This tutorial guides you through the process of setting up Shared VPC (/vpc/docs/shared-vpc) using Deployment Manager (/deployment-manager/), which provides a way to enforce strict network security rules across your organization for access to GCP resources.

In large organizations, you may need to put different departments or different applications into different projects to separate budgeting, access control, and so on. With Shared VPC, Organization (/resource-manager/docs/cloud-platform-resource-hierarchy) administrators can give multiple projects permission to use a single, shared VPC network and corresponding networking resources.

With Shared VPC, as an Organization administrator, you can allow the network and security admins of your organization to manage a VPC network of RFC 1918 (https://tools.ietf.org/html/rfc1918) IP spaces (and related features such as VPNs or firewall rules) that associated projects can use. Administrators in associated projects can create virtual machine (VM) instances in the shared VPC network space. You can apply and enforce consistent policies across an organization.

Because Shared VPC is often used in large organizations, or in organizations with strict security rules, being able to easily reproduce a Shared VPC setup is important. You can use Deployment Manager, an Infrastructure as Code (IaC) tool, to achieve this.

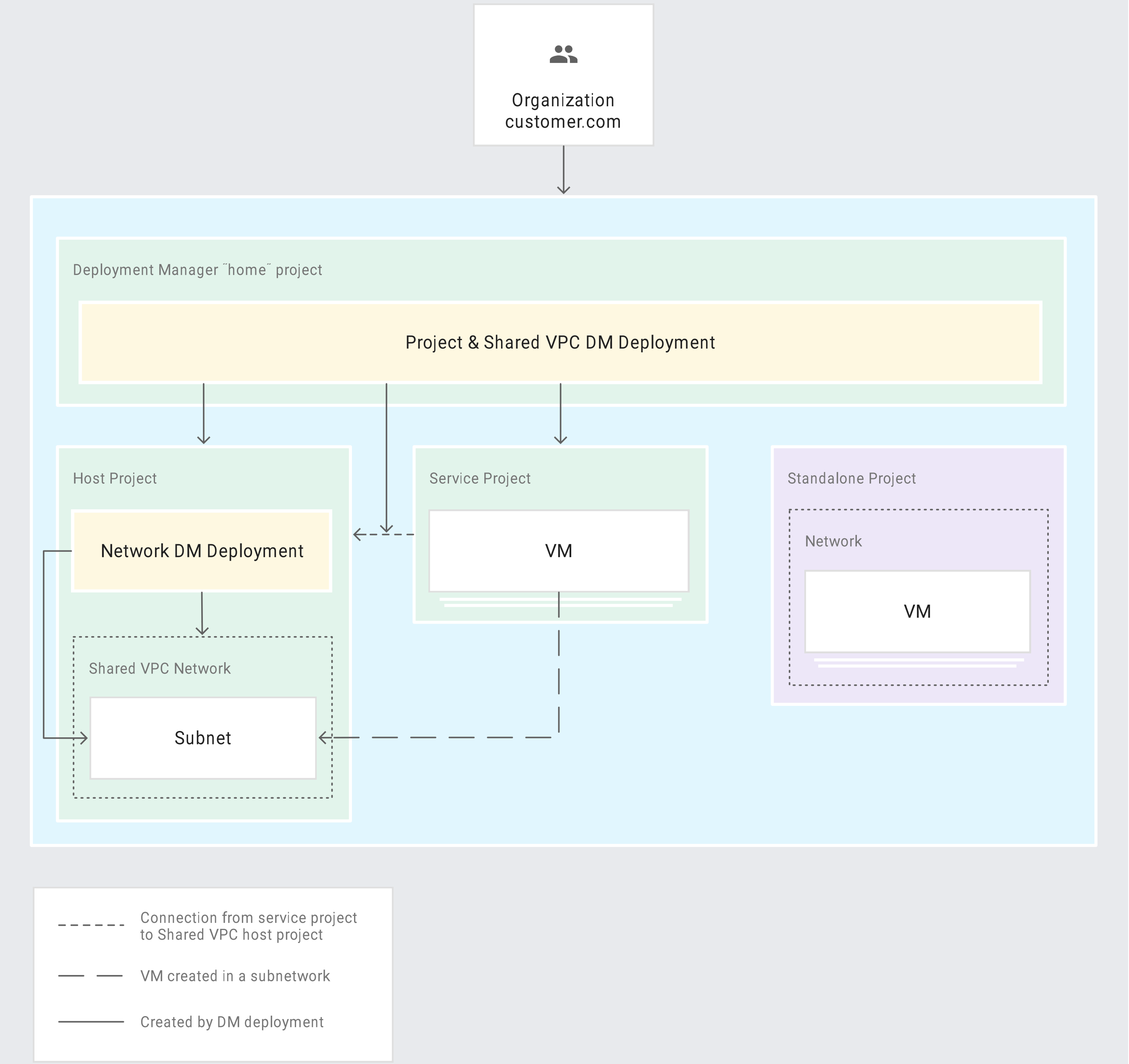
Note: Shared VPC was previously known as Cross-Project Networking (XPN).

This tutorial assumes that you are familiar with Organization resources in Google Cloud Platform (GCP) and that you are the administrator of an Organization resource. Understanding

Shared VPCs and Deployment Manager will help you follow this tutorial. Throughout this tutorial, the word *deployment* refers to a deployment from Deployment Manager.

For simplicity, this tutorial uses a single IAM user—your existing identity as an Organization resource administrator. (If you don't already have an Organization resource, you can find instructions in the Before you begin (#heading=h.d9o9bhwmv3l6) section for creating one.) In a company, three different people are usually involved in setting up the scenario illustrated by this tutorial: an Organization resource administrator, a network administrator (who manages the Shared VPC), and a user of the Shared VPC.

The following diagram shows the architecture of this solution:


Organization
customer.com
Deployment Manager ¨home¨ project
Project & Shared VPC DM Deployment
Host Project
Network DM Deployment
Shared VPC Network
Subnet
Service Project
VM
Standalone Project
Network
VM
Connection from service project to Shared VPC host project
VM created in a subnetwork
Created by DM deployment

In this tutorial, you create three of the projects from this diagram:

- The Deployment Manager home project is managed by an Organization resource administrator (in this tutorial we assume that's you) and is used to create the other projects and the Shared VPC setup.
- The host project is managed by network administrators and hosts the Shared VPC. All the networking configuration will be done in this project.

- The service project is managed by users of the Shared VPC. In this project, resources can be created in the Shared VPC from the host project.

- Create and configure the Deployment Manager home project.
- Create the host and service projects with Deployment Manager.
- Configure the Shared VPC feature.
- Configure the VPC and some subnetworks in the host project.
- Verify that the VPC can be used in the service project.

This tutorial uses billable components of GCP, including:

- Compute Engine

Use the Pricing Calculator (/products/calculator/) to generate a cost estimate based on your projected usage.

This tutorial is set in the context of a GCP Organization. If you do not have one, create one. For details, see Creating and Managing Organizations (/resource-manager/docs/creating-managing-organization).

Later in this tutorial, you create two GCP projects with a deployment (that is, a Deployment Manager deployment). You create this deployment in a dedicated project with a specific configuration. The following steps guide you through the initial setup of this project and its configuration.

Note: Some of the steps of this tutorial can be done in the Cloud Console, but the most important ones can't be. Therefore, we recommend that you use the gcloud command-line tool throughout this tutorial.

1. Open Cloud Shell.

   Open Cloud Shell (https://console.cloud.google.com/cloudshell)

2. If you do not already have one, create a billing account. For details, see Create a Billing Account (/billing/docs/how-to/manage-billing-account#create_a_new_billing_account).

3. Create a new project in your Organization and set a billing account for it. You must choose a unique ID for this project. For instance, you can use a name like `[YOUR_NAME]-[DATE]-dm-home`.

⚠ **Warning:** This project is going to create and own the Deployment Manager deployments. Because of the permissions granted in later steps, this project should not be used for any purpose other than creating other projects.

4. Enable the APIs needed for the rest of the tutorial.

Shared VPC is an Organization-level feature. As such, it requires some Organization-level policies to be configured—the service account used by Deployment Manager needs specific roles at the Organization level.

Note: In a production environment, you should protect the Shared VPC host project against deletion. In order to do that, run the following command:

You now are ready to create the Host and Service project with Deployment Manager. If you have been using the Cloud Console, from here on, you must switch to Cloud Shell.

1. If your session has timed out, or if you have closed it, open a new Cloud Shell session.

   OPEN CLOUD SHELL (https://console.cloud.google.com/cloudshell/)

2. In Cloud Shell, clone the following Git repository:

3. Navigate to the `project_creation` sample in the repository you cloned:

4. Open the `config_shared_vpc.yaml` file:

5. Set the values listed in the following table.

Setting	Description
`HOST_PROJECT`	A unique name for your host project. The host project is where the VPC will be created and managed. Note that you must also change this value in the last line of the file, for a total of two replacements. Example: **`[YOUR_NAME]-[DATE]-host`**
`SERVICE_PROJECT`	A unique name for your service project. The service project is where the VPC from the host project will be used. Example: **`[YOUR_NAME]-[DATE]-svc`**
`ORG_ID`	Your Organization ID. You should have this value from earlier steps. If not, you can get it by running the following command: Use quotation marks around the Organization ID so that it's not considered a numeric value in the YAML file.

Setting	Description
`BILLING_ACCOUNT_ID`	The ID of your billing account. You should have this value from earlier steps. If not, you can get it by running the following command:
`EMAIL`	Your email address. Note that there are a total of five places where you need to set the email address.

★ **Note:** There are two resources of type `project.py` in the `config_shared_vpc.yaml` file. The first is the host project for the Shared VPC, and the second is the service project. You need to modify both with your own values.

6. Save the file and exit `nano` with the following key sequence:

   ^O <Enter> ^X

7. If you used the Cloud Console to create the Deployment Manager home project, set an environment variable to the ID of your home project:

8. Create a preview of the deployment:

   Creating a preview of a Deployment Manager deployment allows you to see what resources will be created, updated, or deleted.

9. Apply the preview of the deployment:

10. View your deployment in the Cloud Console. If needed, select your Deployment Manager home project in the top project selection menu.

    GO TO DEPLOYMENT MANAGER (https://console.cloud.google.com/deployments)

After a few minutes, the deployment is complete and your two new projects are created. Although the service project is already linked to the host project, you have not yet created the VPC that is going to be shared.

If problems occurred while the preview was being created, you can delete the deployment (no resources have been created yet) and retry the process.

However, if the preview was created but the deployment failed, you might not be able to re-create that deployment. Projects cannot be deleted and re-created immediately; they are marked for deletion for a safety period of 30 days. If you do need to re-create the deployment, change the values of the `HOST_PROJECT` and `SERVICE_PROJECT` settings in the `config_shared_vpc.yaml` file before you try again.

You now are going to use another Deployment Manager template to create the VPC in the host project. This is typically an operation that would be done by a network administrator. Because the Shared VPC configuration has already been set up, the VPC is going to be available for use in the service project immediately.

1. Set environment variables to the names of the host project and service project names that you set in the `config_shared_vpc.yaml` file:

2. Navigate to the `network` sample in the Git repository:

   In the `config.yaml` file, you can see one resource of type `network.py` with three subnetworks with their own CIDRs. You can experiment with changing or duplicating this resource to suit your needs.

3. Create a preview of the deployment. This deployment is created in the host project.

★ **Note:** Because it creates the VPC and other networking resources, this deployment is normally managed by a network administrator.

4. Apply the preview of the deployment.

You can now verify access to the host project's network from the service project. You can access this network because you have the role `roles/compute.networkUser` in the host project. For a production deployment, you need to assign this role to every user who is going to use Shared VPC.

1. Create a test instance in the service project using a subnetwork from the host project.

Allow a minute or two for the instance to start up. When the instance is ready, it is listed on the VM Instances page with a green status icon.

2. Verify that your instance is using the Shared VPC.

After you've finished the current tutorial, you can clean up the resources that you created on GCP so they won't take up quota and you won't be billed for them in the future. The following sections describe how to delete or turn off these resources.

1. In Cloud Shell, delete the test instance:

2. If you set up project removal protection, remove it:

3. Delete the `host-network` deployment:

4. Delete the `shared-vpc-projects` deployment:

5. Delete the home project:

- Learn about the Private Google Access feature of VPC (/vpc/docs/private-google-access)
- Learn to share images across projects to be used with Deployment Manager (/deployment-manager/docs/configuration/using-images-from-other-projects-for-vm-instances)
- Learn how to design GCP policies (/solutions/policies/designing-gcp-policies)

- Try out other Google Cloud features for yourself. Have a look at our tutorials (/docs/tutorials).