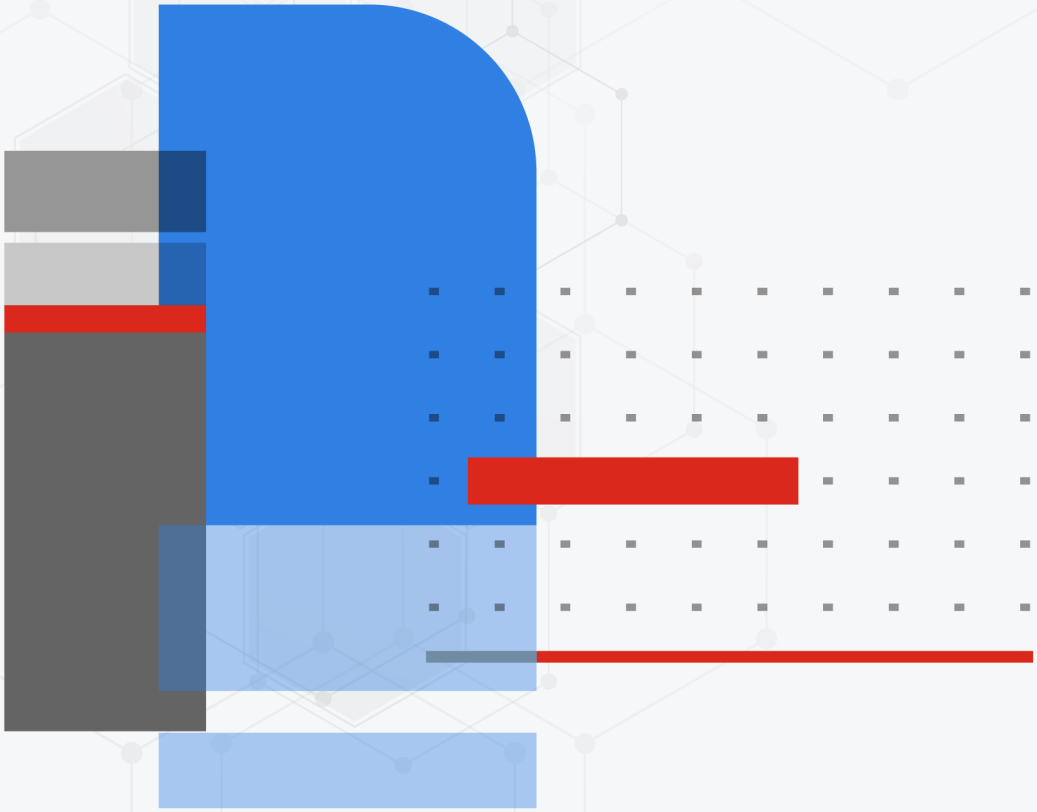
OpenStack Integration Guide

FortiADC 7.6.1



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 8, 2022
FortiADC 7.6.1 OpenStack Integration Guide
01-544-677187-20220608

TABLE OF CONTENTS

Change Log

Date	Change Description
10/16/2019	Second update, adding deploy FortiADC-VM in an OpenStack environment.
03/28/2018	First update, adding notes to the Important Notes section.
01/19/2018	Initial release.
10/10/2024	Openstack 2023.2 Octavia support.

Introduction

This document discusses the integration of FortiADC with OpenStack, providing detailed instructions on installing the FortiADC Octavia Driver and Agent on OpenStack, as well as creating virtual load balancers on FortiADC through the OpenStack Octavia service.

A strong understanding of OpenStack and the Octavia setup is required to successfully install and run the Fortinet drivers and agents.

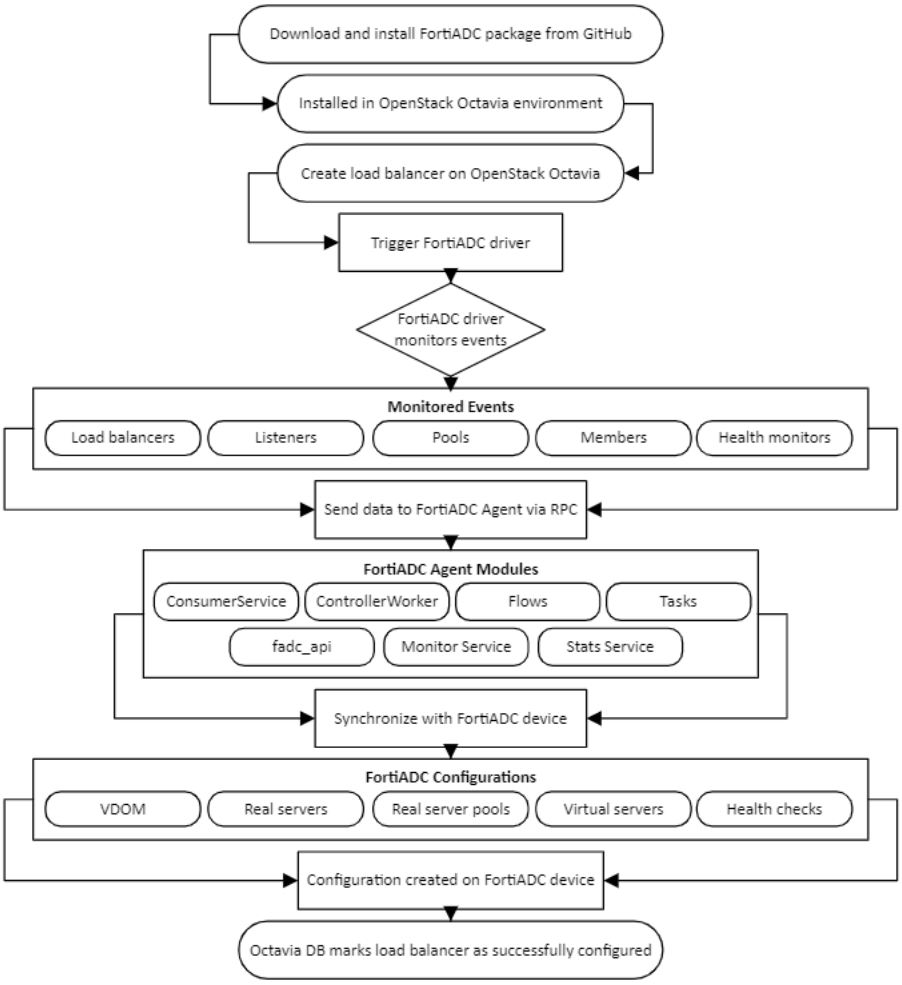
For more information about OpenStack, visit:

- OpenStack Community Forum at https://www.openstack.org/community/
- OpenStack Documentation at https://docs.openstack.org/2023.2/index.html

Implementation

FortiADC Octavia driver and agent in OpenStack environment

The diagram below illustrates the implementation of the FortiADC Octavia driver and agent within an OpenStack environment.

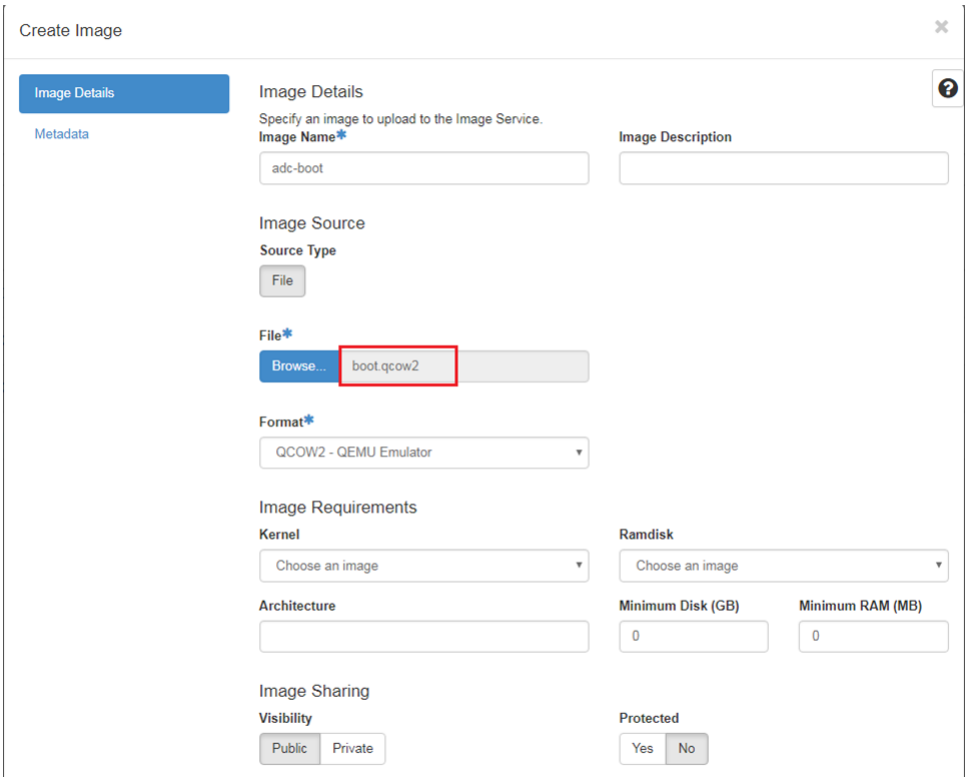


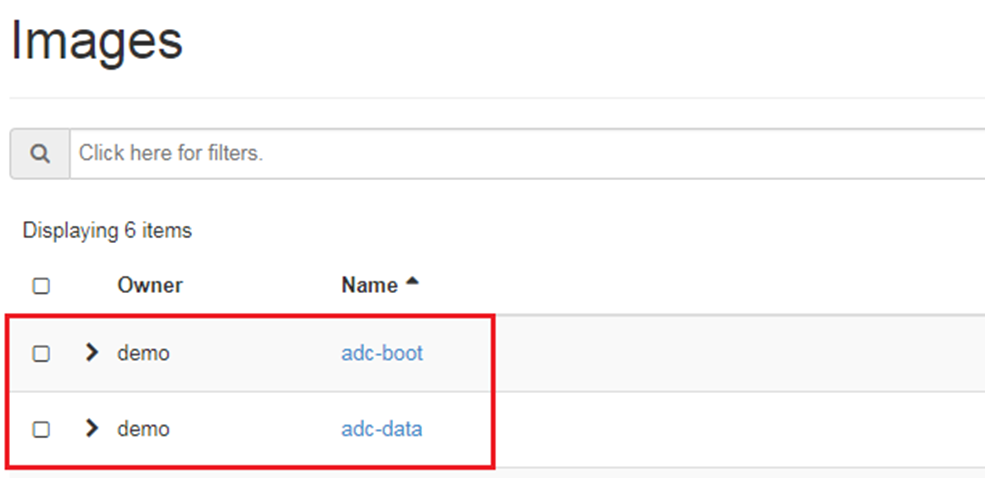
Deploying a FortiADC-VM instance in an OpenStack environment

Deploying a FortiADC-VM instance in an OpenStack environment

1. Creating boot and log images

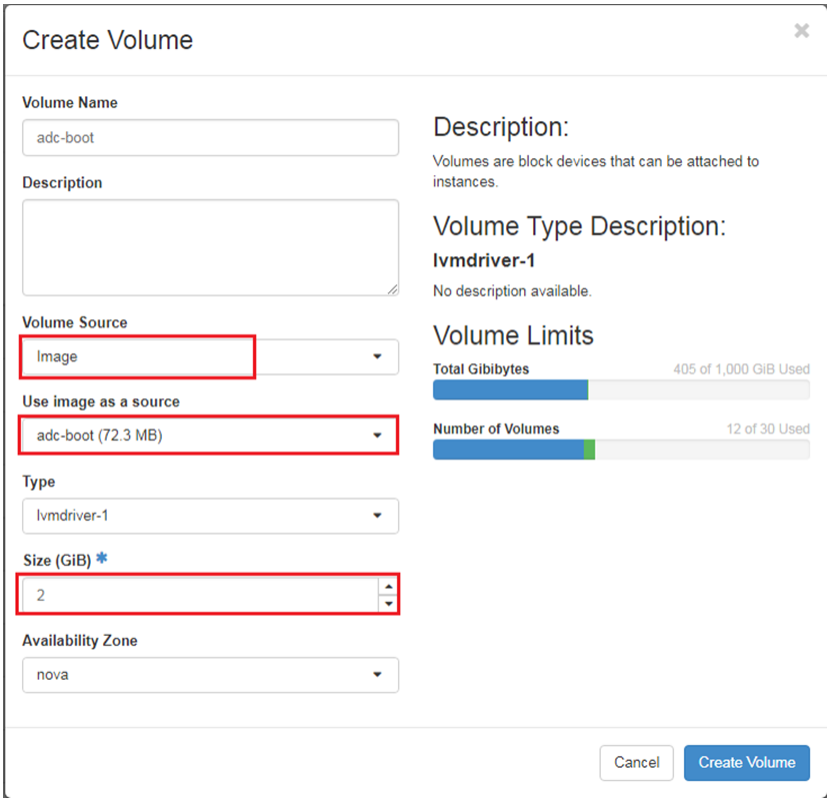
In **Project > Compute > Images**, use the Image File options to navigate to Image Details and select the boot.qcow2 and data.qcow2 file you extracted from the FortiADC-VM KVM software package. For **Format**, select **QCOW2-QEMU Emulator**.

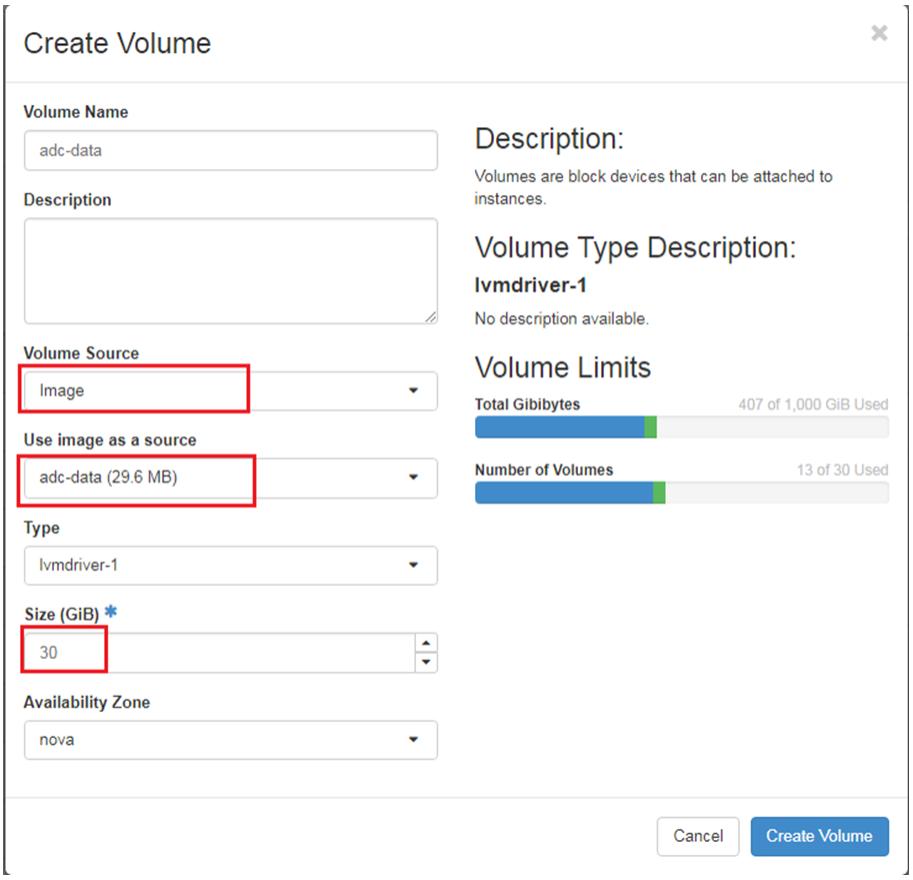


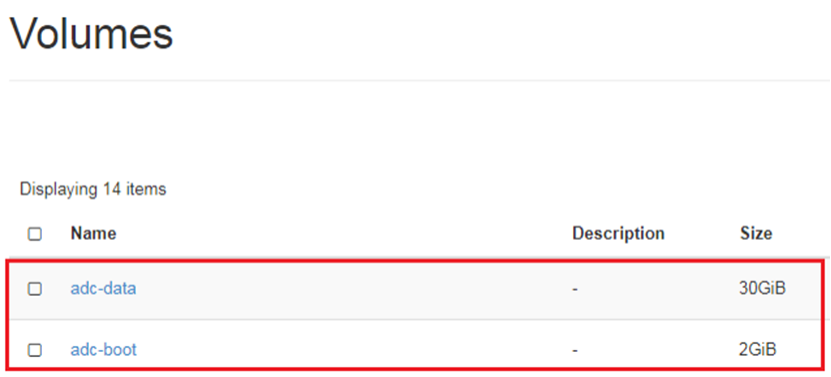


2. Creating Volume

To create the volume FortiADC-VM uses for its boot and log disk, navigate to **Project > Volumes > Volumes**. This step may take a while.

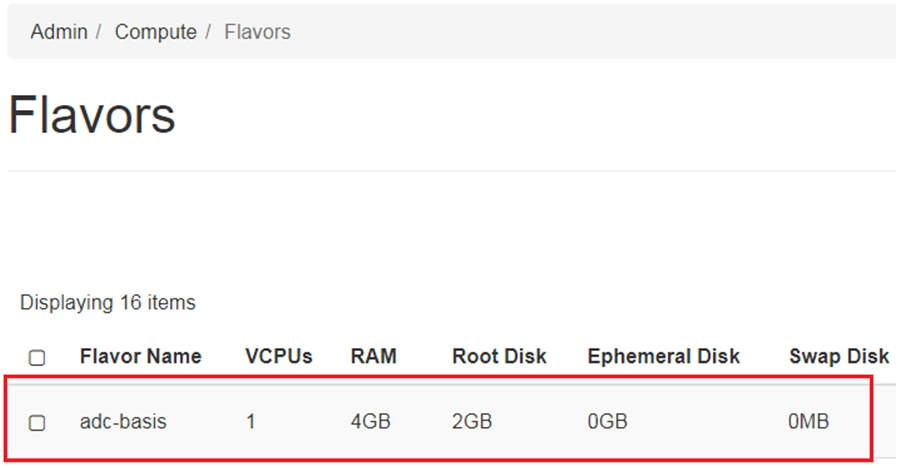






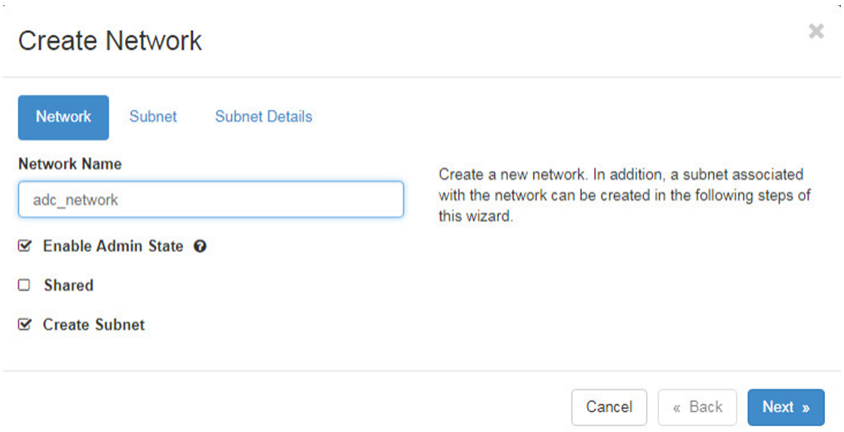
3. Creating Flavor

To specify the size of the instance, go to the OpenStack dashboard, navigate to **Admin > Compute > Flavors** and click Create Flavor. Complete the flavor settings.
We suggest selecting a compute flavor that has a minimum of 8 GB of memory.

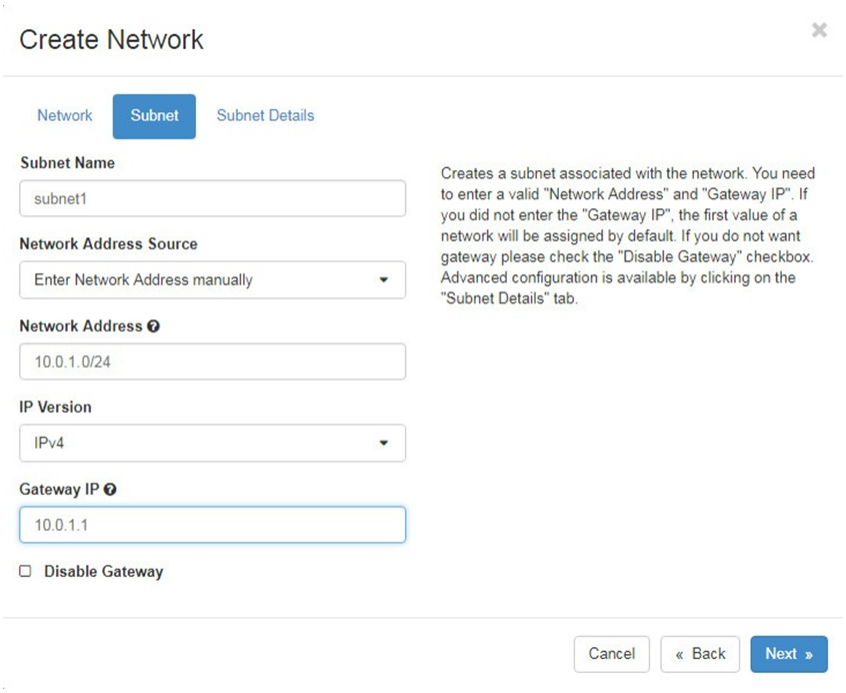


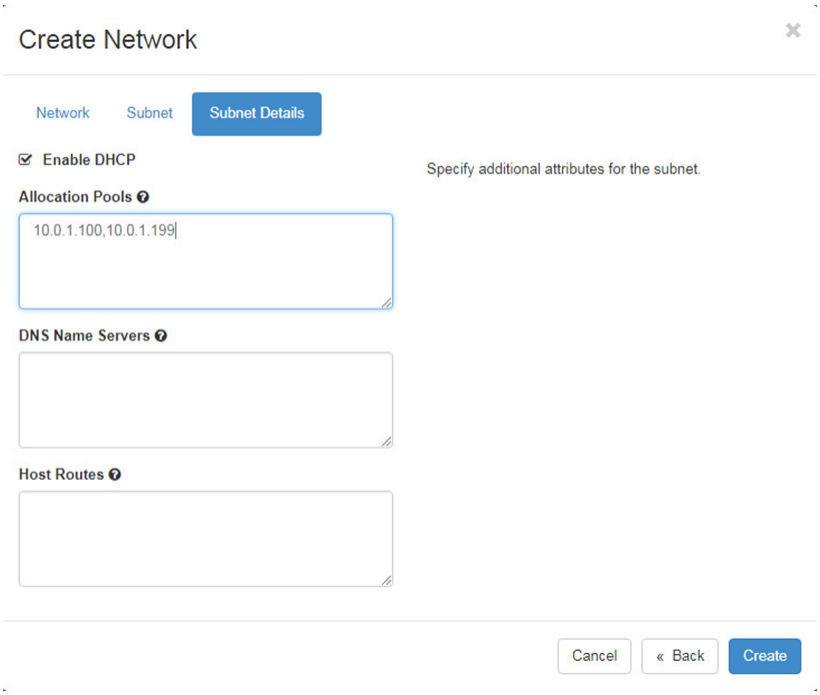
4. Creating Network

Navigate to **Project > Network > Networks**. In the network creation wizard, complete the network and subnet settings.to create Network, 10 Subnets and Ports.

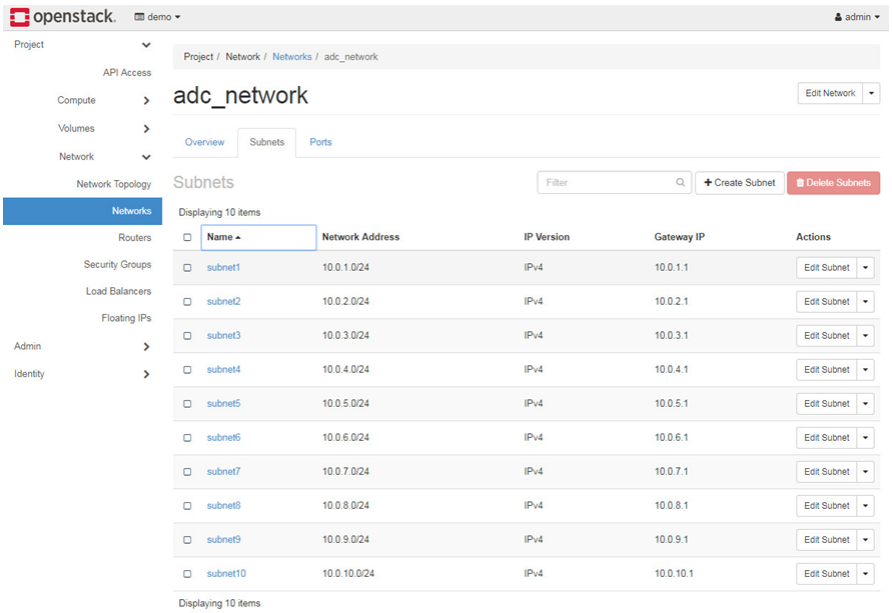


Create 'subnet1' when creating Network.

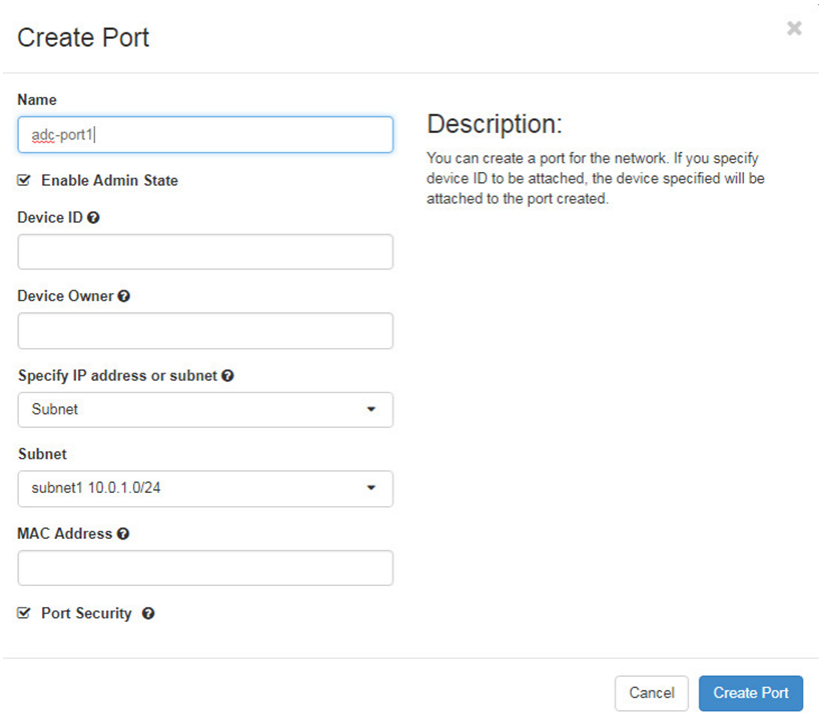


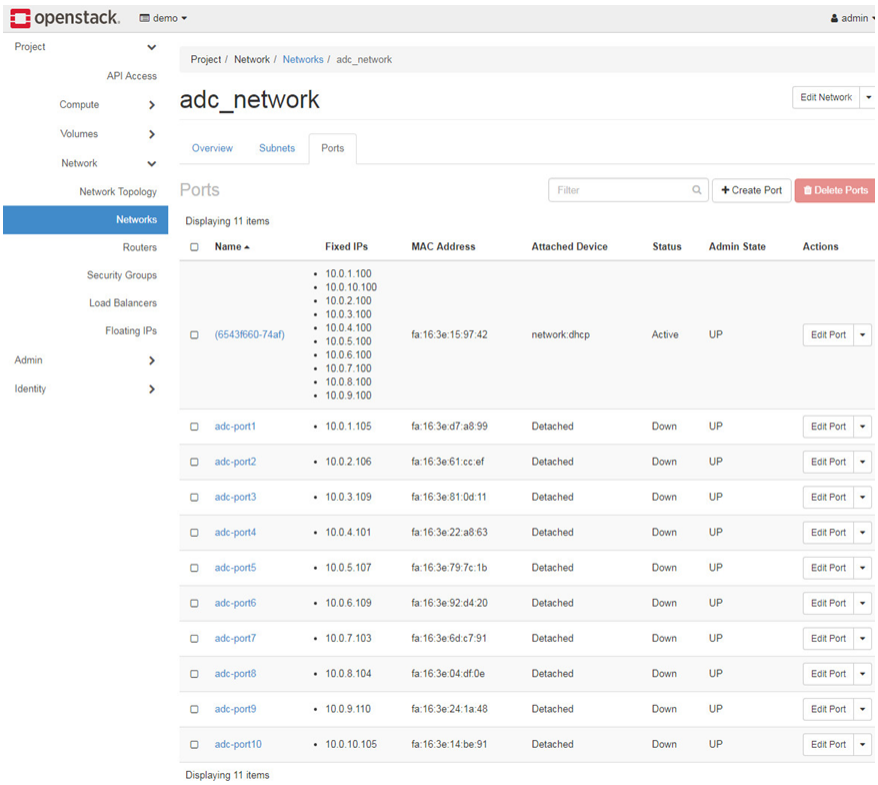


Click on the created network and create 9 more subnets.

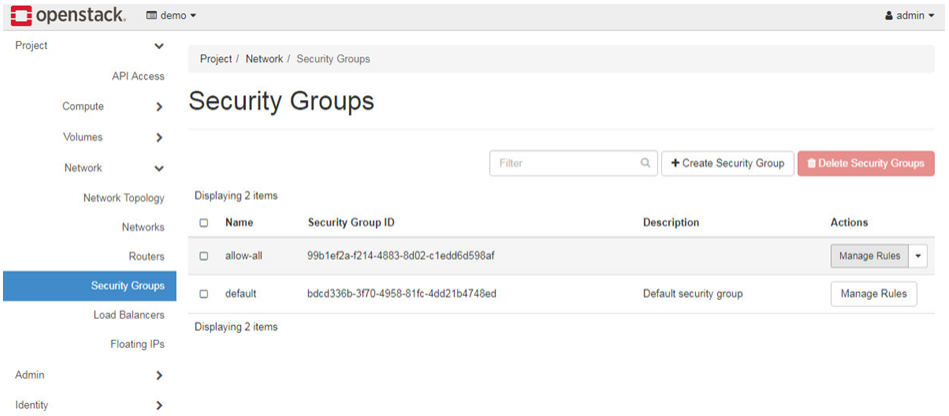


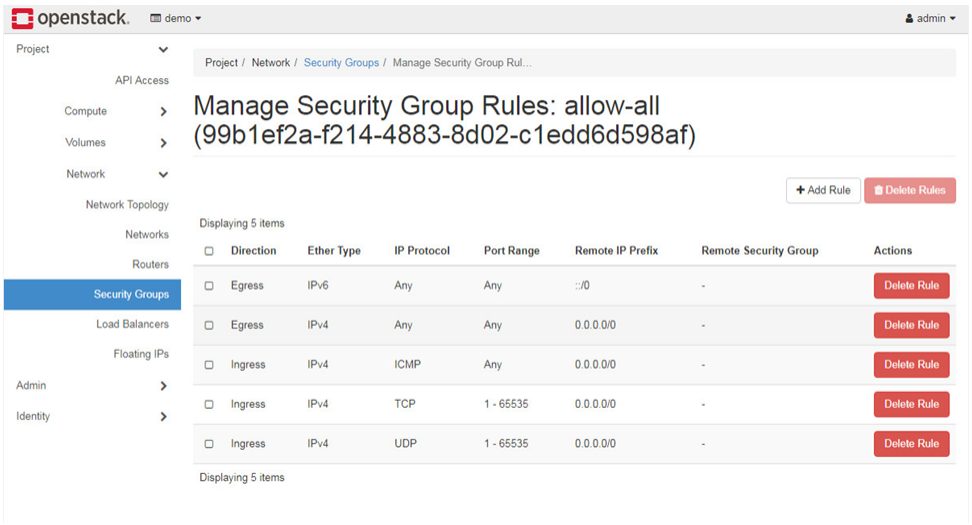
Click Ports tab and then create 10 ports in different subnets for FortiADC interfaces.



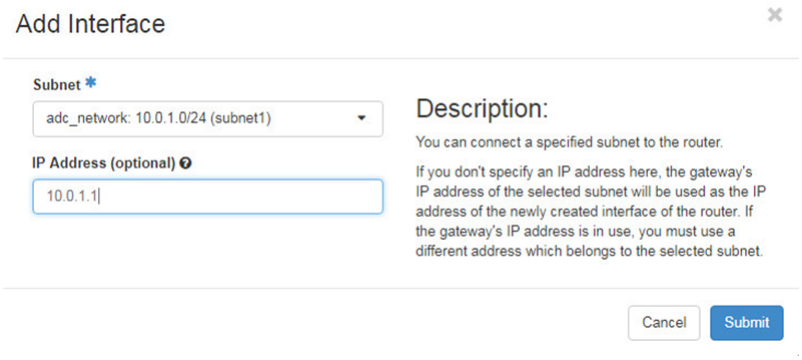


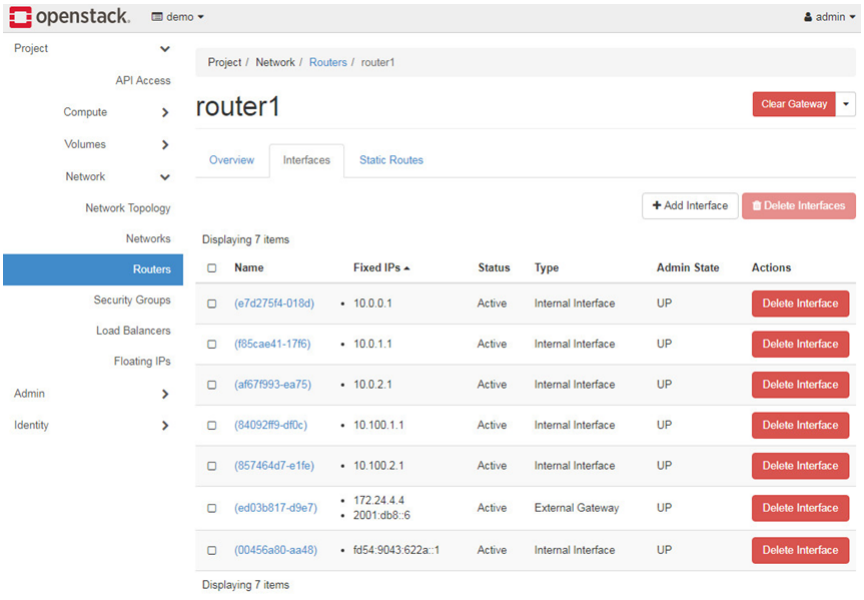
Configure **Security Group in Project > Network > Security Groups** to allow all.



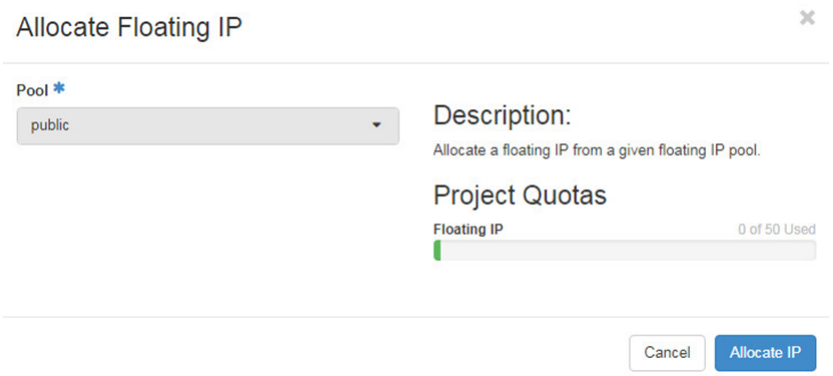


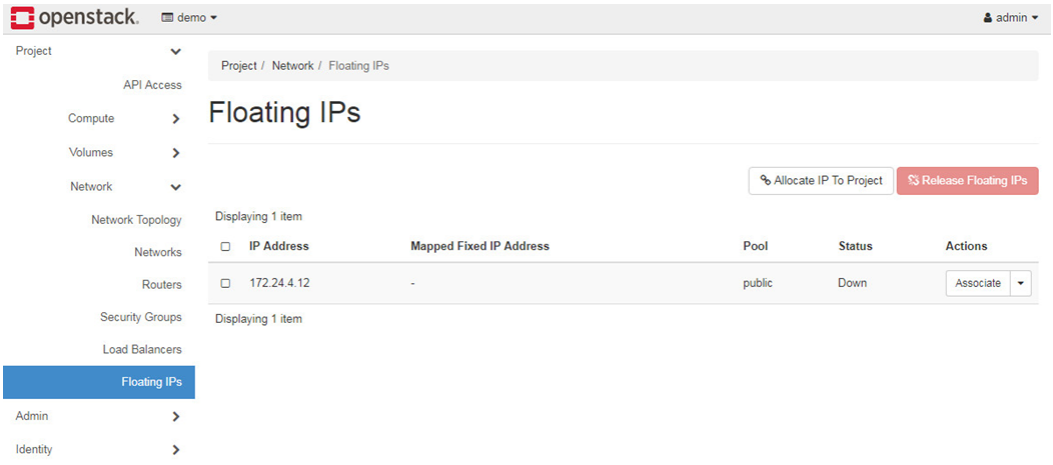
To the router, add subnets which need to be forwarded to the public network in **Project > Network > Routers.**





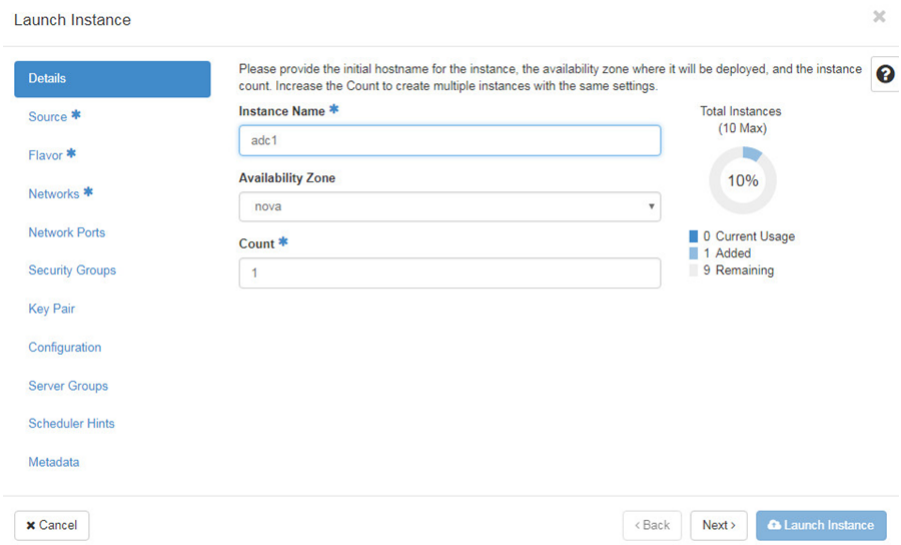
Allocate Floating IP in **Project > Network > Floating IPs**.



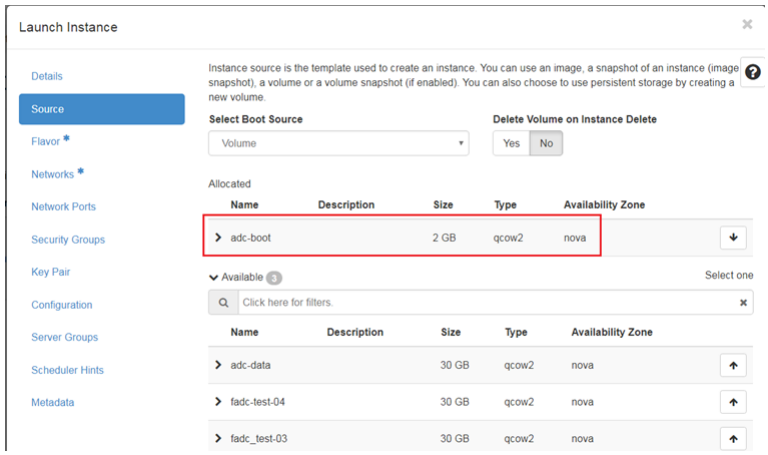


5. Creating Instance

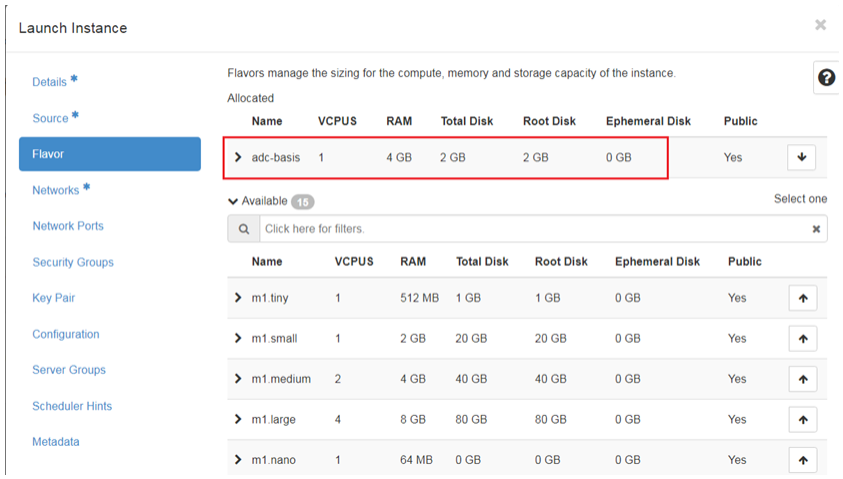
Create Instance in **Project > Compute > Instances.**



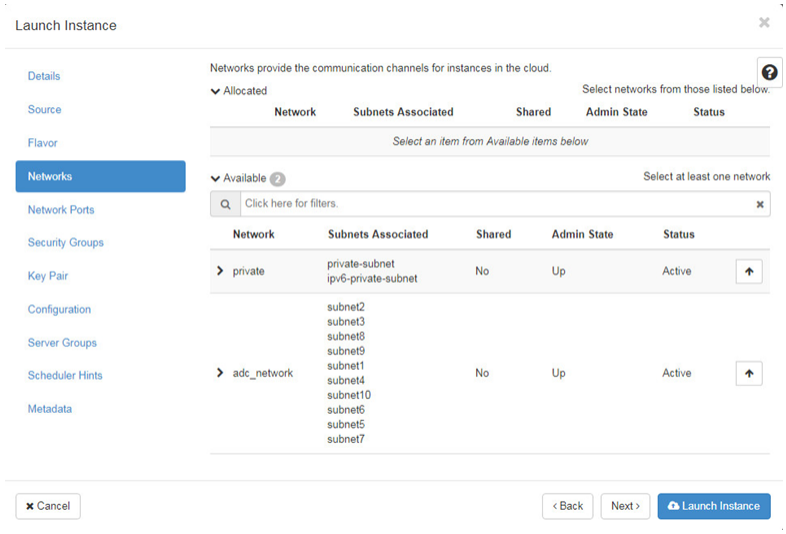
Select created boot disk in Volume.

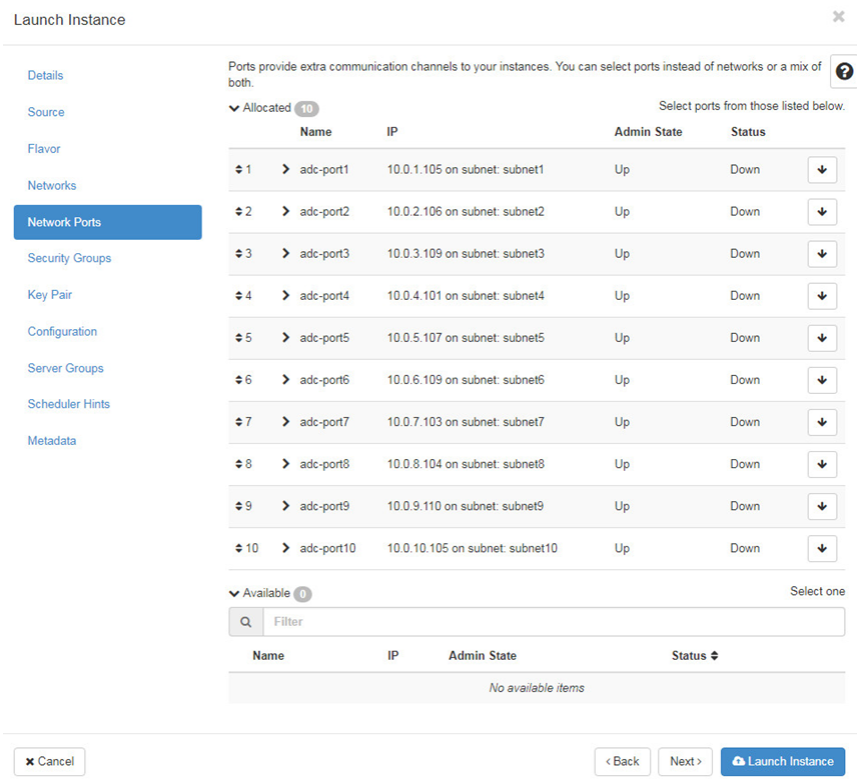


Select created flavor.

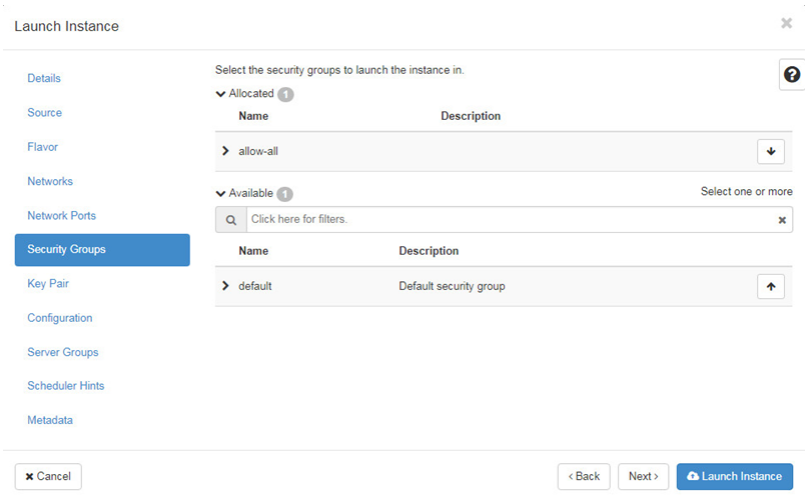


Do not select Networks. Add created Network Ports instead.

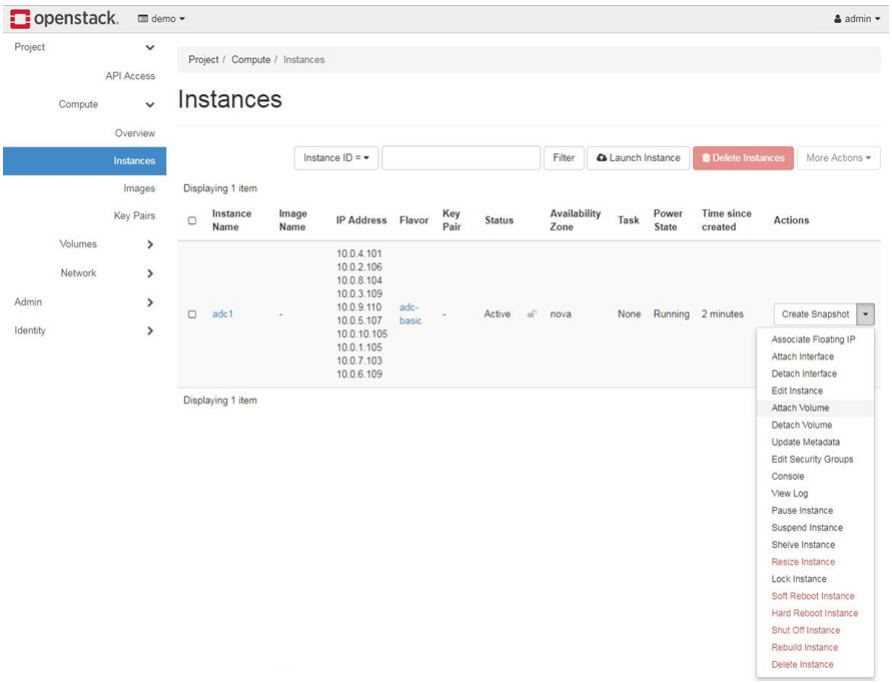




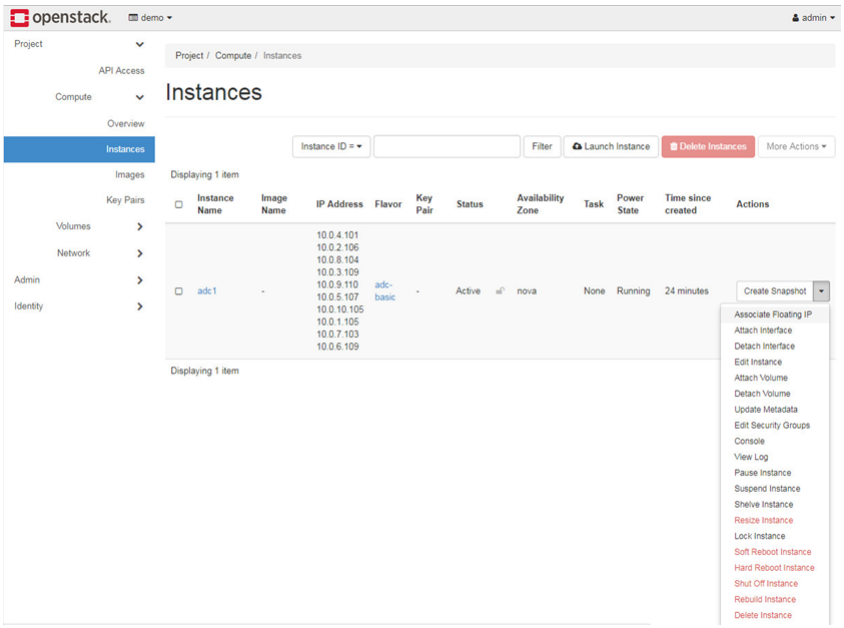
Configure Security Groups and then click "Launch Instance".



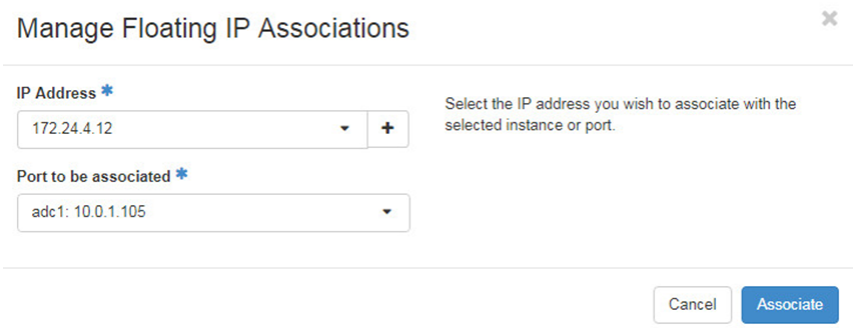
Because only boot disk can be configured during instance creation, attach data disk is needed for the FortiADC instance.



Assign Floating IP 172.24.4.x in public network to Instance.

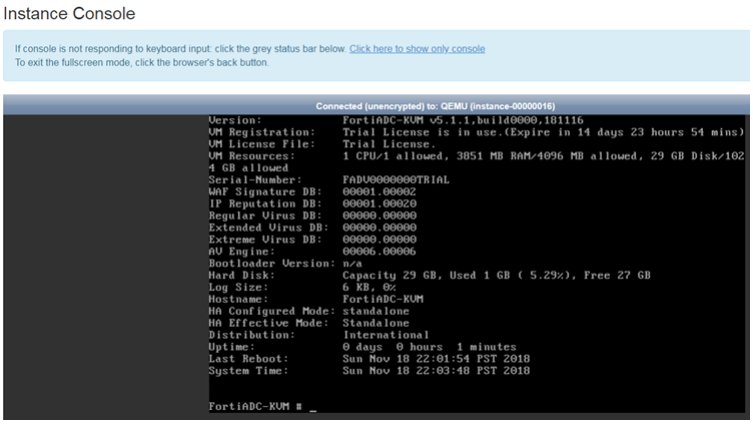


The associated port needs to be in the subnet whose gateway was added in Router in the previous step.



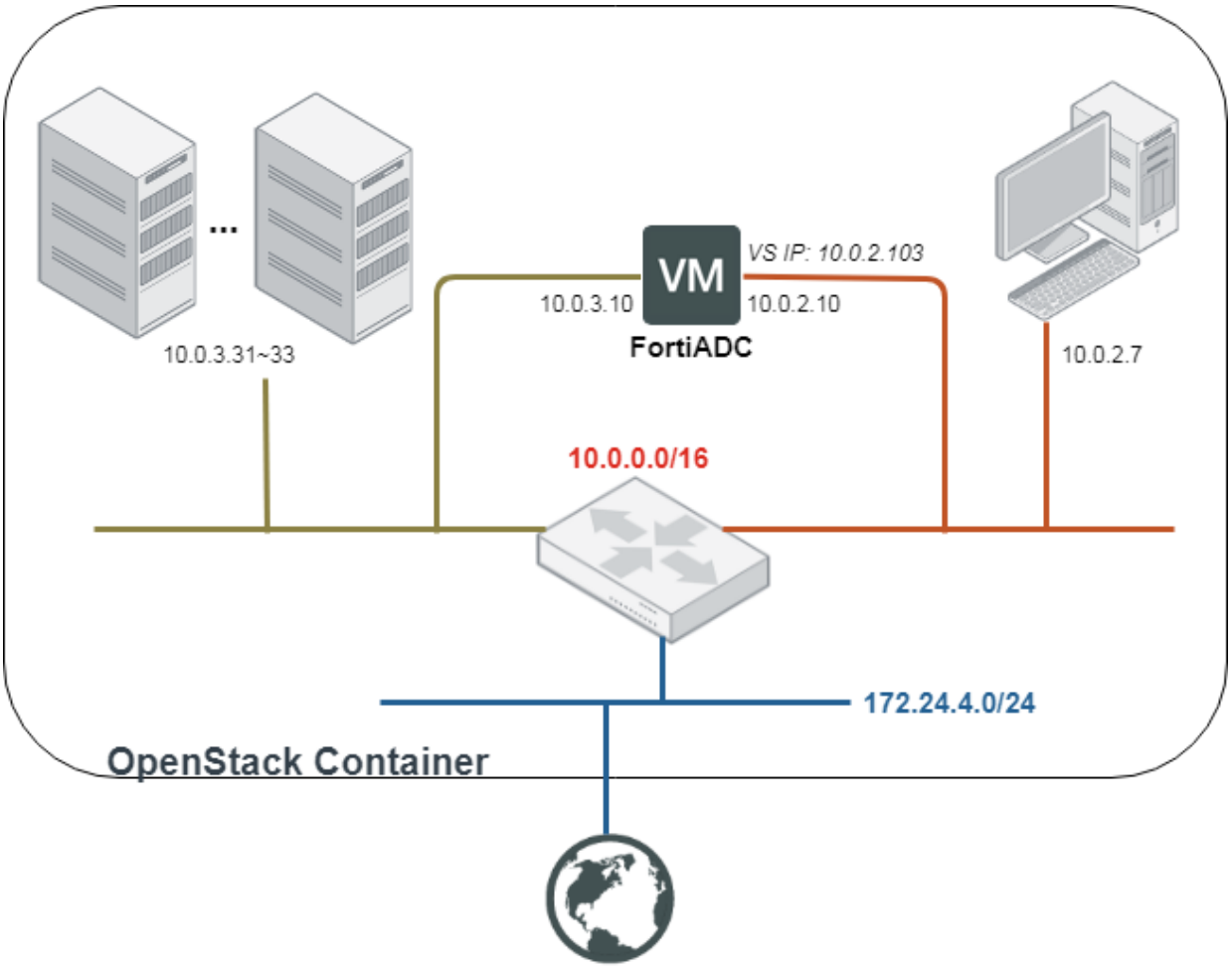
6. Connect to console

Remember to reboot FortiADC Instance after attaching data volume.



Deployment

FortiADC can only be deployed within an OpenStack container environment.



The following are example configurations deployed on FortiADC through Octavia:

Configuring a virtual server:

```
config load-balance virtual-server
   edit "09e01bbc-4076-44ea-8d0e-558ab6503655"
      set type l7-load-balance
      set ip 10.0.2.103
      set load-balance-profile LB_PROF_HTTP
      set load-balance-persistence LB_PERSIS_HASH_SRC_ADDR
      set load-balance-method LB_METHOD_ROUND_ROBIN
      set load-balance-pool 3ed56621-9825-494a-9246-452e591f913e
   next
end
```

Configuring a real server pool:

```
config load-balance pool
   edit "3ed56621-9825-494a-9246-452e591f913e"
      set health-check-ctrl enable
      set health-check-list 7baa43a4-633b-4f35-af0d-02f9aedd9422
      set real-server-ssl-profile NONE
      config pool_member
         edit 1
            set pool_member_cookie rs1
            set real-server 38a40738-becf-4736-a16b-d3b131275f31
         next
         edit 2
            set pool_member_cookie rs2
            set real-server 0cc6107e-8848-4f39-80e3-873a788b9000
         next
         edit 3
            set pool_member_cookie rs3
            set real-server fef07534-ef8e-48a3-89d3-1db551b952a9
         next
      end
   next
end
```

Configuring real servers:

```
config load-balance real-server
   edit "38a40738-becf-4736-a16b-d3b131275f31"
      set ip 10.0.3.31
   next
   edit "0cc6107e-8848-4f39-80e3-873a788b9000"
      set ip 10.0.3.32
   next
   edit "fef07534-ef8e-48a3-89d3-1db551b952a9"
      set ip 10.0.3.33
   next
end
```

Installation requirements

FortiADC-OpenStack integration requires the following software packages:

- OpenStack 2023.2 release
- Octavia 2023.2
- FortiADC 7.4.3
- fadc-octavia-provider: 1.0.0

Installation procedures

Follow the steps below to install the FortiADC software package in your OpenStack environment.

Step 1: Verify your OpenStack environment

Ensure that the system is running OpenStack version 2023.2 with Octavia properly installed and configured.

Step 2: Download and extract the fadc-octavia-provider

1. Download the `fadc-octavia-provider.tar.gz` file from https://github.com/fortinet/fortiadc-openstack.
2. Extract the contents in your OpenStack installation environment using the command: `tar -zxvf fadc-octavia-provider.tar.gz`.

Step 3: Install the FortiADC Driver and Agent

1. Install the driver and agent:

   ```
   If the openstack installed on python virtual environment, it needs to go to
   virtual environment to install package.
   Run the "./install.sh" to install both driver and agent.
   ```

2. Modify `octavia.conf` in `/etc/oectavia/`:

   ```
   enabled_provider_drivers = amphora:The Octavia Amphora driver.,octavia:Deprecated
   alias of the Octavia Amphora driver.,ovn:Octavia OVN driver.,fortiadc_
   driver:fortiadc driver.
   default_provider_driver = fortiadc_driver

   Restart uwsgi service. It can enable Fortiadc driver.
   ```

Step 4: Start the FortiADC Agent

1. Configure the FortiADC Agent:
   The package includes an example configuration file named fadc_octavia_example.conf. Copy this file to `/etc/octavia/fadc_octavia.conf` and modify it with the appropriate values.
   Please ensure that the content of the `fadc_devices` section remains in JSON format after making any changes.

   ```
   fadc_devices = [
                 {
                  "fadc_FQDN": "172.24.4.223",
                  "fadc_username": "admin",
                  "fadc_password": "fortinet",
                  "fadc_vdom_network_mapping": "port2",
   ```

```
                "fadc_bind_vip_port_id": "69dd6263-203f-46ed-835d-327b9f0baf8d",
                "fadc_vdom_network_allowAccess": {"port2":"http ping telnet
https"},
                "fadc_vdom_network_ip": {"port2":"10.20.2.23/24"},
                "fadc_vdom_default_gw": "10.20.2.1",
                "fadc_vs_dev_intf": "port2",
                "fadc_vs_packet_forward_method": "FullNAT",
                "fadc_vs_persistency": "LB_PERSIS_HASH_SRC_ADDR",
                "fadc_get_stats_interval": "2",
                "fadc_vs_nat_pool": ["10.20.2.190","10.20.2.199"],
                "fadc_vs_nat_intf": "port2",
                "fadc_healthcheck_port": "80",
                "certificate_verify": false,
                "projects": [
                              "fe6cb031d610420394ba134f670488a6"
                            ]
              }
          ]
```

2. Install the FortiADC Agent Service:
   Locate the FortiADC agent path by executing the command: which fortiadc_agent in the environment where the fadc-octavia-provider package is installed.
   Then, run the installation script with the following command:

   ```
   sudo ./install_service.sh /path/to/fortiadc_agent
   ```

   To verify that the service has started successfully, use the command:

   ```
   ps -ef | grep fortiadc_agent
   ```

FortiADC Configuration Parameters for Deployment within an OpenStack Container:

Parameter	Description
Debug	
`debug_mode`	Enable or disable debug messages for fadc_api. True = enable False = disable
Device information	
`fadc_FQDN`	The FortiADC's IP address that OpenStack uses to communicate with it.
`fadc_username`	The FortiADC global user log-in name. Note: The default password is `admin`.
`fadc_password`	The FortiADC log-in password. Note: It's blank (no password) by default.
Network	
`fadc_vdom_network_`	The interfaces assigned to the virtual domain.

Parameter	Description
mapping	
fadc_bind_vip_port_id	The bind virtual interface port ID.
fadc_vdom_network_ allowAccess	The applications that the interface allows to access. The value can be HTTPS, HTTP, SNMP, SSH, Ping, and Telnet.
fadc_vdom_network_ip	The IP addresses of the assigned interfaces.
fadc_default_gw	The static route with destination 0.0.0.0/0 in the VDOM.
Virtual server	
fadc_vs_dev_intf	The virtual server interface.
fadc_vs_persistency	The name of the persistence profile in the virtual server.
fadc_vs_packet_ forward_method	The packet-forwarding method in Layer-4 virtual servers. It can be NAT or FullNAT. Note: This applies to Layer-4 virtual servers only.
fadc_vs_nat_pool	The IP address range of the NAT source pool. Note: This applies to Layer-4 virtual servers with NAT only.
fadc_vs_nat_intf	The interface of the NAT source pool. Note: This applies to Layer-4 virtual servers with NAT only.
fadc_get_stats_ interval	The amount of data shown on the FortiADC's FortiView page: • 0=One hour's worth of data • 1=Six hours' worth of data • 2=One day's worth of data • 3=One week's worth of data • 4=One month's worth of data • 5=One year's worth of data
Health check monitor port	
fadc_healthcheck_port	The port number for FortiADC to create healthcheck profiles. The default is 80. Valid values range from 0 to 65535. Note: This applies to HTTP, HTTPS, and TCP only.

Validation

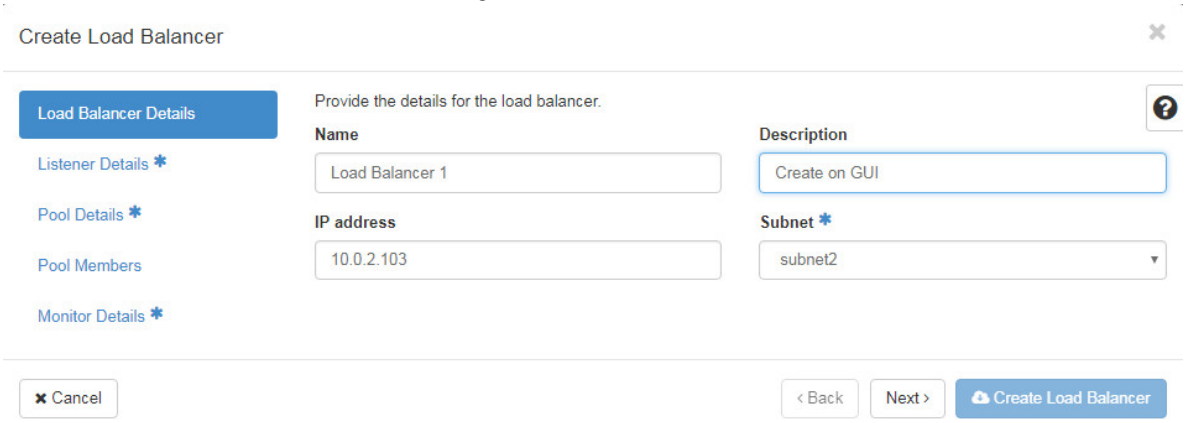
After completing the installation of `fadc-octavia-provider 1.0.0`, the next step is to validate the installation to ensure everything is functioning correctly.

To validate your installation:

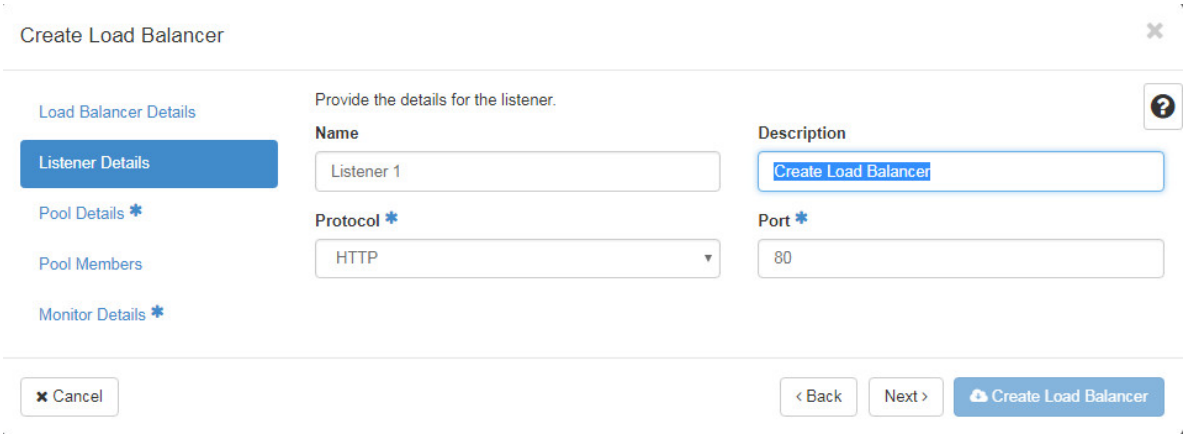
Step 1: Create a load balancer in OpenStack.

From the OpenStack GUI, select Project > Network > Load Balancers to open the Create Load Balancer page, and then follow the tabs on the left to configure the load balancer.

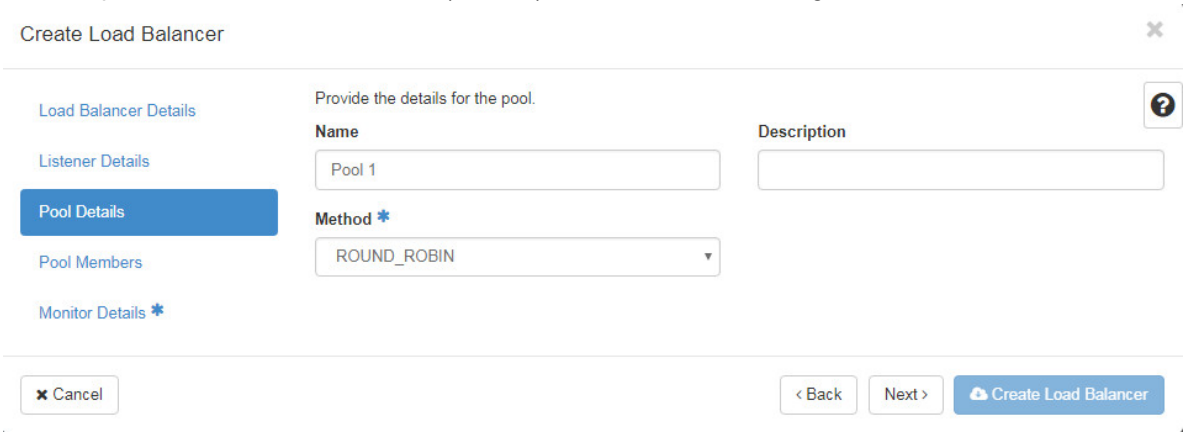
1. Click the Load Balancer Details tab to configure the load balancer.



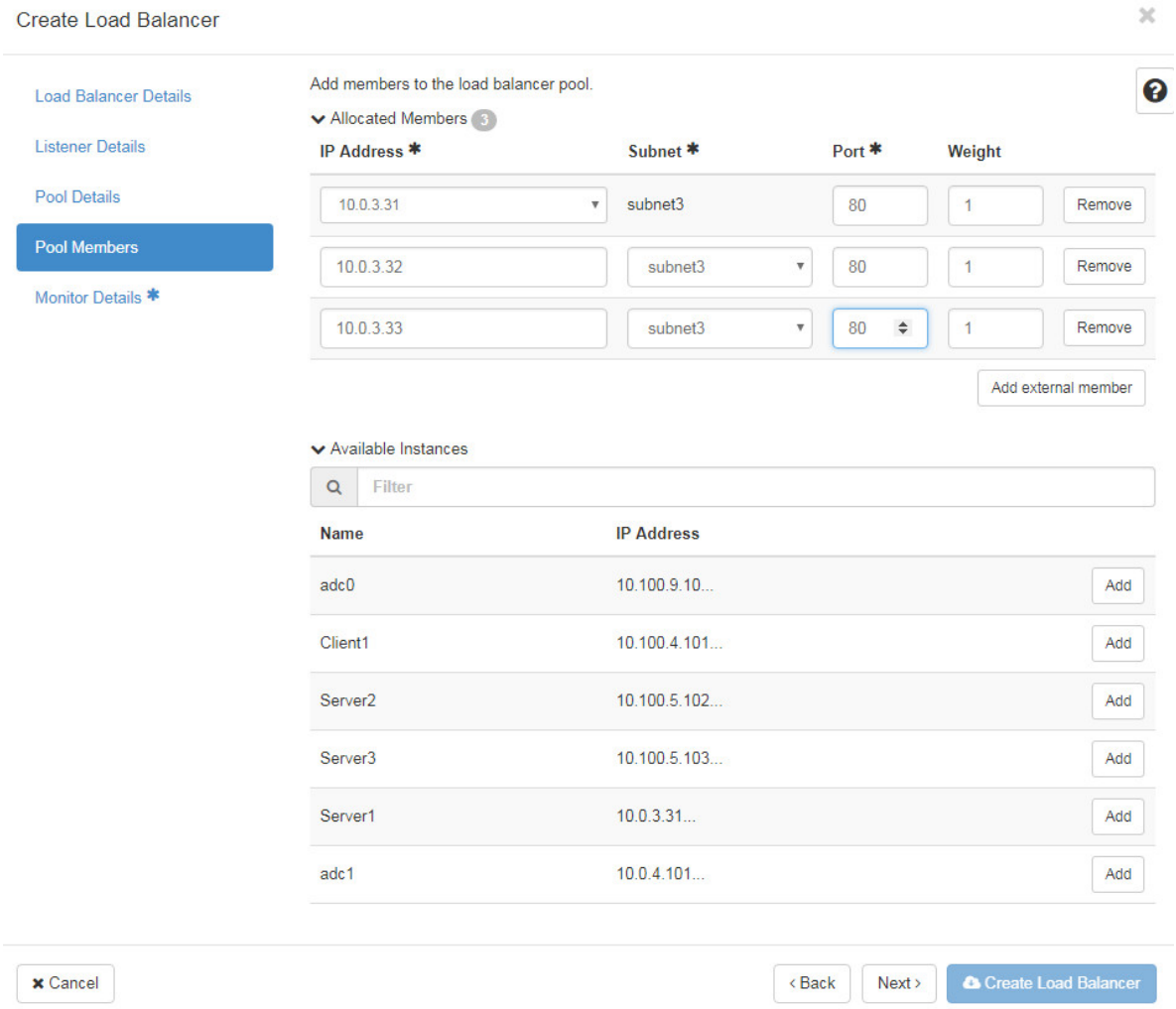
2. Click the Listener Details tab to configure the listener.
Load balancers listen for requests on multiple ports, each of which is specified by a listener.



3. Click Pool Details to configure the server pool.
   A server pool contains a list of members(servers) that serve content through the load balancer.

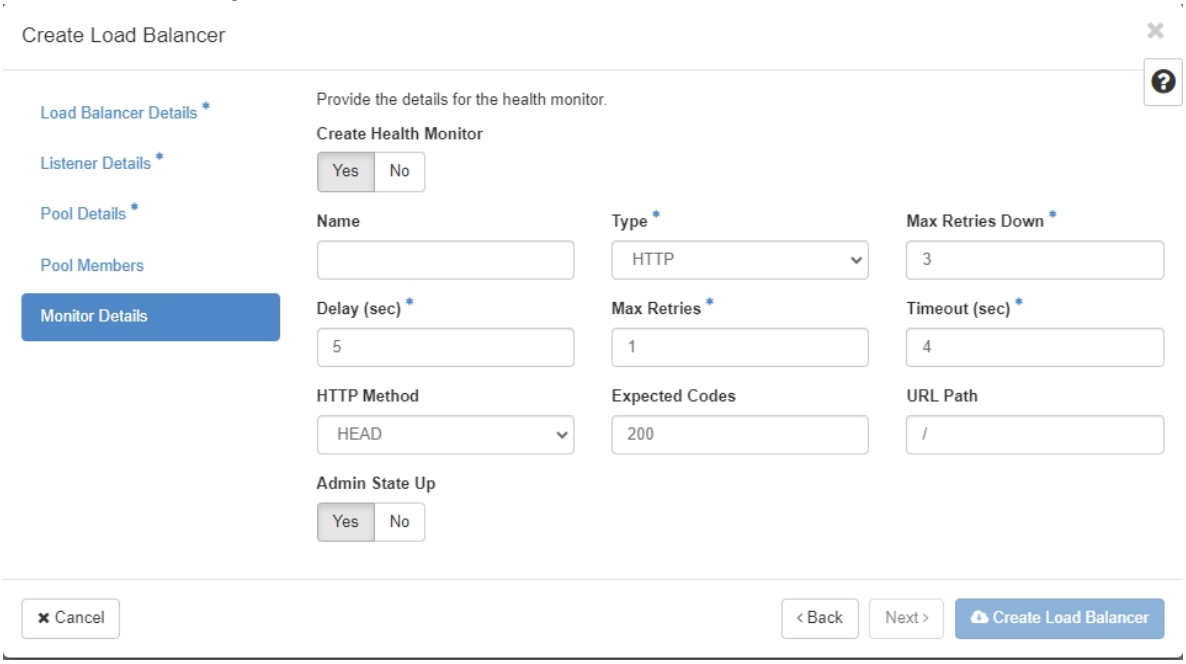


4. Click Pool Members to add servers to the server pool.
   Pool members are servers that handle traffic behind a load balancer. Each member is identified by the IP address and port it uses to serve traffic.



5. Click Monitor Details to configure the health monitor.
   Health monitors keep track of the health of pool members. They divert traffic away from members that are

offline or non-responsive.
For the monitor type **HTTP**, it is recommended to select **HEAD** instead of **GET**. The suggested HTTP health monitor settings are as follows:



Ensure that the Timeout value is set to be less than the Interval value for optimal FortiADC performance.

Step 2: Verify the load balancer configuration in FortiADC.

If your configuration of the load balancer in OpenStack is successful, the project ID that you created in OpenStack should show up in the Name column of the Virtual Domain page on the FortiADC GUI . In other words, the OpenStack project ID becomes the name of the virtual domain in FortiADC.

To verify your load balancer configuration:

1. Log into your FortiADC GUI.
2. Make sure that your Project ID in OpenStack appears in the Name column of the Virtual Domain page.

Key Considerations for Integrating FortiADC with OpenStack

The following key considerations must be kept in mind when integrating FortiADC with OpenStack.

Monitor Configuration for Load Balancer:

- When configuring the monitor details in OpenStack, ensure that the **Timeout** value is set lower than the **Interval** value for optimal performance.

Network Interface Changes:

- If the network interfaces of a FortiADC instance change in OpenStack, you must enable the retrieve_physical_hwaddr setting for the physical ports via the CLI, then reboot the FortiADC appliance. This ensures that FortiADC correctly updates the MAC addresses for the physical ports.
- By default, `retrieve_physical_hwaddr` is not enabled. If network ports are changed in an OpenStack VM, access the FortiADC console and manually enable this setting for the modified ports.

Algorithm Support:

- FortiADC does not support `SOURCE_IP` as an `lb_algorithm` and will default to the Round Robin (RR) algorithm instead.

Virtual Server Creation:

- You cannot create a virtual server if `fadc_vs_persistency` is not supported in the virtual server profile specified in the `fadc_octavia.conf` configuration file.

FortiADC and OpenStack Octavia Value Range Differences:

- **Connection limit**: Starts at `-1` in Octavia, but at `0` in FortiADC. Setting Octavia to 0 or -1 will set the FortiADC connection limit to 0.
- **Pool Member Weight**: Octavia allows a weight range of `0-256`, while FortiADC allows `1-256`. FortiADC will not change the current weight if configured to `0`.
- **Delay and Timeout**: FortiADC's delay and timeout range is `1-3600`, and the **Timeout** value must be less than the **Interval**. Octavia does not have this restriction.

Octavia Agent Capabilities:

- The FortiADC Octavia agent does not support High Availability (HA).
- It only supports Layer 7 (L7) HTTP/HTTPS and Layer 4 (L4) TCP for load balancer creation.

L4 TCP Packet Forwarding:

- L4 TCP supports two packet forwarding methods: **DNAT** and **Full NAT**. Configure `fadc_vs_packet_forward_method` to specify the packet forwarding method for the L4 virtual server. Acceptable values are

`NAT` or `FullNAT`.

NAT Pool for L4 TCP Full NAT:

- A NAT pool is supported exclusively in L4 TCP with Full NAT. Use the following format to define the NAT pool:

  ```
  fadc_vs_nat_pool = ['172.24.4.130', '172.24.4.135']  # Address range from
  172.24.4.130 to 172.24.4.135
  ```

  The parameter `fadc_vs_nat_intf` can be set to specify the interface for the NAT source pool. These parameters apply only to the TCP listener (L4 TCP) with Full NAT packet forwarding.

Address Pair Limits:

- The maximum number of allowed address pairs for a single network port is 10. This means users can create up to 9 load balancers on one ADC port, excluding configurations for the NAT source pool.

Manual Address Pair Configuration for L4 Full NAT:

- When using L4 Full NAT with a NAT source pool, the IP addresses in the pool must be manually added to the allowed address pairs on the ADC port.

Security Rules for Load Balancers:

- Security rules for load balancers must be added manually, or you can disable port security on the specific port or the entire network.

Reboot After Adding Data Disk:

- After deploying FortiADC in OpenStack and adding a data disk, reboot the instance to update its hardware information.

www.fortinet.com