




project-factory

 provider

 Partner

Version 18.0.0 (latest) ▾

Creates an opinionated Google Cloud project by using Shared VPC, IAM, and Google Cloud APIs

Published January 8, 2025 by [terraform-google-modules](#)

Module managed by [cloud-foundation-bot](#)

Source Code: [github.com/terraform-google-modules/terraform-google-project-factory](#) (report an issue)

 Submodules ▾

 Examples ▾

Module Downloads

- Downloads this week
- Downloads this month
- Downloads this year
- Downloads over all time

Provision Instructions

Copy and paste into your Terraform configuration, insert the variables,

```
module "project-factory" {
  source = "terraform-google-modules/project-factory/google"
  version = "18.0.0"
  # insert the 2 required variables here
}
```

- Readme
- Inputs (57)
- Outputs (19)
- Dependencies (13)
- Resources (59)

Google Cloud Project Factory Terraform Module

[FAQ](#) | [Troubleshooting Guide](#) | [Glossary](#).

This module allows you to create opinionated Google Cloud Platform projects. It creates projects and configures aspects like Shared VPC connectivity, IAM access, Service Accounts, and API enablement to follow best practices.

To include G Suite integration for creating groups and adding Service Accounts into groups, use the [gsuite_enabled module](#).

Compatibility

This module is meant for use with Terraform 1.3+ and tested using Terraform 1.10+. If you find incompatibilities using Terraform >= 1.3, please open an issue. If you haven't [upgraded](#) and need a Terraform 0.12.x-compatible version of this module, the last released version intended for Terraform 0.12.x is [9.2.0](#).

Upgrading

See the [docs](#) for detailed instructions on upgrading between major releases of the module.

Usage

There are multiple examples included in the [examples](#) folder but simple usage is as follows:

```
name = "pf-test-1"
random_project_id = true
org_id = "1234567890"
usage_bucket_name = "pf-test-1-usage-report-bucket"
usage_bucket_prefix = "pf/test/1/integration"
billing_account = "ABCDEF-ABCDEF-ABCDEF"
svpc_host_project_id = "shared_vpc_host_name"

shared_vpc_subnets = [
  "projects/base-project-196723/regions/us-east1/subnetworks/default",
  "projects/base-project-196723/regions/us-central1/subnetworks/default",
  "projects/base-project-196723/regions/us-central1/subnetworks/subnet-1",
]
}
```

Features

The Project Factory module will take the following actions:

1. Create a new GCP project using the `project_name` .
2. If a shared VPC is specified, attach the new project to the `svpc_host_project_id` .

It will also give the following users network access on the specified subnets:

- The project's new default service account (see step 4)
 - The Google API service account for the project
 - The project controlling group specified in `group_name`
3. Delete the default compute service account.
 4. Create a new default service account for the project.
 1. Give it access to the shared VPC (to be able to launch instances).
 5. Attach the billing account (`billing_account`) to the project.
 6. Give the controlling group access to the project, with the `group_role` .
 7. Enable the required and specified APIs (`activate_apis`).
 8. Delete the default network.
 9. Enable usage report for GCE into central project bucket (`target_usage_bucket`), if provided.
 10. If specified, create the GCS bucket `bucket_name` and give the following accounts Storage Admin on it:
 1. The controlling group (`group_name`).
 2. The new default compute service account created for the project.
 3. The Google APIs service account for the project.

The roles granted are specifically:

- New Default Service Account
 - `compute.networkUser` on host project or specified subnets
 - `storage.admin` on `bucket_name` GCS bucket
- `group_name` is the controlling group
 - `compute.networkUser` on host project or specific subnets
 - Specified `group_role` on project
 - `iam.serviceAccountUser` on the default Service Account

- `compute.networkUser` on host project or specified subnets
- `storage.admin` on `bucket_name` GCS bucket

Shared VPC subnets and IAM permissions

A service project's access to shared VPC networks is controlled via the `roles/compute.networkUser` role and the location to where that role is assigned. If that role is assigned to the shared VPC host project, then the service project will have access to all shared VPC subnetworks. If that role is assigned to individual subnetworks, then the service project will have access to only the subnetworks on which that role was assigned. The logic for determining that location is as follows:

1. If `var.svpc_host_project_id` and `var.shared_vpc_subnets` are not set then the `compute.networkUser` role is not assigned
2. If `var.svpc_host_project_id` is set but no subnetworks are provided via `var.shared_vpc_subnets` then the `compute.networkUser` role is assigned at the host project and the service project will have access to all shared VPC subnetworks
3. If `var.svpc_host_project_id` is set and `var.shared_vpc_subnets` contains an array of subnetworks then the `compute.networkUser` role is assigned to each subnetwork in the array

Inputs

Name	Description	Type	Default
activate_api_identities	The list of service identities (Google Managed service account for the API) to force-create for the project (e.g. in order to grant additional roles). APIs in this list will automatically be appended to <code>activate_apis</code> . Not including the API in this list will follow the default behaviour for identity creation (which is usually when the first resource using the API is created). Any roles (e.g. service agent role) must be explicitly listed. See https://cloud.google.com/iam/docs/understanding-roles#service-agent-roles-roles for a list of related roles.	<pre>list(object({ api = string roles = list(string) }))</pre> <div>Copy</div>	<code>[]</code>
activate_apis	The list of apis to activate within the project	<code>list(string)</code>	<pre>["compute.googleapiv1"]</pre>
auto_create_network	Create the default network	<code>bool</code>	<code>false</code>
billing_account	The ID of the billing account to associate this project with	<code>string</code>	n/a
bucket_force_destroy	Force the deletion of all objects within the GCS bucket when deleting the bucket (optional)	<code>bool</code>	<code>false</code>
bucket_labels	A map of key/value label pairs to assign to the bucket (optional)	<code>map(string)</code>	<code>{}</code>
bucket_location	The location for a GCS bucket to create (optional)	<code>string</code>	<code>"US"</code>
bucket_name	A name for a GCS bucket to create (in the bucket_project project), useful for Terraform state (optional)	<code>string</code>	<code>""</code>
bucket_pap	Enable Public Access Prevention. Possible values are "enforced" or "inherited".	<code>string</code>	<code>"inherited"</code>
bucket_project	A project to create a GCS bucket (bucket_name) in, useful for Terraform state (optional)	<code>string</code>	<code>""</code>
bucket_ula	Enable Uniform Bucket Level Access	<code>bool</code>	<code>true</code>
bucket_versioning	Enable versioning for a GCS bucket to create (optional)	<code>bool</code>	<code>false</code>
budget_alert_pubsub_topic	The name of the Cloud Pub/Sub topic where budget related messages will be published, in the form of <code>projects/{project_id}/topics/{topic_id}</code>	<code>string</code>	<code>null</code>
budget_alert_spend_basis	The type of basis used to determine if spend has passed the	<code>string</code>	<code>"CURRENT_SPEND"</code>

Name	Description	Type	Default
budget_alert_spent_percents	A list of percentages of the budget to alert on when threshold is exceeded	<code>list(number)</code>	<pre>[0.5, 0.7, 1]</pre>
budget_amount	The amount to use for a budget alert	<code>number</code>	<code>null</code>
budget_calendar_period	Specifies the calendar period for the budget. Possible values are MONTH, QUARTER, YEAR, CALENDAR_PERIOD_UNSPECIFIED, CUSTOM. custom_period_start_date and custom_period_end_date must be set if CUSTOM	<code>string</code>	<code>null</code>
budget_custom_period_end_date	Specifies the end date (DD-MM-YYYY) for the calendar_period CUSTOM	<code>string</code>	<code>null</code>
budget_custom_period_start_date	Specifies the start date (DD-MM-YYYY) for the calendar_period CUSTOM	<code>string</code>	<code>null</code>
budget_display_name	The display name of the budget. If not set defaults to <code>Budget For <projects[0] All Projects></code>	<code>string</code>	<code>null</code>
budget_labels	A single label and value pair specifying that usage from only this set of labeled resources should be included in the budget.	<code>map(string)</code>	<code>{}</code>
budget_monitoring_notification_channels	A list of monitoring notification channels in the form <code>[projects/{project_id}/notificationChannels/{channel_id}]</code> . A maximum of 5 channels are allowed.	<code>list(string)</code>	<code>[]</code>
cloud_armor_tier	Managed protection tier to be set. Possible values are: CA_STANDARD, CA_ENTERPRISE_PAYGO	<code>string</code>	<code>null</code>
consumer_quotas	The quotas configuration you want to override for the project.	<div><pre>list(object({ service = string, metric = string, dimensions = map(string), limit = string, value = string, }))</pre><div>Copy</div></div>	<code>[]</code>
create_project_sa	Whether the default service account for the project shall be created	<code>bool</code>	<code>true</code>
default_network_tier	Default Network Service Tier for resources created in this project. If unset, the value will not be modified. See https://cloud.google.com/network-tiers/docs/using-network-service-tiers and https://cloud.google.com/network-tiers .	<code>string</code>	<code>""</code>
default_service_account	Project default service account setting: can be one of <code>delete</code> , <code>deprivilege</code> , <code>disable</code> , or <code>keep</code> .	<code>string</code>	<code>"disable"</code>
deletion_policy	The deletion policy for the project.	<code>string</code>	<code>"PREVENT"</code>
disable_dependent_services	Whether services that are enabled and which depend on this service should also be disabled when this service is destroyed.	<code>bool</code>	<code>true</code>
disable_services_on_destroy	Whether project services will be disabled when the resources are destroyed	<code>bool</code>	<code>true</code>
domain	The domain name (optional).	<code>string</code>	<code>""</code>
enable_shared_vpc_host_project	If this project is a shared VPC host project. If true, you must <i>not</i> set <code>svpc_host_project_id</code> variable. Default is false.	<code>bool</code>	<code>false</code>
essential_contacts	A mapping of users or groups to be assigned as Essential Contacts to the project, specifying a notification category	<code>map(list(string))</code>	<code>{}</code>
folder_id	The ID of a folder to host this project	<code>string</code>	<code>""</code>
grant_network_role	Whether or not to grant networkUser role on the host project/subnets	<code>bool</code>	<code>true</code>

Name	Description	Type	Default
group_name	A group to control the project by being assigned group_role (defaults to project editor)	string	""
group_role	The role to give the controlling group (group_name) over the project (defaults to project editor)	string	"roles/editor"
labels	Map of labels for project	map(string)	{}
language_tag	Language code to be used for essential contacts notifications	string	"en-US"
lien	Add a lien on the project to prevent accidental deletion	bool	false
name	The name for the project	string	n/a
org_id	The organization ID.	string	null
project_id	The ID to give the project. If not provided, the name will be used.	string	""
project_sa_name	Default service account name for the project.	string	"project-service-account"
random_project_id	Adds a suffix of 4 random characters to the project_id .	bool	false
random_project_id_length	Sets the length of random_project_id to the provided length, and uses a random_string for a larger collusion domain. Recommended for use with CI.	number	null
sa_role	A role to give the default Service Account for the project (defaults to none)	string	""
shared_vpc_subnets	List of subnets fully qualified subnet IDs (ie. projects/\$project_id/regions/\$region/subnetworks/\$subnet_id)	list(string)	[]
svpc_host_project_id	The ID of the host project which hosts the shared VPC	string	""
tag_binding_values	Tag values to bind the project to.	list(string)	[]
usage_bucket_name	Name of a GCS bucket to store GCE usage reports in (optional)	string	""
usage_bucket_prefix	Prefix in the GCS bucket to store GCE usage reports in (optional)	string	""
vpc_service_control_attach_dry_run	Whether the project will be attached to a VPC Service Control Perimeter in Dry Run Mode. vpc_service_control_attach_enabled should be false for this to be true	bool	false
vpc_service_control_attach_enabled	Whether the project will be attached to a VPC Service Control Perimeter in ENFORCED MODE. vpc_service_control_attach_dry_run should be false for this to be true	bool	false
vpc_service_control_perimeter_name	The name of a VPC Service Control Perimeter to add the created project to	string	null
vpc_service_control_sleep_duration	The duration to sleep in seconds before adding the project to a shared VPC after the project is added to the VPC Service Control Perimeter. VPC-SC is eventually consistent.	string	"5s"

Outputs

Name	Description
api_s_account	API service account email
api_s_account_fmt	API service account email formatted for terraform use
budget_name	The name of the budget if created
domain	The organization's domain
enabled_api_identities	Enabled API identities in the project
enabled_apis	Enabled APIs in the project
group_email	The email of the G Suite group with group_name

Name	Description
project_id	ID of the project
project_name	Name of the project
project_number	Numeric identifier for the project
service_account_display_name	The display name of the default service account
service_account_email	The email of the default service account
service_account_id	The id of the default service account
service_account_name	The fully-qualified name of the default service account
service_account_unique_id	The unique id of the default service account
tag_bindings	Tag bindings
usage_report_export_bucket	GCE usage reports bucket

Requirements

Software

- [gcloud sdk](#) >= 269.0.0
- [jq](#) >= 1.6
- [Terraform](#) >= 1.3
- [terraform-provider-google](#) plugin >= 5.41
- [terraform-provider-google-beta](#) plugin >= 5.41
- [terraform-provider-gsuite](#) plugin ~> 0.1.x if GSuite functionality is desired

Permissions

In order to execute this module you must have a Service Account with the following roles:

- `roles/resourcemanager.folderViewer` on the folder that you want to create the project in
- `roles/resourcemanager.organizationViewer` on the organization
- `roles/resourcemanager.projectCreator` on the organization
- `roles/billing.user` on the organization
- `roles/storage.admin` on bucket_project
- If you are using shared VPC:
 - `roles/billing.user` on the organization
 - `roles/compute.xpnAdmin` on the organization
 - `roles/compute.networkAdmin` on the organization
 - `roles/browser` on the Shared VPC host project
 - `roles/resourcemanager.projectIamAdmin` on the Shared VPC host project

Script Helper

A [helper script](#) is included to create the Seed Service Account in the [Seed Project](#), grant the necessary roles to the [Seed Service Account](#), and enable the necessary API's in the Seed Project. Run it as follows:

```
./helpers/setup-sa.sh -o <organization id> -p <project id> [-b <billing account id>] [-f <folder id>] [-n <service account name>]
```

Copy

In order to execute this script, you must have an account with the following list of permissions:

- `resourcemanager.organizations.list`
- `resourcemanager.projects.list`

- `iam.serviceAccountKeys.create`
- `resourcemanager.organizations.setIamPolicy`
- `resourcemanager.projects.setIamPolicy`
- `serviceusage.services.enable` on the project
- `servicemanagement.services.bind` on following services:
 - `cloudresourcemanager.googleapis.com`
 - `cloudbilling.googleapis.com`
 - `iam.googleapis.com`
 - `admin.googleapis.com`
 - `appengine.googleapis.com`
- `billing.accounts.getIamPolicy` on a billing account.
- `billing.accounts.setIamPolicy` on a billing account.

Specifying credentials

The Project Factory module uses the [Google Terraform provider](#) to authenticate all GCP API calls. To configure credentials, you should configure the `google` and `google-beta` providers.

```
provider "google" {
  credentials = "${file(var.credentials_path)}"
}

provider "google-beta" {
  credentials = "${file(var.credentials_path)}"
}
```

Copy

APIs

In order to operate the Project Factory, you must activate the following APIs on the base project where the Service Account was created:

- Cloud Resource Manager API - `cloudresourcemanager.googleapis.com` [troubleshooting](#)
- Cloud Billing API - `cloudbilling.googleapis.com` [troubleshooting](#)
- Identity and Access Management API - `iam.googleapis.com` [troubleshooting](#)
- Admin SDK - `admin.googleapis.com` [troubleshooting](#)

Optional APIs

- Google App Engine Admin API - `appengine.googleapis.com` [troubleshooting](#)
 - Please note that if you are deploying an App Engine Flex application, you should not delete the default compute service account (as is default behavior). Please see the [troubleshooting doc](#) for more information.
- Cloud Billing Budget API - `billingbudgets.googleapis.com`
 - Please note this API is only required if configuring budgets for projects.

Verifying setup

A [preconditions checker script](#) is included to verify that all preconditions are met before the Project Factory runs. The script will run automatically if the script dependencies (Python, "google-auth", and "google-api-python-client") are available at runtime. If the dependencies are not met, the precondition checking step will be skipped.

The precondition checker script can be directly invoked before running the project factory:

```
./helpers/preconditions/preconditions.py \
--credentials_path "./credentials.json" \
--billing_account 000000-000000-000000 \
```

Copy

Caveats

Moving projects from org into a folder

There is currently a bug with moving a project which was originally created at the root of the organization into a folder. The bug and workaround is described [here](#), but as a general best practice it is easier to create all projects within folders to start. Moving projects between different folders *is* supported.

Deleting default service accounts

Default SAs can be removed by setting `default_service_account` input variable to `delete` , but there can be certain scenarios where the default SAs are required. Hence some considerations to be aware of:

1. [Using App Engine SA](#).
2. Cloud Scheduler dependency on AppEngine(default SA). Default SA is required to be able to setup [Cloud scheduler](#), please refer to the [document](#) for more upto date information.

With a combination of project-factory's default behavior, [disable](#), and setting [constraints/iam.automaticIamGrantsForDefaultServiceAccounts](#) org constraint will address removing the default editor IAM role on the SAs and limits the SA usage. However, when the `default_service_account` is set to `delete` please be aware of the default SA dependency for AppEngine/CloudScheduler services. Accounts deleted within 30days can be [restored](#).

G Suite

The core Project Factory solely deals with GCP APIs and does not integrate G Suite functionality. If you would like certain group-management functionality which was previously included in the Project Factory, see the [G Suite module](#).

Install

Terraform

Be sure you have the correct Terraform version (1.3+), you can choose the binary here:

- <https://releases.hashicorp.com/terraform/>

[application-default-credentials]:
https://cloud.google.com/docs/authentication/production#providing_credentials_to_your_application