Networking Products (https://cloud.google.com/products/networking/)
Virtual Private Cloud (https://cloud.google.com/vpc/)
Documentation (https://cloud.google.com/vpc/docs/) Guides

Provisioning Shared VPC

Shared VPC allows you to export subnets from a VPC network (https://cloud.google.com/vpc/docs/vpc) in a *host project* to other *service projects* in the same organization (https://cloud.google.com/resource-manager/docs/creating-managing-organization). Instances in the service projects can have network connections in the shared subnets of the host project. This page describes how to set up and use Shared VPC, including some necessary administrative preparation for your organization.

Note: Shared VPC is also referred to as "XPN" in the API and command-line interface.

Quotas, limits, and eligible resources

Please make sure you are familiar with the Shared VPC Overview (https://cloud.google.com/vpc/docs/shared-vpc) and the IAM Overview (https://cloud.google.com/iam/docs/overview) before you begin. Specifically:

- Make note of the quotas and limits (https://cloud.google.com/vpc/docs/quota#shared-vpc) that pertain to Shared VPC.
- Be sure to understand which resources can participate (https://cloud.google.com/vpc/docs/shared-vpc#resources_that_can_be_attached_to_shared_vpc_networks_from_a_service_project) and which resources cannot participate (https://cloud.google.com/vpc/docs/shared-vpc#ineligible_resources).
- Ensure that you have enabled the Compute Engine API and billing for your host project and all service projects that you plan to attach to the host project.

Prepare your organization

Administrators and IAM

Preparing your organization, setting up Shared VPC host projects, and using Shared VPC networks involves a minimum of three different administrative IAM roles. For more details about each role and information about optional ones, see the administrators and IAM (https://cloud.google.com/vpc/docs/shared-vpc#iam_in_shared_vpc) section of the Shared VPC overview.

Important: The Network User and Network Admin roles are different. Refer to the Network and Security Admins (https://cloud.google.com/vpc/docs/shared-vpc#net_and_security_admins) section of the Shared VPC overview for details.

Organization policies for Shared VPC

Organization policy constraints can protect Shared VPC resources at the project, folder, or organization level. The following sections describe each policy.

Prevent accidental deletion of host projects

The accidental deletion of a host project would lead to outages in all service projects attached to it. When a project is configured to be a Shared VPC host project, a special lock - called a *lien* - is placed upon it. As long as the lien is present, it prevents the project from being deleted accidentally. The lien is automatically removed from the host project when it is no longer configured for Shared VPC.

Caution: By default, a project owner can remove a lien from a project, including a Shared VPC host project, unless an organization-level policy is defined to limit lien removal. (Specifically, lien removal requires an IAM member with the `resourcemanager.projects.get` and `resourcemanager.projects.updateLiens` permissions on the project.) The project owner for the host project could remove the lien then delete the Shared VPC project. To prevent this from happening, follow the directions in this section.

An Organization Admin or other user with the `orgpolicy.policyAdmin` role can define an organization-level policy to limit the removal of liens to just organization owners and other users with the `resourcemanager.lienModifier` role. This effectively prevents a project owner who is not an organization owner and who does not have the `resourcemanager.lienModifier` role from being able to accidentally delete a Shared VPC host project. For more information about the permissions associated with the `resourcemanager.lienModifier` role, refer to Placing a lien on a project

(https://cloud.google.com/resource-manager/docs/project-liens#placing_a_lien_on_a_project) in the Resource Manager documentation.

Because an organization policy applies to all projects in the organization, you only need to follow these steps once to restrict lien removal.

1. Authenticate to `gcloud` as an Organization Admin or IAM member with the `orgpolicy.policyAdmin` role. Replace ***ORG_ADMIN*** with the name of an Organization Admin:

```
gcloud auth login ORG_ADMIN
```

2. Determine your organization ID number by looking at the output of this command.

```
gcloud organizations list
```

3. Enforce the `compute.restrictXpnProjectLienRemoval` policy for your organization by running this command. Replace ***ORG_ID*** with the number you determined from the previous step.

```
gcloud beta resource-manager org-policies enable-enforce \
    --organization ORG_ID compute.restrictXpnProjectLienRemoval
```

4. Log out of `gcloud` if you are finished performing tasks as an Organization Admin to protect your account.

```
gcloud auth revoke ORG_ADMIN
```

Constrain host project attachments

By default, a Shared VPC Admin can attach a non-host to any host project in the same organization. An organization policy administrator can limit the set of hosts projects to which a non-host project or non-host projects in a folder or organization can be attached. For more information, refer to the `constraints/compute.restrictSharedVpcHostProject` (https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints) constraint.

Constrain which subnets in the host project that a service project can use

By default, after you configure Shared VPC, IAM members in service projects can use any subnet the host project if they have the appropriate IAM permissions (https://cloud.google.com/vpc/docs/shared-vpc#svc_proj_admins). In addition to managing individual user permissions, an organization policy administrator can set a policy to define the set of subnets that can be accessed by a particular project or by projects in a folder or organization. For more information, refer to the `constraints/compute.restrictSharedVpcSubnetworks` (https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints) constraint.

Nominate Shared VPC Admins

Beta

This product or feature is in a pre-release state and might change or have limited support. For more information, see the product launch stages (https://cloud.google.com/products/#product-launch-stages).

An Organization Admin can grant one or more IAM members the **Shared VPC Admin** (https://cloud.google.com/iam/docs/understanding-roles#compute.xpnAdmin) and **Project IAM Admin** (https://cloud.google.com/iam/docs/understanding-roles#resourcemanager.projectIamAdmin) roles. The Project IAM Admin role grants Shared VPC Admins permission to share all existing and future subnets, not just individual subnets. This grant creates a binding at the organization or folder level, not the project level. So the IAM members must be defined in the organization, not just a project therein.

CONSOLE GCLOUD API

To grant the Shared VPC Admin role at the organization level

1. Log into the Google Cloud Console as an Organization Admin, then go to the IAM page.
   GO TO THE IAM PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/IAM-ADMIN/IAM/ORGANIZATION
2. From the project menu, select your organization.
   If you select a project, you will not see the correct entries in the **Roles** menu.
3. Click **Add**.
4. Enter the email addresses of the **Members**.
5. In the **Roles** drop down, select **Compute Engine** > **Compute Shared VPC Admin**.

★ **Note:** If you do not see the **Compute Shared VPC Admin** role as an option, you might not be logged in to the Google Cloud Console as an Organization Admin, or you might have selected a project

instead of the whole organization.

6. Click **Add another role**.
7. In the **Roles** drop down, select **Resource Manager** > **Project IAM Admin**.
8. Click **Save**.

To grant the Shared VPC Admin role at the folder level

1. Log into the Google Cloud Console as an Organization Admin, then go to the IAM page.
   GO TO THE IAM PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/IAM-ADMIN/IAM/ORGANIZATION
2. From the project menu, select your folder.
   If you select a project or organization, you will not see the correct options.
3. On the **Members** page, click **Add**.
4. Enter the email addresses of the **New members**.
5. Under **Select a role**, select **Compute Engine** > **Compute Shared VPC Admin**.
6. Click **Add another role**.
7. In the **Roles** drop down, select **Resource Manager** > **Project IAM Admin**.
8. Click **Save**.

Setting up Shared VPC

All tasks in this section must be performed by a Shared VPC Admin.

Enable a host project

Beta

This product or feature is in a pre-release state and might change or have limited support. For more information, see the product launch stages (https://cloud.google.com/products/#product-launch-stages).

Within an organization, Shared VPC Admins can designate projects as Shared VPC *host projects*, subject to quotas and limits (https://cloud.google.com/vpc/docs/quota#shared-vpc), by following this procedure. Shared VPC Admins can also create and delete projects if they have the `resourcemanager.projectCreator` and `resourcemanager.projectDeleter` roles

(https://cloud.google.com/iam/docs/understanding-roles#resource-manager-roles) for your organization.

Note: The Compute Engine API (https://console.cloud.google.com/apis/api/compute_component/overview) must be enabled for the project becoming the Shared VPC host project **and** for any service projects that will attach to it. For more information, please refer to the Compute Engine API documentation (https://cloud.google.com/compute/docs/reference/rest/v1/).

Caution: Shared VPC host projects are protected with a lien to prevent accidental project deletion. This lien remains in effect as long as the project is a host project; **however, the lien can be manually removed**. We recommend that an Organization Admin define an organization-level policy (#protectsharedvpc) to limit the users who can manually remove liens.

CONSOLE GCLOUD API

Note: If you have Shared VPC Admin role at the folder level, you need to use `gcloud beta` or the beta API.

1. Go to the Shared VPC page in the Google Cloud Console.
   GO TO THE SHARED VPC PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/NETWORKING/XPN/DET
2. Log in as a Shared VPC Admin.
3. Select the project you want to enable as a Shared VPC host project from the project picker.
4. Click **Set up Shared VPC**.
5. On the next page, click **Save & continue** under **Enable host project**.
6. Under **Select subnets**, do one of the following:
   a. Click **Share all subnets (project-level permissions)** if you need to share all current and future subnets in the VPC networks of the host project with service projects and Service Project Admins specified in the next steps.
   b. Click **Individual subnets (subnet-level permissions)** if you need to selectively share subnets from the VPC networks of the host project with service projects and Service Project Admins. Then, select **Subnets to share**.
7. Click **Continue**.
   The next screen is displayed.
8. In **Project names**, specify the *service projects* to attach to the host project. Note that attaching service projects does not define any Service Project Admins; that is done in the next step.

9. In the **Select users by role** section, add Service Project Admins. These users will be granted the IAM role of `compute.networkUser` for the shared subnets. Only Service Project Admins can create resources in the subnets of the Shared VPC host project.
10. Click **Save**.

Attach service projects

A service project must attach to a host project before its Service Project Admins can use the Shared VPC. A Shared VPC Admin must perform the following steps to complete the attachment.

A service project can only attach to one host project, but a host project supports multiple service project attachments. Refer to limits specific to Shared VPC (https://cloud.google.com/vpc/docs/quota#shared-vpc) on the VPC quotas page for details.

Note: Before you can attach to a host project, you must enable the Compute Engine API (https://console.cloud.google.com/apis/api/compute_component/overview) for the service project.

CONSOLE GCLOUD API

Note: If you used the Console to enable a host project (#enable-shared-vpc-host), you already attached one or more service projects to it. The following directions detail how to modify the configuration of an existing host project.

Note: If you have Shared VPC Admin role at the folder level, you need to use `gcloud beta` or beta API.

1. Log into the Google Cloud Console as a Shared VPC Admin.
2. Go to the Shared VPC page in the Google Cloud Console.
   GO TO THE SHARED VPC PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/NETWORKING/XPN/DET
3. Click the **Attached projects** tab.
4. Under the **Attached projects** tab, click the **Attach projects** button.
5. Check the boxes for the service projects to attach in the **Project names** section. Note that attaching service projects does not define any Service Project Admins; that is done in the next step.
6. In the **VPC network permissions** section, select the roles whose members will get the `compute.networkUser` role. Cloud IAM members are granted the Network User role for the entire

host project or certain subnets in the host project, based on the **VPC network sharing mode**. These members are known as Service Project Admins in their respective service projects.

7. In the **VPC network sharing mode** section, select one of the following:
    a. Click **Share all subnets (project-level permissions)** to share all current and future subnets in VPC networks of the host project with all service projects and Service Project Admins.
    b. Click **Individual subnets (subnet-level permissions)** if you need to selectively share subnets from VPC networks of the host project with service projects and Service Project Admins. Then, select **Subnets to share**.
8. Click **Save**.

Service Project Admins for all subnets

A Shared VPC Admin can assign an Cloud IAM member from a service project to be a *Service Project Admin* with access to all subnets in the host project. Service Project Admins of this type are granted the role of `compute.networkUser` for *the whole host project*. This means that they have access to all of the currently defined and future subnets in the host project.

Note: If you cannot create new resources in a particular subnet, an organization policy might be constraining the subnets that this project can use. For more information, refer to the `constraints/compute.restrictSharedVpcSubnetworks` (https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints) constraint.

CONSOLE GCLOUD API

To define an IAM member from a service project as Service Project Admin with access to all subnets in a host project using the Cloud Console, see the attach service projects (#create-shared) section.

Service Project Admins for some subnets

A Shared VPC Admin can assign an IAM member from a service project to be a *Service Project Admin* with access to only some of the subnets in the host project. This option provides a more granular means to define Service Project Admins by granting them the `compute.networkUser` role for only some subnets in the host project.

CONSOLE GCLOUD API

To define an IAM member from a service project as Service Project Admin with access to only some subnets in a host project using the Cloud Console, see the attach service projects (#create-shared) section.

Service Accounts as Service Project Admins

A Shared VPC Admin can also define service accounts (https://cloud.google.com/iam/docs/service-accounts) from service projects as Service Project Admins. This section illustrates how to define *two different types of service accounts* as Service Project Admins:

- User-managed service accounts (https://cloud.google.com/iam/docs/service-accounts#user-managed_service_accounts) having this format: ***USER_ID***@***SERVICE_PROJECT_ID***.iam.gserviceaccount.com
- The Google APIs service account (https://cloud.google.com/iam/docs/service-accounts#google-managed_service_accounts) having this format: ***SERVICE_PROJECT_NUMBER***@cloudservices.gserviceaccount.com

Like other IAM members, the role for Service Project Admin (`compute.networkUser`) can be granted (https://cloud.google.com/iam/docs/granting-roles-to-service-accounts) for all subnets (#networkuseratproject) or only some subnets (#networkuseratsubnet) of the host project. However, for instructional simplicity, this section only illustrates how to define each of the two service account types as Service Project Admins for all subnets (#networkuseratproject) of the host project.

User-managed service accounts as Service Project Admins

These directions describe how to define a user-managed service account as a Service Project Admin for all subnets of the Shared VPC host project.

CONSOLE GCLOUD API

1. Log into the Google Cloud Console as a Shared VPC Admin.
2. Go to the Settings page in the Google Cloud Console.
   GO TO THE SETTINGS PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/IAM-ADMIN/SETTINGS/PR
3. Change the project to the service project containing the service account that needs to be defined as a Service Project Admin.

4. Copy the **Project ID** of the service project. For instructional clarity, this procedure refers to the service project ID as ***SERVICE_PROJECT_ID***.
5. Change the project to the Shared VPC host project.
6. Go to the IAM page in the Google Cloud Console.
   GO TO THE IAM PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/IAM-ADMIN/IAM/PROJECT)
7. Click **Add**.
8. Add ***SERVICE_ACCOUNT_NAME***@***SERVICE_PROJECT_ID***.iam.gserviceaccount.com to the **Members** field, replacing ***SERVICE_ACCOUNT_NAME*** with the name of the service account.
9. Select **Compute Engine > Compute Network User** from the **Roles** menu.
10. Click **Add**.

Google APIs service account as a Service Project Admin

These directions describe how to define the *Google APIs service account* as a Service Project Admin for all subnets of the Shared VPC host project. Making the Google APIs service account a Service Project Admin is a requirement for managed instance groups (https://cloud.google.com/compute/docs/instance-groups/) used with Shared VPC because tasks like instance creation are performed by this type of service account. Refer to Managed Instance Groups and IAM (https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-managed-instances#managedinstancegroupiam) for more information about this relationship.

CONSOLE GCLOUD API

1. Log into the Google Cloud Console as a Shared VPC Admin.
2. Go to the Settings page in the Google Cloud Console.
   GO TO THE SETTINGS PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/IAM-ADMIN/SETTINGS/PR
3. Change the project to the service project containing the service account that needs to be defined as a Service Project Admin.
4. Copy the **Project number** of the service project. For instructional clarity, this procedure refers to the service project number as ***SERVICE_PROJECT_NUMBER***.
5. Change the project to the Shared VPC host project.

6. Go to the IAM page in the Google Cloud Console.
   GO TO THE IAM PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/IAM-ADMIN/IAM/PROJECT)
7. Click **Add**.
8. Add ***SERVICE_PROJECT_NUMBER***@cloudservices.gserviceaccount.com to the **Members** field.
9. Select **Compute Engine > Compute Network User** from the **Roles** menu.
10. Click **Add**.

Using Shared VPC

Once a Shared VPC Admin completes the tasks of enabling a host project (#enable-shared-vpc-host), attaching the necessary service projects to it (#create-shared), and defining Service Project Admins for all (#networkuseratproject) or some (#networkuseratsubnet) of the host project subnets, the Service Project Admins can create instances, templates, and internal load balancers in the service projects using the subnets of the host project.

All tasks in this section must be performed by a Service Project Admin.

It's important to note that a Shared VPC Admin only grants the Service Project Admins the `compute.networkUser` role (to either the whole host project or just some of its subnets). Service Project Admins should also have other roles necessary to administer their respective service projects. For example, a Service Project Admin could also be a project owner (https://cloud.google.com/iam/docs/understanding-roles#primitive_role_definitions) or should at least have the `compute.instanceAdmin` role (https://cloud.google.com/iam/docs/understanding-roles#compute-engine-roles) for the project.

Caution: The `compute.networkUser` (https://cloud.google.com/compute/docs/access/iam#compute.networkUser) and `compute.networkAdmin` (https://cloud.google.com/compute/docs/access/iam#compute.networkAdmin) roles have different permission sets. The `compute.networkUser` role includes permissions that are not available in the `compute.networkAdmin` role. *An IAM member having the* `compute.networkAdmin` *role for an organization or project but lacking the* `compute.networkUser` *role for the host project or at least one of the subnets in the host project is* ***not*** *a Service Project Admin.*

Listing available subnets

Service Project Admins can list the subnets to which they have been given permission by following these steps.

CONSOLE GCLOUD API

Go to the Shared VPC page in the Google Cloud Console.

GO TO THE SHARED VPC PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/NETWORKING/XPN/DETAILS)

Reserving a static internal IP

Service Project Admins can reserve an internal IP address in a subnet of a Shared VPC network. Note that the IP address configuration object is created *in the service project*, while its value comes from the range of available addresses in the chosen shared subnet.

GCLOUD API

1. If you have not already, authenticate to `gcloud` as a Service Project Admin. Replace ***SERVICE_PROJECT_ADMIN*** with the name of the Service Project Admin:

```
gcloud auth login SERVICE_PROJECT_ADMIN
```

2. Run the following command, replacing ***HOST_PROJECT_ID*** with the project ID of the Shared VPC host project:

```
gcloud compute addresses create IP_ADDR_NAME \
--project SERVICE_PROJECT_ID \
--subnet projects/HOST_PROJECT_ID/regions/REGION/subnetworks/SUBNET \
--region=REGION
```

Where you would replace the following:

- ***IP_ADDR_NAME*** with a name for the IP address object
- ***SERVICE_PROJECT_ID*** with the ID of the service project
- ***HOST_PROJECT_ID*** with the ID of the Shared VPC host project
- ***REGION*** with the region containing the shared subnet
- ***SUBNET*** with the name of the shared subnet

Additional details for creating IP addresses are published in the SDK documentation (https://cloud.google.com/sdk/gcloud/reference/compute/addresses/create).

Creating an instance

Keep the following in mind when creating an instance using Shared VPC:

- The standard process for creating an instance (https://cloud.google.com/compute/docs/instances/create-start-instance) involves selecting a zone, a network, and a subnet. Both the selected subnet and the selected zone must be in the same region. When a Service Project Admin creates an instance using a subnet from a Shared VPC network, the zone selected for that instance must be one in the same region as the selected subnet.
    - When creating an instance with a reserved static internal IP address, the subnet (and region) were already selected when the static IP address was created (#reserve_internal_ip). A `gcloud` example for creating an instance with a static internal IP address is given in this section.
- Service Project Admins can only create instances using subnets to which they have been granted permission. See listing available subnets (#discovering_subnets_that_can_be_used) to determine which subnets are available.
- When Google Cloud receives a request to create an instance in a subnet of a Shared VPC network, it checks to see if the IAM member making the request has permission to use that shared subnet. If the check fails, the instance will not be created, and Google Cloud will return a permissions error. Contact the Shared VPC Admin for assistance.

CONSOLE GCLOUD API

1. Go to the VM instances page in the Google Cloud Console.
   GO TO THE VM INSTANCES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/COMPUTE/INSTANCE
2. Click **Create**.
3. Specify a **Name** for the instance.
4. Click **Management, security, disks, networking, sole tenancy**.
5. Click **Networking**.
6. Click the **Networks shared with me** radio button.
7. Select the **Shared subnet** where you want to create the instance.

8. Specify any other necessary parameters for the instance.
9. Click **Create**.

Creating an instance template

Keep the following in mind when creating an instance template using Shared VPC:

- The process for creating an instance template (https://cloud.google.com/compute/docs/instance-templates/create-instance-templates) involves selecting a network and a subnet.
  - Templates created for use in a custom mode Shared VPC network must specify both the network and a subnet.
  - Templates created for use in an auto mode (https://cloud.google.com/vpc/docs/vpc#subnet-ranges) Shared VPC network may optionally defer selecting a subnet. In these cases, a subnet will be automatically selected in the same region as any managed instance group that uses the template. (Auto mode networks have a subnet in every region by definition.)
- When an IAM member creates an instance template, Google Cloud does **not** perform a permissions check to see if the member can use the specified subnet. This permissions check is **always** deferred to when a managed instance group using the template is requested.

CONSOLE GCLOUD API

1. Go to the Instance templates page in the Google Cloud Console.
   GO TO THE INSTANCE TEMPLATES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/COMPUTE/IN
2. Click **Create instance template**.
3. Specify a **Name** for the instance template.
4. Click **Management, security, disks, networking, sole tenancy**.
5. Click **Networking**.
6. Click the **Networks shared with me** radio button.
7. Select the **Shared subnet** where you want to create the instance template.
8. Specify any other necessary parameters for the instance template.
9. Click **Create**.

Creating a managed instance group

Keep the following in mind when creating a managed instance group using Shared VPC:

- Managed instance groups used with Shared VPC require making the Google APIs service account a Service Project Admin (#sa-as-spa) because tasks like automatic instance creation via autoscaling are performed by that service account.
- The standard process for creating a managed instance group (https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-managed-instances) involves selecting a zone or region, depending on the group type, and an instance template. (Network and subnet details are tied to the instance template (#creating_an_instance_template_in_the_shared_vpc_network).) Eligible instance templates are restricted to those that reference subnets in the same region used by the managed instance group.
- Service Project Admins can only create managed instance groups whose member instances use subnets to which they have been granted permission. Because the network and subnet details are tied to the instance template, Service Project Admins can only use templates that reference subnets that they are authorized to use.
- When Google Cloud receives a request to create a managed instance group, it checks to see if the IAM member making the request has permission to use the subnet (in the same region as the group) specified in the instance template. If the check fails, the managed instance group will not be created, and Google Cloud will return a permissions error. List available subnets (#discovering_subnets_that_can_be_used) to determine which ones can be used, and contact the Shared VPC Admin for assistance.

For more information, refer to Creating Groups of Managed Instances (https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-managed-instances) in the Compute Engine documentation.

Creating an internal TCP/UDP load balancer

The following example illustrates what you must consider when creating an internal TCP/UDP load balancer in a Shared VPC network. Service Project Admins can create an internal TCP/UDP load balancer that uses a subnet (in the host project) to which they have access. The load balancer's internal forwarding rule

(https://cloud.google.com/load-balancing/docs/internal/#forwarding_rule) is defined in the service project, but its subnet reference (https://cloud.google.com/sdk/gcloud/reference/compute/forwarding-rules/create) points to a subnet in a Shared VPC network of the host project.

Before you create an internal TCP/UDP load balancer in a Shared VPC environment, review the following documents:

- Internal TCP/UDP Load Balancing Concepts (https://cloud.google.com/load-balancing/docs/internal/)
- Setting Up Internal TCP/UDP Load Balancing (https://cloud.google.com/load-balancing/docs/internal/setting-up-internal)
- Special notes for load balancing in a Shared VPC environment (https://cloud.google.com/vpc/docs/shared-vpc#shared_vpc_with_load_balancing).

CONSOLE GCLOUD API

1. Go to the Load balancing page in the Google Cloud Console.
   GO TO THE LOAD BALANCING PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/NETWORKING/LOA
2. Create your internal TCP/UDP load balancer, making the following adjustment: In the **Configure frontend services** section, select the Shared VPC subnet you need from the **Networks shared by other projects** section of the **Subnet** menu.
3. Finish creating the load balancer.

What's next

- See the Shared VPC Overview (https://cloud.google.com/vpc/docs/shared-vpc) for more information on Shared VPC.
- See Setting up Clusters with Shared VPC (https://cloud.google.com/kubernetes-engine/docs/how-to/cluster-shared-vpc) for instructions on setting up Kubernetes Engine clusters with Shared VPC.
- See Deprovisioning Shared VPC (https://cloud.google.com/vpc/docs/deprovisioning-shared-vpc) for instructions on deleting a Shared VPC setup.

Last updated November 21, 2019.