**Configuring and Using VPC Flow Logs in Cloud Logging**

experimentLabschedule1 hour 30 minutesuniversal\_currency\_alt1 Creditshow\_chartIntroductory

infoThis lab may incorporate AI tools to support your learning.

**Overview**

In this lab, you will investigate [VPC flow logs](https://cloud.google.com/vpc/docs/flow-logs). VPC flow logs record network flows sent from or received by VM instances. These logs can be used for network monitoring, forensics, real-time security analysis, and even for expense optimization.

During this lab you enable VPC flow logging and use Cloud Logging to view the logs. Next, you perform network monitoring, forensics, and real-time security analysis, before finally, disabling VPC flow logging.

Objectives

In this lab, you learn how to:

* Enable VPC flow logging for a subnet.
* Access logs via Cloud Logging.
* Filter logs for specific subnets, VMs, ports, or protocols.
* Perform network monitoring, forensics, and real-time security analysis.
* Disable VPC flow logging.

**Setup and requirements**

For each lab, you get a new Google Cloud project and set of resources for a fixed time at no cost.

1. Sign in to Qwiklabs using an **incognito window**.
2. Note the lab's access time (for example, 1:15:00), and make sure you can finish within that time.  
   There is no pause feature. You can restart if needed, but you have to start at the beginning.
3. When ready, click **Start lab**.
4. Note your lab credentials (**Username** and **Password**). You will use them to sign in to the Google Cloud Console.
5. Click **Open Google Console**.
6. Click **Use another account** and copy/paste credentials for **this** lab into the prompts.  
   If you use other credentials, you'll receive errors or **incur charges**.
7. Accept the terms and skip the recovery resource page.

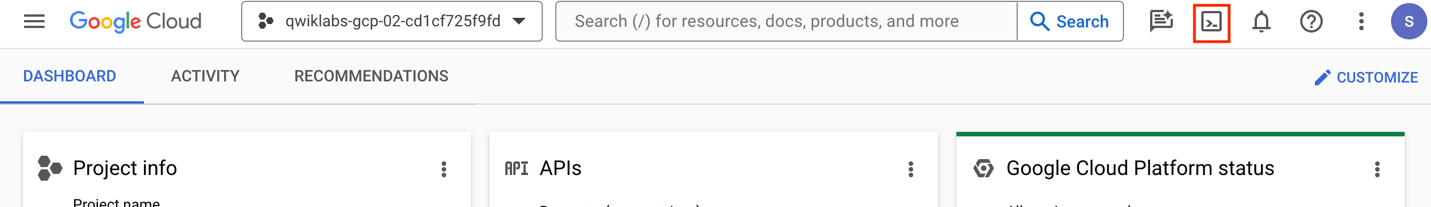
**Note:** Do not click **End Lab** unless you have finished the lab or want to restart it. This clears your work and removes the project.

Activate Google Cloud Shell

Google Cloud Shell is a virtual machine that is loaded with development tools. It offers a persistent 5GB home directory and runs on the Google Cloud.

Google Cloud Shell provides command-line access to your Google Cloud resources.

1. In Cloud console, on the top right toolbar, click the Open Cloud Shell button.



1. Click **Continue**.

It takes a few moments to provision and connect to the environment. When you are connected, you are already authenticated, and the project is set to your *PROJECT\_ID*. For example:



**gcloud** is the command-line tool for Google Cloud. It comes pre-installed on Cloud Shell and supports tab-completion.

* You can list the active account name with this command:

gcloud auth list

Copied!

content\_copy

**Output:**

Credentialed accounts:

- @.com (active)

**Example output:**

Credentialed accounts:

- google1623327\_student@qwiklabs.net

* You can list the project ID with this command:

gcloud config list project

Copied!

content\_copy

**Output:**

[core]

project =

**Example output:**

[core]

project = qwiklabs-gcp-44776a13dea667a6

**Note:**Full documentation of **gcloud** is available in the [gcloud CLI overview guide](https://cloud.google.com/sdk/gcloud" \t "_blank).

**Task 1. Enable VPC flow logging**

In this task, you enable flow logging for two subnets. Flow logging can also be enabled in exactly the same manner for custom user-defined networks. Flow logging can also be enabled when you create a subnet in one step.

**Use gcloud in Cloud Shell to enable VPC flow logging on two subnets**

1. To enable flow logging in two subnets, run the following commands in Cloud Shell:

gcloud compute networks subnets update default \

--region us-central1 --enable-flow-logs \

--logging-metadata=include-all

Copied!

content\_copy

gcloud compute networks subnets update default \

--region europe-west1 --enable-flow-logs \

--logging-metadata=include-all

Copied!

content\_copy

Notice that you enabled VPC flow logging for the subnets in us-central1 and europe-west1. None of the other subnets have flow logging enabled.

1. To create three instances in different subnets (to be used for later testing), run the following commands:

gcloud compute instances create default-us-vm \

--machine-type e2-micro \

--zone=us-central1-a --network=default

Copied!

content\_copy

gcloud compute instances create default-eu-vm \

--machine-type e2-micro \

--zone=europe-west1-b --network=default

Copied!

content\_copy

gcloud compute instances create default-ap-vm \

--machine-type e2-micro \

--zone=asia-east1-a --network=default

Copied!

content\_copy

**Note:** If you get a ZONE\_RESOURCE\_POOL\_EXHAUSTED error, update the zone in the gcloud command and try running it again. For example, if us-central1-a is failing, try us-central1-binstead.

Click *Check my progress* to verify the objective.

Enable VPC flow logging on subnets and create instances

Check my progress

**Task 2. Generate network traffic for testing**

In this task, you create network traffic to test the connectivity between the instances.

1. In the Google Cloud Console, on the **Navigation menu**, click **Compute Engine > VM instances** to display a list of VM instances.
2. Record both the internal and external IP addresses of each instance. You will need these IPs later in this lab.

|  |  |  |
| --- | --- | --- |
| **Instance** | **Internal IP** | **External IP** |
| default-ap-vm | \*\*\*\*\* | \*\*\*\*\* |
| default-eu-vm | \*\*\*\*\* | \*\*\*\*\* |
| default-us-vm | \*\*\*\*\* | \*\*\*\*\* |

1. In the row for the default-us-vm instance, click **SSH**.
2. When connected via SSH, issue the following commands:

sudo apt-get install -y host

host www.wikipedia.org 8.8.8.8

ping -c 5 default-eu-vm.europe-west1-b

ping -c 5 www.google.com

curl http://www.google.com

Copied!

content\_copy

These commands did the following:

* Installed the host DNS resolution utility.
* Performed a DNS lookup of www.wikipedia.org using the 8.8.8.8 DNS server.
* Pinged the **default-eu-vm** instance and [www.google.com](https://www.google.com/)
* Used curl to create an HTTP connection to [www.google.com](https://www.google.com/)

Next, you run the same commands as above, but instead of pinging the default-eu-vm from the default-us-vm, you ping the default-us-vm from the default-eu-vm.

1. Return to the Cloud Console, and in the row for the default-eu-vm instance, click **SSH**.
2. When connected via SSH, issue the following commands:

sudo apt-get install -y host

host www.wikipedia.org 8.8.8.8

ping -c 5 default-us-vm.us-central1-a

ping -c 5 cloud.google.com

curl http://www.google.com

Copied!

content\_copy

1. Return to the Cloud Console, and in the row for the default-ap-vm instance, click **SSH**.
2. When connected via SSH, issue the following commands:

sudo apt-get install -y host

host www.bitnami.com 8.8.8.8

curl http://www.bitnami.com

Copied!

content\_copy

**Task 3. View flow logs in Cloud Logging**

In this task, you view the VPC flow logs for all the projects in Cloud Logging.

**Access all flow logs**

1. In the Cloud Console, go to the **Navigation menu** > **Logging** > **Logs Explorer**. (If you do not see this menu option, then continue this lab, at step 3).
2. In the **Query** panel, under **Resource**, click **Subnetwork**.
3. Under **Log name**, click **compute.googleapis.com/vpc\_flows**.

**Note:** If no log names appear for the above, try pasting in compute.googleapis.com%2Fvpc\_flows instead.

1. Click **Run query**.
2. In the Query results panel, entries from the VPC flow logs appear. If you do not see **compute.googleapis.com/vpc\_flows**, wait a few minutes for this log type to show up.

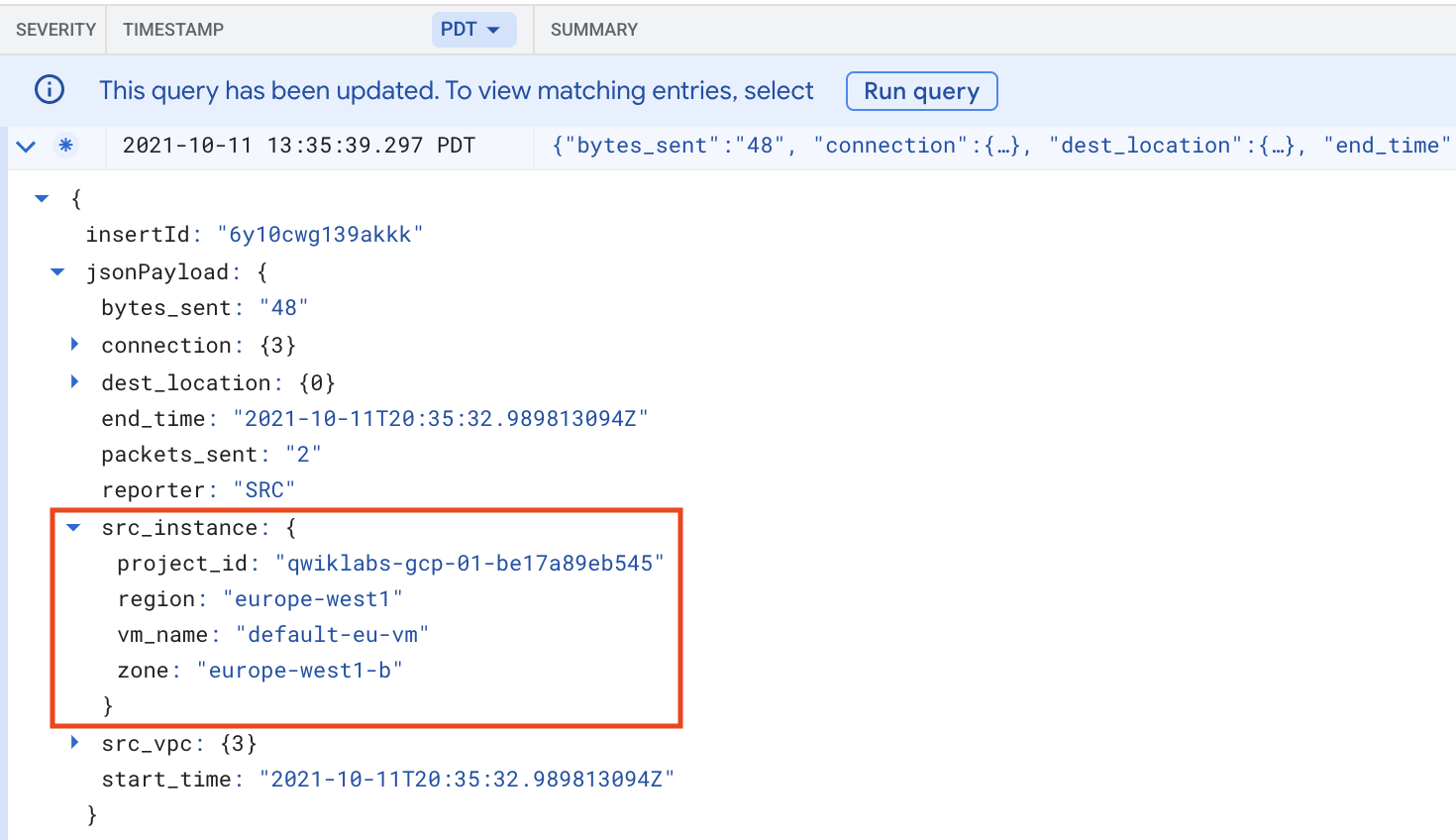
**Note:**This should show all the VPC flow logs for your project. Remember, you only have the flow logs enabled for two of the subnets.

1. Expand one of the log entries.
2. Within that log entry, expand jsonPayload, and then expand connection.

**Note:**Some entries do not have jsonPayload fields. You may need to open other entries until you find one that does.

1. Investigate the information about the connection; specifically notice that the port and IP address of both the source and destination have been logged.
2. Find a log that has src\_instance in jsonPayload. Investigate the information about this src instance.

The src\_instance may be one of your instances or an outside IP address if the traffic came from outside your VPC network.



1. Investigate any other information in this log entry or another.

**Task 4. Perform advanced filtering**

In this task, you perform advanced filtering using Query builder. You also explore access logs for specific source or destination IP, and for specific ports and protocols.

An advanced logs filter is a Boolean expression that specifies a subset of all the log entries in your project. A few things it can be used for include:

* Choosing log entries for specific VMs.
* Choosing log entries for specific source or destination ports.
* Choosing log entries for specific source or destination IP address.
* Choosing log entries specific protocols.

1. Click inside the **Query** box.
2. Remove the current query and paste in the following, replacing <INSERT\_PROJECT\_ID> with your Qwiklabs Google Cloud Project ID:

resource.type="gce\_subnetwork"

log\_name="projects/<INSERT\_PROJECT\_ID>/logs/compute.googleapis.com%2Fvpc\_flows"

Copied!

content\_copy

1. Click **Run query**.

**Note:** For the remainder of this lab, be sure to always leave these two lines at the start of the filter. You will be adding additional lines after these two. If you accidentally delete or modify these two lines, copy them from above (be sure to change the project ID).

**Access logs for a specific source or destination IP address**

1. Add the following line to the end of the filter. Replace Internal\_IP\_Of\_default\_us\_vm with the internal IP address of your default\_us\_vm instance (you recorded this earlier):

jsonPayload.connection.src\_ip="Internal\_IP\_Of\_default\_us\_vm"

Copied!

content\_copy

1. Click **Run Query**.

You now see all the log entries where the source IP address is the internal IP address of the default-us-vm instance. These should be the same entries as for the earlier filter that showed the source instance of default-us-vm.

**Access logs for specific ports and protocols**

1. Delete the last line in the filter (the one matching src\_ip) and replace it with the following line that will only show entries with a destination port of 22 (SSH):

jsonPayload.connection.dest\_port=22

Copied!

content\_copy

1. Click **Run Query** and observe the results. You should see three logs because you SSH-ed into the VMs three times.
2. Modify the last line of the filter to only show traffic with a destination port of 80 (HTTP):

jsonPayload.connection.dest\_port=80

Copied!

content\_copy

1. Click **Run Query** and observe the results.
2. Match multiple ports by replacing the last line and adding this statment with an OR to the end of the port filter:

jsonPayload.connection.dest\_port=(80 OR 22)

Copied!

content\_copy

1. Change the last line in the filter to only show entries using the UDP protocol (protocol #17):

jsonPayload.connection.protocol=17

Copied!

content\_copy

1. Click **Run Query** and observe the results.

You may see a few entries in the log. These would correspond to the DNS calls you made with the host utility.

1. Investigate one of the log entries and locate the destination port number that DNS uses.

**Note:**DNS uses port 53.

1. Modify the filter to show all entries with a protocol of 17 and destination port of 53:

jsonPayload.connection.protocol=17

jsonPayload.connection.dest\_port=53

Copied!

content\_copy

1. Click **Run Query** and observe the results.

**Note:** Currently, flow logs only monitor UDP (protocol #17) and TCP (protocol #6). Earlier, you generated some ICMP traffic on the instances using ping. ICMP is protocol #1. If you create a filter to show protocol #1, you will not see any entries. Try this if you want.

**Task 5. Perform network monitoring and support real-time security analysis**

In this task, you create a filter and use it to see whether any RDP traffic is attempting to access the VPC.

**Search for unexpected ports and protocols**

Because you are running Linux instances within the VPC network, you should not see any RDP traffic. However, there is a firewall rule within the default settings that allows RDP traffic from anywhere, and this means that someone or something on the internet could attempt to connect to your servers using the RDP protocol.

1. Modify the flow log filter to show all traffic with a destination port of 3389 (RDP). Be sure to leave the first two lines of the existing filter, but delete and replace the other lines with the following and click **Run query**:

jsonPayload.connection.dest\_port=3389

Copied!

content\_copy

1. If you see any RDP traffic, investigate where the traffic is coming from. You may not see any RDP traffic, but it is common to see at least some. If you did not see any traffic, wait a few minutes and check again.

If you did see some RDP traffic, which often happens, that demonstrates how pervasive unwanted traffic can be on the internet. It also shows why ensuring that VPC networks and firewall rules are set up correctly is important.

By using the default VPC in this lab, with all of the default firewall rules, you saw the results of not fine-tuning these rules to help exclude unwanted traffic.

**Note:** It is a recommended best practice for production systems to use a custom VPC with very specific firewall rules and delete the default VPC.**Note:** Another service that can help with issues like restricting unwanted traffic is [Google Cloud Armor](https://cloud.google.com/armor/). Google Cloud Armor delivers defense at scale against infrastructure and application Distributed Denial of Service (DDoS) attacks using Google's global infrastructure and security systems.

Create exports to support real-time security analysis

Flow logs can be exported to any destination that Cloud Logging export supports (Pub/Sub, BigQuery, etc.). Creating an export will export future matching logs to the selected destination, existing logs will not be exported.

Exporting logs to BigQuery allows for the BigQuery analysis tools to be used on your logs to perform analysis. Exporting logs to Pub/Sub allows your logs to be streamed to other applications, other repositories, or third parties.

When you create a Cloud export, the current filter will be applied to the export. This means that only events that match the filter will be exported. For example, if you have a filter that only displays traffic to the destination port 3389, only traffic that matches that filter will be exported.

This can help reduce the amount of data that is exported (which could lower costs) or allow for different exports depending on what the data contains. For this lab you will clear the filter and export all logs because you do not have much traffic.

1. Clear all the text in the query editor and click **Run query**.
2. Click **More Actions** > **Create Sink**.
3. For "Sink Name", type **FlowLogBQExport** and click **Next**.
4. For "Select sink service", select **BigQuery dataset**.
5. For "Sink Destination", select **Create new BigQuery dataset**.
6. For "Dataset ID", type flowlogs\_dataset, and then click **Create Dataset**.
7. Click **Create Sink**. The Logs Router Sinks page appears.

You should be able to see the sink you created **(FlowLogBQExport)**. If you are unable to see the sink click on **Logs Router**.

1. On the right side, click the **More actions** menu () for your export and select **View sink details**.
2. Click **Cancel**.

**Note:** All future logs will now be exported to BigQuery. The BigQuery tools can now be used to perform analysis on the flow log data. You will perform a simple query in BigQuery later in the lab.**Note:** You could also export log entries to Pub/Sub or Cloud Storage. Exporting to Pub/Sub can be useful if you want to flow through an ETL process before storing in a database **(Operations > Pub/Sub > Dataflow > BigQuery/Cloud Bigtable)**. Exporting to Cloud Storage will batch up entries and write them into Cloud Storage objects approximately every hour.

Now create an export to Pub/Sub.

1. On the Logs Router page, click **Create Sink**.
2. For "Sink Name", type **FlowLogPubSubExport**, and click **Next**.
3. Select "Select sink service" as **Cloud Pub/Sub topic**.
4. For "Cloud Pub/Sub topic", select **Create a Topic**.
5. For Topic ID, type **FlowLogsTopic**, and then click **Create**.
6. Click **Create Sink**.

The Logs Router Sinks page appears. You should be able to see the sink you created (FlowLogsTopic). If you are unable to see the sink click on **Logs Router**.

1. On the right side, click the **More actions** menu for your export and select **View sink details**.

This will show the filter that was present when the export was created.

1. Click **Cancel**.

You can now subscribe to the new Pub/Sub topic and receive notifications when new logs are available. This allows for the logs to be streamed to and integrated with a SIEM (Security Information and Event Management) tool.

SIEM tools are used to gain real-time operational insights and create audit reports using powerful visualization capabilities.

**Task 6. Analyzing flow logs in BigQuery**

In this task, you analyze flow logs in BigQuery.

**Note:** When you export logs to a BigQuery dataset, Cloud Logging creates dated tables to hold the exported log entries. Log entries are placed in tables whose names are based on the entries' log names.

1. In the Cloud Console, on the **Navigation menu**, click **BigQuery**.
2. In the navigation pane under **Explorer**, expand the project name to see the **flowlogs\_dataset** dataset.
3. Expand the dataset to see the table with your exported flow logs.
4. Click on the table name that starts with compute\_googleapis\_com\_vpc\_flows\_ and review the schemas and details of the tables that are being used.

**Note:** If you don't see that table appear in the dataset, open the navigation menu and click "Cloud Overview" or any other service. Then, open the navigation menu and select BigQuery and try to find the table again (it sometimes takes a minute or two for the table to appear in the dataset).

1. Click **Query** > **In new tab**.
2. Delete the text provided in the **New query** window and paste in the query below:

#standardSQL

SELECT

jsonPayload.connection.dest\_ip,

resource

FROM

`flowlogs\_dataset.compute\_googleapis\_com\_vpc\_flows\*` WHERE

jsonPayload.connection.dest\_port = 22

LIMIT 1000

Copied!

content\_copy

1. Click **Run**.

This query returns information about traffic connecting to port 22.

After a couple of seconds, the results are displayed. You should see one or two entries, which is the activity you generated in this lab. Remember, BigQuery is only showing activity since the export was created.

**Note:** If you did not see any results, you may need to generate some traffic to the instances. To do so, go to the **Navigation menu > Compute Engine** and click **SSH** for each instance. Then try the query again.

Click *Check my progress* to verify the objective.

Create exports and analyze flow logs in BigQuery

Check my progress

**Task 7. Disable flow logging**

In this task, you disable VPC flow logging. VPC flow logging can be turned off with the --no-enable-flow-logs option.

1. Try disabling it on one of your subnets by running the following command in the Cloud Shell terminal:

gcloud compute networks subnets update default \

--region europe-west1 --no-enable-flow-logs

Copied!

content\_copy

1. You can verify that it has been disabled by viewing the VPC in the Cloud Console. On the **Navigation menu**, click **VPC network > VPC networks**. If prompted click on **LEAVE**.

**Task 8. Review**

In this lab, you enabled VPC flow logging for a subnet. You accessed logs via Cloud Logging. You also filtered logs for specific subnets, VMs, ports, and protocols. Next, you performed network monitoring, forensics, and real-time security analysis. Finally, you disabled VPC flow logging.

**End your lab**

When you have completed your lab, click **End Lab**. Google Cloud Skills Boost removes the resources you’ve used and cleans the account for you.

You will be given an opportunity to rate the lab experience. Select the applicable number of stars, type a comment, and then click **Submit**.

The number of stars indicates the following:

* 1 star = Very dissatisfied
* 2 stars = Dissatisfied
* 3 stars = Neutral
* 4 stars = Satisfied
* 5 stars = Very satisfied

You can close the dialog box if you don't want to provide feedback.

For feedback, suggestions, or corrections, please use the **Support** tab.

Copyright 2022 Google LLC All rights reserved. Google and the Google logo are trademarks of Google LLC. All other company and product names may be trademarks of the respective companies with which they are associated.