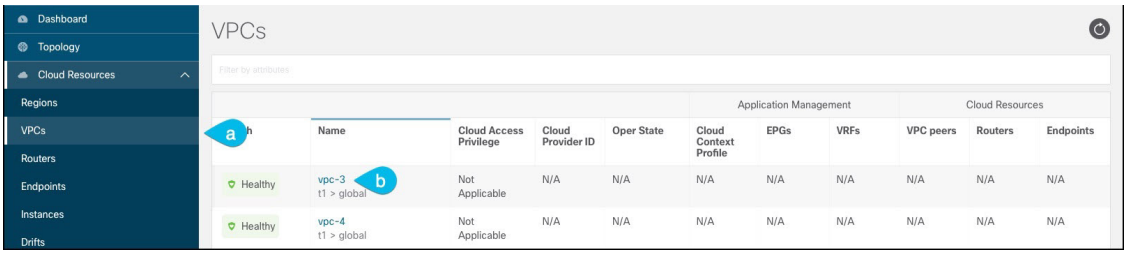
Beginning with Cisco Cloud Network Controller Release 25.1(1), you can view filtered statistics and statistics filtered aggregation for VPCs, regions and endpoints.

This example procedure shows you how to view the flow log statistics for VPCs in the Cisco Cloud Network Controller GUI. You can also view the statistics for regions or endpoints in the same manner by selecting **Regions** or **Endpoints** instead of **VPCs** in the following steps.

Before you begin

Enable Google Cloud flow log statistics for the desired cloud context profile using the procedure in Enabling Flow Log Statistics, on page 6.

Step 1 Select the resource whose statistics you would like to view.



a) From the navigation menu, select **Cloud Resources** > **VPCs**.

A **VPCs** summary table appears in the work pane.

b) In the summary table, double-click the name of the VPC.

The VPC dialog box appears over the work pane. The VPC dialog box displays the **Overview**, **Application Management**, **Cloud Resources**, **Statistics**, and **Event Analytics** tabs.

Step 2 Click the **Statistics** tab.

A graphical view of the VPC statistics appears along with a table of aggregated filtered statistics.

Step 3 Configure the display of the statistics.

To configure the parameters of the displayed statistics, you can modify the following settings:

Properties	Description
Sampling Interval	Choose the interval: • 1 hour • 12 Hours • 1 Day • 1 Week • 1 Month
Stats Type	Choose the display type: • Periodic- the value of the counter for this interval – for example '1 hour' interval • Cumulative- the total value of the counter from the beginning • Trend- compares the prior interval to this interval and determines if the trend is increasing or decreasing • Rate- periodic value/interval
Bytes	Check the checkbox to display the byte counter graph. The vertical axis on the left side of the graph indicates the byte count.
Packets	Check the checkbox to display the packet counter graph. The vertical axis on the right side of the graph indicates the packet count.
Flow Filter	Choose any one of the filters created to be applied to the flow log statistics. Once the filter is applied, the filtered statistics will be aggregated automatically.

Enabling VPC Flow Log Statistics Using the REST API

Google Cloud flow log statistics can be enabled for individual context profiles within a tenant.

Step 1 Define a flow log policy (`cloudGcpFlowLogPol`) under the tenant.

No configuration settings are needed except for the name.

Note For the name of the flow log policy, note the following restrictions:

- Match the regular expression:

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

  This means that the first character must be a lowercase letter, and all the following characters must be hyphens, lowercase letters, or digits, except the last character, which cannot be a hyphen.

- We recommend using 14 characters or fewer for this name.

Example:

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

Step 2 Within the cloud context profile, add a reference to the flow log policy.

Flow log statistics for the cloud context profile are enabled by the presence of the reference object (`cloudRsCtxToGcpFlowLog`). To disable flow log statistics for the cloud context profile, remove the reference object.

Example:

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

Defining Statistics Filter using REST API

This section demonstrates how to define the GCP statistics filter policy using REST API.

Before you begin

Enable Google Cloud flow log statistics for the desired cloud context profile using the procedure in Enabling VPC Flow Log Statistics Using the REST API, on page 10.

```
<polUni>
    <fvTenant name="t1" status="">
        <cloudGcpFlowLogPol name="fl1" 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>
```