Deploy VOS Devices from Google Marketplace

For supported software information, click here.

This article describes how to deploy Versa Operating System™ (VOS™) devices from Google Cloud Platform Marketplace.

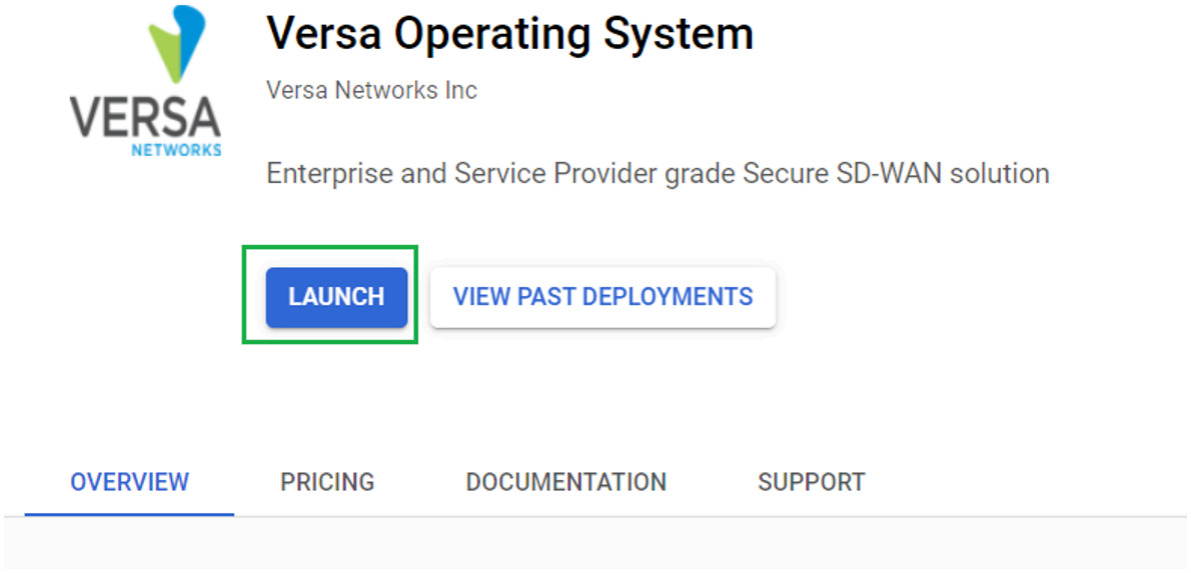
Before You Begin

Before you install a VOS branch device on Google Cloud Platform, ensure that you have done the following:

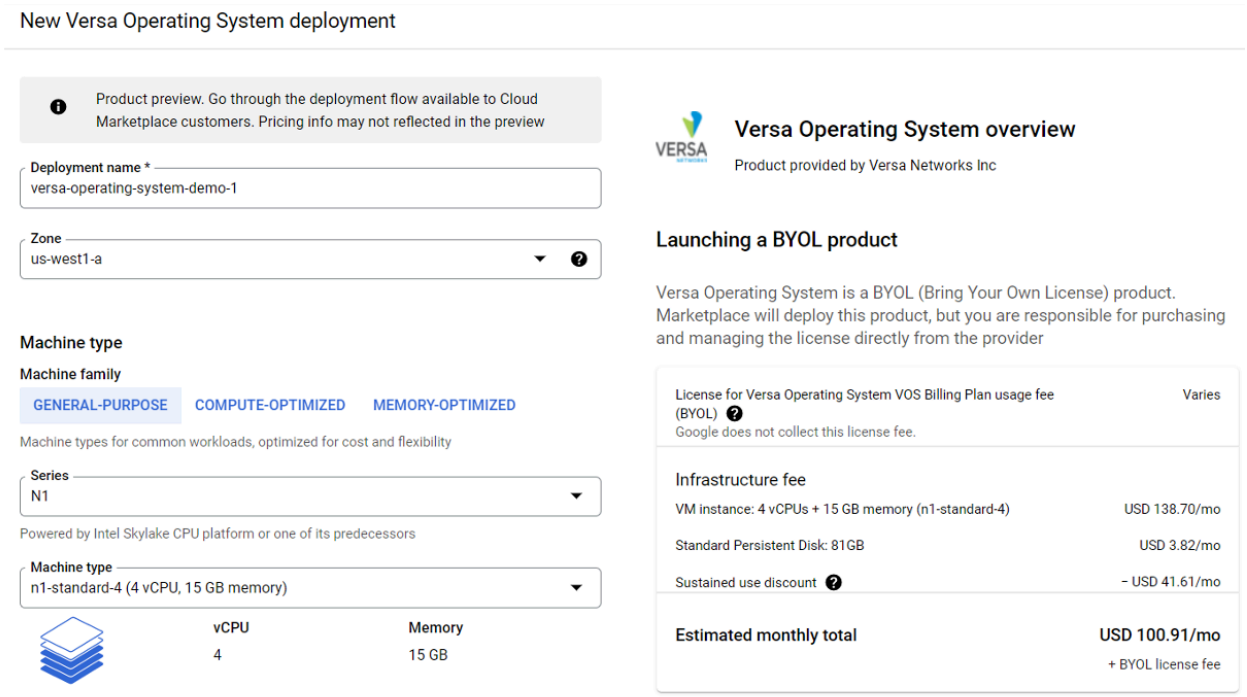
- Create three subnets for the VOS instance. Note that you must place the three subnets in three different private clouds (VPCs).
  - Management subnet
  - WAN subnet, to communicate with the SD-WAN Controller node
  - LAN subnet, to communicate with the LAN side
- Create firewall rules and associate them with the VPC and subnet. For more information, see Firewall Requirements.

Deploy VOS Devices

1. Search for Versa Operating System solution in Google Marketplace.
2. Click the Launch button.



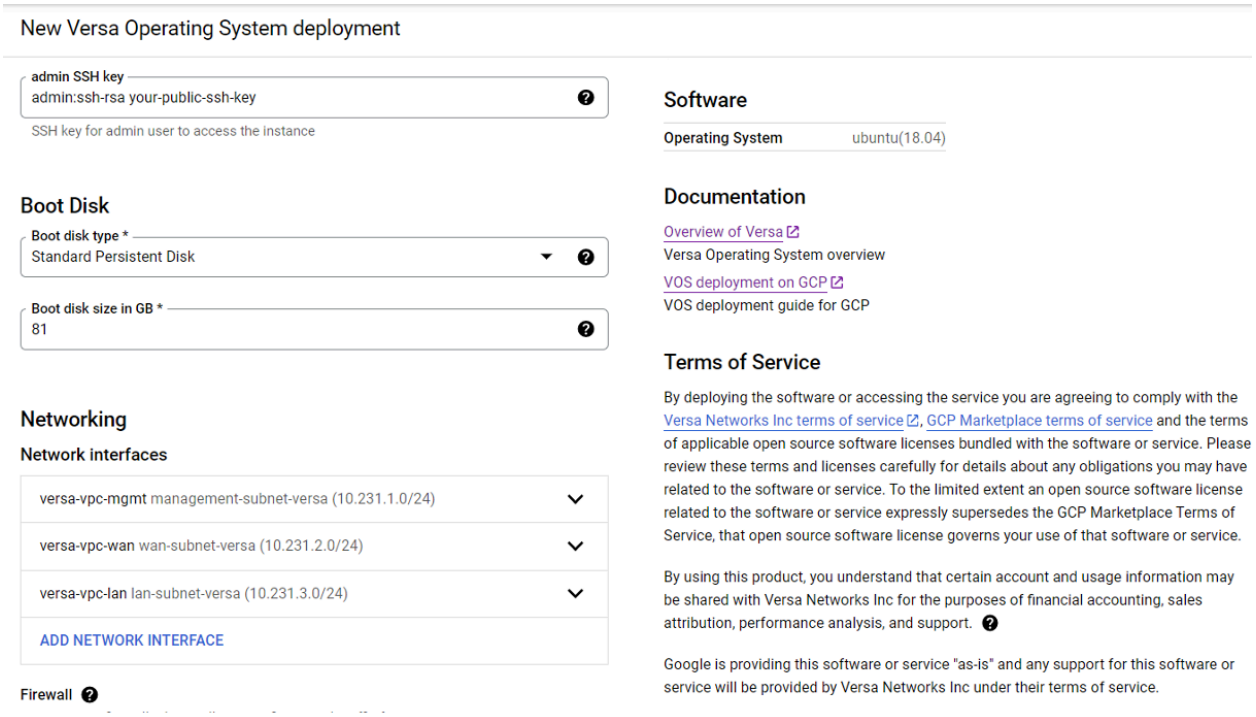
3. In the New Versa Operating System Deployment window, enter information for the following fields.

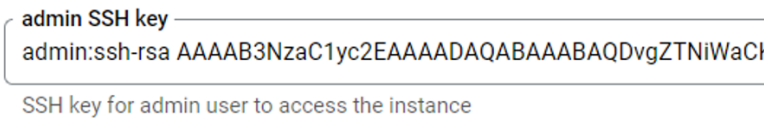
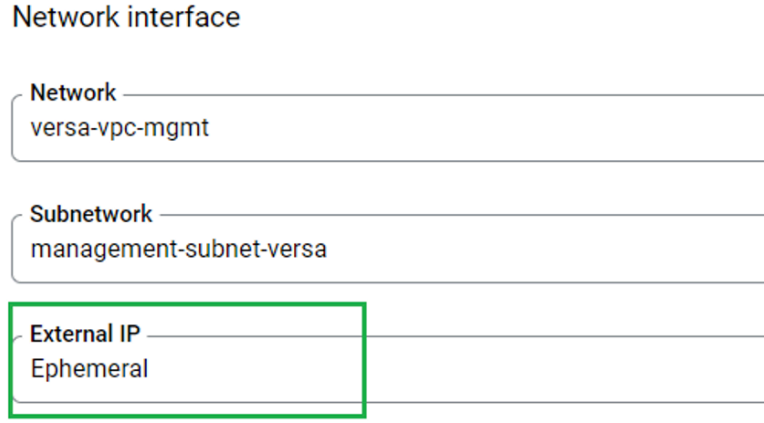


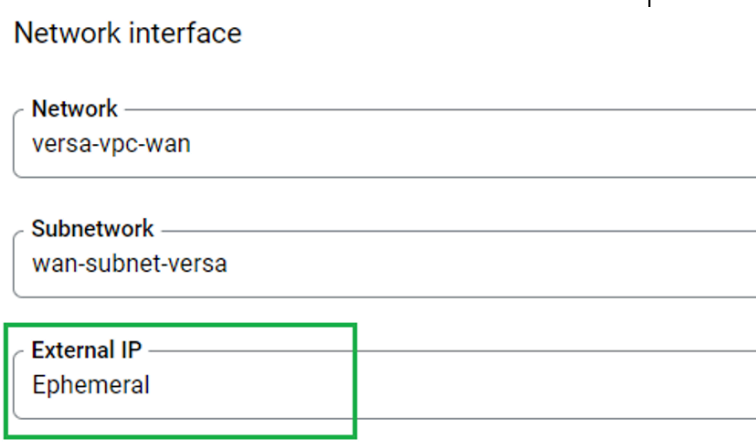
Field	Description
Deployment Name	Enter a name for the deployment.
Zone	Select the zone in which the deployment is planned.

Field	Description
Machine Type	Select the machine type to use. For more information, see Qualified Google Cloud Instances.

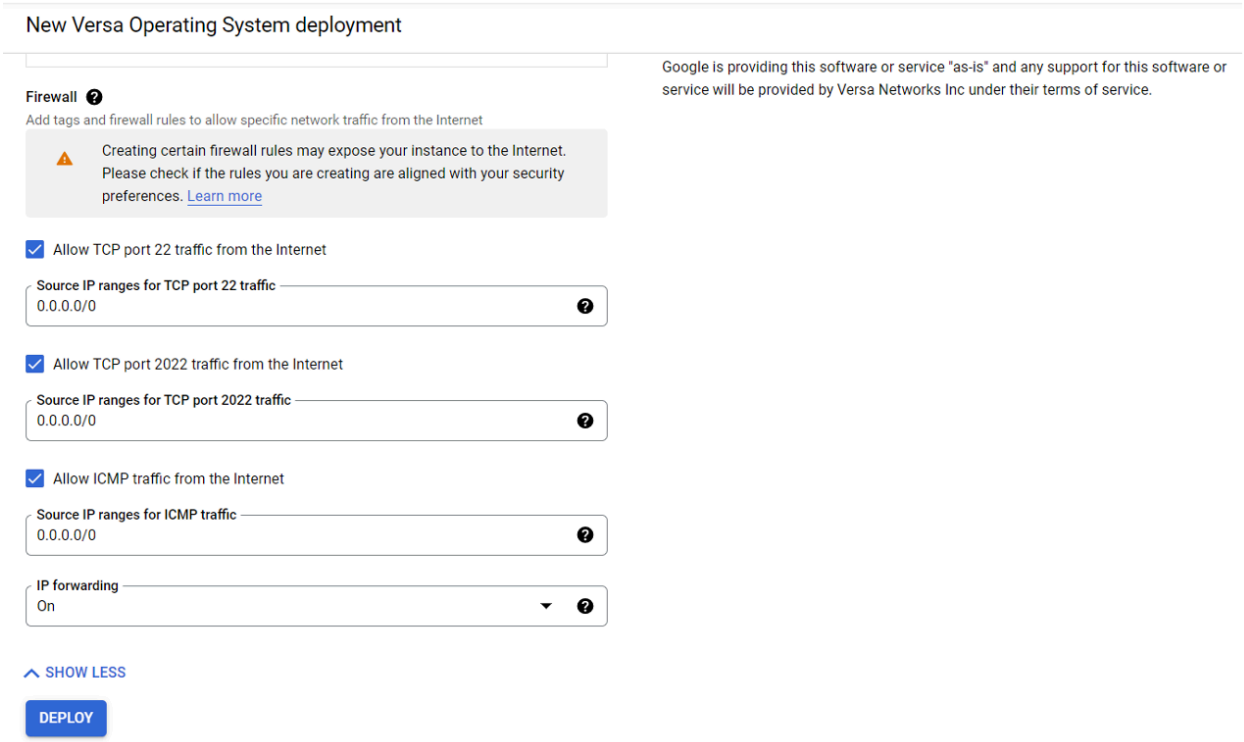
4. Scroll down the New Versa Operating System Deployment screen, and enter information for the following fields.



Field	Description
Admin SSH Key	Enter or paste the RSA public key for the admin user here. This key pair is used to log in to later VOS instance. Remove the text “your-public-ssh-key” and add actual RSA public key. For example: 
Boot Disk	Use the default values.
Networking (Group of Fields)	Select the networks and network interfaces to use. You use a minimum of three networks interfaces.
◦ First network interface	Select the network interface to use for management. In the External IP field, select Ephemeral to assign a public IP address to this interface. For example: 
◦ Second network interface	Select the network interface to use for the WAN network. In the External IP field, select Ephemeral to assign a public IP address to this interface in case the Versa Controller node is reachable using a public IP address. For example:

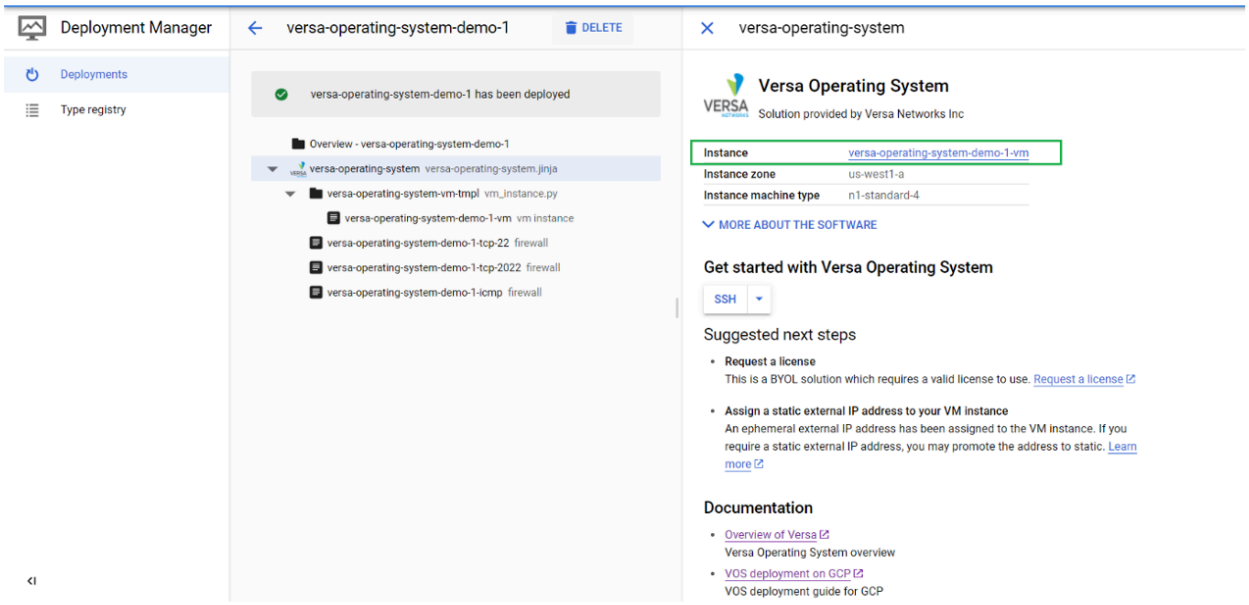
	
◦ Third network interface	Select the network interface to use for the LAN network.

5. Scroll down the New Versa Operating System Deployment screen, and enter information for the following fields.

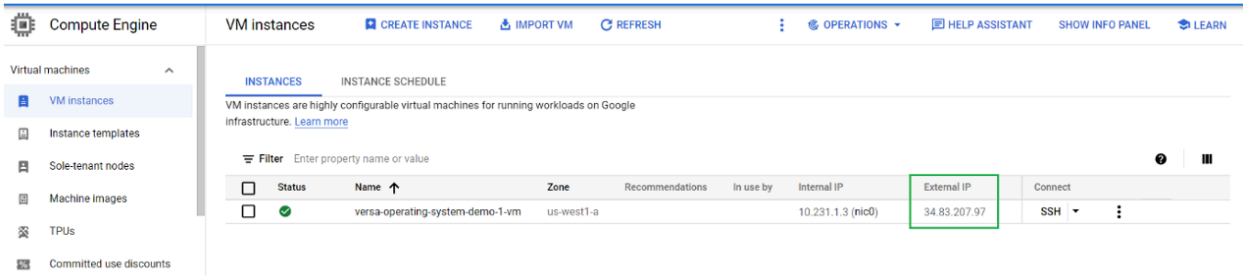


Field	Description
Firewall (Group of Fields)	Allow traffic from these source IP addresses on TCP ports 22 and 2022 and to allow ICMP on the instance created by the deployment.
◦ Allow TCP Port 22 Traffic from the Internet	Add a source IP range to allow traffic from the internet over TCP port 22. To allow traffic from everywhere, enter the address range 0.0.0.0/0.
◦ Allow TCP Port 2022 Traffic from the Internet	Add a source IP range to allow traffic from the internet over port 2022. To allow traffic from everywhere, enter the address range 0.0.0.0/0.
◦ Allow ICMP Traffic from the Internet	Add a source IP range to allow ICMP traffic from the internet. To allow traffic from everywhere, enter the address range 0.0.0.0/0.
IP Forwarding	Select the default, which is On.

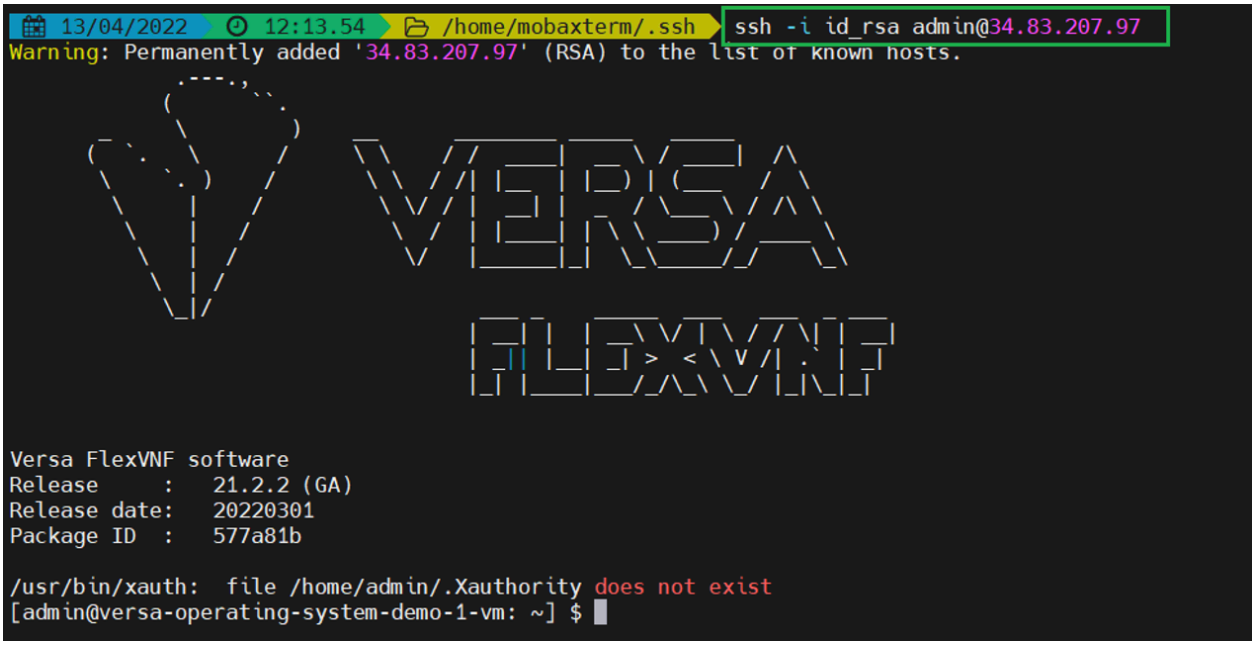
6. Click Deploy to start the deployment.
7. When the deployment successfully completes, click the instance name to display information about the instance.



8. From the instance page, copy the Public/External IP address.



9. Log in to the instance using the Public/External IP address and the private RSA key with admin user that you configured in Step 4, above.



10. Edit the sshd_config file to add the IP addresses of the Versa Director northbound and southbound interfaces as match address exceptions. Doing this allows the Director node to log in to the node using a password and to perform the zero-touch provisioning (ZTP) process using the staging.py script. For example:

```
$ sudo vi /etc/ssh/sshd_config
...
Match address 10.192.220.193/32,192.168.220.193/32
  PasswordAuthentication yes
Match all
```

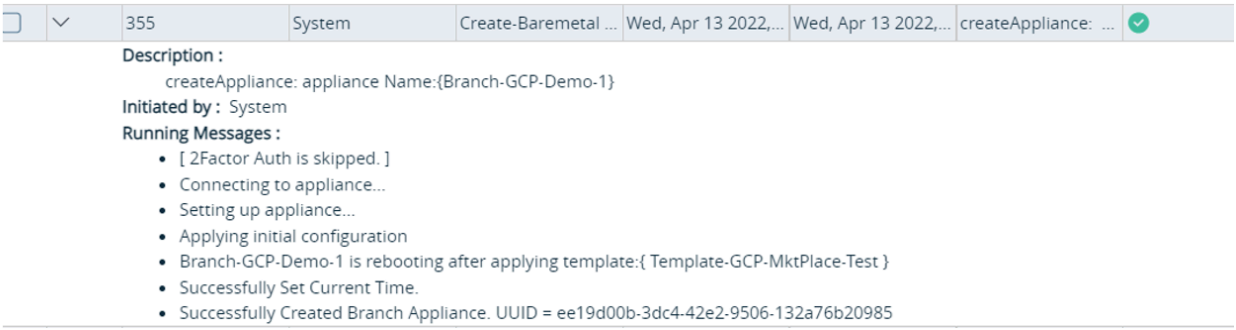
11. Restart SSH services on the instance:

```
$ sudo service ssh restart
```

12. Execute the staging.py script to trigger the ZTP process. Here, provide the required parameters as per your infrastructure and controller configuration. For example:

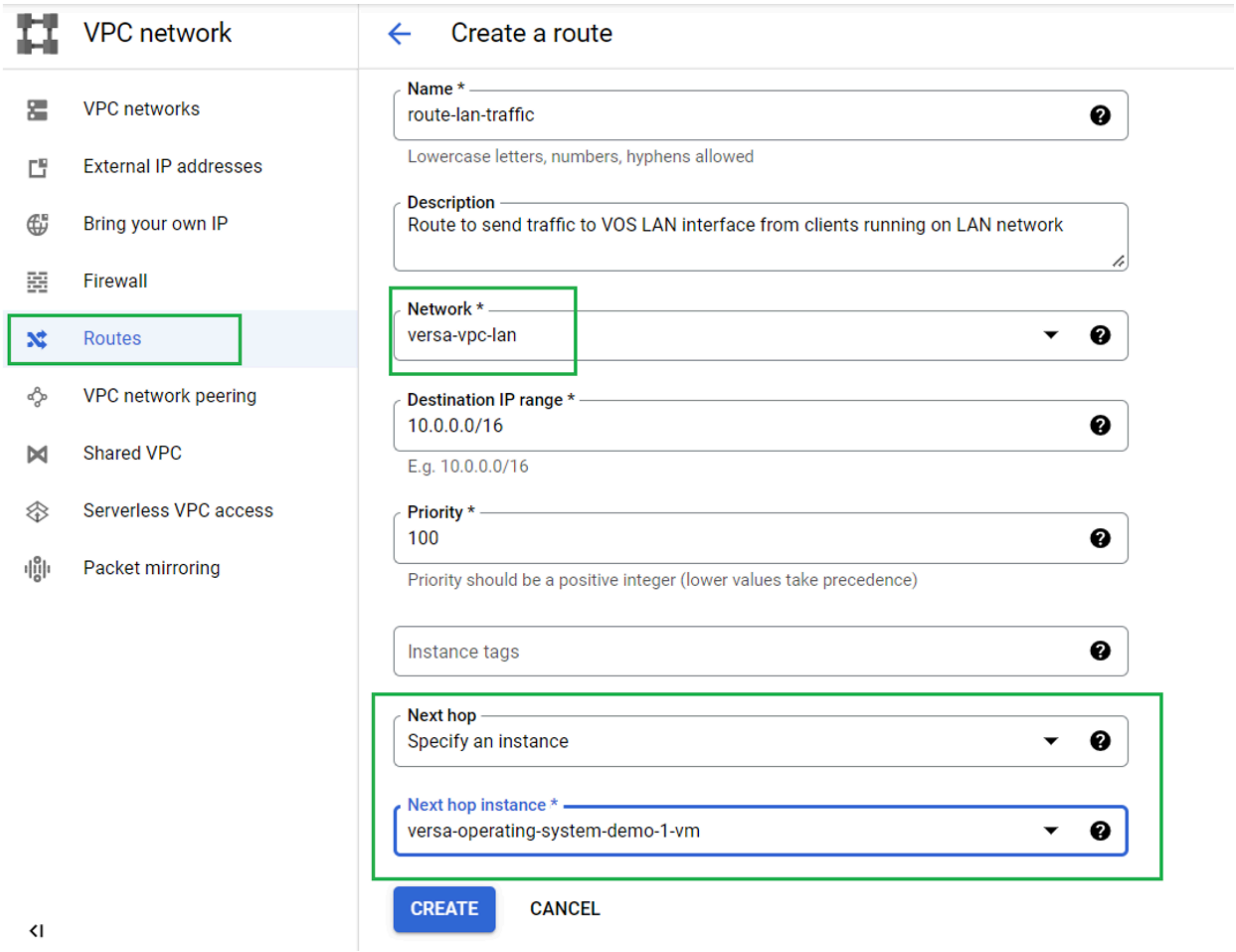
```
[admin@versa-operating-system-demo-1-vm: scripts] $ sudo ./staging.py -l SDWAN-Branch@Versa-Provider.com -r Controller-Provider-staging@Versa-Provider.com -c
1[redacted]6 -d -n SR1400
=> Setting up staging config
=> Checking if all required services are up
=> Checking if there is any existing config
=> Generating staging config
=> Config file saved /opt/versa/scripts/staging.cfg
=> Saving serial number
=> Check if control-plane is up and runnning
=> Loading generated config into CDB
```

13. The ZTP process creates the appliance task on the Director node. For example:



14. In the Director Appliance tab, check that the appliance has been created and is reachable. For example:

15. After ZTP completes, in Google Cloud Platform, add a custom route to pass the traffic from VOS interface instead of Google backbone network. For example:



16. Click Create.

Supported Software Information

Releases 21.2.2 and later support all content described in this article.

Additional Information

Qualified AWS, Azure, and Google Cloud Instances