Cloud VPN (https://cloud.google.com/vpn/)
Documentation (https://cloud.google.com/vpn/docs/) Guides

Viewing logs and metrics

Cloud VPN gateways send logging information to Stackdriver Logging, and Cloud VPN tunnels send monitoring metrics to Stackdriver Monitoring. This page describes logs and metrics and how to view them.

Logs

Cloud VPN gateways send certain logs to Logging (https://cloud.google.com/logging/docs/).

How to view logs

To view logs for Cloud VPN, perform the following steps.

CONSOLE

1. To view logs, go to the LOGS VIEWER (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/LOGS).

   VPN logs are indexed by the VPN gateway that created them.

   - To see all VPN logs, in the first pull-down menu select **Cloud VPN Gateway > All gateway_id**.
   - To see logs for just one gateway, select a single gateway name from the menu.

   Log fields of type *boolean* typically only appear if they have a value of `true`. If a boolean field has a value of `false`, that field is omitted from the log.

   UTF-8 (https://wikipedia.org/wiki/UTF-8) encoding is enforced for log fields. Characters that are not UTF-8 characters are replaced with question marks.

Exporting logs

You can configure the export (#exporting-logs) of Logging logs based metrics (https://cloud.google.com/logging/docs/logs-based-metrics/) for Cloud VPN resource logs.

Logging stores Cloud VPN logs for only 30 days. If you want to keep your logs for a longer period, you must export them (https://cloud.google.com/logging/docs/export/).

You can export Cloud VPN logs to Pub/Sub (https://cloud.google.com/pubsub/) or BigQuery (https://cloud.google.com/bigquery/) for analysis.

What is logged

Cloud VPN log entries contain information useful for monitoring and debugging your VPN tunnels. Log entries contain the following types of information:

- General information shown in most Google Cloud logs, such as severity, project ID, project number, and timestamp.
- Other information that varies depending on the log entry.

See Checking VPN logs (https://cloud.google.com/vpn/docs/support/troubleshooting#vpn-logging) for a list of useful logs.

Monitoring metrics

Note: Stackdriver Monitoring in the Cloud Console is now Generally Available and the default experience. For a limited period of time, you also have the option to use the classic Stackdriver Monitoring console. For more information, see Stackdriver Monitoring in the Cloud Console (https://cloud.google.com/monitoring/docs/monitoring_in_console).

To view metrics and create alerts related to your VPN tunnels, use Monitoring (https://cloud.google.com/monitoring/docs).

In addition to the predefined dashboards in Stackdriver Monitoring, you can create custom dashboards, set up alerts, and query the metrics through the Monitoring API (https://cloud.google.com/monitoring/api/).

Viewing Monitoring dashboards

You can view Monitoring dashboards for Cloud VPN in multiple ways.

Known issue: For HA VPN gateways, you must use Metrics Explorer (#viewing-metrics-explorer) to view Monitoring metrics.

Viewing metrics in the Monitoring VPN resource

1. Go to **Monitoring**.

   GO TO MONITORING (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/MONITORING)
2. If the Monitoring navigation pane displays **Resources**, then select **Resources** and select **VPN**. To view the dashboard for a specific gateway, locate it in the list and then click its name.
3. Otherwise, select **Dashboards**, and then select the dashboard named **VPN**. The **Inventory** card contains a list of VPNs. To view the dashboard for a specific gateway, locate it in the list and then click its name.

Viewing metrics in Metrics Explorer

To view the metrics for a monitored resource using Metrics Explorer, do the following:

1. In the Google Cloud Console, go to **Monitoring** or use the following button:

   GO TO MONITORING (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/MONITORING)
2. If the navigation pane isn't expanded, click **Expand >|** . This button is located on the lower left of the console.
3. If **Metrics Explorer** is shown in the navigation pane, click **Metrics Explorer**. Otherwise, select **Resources** and then select **Metrics Explorer**.
4. Ensure **Metric** is the selected tab.
5. Click in the box labeled **Find resource type and metric**, and then select from the menu or enter the name for the resource and metric. Use the following information to complete the fields for this text box:
   a. Enter or select **Cloud VPN** as the **Resource**. This resource type is valid for either Classic VPN gateways or HA VPN gateways.

    b. Enter a metric name from Cloud VPN metrics list (https://cloud.google.com/vpn/docs/how-to/viewing-logs-metrics#vpn-monitoring-metrics) or select a metric that appears in the menu.

6. Use the **Filter**, **Group By**, and **Aggregation** menus to modify how the data is displayed. For example, you can group by resource or metric labels. For more information, see Selecting metrics - additional configuration (https://cloud.google.com/monitoring/charts/metrics-selector#additional_configuration).

Viewing metrics from within a VPN tunnel

You can also view metrics by clicking the **Monitoring** tab for a tunnel in the Cloud Console.

In the left pane, you can see various details for this gateway. In the right pane, you can see timeseries graphs. Click the **Breakdowns** link to see specific breakdowns.

Defining Monitoring alerts

You can create alerting policies to monitor the values of metrics and to notify you when those metrics violate a condition. The general steps for creating an alerting policy that monitors the **Cloud VPN Gateway** (https://cloud.google.com/monitoring/api/resources#tag_vpn_gateway) resource are listed below:

1. In the Google Cloud Console, go to **Monitoring** or use the following button:

   GO TO MONITORING (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/MONITORING)

2. Select **Alerting** and then select **Create Policy**.
3. Enter a name for the alerting policy.
4. Click **Add Condition**:
    a. The settings in the **Target** pane specify the resource and metric to be monitored. Click the text box to enable a menu and then select the resouce **Cloud VPN Gateway** (https://cloud.google.com/monitoring/api/resources#tag_vpn_gateway). Next, select a metric from the metrics list.
    b. The settings in the **Configuration** pane of the alerting policy determine when the alert is triggered. Most fields in this pane is populated with default values. For more information on the fields in the pane, see Configuration

(https://cloud.google.com/monitoring/alerts/ui-conditions-ga#configuration) in the alerting policy documentation.

   c. Click **Save**.

5. (Optional) Click **Add Notification Channel** and enter your notification channel information.
6. (Optional) Click **Documentation** and add any information that you want included in a notification message.
7. Click **Save**.

For more information, see Alerting policies (https://cloud.google.com/monitoring/alerts/).

Defining Monitoring custom dashboards

You can create custom Monitoring dashboards over Cloud VPN metrics:

1. Go to **Monitoring**.

   GO TO MONITORING (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/MONITORING)

2. Select **Dashboards > Create Dashboard**.
3. Click **Add Chart**.
4. Give the chart a title.
5. Select metrics and filters. For metrics, the resource type is **Cloud VPN Gateway**.
6. Click **Save**.

Monitoring metrics for Cloud VPN

The following metrics for Cloud VPN are reported into Monitoring (https://cloud.google.com/monitoring/api/metrics). Metrics that are not individual events are for the time interval.

Metric name	Metric name in the Monitoring AI
Tunnel established	`vpn.googleapis.com/tunnel_esta`
Number of connections	`vpn.googleapis.com/gateway/con`

(https://cloud.google.com/vpn/docs/concepts/overview#connection)	
Received bytes	`vpn.googleapis.` `com/network/received_bytes_cou`
Received packets	`vpn.googleapis.` `com/network/received_packets_c`
Incoming packets dropped	`vpn.googleapis.` `com/network/dropped_received_p`
Sent bytes	`vpn.googleapis.` `com/network/sent_bytes_count`
Sent packets	`vpn.googleapis.` `com/network/sent_packets_count`

Outgoing packets dropped	`vpn.googleapis.com/network/dropped_sent_packe`

HA connection health

The following metrics indicate if the connection (https://cloud.google.com/vpn/docs/concepts/overview#connection) for an HA VPN gateway is healthy and if its configuration meets the 99.99% SLA.

Status	Description
`configured_for_sla`	Indicates if the HA connection has been fully configured, meaning that the connection contains the necessary number of tunnels and is properly connected to a Cloud Router.
`gcp_service_health`	Indicates if the HA connection is functioning properly on the Google Cloud side. For example, the tunnel is allocated.
`end_to_end_health`	Indicates if packets are being successfully sent and received inside the HA connection.

Reasons for drop

When a Cloud VPN gateway drops a packet, the gateway provides a reason for the drop.

Reason	Description	Source of traffic
`dont_fragment_icmp`	The dropped packet was an ICMP packet of a size greater the MTU with the "do not fragment" bit set. Such packets are used for path-mtu-discovery.	GCP VM
`exceeds_mtu`	The first fragment of a UDP or ESP egress packet is greater than the MTU and has the "do not fragment" bit set.	GCP VM
`dont_fragment_nonfirst_fragment`	A fragment of a UDP or ESP egress packet that is not the first fragment, and which is greater than the MTU and has the "do not fragment" bit set.	GCP VM
`Sent packets::invalid`	Packet was invalid or corrupt in some way. For example, the packet may have had an invalid IP header.	GCP VM
`Sent packets::throttled`	Packet dropped due to excessive load (https://cloud.google.com/vpn/docs/concepts/classic-topologies#vpn-throughput) on the Cloud VPN gateway.	GCP VM
`fragment_received`	Received a fragmented packet from the peer.	Peer VPN gateway
`sequence_number_lost`	A packet has arrived at the gateway with a sequence number greater than the expected sequence number, indicating that a packet with an earlier sequence number might have been dropped.	Peer VPN gateway
`suspected_replay`	ESP packet received with a sequence number that had already been received.	Peer VPN gateway
`Received packets::invalid`	Packet was invalid or corrupt in some way. For example, the packet may have had an invalid IP header.	Peer VPN gateway
`Received packets::throttled`	Packet dropped due to excessive load on the Cloud VPN gateway.	Peer VPN gateway
`sa_expired`	Received a packet with unknown SA. Could be as a result of using an SA that is already expired or one that was never negotiated.	Peer VPN gateway

unknown	Packet was dropped for a reason that the gateway could not or did not know how to categorize.	either

What's next

- Refer to the Monitoring docs (https://cloud.google.com/monitoring/docs/) or to the Logging docs (https://cloud.google.com/logging/docs) for more information on logging, monitoring, and exporting.
- Get troubleshooting help (https://cloud.google.com/vpn/docs/support/troubleshooting).
- Calculate network throughput (https://cloud.google.com/community/tutorials/network-throughput).

Previous
← **Maintenance overview** (https://cloud.google.com/vpn/docs/how-to/maintaining-vpns)

Next
Adding a VPN tunnel (https://cloud.google.com/vpn/docs/how-to/adding-a-tunnel) →

Last updated January 10, 2020.