Google Cloud setup checklist

This checklist helps you set up Google Cloud for scalable, production-ready enterprise workloads. The checklist is designed for administrators who are trusted with complete control over the company's Google Cloud resources.

The checklist consists of 10 tasks that have step-by-step procedures. Some tasks can be accomplished multiple ways; in general, we describe the way that will be helpful to the largest number of users. As you go through the checklist, take into account your own business needs. If you make choices that differ from what we've recommended, keep track of those differences for later tasks in the checklist.

You can set up Google Cloud interactively by using the Cloud Console version of the checklist. The Cloud Cons
offers the ability to automate and simplify key steps, and to track progress of all users who participate in the
ist. Go to the Cloud Console version of the checklist (https://console.cloud.google.com/getting-started/enterp

Click a checklist item to see the detailed steps for that item.

Checklist

□ 1. Set up or confirm an identity account

You must use Cloud Identity or G Suite to centrally manage Google Cloud and create the organization resource that is required to perform many actions in the checklist. To enable employees to use their existing identity with Google Cloud, you must federate Cloud Identity or G Suite with your external identity provider.

In this task, you create an identity that you can use to work in Google Cloud using G Suite, Cloud Identity, or a combination of the two:

- If you are a G Suite customer (that is, your company has corporate Gmail and other Google services), your G Suite user license lets you manage your Google Cloud resources.
- If you are not a G Suite customer, you may use Cloud Identity, which is an *identity as a service* (IDaaS) solution for centrally creating and managing the users and

groups who can access your cloud resources. (In a later task, you configure the resources that those users and groups can access.)

- Cloud Identity may be used with G Suite to provide licenses for users who do not require the more robust and costly features of G Suite.

You can also let employees use their existing identity and credentials to sign in to Google services by federating a Cloud Identity or G Suite account with an external identity provider (IdP).

You can learn about G Suite (https://gsuite.google.com/) and Cloud Identity (https://cloud.google.com/identity).

Each G Suite or Cloud Identity account is associated with exactly one organization. An organization is associated with exactly one domain, which is set when the organization resource is created. You must use an organization resource in Cloud Console to perform tasks later in this checklist.

The following section provides instructions for setting up both identity services.

Who performs this task

This task requires multiple people:

1. A person who will act as the identity administrator for Google Cloud for your company. You can give this access to a group of people later. If your company already uses a paid G Suite service, a person with G Suite Super Admin access must perform this step.
2. A person with access to the company's domain host, to see and edit domain settings such as DNS configurations.

What you do

- If you are a new customer, sign up for a Cloud Identity account, and verify your company's domain.
- If you are a G Suite customer, you can optionally enable Cloud Identity, and disable automatic G Suite licensing.

Why we recommend this task

You need either a Cloud Identity or a G Suite account in order to:

- Manage users and groups to control access to your cloud resources.
- Establish a Google Cloud organization.
- Create organizational controls and structure.

If you use G Suite, but some of your users don't need its robust features, you can save costs by providing these users with licenses via Cloud Identity.

Set up or confirm an identity account

New customersG Suite customers (#g-suite-...

Cloud Identity provides a paid, Premium edition as well as a free tier with a subset of Premium features. To compare the editions, see Compare Cloud Identity features and editions (https://support.google.com/cloudidentity/answer/7431902?hl=en). This checklist shows steps for the free edition, but you can choose to upgrade to the Premium edition at any time.

To complete this process, the domain that you want to use needs to be registered, and you need access to your domain settings through your domain host.

1. Create your Cloud Identity account and first admin user (https://gsuite.google.com/signup/gcpidentity/welcome#0).

   This starts a multi-page process where you specify your user and company information. In the last step of the process, provide a username. Cloud Identity adds `<username>@<your-domain>.com` as a Super Admin for Cloud Identity. Super Admin accounts can manage all aspects of your organization's account.

   When it asks you how you'll sign in, we recommend that you use the username `admin`.

2. Verify your domain (https://support.google.com/cloudidentity/answer/7331243). If you run into issues, see the Troubleshooting section (/docs/enterprise/onboarding-checklist#troubleshooting).

   When you're prompted to add users to your account, skip that process because you add users later on. To skip this step:

   a. Click the **Create users** button.

b. Select the **I have finished adding users for now** checkbox, and then click the **Next** button.

c. Click the **Continue to Cloud Console** button.

By default, the free edition of Cloud Identity provides 50 user licenses. This checklist requires you to set up 4 users. You can view existing licenses at the Google Admin console Billing page (https://admin.google.com/AdminHome#DomainSettings/subtab=subscriptions&notab=1) . If you need additional free licenses, you can request them by completing the following steps:

1. Sign in to Google Admin console (https://admin.google.com) with the Super Admin account that was created in the preceding procedure.
2. Go to the Your Cloud Identity free edition user cap (https://support.google.com/cloudidentity/answer/7295541?hl=en) page and follow the instructions for increasing the number of available licenses.

Troubleshooting

Unable to sign up my domain for a Google service

For more information about common problems and solutions, see Can't sign up my domain for a Google service (https://support.google.com/a/answer/80610?hl=en&ref_topic=1687139).

The Google account already exists

See 'Google Account already exists' error (https://support.google.com/a/answer/1275816) for a workaround.

□ 2. Add users and groups to your identity account

For this task, you create managed Google accounts for your administrator users.

Who performs this task

A person that will act as the identity administrator for Google Cloud for your company.

What you do

- Add users to your Cloud Identity account who will participate in the checklist tasks.
- Create a set of Google Groups.
- Add users to the Google Groups who will participate in the checklist tasks.

Why we recommend this task

Creating these user accounts and Google Groups are a requirement for assigning Identity and Access Management (IAM) roles in order to control access later.

Add initial users

For the purpose of this onboarding checklist, we recommend that you initially add users who will participate in the checklist tasks, such as administrators and decision makers involved with cloud setup practices. You can continue the rest of the checklist without adding all users. You create groups of users later in this task. After you've finished this checklist, you can scale to a larger number of users using one of the tools we will describe later.

1. Sign in to Google Admin console (https://admin.google.com) using the Super Admin account that was created when a Cloud Identity account was set up in task 1.
2. Add users using one of the following options:
   - Add several users at once (https://support.google.com/cloudidentity/answer/40057).
   - Add users individually (https://support.google.com/cloudidentity/answer/33310).

Create Google Groups

Next, you create a set of Google Groups. Google Groups enable you to quickly assign permissions to a group of Cloud Identity or G Suite users. You set permissions for the groups later in this checklist.

We recommend that you initially create the following Google Groups:

- `gcp-organization-admins`
- `gcp-network-admins`
- `gcp-security-admins`
- `gcp-billing-admins`
- `gcp-devops`
- `gcp-developers`

These groups will be essential in the setup process later when you start adding Google Cloud access permissions. For more information why we recommend these groups, see the Best practices for enterprise organizations (https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#groups-and-service-accounts) guide.

1. Open the Ways to create groups (https://support.google.com/cloudidentity/answer/33343) topic, select **In the Admin console**, and follow the instructions to create each of the recommended Google Groups.
2. Add users (https://support.google.com/cloudidentity/answer/6191469) to each Google Group. To be able to complete this checklist, you must add at least one user to each of the following groups:
    - `gcp-organization-admins`
    - `gcp-network-admins`
    - `gcp-billing-admins`
    - `gcp-devops`

★ **Note:** We recommend assigning at least two people to these administrative groups. Having multiple people in a group avoids having only a single point of contact for the group.

Assess existing consumer accounts

Assess (/architecture/identity/assessing-existing-user-accounts) whether some of your organization's employees are currently using consumer accounts to access Google services, and decide whether you want to migrate them to Cloud Identity or G Suite.

Automate user provisioning and enable single sign-on

If your organization already uses an identity provider such as Active Directory, Azure AD, Okta, or Ping Identity, then you can integrate Google Cloud with this external IdP by using federation (/architecture/identity/reference-architectures#using_an_external_idp):

- Federate Cloud Identity with Active Directory (/architecture/identity/federating-gcp-with-active-directory-introduction) to automatically provision users and enable single sign-on.
- Integrate with Azure Active Directory (/architecture/identity/federating-gcp-with-active-directory-introduction).
- Create a custom solution by using the G Suite Admin SDK (https://developers.google.com/admin-sdk/).

□ 3. Set up administrator access to your organization

In this task you set up administrator access for your organization, which gives the administrators central visibility and control over every cloud resource that belongs to your organization.

Who performs this task

If your company already uses a paid G Suite service, a person with G Suite Super Admin access must perform this step. If not, use the Cloud Identity account that was created in task 2.

What you do

- Verify that your organization was created.
- Assign administrative roles to the `gcp-organization-admins@<your-domain>.com` group that was created in task 2.

- Add administrative permissions to yourself, and to other administrators in your organization, so that you can perform later tasks in the checklist.

Why we recommend this task

For security reasons, you must explicitly define all administrative roles for your organization.

Verify that your organization was created

1. Log in to the Cloud Console using either your G Suite super administrator account, or using the Cloud Identity Super Admin account that you set up in task 1.
2. Go to the Identity & Organization (https://console.cloud.google.com/iam-admin/cloudidentity) page to finish creating the organization. After you go to the link, you might need to wait a few minutes for the process to complete.
3. Make sure that your organization name appears in the **Select an organization** list. It can take a few minutes for your organization to be created from the steps in task 1. If you don't see the organization name, wait a few minutes and then refresh the page.

Set up administrator access

Next, you assign administrative roles to the `gcp-organization-admins@<your-domain>.com` group that was created in task 2.

1. Complete the steps at Grant access (/iam/docs/granting-changing-revoking-access#grant_access), with the following changes:
   - After you open the IAM page in the Cloud Console, make sure that your organization name is selected in the organization list at the top of the page.
   - When you're asked to enter an email address, use `gcp-organization-admins@<your-domain>.com`.

- When you're asked to select a role, select **Resource Manager** > **Organization Administrator**.

2. After you've added the first role, click **Add another role** and then add the following additional roles for the `gcp-organization-admins@<your-domain>.com` member:

    - **Resource Manager** > **Folder Admin**
    - **Resource Manager** > **Project Creator**
    - **Billing** > **Billing Account User**
    - **Roles** > **Organization Role Administrator**
    - **Organization Policy** > **Organization Policy Administrator**
    - **Security Center** > **Security Center Admin**
    - **Support** > **Support Account Administrator**

3. When you're done adding roles, click **Save**.

□ 4. Set up billing

In this task, you set up a billing account to pay for Google Cloud resources, and you set administrator access for your billing accounts.

Who performs this task

This task requires multiple people:

1. A person in the `gcp-organization-admins@<your-domain>.com` group that was created in task 2.
2. A person in the `gcp-billing-admins@<your-domain>.com` group that was created in task 2.

What you do

- Assign administrative access to the `gcp-billing-admins@<your-domain>.com` group that was created in task 2.

- Choose and set up a billing account type, and a payment method.

Why we recommend this task

Cloud Billing (/billing/docs) accounts are linked to one or more Google Cloud projects and are used to pay for the resources you use, such as virtual machines, networking, and storage. IAM roles control access to Cloud Billing accounts.

Set up administrator access

Team members who are assigned the Billing Account Administrator IAM role can complete tasks such as managing payments and invoices, setting budgets, and associating projects with billing accounts. The role does not give team members permission to view the contents of the projects.

1. Make sure that you're logged in to the Cloud Console as a user in the `gcp-organization-admins` Google Group that was created in task 2.
2. Complete the steps at Grant access (/iam/docs/granting-changing-revoking-access#grant_access), with the following changes:
   - When you're asked to enter an email address, use `gcp-billing-admins@<your-domain>.com`.
   - When you're asked to select a role, select **Billing** > **Billing Account Administrator**.
   - After you've added the first role, click **Add another role** and then add the following additional roles for the `gcp-billing-admins@<your-domain>.com` member:
     - **Billing** > **Billing Account Creator**
     - **Resource Manager** > **Organization Viewer**

Set up the billing account

Next, you choose and set up a billing account type. There are two types of billing accounts:

- **Self-serve**. You sign up online using a credit or debit card, or ACH direct debit. Costs are charged automatically.
- **Invoiced**. You pay by check or wire transfer. Invoices are sent by mail or electronically.

For more information, including eligibility requirements for invoiced billing accounts, see Billing account types (/billing/docs/concepts#billing_account_types).

Self-serve accountsInvoiced accounts (#invoice…

1. Log in to the Cloud Console as a user in the `gcp-billing-admins` Google Group that was created in task 2.
2. Create a new billing account (/billing/docs/how-to/manage-billing-account#create_a_new_billing_account).
3. To verify that the billing account was created, go to the Billing page (https://console.cloud.google.com/billing), and then select your organization in the **Select an organization** list. If the billing account was successful, you see it in the list.

□ 5. Set up the resource hierarchy

In this task, you create a basic structure for *folders* and *projects* in your resource hierarch

- Folders (/resource-manager/docs/cloud-platform-resource-hierarchy#folders) provide a grouping mechanism and isolation boundaries between projects. For example, they can represent the main departments in your organization such as finance or retail, c environments such as production versus non-production.
- Projects (/resource-manager/docs/cloud-platform-resource-hierarchy#projects) contain yo cloud resources, such as virtual machines, databases, and storage buckets. For bes practices related to projects, see Specify your project structure (/docs/enterprise/best-practices-for-enterprise-organizations#project-structure).

You can set IAM policies to control access at different levels of the resource hierarchy. Yc will set these policies as a later task in this checklist.

Who performs this task

A person in the `gcp-organization-admins@<your-domain>.com` group that was created in task 2.

What you do

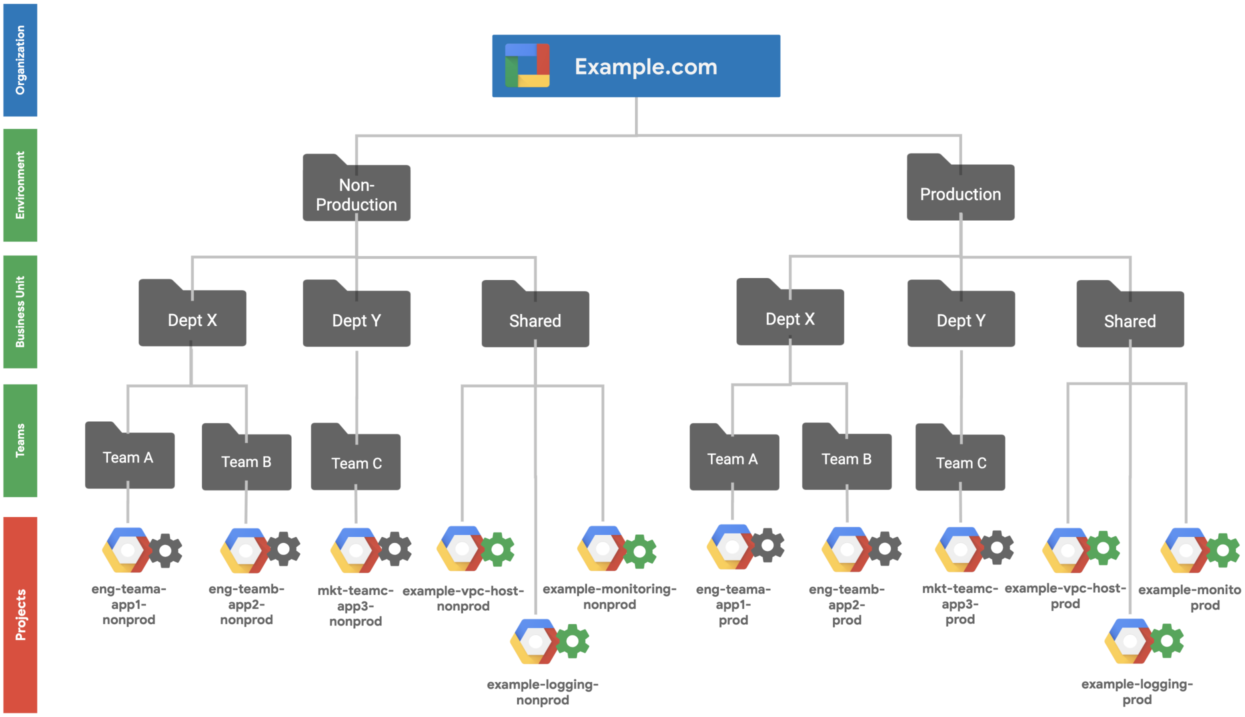
Create the initial hierarchy structure with folders and projects.

Why we recommend this task

Creating the structure is a requirement for a later task where you set IAM policies in order control access at different levels of the resource hierarchy.

Resource hierarchy diagram

There are many ways to create your resource hierarchy. The following diagram shows a typical example.



In the example, the organization resource hierarchy contains three levels of folders:

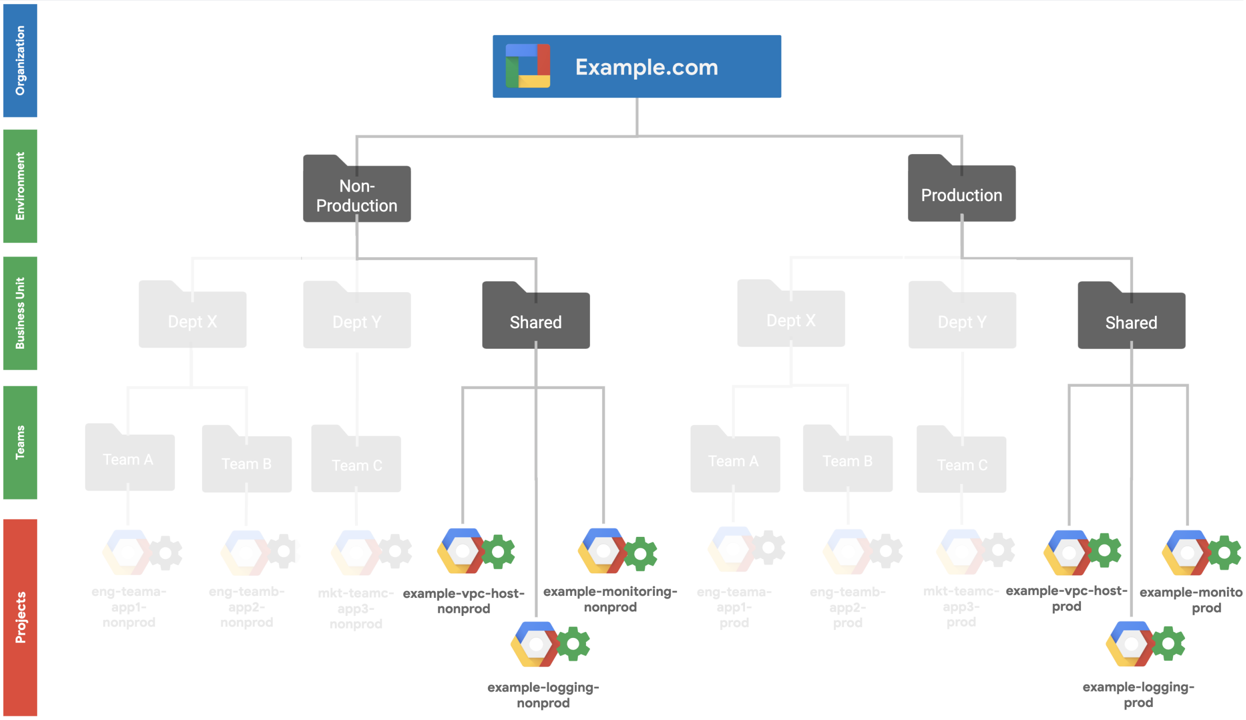
- Environment (non-production and production). By isolating environments from eacl other, you can better control access to production environments and avoid non-production changes accidentally impacting production.

- Business units. In the diagram, these are represented by `Dept X` and `Dept Y`, which might be business units such as Engineering and Marketing, and a `Shared` folder th has projects that contain resources shared across the hierarchy, such as networkin logging, and monitoring.

- Teams. In the diagram, these are represented by `Team A`, `Team B`, and `Team C`, which might be teams like Development, Data Science, QA, and so on.

Create the initial resource hierarchy

In these checklist steps, you create basic folders and projects for your initial setup, as shown in the following diagram. These folders and projects are used in the remaining tasks of the checklist. Later on, you can build on this hierarchy to mirror your organizatio and customize it to your company's needs as you grow your workloads on Google Cloud.



1. Make sure that you're logged in to the Cloud Console as a user in the `gcp-organization-admins` Google Group that was created in task 2.

2. Create folders (/resource-manager/docs/creating-managing-folders#creating-folders). Follo the procedure four times to create the following folders:

   a. `Production`

   b. `Non-Production`

c. `Shared`, using `Production` as a parent folder

d. `Shared`, using `Non-Production` as a parent folder

Next, you create projects. Following the principle of separating production and non-production environments, for this checklist you need to create the following projects:

- `example-vpc-host-nonprod`. This project is used to help connect non-production resources from multiple projects to a common VPC network.
- `example-vpc-host-prod`. This project is used to help connect production resources from multiple projects to a common VPC network.
- `example-monitoring-nonprod`. This project is used to host non-production monitori resources.
- `example-monitoring-prod`. This project is used to host production monitoring resources.
- `example-logging-nonprod`. This project is used to host exported log data from your non-production environment.
- `example-logging-prod`. This project is used to host exported log data from your production environment.

Project names are limited to 30 characters. Typically, you would use your own company name in place of `example`, as long as you can do so within the 30-character limit. When y create projects in the resource hierarchy in the future, we recommend using a naming convention such as `<business unit name>-<team name>-<application name>-<environment>`, according to the resource hierarchy of your organization.

To create the projects:

1. In the Cloud Console, go to the **Manage resources** page:

   Go to the Manage resources page (https://console.cloud.google.com/cloud-resource-manag

2. Click **Create Project**.
3. In the **New Project** window, enter one of the project names listed earlier.
4. If you're prompted to select a billing account, select the billing account you want to use for this checklist.

5. For **Location**, click **Browse** and then set the location as follows:
   - If the name of the project you're creating ends with `prod`, select **Production** > **Shared**.
   - If the name of the project you're creating ends with `nonprod`, select **Non-Production** > **Shared**.
6. Click **Create**.
7. Repeat steps 2 through 6 for each of the recommended projects.

□ 6. Set up access control for your resource hierarchy

In this task, you set up access control for your resource hierarchy by adding IAM policies (/iam/docs/overview#iam_policy) to the resources. An IAM policy is a collection of statemen that define who has what type of access. A policy is attached to a resource and is used t enforce access control whenever that resource is accessed.

To set permissions, you perform the same basic procedure, but you do it for resources at different levels of the hierarchy (organization, folders, and projects). We recommend that you use the principle of least privilege and grant the least amount of access that's necessary to resources in each level. The roles that we recommend in the following procedures help you enforce the principle of least privilege.

Who performs this task

A person in the `gcp-organization-admins@<your-domain>.com` group that was created in task 2.

What you do

Set IAM policies on the organization, folder, and project level.

Why we recommend this task

Setting IAM policies across your resource hierarchy lets you scalably control access to yo cloud resources.

Set IAM policies at the organization level

Policies that you set at the organization level apply to all folders and projects in the organization. The following table lists the members and the roles that you assign to them at the organization level. The steps for how to perform this procedure are listed after the table.

Member	Roles to grant
`gcp-network-admins@<your-domain>.com`	• **Compute Engine** > **Compute Network Admin**. This grants permissions to create, modify, and delete networking resources, except for firewall rules and SSL certificates. • **Compute Engine** > **Compute Shared VPC Admin**. This grants permissions to administer Shared VPC host projects. • **Compute Engine** > **Compute Security Admin**. This grants permissions to create, modify, and delete firewall rules and SSL certificates. • **Resource Manager** > **Folder Viewer**. This grants permissions to vie folders.

Member	Roles to grant
`gcp-security-admins@<your-domain>.com`	• **Organization Policy** > **Organization Policy Admin**. This grants permissions to set organization-level IAM policies. • **Organization Policy** > **Organization Policy Viewer**. This grants permissions to view the IAM policies that apply to the organization • **IAM** > **Security Reviewer**. This grants permissions to view all resources for the organization, and to view the IAM policies that apply to them. • **Roles** > **Organization Role Viewer**. This grants permissions to view all custom IAM roles in the organization, and to view the projects th they apply to. • **Security Center** > **Security Center Admin**. This grants administrato access to the security command center. • **Resource Manager** > **Folder IAM Admin**. This grants permissions t set folder-level IAM policies. • **Logging** > **Private Logs Viewer**. This grants read-only access to Cloud Logging features, including the ability to read private logs. • **Logging** > **Logs Configuration Writer**. This grants permissions to create logs-based metrics and export sinks. • **Kubernetes Engine** > **Kubernetes Engine Viewer**. This grants read only access to Google Kubernetes Engine resources. • **Compute Engine** > **Compute Viewer**. This grants read-only access Compute Engine resources. • **BigQuery** > **BigQuery Data Viewer**. This grants permissions for BigQuery datasets.
`gcp-devops@<your-domain>.com`	**Resource Manager** > **Folder Viewer**. This grants permissions to view folders.

1. Make sure that you're logged in to the Cloud Console as a user in the `gcp-organization-admins` Google Group that was created in task 2.
2. Go to the **Manage resources** page in the Cloud Console:

   Go to the Manage resources page (https://console.cloud.google.com/cloud-resource-manag

3. Select your organization from the organization tree grid.

4. If the **Info Panel** pane on the right is hidden, click **Show Info Panel** in the top right corner.
5. Select the checkbox for the organization.
6. In the **Info Panel** pane, in the **Permissions** tab, click **Add Member**.
7. In the **New members** field, enter the name of a member from the table. For exampl start by entering `gcp-network-admins@<your-domain>.com`, as listed in the precedin table.
8. In the **Select a role** list, select the first role for that member as listed in the table. Fo example, for the first member, the first role that you select is **Compute Engine** > **Compute Network Admin**.
9. Click **Add another role**, and then add the next role for that member.
10. Add the next role for that member.
11. When you've added all the roles for a member, click **Save**.
12. Repeat step 2 through 7 for the other members listed in the table.

Set IAM policies at the folder level

Policies set on the folder level also apply to projects in the folders. The procedure is simil to what you did for your organization, except that you select a different level in the hierarchy.

1. Clear the checkbox for the organization and for any other resource that is selected.
2. Select the checkbox for the `Production` folder.
3. In the **Info Panel** pane, in the **Permissions** tab, click **Add Member**.
4. In the **New members** field, enter `gcp-devops@<your-domain>.com`.
5. Using the same steps you used for adding roles to organization members, add the following roles to the `gcp-devops@<your-domain>.com` member:
    - **Logging** > **Logging Admin**. This grants full permissions to Cloud Logging.
    - **Error Reporting** > **Error Reporting Admin**. This grants full permissions to erro reporting data.

  - **Service Management** > **Quota Administrator**. This grants access to administ service quotas.
  - **Monitoring** > **Monitoring Admin**. This grants full permissions to monitoring data.
  - **Compute Engine** > **Compute Admin**. This grants full permissions to Compute Engine resources.
  - **Kubernetes Engine** > **Kubernetes Engine Admin**. This grants full permissions to Google Kubernetes Engine container clusters.

6. When you've finished adding roles, click **Save**.
7. Clear the checkbox for the `Production` folder.
8. Select the checkbox for the `Non-Production` folder.
9. Add `gcp-developers@<your-domain>.com` as a new member.
10. Assign the following IAM roles to the `gcp-developers@<your-domain>.com` member:
    - **Compute Engine** > **Compute Admin**. This grants full permissions to Compute Engine resources.
    - **Kubernetes Engine** > **Kubernetes Engine Admin**. This grants full permissions to Google Kubernetes Engine container clusters.

Set IAM policies at the project level

Policies that you set at the project level apply only to the projects they are applied to. This lets you set fine-grained permissions for individual projects.

1. Clear the checkbox for any folders and for any other resource that has been selecte
2. Select the checkboxes for the following projects:
    - `example-vpc-host-nonprod`
    - `example-vpc-host-prod`
3. Add `gcp-network-admins@<your-domain>.com` as a member.
4. Assign the following role to the `gcp-network-admins@<your-domain>.com` member:

   - **Project** > **Owner**. This grants full permissions to all resources in the selected projects.

5. Click **Save**.
6. Clear the checkboxes for the selected projects.
7. Select the checkboxes for the following projects:
   - `example-monitoring-nonprod`
   - `example-monitoring-prod`
   - `example-logging-nonprod`
   - `example-logging-prod`
8. Add `gcp-devops@<your-domain>.com` as a new member.
9. Assign the following role to the `gcp-devops@<your-domain>.com` member:
   - **Project** > **Owner**. This grants full permissions to all resources in the selected projects.
10. Click **Save**.

□ 7. Set up support

In this task, you can choose a support option.

Who performs this task

A person in the `gcp-organization-admins@<your-domain>.com` group that was created in task 2.

What you do

Choose a support plan based on your company's needs.

Why we recommend this task

A premium support plan provides you with business-critical support to quickly resolve issues with help from experts at Google.

Choose a support option

Every Google Cloud customer automatically gets free support that includes support produ documentation (/support/docs/best-practice), community support (/support/docs/community) and support for billing issues (/support/billing). However, we recommend that enterprise customers sign up for a premium support plan, which offers one-on-one technical suppor with Google support engineers. For more information, you can compare support plans (/support#support-plans).

1. Read about the support plans (/support#support-plans) and decide which plan you wa You set up the support plan in a later step. If you decide to stay with free support options, you can continue to the next task.
2. Make sure that you're logged in to the Cloud Console as a user in the `gcp-organization-admins` Google Group that was created in task 2.
3. Set up the support plan.
   - To request Premium Support, contact your Google sales representative. If you don't have a representative, contact sales (/docs/enterprise/support/upgrade).
   - To enable Role-Based Support, go to the **Enable Role-Based Support** page in Google Cloud Console and follow the on-screen prompts to complete the required steps.

     Go to the Enable Role-Based Support page (https://console.cloud.google.com/suppor
4. Follow the instructions at Support user roles (/support/docs/role-based-support#support_user_roles) to assign the **Support User** and **Org Viewer** roles to each user who needs to interact with Google Cloud Support.

☐ 8. Set up your networking configuration

In this task, you set up your initial networking configuration. Typically, you need to do the following:

- Design, create, and configure a virtual private cloud architecture.

- If you have on-premises networking, or networking in another cloud provider, config connectivity between that provider and Google Cloud.
- Set up a path for external egress traffic.
- Implement network security controls, such as firewall rules.
- Choose a preferred ingress traffic option for services that are hosted on the cloud.

This task shows you an example for item 1 as a basis for your own virtual private cloud architecture.

The remaining items—external connectivity, egress traffic configuration, implementing firewall rules, and choosing an ingress option—are dependent on your business needs. Therefore, we don't cover those in this checklist. However, we provide links to additional information for these items.

Who performs this task

A person in the `gcp-network-admins@<your-domain>.com` group that was created in task 2

What you do

Set up an initial networking configuration.

- Create Shared VPC networks
- Configure connectivity between the external provider and Google Cloud
- Set up a path for external egress traffic
- Implement network security controls
- Choose an ingress traffic option

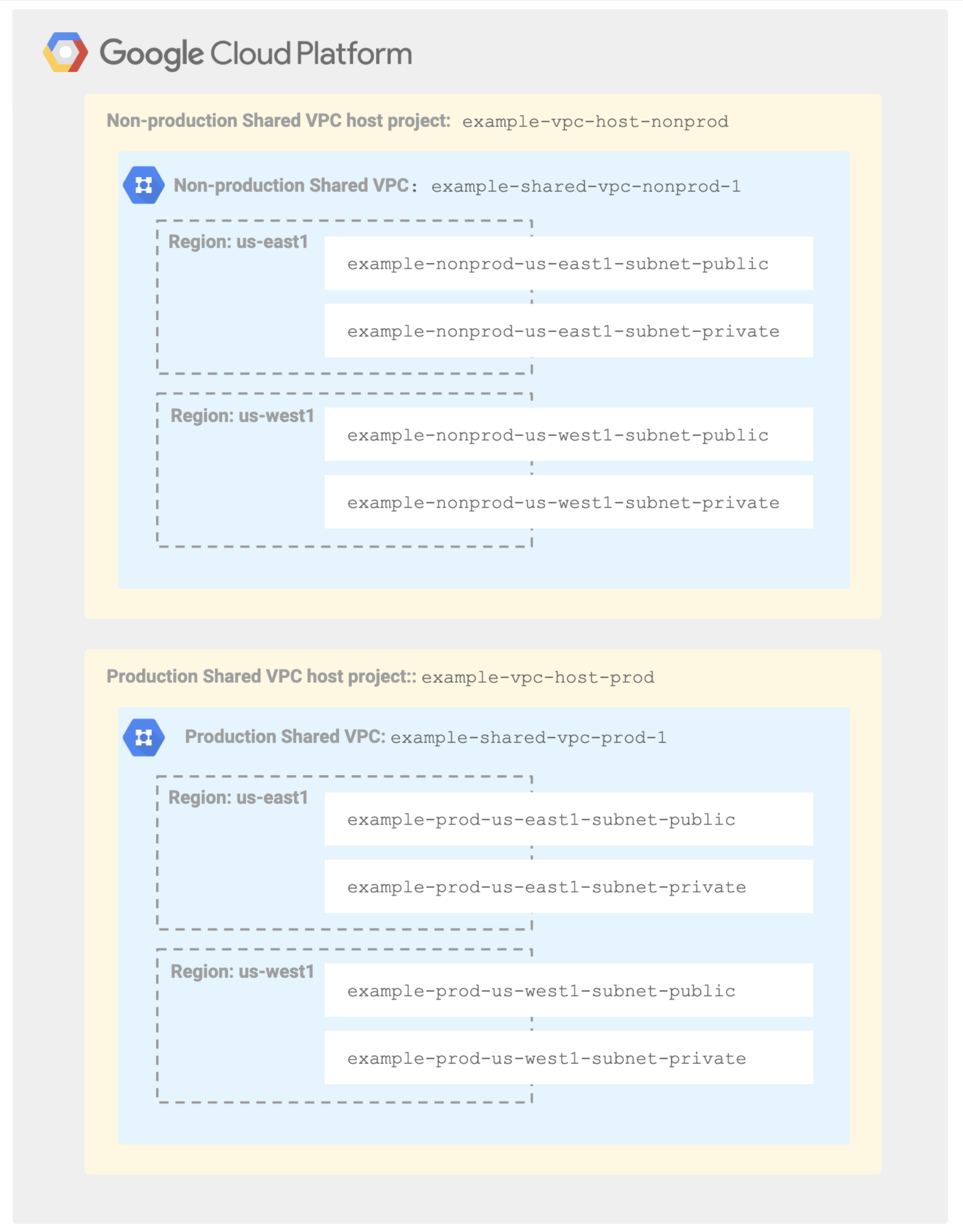
Why we recommend this task

- Shared VPC allows separate teams to connect to a common, centrally-managed VP network from multiple distinct products.
- Configuring hybrid connectivity allows seamless migration of applications to Goog Cloud while still connecting to service dependencies.

- Designing secure ingress and egress pathways from the start enables your teams t productively work in Google Cloud without compromising security.

Virtual private cloud architecture

Google offers Virtual Private Cloud (VPC), which provides networking functionality to you Google Cloud resources such as Compute Engine virtual machine instances, GKE containers, and App Engine flexible environment. The following diagram shows a basic multi-regional architecture:


Google Cloud Platform
Non-production Shared VPC host project: example-vpc-host-nonprod
Non-production Shared VPC: example-shared-vpc-nonprod-1
Region: us-east1
example-nonprod-us-east1-subnet-public
example-nonprod-us-east1-subnet-private
Region: us-west1
example-nonprod-us-west1-subnet-public
example-nonprod-us-west1-subnet-private
Production Shared VPC host project:: example-vpc-host-prod
Production Shared VPC: example-shared-vpc-prod-1
Region: us-east1
example-prod-us-east1-subnet-public
example-prod-us-east1-subnet-private
Region: us-west1
example-prod-us-west1-subnet-public
example-prod-us-west1-subnet-private

This architecture has two Shared VPC host projects. One host project is for your producti environment, and the other is for your non-production environment. Shared VPC allows organizations to connect resources from multiple projects to a common VPC network, so that the resources can communicate with each other more securely and efficiently using internal IP addresses from that network.

A Shared VPC host project contains one or more Shared VPC networks. In this architectur each Shared VPC network (both production and non-production) contains public and priv subnets across two regions (in this case, `us-east1` and `us-west1`):

- The public subnet can be used for instances that are internet-facing to provide external connectivity.
- The private subnet can be used for instances that are solely internal-facing and sho not be allocated public IP addresses.

The architecture that's shown in the preceding diagram uses example names for various resources. For your own setup, you might change elements of the name, such as your company (`example` in the example names) and the region you're using (`us-east1` and `us-west1` in the examples).

Create the Shared VPC networks

1. In the project selector page, select `example-vpc-host-nonprod`:

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

2. Follow the instructions at Deleting a network (/vpc/docs/using-vpc#deleting_a_network) delete the VPC network named `default`.
3. Follow the instructions to Create a custom mode network (/vpc/docs/using-vpc#create-custom-network) using the following values:

   a. For **Name**, enter `example-shared-vpc-nonprod-1`.

   b. For the **New subnet** section parameters:

   - For **Name**, enter `example-nonprod-us-east1-subnet-public`.
   - For **Private Google access**, select **On** to enable VMs to communicate wi Google APIs without an external IP address.

   c. Choose **Add subnet**, and follow the instructions for adding the following subr names:

      - `example-nonprod-us-east1-subnet-private`
      - `example-nonprod-us-west1-subnet-public`
      - `example-nonprod-us-west1-subnet-private`

4. Enable the Shared VPC host project (/vpc/docs/provisioning-shared-vpc#enable-shared-vpc-host), using the following values:

   a. For the project, select `example-vpc-host-nonprod`.

   b. Under **Select subnets**, click **Individual subnets (subnet-level permissions)** an select all of the non-production subnets that you created earlier.

   c. In **Attach service projects**, attach all of the remaining monitoring and logging non-production projects.

5. In the project selector page, select `example-vpc-host-prod`:

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

6. Repeat steps 2 through 4 for the production environment. Make sure that you selec of the previously created production subnets.

Configure connectivity between the external provider and Google Cloud

If you have on-premises networking, or networking in another cloud provider, you can set Cloud VPN, a service that helps securely connect your peer network to your Google Cloud VPC network through an IPSec VPN connection. Cloud VPN is suitable for speeds up to 3 Gbps. If you need higher bandwidth to connect your on-premises system to Google Clouc see Partner Interconnect (/network-connectivity/docs/interconnect/partners) and Dedicated Interconnect (/network-connectivity/docs/interconnect/concepts/dedicated-overview).

To create a VPN connection, follow the instructions at Creating a gateway and tunnel (/network-connectivity/docs/vpn/how-to/creating-vpn-dynamic-routes#creating_a_gateway_and_tunnel) for both the production and non-production Shared VPC networks that was created in the previous procedure.

Set up a path for external egress traffic

You use Cloud NAT to allow your VMs to connect to the internet without using external IP addresses. Cloud NAT is a regional resource. You can configure it to allow traffic from all primary and secondary IP ranges of subnets in a region, or you can configure it to apply t only some of those ranges.

Follow the instructions at Create NAT (/nat/docs/using-nat#create_nat) for all regions in the Shared VPC networks that was created in the previous procedure for both production anc non-production networks.

Implement network security controls

Firewall rules let you allow or deny traffic to and from your virtual machine (VM) instance based on a configuration that you specify. Follow the instructions at Using firewall rules (/vpc/docs/using-firewalls)to configure these controls for both production and non-producti Shared VPC networks that was created in the previous procedure.

Choose an ingress traffic option

Cloud Load Balancing gives you the ability to distribute compute resources in single or multiple regions. This lets you meet your high-availability requirements both for incominc external traffic and for traffic within your VPC network. As you plan your application architecture on Google Cloud, review Choosing a Load Balancer (/load-balancing/docs/choosing-load-balancer) to decide which types of load balancers you need.

□ 9. Set up logging and monitoring

In this task, you set up basic logging and monitoring features using Cloud Logging and Cloud Monitoring.

Who performs this task

A person in the `gcp-devops@<your-domain>.com` group that was created in task 2.

What you do

Set up basic logging and monitoring features using Cloud Logging and Cloud Monitoring.

Why we recommend this task

Comprehensive logging and monitoring is key to maintaining observability in your cloud environment. Configuring appropriate logging retention from the start allows you to build and have confidence that an audit trail is preserved, while setting up centralized monitoring will give your team a central dashboard for viewing your environments.

Set up monitoring

Cloud Monitoring (/monitoring) collects metrics, events, and metadata from Google Cloud services, hosted uptime probes, application instrumentation, and other common application components.

1. Make sure that you're logged in to the Cloud Console as a user in the `gcp-devops` group that was created in task 2.
2. Create a Workspace for Monitoring (/monitoring/workspaces/manage#single-project-ws) using a host project. The first monitored Google Cloud project in a Workspace is the host project; you should make sure that you choose the right project to act as the host project. When the steps prompt you to select a project, select the non-production monitoring project (`example-monitoring-nonprod`) that was created in task 5.
3. Add other projects (/monitoring/workspaces/manage#multi-project-ws) that you want to monitor from this Workspace. For example, add all of the other non-production projects.
4. Repeat this procedure for your production projects. Use `example-monitoring-prod` as the Workspace project, and add the production projects to monitor.

Set up logging

Cloud Logging allows you to store, search, analyze, monitor, and alert on log data and events from Google Cloud and Amazon Web Services (AWS). Cloud Logging also allows you to ingest custom log data from any source, and to export logs to external data sinks.

1. Make sure that you're logged in to the Cloud Console as a user in the `gcp-devops` group that was created in task 2.
2. Enable logging export for BigQuery (/solutions/exporting-stackdriver-logging-for-security-and-access-analytics#set_up_the_logging_export) , using the following values:
    - Select the `example-logging-nonprod` project.
    - Create a BigQuery dataset (/bigquery/docs/datasets#create-dataset). For **Dataset ID**, use a name like `example_logging_export_nonprod`.
    - After you've named the dataset, click **Create dataset**.
3. Repeat the previous step for the `example-logging-prod` project, but use `example_logging_export_prod` for the dataset ID.
4. Review the logs retention periods (/logging/quotas#logs_retention_periods) to determine whether they meet your compliance requirements. If they don't, set up log export to Cloud Storage (/solutions/exporting-stackdriver-logging-for-compliance-requirements), which can be helpful for long-term retention.

□ 10. Configure organizational security settings

In this task, you configure Google Cloud products to help protect your organization. Google Cloud provides many security offerings (/security/products).

★ **Note:** The security settings that you make for this task are just a first step in configuring security. Every deployment presents unique challenges, and it's up to you to perform security audits, understand the attack surface for your system, and so on.

Who performs this task

A person in the `gcp-organization-admins@<your-domain>.com` group that was created in task 2.

What you do

- Enable the Security Command Center dashboard
- Set up Organization Policy

Why we recommend this task

We recommend setting up the following two products:

- Security Command Center (/security-command-center). This comprehensive security management and data risk platform enables you to monitor your cloud assets, scan storage systems for sensitive data, detect common web vulnerabilities, and review access rights to critical resources.
- Organization Policy Service (/resource-manager/docs/organization-policy/overview). This service gives you centralized and programmatic control over your organization's cloud resources.

Set up the products

1. Make sure that you're logged in to the Cloud Console as a user in the `gcp-organization-admins` group that was created in task 2.
2. Enable the Security Command Center dashboard (/security-command-center/docs/quickstart-scc-setup#enable-dashboard).
3. Set up Organization Policy by following the steps at Customizing policies for boolean constraints (/resource-manager/docs/organization-policy/creating-managing-policies#boolean_constraints)
   , with the following details:
   a. Set the **Skip default network creation** constraint with the following changes:
      - When you're asked to select a project, folder, or organization, select your organization.
      - When you're asked to select a constraint from the list on the **Organization policies** page, select **Skip default network creation**.

- When you're asked to select an enforcement option, select **On**.

b. Set up the **Domain restricted sharing** constraint (/resource-manager/docs/organization-policy/restricting-domains#setting_the_organization_policy)
.

c. Disable external IP address access for VM instances (/compute/docs/configure-ip-addresses#disableexternalip).

★ **Note:** If you need VMs that have external access but don't expose public IP addresses, configure Cloud NAT as explained in task 8.

Last updated 2020-08-20 UTC.