Google Cloud Platform Data Collection Prerequisites

The following prerequisites are required for each Google Cloud Platform (GCP) project in order to connect to and collect compute engine (GCE) instance data from GCP:

1. Data collection APIs
   - Enable Cloud Resource Manager API;
   - Verify Cloud Monitoring API is enabled.
2. Google Cloud Platform Service Account
   - Create a service account with Project role set to "Viewer". Alternatively, you can create a role with the minimum permissions required for data collection.
   - Create the JSON key credentials;
   - Optionally, link this service account to other GCP projects from which you want to collect data.
3. Optionally, you can install the Ops agent on each GCE instance to collect memory data. See https://cloud.google.com/stackdriver/docs/solutions/agents/ops-agent for details.

To learn more watch the following video: Google Cloud Platform Prerequisites for Collecting Data.

Verify GCP Data Collection APIs are Enabled

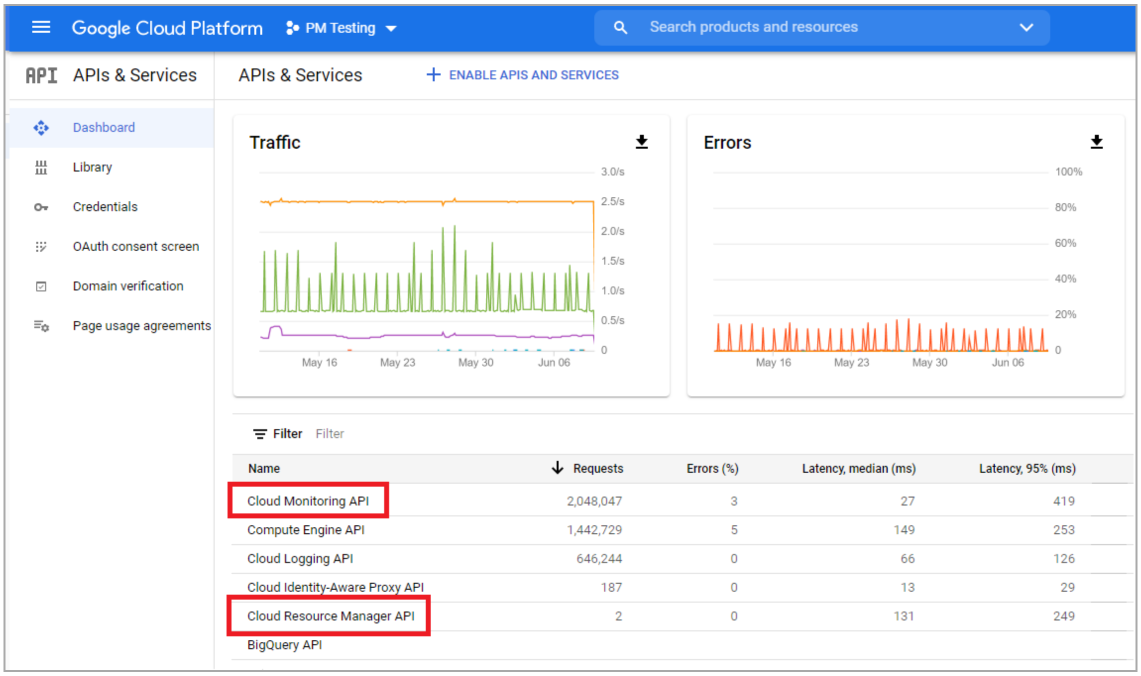
You need to verify that the following APIs are enabled for your project:

- Cloud Resource Manager API—Needs to be enabled, if not listed.
- Cloud Monitoring API—is enabled by default when the project is created.

Verify these APIs are enabled before creating the service account. When you create the keys for the service account the permissions for the required APIs will be included in the key file and are required by Densify.

1. Login to the GCP console and select your project.
2. From the GCP console main menu, navigate to **APIs & services** > **Dashboard**.
3. From the **APIs & services** Dashboard, ensure that the following APIs are enabled and listed in the **Enabled APIs and services** list:
   - Cloud Resource Manager API
   - Cloud Monitoring API (previously named, Stackdriver Monitoring API)

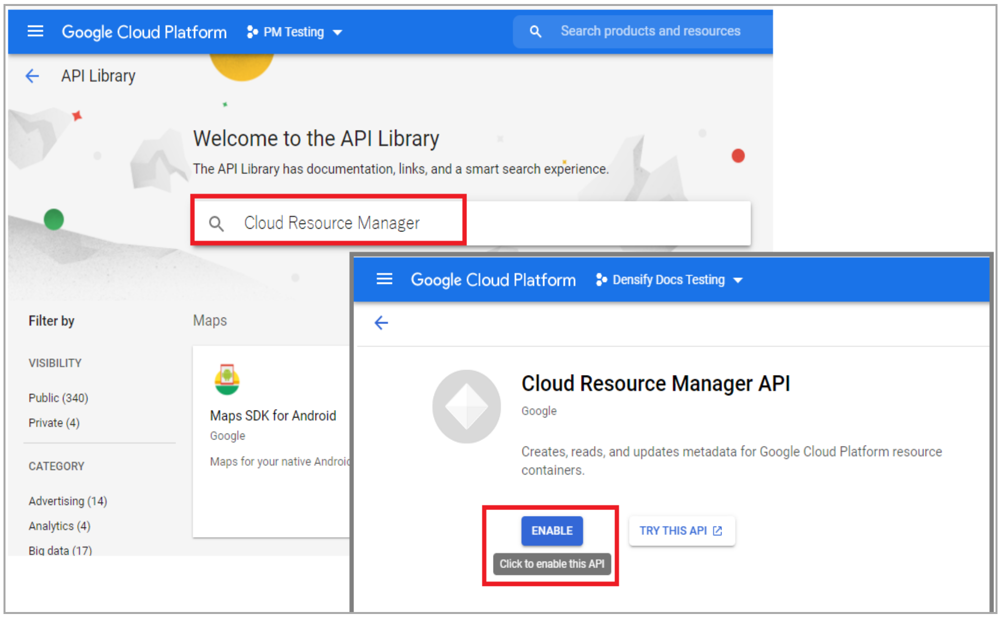
   Figure: APIs & Services Dashboard



Name	↓ Requests	Errors (%)	Latency, median (ms)	Latency, 95% (ms)
Cloud Monitoring API	2,048,047	3	27	419
Compute Engine API	1,442,729	5	149	253
Cloud Logging API	646,244	0	66	126
Cloud Identity-Aware Proxy API	187	0	13	29
Cloud Resource Manager API	2	0	131	249
BigQuery API				

4. If the Cloud Resource Manager API is not listed, click on **ENABLE APIS AND SERVICES** at the top of the dashboard. Search for the Cloud Resource Manager API and click **Enable**:

Figure: Enabling Cloud Resource Manager API



The API Library has documentation, links, and a smart search experience.

Creates, reads, and updates metadata for Google Cloud Platform resource containers.

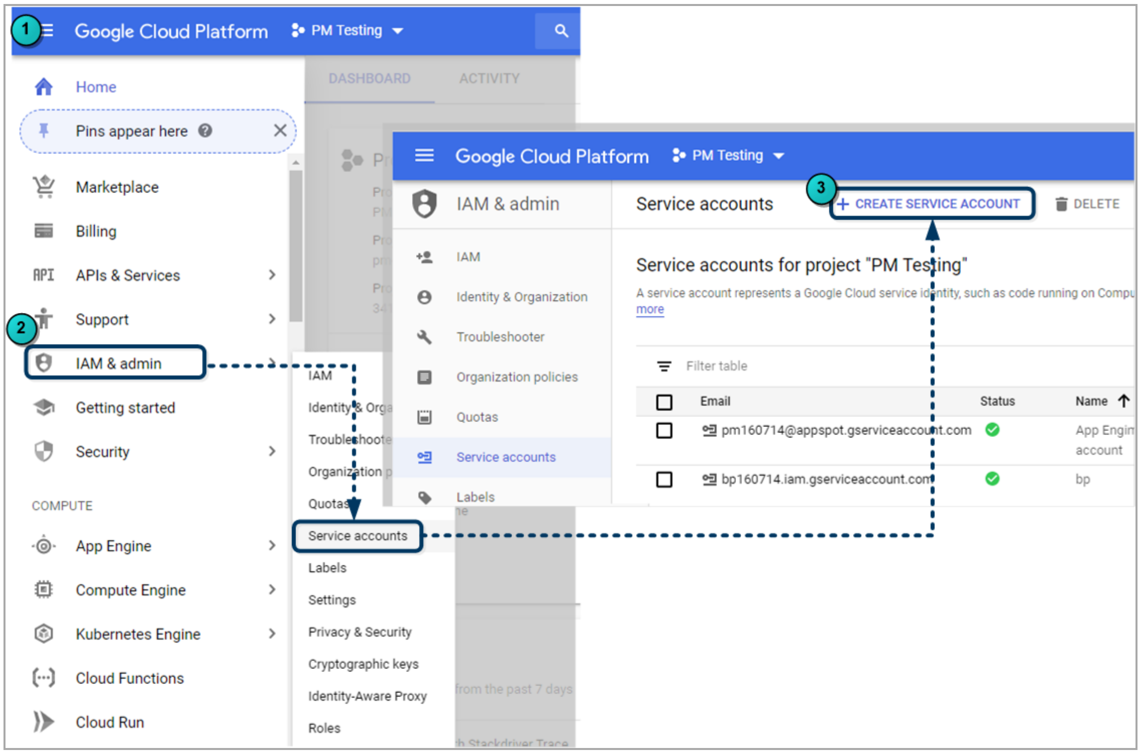
Creating a GCP Service Account

To connect Densify to your GCP project, you will need a GCP service account and corresponding credentials in JSON format. You need to repeat this process for each of your GCP projects and save the credential JSON files in an encrypted .ZIP file. You will then import this file to create a connection to collect data from your GCP projects.

Use the following instructions to create and configure the GCP service account:

1. Login to the GCP console and select your project.
2. From the main menu, select **IAM & Admin** > **Service accounts**.

Figure: Creating Service Account



Service accounts for project "PM Testing"

A service account represents a Google Cloud service identity, such as code running on Compu more

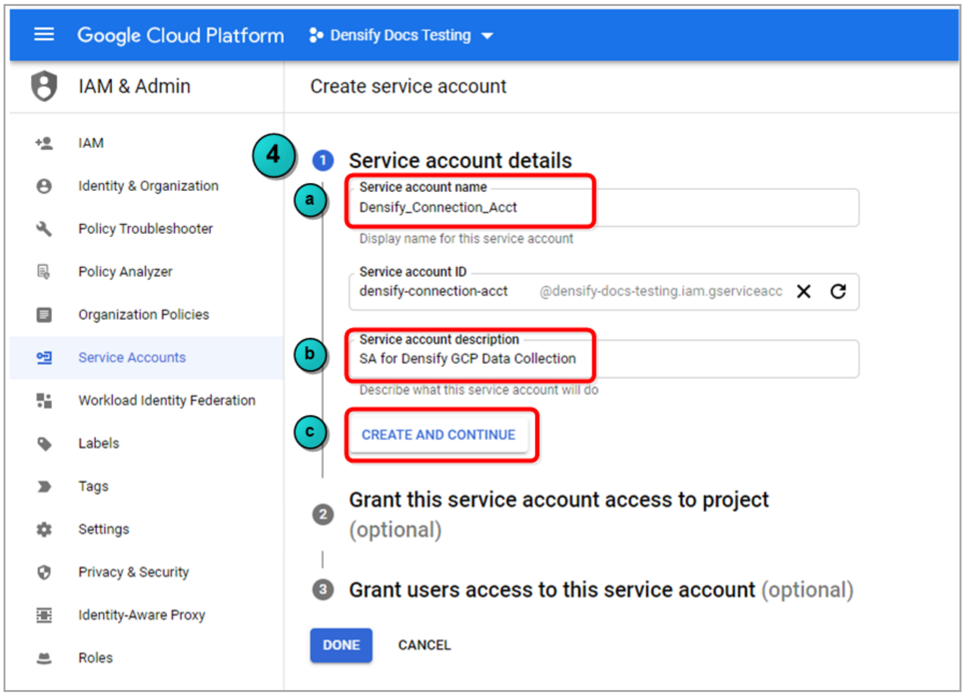
□	Email	Status	Name ↑
□	pm160714@appspot.gserviceaccount.com	✓	App Engin account
□	bp160714.iam.gserviceaccount.com	✓	bp

3. From the Service Accounts page, click **Create Service Account**.
4. In the **Create service account** pane:
   a. Specify **Service account name**. As a best practice, use the display name to keep track of what the account will be used for and what permissions are assigned. (e.g. Densify_Connection_Viewer)

   b. Provide a description of the service. This step is optional, but may help you link this account to other projects later on.

   c. Click **Create and Continue** to create the service account.

Figure: Creating Service Account



Create service account

1 Service account details

Service account name: Densify_Connection_Acct

Display name for this service account

Service account ID: densify-connection-acct @densify-docs-testing.iam.gserviceacc

Service account description: SA for Densify GCP Data Collection

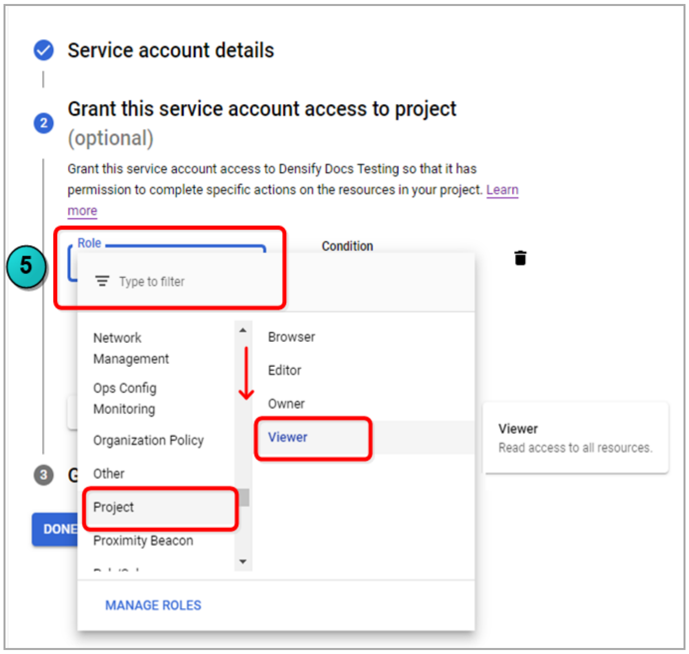
Describe what this service account will do

2 Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

5. In the **Role** field scroll down the list and select "Project" and then set the role for the whole project to "Viewer".

Figure: Assigning a Role to the Service Account



Service account details

2 Grant this service account access to project (optional)

Grant this service account access to Densify Docs Testing so that it has permission to complete specific actions on the resources in your project. Learn more

Viewer
Read access to all resources.

6. You do not need to add users to the this account so click **DONE**.

Creating Credentials for the Service Account

You now need to create the key for the service account. Densify uses this key to verify its identity

1. In the GCP console, from the main menu, select **IAM & Admin** > **Service accounts**.
2. You should see the account that you just created. In the **Key ID** column you can see that no keys have been created.
3. Click the options in the **Actions** column. Select **Manage keys** from the dropdown menu.
4. Select **Add Key** and then **Create new key**.
5. The key is generated and downloaded to your computer. Retain the generated keys for creating the Densify cloud connection.

Note: *Do not check these service account keys into your source code or leave them in the download directory.*

Creating a Role with Minimum Permissions for Data Collection

Densify recommends using the viewer role, as indicated above, to simplify setup and maintenance of data collection. The viewer role provides read-only access to your GCP services and resources and supports the requirements of Densify data collection and analysis. As the Densify data collection continues to evolve and expand, you do not need to update this permission policy to include newly added services and features.

Alternatively, you create a custom role and grant the minimum required permissions to the service account to be used Densify for data collection.

You must have the `iam.roles.create permission`, to create the custom role. The custom role must be created at the Organization level.

Note: *This custom role must be updated periodically as Densify’s standard data collection requirements are updated to support additional services and features.*

The custom role must have the following permissions to perform the GCP data collection:

- compute.disks.get
- compute.disks.list
- compute.firewalls.list
- compute.licenses.get
- compute.machineTypes.get
- compute.machineTypes.list
- compute.zones.list
- monitoring.metricDescriptors.list
- monitoring.timeSeries.list

- compute.images.list
- compute.instances.get
- compute.instances.list
- compute.projects.get
- compute.regions.list
- resourcemanager.projects.get
- resourcemanager.projects.list

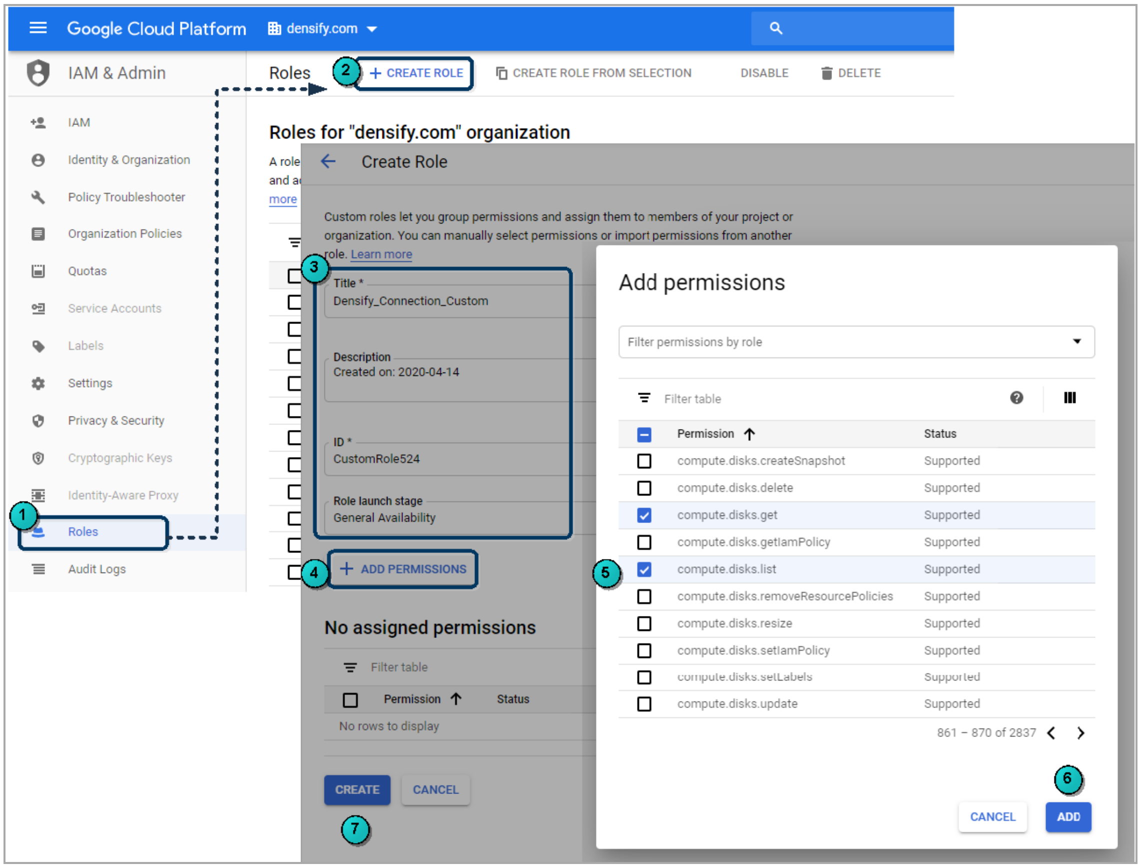
Use the following instructions to create the custom role:

1. Login to the GCP console and navigate to **Roles** in the main menu.
2. Select your organization from the Organization drop-down.
3. From the **Roles** page, click **Create Role**.
4. Enter a **Title**, **Description** for the role.

   Roles have both an ID and a title. The role ID is a unique identifier for the role and can be auto-generated. The role title appears in the list of roles in the GCP Console.

   The **Role Launch Stage** property is optional for this use case.
5. Click **Add Permissions**. See the above list and select all 15 permission for your custom role.
6. Click **Add** to grant the selected permissions to your custom role.
7. Click **CREATE** to create the role. You will now see your new role in the list on the **Roles** page.

   Figure: Creating Custom Role



Roles for "densify.com" organization

Create Role

Custom roles let you group permissions and assign them to members of your project or organization. You can manually select permissions or import permissions from another role. Learn more

Title *
Densify_Connection_Custom

Description
Created on: 2020-04-14

ID *
CustomRole524

Role launch stage
General Availability

Add permissions

	Permission ↑	Status
□	compute.disks.createSnapshot	Supported
□	compute.disks.delete	Supported
☑	compute.disks.get	Supported
□	compute.disks.getIamPolicy	Supported
☑	compute.disks.list	Supported
□	compute.disks.removeResourcePolicies	Supported
□	compute.disks.resize	Supported
□	compute.disks.setIamPolicy	Supported
□	compute.disks.setLabels	Supported
□	compute.disks.update	Supported

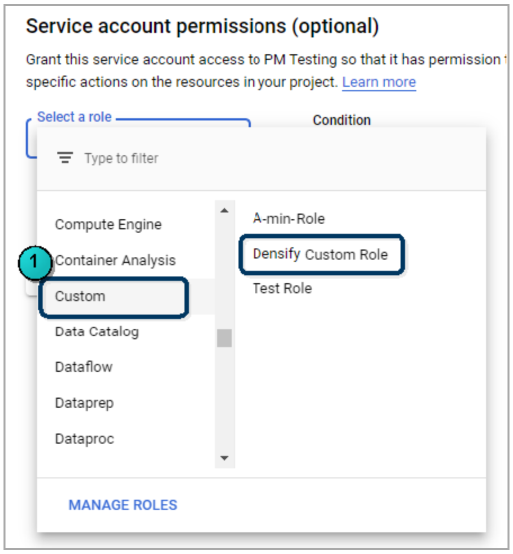
No assigned permissions

□	Permission ↑	Status

No rows to display

8. When you create the service account, select this custom role as follows:

Figure: Selecting Custom Role



Service account permissions (optional)

Grant this service account access to PM Testing so that it has permission t specific actions on the resources in your project. Learn more

Refer to Creating a GCP Service Account and Credentials, above for details.

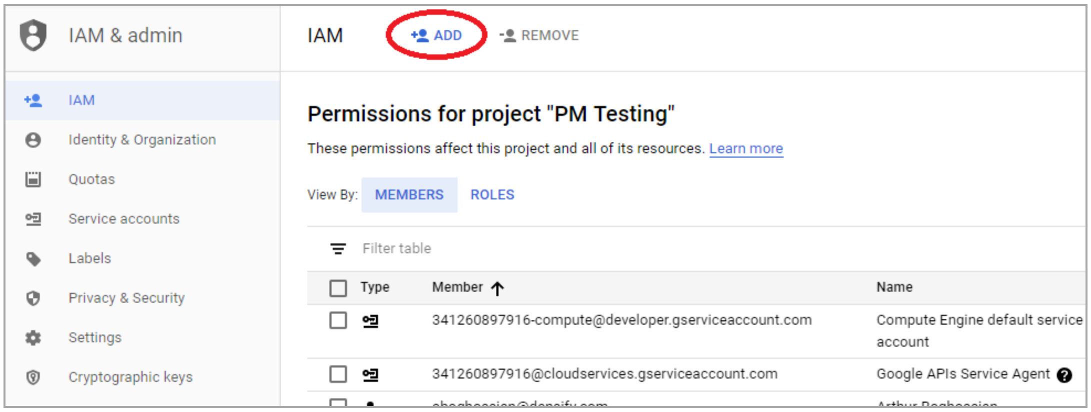
Using a Single GCP Service Account to Access Multiple Projects

In order to simplify data collection you can grant a single GCP service account access to other projects. This can be done by adding the service account ID from one project to another, through the account's **IAM & admin** dashboard.

You would then use this master service account to create your Densify cloud connection.

1. Login to the GCP console and select the project that contains the service account that will become the master account.
2. From the GCP console main menu, select **IAM & admin** > **Service accounts**.
3. Select the Service account ID to be used as the master account, from the list of service accounts. Copy the Service account ID onto the clipboard, as you cannot search from the **Add Members** function (in the steps below).
4. Select the project to which you want to add the service account.
5. From the **IAM & admin** menu, select **IAM**.
6. Click the **ADD** in the toolbar.

Figure: IAM & admin Dialog Box



Permissions for project "PM Testing"

These permissions affect this project and all of its resources. Learn more

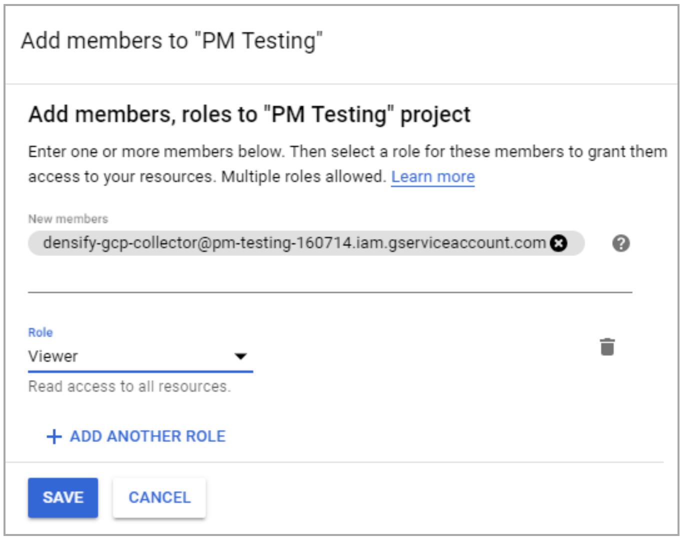
View By: MEMBERS ROLES

Filter table

□ Type	Member	Name
□	341260897916-compute@developer.gserviceaccount.com	Compute Engine default service account
□	341260897916@cloudservices.gserviceaccount.com	Google APIs Service Agent
□	aboghossian@densify.com	Arthur Boghossian

7. The **Add Members** dialog box opens. Paste the Service Account ID into the **New Members** field,
8. Select the account's role in the project. Select the **Project** > **Viewer** role for the newly added member.

Figure: Add Member Dialog Box



Add members to "PM Testing"

Add members, roles to "PM Testing" project

Enter one or more members below. Then select a role for these members to grant them access to your resources. Multiple roles allowed. Learn more

New members: densify-gcp-collector@pm-testing-160714.iam.gserviceaccount.com

Role: Viewer

Read access to all resources.

9. Click **Add** to complete and save the change. You can now use the private key previously generated from the service account to access the selected project.
10. You can repeat these steps for your other projects.

Collecting GCP Memory Metrics

The Ops Agent is the primary agent for collecting memory and other metrics from your Compute Engine instances. The Ops Agent replaces the stackdriver agent and cloud monitoring agent.

Refer to https://cloud.google.com/stackdriver/docs/solutions/agents/ops-agent for details of installing and configuring the agent.

Creating the Cloud Connection in Densify

Once all of the prerequisites are complete, you can create the cloud connection through the Cloud Connection wizard. See *Using the Public Cloud Connection Wizard* (Help Topic ID 380290).

Modifying Your Google Cloud Connection

When you create the GCP cloud connection for the first time, Densify discovers all of the projects, associated with the role or service account. Upon saving the connection Densify will schedule data collection from each of the discovered and selected projects.

If subsequently, projects are added, they will not be included in data collection. Additionally, projects that are removed will continue to be included, resulting in wasted time and resources. To add new projects or remove old ones, edit the cloud connection. See *Editing a Connection*, in the topic *Using the Public Cloud Connection Wizard* (Help Topic ID 380290).