Quickstart for AWS

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

This quickstart shows you how to connect Monitoring to your Amazon Web Services (AWS) account. It also covers how to install the Monitoring and Logging agents on your EC2 instances.

Before you begin

You must have an AWS account that isn't currently monitored by a Workspace (https://cloud.google.com/monitoring/workspaces). You cannot monitor an AWS account from more than one Workspace.

To disconnect an AWS account from a Workspace, go to Removing a project from a Workspace (https://cloud.google.com/monitoring/workspaces/manage#remove-project).

Overview of steps

Adding an AWS account to a Workspace requires that you create a Google Cloud project to serve as the host project for the workspace. After the Workspace is created, you add the AWS account to the Workspace.

The following steps connect your AWS account to Monitoring:

1. Create a new Google Cloud project (#create-a-project).
2. Create a new Workspace (#configure-sd-acct) (recommended) or Connect an AWS account (#connect-aws-and-sd) (if you want to use an existing Workspace).

3. Identify your trusted account ID and external ID.
4. Create an AWS role using the Account ID and External ID.
5. Connect your Workspace and AWS account using the AWS Role to create a new AWS connector project.
6. Create a service account in the AWS connector project to authorize access to Google Cloud.

Each of the preceding steps is described in detail in the following sections.

Configuring your Workspace

It is recommended that you Create a new Workspace (#configure-sd-acct) for this quickstart. However, if you want to use an existing Workspace, skip ahead to Connect an AWS account (#connect-aws-and-sd).

In either case, be sure to get the **Account ID** and **External ID** that you need for your AWS account. For more information, go to Getting your account and external IDs (#get-ids).

Create a Google Cloud project

To create a Google Cloud project:

1. In the Cloud Console, go to **New Project**.

   CREATE A NEW PROJECT (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/PROJECTCREATE)

2. In the **Project Name** field, enter `Quickstart`.
3. Click **Create**.

Get your account and external IDs

To identify the trusted account ID and external ID required by AWS:

1. Go to Monitoring

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

The first time you access Monitoring for a Google Cloud project, Monitoring creates a Workspace and associates it with your project. This process is automatic unless you have a multi-project Workspace. In this case, a dialog appears that asks you to select between creating a Workspace and adding the project to an existing Workspace. Select the option to create a Workspace.

2. Do the following:
    - If **Settings** is displayed in the navigation pane, click **Settings** and select the **Summary** tab.
    - Otherwise, in the toolbar, click **Menu** ▾ and then select **Workspace Settings**. In the **Workspace settings** page, select **Monitored accounts**.
3. Click **Add AWS account**.
4. Record the **Account ID** and **External ID**. You need this data to create your AWS Role.
5. Click **Cancel**. You add your AWS account *after* you create your AWS role.

Note: The instructions on the **Monitored accounts** page direct you to go to AWS to create an AWS role and connect your account. These quickstart instructions follow an alternate path: complete the creation of your Workspace first, and then later complete the connection of your AWS account to your Workspace. Both approaches are acceptable.

Creating an AWS role

To create your AWS role needed to authorize Stackdriver Monitoring, you must have the **Account ID** and **External ID** for your Workspace. If you don't have them, follow the instructions in Getting your account and external IDs (#get-ids).

To create the AWS role, do the following:

1. Log into your AWS IAM console and click **Roles** in the left-side menu.
2. Click **Create role** and do the following:
    - For the **Role type**, select **Another AWS account**.
    - In the **Account ID** field, enter the account ID provided by Monitoring.
    - Select the **Require external ID** checkbox.
    - In the **External ID** field, enter the external ID provided by Monitoring.

- Don't select **Require MFA**.

3. Click **Next: Permissions**.
4. From the **Policy name** drop-down list, select **ReadOnlyAccess**:
5. Click **Next: Tags**.
6. (Optional) Add metadata to the role by attaching tags as key–value pairs.
7. Click **Next: Review** and fill in or verify the following information:
    - In the **Role name** field, enter a name such as `GoogleStackdriver`.
    - (Optional) In the **Role description** field, enter anything you wish.
    - In the **Trusted entities** field, verify it's the **Account ID** you entered earlier.
    - In the **Policies** field, verify the value is **ReadOnlyAccess**.
8. In the **AWS IAM** page, click **Create Role**.
9. On the **Summary** page, copy the **Role ARN** string so that you can give it to Monitoring. If you don't see the summary, click the name of your role (for example, **GoogleStackdriver**) in the list of AWS roles.

Connecting an AWS account

Note: These instructions work for a newly-created Workspace or for an existing Workspace. If you encounter any issues, go to Troubleshooting (#troubleshooting).

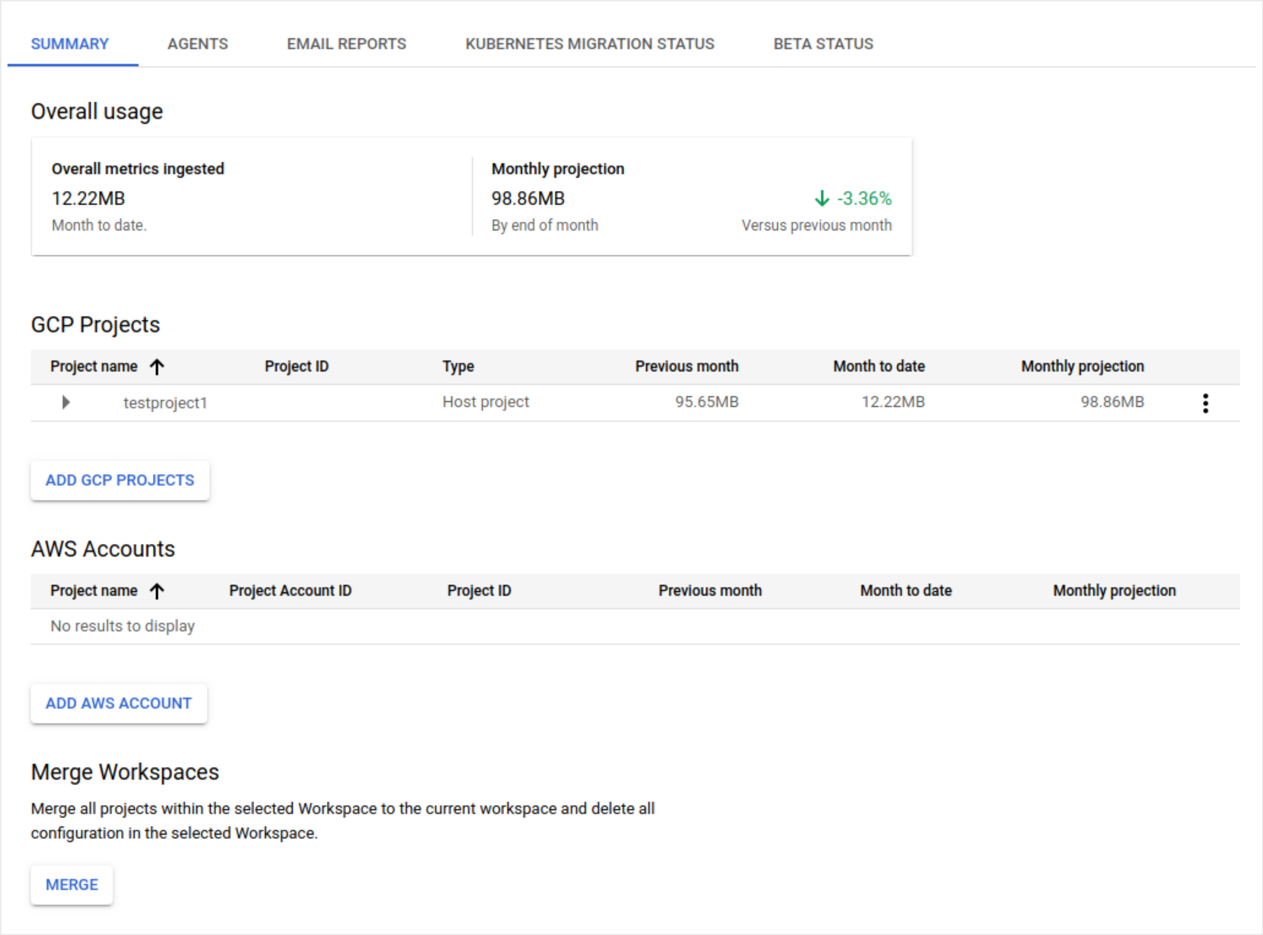
To add an AWS account to an existing Workspace, do the following:

1. In the Cloud Console, go to **Monitoring**:

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

2. Do the following:
    - If **Settings** is displayed in the navigation pane, click **Settings** and select the **Summary** tab.
    - Otherwise, in the toolbar, click **Menu** ▾ and then select **Workspace Settings**. In the **Workspace settings** page, select **Monitored accounts**.

The pane in the following screenshot shows that you are monitoring a single Google Cloud project—the Workspace's hosting project. You aren't yet monitoring any AWS accounts.



Overall usage

Overall metrics ingested	Monthly projection	
12.22MB	98.86MB	↓ -3.36%
Month to date.	By end of month	Versus previous month

GCP Projects

Project name ↑	Project ID	Type	Previous month	Month to date	Monthly projection	
▸ testproject1		Host project	95.65MB	12.22MB	98.86MB	⋮

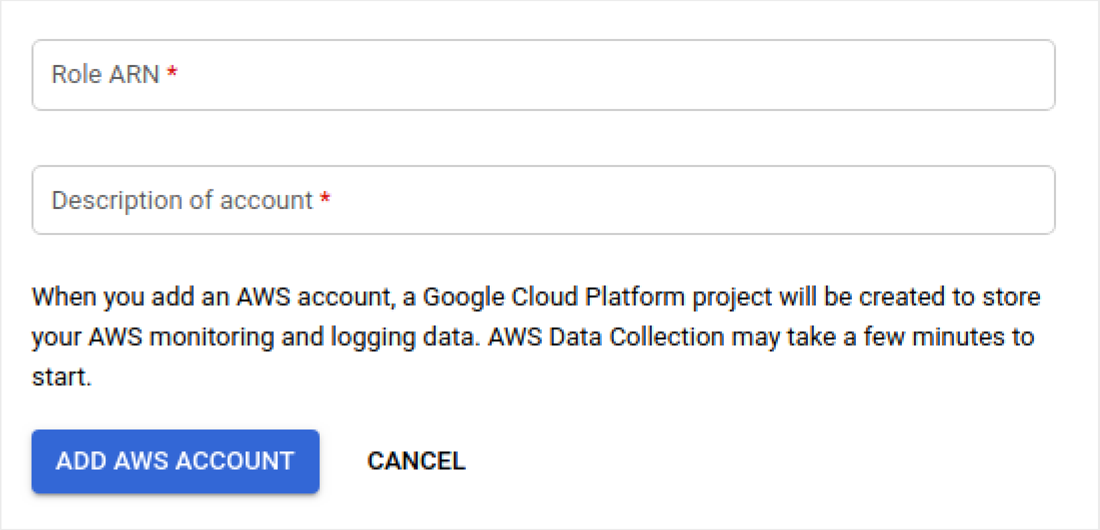
AWS Accounts

Project name ↑	Project Account ID	Project ID	Previous month	Month to date	Monthly projection
No results to display					

Merge Workspaces

Merge all projects within the selected Workspace to the current workspace and delete all configuration in the selected Workspace.

3. Click **Add AWS account**. Enter the **Account ID** and **External ID** from when you created a Workspace (#configure-sd-acct).
4. Enter the following information in the form:
   - In the **Role ARN** field, enter your Role ARN from Creating an AWS role (#creating-aws-role) or follow the instructions on the **Add AWS account** page to create the role.
   - In the **Description of account** field, enter a short description of your AWS account. The first word or two is used to create a new project ID.



Role ARN *

Description of account *

When you add an AWS account, a Google Cloud Platform project will be created to store your AWS monitoring and logging data. AWS Data Collection may take a few minutes to start.

5. Click **Add AWS account**. In a moment, the connection is confirmed.

★ **Note:** There can be up to a 5 minute delay before the resources in your AWS account appear in Monitoring.

AWS connector projects

When you connect to an AWS account, Monitoring creates an **AWS connector project** for you. The **Monitored accounts** page in your Workspace settings now includes the ID for this project:

Your AWS account description [YOUR_AWS_ACCOUNT_NUMBER]
Connected to [CONNECTOR_PROJECT_ID]

Where:

- `[YOUR_AWS_ACCOUNT_NUMBER]` represents the account number for your AWS account.
- `[CONNECTOR_PROJECT_ID]` represents the connector project where you receive logs and metrics from your AWS account and where you set up authorization for agents and other AWS applications that need to access Google Cloud.

  The connector project's ID always begins with `aws-`, and the project's name always begins with `AWS Link`.

Next step: Authorizing AWS applications (#provision-aws)

Troubleshooting

If you are told that your AWS account is already being monitored, do the following:

- If another Workspace is monitoring your AWS account, then you must remove your AWS account from it. You cannot monitor an AWS account from more than one Workspace. To disconnect an AWS account from a Workspace, go to Removing a project from a Workspace (https://cloud.google.com/monitoring/workspaces/guide#remove-project).
- This message can also appear if you didn't use the correct **Account ID** and **External ID** from your present Workspace when you created your AWS Role. The **External ID** is unique for each Workspace.

Authorizing AWS applications

You must perform the following steps if you do any of the following:

- Run the Monitoring or Logging agents on your AWS VM instances.
- Use any Google Cloud services from AWS applications.

To authorize applications running on AWS to access Google Cloud services, you give them access to a Google Cloud **service account** that has suitable Google Cloud IAM roles.

A single service account can authorize multiple AWS VM instances and applications in the same AWS account, or you can create multiple service accounts.

Create a service account

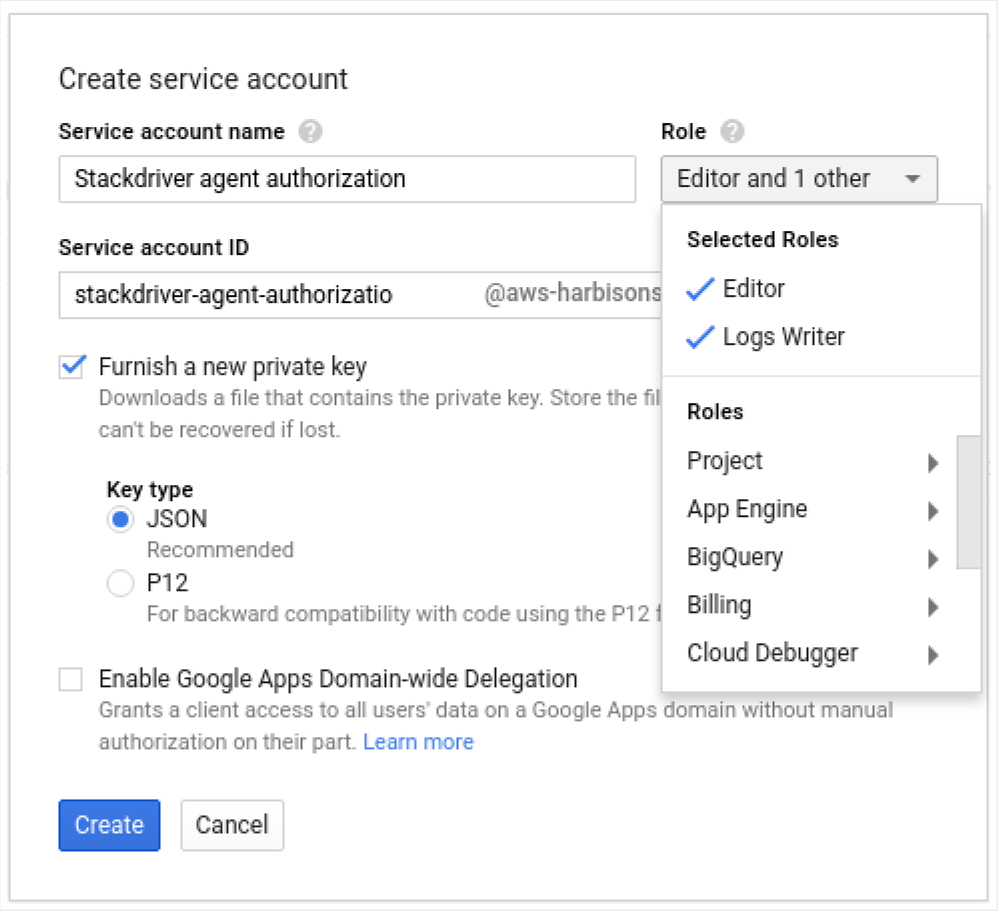
Note: Before starting these instructions, you must know the name of the **connector project** for your AWS account. To find the connector project, go to **Settings** and select the **Summary** tab. If **Settings** isn't displayed in the navigation pane, in the toolbar, click **Menu** ▾ , select **Workspace Settings**, and then select **Monitored accounts**.

To create the service account, do the following:

1. Go to the **IAM & Admin > Service accounts** page for your connector project:

   GO TO SERVICE ACCOUNTS (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/IAM-ADMIN/SERVICEACCOU

2. Select the AWS connector project (named `AWS Link...`) for your AWS account.
3. Your connector project likely has no service accounts, so you are asked to create one. Click **Create service account** and enter the following information:
    - In the **Service account name** field, enter `Stackdriver agent authorization`.
    - In the **Role** field, add both of the following values:
        - **Monitoring** > **Monitoring Metric Writer**
        - **Logging** > **Logs Writer**
    - Select the **Furnish a new private key** checkbox.
    - For **Key type**, click **JSON**.
    - Clear the **Enable G Suite Domain-wide Delegation** checkbox.



Create service account

Service account name: Stackdriver agent authorization

Role: Editor and 1 other

Service account ID: stackdriver-agent-authorizatio @aws-harbisons

☑ Furnish a new private key
Downloads a file that contains the private key. Store the fil
can't be recovered if lost.

Key type
● JSON
Recommended
○ P12
For backward compatibility with code using the P12 f

□ Enable Google Apps Domain-wide Delegation
Grants a client access to all users' data on a Google Apps domain without manual authorization on their part. Learn more

4. Click **Create**. The service account's private-key file is downloaded to your workstation with a name such as `Downloads/[PROJECT_NAME]-[KEY_ID].json`.

   Where:

    - `[PROJECT_NAME]` represents the name of your Google Cloud project.

- `[KEY_ID]` represents the generated private key.

To make the following instructions simpler, save the location of the credentials file in the variable `CREDS` on your workstation:

```
CREDS="Downloads/[PROJECT_NAME]-[KEY_ID].json"
```

Add a service account to a VM instance

To add a service account, do the following:

1. From your workstation, copy the private-key credentials file to your AWS EC2 instance and save it in a file named `temp.json`. In the `scp` command, specify the path to `key.pem`, your AWS SSH key pair file, and provide your AWS credentials:

```
KEY="/path/to/key.pem"
scp -i "$KEY" "$CREDS" AWS_USERNAME@AWS_HOSTNAME:temp.json
```

2. On your EC2 instance, move the credentials to `/etc/google/auth/application_default_credentials.json`:

```
GOOGLE_APPLICATION_CREDENTIALS="/etc/google/auth/application_default_credential
sudo mkdir -p $(dirname "$GOOGLE_APPLICATION_CREDENTIALS")
sudo mv "$HOME/temp.json" "$GOOGLE_APPLICATION_CREDENTIALS"
```

★ **Note:** `/etc/google/auth/application_default_credentials.json` is where the monitoring and logging agents look for the private key.

3. (Optional): Restrict access to the private-key credentials for the service account. For example:

```
sudo chown root:root "$GOOGLE_APPLICATION_CREDENTIALS"
sudo chmod 0400 "$GOOGLE_APPLICATION_CREDENTIALS"
```

4. Make sure the environment variable `GOOGLE_APPLICATION_CREDENTIALS` is visible to the agents and other applications that are authorized to use Google Cloud. The environment variable name is understood by the standard Google Cloud client libraries.

Install the agents

1. (Optional): Install the Stackdriver Monitoring and Logging agents by running the following commands on your EC2 instance:

```
curl -sSO https://dl.google.com/cloudagents/install-monitoring-agent.sh
sudo bash install-monitoring-agent.sh

curl -sSO https://dl.google.com/cloudagents/install-logging-agent.sh
sudo bash install-logging-agent.sh --structured
```

   The `--structured` flag lets the Logging agent send structured data to Stackdriver Logging. For more information, go to Structured logging operations (https://cloud.google.com/logging/docs/structured-logging).

2. Verify that the agents are running.

```
ps ax | grep fluentd
ps ax | grep collectd
```

   The expected output should be similar to the following:

```
[PROCESS_ID] ?    Sl   0:00 /opt/google-fluentd/embedded/bin/ruby /usr/sbin/goo
[PROCESS_ID] ?    Ssl  0:00 /opt/stackdriver/collectd/sbin/stackdriver-collectd
```

Using Monitoring services with AWS

This section shows you how to use Monitoring services with your AWS account.

Create an uptime check

Uptime checks verify that your web server is accessible from locations around the world. The alerting policy controls who is notified if the uptime checks should fail.

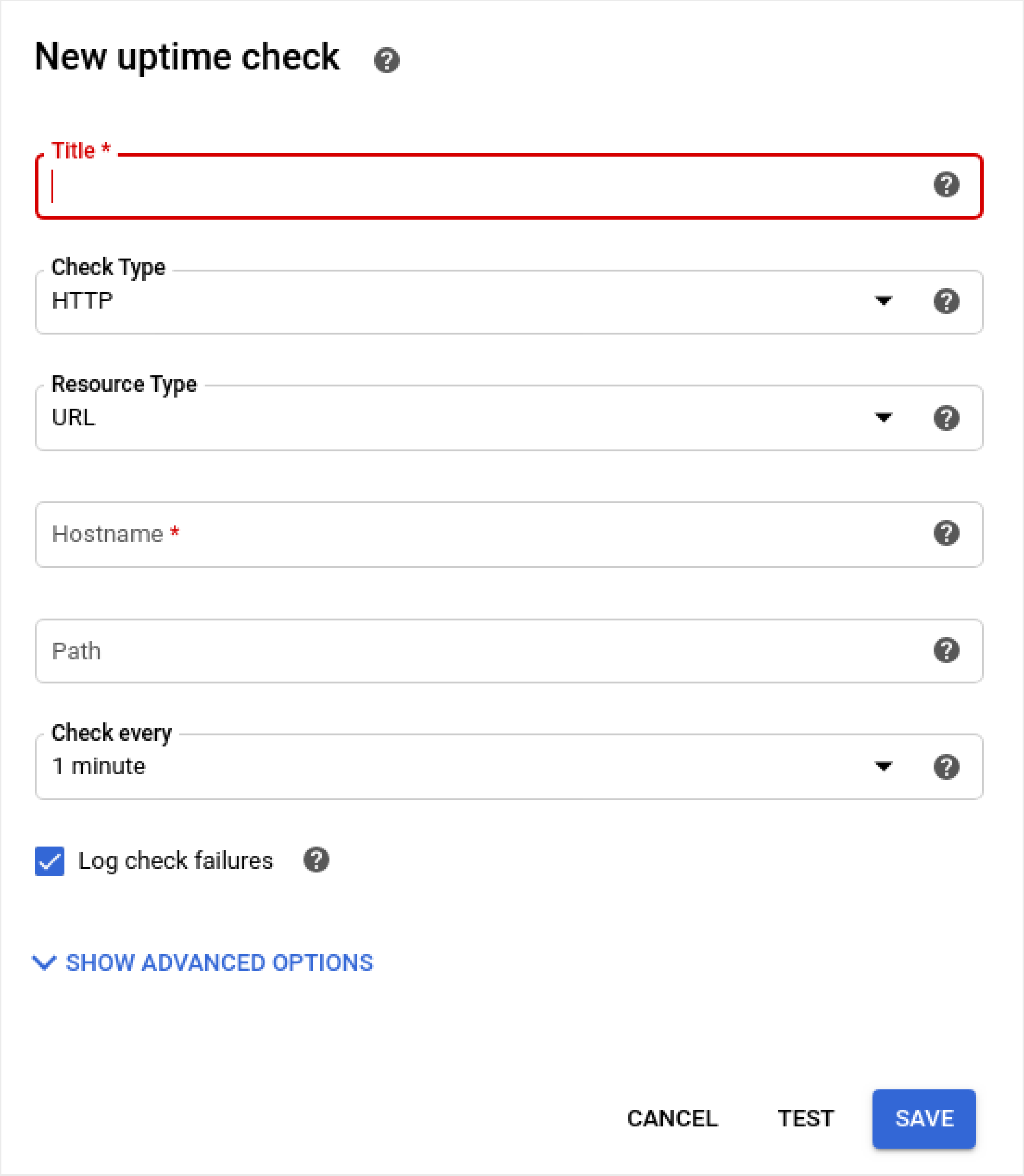
To create an uptime check, do the following:

1. Go to Monitoring:

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

The first time you access Monitoring for a Google Cloud project, Monitoring creates a Workspace and associates it with your project. This process is automatic unless you have a multi-project Workspace. In this case, a dialog appears that asks you to select between creating a Workspace and adding the project to an existing Workspace. Select the option to create a Workspace.

2. If you see the invitation **Create an Uptime Check** on the dashboard, then click it. Otherwise, go to **Uptime Checks** and then select **Create Uptime Check**.
3. In the **New Uptime Check** window, fill in the following fields:
   - In the **Title** field, enter`My Uptime Check`.
   - In the **Check type** menu, select **HTTP**.
   - In the **Resource Type** menu,choose an available resource
   - Depending on the select resource type, you might have other additional fields.



New uptime check

Title *

Check Type: HTTP

Resource Type: URL

Hostname *

Path

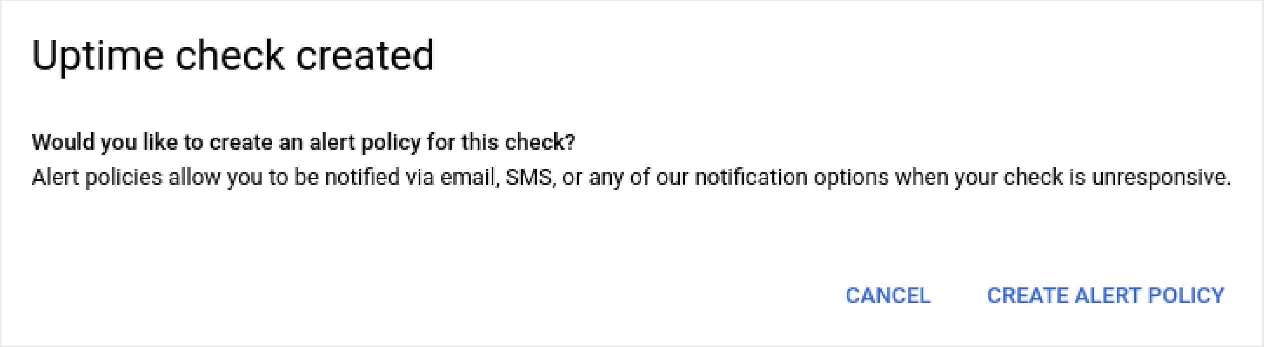
Check every: 1 minute

☑ Log check failures

4. To verify that your uptime check is working, click **Test**. If you see a `Connection error - refused` message, you either didn't install the Apache HTTP Server (#install-apache) or you might have specified the **HTTPS** check type rather than **HTTP**. For other errors, go to Verify your uptime check (https://cloud.google.com/monitoring/alerts/uptime-checks/#verify-check).
5. Click **Save**.

Create an alerting policy

1. In the **Uptime Check Created** pane, click **Create Alerting Policy**:

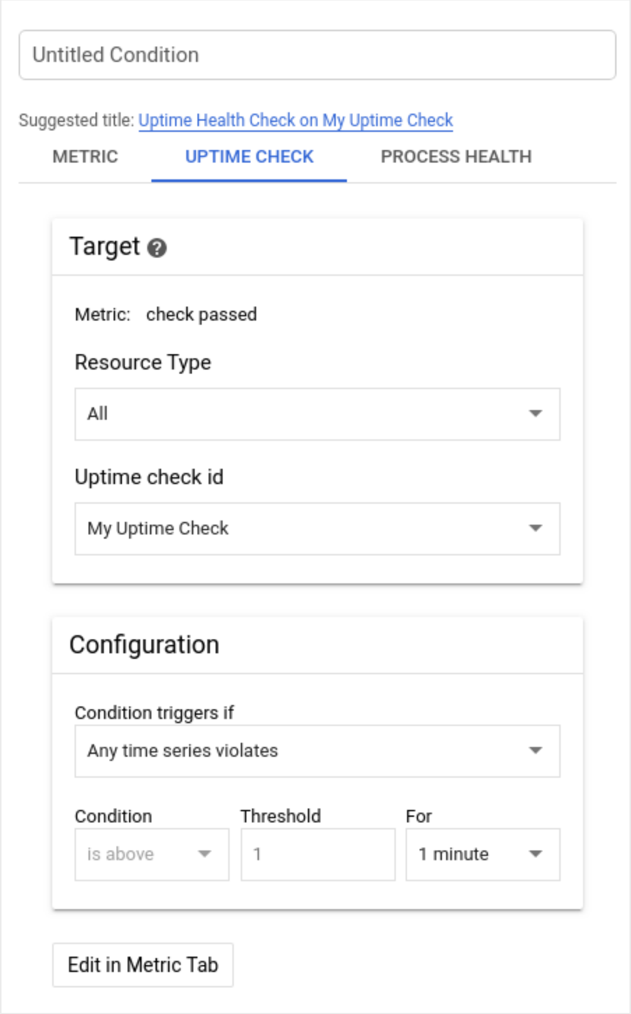


Uptime check created

Would you like to create an alert policy for this check?

Alert policies allow you to be notified via email, SMS, or any of our notification options when your check is unresponsive.

2. In the **Untitled Condition** field, enter a title for the alert policy condition. All other fields in the conditions pane are automatically populated from the uptime check you created.



Untitled Condition

Suggested title: Uptime Health Check on My Uptime Check

Target

Metric: check passed

Resource Type: All

Uptime check id: My Uptime Check

Configuration

Condition triggers if: Any time series violates

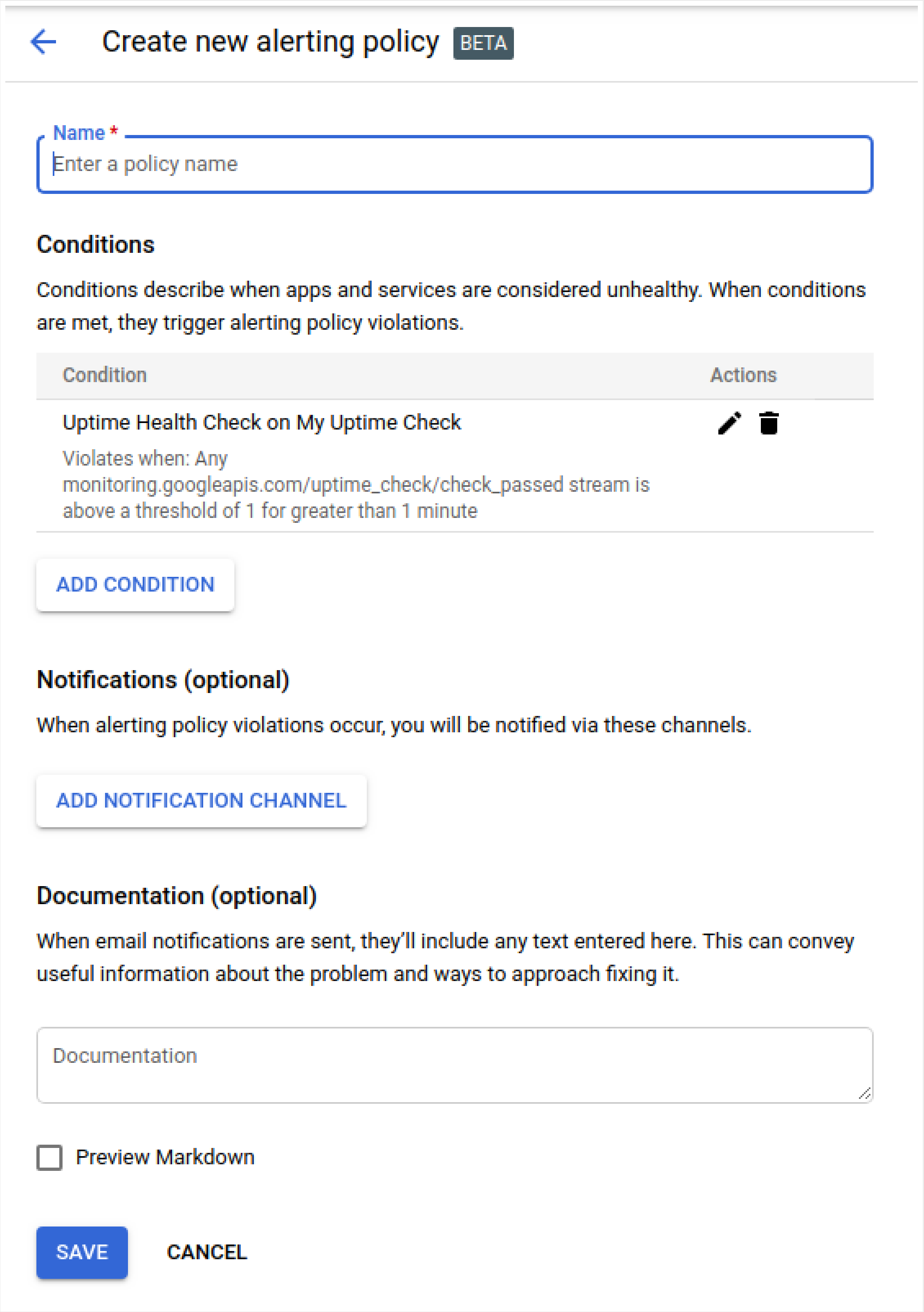
Condition: is above

Threshold: 1

For: 1 minute

3. Click **Save**.

4. Enter `My Uptime Check Policy` as the **Name** for the alerting policy.



Create new alerting policy BETA

Name *

Enter a policy name

Conditions

Conditions describe when apps and services are considered unhealthy. When conditions are met, they trigger alerting policy violations.

Condition	Actions
Uptime Health Check on My Uptime Check Violates when: Any monitoring.googleapis.com/uptime_check/check_passed stream is above a threshold of 1 for greater than 1 minute	

Notifications (optional)

When alerting policy violations occur, you will be notified via these channels.

Documentation (optional)

When email notifications are sent, they'll include any text entered here. This can convey useful information about the problem and ways to approach fixing it.

Documentation

□ Preview Markdown

5. (Optional) To configure an email notification, click **Add notification channel**, select **Email** from the menu, enter your email address, and then click **Add**.

6. Click **Save**. You see a summary of the policy.

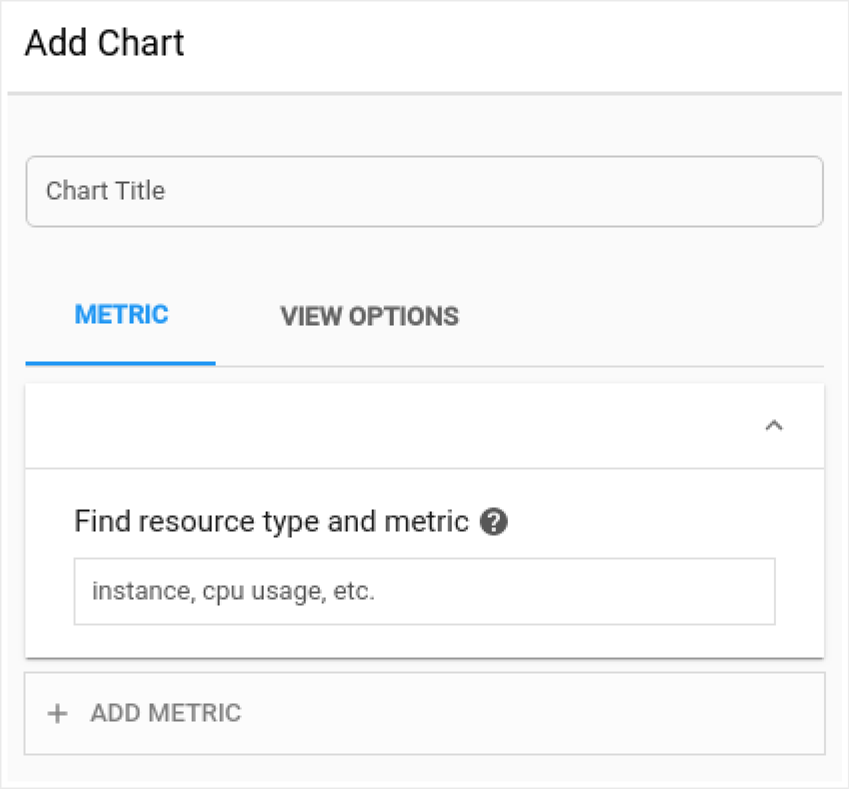
Create a dashboard and chart

To display the metrics collected by Monitoring, complete the following steps:

1. Go to Monitoring:

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

2. Select **Dashboards** and then select **Create dashboard**.
3. Enter `Quickstart dashboard` as the name for the dashboard and click **Confirm**.
4. Click **Add Chart**.
5. Ensure the **Metric** tab is selected:

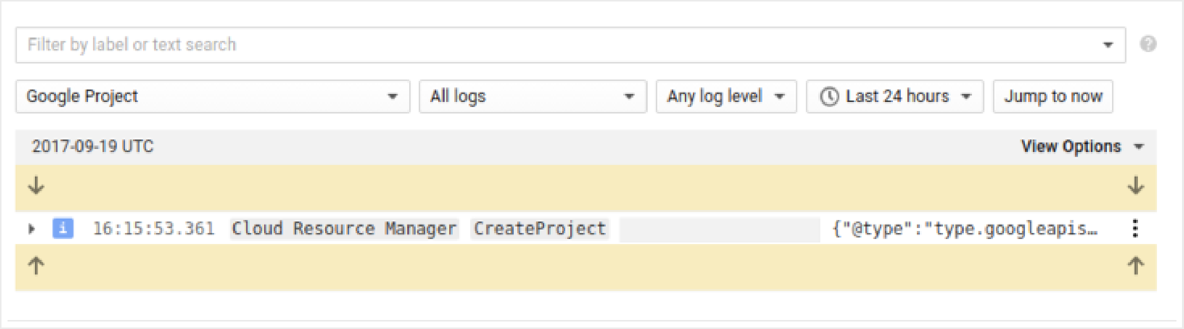
   

6. Under the heading **Find resource type and metric**, click the textbox and select an AWS metric.
7. Click **Save**.

View your logs

Monitoring and Logging are closely integrated.

1. In the Cloud Console , go to **Logging** and then select **AWS Link**.
2. The Logs Viewer for your AWS connector project, contains your AWS logs. To change the Logs Viewer focus to see the logs you want:
   - Go to **Google Project** > **All project_id** You should see at least one audit log (https://cloud.google.com/logging/docs/audit/) from setting up your AWS connector project:

     ```
     16:15:53.361 Cloud Resource Manager CreateProject {"@type":"type.googleapis…
     ```

   - If you installed the Stackdriver Monitoring agent on your supported AWS VM instances, you might see other log options.

Note: You don't see your AWS logs in your Workspace `aws-quickstart`. You must look in your AWS connector project.

Clean up

To avoid incurring charges to your Google Cloud account for the resources used in this quickstart, follow these steps.

1. Remove your Monitoring charts and alerts. Go to Monitoring:
   a. Delete your alerting policy from **Alerting**.
   b. Delete your uptime check from **Alerting**.
   c. Delete your charts from **Dashboards**.
2. In Monitoring, do the following:
   - If **Settings** appears in the navigation pane, click **Settings** and select the **Summary** tab. In the **Monitored accounts** section, remove your AWS account.

- Otherwise, in the toolbar, click **Menu** ▾ and then select **Workspace Settings**. In the **Workspace settings** page, select **Monitored accounts** and then remove your AWS account.

3. In your Amazon account, delete the AWS IAM role that you created for the quickstart.
4. In the Google Cloud Console, delete your AWS connector project and—if you created it for this quickstart—your Google Cloud project, `aws-quickstart`. To delete a project, you select the project, go to **IAM & Admin** and select **Settings**, and then click **Delete Project**.

What's next

- Go to Supported metrics (https://cloud.google.com/monitoring/api/metrics) for a list of all the built-in metrics. There are over 500 metrics for Amazon AWS. If you want to create your own Monitoring metrics, go to Custom metrics (https://cloud.google.com/monitoring/custom-metrics).
- To use the Monitoring API, go to the API reference (https://cloud.google.com/monitoring/api/ref_v3/rest).
- For more information on logging and its relation to monitoring, go to Logging (https://cloud.google.com/logging/docs).

Last updated January 13, 2020.