Cisco Secure Cloud Analytics

Google Cloud Platform Integration Quick Start Guide

Table of Contents

Public Cloud Monitoring Configuration for Google Cloud Platform

Cisco Secure Cloud Analytics public cloud monitoring (formerly Stealthwatch Cloud Public Cloud Monitoring) is a visibility, threat identification, and compliance service for Google Cloud Platform (GCP). Secure Cloud Analytics consumes network traffic data, including Virtual Private Cloud (VPC) flow logs, from your GCP public cloud network. It then performs dynamic entity modeling by running analytics on that data to detect threats and indicators of compromise. Secure Cloud Analytics consumes VPC flow logs directly from your GCP account using a cross-account IAM service account with the proper permissions.

Single GCP Project Configuration

To configure GCP to generate and store flow log data for **a single project**, and Secure Cloud Analytics to ingest that data:

1. In GCP, configure a service account with the proper permissions to view flow log and other data, and save the JSON credentials. See **Configure a Service Account to View VPC Flow Logs** for more information.
2. In GCP, enable flow logging and the Stackdriver monitoring API for metrics gathering. See **Configure GCP to Generate VPC Flow Logs and Enable Permissions**for more information.
3. In the Secure Cloud Analytics web portal UI, upload the service account JSON credentials. See **Upload JSON Credentials** for more information.

If you have a high-throughput GCP environment, you can optionally configure Pub/Sub to deliver flow log data to Secure Cloud Analytics:

> We strongly recommend configuring Pub/Sub to prevent the integration from exceeding GCP Stackdriver API quotas and dropping flow data.

1. Determine if your deployment is high-throughput. See **Identifying a High-throughput Environment** for more information.
2. Configure a Pub/Sub topic to ingest flow log data, and a Pub/Sub subscription for the topic to deliver the flow log data. See **Creating a GCP Pub/Sub Subscription** for more information.

Multiple GCP Project Configuration

To configure GCP to generate and store flow log data for **multiple projects**, and Secure Cloud Analytics to ingest that data:

1. In GCP, configure a service account with the proper permissions to view flow log and other data, and save the JSON credentials. Configure the additional projects to use a single service account. See **Configure a Service Account to View VPC Flow Logs** for more information.
2. In GCP, configure the additional projects to use the service account. See **Configuring a Single Service Account to View VPC Flow Logs for Multiple Projects** for more information.
3. In GCP, enable flow logging and the Stackdriver monitoring API for metrics gathering. See **Configure GCP to Generate VPC Flow Logs and Enable Permissions**for more information.
4. In the Secure Cloud Analytics web portal UI, upload the service account JSON credentials. See **Upload JSON Credentials** for more information.

If you have a high-throughput GCP environment, you can optionally configure Pub/Sub to deliver flow log data to Secure Cloud Analytics:

> We strongly recommend configuring Pub/Sub to prevent the integration from exceeding GCP Stackdriver API quotas and dropping flow data.

1. Determine if your deployment is high-throughput. See **Identifying a High-throughput Environment** for more information.
2. Configure a Pub/Sub topic to ingest flow log data, and a Pub/Sub subscription for the topic to deliver the flow log data. See **Creating a GCP Pub/Sub Subscription** for more information.
3. Configure additional Pub/Sub topics and subscriptions for the additional projects. See **Configuring Pub/Sub Topics and Subscriptions** for more information.

Configure a Service Account to View VPC Flow Logs

To configure the IAM service account, create a custom role with permissions required to gather information for Secure Cloud Analytics. Then, create the service account, and associate several roles, including the custom role. GCP creates the account with private key information. Save the private key in a secure location.

1. In your GCP console, select **IAM & Admin > IAM > Service Accounts**.
2. Click **Create service account**.
3. In the **Service account name** field, enter `logs-viewer`.
   The Cloud console generates a service account ID based on this name. Edit the ID if necessary. You cannot change the ID later.
4. Click **Create and continue**.
5. Click the **Select a role** drop-down, then select the **Logs Viewer** role.
6. Click **Add another role**.
7. Click the new **Select a role** drop-down, then select the **Compute Viewer** role.
8. Repeat steps 6 and 7 to add the following roles: **Monitoring Viewer** and **Pub/Sub Subscriber**.
9. **(Optional)** For cloud posture analysis, repeat steps 6 and 7 to add the following roles: **Security Center Service Agent** and **Security Reviewer**.
10. Click **Continue**.
11. Click **Create key**.
12. Select `JSON` as the **Key type**, then click **Create**.

    > ⚠ Save the generated JSON private key file in a secure location, as it contains the information necessary for the account to access the VPC flow logs.

13. Click **Close** after saving the JSON private key.
14. Click **Done**.

> ⓘ If restricting access to your GCP environment, make sure that communication with the relevant IPs is allowed. Go to your Secure Cloud Analytics web portal, select **Settings > Integrations > GCP > About** to see the list of public IPs used by Secure Cloud Analytics.

What To Do Next

- If you want to monitor a **single project**, enable flow logging in your deployment. See **Configure GCP to Generate VPC Flow Logs and Enable Permissions** for more information.
- If you want to monitor **multiple projects**, associate your service account with each additional project before you enable flow logging in your deployment. See **Configuring a Single Service Account to View VPC Flow Logs for Multiple Projects** for more information.

Configuring a Single Service Account to View VPC Flow Logs for Multiple Projects

If you want to **monitor multiple projects** in your GCP deployment, you can use a single service account to monitor the projects. Enable the cloud resource manager API for each project you want to monitor, then add the created service account email address and proper role permissions to that project.

Locate Your Service Account's Email Address

1. In your GCP console, select **IAM & Admin > IAM**.
2. Click the edit icon for your new service account.
3. Copy the **Member** email address, in the following format, and paste this into a plaintext editor:

   `[account-name]@[project-id].[gcp-info].com`

Enable the Cloud Resource Manager API for an Additional Project

1. In your GCP console, select **APIs & Services > Library**.
2. Click **Select** for your project.
3. Search for `Cloud Resource Manager API`, select **Cloud Resource Manager API**, and click **Enable**.

Add a Service Account to an Additional Project

1. In your GCP console, select **IAM & Admin > IAM**.
2. Select an additional project from the project drop-down.
3. Click **Add**.

4. Copy the Member service account email address from the plaintext editor and paste it in the New members field.
5. Click the **Select a role** drop-down. Enter, then select the **Logs Viewer** role.
6. Click **Add Another Role**.
7. Click the new **Select a role** drop-down. Enter, then select the **Compute Viewer** role.
8. Repeat steps 6 and 7 to add the following roles: **Monitoring Viewer** and **Pub/Sub Subscriber**.
9. **(Optional)** For cloud posture analysis, repeat steps 6 and 7 to add the following roles: **Security Center Service Agent** and **Security Reviewer**.
10. Click **Save**.
11. Repeat steps 2-9 for each additional project.

What To Do Next

- Enable flow logging in your deployment. See **Configure GCP to Generate VPC Flow Logs and Enable Permissions** for more information.

Configure GCP to Generate VPC Flow Logs and Enable Permissions

After you configure the service account, enable flow logging in your GCP deployment per subnet before making them available for ingestion by Secure Cloud Analytics. Then, enable the Stackdriver Monitoring API, to gather various GCP metrics.

Configure a GCP Subnet to Generate VPC Flow Logs

1. In your GCP console, select **VPC network**.
2. Select a subnet.
3. Click **Edit**.
4. Select `On` from **Flow logs**.
5. Click **Save**. Repeat steps 1–4 for each additional subnet you want to setup.

Enable the Stackdriver Monitoring API (Recommended)

> Secure Cloud Analytics uses this permission for the GCP Cloud Function Invocation Spike alert and to monitor the health and status of the integration.

1. In your GCP console, select the Cloud project for which you want to enable the API, and then go to the **APIs & Services** page.
2. Click **Enable APIs and Service**.
3. In the search field, enter **Monitoring**, then select **Stackdriver Monitoring API**.
4. Click **Enable** if the API is not enabled.
5. Click **Save**.

What To Do Next

- Upload the saved JSON credentials to the Secure Cloud Analytics portal. See for more information. **Upload JSON Credentials** for more information.

Upload JSON Credentials

To complete configuration, upload your JSON service account credentials to the Secure Cloud Analytics web portal UI.

1. Log in to the Secure Cloud Analytics web portal as a site administrator.
2. Select **Settings > Integrations > GCP > Credentials**.
3. Click **Upload Credentials File**, then select your JSON credentials file.

What To Do Next

- Determine if you have a high-throughput environment, and if so, configure Pub/Sub to ingest flow log data.

Identifying a High-throughput Environment

You can configure a Pub/Sub topic and subscription to guarantee transmission of your flow data in a high-throughput environment. GCP Pub/Sub collection is ideal if your VCP flow data exceeds the logging read limits imposed by GCP and is highly recommended for large GCP deployments.

Review the GCP Logging Quota

To check if your environment is exceeding GCP logging limits with an existing log-based GCP integration:

1. Log in to https://console.cloud.google.com/apis/api/logging.googleapis.com/quotas.
2. Select your project.
3. Search for *Quota exceeded errors count (1 min) - Read requests per minute*. If you exceed the quota, see **Creating a GCP Pub/Sub Subscription** for more information on configuring Pub/Sub.

Creating a GCP Pub/Sub Subscription

If your GCP deployment has high traffic throughput, we recommend that you configure Pub/Sub for flow log data delivery. To configure Pub/Sub for flow log data ingestion, obtain your primary project ID, create a log export sink, then create a Pub/Sub subscription for the topic.

Find Your GCP Project ID

1. In your GCP console, select **Manage resources**.
2. Select your primary project, and copy the Project **ID**.
3. Paste the Project ID into a text editor.

Create a GCP Log Export Sink for the Project

1. In your GCP console, select **Stackdriver Logging > Logs Router**.
2. Click **Create Sink**.
3. Select **Convert to advanced filter** from the **Filter by label or text search** drop-down field, above the log entries.
4. Copy the following and paste it into a plaintext editor:

```
resource.type="gce_subnetwork"
logName="projects/MY_PROJECT_
NAME/logs/compute.googleapis.com%2Fvpc_flows"
```

5. Replace `MY_PROJECT_NAME` with your Project ID.
6. Copy the updated text and paste it in the **Filter by label or text search** field, overwriting any existing text.
7. In the Edit Sink pane, enter `vpc_flows-sink` in the **Sink Name** field.
8. Select `Pub/Sub` from the **Sink Service** drop-down.
9. Select `Create new Cloud Pub/Sub topic` from the **Sink Destination** drop-down.
10. Enter `vpc_flows-topic` in the **Name** field, then click **Create**.
11. Click **Create Sink**.

Create a GCP Pub/Sub Subscription for the Project

1. In your GCP console, select **Pub/Sub > Topics**.
2. Select **Create subscription** from `vpc_flows-topic`'s menu.

3. Enter `swc_subscription` in the **Subscription Name** field.
4. Select the `Pull`**Delivery Type**.
5. Enter `600` Seconds in the **Acknowledgment Deadline** field.
6. Enter `2` hours in the **Message Retention Duration** field.
7. Uncheck **Retain Acknowledged Messages**.
8. Click **Create**.

What To Do Next

- If you are monitoring **multiple projects**, configure a Pub/Sub topic and subscription for each additional project. See **Configuring Pub/Sub Topics and Subscriptions** for more information.

Configuring Pub/Sub Topics and Subscriptions

If you want to monitor multiple projects in your GCP deployment, after you configure Pub/Sub for your primary project, create a log export sink and Pub/Sub subscription for each additional project that references your primary project ID.

Create a GCP Log Export Sink for Additional Projects

1. In your GCP console, select a project other than the primary project.
2. Select **Stackdriver Logging > Logs Router**.
3. Click **Create Sink**.
4. Select **Convert to advanced filter** from the **Filter by label or text search** drop-down field, above the log entries.
5. Copy the following and paste it into a plaintext editor:

```
resource.type="gce_subnetwork"
logName="projects/MY_PROJECT_
NAME/logs/compute.googleapis.com%2Fvpc_flows"
```

6. Replace `MY_PROJECT_NAME` with your **primary** project ID.
7. Copy the updated text and paste it in the **Filter by label or text search** field, overwriting any existing text.
8. In the **Edit Sink** pane, enter `vpc_flows-sink` in the **Sink Name** field.
9. Enter `vpc_flows-sink` in the **Sink Name** field.
10. Select `Pub/Sub` from the **Sink Service** drop-down.
11. Select `Create new Cloud Pub/Sub topic` from the **Sink Destination** drop-down.

12. Enter `vpc_flows-topic` in the **Name** field, then click **Create**.
13. Click **Create Sink**.
14. Repeat steps 1–13 for each additional project.

Create a GCP Pub/Sub Subscription for Additional Projects

1. In your GCP console, select a project other than the primary project.
2. Select **Pub/Sub > Topics**.
3. Select **Create subscription** from `vpc_flows-topic`'s menu.
4. Enter `swc_subscription` in the **Subscription Name** field.
5. Select the `Pull` **Delivery Type**.
6. Enter `600` seconds in the **Acknowledgment Deadline** field.
7. Enter `2` hours in the **Message Retention Duration** field.
8. Uncheck **Retain Acknowledged Messages**.
9. Click **Create**.

   Repeat steps 1–9 for each additional project.

Additional Resources

For more information about Secure Cloud Analytics, refer to the following:

- https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html for a general overview
- https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html to sign up for a 60-day Free Trial
- https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html for documentation resources
- https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html for installation and configuration guides, including the Secure Cloud Analytics Initial Deployment Guide

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html
- For Secure Cloud Analytics Free Trial customers, open a case by email: swatchc-support@cisco.com

Change History

Revision	Revision Date	Description
1.0	August 29, 2022	Initial version.

Copyright Information