**Steps to create GCE VM and deploy nginx**

1. Go to the **VM instances** page.
2. Select your project and click **Continue**.
3. Click the **Create instance** button.
4. Specify a **Name** for your instance.
5. Optionally, change the **Zone** for this instance.
6. Select a **Machine configuration** for your instance.
7. In the **Boot disk** section, click **Change** to configure your boot disk.  
   Create a boot disk no larger than 2 TB to account for the limitations of [MBR](https://wikipedia.org/wiki/Master_boot_record) partitions.
8. In the **OS images** tab, choose an image.  
   Select **Show images with Shielded VM features** to see only [Shielded VM](https://cloud.google.com/security/shielded-cloud/shielded-vm) images.
9. Click **Select**.
10. To permit HTTP or HTTPS traffic to the VM instance, select **Allow HTTP traffic** or **Allow HTTPS traffic**.

The Cloud Console adds a network tag to your instance and creates the corresponding ingress firewall rule that allows all incoming traffic on tcp:80 (HTTP) or tcp:443 (HTTPS). The network tag associates the firewall rule with the instance. For more information, see [Firewall rules overview](https://cloud.google.com/vpc/docs/firewalls/) in the Virtual Private Cloud documentation.

1. To add secondary non-boot disks to your VM instance:
   1. Click the **Management, security, disks, networking, sole tenancy** section.
   2. Click the **Disks** tab.
   3. Under **Additional disks** click **Add new disk**.
   4. Specify a disk **Name**, **Type**, **Source type**, **Mode**, and **Deletion rule**.
   5. Click **Done**.
   6. Add additional disks as needed.
2. Optionally, change the instance's [Shielded VM](https://cloud.google.com/security/shielded-cloud/shielded-vm) settings, if you chose an image that supports Shielded VM:
   1. Click the **Security** tab in the **Management, security, disks, networking, sole tenancy** section.
   2. If you want to disable Secure Boot, uncheck **Turn on Secure Boot**. Secure Boot helps protect your VM instances against boot-level and kernel-level malware and rootkits. For more information, see [Secure boot](https://cloud.google.com/security/shielded-cloud/shielded-vm#secure-boot).
   3. If you want to disable the virtual trusted platform module (vTPM), uncheck **Turn on vTPM**. The vTPM enables Measured Boot, which validates the VM pre-boot and boot integrity. For more information, see [Virtual Trusted Platform Module (vTPM)](https://cloud.google.com/security/shielded-cloud/shielded-vm#vtpm).

**Important:** Disabling the vTPM also disables integrity monitoring, because integrity monitoring relies on data gathered by Measured Boot.

* 1. If you want to disable integrity monitoring, clear the **Turn on Integrity Monitoring** checkbox. Integrity monitoring lets you monitor the boot integrity of your Shielded VM instances using Stackdriver Monitoring. For more information, see [Integrity monitoring](https://cloud.google.com/security/shielded-cloud/shielded-vm#integrity-monitoring).

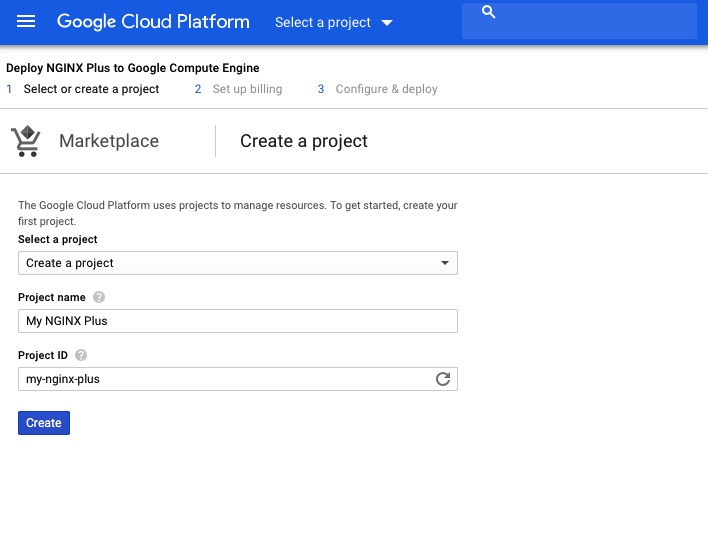
1. Click the **Create** button to create and start the instance.

Installing the NGINX Plus VM

To quickly set up an NGINX Plus environment on the Google Cloud Platform, perform the following steps.

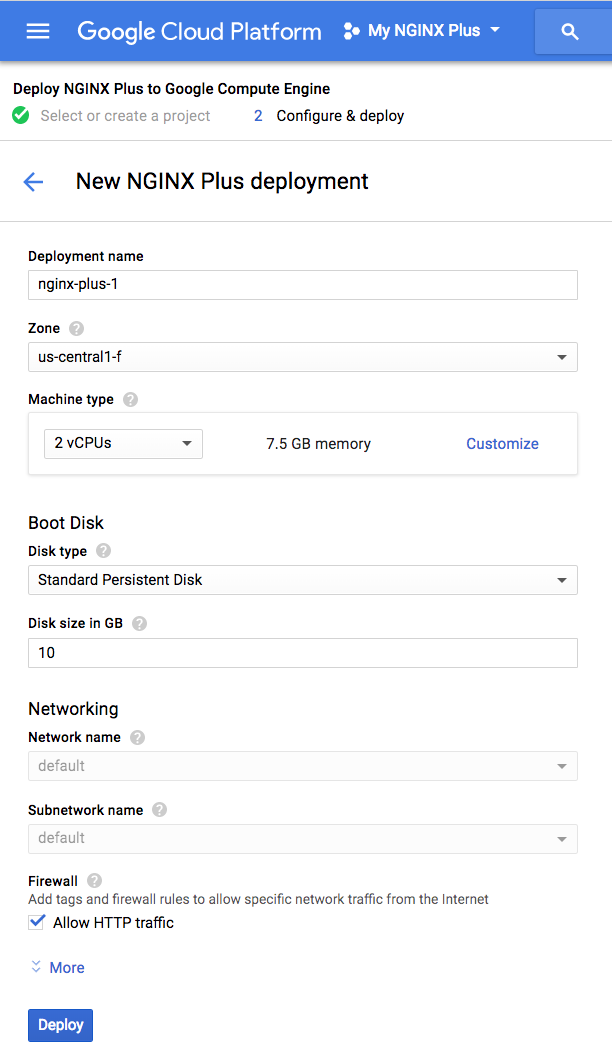
Access the [NGINX Plus page](https://console.cloud.google.com/marketplace/details/nginx-public/nginx-plus) in Google Marketplace and click the **LAUNCH ON COMPUTE ENGINE** button.

1. The **Select or create a project** window opens. Enter a project name and select a value from the **Organization** drop‑down, then click the **Create** button.

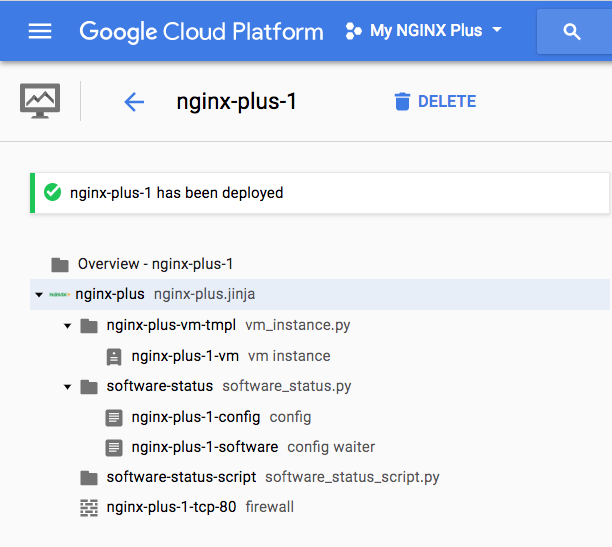


1. In the **Configure & Deploy** window, enter or select appropriate values for zone, machine type, and so on. Click the **Deploy** button.

Note: In the Firewall section, be sure the Allow HTTP traffic checkbox is checked. For more information on controlling incoming traffic, see the [Firewall Rules Overview](https://cloud.google.com/vpc/docs/firewalls) in the Google Cloud Platform documentation.



1. Click the **Create** button. The Google Developers Console confirms that NGINX Plus was deployed.



As soon as the project deploys and the new virtual machine (VM) instance starts running, NGINX Plus starts automatically and serves a default **index.html** page. To verify that NGINX Plus is working properly, use a web browser to access the public DNS name of the new VM and view the page.