



Create Project and Launch VM

- [Create Project and Launch VM, page 1](#)
- [Steps to Create a Project, page 1](#)
- [Steps to Create a User for the Project, page 2](#)
- [Steps to Create the Network, page 2](#)
- [Steps to Create a Security Group, page 4](#)
- [Steps to Launch the VM, page 5](#)

Create Project and Launch VM

The information provided in this section is generic to OpenStack and it is provided here for your convenience with the exception of ConfigProfile, which is Cisco Nexus fabric specific.

Steps to Create a Project

Follow these steps to create a project:

- 1 Login to the Horizon dashboard as an administrator. Use the password that you used in the OpenStack configuration file.
- 2 Click **Projects** and then **Create Project**.
- 3 Enter relevant project information and click **Create Project** to create the project.



Note

The project name is used as vrfName in the fabric (vrfName = "project_name:CTX") for fabric auto-configuration. The fabric limits the size of the vrfName string to 32 characters. Ensure that the project name length is less than 29 characters when creating the project. Do not use hyphens in the project name.

DCI Support

You can use OpenStack to configure the DC Inter-connect function. Support is only provided for Layer-3 DCI with the Cisco Prime DCNM 7.1(1) release, and Cisco NX-OS 7.1(0)N1(1) release or later.

As part of the project name string, type `xyz:dci_id:129` to enable DCI support ('129' is used here as an example). Type `xyz` or `xyz:dci_id:0` to remove DCI support for this project.

The integer 129 is the DCI ID. Cisco Prime DCNM uses it as an indication that the user desires to auto-configure the border leaf switches with this VRF, and extend to the DCI edge device(s). If the value is 0, Cisco Prime DCNM removes VRF configurations from the border leaf switches and the configurations that extend the VRF from the border leaf switch to the DC edge device(s).

Steps to Create a User for the Project

Follow these steps to create a user for the project:

- 1 Click **Users**, and then **Create User**.
- 2 Fill in all the fields, select the project you just created and select the role as *admin*. The network information will not be populated correctly to DCNM if you fail to specify the role as *admin*.

Steps to Create the Network

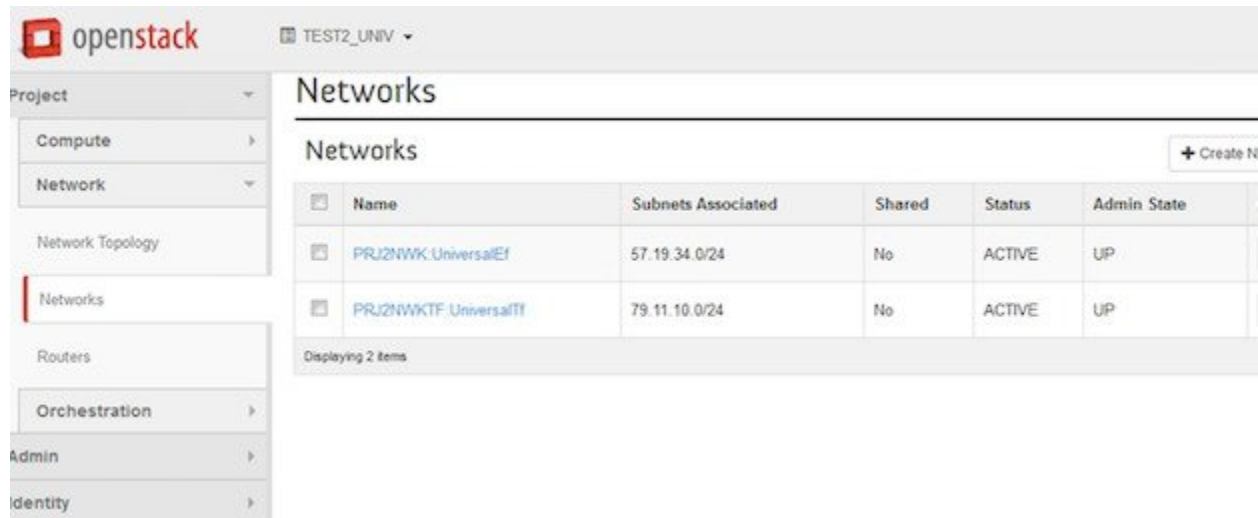
Follow these steps to create the network:

- 1 Login as a user using login credentials created by the administrator.
- 2 Click the **Project** tab.
- 3 Click **Networks** and then click **Create Network**. Specify a Name for the network and go to the **subnet** tab. This is mandatory.
- 4 Specify a Network Address for the subnet.

Use non-default network profiles

By default, for Cisco Prime DCNM with version 7.1, `defaultNetworkUniversalEfProfile` is the network profile used automatically by the system. Additionally, `defaultNetworkUniversalTfProfile` can also be specified when creating a network in OpenStack. A sample screen shot is given below:

Figure 1: Default Network



The screenshot shows the OpenStack interface for the 'TEST2_UNIV' project. The 'Networks' section displays a table with two entries:

Name	Subnets Associated	Shared	Status	Admin State
PRJ2NWK.UniversalEf	57.19.34.0/24	No	ACTIVE	UP
PRJ2NWKTF.UniversalTf	79.11.10.0/24	No	ACTIVE	UP

The interface also includes a sidebar with navigation options like Compute, Network, Network Topology, Routers, and Admin, and a '+ Create N' button in the top right corner.

Following are the supported network profiles with Cisco Prime DCNM version 7.1(1):

- `defaultNetworkUniversalEfProfile`
- `defaultNetworkUniversalTfProfile`
- `defaultNetworkL2Profile`

If it is an upgrade from version 7.0(1) or 7.0(2) to 7.1(1), the default profile will be `defaultNetworkIpv4EfProfile`, and the supported profiles will be the sum of the profiles for versions 7.0(1), 7.0(2) and 7.1(1) or later, as shown below:

- `defaultNetworkIpv4EfProfile`
- `defaultNetworkIpv4TfProfile`
- `defaultNetworkL2Profile`
- `defaultNetworkUniversalEfProfile`
- `defaultNetworkUniversalTfProfile`
- `defaultNetworkL2Profile`

The syntax to use non-default profiles when creating a network is given below. In the examples, `network_name` signifies the name of the network followed by a sub-string of the profile name:

- `network_name:L2`
- `network_name: Ipv4Ef`
- `network_name: Ipv4Tf`

- network_name: UniversalTf
- network_name: UniversalEf

Use defaultNetworkL2Profile

If this profile is chosen when a network is created in OpenStack, DCNM DHCP server will not assign an IP address for the VM associated with the network. Users are required to configure a static IP address for the VM. Additionally, the following command needs to be run on the OpenStack control node:

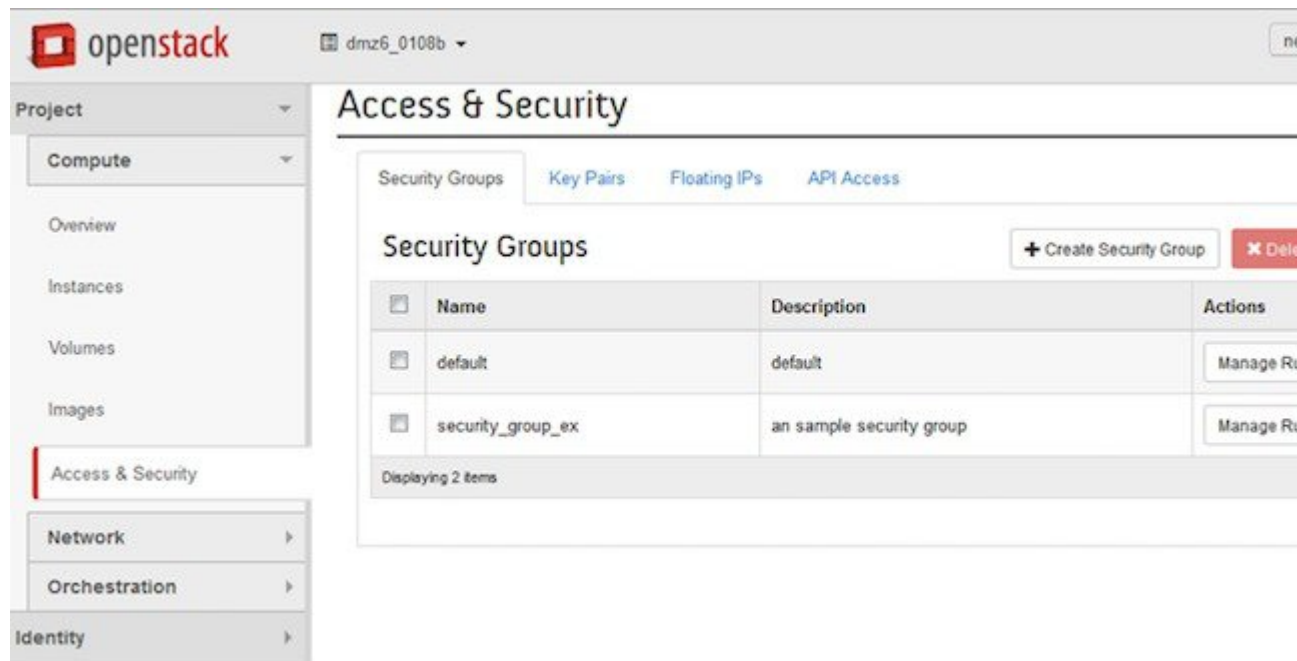
```
$fabric_enabler_cli
Cisco Nexus Fabric Command Line Interface
(Nexus-Fabric) set_static_ip --mac fa:16:3e:72:ab:dc --ip 136.10.0.16
```

The MAC address is the VM's vNIC and the IP address is the statically configured VM IP address. When a VM is removed from OpenStack, the above entry is automatically removed by the system.

Steps to Create a Security Group

You need to create and add a security group with appropriate rules before launching the VM. Create a security group and security rules that allow DHCP (from DCNM) and your data traffic to go through. After logging into Horizon as a user, click **Project > Compute > Access Security**. Use the **Create Security Group** tab to create a security group. After a security group is created, it appears in the **Security Groups** tab. A newly added group *security_group_ex* is displayed in the following sample screen shot.

Figure 2: Access and Security



Click **Manage Rules** for the security group you just created and add new rules. For example, if the following rule displayed in the *Add Rule* screen shot is added for the security group, it will allow all traffic.

Figure 3: Add Rule

Add Rule

Rule *
Other Protocol

Direction
Ingress

IP Protocol
-1

Remote *
CIDR

CIDR
0.0.0.0/0

Description:
Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

Steps to Launch the VM

Follow these steps to launch the VM:

- 1 Click **Instances** and then click **Launch Instance**.
- 2 Click the **Image** drop-down menu and select the image.
By default, the *CirrOS* image is selected.
- 3 Specify a name for the Instance.
- 4 Select the **Security** tab and choose the security group created (it is recommended to uncheck the default rule and select the one you specified).
- 5 Click the **Networking** tab and select the network from the **Available network** list.

6 Click **Launch**.