This page describes how to profile applications running outside Google Cloud.

In this scenario, your application and the Stackdriver Profiler agent run outside Google Cloud, but you use the Stackdriver Profiler interface to analyze the profiling data.

Using the Profiler interface to analyze profiling data requires a Google Cloud project. The profiling agent running elsewhere must be able to send the profiles back for analysis. To enable this, you must:

1. Create a Google Cloud project and enable the API.
2. Obtain credentials for the profiling agent to use when uploading profiles.
3. Configure the agent to use the credentials and the ID of the Google Cloud project.

In the Cloud Console, on the project selector page, click **Create** to begin creating a new Cloud project.

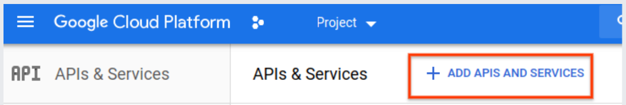
Go to the project selector page (https://console.cloud.google.com/projectselector2/home/dashboard)

In the Cloud Console page for your new project, go to the **APIs & Services** page:

1. Go to the **APIs & Services** dashboard:

   Go to APIs & services (https://console.cloud.google.com/apis/dashboard)

2. Click the **Add APIs and Services** button.



3. Search for **Profiler API**.

4. In the search results, select **Stackdriver Profiler API**.
5. If **API enabled** is displayed, then the API is already enabled. If not, click the **Enable** button.

There are two ways to obtain credentials for the agent to use:

- Let the agent use a service account with private-key authentication
- Let the agent use application default credentials (ADC).

To enable the agent to use a service account with private-key authentication, you must:

1. Create a service account. For example, using the Cloud SDK:

   See Creating a service account (/iam/docs/creating-managing-service-accounts#creating_a_service_account) for more information.
2. Grant the service account the **roles/cloudprofiler.agent** role (/profiler/docs/iam), so that it can write profiling data. For example, using the Cloud SDK:

   See Granting roles to service accounts (/iam/docs/granting-roles-to-service-accounts#granting_access_to_a_service_account_for_a_resource) for more information.
3. Create a JSON key for the service account. For example, using the Cloud SDK:

See Creating service account keys (/iam/docs/creating-managing-service-account-keys) for more information.

4. On the machine where the profiling agent will run:

   a. Put a copy of the file containing the JSON key you just created.

   b. Set the environment variable `GOOGLE_APPLICATION_CREDENTIALS` to the fully qualified name of the file containing the JSON key. This environment variable must be visible to the process running the profiling agent, so if you use a script or Dockerfile to run the process, include the environment variable there.

To enable the agent to use application default credentials, you obtain user-access credentials via a web flow and put them where the Application Default Credentials library expects them. These credentials act as a proxy for a service account.

To use application default credentials, run the following Cloud SDK command:

and follow the steps this command guides you through.

The profiling agent must be configured to specify the ID of your Google Cloud project so it can upload profiles. The mechanism for doing this depends on the language.

To learn about the Profiler graph and controls, go to Using the Stackdriver Profiler Interface (/profiler/docs/using-profiler). For advanced information, go to the following:

- Filtering profiles (/profiler/docs/filtering-profiles)
- Focusing the graph (/profiler/docs/focusing-profiles)
- Compare profiles (/profiler/docs/comparing-profiles)