VMware Integrated OpenStack Administration Guide

13 MAY 2021

VMware Integrated OpenStack 7.1

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

VMware Integrated OpenStack Administration Guide

1

The *VMware Integrated OpenStack Administration Guide* shows you how to perform administrative tasks in VMware Integrated OpenStack, including how to create and manage projects, users, accounts, flavors, images, and networks.

Intended Audience

This guide is for cloud administrators who want to create and manage resources with an OpenStack deployment that is fully integrated with VMware vSphere®. To do so successfully, you should be familiar with the OpenStack components and functions.

Terminology

For definitions of terms as they are used in this document, see the VMware Glossary at https://www.vmware.com/topics/glossary and the OpenStack Glossary at https://docs.openstack.org/doc-contrib-guide/common/glossary.html.

Deployment Configuration 2

You can modify the configuration of your VMware Integrated OpenStack deployment to add capacity, enable profiling, update credentials, and change or customize various settings.

This chapter includes the following topics:

Update Deployment Capacity

You can scale out the nodes, services, clusters, and datastores in your VMware Integrated OpenStack deployment to adapt to higher load.

Add Controller Nodes to Your Deployment

You can scale out your deployment by adding more controller nodes.

Note The following limitations apply to controller nodes:

- Ensure that you have sufficient resources before initiating a scale-out operation.
- Do not reduce the number of controller nodes in a deployment.
- Do not delete the controller nodes through vSphere as it can cause unexpected behavior. For details, see KB 82608.

Procedure

1. Log in to the Integrated OpenStack Manager web interface as the `admin` user.
2. In **OpenStack Deployment**, click the name of your deployment and open the **Nodes** tab.
3. Click **Scale Out Controller Node**.
4. Enter the desired number of controller nodes and click **OK**.

Results

The new controller nodes are created. Once the nodes are displayed in the table and their status has changed to `Ready`, they can be used as part of your deployment.

Scale OpenStack Services

You can dynamically scale OpenStack services in or out to adapt to a changing system load.

Note VMware Integrated OpenStack does not support scaling the following services in or out:

- Gnocchi
- Ingress
- MariaDB
- Memcached
- Nova compute
- RabbitMQ

Do not attempt to scale these services in or out using the web interface, command-line interface, or API.

Procedure

1. Log in to the Integrated OpenStack Manager web interface as the `admin` user.
2. In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.
3. On the **Services** tab, find the desired OpenStack component and select **Actions > Scale out**.

4 For each service in the component, enter the desired number of pods.

Note The maximum number of replicas for each service cannot be greater than the number of worker nodes.

5 Click **OK**.

Results

Service pods are created or terminated to reach the specified number.

Add Compute Clusters to Your Deployment

You can add compute clusters to your VMware Integrated OpenStack deployment to increase processing capacity.

Prerequisites

Note If you want to add compute clusters from a separate vCenter Server instance, you must deploy VMware Integrated OpenStack with NSX-T Data Center networking. Other networking modes do not support adding compute clusters from separate vCenter Server instances.

If you have added resources to your vSphere environment after deploying OpenStack, refresh your vCenter Server instance before proceeding.

1 Log in to the Integrated OpenStack Manager web interface as the `admin` user.

2 In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.

3 On the **Settings** tab, click **vCenter Credentials**.

4 In the **VC Resources** column for the desired vCenter Server instance, click **Refresh**.

Procedure

1 Log in to the Integrated OpenStack Manager web interface as the `admin` user.

2 In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.

3 On the **Compute** tab, click **Add**.

4 Under **Configure Nova computes**, click **Add**.

5 From the **vCenter Server** drop-down menu, select the vCenter Server instance containing the compute cluster that you want to add.

(NSX-T Data Center only) If the desired vCenter Server instance is not displayed, click the **Add** (plus sign) icon and enter its host name and credentials.

6 Enter an availability zone for the new compute cluster.

Compute clusters located in different vCenter Server instances cannot be in the same availability zone.

7 From the **Cluster name** drop-down menu, select the desired compute cluster.

8 Select one or more datastores for the compute cluster to consume and click **Submit**.

Results

The capacity of your deployment increases accordingly with the size of the additional compute cluster.

What to do next

You can add or remove datastores from a compute cluster by selecting the desired cluster and clicking **Edit**.

You can remove compute clusters from your deployment by selecting the desired cluster and clicking **Delete**. Ensure that all OpenStack instances in the cluster have been deleted before you remove the cluster.

Add Storage to the Image Service

You can increase the number of datastores available to the image service in your VMware Integrated OpenStack deployment.

Adding a datastore causes the image service to restart and might temporarily interrupt OpenStack services.

Prerequisites

Note If you want to add compute clusters from a separate vCenter Server instance, you must deploy VMware Integrated OpenStack with NSX-T Data Center networking. Other networking modes do not support adding compute clusters from separate vCenter Server instances.

If you have added resources to your vSphere environment after deploying OpenStack, refresh your vCenter Server instance before proceeding.

1 Log in to the Integrated OpenStack Manager web interface as the `admin` user.

2 In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.

3 On the **Settings** tab, click **vCenter Credentials**.

4 In the **VC Resources** column for the desired vCenter Server instance, click **Refresh**.

Procedure

1 Log in to the Integrated OpenStack Manager web interface as the `admin` user.

2 In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.

3 Open the **Glance** tab and click **Add**.

4 From the **vCenter Server** drop-down menu, select the vCenter Server instance containing the compute cluster that you want to add.

(NSX-T Data Center only) If the desired vCenter Server instance is not displayed, click the **Add** (plus sign) icon and enter its host name and credentials.

5 Select one or more datastores to add and click **Next**.

6 Review the proposed configuration and click **Submit**.

Results

The storage capacity for the image service increases accordingly with the size of the additional datastore.

What to do next

You can select a datastore and click **Delete** to remove it from the image service.

Add Clusters to the Block Storage Service

You can add clusters to the block storage service to increase storage capacity for volumes.

Prerequisites

Note If you want to add compute clusters from a separate vCenter Server instance, you must deploy VMware Integrated OpenStack with NSX-T Data Center networking. Other networking modes do not support adding compute clusters from separate vCenter Server instances.

If you have added resources to your vSphere environment after deploying OpenStack, refresh your vCenter Server instance before proceeding.

1 Log in to the Integrated OpenStack Manager web interface as the `admin` user.

2 In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.

3 On the **Settings** tab, click **vCenter Credentials**.

4 In the **VC Resources** column for the desired vCenter Server instance, click **Refresh**.

Procedure

1 Log in to the Integrated OpenStack Manager web interface as the `admin` user.

2 In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.

3 On the **Cinder** tab, click **Add**.

4 From the **vCenter Server** drop-down menu, select the vCenter Server instance containing the compute cluster that you want to add.

(NSX-T Data Center only) If the desired vCenter Server instance is not displayed, click the **Add** (plus sign) icon and enter its host name and credentials.

5 Select **VMDK** or **FCD** as the back-end driver.

6 Enter an availability zone for the new cluster.

7 From the table, select the desired compute cluster.

Results

The capacity of the block storage service increases accordingly with the size of the additional cluster.

What to do next

You can remove clusters from your deployment by selecting the desired cluster and clicking **Delete**.

Update Deployment Networks

If you deployed the management network and API access network without DHCP, you can add IP address ranges and change DNS servers after deployment.

You cannot modify networks that use DHCP. Modifying the DNS settings will briefly interrupt the network connection.

Procedure

1. Log in to the Integrated OpenStack Manager web interface as the `admin` user.
2. In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.
3. On the **Network** tab, select the network that you want to modify.
   - To add an IP address range, select **Add IP Range** and enter the IP address range that you can add to the network.

     In the dialog box displayed, you can click **Add IP Range** again for adding multiple IP address ranges at once.

     Important The Management and the API access networks cannot include more than 100 IP addresses each.
   - To change the DNS servers for new controllers, select **Change DNS**.

     For example, DNS=**`192.168.10.11 192.168.10.12`**.

     1. In the dialog box displayed, enter the DNS server for DNS1.

        DNS1: **`192.168.10.11`**
     2. To add new DNS servers to the network, click **Add DNS**.
     3. Enter the new DNS server for DNS2.

        DNS2: **`192.168.10.12`**
     4. Click **OK**. You can see that the new DNS server is present on each of the Management and the API networks.

5 You can use the following command for changing DNS server on existing controllers. New DNS server can be used for new controllers created after this change.

```
/etc/systemd/resolved.conf
systemctl restart systemd-resolved
systemd-resolve --status
```

Note You can use generic DNS server addresses for verifying the configuration changes. DNS servers for both the Management and the API networks are the same and in one line. DNS server from the Management network is at the beginning.

- To change the DNS servers for the vio manager:

  1 Edit the DNS server setting.

  ```
  /etc/systemd/resolved.conf
  ```

  For example, DNS=**172.20.3.41 172.30.3.42**.

  You can only use the DNS server from the Management network.

  2 Restart the DNS server.

  ```
  systemctl restart systemd-resolved
  ```

  3 Verify the DNS server status.

  ```
  systemd-resolve --status
  ```

  4 Delete the coredns pods.

  5 Add the new DNS server to the vio manager.

  ```
  ovfenv -k vami.DNS.vio-manager --value <new dns server>
  ```

  For example, `ovfenv -k vami.DNS.vio.manager --value "172.30.3.41,170.30.3.42"`.

Update Deployment Credentials

You can modify the credentials with which your VMware Integrated OpenStack deployment accesses and connects with your NSX Manager and vCenter Server instance.

- If you want to change the password for VMware Integrated OpenStack Manager Web UI admin user, see viocli reset Command.
- If you want to change the password for OpenStack KeyStone admin user, see Update the Keystone Admin Password .

Procedure

1 Log in to the Integrated OpenStack Manager web interface as the `admin` user.

2 In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.

3 On the **Settings** tab, update the desired credentials.

- To update the credentials for a vCenter Server instance, select **vCenter Credentials**. You can click **Add** to add an instance to your deployment, or select an existing instance and click **Edit** or **Delete**.
- To update the credentials for NSX-T Data Center, select **NSX-T Credentials**, select your credentials, and click **Edit**.

4 Enter the desired credentials and click **OK**.

Enable Deployment HA

If you deployed VMware Integrated OpenStack in non-HA mode, you can convert your deployment to HA mode.

Note This action cannot be reversed. HA deployments cannot be converted to non-HA mode.

Prerequisites

Verify that your environment contains sufficient resources to deploy the additional nodes required for HA mode. See "Hardware Requirements for VMware Integrated OpenStack" in the *VMware Integrated OpenStack Installation and Configuration Guide*.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Enable HA mode on your deployment.

```
viocli update deployment --enable-ha
```

Results

Additional controller nodes are created and service configurations are updated to enable HA on your deployment.

Update Certificates

You can update the digital certificates for the OpenStack services in your deployment.

The certificates that you add must be signed by a certificate authority (CA) and created from a certificate signing request (CSR) generated by VMware Integrated OpenStack. There is no support for using wildcard certificates.

Note If you want public CA to sign VMware Integrated OpenStack certificate, you must call VMware GSS for detailed steps.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Run the `viocli create csr` command to generate certificate signing requests for the desired services.

```
viocli create csr [-c country-name] [-t state-name] [-l city-name] [-n org-name] [-u org-unit] -s vio [-d output-directory]
```

For command syntax, see viocli create Command.

3 Use the generated CSRs to obtain certificate from a CA.

4 Transfer the certificate, CAs root certificate and all intermediate CA certificates to a directory on the Integrated OpenStack Manager.

5 Run the `viocli import certificate` command to import the certificates into VMware Integrated OpenStack.

```
viocli import certificate -d cert-directory
```

6 Restart the OpenStack services for the new certificate.

```
viocli stop services
viocli start services
```

Results

You can see the newly imported certificate in your deployment. To view the current certificate, run the `viocli get certificates -s vio`. For more information about adding certificates, see KB 78050.

Customize Backend Datastores

You can use the `viocli update` command to rename a datastore.The datastore specification varies depending on the service type.

To modify OpenStack parameters, you use the `viocli update` command. For more information, see viocli update Command.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 List the resources for each service type.

- For cinder, type: `viocli get cinder`.
- For glance, type: `viocli get glance`.
- For nova-compute, type: `viocli get novacompute`.

3 Specify the resource to update. If a service type has multiple resources, include the name of the resource to update as in the nova-compute example.

- For cinder, type: `viocli update cinder`.
- For glance, type: `viocli update glance`.
- For nova-compute, type: `viocli update novacompute <name_of_resource>`.

The specified service configuration opens in a text editor.

4 Change the name or regular expression to a value that matches the name of the datastore.

- For cinder, change the value of the `vmware_datastore_regex` parameter.
- For glance, change the value of the `vmware_datastores` parameter.
- For nova-compute, change the values of the `datastore_regex` and the `shared_datastore_regex` parameters.

5 Save the file, and quit the text editor.

Results

You have renamed a datastore in your OpenStack deployment.

Customize OpenStack Services

You use the `viocli update` command to set custom values for OpenStack parameters.

In previous versions of VMware Integrated OpenStack, the `custom.yml` file was used to modify OpenStack parameters. This implementation has been replaced with the `viocli update` command. For more information, see viocli update Command.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Modify the configuration of a service.

```
viocli update service-name
```

The specified service configuration is opened in a text editor.

3 Make the desired changes, save the file, and quit the text editor.

Results

Your OpenStack deployment is updated to reflect the settings that you changed.

Customize Horizon Dashboard

You can modify the styling, logos, and bookmark icon of the VMware theme on the VMware Integrated OpenStack dashboard.

Your custom theme can include the following items:

- `_styles.scss`: additional styles
- `_variables.scss`: color code definitions
- `favicon.ico`: bookmark icon of the VMware Integrated OpenStack dashboard
- `logo.svg`: graphic displayed in the top-left corner of each page
- `logo-splash.svg`: graphic displayed on the login page

Prerequisites

- Custom logos should be 216 pixels long by 35 pixels wide. Graphics with different dimensions might not be displayed properly.
- Custom logo files must be in SVG format.

Procedure

1 Create a directory named `themes` that includes your custom theme files.

Use the following directory structure:

- The `_styles.scss` and `_variables.scss` files must be in the `themes` directory.
- The `favicon.ico`, `logo.svg`, and `logo-splash.svg` files must be in the `themes/img` directory.

It is not necessary to include all five files in your theme. For example, you can choose to include custom logos only and use the default styles.

2 Archive the `themes` directory into a TAR file named `themes.tar`.

Note The TAR filename must be `themes.tar`.

3 In vSphere, create a content library and upload your `themes.tar` file to it.

   For information about content libraries, see "Using Content Libraries" in *vSphere Virtual Machine Administration*.

4 Log in to the Integrated OpenStack Manager web interface as the `admin` user.

5 In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.

6 On the **Settings** tab, select **Horizon Theme** and click **Enable**.

7 Enter the name of the content library containing your `themes.tar` file and click **OK**.

Results

The VMware Integrated OpenStack dashboard service restarts and loads your custom theme files. After the service becomes available, you can log in and switch to the VMware theme to display your customizations.

What to do next

On the **Horizon Theme** page, you can click **Edit** to specify a different content library or **Disable** to stop using your custom theme.

Note After you edit or disable the custom theme, clear the browser cache so that the updated theme can be displayed.

Customize TLS Cipher Suite

VMware Integrated OpenStack services support TLS 1.2 with cipher suites `ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256` by default. To customize a TLS cipher suite, you use the Kubernetes command-line utility.

Note If you use choose to configure a security protocol other than TLS, you assume a potential security risk.

The following procedure shows how to add a cipher suite for TLS 1.1 to the VMware Integrated OpenStack Horizon service.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Type the command to configure the Horizon service.

```
osctl edit Horizon
```

3 To use TLS 1.1 and add the cipher suite **ECDHE-RSA-AES256-SHA384**, specify the following configuration.

```
spec:
  conf:
    ssl:
      protocol: TLSv1.1
      ciphersuite: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-
AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384
    horizon:
      local_settings:
        config:
          openstack_neutron_network:
```

4 Save the configuration.

5 After the Horizon service restarts, verify the protocol and cipher suite settings.

a Type the following command.

```
osctl exec -it <pod-name> bash
```

b Open the configuration file `/etc/apache2/mods-enabled/ssl.conf`.

c To verify settings, look for the keywords `SSLProtocol` and `SSLCipherSuite` and check their values.

Configure Multiple Regions

You can add Keystone endpoints to your deployment to create multiple Horizon regions.

Procedure

1 Log in to the Integrated OpenStack Manager web interface as the `admin` user.

2 In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.

3 On the **Horizon Region** tab, click **Add**.

4 Enter the name of the region and the corresponding Keystone endpoint (for example, https://192.0.2.45:5000/v3).

5 Click **OK**.

Results

The new region is created and displayed in the table. Note that the default Horizon region is not displayed and cannot be modified.

Users can now select the desired region when logging in to Horizon.

Delete Deployment

If your deployment was unsuccessful or requires reconfiguration, you can delete your deployment and recreate it.

Prerequisites

Verify that a snapshot of the Integrated OpenStack Manager was taken before the current deployment was created. If you do not have a snapshot of the Integrated OpenStack Manager, you must delete the VMware Integrated OpenStack virtual appliance and install it again.

Procedure

1. In the vSphere Client, power off the VMware Integrated OpenStack virtual appliance and controller virtual machines.
2. Delete all VMware Integrated OpenStack controller virtual machines from your resource pool.

   Do not delete the controller template in the VMware Integrated OpenStack virtual appliance.
3. Restore the Integrated OpenStack Manager virtual machine to the snapshot taken before deployment.
4. Power on the VMware Integrated OpenStack virtual appliance.

Results

You can now create a new deployment on the Integrated OpenStack Manager. See "Create an OpenStack Deployment" in the *VMware Integrated OpenStack Installation and Configuration Guide*.

Tenant Virtual Data Center

You can create tenant virtual data centers to enable secure multi-tenancy and resource allocation. These data centers can be created on different compute nodes that offer specific service level agreements for each telecommunication workload.

The tenant virtual data center has the following limitations:

- Do not use the standard resize capability to create instances for virtual machine with tenant virtual data center settings. The resize is not supported on the tenant virtual data center.
- Do not use the live-migration operation on virtual machine with tenant virtual data center settings. The live-migration is not supported on the tenant virtual data center.

Important This feature is offered in VMware Integrated OpenStack Carrier Edition only. For more information, see "VMware Integrated OpenStack Licensing" in the *VMware Integrated OpenStack Installation and Configuration Guide*.

Project quotas limit OpenStack resources across multiple compute nodes or availability zones, but they do not guarantee resource availability. By creating a tenant virtual data center to allocate CPU and memory for an OpenStack project on compute node, you provide a resource guarantee for tenants and avoid noisy neighbor scenarios in a multi-tenant environment.

The tenant virtual data center allocates resources at the compute node level. You can also allocate resources on the virtual network function (VNF) level using the same flavor. For instructions, see Configure Resource QoS.

You can manage tenant virtual data centers using the `viocli` utility, vAPI, or Data Center Command-Line Interface (DCLI). This procedure uses the `viocli` utility as an example. For information about vAPI or DCLI usage, see Using the Tenant Virtual Data Center vAPIs.

Prerequisites

- Enable VMware Integrated OpenStack Carrier Edition features. See "Enable Carrier Edition Features" in the *VMware Integrated OpenStack Installation and Configuration Guide*.
- Determine the UUID of the project under which you want to create the tenant VDC. You can find the project UUID by running the `openstack project list` command.
- Determine the name of the compute node on which you want to create the tenant VDC. You can find the names of compute nodes by running the `openstack compute service list` command.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Create a tenant virtual data center.

```
viocli create tenant-vdc --name display-name --project-id project-uuid --compute compute-node [--cpu-limit max-cpu-mhz] [--cpu-reserve min-cpu-mhz] [--mem-limit max-memory-mb] [--mem-reserve min-memory-mb]
```

Option	Description
`--compute` ***compute-node***	Enter the compute node on which to create the tenant VDC. You can find the names of compute nodes by running the `openstack compute service list` command.
`--name` ***vdc-name***	Enter the name of the tenant VDC.
`--project-id` ***project-uuid***	Enter the UUID of the project under which to create the tenant VDC.
`--cpu-reserve` ***cpu-min***	Enter the CPU cycles in megahertz to reserve for the VDC. If you do not include this parameter, `0` is used by default.
`--cpu-limit` ***cpu-max***	Enter the maximum limit for CPU usage on the VDC (in megahertz). If you do not include this parameter, CPU usage is not limited.

Option	Description
--mem-reserve *memory-min*	Enter the memory in megabytes to reserve for the VDC. If you do not include this parameter, `0` is used by default.
--mem-limit *memory-max*	Enter the maximum limit for memory consumption on the VDC (in megabytes). If you do not include this parameter, memory consumption is not limited.

3 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

4 Select the **admin** project from the drop-down menu in the title bar.

5 Configure a flavor to use the tenant virtual data center.

   a Select **Admin > Compute > Flavors**.

   b Create a new flavor or choose an existing flavor to use the tenant virtual data center.

   c Select **Update Metadata** next to the flavor that you want to use.

   d In the **Available Metadata** pane, expand **VMware Policies** and click the **Add** (plus sign) icon next to **Tenant Virtual Datacenter**.

   e Set the value of `vmware:tenant_vdc` to the UUID of the tenant virtual data center and click **Save**.

   You can run the `viocli get tenant-vdcs` command on the Integrated OpenStack Manager to find the UUID of all tenant virtual data centers.

Results

The tenant virtual data center is created. You can now launch instances in the tenant virtual data center by configuring them with the flavor that you modified in this procedure.

What to do next

You can display the resource pools in a tenant virtual data center by running the `viocli get tenant-vdcs` *`tvdc-uuid`* command. Each resource pool is listed with its provider ID, project ID, status, minimum and maximum CPU, minimum and maximum memory, and compute node information. If a tenant virtual data center includes multiple resource pools, the first row displays aggregate information for all pools.

You can update a tenant virtual data center by running the `viocli update tenant-vdc` command or delete a tenant virtual data center by running the `viocli delete tenant-vdc` command..

Using the Tenant Virtual Data Center vAPIs

VMware Integrated OpenStack includes a vAPI that you can use to manage tenant virtual data centers.

If you have logged in to the OpenStack Management Server, you can also manage tenant virtual data centers using the Data Center Command-Line Interface (DCLI) or the `viocli` utility.

Before using the vAPI, you must authenticate with the vAPI endpoint using the administrator credentials for your vCenter Server instance.

You can use any HTTPS client to send requests to the vAPI endpoint. This document uses cURL as an example.

Create a Tenant Virtual Data Center

```
curl -k POST -u vcserver-admin -H "Content-Type: application/json"
   https://public-or-private-vip:9449/rest/vio/tenant/vdc
   -d '{
      "spec":{
         "compute":"compute-node",
         "display_name":"vdc-name",
         "project_id":"project-uuid",
         "cpu_limit":max-cpu-mhz,
         "cpu_reserve":min-cpu-mhz,
         "mem_limit":max-memory-mb,
         "mem_reserve":min-memory-mb
      }
   }'
```

The `cpu_limit`, `cpu_reserve`, `mem_limit`, and `mem_reserve` parameters are optional.

The ID of the new tenant virtual data center is returned in JSON format.

The equivalent DCLI command is as follows:

```
com vmware vio tenant vdc create --compute compute-node --display-name vdc-name --project-
id project-uuid [--cpu-limit max-cpu-mhz] [--cpu-reserve min-cpu-mhz] [--mem-limit max-memory-
mb] [--mem-reserve min-memory-mb]
```

Update a Tenant Virtual Data Center

```
curl -k PATCH -u vcserver-admin -H "Content-Type: application/json"
   https://public-or-private-vip:9449/rest/vio/tenant/vdc/tenant-vdc-id
   -d '{
      "spec":{
         "compute":"compute01"
         "cpu_limit":max-cpu-mhz,
         "cpu_reserve":min-cpu-mhz,
         "mem_limit":max-memory-mb,
         "mem_reserve":min-memory-mb
      }
   }'
```

The `cpu_limit`, `cpu_reserve`, `mem_limit`, and `mem_reserve` parameters are optional.

The equivalent DCLI command is as follows:

```
com vmware vio tenant vdc update --compute compute-node --tvdc-id tenant-vdc-id [--cpu-limit max-cpu-mhz] [--cpu-reserve min-cpu-mhz] [--mem-limit max-memory-mb] [--mem-reserve min-memory-mb]
```

List All Tenant Virtual Data Centers

```
curl -ku vcserver-admin https://public-or-private-vip:9449/rest/vio/tenant/vdc
```

The information is returned in JSON format.

The equivalent DCLI command is as follows:

```
com vmware vio tenant vdc list
```

Display Information About a Tenant Virtual Data Center

```
curl -ku vcserver-admin https://public-or-private-vip:9449/rest/vio/tenant/vdc/tenant-vdc-id
```

The status, provider ID, display name, and quotas of the tenant virtual data center are returned in JSON format.

The equivalent DCLI command is as follows:

```
com vmware vio tenant vdc get --tvdc-id tenant-vdc-id
```

Delete a Tenant Virtual Data Center

```
curl -k POST -u vcserver-admin -H "Content-Type: application/json"
   https://public-or-private-vip:9449/rest/vio/tenant/vdc/tenant-vdc-id?action=delete-tvdc
   -d '{
      "spec":{
         "compute":"compute-node"
      }
   }'
```

The `compute` parameter is optional. If you specify `compute`, the tenant virtual data center is deleted from the specified compute node only. If you do not specify `compute`, the tenant virtual data center is deleted from all compute nodes.

The equivalent DCLI command is as follows:

```
com vmware vio tenant vdc deletetvdc --tvdc-id tenant-vdc-id [--compute compute-node]
```

Keystone Authentication 3

In VMware Integrated OpenStack, authentication and identity management are provided by the Keystone component. In addition to SQL-backed OpenStack users, you can also configure authentication through LDAP or through identity federation.

For more information about Keystone, see the OpenStack Keystone documentation at https://docs.openstack.org/keystone/train.

VMware Integrated OpenStack supports identity federation with VMware Identity Manager as the identity provider. You can also implement federation with a third-party identity provider over the SAML 2.0 protocol, but this is not supported by VMware.

This chapter includes the following topics:

Create an OpenStack Project

Projects are organizational units in OpenStack. They can contain users, instances, and other objects such as images.

Note The domain of a project cannot be specified through the VMware Integrated OpenStack dashboard. To create a project in a specified domain, use the OpenStack command-line interface.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

2 Select the **admin** project from the drop-down menu in the title bar.

3 Select **Identity > Projects**.

4 Click **Create Project** and enter the desired configuration.

Option	Description
Name	Enter a name for the project.
Description	Enter a description of the project.
Enabled	Select the checkbox to enable the project.

5 (Optional) Open the **Project Members** tab and add users to the project.

6 (Optional) Open the **Project Groups** tab and add user groups to the project.

7 Click **Create Project**.

Results

The project is created and assigned a UUID.

Note The project UUID generated is 32 characters in length. However, when filtering by project ID specific to the security group section in Neutron server logs or in vRealize Log Insight, use only the first 22 characters.

What to do next

In the **Actions** column to the right of each project, you can modify project settings, including adding and removing users and groups, modifying project quotas, and changing the name or enabled status of the project.

If you disable a project, it is no longer accessible to its members, but its instances continue to run, and project data is retained. Users that are assigned only to disabled projects cannot log in to the VMware Integrated OpenStack dashboard.

You can select one or more projects and click **Delete Projects** to remove them permanently. Deleted projects cannot be restored.

Create a Cloud User

Cloud users have fewer permissions than cloud administrators. Cloud users can create and manage instances, volumes, networks, and images for the project to which they are assigned.

Prerequisites

Create and enable at least one OpenStack project. See Create an OpenStack Project.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

2 Select the **admin** project from the drop-down menu in the title bar.

3 Select **Identity > Users** and click **Create User**.

4 Configure the user settings.

Option	Description
User Name	Enter the user name.
Description	(Optional) Enter a description for the user.
Email	(Optional) Enter an email address for the user.
Password/Confirm Password	Enter a preliminary password for the user. The password can be changed after the user logs in for the first time.
Primary Project	Select the project to which the user is assigned. A user account must be assigned to at least one project.
Role	Select a role for the user. The user inherits the permissions assigned to the specified role.
Enable	Select **Enable** to allow to user to log in and perform OpenStack operations.

5 Click **Create User**.

What to do next

In the **Actions** column to the right of each user, you can modify user settings, change the user password, and enable or disable the user.

If you want to assign a single user to multiple projects, select **Identity > Projects** and click **Manage Members** next to the desired project.

You can create a group containing multiple users for simpler administration. See Create a User Group.

You can select one or more users and click **Delete Users** to remove them permanently. Deleted users cannot be restored.

Create a User Group

You can create a group containing multiple users for easier administration.

Prerequisites

Create the desired users. See Create a Cloud User.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

2 Select the **admin** project from the drop-down menu in the title bar.

3 Select **Identity > Groups** and click **Create Group**.

4 Enter a name and description and click **Create Group**.

5 In the **Actions** column to the right of the new group, click **Manage Members**.

6 Click **Add Users**.

7 Select one or more users and click **Add Users**.

What to do next

You can add the user group when you create or modify a project. All users in the group inherit the roles specified in the project for the group.

Manage Keystone Domains

Keystone domains are containers for projects and users.

You can create and manage additional domains as needed. For example, you can create a separate domain for federated users. To manage domains, log in to the VMware Integrated OpenStack dashboard as a cloud administrator and select **Identity > Domains**.

All VMware Integrated OpenStack deployments contain the `service` and `Default` domains. The `service` domain contains accounts used by OpenStack services, and the `Default` domain contains accounts used by OpenStack users, including the `admin` account.

Important Do not disable or delete the `service` or `Default` domains.

In earlier versions of VMware Integrated OpenStack, if you configured LDAP authentication during installation, the `Default` domain contained LDAP users, and the `local` domain contained OpenStack service and user accounts. If you have upgraded your deployment from a previous version of VMware Integrated OpenStack, these settings are retained for backward compatibility. However, service users are moved to the `service` domain.

Update the Keystone Admin Password

The process to update the Keystone admin user password includes steps that stop and start the nova services.

Note The update triggers the OpenStack Lifecycle Manager pipeline and updates each Helm chart. The update might interrupt OpenStack services for a short time.

Because nova services use the Keystone admin password to check the service status, we need to stop these services before changing the Keystone admin password.

Prerequisites

Verify that you have a base64 encoded password.

Important You can encrypt the base64 password with the following command. If you do not include -n, then the new encrypted password contains a new line, which will result in errors.

```
echo -n 'input' | openssl base64
```

Procedure

1 Stop nova services.

a Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

b Stop nova services.

```
viocli stop service nova
```

c Stop nova-compute services.

```
viocli stop service nova-compute
```

Note nova services will be down from this point.

2 Change the password for the Keystone admin user.

a Log in to the VMware Integrated OpenStack dashboard.

b Select **Identity > Users**.

c In the Actions column, select **Change Password**.

You can also use the OpenStack CLI to change the password with the following command.

```
openstack user set --password <password> admin
```

To change the password with a prompt, instead of typing the password, use the following command.

```
openstack user set --password-prompt admin
```

3 In the OpenStack namespace, change the Keystone admin password.

a Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

b Edit `secret managedpasswords`.

```
osctl edit secret managedpasswords
```

c Update the value for the **`data.admin_password`**.

```
apiVersion: v1
data:
  admin_password: <new_password>
```

The value of the *new_password* must be base64 encoded.

d Edit `secret nova-keystone-admin`.

```
osctl edit secret nova-keystone-admin
```

e Update the value for the **`data.OS_PASSWORD`**.

```
apiVersion: v1
data:
  OS_PASSWORD: <new_password>
```

The value of the *new_password* must be base54 encoded.

4 Start nova services.

a Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

b Start nova services.

```
viocli start service nova
```

c Start nova-compute services.

```
viocli start service nova-compute
```

5 Check the deployment status.

```
viocli get deployment
```

The deployment status first appears as `reconfiguring`. When it reaches `running`, the password update is complete.

Configure LDAP Authentication

You can configure LDAP authentication, add new domains, or modify your existing LDAP configuration.

Important All LDAP attributes must use ASCII characters only.

By default, VMware Integrated OpenStack connects with your LDAP server using SSL on port 636. If this configuration is not appropriate for your environment, specify the correct port and protocol under **Advanced settings**.

Prerequisites

- Contact your LDAP administrator to obtain the correct LDAP settings for your environment.
- If you want to use a new Keystone domain for LDAP users, create the domain in Keystone before proceeding. The domains `default`, `local`, and `service` cannot be used for LDAP.

Procedure

1 Log in to the Integrated OpenStack Manager web interface as the `admin` user.

2 In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.

3 On the **Settings** tab, click **Configure Identity Sources**.

4 Click **Add** to configure a new LDAP source or **Edit** to modify an existing configuration.

5 Enter your LDAP configuration.

Option	Description
Active Directory domain name	Specify the full Active Directory domain name.
Keystone domain name	Enter the Keystone domain name for the LDAP source. **Note** ■ Do not use `default`, `local`, or `service` as the Keystone domain. ■ The Keystone domain cannot be changed after the LDAP source has been added. ■ You must specify an existing Keystone domain. Create the desired domain before configuring LDAP authentication.
Bind user	Enter the user name to bind to Active Directory for LDAP requests.
Bind password	Enter the password for the LDAP user.
Domain controllers	(Optional) Enter the IP addresses of one or more domain controllers, separated with commas (,). If you do not specify a domain controller, VMware Integrated OpenStack will automatically choose an existing Active Directory domain controller.
Site	(Optional) Enter a specific deployment site within your organization to limit LDAP searching to that site.
Query scope	Select **SUB_TREE** to query all objects under the base object or **ONE_LEVEL** to query only the direct children of the base object.
User Tree DN	(Optional) Enter the search base for users (for example, **`DC=example,DC=com`**).
User Filter	(Optional) Enter an LDAP search filter for users. **Important** If your directory contains more than 1,000 objects (users and groups), you must apply a filter to ensure that fewer than 1,000 objects are returned. For more information about filters, see "Search Filter Syntax" in the Microsoft documentation at https://docs.microsoft.com/en-us/windows/win32/adsi/search-filter-syntax.
Group tree DN	(Optional) Enter the search base for groups. The LDAP suffix is used by default.

Option	Description
Group filter	(Optional) Enter an LDAP search filter for groups.
LDAP admin user	Enter an LDAP user to act as an administrator for the domain. If you specify an LDAP admin user, the `admin` project will be created in the Keystone domain for LDAP, and this user will be assigned the `admin` role in that project. This user can then log in to Horizon and perform other operations in the Keystone domain for LDAP. If you do not specify an LDAP admin user, you must use the OpenStack command-line interface to add a project to the Keystone domain for LDAP and assign the `admin` role to an LDAP user in that project.

6 (Optional) Select the **Advanced settings** check box to display additional LDAP configuration fields.

Option	Description
Encryption	Select **None**, **SSL**, or **StartTLS**.
Hostname	Enter the hostname of the LDAP server. Multiple LDAP servers can be supplied to provide high-availability support for a single LDAP backend. To specify multiple LDAP servers, simply separate by commas.
Port	Enter the port number to use on the LDAP server.
User objectclass	(Optional) Enter the LDAP object class for users. The default value is `organizationalPerson`.
User ID attribute	(Optional) Enter the LDAP attribute mapped to the user ID. This value cannot be a multi-valued attribute. The default value is `cn`.
User name attribute	(Optional) Enter the LDAP attribute mapped to the user name. The default value is `userPrincipalName`.
User mail attribute	(Optional) Enter the LDAP attribute mapped to the user email. The default value is `mail`.
User password attribute	(Optional) Enter the LDAP attribute mapped to the password. The default value is `userPassword`.
User enabled bitmask	Enter the bitmask that determines which bit indicates that a user is enabled. Enter this value as an integer. If a bitmask is not used, enter `0`. The default value is `2`.
Group objectclass	(Optional) Enter the LDAP object class for groups. The default value is `group`.
Group ID attribute	(Optional) Enter the LDAP attribute mapped to the group ID. The default value is `cn`.
Group name attribute	(Optional) Enter the LDAP attribute mapped to the group name. The default value is `sAMAccountName`.
Group member attribute	(Optional) Enter the LDAP attribute mapped to the group member name. The default value is `member`.
Group description attribute	(Optional) Enter the LDAP attribute mapped to the group description. The default value is `description`.

7 Click **OK**.

VMware Integrated OpenStack validates the specified LDAP configuration.

8 After validation succeeds, accept the certificate in the **CERT** column.

9 Click **Configure**.

10 If you did not specify an LDAP admin user, configure a project and administrator for the Keystone domain for LDAP.

a Log in to the Integrated OpenStack Manager as the `root` user and open the toolbox.

```
ssh root@mgmt-server-ip
toolbox
```

b Create a project in the Keystone domain for LDAP.

```
openstack project create new-project --domain ldap-domain
```

c In the Keystone domain for LDAP, assign the `admin` role to the LDAP user.

```
openstack role add admin --user ldap-username --user-domain ldap-domain --domain ldap-domain
```

d In the new project, assign the `admin` role to the LDAP user.

```
openstack role add admin --user ldap-username --user-domain ldap-domain --project new-project --project-domain ldap-domain
```

e Multiple LDAP servers can be supplied to url to provide high-availability support for a single LDAP backend. To specify multiple LDAP servers, simply change the url option in the *ldap* section to a list, separated by commas.

```
ldaps/ldap://ldap server1:636/389, ldaps/ldap://ldap backup:636/389
```

Results

LDAP authentication is configured on your VMware Integrated OpenStack deployment. You can log in to the VMware Integrated OpenStack dashboard as the LDAP admin user that you specified during configuration.

Note If you need to modify your LDAP configuration, you must use the Integrated OpenStack Manager web interface. Modifying the LDAP configuration over the command line is not supported.

Configure VMware Identity Manager Federation

You can configure VMware Integrated OpenStack to use VMware Identity Manager as an identity provider solution.

Users can authenticate with VMware Identity Manager over the Security Association Markup Language (SAML) 2.0 protocol or the OpenID Connect (OIDC) protocol.

- SAML 2.0 users must authenticate using the VMware Integrated OpenStack dashboard. The OpenStack command-line interface is not supported for SAML 2.0.
- OpenID Connect users can authenticate using the VMware Integrated OpenStack dashboard or the OpenStack command-line interface.

Prerequisites

- Deploy and configure VMware Identity Manager. For more information, see the VMware Identity Manager documentation.
- If you want to use the OIDC protocol and your VMware Identity Manager instance is using a self-signed certificate, ensure that the CA is installed as a trusted CA in VMware Identity Manager. For instructions, see "Installing Trusted Root Certificates" in the *Installing and Configuring VMware Identity Manager* document.
- Ensure that your VMware Identity Manager instance can communicate with the VMware Integrated OpenStack management network.
- The OpenStack `admin` user and VMware Identity Manager `admin` user cannot be in the same Keystone domain. If you want to import federated users into the `default` domain, ensure that the VMware Identity Manager `admin` user is not part of the VMware Identity Manager group that you use for federation.
- You must use different federation names for configuring multiple VMware Integrated OpenStack to the same VMware Identity Manager.

Procedure

1. Log in to the Integrated OpenStack Manager web interface as the `admin` user.
2. In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.
3. On the **Identity Federation** tab, click **Add**.
4. From the **Federation type** drop-down menu, select **VIDM**.
5. Enter the required parameters.

Option	Description
Protocol type	Select **SAML2** or **OIDC** as the identity protocol.
Name	Enter a name for the identity provider. **Note** The identity provider name cannot be changed after the identity provider has been added.
Description	Enter a description of the identity provider.

Option	Description
VIDM address	Enter the FQDN of your VMware Identity Manager instance without the protocol (for example, vidm.example.com). **Note** The FQDN must be unique. A single VMware Identity Manager instance cannot be added to VMware Integrated OpenStack as two separate identity providers.
VIDM username	Enter the username of a VMware Identity Manager administrator.
VIDM password	Enter the password for the specified administrator.
VIDM validate certs	Select the checkbox to validate VMware Identity Manager certificates. **Important** If you have selected the OIDC protocol and your VMware Identity Manager instance is using a self-signed certificate, you must validate certificates.

6 (Optional) Select the **Advanced settings** checkbox to configure additional parameters.

a Under **Common advanced settings**, enter an OpenStack domain, project, and group into which federated users will be imported.

Note

- If you do not enter a domain, project, or group, the following default values are used:
  - Domain: `federated_domain`
  - Project: `federated_project`
  - Group: `federated_group`
- Do not enter `federated` as the domain name. This name is reserved by Keystone.
- If you provide custom mappings, you must enter all OpenStack domains, projects, and groups that are included in those mappings.

b In the **Attribute mapping** field, enter additional attributes in JSON format or upload a JSON file containing the desired attributes.

c Under **VIDM advanced settings**, enter a VMware Identity Manager tenant and group from which to import users.

If you are using a VMware Identity Manager instance in a vRealize Automation deployment, enter **`vsphere.local`** as the tenant. If you are using a standalone VMware Identity Manager instance, do not enter a tenant.

d Under **SAML2 advanced settings**, enter the URL to the federation metadata file for your VMware Identity Manager instance.

e In the **SAML2 mapping** field, enter SAML mappings in JSON format or upload a JSON file containing the desired mappings.

f Under **OIDC advanced settings**, enter the URL to the federation metadata file for your VMware Identity Manager instance.

g In the **OIDC mapping** field, enter OIDC mappings in JSON format or upload a JSON file containing the desired mappings.

h In the **Mapped mapping** field, enter OAuth mappings in JSON format or upload a JSON file containing the desired mappings.

7 Click **OK**.

Results

VMware Integrated OpenStack is created as a web application in VMware Identity Manager, and federated users and groups are imported from VMware Identity Manager into OpenStack. When you access the VMware Integrated OpenStack dashboard, you can choose the VMware Identity Manager identity provider to log in as a federated user.

Federated users are automatically assigned the member role. You can use the OpenStack command-line interface to assign cloud administrator privileges to federated users if necessary.

Note When using identity federation, you must access the VMware Integrated OpenStack dashboard over the public OpenStack endpoint. Do not use the private OpenStack endpoint or a controller IP address to log in as a federated user.

What to do next

If you want to create a new identity federation that uses the same VMware Identity Manager instance, delete the configured identity provider and ensure that the deletion is complete before adding it again.

To delete a configured identity provider, first select it in the Integrated OpenStack Manager web interface and click **Delete**, then wait until the deletion is complete.

Configure Keystone to Keystone Federation

Keystone to Keystone (K2K) federation allows multiple OpenStack deployments to share the same identity source. It is useful for cross-region sites where one site is used as the identity source.

A VMware Integrated OpenStack deployment can be configured as an identity provider or service provider for Keystone to Keystone federation. An identity provider provides user authentication services to a service provider.

Procedure

1 Configure an OpenStack deployment as a Keystone identity provider.

a Log in to the Integrated OpenStack Manager web interface as the `admin` user.

b In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.

c On the **Identity Federation** tab, click **Add**.

d From the **Federation type** drop-down menu, select **K2K**.

e Enter the required parameters.

Option	Description
Name	Enter a name for the identity provider.
Description	Enter a description of the identity provider.
K2K provider type	Select **Keystone as identity provider**.
K2K service provider address	Enter the public OpenStack endpoint of the OpenStack deployment that will act as the service provider (for example, 198.51.100.100).
K2K service provider CA CERT	Enter the contents of the `vio.pem` certificate from the OpenStack deployment that will act as the service provider. You can display the contents of the `vio.pem` file by running the following command: `kubectl -n openstack get secrets certs -o jsonpath='{@.data.vio_certificate}' | base64 --decode`

f Click **OK**.

2 Configure the second OpenStack deployment as a Keystone service provider.

a Log in to the Integrated OpenStack Manager web interface as the `admin` user.

b In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.

c On the **Identity Federation** tab, click **Add**.

d From the **Federation type** drop-down menu, select **K2K**.

e Enter the required parameters.

Option	Description
Name	Enter the name of the target identity provider. The value of this field must be the same on both deployments.
Description	Enter a description of the service provider.
K2K provider type	Select **Keystone as service provider**.
K2K identity provider address	Enter the public OpenStack endpoint of the OpenStack deployment acting as the identity provider (for example, 192.0.2.100).
K2K identity provider port	Enter the Keystone port number of the OpenStack deployment acting as the identity provider (for example, 5000).

f (Optional) You can select **Advanced settings > Common advanced settings** and enter an OpenStack domain, project, and group into which federated users will be imported.

Note

- If you do not enter a domain, project, or group, the following default values are used:
  - Domain: `federated_domain`
  - Project: `federated_project`
  - Group: `federated_group`
- Do not enter `federated` as the domain name. This name is reserved by Keystone.
- If you provide custom mappings, you must enter all OpenStack domains, projects, and groups that are included in those mappings.

g Click **OK**.

Results

Users and groups are federated from the service provider deployment to the identity provider deployment. When you log in to the VMware Integrated OpenStack dashboard on the identity provider deployment, you can select the service provider in the top-right of the page. You can then perform actions on the service provider deployment.

Note When using identity federation, you must access the VMware Integrated OpenStack dashboard over the public OpenStack endpoint. Do not use the private OpenStack endpoint or a controller IP address to log in as a federated user.

Configure SAML 2.0 Federation

You can integrate VMware Integrated OpenStack with any third-party identity provider solution that uses the Security Association Markup Language (SAML) 2.0 protocol. The Keystone in VMware Integrated OpenStack works as the service provider for this configuration.

Important VMware does not support third-party identity providers. Contact your identity provider administrator for obtaining the information required for this procedure.

If you want to integrate VMware Integrated OpenStack with VMware Identity Manager using SAML 2.0, see Configure VMware Identity Manager Federation.

Prerequisites

- Determine the location of your identity providers metadata file and the `entityID` attribute in the file.
- Ensure that your VMware Integrated OpenStack deployment can access the FQDN of the identity provider.

- For SAML2 Attribute Mapping, Keystone uses Shibboleth as the SSO component. Shibboleth maps the IdP user attributes to the local attributes used by Keystone. Contact your IdP admin for the user attributes.
- For SAML2 Rule Mapping, Keystone requires rules for mapping remote users to the local domains, the projects, and the groups. For more information, see "Mapping Combinations" in the OpenStack documentation at https://docs.openstack.org/keystone/train/admin/federation/mapping_combinations.html.
- On the identity provider side, you must properly configure the service provider. The service provider metadata can be accessed with the following URL: **`https://<vio_public_endpoint>:5000/<your_idp_name>/Shibboleth.sso/Metadata`**

Procedure

1 Log in to the Integrated OpenStack Manager web interface as the `admin` user.

2 In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.

3 On the **Keystone Federation** tab, click **Add**.

4 From the **Federation type** drop-down menu, select **Generic SAML2**.

5 Enter the required parameters.

Option	Description
Name	Enter a name for the identity provider. VMware Integrated OpenStack uses this name for creating OpenStack identity provider.
Description	Enter a description for the identity provider.
Attribute mapping	Enter additional SAML attributes in JSON format or upload a JSON file containing the desired attributes. VMware Integrated OpenStack uses the JSON data for configuring the Shibboleth `attribute-map.xml` file.
Generic SAML2 insecure	Deselect the check box so that you can validate the certificates of your identity provider.
Generic SAML2 entity ID	Enter the `entityID` attribute for your identity provider. You can find this value in the federation metadata file. VMware Integrated OpenStack uses this value for creating OpenStack identity provider.
SAML2 metadata URL	Enter the URL to the federation metadata file for your identity provider. VIO manager can access this URL for downloading the metadata file.
SAML2 mapping	Enter SAML mappings in JSON format or upload a JSON file containing the desired mappings. VMware Integrated OpenStack uses this value for creating OpenStack mapping and sets it to the federation protocol for this identity provider.

Attribute mapping format and examples:

```
[
      {
        "name": "urn:oid:0.9.2342.19200300.100.1.1",
        "nameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:uri",
```

```
        "id": "username"
      },
      {
        "name": "urn:oid:0.9.2342.19200300.100.1.3",
        "nameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:uri",
        "id": "email"
      }
    ]
```

Option	Description
`name`	Enter the attribute name. Keystone requires at least one attribute which can be used as users unique identification. For example, `username`, `email`, and so on. Contact your IdP admin for determining the attribute name, it can be different from the IdP servers.
`nameFormat`	Enter the attribute name format. Contact your IdP admin for determining the format value. This attribute is optional.
`id`	Enter the string value for this attribute. Do not use space for the string value. For example, do not use "user name", instead use "`username`". This value can be used in Mapping Rules as `remote:type`.

SAML2 Rule Mapping format and examples:

```
[
  {
    "local": [
      {
        "user": {
          "name": "{1}"
        },
        "group": {
          "name": "federated_users",
          "domain": {
            "name": "federated_domain"
          }
        }
      }
    ],
    "remote": [
      {
        "type": "username"
      },
      {
        "type": "email"
      }
    ]
  }
]
```

You can find the rule mapping definition under Mapping Combinations for Keystone in OpenStack community.

Option	Description
`local`	The JSON defines the OpenStack local domains and projects. This attribute can be used for users mapped from IdP. For example, in SAML2 Rule Mapping, `"name": "{1}"` is same as using `"type": "email"` as the login name for Keystone, and login for the specified domain and project.
`remote`	The section defines the rules and conditions for mapping the remote attributes.

6 (Optional) Select the **Advanced settings** check box for configuring domain, projects, and group parameters.

a Under **Common advanced settings**, enter `federated_domain` as OpenStack domain, `federated_project` as project, and `federated_group` as group.

b The OpenStack domain, project, and group name must match the information provided in Rule Mapping `"local"` JSON.

c VMware Integrated OpenStack creates the domain and project for the specified federation users.

Note Do not enter `federated` as the domain name because this name is used by Keystone.

7 Click **OK**.

Note After you finish the SAML2 configuration, you can see that the Keystone service is restarting automatically. Before downloading the metadata, ensure that your deployment status has changed to `RUNNING` by executing `viocli get deployment`.

8 Ensure that **`https://<vio_public_endpoint>:5000/<your_idp_name>/Shibboleth.sso/Metadata`** is accessible, and configure your IdP service for trusting VMware Integrated OpenStack Keystone as the service provider.

Results

VMware Integrated OpenStack is integrated with your identity provider solution, and federated users and groups are imported into OpenStack. When you access the VMware Integrated OpenStack dashboard, you can select the specified identity provider to log in as a federated user.

Note When using identity federation, you must access the VMware Integrated OpenStack dashboard over the public OpenStack endpoint. Do not use the private OpenStack endpoint or a controller IP address to log in as a federated user.

Example: Integrating VMware Integrated OpenStack with Active Directory Federation Services

The following procedure implements identity federation between VMware Integrated OpenStack and Active Directory Federation Services (ADFS) based on the User Principal Name (UPN). The procedure of ADFS configuration is an example for your reference, the real enterprise configuration can be different. You must change the corresponding VMware Integrated OpenStack SAML configuration.

In this example, the public virtual IP address of the VMware Integrated OpenStack deployment is `192.0.2.160` and the ADFS role is part of the Windows Server virtual machine located at `adfs.example.com`. The name of the identity provider in VMware Integrated OpenStack is `adfsvio`.

1 In ADFS, add a relying party trust for VMware Integrated OpenStack.
   a In **ADFS Management**, select **Action > Add Relying Party Trust...**.
   b Click **Start**.
   c Select **Enter data about the relying party manually** and click **Next**.
   d Enter **`OpenStack`** for the display name and click **Next**.
   e Select **ADFS profile** and click **Next**.
   f Click **Next**.
   g Select **Enable support for the SAML 2.0 WebSSO protocol**.
   h Enter **`https://192.0.2.160:5000/adfsvio/Shibboleth.sso/SAML2`** for the relying party URL and click **Next**.
   i Enter **`https://192.0.2.160:5000/adfsvio`** for the relying party trust identifier, click **Add** and click **Next**.
   j Select **I do not want to configure multi-factor authentication** and click **Next**.
   k Select **Permit all users to access this relying party** and click **Next**.
   l Click **Next**, select **Edit Claim Rules** and click **Close**.
   m Click **Add Rule...**.
   n Select **Pass Through or Filter an Incoming Claim** and click **Next**.
   o Enter **UPN passthrough** for the rule name and select **UPN** for the incoming claim type.
   p Select **Pass through all claim values** and click **Finish**.
2 Log in to the Integrated OpenStack Manager web interface as the `admin` user.
3 In **OpenStack Deployment**, click the name of the deployment and open the **Manage** tab.
4 On the **Identity Federation** tab, click **Add**.
5 From the **Federation type** drop-down menu, select **Generic SAML2**.

6 Enter the following configuration:

Option	Description
Name	**adfsvio**
Description	**ADFS identity provider**
Attribute mapping	`[ { "name": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn", "id": "upn" } ]`
Generic SAML2 entity ID	**http://adfs.example.com/adfs/services/trust**
SAML2 metadata URL	**https://adfs.example.com/federationmetadata/2007-06/federationmetadata.xml**
SAML2 mapping	`[ { "local": [ { "user": { "name": "{0}" }, "group": { "domain": { "name": "adfs-users" }, "name": "Federated Users" } } ], "remote": [ { "type": "upn" } ] } ]`

7 Select the **Advanced settings** checkbox.

8 Select **Common advanced settings** and enter the following configuration.

Option	Description
Domain	**adfs-users**
Project	Leave the text box blank.
Group	**Federated Users**

After the configuration verification and update is finish, open the VMware Integrated OpenStack dashboard. You can now select the ADFS identity provider and log in as a federated user.

What to do next

To delete a configured identity provider, select the Integrated OpenStack Manager web interface and click **Delete**. Then log in to the VMware Integrated OpenStack dashboard, select **Identity > Federation > Identity Providers**, select the desired provider, and click **Unregister Identity Providers**.

Neutron Networkings

4

With Neutron, you can create networks, configure availability zones, and perform other advanced networking tasks for your OpenStack deployment.

For more information about Neutron, see the OpenStack Neutron documentation at https://docs.openstack.org/neutron/train.

This chapter includes the following topics:

Configure NSX-T Manager Cluster

NSX-T Data Center 2.4 and later support the deployment of multiple NSX Manager nodes to form a cluster in a single NSX-T Data Center instance. If you want to use an NSX Manager cluster

with VMware Integrated OpenStack, add the IP addresses of all cluster nodes to your deployment configuration.

Note The following limitations apply to the NSX Manager cluster:

- An NSX Manager cluster provides high availability for a single NSX-T Data Center instance. Multiple instances of NSX-T Data Center cannot be used with the same VMware Integrated OpenStack deployment.
- In the VMware Integrated OpenStack deployment, after configuring the 3 NSX-T managers, if you make any changes to the NSX-T manager, you can see that all the configurations on this page are displayed correctly, except the NSX Policy configuration, which is still loading.

Prerequisites

Create the NSX Manager cluster in NSX-T Data Center. See "Deploy NSX Manager Nodes to Form a Cluster from UI" in the *NSX-T Data Center Installation Guide*.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Add the other two NSX-T managers into VMware Integrated OpenStack.

a Refer to the `kubectl -n openstack get nsxs.vio.vmware.com -o yaml` format to create a `nsx` YAML file for the other two NSX-T managers. For example:

```
vi nsx_sample.yaml
apiVersion: vio.vmware.com/v1alpha1
kind: NSX
metadata:
  labels:
    app: lcm
    clusterController: "true"
    group: vio.vmware.com
    kind: NSX
    name: nsx2
    openstackController: "true"
    version: v1alpha1
  name: nsx2
  namespace: openstack
  selfLink: /apis/vio.vmware.com/v1alpha1/namespaces/openstack/nsxs/nsx2
spec:
  hostname: <the second nsx manager ip address>
  insecure: true
  kind: nsxp
  password: .VIOSecret:viosecret1:spec.nsx_password
  username: admin
---
apiVersion: vio.vmware.com/v1alpha1
kind: NSX
metadata:
  labels:
    app: lcm
    clusterController: "true"
    group: vio.vmware.com
    kind: NSX
    name: nsx3
    openstackController: "true"
    version: v1alpha1
  name: nsx3
  namespace: openstack
  selfLink: /apis/vio.vmware.com/v1alpha1/namespaces/openstack/nsxs/nsx3
spec:
  hostname: <the third nsx manager ip address>
  insecure: true
  kind: nsxp
  password: .VIOSecret:viosecret1:spec.nsx_password
  username: admin
```

b Check that the `nsx` YAML format is created for the two NSX-T managers.

```
kubectl -n openstack apply -f nsx_sample.yaml
```

c Verify that there are three `nsx` pods.

```
kubectl -n openstack get pod | grep nsx
```

d Modify the Neutron configuration to include the IP addresses of each `nsx` pod.

```
kubectl edit neutrons.vio.vmware.com -o yaml -n openstack
nsx_api_managers: .NSX:nsx1:spec.hostname,.NSX:nsx2:spec.hostname,.NSX:nsx3:spec.hostna
me
```

What to do next

If the IP address of any node changes, or if you add or remove nodes in your NSX Manager cluster, you must modify the Neutron configuration to include the updated IP address information.

Provider Network

Provider networks map to physical networks in your data center, and their networking functions are performed by physical devices.

A provider network can be dedicated to one project or shared among multiple projects. Tenants can create virtual machines in provider networks or connect their tenant networks to a provider network through a Neutron router.

The specific configuration for creating a provider network depends on the networking mode of your VMware Integrated OpenStack deployment.

Provider Network with NSX-T Data Center

With NSX-T Data Center networking, you can create a VLAN-based provider network.

Prerequisites

- Define a VLAN for the provider network and record its ID.
- To use DHCP with VM form-factor NSX Edge nodes, enable forged transmit and promiscuous mode on the port group containing the edge nodes. For instructions, see "Configure the Security Policy for a Distributed Port Group or Distributed Port" in the *vSphere Networking* document.

Procedure

1. Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.
2. Select the **admin** project from the drop-down menu in the title bar.
3. Select **Admin > Network > Networks**.

4 Click **Create Network** and configure the provider network.

Option	Description
Name	Enter a name for the network.
Project	Select the desired project from the drop-down menu.
Provider Network Type	Select **VLAN** from the drop-down menu.
Physical Network	Enter the UUID of the VLAN transport zone.
Segmentation ID	Enter the VLAN ID defined for the provider network.

5 Select **Enable Admin State** and **Create Subnet**.

6 If you want multiple projects to use the provider network, select **Shared**.

7 Click **Next** and configure the subnet.

Option	Description
Subnet Name	Enter a name for the subnet.
Network Address	Enter the IP address range for the subnet in CIDR format (for example, 192.0.2.0/24).
IP Version	Select **IPv4** or **IPv6**.
Gateway IP	Enter the gateway IP address. If you do not enter a value, the first IP address in the subnet is used. If you do not want a gateway on the subnet, select **Disable Gateway**.

8 (Optional) Configure additional settings for the subnet.

a Under **Allocation Pools**, enter IP address pools from which to allocate the IP addresses of virtual machines created on the network. Enter pools as two IP addresses separated by a comma (for example, **`192.0.2.10,192.0.2.15`**). If you do not specify any IP address pools, the entire subnet is available for allocation.

b Under **DNS Name Servers**, enter the IP address of one or more DNS servers to use on the subnet.

c Under **Host Routes**, enter additional routes to advertise to the hosts on the subnet. Enter routes as the destination IP address in CIDR format and the next hop separated by a comma (for example, **`192.0.2.0/24,192.51.100.1`**).

9 Click **Create**.

Provider Network with NSX Data Center for vSphere

With NSX Data Center for vSphere networking, you can create a flat, VLAN-based, port group-based, or VXLAN-based provider network.

Prerequisites

- If you want to create a VLAN-based network, define a VLAN for the provider network and record its ID.
- To use DHCP on a VLAN-based network with VM form-factor NSX Edge nodes, you must enable forged transmit and promiscuous mode on the port group containing the edge nodes. For instructions, see "Configure the Security Policy for a Distributed Port Group or Distributed Port" in the *vSphere Networking* document.
- If you want to create a port group-based network, create a port group for the provider network and record its managed object identifier (MOID).

Procedure

1 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

2 Select the **admin** project from the drop-down menu in the title bar.

3 Select **Admin > Network > Networks**.

4 Click **Create Network** and configure the provider network.

Option	Description
Name	Enter a name for the network.
Project	Select the desired project from the drop-down menu.
Provider Network Type	Select **Flat**, **VLAN**, **Port Group**, or **VXLAN** from the drop-down menu.
Physical Network	■ If you selected **Flat** or **VLAN** for the network type, enter the MOID of the distributed switch for the provider network. ■ If you selected **Port Group** for the network type, enter the MOID of the port group for the provider network. ■ If you selected **VXLAN** for the network type, this value is determined automatically.
Segmentation ID	If you selected **VLAN** for the network type, enter the VLAN ID defined for the provider network.

5 Select **Enable Admin State** and **Create Subnet**.

6 If you want multiple projects to use the provider network, select **Shared**.

7 Click **Next** and configure the subnet.

Option	Description
Subnet Name	Enter a name for the subnet.
Network Address	Enter the IP address range for the subnet in CIDR format (for example, 192.0.2.0/24).

Option	Description
IP Version	Select **IPv4** or **IPv6**.
Gateway IP	Enter the gateway IP address. If you do not enter a value, the first IP address in the subnet is used. If you do not want a gateway on the subnet, select **Disable Gateway**.

8 (Optional) Configure additional settings for the subnet.

a Under **Allocation Pools**, enter IP address pools from which to allocate the IP addresses of virtual machines created on the network. Enter pools as two IP addresses separated by a comma (for example, **`192.0.2.10,192.0.2.15`**). If you do not specify any IP address pools, the entire subnet is available for allocation.

b Under **DNS Name Servers**, enter the IP address of one or more DNS servers to use on the subnet.

c Under **Host Routes**, enter additional routes to advertise to the hosts on the subnet. Enter routes as the destination IP address in CIDR format and the next hop separated by a comma (for example, **`192.0.2.0/24,192.51.100.1`**).

9 Click **Create**.

Provider Network with VDS

With VDS networking, you can create a VLAN-based provider network.

Prerequisites

Define a VLAN for the provider network and record its ID.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

2 Select the **admin** project from the drop-down menu in the title bar.

3 Select **Admin > Network > Networks**.

4 Click **Create Network** and configure the provider network.

Option	Description
Name	Enter a name for the network.
Project	Select the desired project from the drop-down menu.
Provider Network Type	Select **VLAN** from the drop-down menu.
Physical Network	Enter **`dvs`**.
Segmentation ID	Enter the VLAN ID defined for the provider network.

5 Select **Enable Admin State** and **Create Subnet**.

6 If you want multiple projects to use the provider network, select **Shared**.

7 Click **Next** and configure the subnet.

Option	Description
Subnet Name	Enter a name for the subnet.
Network Address	Enter the IP address range for the subnet in CIDR format (for example, 192.0.2.0/24).
IP Version	Select **IPv4** or **IPv6**.
Gateway IP	Enter the gateway IP address. If you do not enter a value, the first IP address in the subnet is used. If you do not want a gateway on the subnet, select **Disable Gateway**.

8 (Optional) Configure additional settings for the subnet.

a Under **Allocation Pools**, enter IP address pools from which to allocate the IP addresses of virtual machines created on the network. Enter pools as two IP addresses separated by a comma (for example, **`192.0.2.10,192.0.2.15`**). If you do not specify any IP address pools, the entire subnet is available for allocation.

b Under **DNS Name Servers**, enter the IP address of one or more DNS servers to use on the subnet.

c Under **Host Routes**, enter additional routes to advertise to the hosts on the subnet. Enter routes as the destination IP address in CIDR format and the next hop separated by a comma (for example, **`192.0.2.0/24,192.51.100.1`**).

9 Click **Create**.

External Network

External networks act as floating IP address pools to provide external access for instances in your deployment.

An external network can be dedicated to one project or shared among multiple projects. Tenants cannot create virtual machines in external networks.

The specific configuration for creating an external network depends on the networking mode of your VMware Integrated OpenStack deployment.

External Network with NSX-T Data Center

For NSX-T Data Center deployments, you create an external network to contain the floating IP addresses of future tenant logical (tier-1) routers.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

2 Select the **admin** project from the drop-down menu in the title bar.

3 Select **Admin > Network > Networks**.

4 Click **Create Network** and configure the provider network.

Option	Description
Name	Enter a name for the network.
Project	Select the desired project from the drop-down menu.
Provider Network Type	Select **External** for connecting tenant logical routers to tier-0 router.
Physical Network	If you selected **External** as the provider network type, enter the ID of the tier-0 logical router to which you can connect future tenant logical routers. ■ If the Neutron Policy Plugin is used, the router ID is the policy ID. ■ If the Neutron Management Plugin is used, the router ID is the management UUID. If you use the vRF Lite feature in NSX-T, enter the ID of the vRF instance.

The process to find the router ID depends on the ID type.

- To obtain the policy ID from the NSX-T policy UI, select **Tier-0 Gateways**. Click the three dots to the left of the gateway entry, and select **Copy Path to Clipboard**. The full path with the ID is copied to the clipboard.
- For a management UUID, check the UUID of the tier-0 router in either the NSX-T 3.0 Manager UI or the NSX-T 2.5 Advanced Networking & Security UI.

You can also create the network from the command line.

```
openstack network create <ext_network_name> --external --provider-physical-network
<tier_0_router>
```

Where *ext_network_name* is the OpenStack external network name and *tier_0_router_name* is the NSX-T tier-0 router name or ID.

5 Select **Enable Admin State**, **External Network**, and **Create Subnet**.

6 If you want multiple projects to use the external network, select **Shared**.

7 Click **Next** and configure the subnet.

Option	Description
Subnet Name	Enter a name for the subnet.
Network Address	Enter the IP address range for the subnet in CIDR format (for example, 192.0.2.0/24).
IP Version	Select **IPv4** or **IPv6**.
Gateway IP	Enter the gateway IP address. If you do not enter a value, the first IP address in the subnet is used. If you do not want a gateway on the subnet, select **Disable Gateway**.

You can also configure the subnet from the command line.

```
openstack subnet create --subnet-range 192.0.2.0/24 --allocation-pool
start=192.0.2.10,end=192.0.2.15 --no-dhcp --network <ext_network_name> <ext_subnet_name>
```

Where *ext_network_name* is the OpenStack external network name and *ext_subnet_name* is the subnet name.

8 Click **Next** and deselect **Enable DHCP**.

9 (Optional) Configure additional settings for the subnet.

a Under **Allocation Pools**, enter IP address pools from which to allocate the floating IP addresses of tenant logical routers. Enter pools as two IP addresses separated by a comma (for example, **`192.0.2.10,192.0.2.15`**). If you do not specify any IP address pools, the entire subnet is available for allocation.

b Under **DNS Name Servers**, enter the IP address of one or more DNS servers for using on the subnet.

c Under **Host Routes**, enter routes for advertising to the hosts on the subnet. Enter routes as the destination IP address in CIDR format and the next hop separated by a comma (for example, **`192.0.2.0/24,192.51.100.1`**).

10 Click **Create**.

External Network with NSX Data Center for vSphere

With NSX Data Center for vSphere networking, you can create a flat, VLAN-based, port group-based, or VXLAN-based external network.

Prerequisites

- If you want to create a VLAN-based network, define a VLAN for the external network and record its ID.
- If you want to create a port group-based network, create a port group for the external network and record its managed object identifier (MOID).

Procedure

1 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

2 Select the **admin** project from the drop-down menu in the title bar.

3 Select **Admin > Network > Networks**.

4 Click **Create Network** and configure the provider network.

Option	Description
Name	Enter a name for the network.
Project	Select the desired project from the drop-down menu.
Provider Network Type	Select **Flat**, **VLAN**, **Port Group**, or **VXLAN** from the drop-down menu.

Option	Description
Physical Network	■ If you selected **Flat** or **VLAN** for the network type, enter the MOID of the distributed switch for the provider network. ■ If you selected **Port Group** for the network type, enter the MOID of the port group for the provider network. ■ If you selected **VXLAN** for the network type, this value is determined automatically.
Segmentation ID	If you selected **VLAN** for the network type, enter the VLAN ID defined for the provider network.

5 Select **Enable Admin State**, **External Network**, and **Create Subnet**.

6 If you want multiple projects to use the provider network, select **Shared**.

7 Click **Next** and configure the subnet.

Option	Description
Subnet Name	Enter a name for the subnet.
Network Address	Enter the IP address range for the subnet in CIDR format (for example, 192.0.2.0/24).
IP Version	Select **IPv4** or **IPv6**.
Gateway IP	Enter the gateway IP address. If you do not enter a value, the first IP address in the subnet is used. If you do not want a gateway on the subnet, select **Disable Gateway**.

8 Click **Next** and deselect **Enable DHCP**.

9 (Optional) Configure additional settings for the subnet.

a Under **Allocation Pools**, enter IP address pools from which to allocate the floating IP addresses of tenant logical routers. Enter pools as two IP addresses separated by a comma (for example, **`192.0.2.10,192.0.2.15`**). If you do not specify any IP address pools, the entire subnet is available for allocation.

b Under **DNS Name Servers**, enter the IP address of one or more DNS servers to use on the subnet.

c Under **Host Routes**, enter additional routes to advertise to the hosts on the subnet. Enter routes as the destination IP address in CIDR format and the next hop separated by a comma (for example, **`192.0.2.0/24,192.51.100.1`**).

10 Click **Create**.

Tenant Network

You can create tenant logical networks on the VMware Integrated OpenStack dashboard.

Note VMware Integrated OpenStack does not support a tenant network with VDS networking.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard.

2 Select your project from the drop-down menu in the title bar.

3 Select **Project > Network > Networks**.

4 Click **Create Network** and enter the desired configuration.

Option	Description
Network Name	Enter a name for the tenant network.
Enable Admin State	Select the checkbox to enable the network. The network cannot be used while the admin state is down.
Shared	Select the checkbox to allow the network to be used by multiple projects.
Create Subnet	Select the checkbox to use this wizard to create a subnet in the network.
Availability Zone Hints	Select an availability zone to create the network in that zone.

5 If you selected **Create Subnet**, click **Next** and enter the desired subnet configuration.

Option	Description
Subnet Name	Enter a name for the subnet.
Network Address	Enter the network address of the subnet in CIDR format (for example, 192.0.2.0/24).
IP Version	Select **IPv4** or **IPv6**.
Gateway IP	Enter the IP address of the network gateway. If you do not enter a value, the first IP address in the subnet is used. If you do not want a gateway on the network, select **Disable Gateway**.

6 Click **Next** and specify additional attributes for the subnet.

Option	Description
Enable DHCP	Select the checkbox to enable DHCP on the network.
Allocation Pools	Enter IP address pools from which to allocate the IP addresses of virtual machines created on the network. Enter each pool on a separate line as two IP addresses separated by a comma (for example, `192.0.2.10,192.0.2.15`). If you do not specify any IP address pools, the entire subnet is available for allocation.
DNS Name Servers	Enter the IP addresses of DNS servers to use on the subnet. Enter each IP address on a separate line.
Host Routes	Enter additional routes to advertise to the hosts on the subnet. Enter routes as the destination IP address in CIDR format and the next hop separated by a comma (for example, `192.0.2.0/24,192.51.100.1`).

7 Click **Create**.

Results

The network is created and displayed in the table below.

What to do next

In the **Actions** column, you can add more subnets to the network, edit its configuration, or delete it.

NSX-T Enhanced Data Path

For NSX-T Data Center deployments, you can create networks and ports backed by a transport zone using N-VDS enhanced data path mode.

Important This feature is offered in VMware Integrated OpenStack Carrier Edition only. For more information, see "VMware Integrated OpenStack Licensing" in the *VMware Integrated OpenStack Installation and Configuration Guide*.

An NSX-managed virtual distributed switch (N-VDS) can operate in enhanced data path mode to provide network performance improvements needed by NFV workflows. For more information, see "Enhanced Data Path" in the *NSX-T Data Center Installation Guide*.

Note If you are using NSX-T Data Center 2.3.1, port security is not supported for N-VDS enhanced data path mode. You must disable port security globally or for each Neutron network created. This limitation is resolved in NSX-T Data Center 2.4.

Prerequisites

If you are using both standard and enhanced data path mode, create a separate availability zone for enhanced data path mode. See Neutron Availability Zone.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Modify the Neutron configuration.

```
viocli update neutron
```

3 In the `nsx_v3` section, set the value of the `ens_support` parameter to `true`.

4 If you are using NSX-T Data Center 2.3.1, add the `disable_port_security_for_ens` parameter and set its value to `true`.

Alternatively, you can include the `--port-security-enabled=false` parameter when you create a Neutron network.

What to do next

When you create networks that consume N-VDS in enhanced data path mode, specify the availability zone created for it.

L2 Bridge

A Layer 2 bridge allows compute nodes on an overlay network to communicate with a physical VLAN.

L2 Bridge with NSX-T Data Center

You can create a Layer 2 bridge in NSX-T Data Center through a bridge cluster.

Note The NSX-T Policy Plugin does not support the Layer 2 bridge.

Prerequisites

In NSX-T Data Center, create an edge bridge profile. See "Create an Edge Bridge Profile" in the *NSX-T Administration Guide*.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Open the toolbox and set the password for the `admin` account.

```
toolbox
export OS_PASSWORD=admin-account-password
```

3 Create a logical Layer 2 gateway,

```
neutron l2-gateway-create gateway-name --device name=edge-cluster-
uuid,interface_names="temp"
```

For the *edge-cluster-uuid* value, enter the UUID of the NSX Edge cluster for which you configured the edge bridge profile.

Note The interface name value is ignored, and this name is automatically assigned.

4 Create the logical Layer 2 gateway connection using the gateway created in the previous step.

```
neutron l2-gateway-connection-create gateway-name network-name --default-segmentation-
id=vlan-id
```

Results

Compute nodes on the overlay network can now access the specified VLAN.

L2 Bridge with NSX Data Center for vSphere

You can create a Layer 2 bridge in NSX Data Center for vSphere through a port group.

Prerequisites

Create a port group and tag it with the ID of the VLAN to which you want to connect your compute nodes.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Open the toolbox and set the password for the `admin` account.

```
toolbox
export OS_PASSWORD=admin-account-password
```

3 Create a logical Layer 2 gateway, specifying the managed object identifier (MOID) of the port group as the interface name.

```
neutron l2-gateway-create gateway-name --device name=temp,interface_names="portgroup-moid"
```

NSX Data Center for vSphere creates a dedicated distributed logical router (DLR) from the backup edge pool. The device name value is ignored, and the object is automatically assigned a name in the format "L2 bridging-*gateway-id*".

4 Create the logical Layer 2 gateway connection using the gateway created in the previous step.

```
neutron l2-gateway-connection-create gateway-name network-name --default-segmentation-
id=vlan-id
```

Results

VXLAN compute nodes can now access the specified VLAN.

Neutron Availability Zone

You can create additional Neutron availability zones with NSX-T Data Center by updating your VMware Integrated OpenStack deployment.

This procedure shows how to create an availability zone using the VMware Integrated OpenStack UI. You can also create an availability zone using the **`viocli update neutron`** command. See "Create a Neutron Availability Zone with NSX-T Data Center" in the *VMware Integrated OpenStack Administration Guide* for VMware Integrated OpenStack 6.0.

Prerequisites

Create a separate DHCP profile and metadata proxy server for each availability zone. Availability zones can share an edge cluster or use separate edge clusters.

- For information about creating a DHCP profile, see "Create a DHCP Server Profile" in the *NSX-T Administration Guide*.
- For information about creating a metadata proxy server, see "Add a Metadata Proxy Server" in the *NSX-T Administration Guide*.

Procedure

1. Log in to VMware Integrated OpenStack.
2. Click **OpenStack Deployment** and select the deployment you want to configure.
3. Click the **Manage** tab, then click **Configure Neutron**.
4. Click the **Add** button and enter values for the availability zone.

Option	Description
Availability Zone	Enter a name for the availability zone. The alphanumeric string can include special characters (_) and (-).
Default overlay TZ	Select a default overlay transport zone for the availability zone.
Default VLAN TZ	Select a default VLAN transport zone for the availability zone.
Default Tier0 router	Select a default tier0 router for the availability zone.
DHCP profile	Select a DHCP profile configured for the availability zone.
Metadata proxy	Select the metadata proxy server configured for the availability zone.

5. Click **OK**.

Results

The new availability zone is created.

Example: Creating Separate Availability Zones for N-VDS Standard and Enhanced Data Path

The following procedure implements separate availability zones so that you can deploy NFV workloads on N-VDS in enhanced data path mode and other workloads in standard mode. In this example, VMware Integrated OpenStack has been deployed with NSX-T Data Center in standard mode. The availability zones are configured on the same tier-0 router and edge cluster. The VMware Integrated OpenStack management network uses the IP address range 192.0.2.10 to 192.0.2.50.

1. In NSX-T Data Center, configure an overlay transport zone and VLAN transport zone using N-VDS in enhanced data path mode. See "Enhanced Data Path" in the *NSX-T Data Center Installation Guide*.

The overlay transport zone is named `nfv-overlay-tz` and the VLAN transport zone is named `nfv-vlan-tz`.

2 Create a DHCP profile for the new availability zone.
   a In NSX Manager, select **Networking > DHCP**.
   b In the **Server Profiles** tab, click **Add**.
   c Enter **`nfv-dhcp`** as the name and select the existing edge cluster.
   d Click **Add**.
3 Create a metadata proxy server for the new availability zone.
   a In NSX Manager, select **Networking > DHCP**.
   b In the **Metadata Proxies** tab, click **Add**.
   c Enter **`nfv-mdp`** as the name.
   d Enter **`http://192.0.2.10:8775`** as the Nova server URL.
   e Enter **`mdpassword`** as the secret.
   f Select the existing edge cluster.
   g Click **Add**.
4 Log in to VMware Integrated OpenStack.
5 Select **OpenStack Deployment** and select the deployment you want to configure.
6 Click the **Manage** tab, then click **Configure Neutron**.
7 Click the **Add** button and enter values for the NFV availability zone.
   a Enter **`nfv-az`** for the name of the availability zone.
   b For the default overlay transport zone, select **nfv-overlay-tz**.
   c For the default VLAN transport zone, select **nfv-vlan-tz**.
   d Select a default tier0 router.
   e For the DHCP profile, select **nfv-dhcp**.
   f For the metadata proxy server, select **nfv-mdp**.
   g Click **OK**.
8 Create a network in the new availability zone.
   a Log in to the Integrated OpenStack Manager as the `root` user.
   b Load the cloud administrator credentials file.

```
sudo su -
source ~/cloudadmin.rc
```

c Create the network.

```
neutron net-create nfv-network --tenant-id nfv-project --availability-zone-hint nfv-az
```

vLAN Transparency

VLAN-transparent networks allow tagged packets to pass through without tags being removed or changed.

Note For VDS deployments, only provider networks can be transparent. For NSX Data Center for vSphere and NSX-T Data Center deployments, only tenant networks can be transparent.

To enable VLAN transparency on a network, include the `--transparent-vlan` parameter and disable port security when you create the network. For example:

```
openstack network create network-name --project project-uuid --transparent-vlan --disable-port-security
```

MAC Learning

MAC learning enables network connectivity for multiple MAC addresses behind a single vNIC. MAC learning is useful for distributing workloads in large OpenStack deployments.

MAC learning in VMware Integrated OpenStack is implemented differently for NSX-T Data Center and NSX Data Center for vSphere deployments.

- For NSX-T Data Center deployments, MAC learning in VMware Integrated OpenStack is provided by NSX-T Data Center MAC learning. For more information, see "Understanding MAC Management Switching Profile" in the *NSX-T Administration Guide*.
- For NSX Data Center for vSphere deployments, MAC learning in VMware Integrated OpenStack is implemented by enabling forged transmit and promiscuous mode. The guest must request promiscuous mode.

The following conditions apply to MAC learning:

- MAC learning is not compatible with port security or security groups.
- For NSX Data Center for vSphere deployments, performance will be affected because vNICs that request promiscuous mode receive a copy of every packet.
- For NSX Data Center for vSphere deployments, no RARP requests are generated for the multiple MAC addresses behind a single vNIC when a virtual machine is migrated with vMotion. This can result in a loss of connectivity.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user and open the toolbox.

```
ssh root@mgmt-server-ip
toolbox
```

2 Disable port security and security groups on the port where you want to configure MAC learning.

```
neutron port-update port-uuid --port-security-enabled false --no-security-groups
```

3 Enable MAC learning on the port.

```
neutron port-update port-uuid --mac-learning-enabled true
```

Provider Security Group

You can create a provider security group to block specific traffic for a project.

Standard security groups are created and managed by tenants, whereas provider security groups are created and managed by the cloud administrator. Provider security groups take precedence over standard security groups and are enforced on all virtual machines in a project.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Open the toolbox and set the password for the `admin` account.

```
toolbox
export OS_PASSWORD=admin-account-password
```

3 Create a provider security group for a specific project.

```
neutron security-group-create group-name --provider=True --tenant-id=project-id
```

4 Create rules for the provider security group.

Note Provider security group rules block the specified traffic, whereas standard security rules allow the specified traffic.

```
neutron security-group-rule-create group-name --tenant-id=project-id [--description rule-
description] [--direction {ingress | egress}] [--ethertype {IPv4 | IPv6}] [--protocol
protocol] [--port-range-min range-start --port-range-max range-end] [--remote-ip-prefix ip/
prefix | --remote-group-id remote-security-group]
```

Option	Description
group-name	Enter the provider security group.
--tenant-id	Enter the ID of the project containing the provider security group.
--description	Enter a custom description of the rule.
--direction	Specify **ingress** to block incoming traffic or **egress** to block outgoing traffic. If you do not include this parameter, `ingress` is used by default.
--ethertype	Specify **IPv4** or **IPv6**. If you do not include this parameter, `IPv4` is used by default.
--protocol	Specify the protocol to block. Enter an integer representation ranging from 0 to 255 or one of the following values: ■ **icmp** ■ **icmpv6** ■ **tcp** ■ **udp** To block all protocols, do not include this parameter.
--port-range-min	Enter the first port to block. To block all ports, do not include this parameter. To block a single port, enter the same value for the `--port-range-min` and `--port-range-max` parameters.
--port-range-max	Enter the last port to block. To block all ports, do not include this parameter. To block a single port, enter the same value for the `--port-range-min` and `--port-range-max` parameters.
--remote-ip-prefix	Enter the source network of traffic to block (for example, 10.10.0.0/24). This parameter cannot be used together with the `--remote-group-id` parameter.
--remote-group-id	Enter the name or ID of the source security group of traffic to block. This parameter cannot be used together with the `--remote-ip-prefix` parameter.

Results

The provider security group rules are enforced on all newly created ports on virtual machines in the specified project and cannot be overridden by tenant-defined security groups.

What to do next

You can enforce one or more provider security groups on existing ports by running the following command:

```
neutron port-update port-id --provider-security-groups list=true group-id1...
```

NSX-V Security Policy

You can enforce NSX Data Center for vSphere security policies through Neutron security groups. This feature can also be used to insert third-party network services.

Provider and standard security groups can both consume NSX Data Center for vSphere security policies. Rule-based provider and standard security groups can also be used together with security policy-based security groups. However, a security group associated with a security policy cannot also contain rules.

Security policies take precedence over all security group rules. If more than one security policy is enforced on a port, the order in which the policies are enforced is determined by NSX Data Center for vSphere. You can change the order in the vSphere Client on the **Security > Firewall** page under **Networking and Security**.

Prerequisites

Create the desired security policies in NSX Data Center for vSphere. See "Create a Security Policy" in the *NSX Administration Guide*.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Modify the Neutron configuration.

```
viocli update neutron
```

3 In the `nsxv` section, add the `use_nsx_policies`, `default_policy_id`, and `allow_tenant_rules_with_policy` parameters and configure them.

Option	Description
`use_nsx_policies`	Enter **`true`**.
`default_policy_id`	Enter the ID of the NSX Data Center for vSphere security policy that you want to associate with the default security group for new projects. If you do not want to use a security policy by default, you can leave this parameter commented out. To find the ID of a security policy, log in to the vSphere Client and select **Menu > Networking & Security**. Click **Service Composer** and open the **Security Policies** tab. Click the **Show Columns** icon at the bottom left of the table. Select **Object Id** and click **OK**. The ID of each security policy is displayed in the table.
`allow_tenant_rules_with_policy`	Enter **`true`** to allow tenants to create security groups and rules or **`false`** to prevent tenants from creating security groups or rules.

The configuration file now looks similar to the following:

```
conf:
  [...]
  plugins:
    nsx:
      [...]
      nsxv:
        use_nsx_policies: true
        default_policy_id: policy-5
        allow_tenant_rules_with_policy: true
```

4 If you want to use additional security groups with security policies, you can perform the following steps:

- To associate an NSX Data Center for vSphere security policy with a new security group, specify the desired policy when creating the group:

  ```
  toolbox
  export OS_PASSWORD=admin-account-password
  neutron security-group-create security-group-name --tenant-id tenant-uuid --
  policy=policy-id
  ```

- To migrate an existing security group to a security policy-based group, run the following command from the Neutron server:

  ```
  kubectl -n openstack exec -it neutron-server-pod-name -- /bin/bash
  nsxadmin -r security-groups -o migrate-to-policy --property policy-id=policy-id --
  property security-group-id=security-group-uuid
  ```

  Note This command removes all rules from the specified security group. Ensure that the target policy is configured such that the network connection will not be interrupted.

5 Configure Neutron to prioritize NSX Data Center for vSphere security policies over security groups.

```
kubectl -n openstack exec -it neutron-server-pod-name -- /bin/bash
sudo -u neutron nsxadmin --config-file /etc/neutron/neutron.conf --config-file /etc/
neutron/plugins/vmware/nsx.ini -r firewall-sections -o nsx-reorder
```

Load Balancer

You can create load balancers to distribute incoming requests among designated instances. Load balancers ensure that workloads are shared predictably among instances and system resources are used more effectively.

VMware Integrated OpenStack 7.1 supports the OpenStack Octavia component.

Note

- Starting from VIO 7.1, you can use the Octavia flavors and this is supported only with NSX-T Policy plugin. Support for Octavia flavors allows users for leveraging the OpenStack Octavia flavors capability on load balancers. For information about OpenStack Octavia flavors, see https://docs.openstack.org/octavia/latest/admin/flavors.html.

Prerequisites

- Create a public subnet and router on your network. For an NSX Data Center for vSphere deployment, the router type must be `exclusive`.

  Note You can create the load balancer on a tenant subnet, but you must assign it a floating IP address.

- Configure at least one client and at least two server instances.
- Verify that you have one of the following roles so that you can operate Horizon or the OpenStack CLI.

Role	Description
load-balancer_observer	User with access to load-balancer read-only APIs.
load-balancer_global_observer	User with access to load-balancer read-only APIs including resources owned by others.
load-balancer_member	User with access to load-balancer read and write APIs.
load-balancer_quota_admin	Admin for quota APIs only.
load-balancer_admin	Admin for all load-balnacer APIs including resources owned by others.
admin	Admin to all APIs.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard.

2 Select your project from the drop-down menu in the title bar.

3 Select **Project > Network > Load Balancers** and click **Create Load Balancer**.

4 On the **Load Balancer Details** page, enter the desired configuration and click **Next**.

Option	Description
Name	Enter a name for the load balancer.
Description	(Optional) Enter a description of the load balancer.
IP Address	(Optional) Enter the IP address of the load balancer.
Subnet	Select a subnet for the load balancer. Only members of this subnet can be added to the LBaaS pool.

5 On the **Listener Details** page, enter the desired configuration and click **Next**.

Option	Description
Name	Enter a name for the listener.
Description	Enter a description of the listener.
Protocol	Select the protocol for the listener to use. The following protocols are supported: ■ HTTP ■ TCP ■ Terminated HTTPS ■ HTTPS If you select terminated HTTPS as the protocol, you must also provide the ID of the TLS container.
Port	Enter the port for the listener to use.

6 Specify the name, description, and load balancing method for your LBaaS pool and click **Next**.

Supported load balancing methods are described as follows:

Method	Description
LEAST_CONNECTIONS	New client requests are sent to the server with the fewest connections.
ROUND_ROBIN	Each server is used in turn according to the weight assigned to it.
SOURCE_IP	All connections that originate from the same source IP address are handled by the same member of the pool.

7 Select the server and client instances to add to the load balancer pool and click **Next**.

8 Specify parameters for the health monitor and click **Next**.

Parameter	Description
Monitor type	Specify **HTTP**, **PING**, or **TCP**.
Interval	Enter the time in seconds between sending probes to members.

Parameter	Description
Retries	Enter the number of connection failures allowed before changing the member status to `INACTIVE`.
Timeout	Enter the time in seconds that a monitor will wait for a connection to be established before it times out. The timeout value must be less than the interval value.

If you select **HTTP**, you must also configure the HTTP method, expected status code, and URL.

9 If you selected the `TERMINATED_HTTPS` protocol for listener details, specify one or more certificates for the listener and click **Next**.

10 Click **Create Load Balancer**.

11 If you created the load balancer on a tenant subnet, associate a floating IP address with the load balancer.

a Click the down arrow to the right of the load balancer and select **Associate Floating IP**.

b Select a floating IP address or pool and click **Associate**.

12 (Optional) Send test requests to validate your LBaaS configuration.

a Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

b Create a test `index.html` file.

c In the same directory, start a web server.

```
sudo python -m SimpleHTTPServer 80
```

d Log in to the client instance.

e Run the `wget` command to view whether your requests are being correctly load-balanced across the servers in the pool.

```
wget -O - http://mgmt-server-ip
```

What to do next

You can open the load balancer and click **Create Listener** to add listeners to it.

DNS Zone

If OpenStack Designate (DNS as a service) is configured for your environment, you can create DNS zones and record sets on demand using the VMware Integrated OpenStack dashboard.

Prerequisites

Verify that your cloud administrator has enabled Designate for your environment. For more information, see "Enable the Designate Component" in the *VMware Integrated OpenStack Installation and Configuration Guide*.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard.

2 Select your project from the drop-down menu in the title bar.

3 Select **Project > DNS > Zones** and click **Create Zone**.

If the **DNS** option does not appear, Designate has not been enabled.

4 Specify the parameters for your DNS zone and click **Submit**.

Option	Description
Name	Enter your DNS zone. The value must end with a period (.).
Description	Enter details about the zone.
Email Address	Enter the email address of the zone owner.
TTL	Specify the time to live (TTL) in seconds for records in the zone.
Type	Select whether to create a primary or secondary zone.

5 Click **Create Record Set**.

6 Specify the parameters for your record set and click **Submit**.

Option	Description
Type	Select the type of record set. The following values are supported: ■ A (address record) ■ AAAA (IPv6 address record) ■ CNAME (canonical name record) ■ MX (mail exchange record) ■ PTR (pointer record) ■ SPR (sender policy framework) ■ SRV (service locator) ■ SSHFP (SSH public key fingerprint) ■ TXT (text record)
Name	Enter the domain name for the record set. The value must end with a period (.).
Description	Enter details about the record set.
TTL	Specify the TTL in seconds for records in the record set.
Records	Specify one or more records to include in the record set. Click **Add Record** to add multiple records.

You can create one or more record sets for each zone.

What to do next

You can click the name of your zone on the **DNS Zones** page to view information about it. Click the down arrow next to **Create Record Set** and select **Update** or **Delete** to modify or remove your zone. On the **Record Sets** tab, you can update or delete the record sets in your zone.

NSX-MP to NSX-P Migration

In VMware Integrated OpenStack 7.1, the Neutron driver supports NSX-MP to NSX-P migration.

You can migrate your VMware Integrated OpenStack deployments leveraging NSX-T Management plane to NSX-T Policy Manager.

You can also leverage the NSX-T capabilities exposed only with Policy Manager such as IPv6 support with DHCPv6 and SLAAC.

In addition, objects created by VMware Integrated OpenStack on NSX-T can also be displayed in NSX Policy user interface. The migration process performs the following operations:

- Verifies that you use the minimum required NSX-T version.
- Validate tests, more specifically:
  - The test ensures that it does not configure unsupported service plugins. VMware Integrated OpenStack with NSX-T Policy does not support Neutron layer-2 gateway extension.
  - The test verifies that BGP is enabled on the Tier-0 gateways and the DHCP relay is not configured for any availability zone.
- Migrates all resources managed by VMware Integrated OpenStack, Tier-0 routers, profiles, and other NSX-T resources not consumed by VMware Integrated OpenStack.
  - At the end of the process, NSX-T resource corresponding to Neutron objects can have the same id as the Neutron.
  - Tags applied to resources on NSX-Policy Manager are the same as tags previously applied on NSX-T Management Plane.

- Reconfigures the VMware Integrated OpenStack control plane for using the policy plugin instead of the MP plugin. It also updates the Neutron custom resource required for running the NSX Policy plugin.

Note

- When migrating from NSX MP to the NSX Policy, the VMware Integrated OpenStack orchestrates the NSX migration coordinator for promoting Management Plane objects to Policy objects.
- The VMware Integrated OpenStack controls each NSX objects associated with Neutron resources, and other dependent objects such as certificates and profiles.
- If you modify backend resources directly, the NSX resource is not in sync with Neutron status and VMware Integrated OpenStack cannot perform the promotion for that specific resource causing the migration to the Policy fail.
- After you finish the migration, ensure that the NSX resources managed by VMware Integrated OpenStack remain unaltered at the backend.

Prerequisites

- Verify that you use NSX-T 3.1.0 or later for the MP to the Policy migration.
- Verify that the migration coordinator service is running on NSX-T.

  Note You must backup NSX-T manager before triggering the migration. If the migration fails, you must restore the NSX manager and retry the migration from VMware Integrated OpenStack once restore has been successful. After the migration, you cannot revert to NSX-T Management plane. There is no supported solution to revert to the NSX MP plugin after a successful migration to the NSX-T Policy manager.

Procedure

1 Start the migration service on `nsx`. SSH to the first `nsx` manager as the `admin` user and run:

```
start service migration-coordinator
```

2 Log in to the VMware Integrated OpenStack manager and run:

```
viocli update neutron
```

Add the following code in Neutron configuration. After the update, you can see `neutron-mp2p-migration` pod `CREATED` and `RUNNING`.

```
manifests:
 mp2p_migration: true
```

3 Monitor the `neutron-mp2p-migration` pod. If the migration process is complete, the status of the pod appears as: `COMPLETED`. You can use the following code for verifying that the Neutron server uses the policy plugin.

```
viocli update neutron
manifests:
  mp2p_migration: true
  vmware_dvs_plugin: false
  vmware_nsxpolicy_plugin: true
  vmware_nsxv_plugin: false
  vmware_nsxv3_plugin: false
```

4 Once the migration is complete and the Neutron server pods have started the new configuration, SSH to the `nsx` manager to stop the migration, by running:

```
stop service migration-coordinator
```

Results

After successful migration, you can see that the migrated resources from MP are in the Policy.

Nova Instances

5

Instances are virtual machines that run in the cloud.

You can manage instances for users in various projects. You can view, terminate, edit, perform a soft or hard reboot, create a snapshot from, and migrate instances. You can also view the logs for instances or start a VNC console for an instance.

This chapter includes the following topics:

OpenStack Flavors

In OpenStack, a flavor is a preset configuration that defines the compute, memory, and storage capacity of an instance.

All VMware Integrated OpenStack deployments contain the following default flavors.

Name	vCPUs	RAM (GB)	Root Disk (GB)
m1.tiny	1	0.5	1
m1.small	1	2	20
m1.medium	2	4	40
m1.large	4	8	80
m1.xlarge	8	16	160

Important Do not delete the default flavors.

You can create and manage additional flavors as needed. To manage the flavors in your deployment, log in to the VMware Integrated OpenStack dashboard as a cloud administrator and select **Admin > Compute > Flavors**.

Create Instance

You can launch an instance from an image, volume, instance snapshot, or volume snapshot.

Prerequisites

- Verify that your OpenStack deployment contains the image, volume, or snapshot from which you want to launch the instance.
- Verify that the flavor and network for the instance have been created.

Procedure

1. Log in to the VMware Integrated OpenStack dashboard.
2. Select your project from the drop-down menu in the title bar.
3. Select **Project > Compute > Instances** and click **Launch Instance**.
4. On the **Details** page, enter the desired configuration and click **Next**.

Option	Description
Instance Name	Enter a name for the instance.
Description	Enter a description of the instance.
Availability Zone	Select a Nova availability zone in which to place the instance.
Count	Specify the number of copies of this instance that you want to create.

5. On the **Source** page, select whether you want to boot the instance from an image, instance snapshot, volume, or volume snapshot.

   For instances booted from images or instance snapshots, you can choose to use persistent storage by creating a new volume. For instances booted from volumes or volume snapshots, you can choose to delete the specified volume or snapshot when the instance is deleted.

6 From the **Available** table, select the desired object and click **Next**.

7 On the **Flavor** page, select the desired flavor and click **Next**.

8 On the **Networks** page, select one or more networks and click **Next**.

9 On the **Network Ports** page, select one or more ports and click **Next**.

You must select at least one network or at least one port to launch the instance.

10 (Optional) Proceed through the wizard to specify security groups, a key pair, custom configurations, server groups, scheduler hints, and metadata.

11 Click **Launch Instance**.

Results

The instance is created in OpenStack, and the corresponding virtual machine is created in vSphere.

What to do next

In the **Actions** column, you can attach and detach interfaces and volumes, associate a floating IP address with the instance, and perform a variety of other actions.

Migrate Instance

You can live-migrate an OpenStack instance to a different compute node.

VMware Integrated OpenStack does not support the following VM migration scenarios:

- Migration of a VM between two different vCenter Servers.
- Migration of a VM within a cluster. To migrate a VM within a cluster, you must use vSphere.

To migrate VMs between clusters, you can use VMware Integrated OpenStack, if the source and the target clusters are in the same vCenter instance.

Note Instances managed by VMware Integrated OpenStack must be migrated by using OpenStack commands. Do not use vCenter Server, or other methods to migrate OpenStack instances.

Prerequisites

- Verify that the source and target compute nodes are present within the same vCenter Server instance.
- Verify that your environment includes a shared datastore that all hosts and clusters can access.
- Verify that the source and target compute nodes have at least one distributed switch in common. If two distributed switches are attached to the source compute node but only one distributed switch is attached to the target compute node, live migration can succeed but the OpenStack instance must be connected only to the port group of the distributed switch common to both compute nodes.

- Verify that any FCD volumes are detached.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 If the instance has a CD-ROM drive attached, configure a shared datastore for CD-ROM migration.

a Edit the Nova compute configuration.

```
viocli update nova-compute
```

b In the `vmware` section, add the `shared_datastore_regex` parameter and set its value to the name of the shared datastore in vSphere.

3 Open the toolbox.

```
toolbox
```

4 For the migration, if you are not selecting compute node as the target, you can run the following command:

```
openstack server migrate --live-migration instance-uuid --os-compute-api-version 2.30
```

For migrating an instance to the specified host, run the following command:

```
nova --os-compute-api-version 2.67 live-migration --force [--block-migrate] <server>
[<host>]
```

For example:

```
nova --os-compute-api-version 2.67 live-migration --force 7a9fd8a8-b3f2-4c72-af0e-
ef0b856d7715  compute-35a9679c-c97
```

You must specify `--os-compute-api-version 2.67`, `[host]`, and `--force` options in the command.

- To find the name of a compute node, run the `openstack host list` command and view the **Host Name** column.
- To find the UUID of the instance, run the `openstack server list` command and view the **ID** column.

What to do next

You can run the `openstack server show instance-uuid` command to confirm that the instance has been migrated to the desired compute node.

Instance Live Resize

You can enable live resize for OpenStack instances by configuring image metadata. With live resize, you can change the disk size, memory, and vCPUs of an instance while the instance is powered on.

The following limitations apply to live resizing:

- Do not use live resize to create instances using SR-IOV-enabled ports. Live resize is not compatible with SR-IOV.
- Do not use instances that have been enabled for live resize in tenant virtual data centers. Live resize is not compatible with tenant virtual data centers.
- Do not add more than 3GB of memory to a Linux 64-bit or a Windows 7 32-bit operating system. For details, see KB 2008405.

Note Live resize only supports increasing values for disk size, memory, and vCPUs of an instance.

Additionally, the following conditions apply for live resizing of disk size:

- Use VMDK as the disk format for the image.
- Use a SCSI virtual disk adapter type for the image. IDE adapter types are not supported.
- Deploy virtual machines from the image as full clones. Linked clones cannot be live resized.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user and open the toolbox.

```
ssh root@mgmt-server-ip
toolbox
```

2 Create a new image with live resize enabled.

```
openstack image create image-name --disk-format {vmdk | iso} --container-format bare
--file image-file {--public | --private} [--property vmware_adaptertype="vmdk-adapter-
type"] [--property vmware_disktype="{sparse | preallocated | streamOptimized}"] --
property vmware_ostype="operating-system" --property img_linked_clone="false" --property
os_live_resize="{vcpu | memory | disk}"
```

Option	Description
image-name	Enter the name of the source image.
--disk-format	Enter **vmdk**.
--container-format	Enter **bare**. The container format argument is not currently used by Glance.
--file	Specify the image file to upload.
{--public | --private}	Include `--public` to make the image available to all users or `--private` to make the image available only to the current user.

Option	Description
--property vmware_adaptertype	Specify the adapter type of the VMDK disk. For disk live resize, you must specify a SCSI adapter. If you do not include this parameter, the adapter type is determined by introspection.
--property vmware_disktype	Specify **sparse**, **preallocated**, or **streamOptimized**. If you do not include this parameter, the disk type is determined by introspection.
--property vmware_ostype	Specify the operating system on the image.
--property img_linked_clone	Enter **false**.
--property os_live_resize	Specify **vcpu**, **memory**, **disk**, or any combination separated by commas (for example, **vcpu,memory,disk**).

Results

When you create virtual machines using the image that you defined in this procedure, those virtual machines can be resized without needing to be powered off.

Instance with Multi vNIC

You can configure the virtual interfaces on an OpenStack instance to use different drivers.

You specify virtual interface drivers by adding the `vmware_extra_config` metadata to a Glance image. Any virtual interfaces that are not specifically assigned a driver in this procedure will use the value of the `hw_vif_model` metadata. If the `hw_vif_model` metadata is not set, those interfaces will use the default driver for the image.

The following values are supported for virtual interface drivers:

- `e1000`
- `e1000e`
- `pcnet`
- `sriov`
- `vmxnet`
- `vmxnet3`

Procedure

1. Log in to the VMware Integrated OpenStack dashboard.
2. Select your project from the drop-down menu in the title bar.
3. Select **Project > Compute > Images**.
4. Create a new image or select an existing image on which you want to configure multiple drivers.

5 Select **Update Metadata** next to the image that you want to use.

6 In the **Custom** field under **Available Metadata**, type **`vmware_extra_config`** and click the **Add** (plus sign) icon.

7 Set the value of `vmware_extra_config` to a JSON array in the following format:

```
{"hw_vif_models": {"vif1-id": "driver-name", ...}
```

For example, the following value configures the first virtual interface with the `e1000` driver and the third virtual interface with the `vmxnet3` driver:

```
{"hw_vif_models": {"1": "e1000", "3": "vmxnet3"}
```

Instance with Huge Page

Huge pages (known as large pages in Windows) can improve performance for some workloads. VMware Integrated OpenStack supports a maximum page size of 1 GB.

Prerequisites

Verify that your deployment is running on vSphere 6.7 or later.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

2 Select the **admin** project from the drop-down menu in the title bar.

3 Configure a flavor for huge page support.

a Select **Admin > Compute > Flavors**.

b Create a new flavor or choose an existing flavor to use for instances with huge page support.

c Select **Update Metadata** next to the flavor that you want to use.

d In the **Available Metadata** pane, expand **Guest Memory Backing** and click the **Add** (plus sign) icon next to **Size of memory page**.

e Set the value of `hw:mem_page_size` to **`large`**.

f In the **Available Metadata** pane, expand **VMware Quota** and click the **Add** (plus sign) icon next to **Quota: Memory Reservation in Percentage**.

g Set the value of `quota:memory_reservation_percent` to **`100`** and click **Save**.

4 Configure an image for huge page support.

a Select **Admin > Compute > Images**.

b Create a new image or choose an existing image to use for instances with huge page support.

c Select **Update Metadata** next to the image that you want to use.

d In the **Available Metadata** pane, expand **Guest Memory Backing** and click the **Add** (plus sign) icon next to **Size of memory page**.

e Set the value of `hw_mem_page_size` to **`large`**.

f In the **Available Metadata** pane, expand **VMware Quota** and click the **Add** (plus sign) icon next to **Quota: Memory Reservation in Percentage**.

g Set the value of `quota_memory_reservation_percent` to **`100`** and click **Save**.

5 Launch an OpenStack instance using the flavor and image created in this procedure.

For instructions, see Create Instance.

6 Log in to the guest operating system of the instance and enable huge page support.

For instructions, see the documentation for your guest operating system.

Instance with vCPU Pinning

When running latency-sensitive applications inside a virtual machine, you can use virtual CPU pinning to eliminate the extra latency that virtualization imposes.

Important This feature is offered in VMware Integrated OpenStack Carrier Edition only. For more information, see "VMware Integrated OpenStack Licensing" in the *VMware Integrated OpenStack Installation and Configuration Guide*.

Virtual CPU pinning enables high latency sensitivity and ensures that all memory and an entire physical core are reserved for the virtual CPU of an OpenStack instance. You configure virtual CPU pinning on a flavor and then create instances with that flavor.

To enable high latency sensitivity for selected virtual CPUs within a VM, you can use flavor extra specs. See Supported Extra Specs for Flavor.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

2 Select the **admin** project from the drop-down menu in the title bar.

3 Select **Admin > Compute > Flavors**

4 Create a flavor or choose an existing flavor to use for virtual CPU pinning.

5 Select **Update Metadata** next to the flavor that you want to use.

6 In the **Available Metadata** pane, select and configure the required metadata.

a Expand **CPU Pinning** and click the **Add** (plus sign) icon next to **CPU Pinning policy**.

b Set the value of `hw:cpu_policy` to **`dedicated`**.

c Expand **VMware Policies** and click the **Add** (plus sign) icon next to **VM latency sensitivity**.

d Set the value of `vmware:latency_sensitivity_level` to **`high`**.

e Expand **VMware Quota** and click the **Add** (plus sign) icon next to **CPU Reservation in Percentage** and **Memory Reservation in Percentage**.

f Set the value of `quota:cpu_reservation_percent` and `quota:memory_reservation_percent` to **`100`**.

7 Click **Save**.

What to do next

You can now enable virtual CPU pinning on an instance by configuring it with the flavor that you modified in this procedure.

Instance with NUMA Affinity

VMware Integrated OpenStack supports non-uniform memory access (NUMA)-aware placement of OpenStack instances on the underlying vSphere environment.

Important This feature is offered in VMware Integrated OpenStack Carrier Edition only. For more information, see "VMware Integrated OpenStack Licensing" in the *VMware Integrated OpenStack Installation and Configuration Guide*.

NUMA links small, cost-effective nodes using a high-performance connection to provide low latency and high throughput. This performance is often required for virtual network functions (VNFs) in telecommunications environments. For information about NUMA in vSphere, see "Using NUMA Instances with ESXi" in *vSphere Resource Management*.

To obtain information about your current NUMA configuration, run the following command on your ESXi hosts:

```
vsish -e get /net/pNics/vmnic<id>/properties | grep 'Device NUMA Node'
```

Prerequisites

- Ensure that vCPUs, memory, and physical NICs intended for virtual machine traffic are placed on same node.
- In vSphere, create a teaming policy that includes all physical NICs on the NUMA node. See "Teaming and Failover Policy" in *vSphere Networking*.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Open the toolbox and set the password for the `admin` account.

```
toolbox
export OS_PASSWORD=admin-account-password
```

3 Create a Neutron network on which all physical NICs are located on a single NUMA node.

4 Create an OpenStack flavor that includes the `numa.nodeAffinity` property.

```
nova flavor-key flavor-id set vmware:extra_config='{"numa.nodeAffinity": "numa-node-id"}'
```

5 Launch an OpenStack instance using the flavor and network created in this procedure.

Instance with Storage Policy

You can use Storage Policy Based Management (SPBM) in vSphere to create storage policies that control the datastores on which OpenStack instances are created.

Note After you set a storage policy on an FCD volume, you cannot remove the storage policy from the volume. However, you can change the storage policy used by an unattached volume.

Prerequisites

Create the desired storage policy in vSphere. For details, see "Storage Policy Based Management" (SPBM) in the *vSphere Storage* document.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Edit the Nova compute configuration.

```
viocli update nova-compute
```

a In the `DEFAULT` section, add the `enabled_filters` parameter with the values listed in the following example.

```
enabled_filters: "RetryFilter, AvailabilityZoneFilter, ComputeFilter,
ComputeCapabilitiesFilter,
ImagePropertiesFilter, ServerGroupAntiAffinityFilter, ServerGroupAffinityFilter,
PciPassthroughFilter, AggregateInstanceExtraSpecsFilter"
```

b In the `vmware` section, add the `pbm_default_policy` parameter. Set its value to the name of the storage policy to use by default when an instance is created with a flavor that is not associated with a storage policy. The value must reference a storage policy that you configure on the vCenter Server.

c In the `vmware` section, add the `pbm_enabled` parameter and set its value to **`true`**.

d In the `vmware` section, add the `use_linked_clone` parameter and set its value to **`false`**.

The following example shows an updated configuration.

```
conf:
nova:
  DEFAULT:
    enabled_filters: "RetryFilter, AvailabilityZoneFilter, ComputeFilter,
ComputeCapabilitiesFilter, ImagePropertiesFilter, ServerGroupAntiAffinityFilter,
ServerGroupAffinityFilter, PciPassthroughFilter, AggregateInstanceExtraSpecsFilter"
  neutron:
    metadata_proxy_shared_secret:
".Secret:managedencryptedpasswords:data.metadata_proxy_shared_secret"
  vmware:
    passthrough: "false"
    pbm_default_policy: "Your Default Storage Policy"
    pbm_enabled: "true"
    tenant_vdc: "false"
    use_linked_clone: "false"
```

3 Edit the Nova configuration.

```
viocli update nova
```

a In the `DEFAULT` section, add the `enabled_filters` parameter with the values listed in the following example.

```
enabled_filters: "RetryFilter, AvailabilityZoneFilter, ComputeFilter,
ComputeCapabilitiesFilter, ImagePropertiesFilter, ServerGroupAntiAffinityFilter,
ServerGroupAffinityFilter, PciPassthroughFilter, AggregateInstanceExtraSpecsFilter"
```

b In the `vmware` section, add the `pbm_default_policy` parameter. Set its value to the name of the storage policy to use by default when an instance is created with a flavor that is not associated with a storage policy. The value must reference a storage policy that you configure on the vCenter Server.

c In the `vmware` section, add the `pbm_enabled` parameter and set its value to **`true`**.

d In the `vmware` section, add the `use_linked_clone` parameter and set its value to **`false`**.

The following example shows an updated configuration.

```
conf:
nova:
  DEFAULT:
    enabled_filters: "RetryFilter, AvailabilityZoneFilter, ComputeFilter,
ComputeCapabilitiesFilter, ImagePropertiesFilter, ServerGroupAntiAffinityFilter,
ServerGroupAffinityFilter, PciPassthroughFilter, AggregateInstanceExtraSpecsFilter"
  neutron:
    metadata_proxy_shared_secret:
".Secret:managedencryptedpasswords:data.metadata_proxy_shared_secret"
  vmware:
```

```
    passthrough: "false"
    pbm_default_policy: "Your Default Storage Policy"
    pbm_enabled: "true"
    tenant_vdc: "false"
    use_linked_clone: "false"
```

4 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

5 Select the **admin** project from the drop-down menu in the title bar.

6 Select **Admin > Compute > Flavors**.

7 Create a new flavor or choose an existing flavor.

8 Click **Update Metadata** to the right of the flavor.

9 In the **Available Metadata** pane, expand **VMware Policies** and click the **Add** (plus sign) icon next to **Storage Policy**.

10 Enter the desired storage policy name as the value of the `vmware:storage_policy` parameter and click **Save**.

Results

The specified vSphere storage policy is applied to all new OpenStack instances that are created from the flavor. The default storage policy is applied to all new instances that are created from a flavor not associated with a storage policy.

Instance Placement with Affinity

You can place instances using OpenStack server groups with an affinity or anti-affinity policy. Affinity indicates that all instances in the group must placed on the same host, and anti-affinity indicates that no instances in the group can be placed on the same host.

Affinity and anti-affinity policies cannot determine the specific ESXi host on which instances are placed. These policies only control whether instances are placed on the same hosts as other instances in a server group. To place instances on specific hosts, see Instance Placement with DRS.

Prerequisites

Verify that the intended filter configuration does not conflict with any existing administrative configuration, such as DRS rules that manage instance placement on hosts.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

2 Select the **admin** project from the drop-down menu in the title bar.

3 Select **Project > Compute > Server Groups**.

4 Click **Create Server Group** and enter the desired configuration.

Option	Description
Name	Enter a name for the server group.
Policy	Select the desired policy. ■ **Affinity**: places instances on the same host. ■ **Anti Affinity**: place instances on separate hosts. ■ **Soft Anti Affinity**: place instances on separate hosts if possible. ■ **Soft Affinity**: place instances on the same host if possible.

What to do next

When you launch an instance, select the appropriate server group to implement affinity or anti-affinity.

Instance Placement with DRS

You can use vSphere DRS settings to control how OpenStack instances are placed on hosts in the compute cluster. After configuring DRS, you modify the metadata of source images in OpenStack to ensure that instances generated from those images are correctly identified for placement.

Define VM and Host Groups for Placing OpenStack Instances

You define VM and host groups to contain and manage specific OpenStack instances.

Prerequisites

- Ensure that the compute cluster contains at least one virtual machine. If the compute cluster does not contain any virtual machines, create a dummy virtual machine for this procedure.
- On the compute cluster, enable DRS and set **DRS Automation** to **Partially automated** or **Fully automated**.
- On the compute cluster, set **Power Management** to **Off**.

Procedure

1 In the vSphere Client, select the compute cluster and click **Configure**.

2 Under **Configuration**, click **VM/Host Groups**.

3 Create a VM group.

   a Click **Add**.

   b Enter a name and select **VM Group** from the **Type** drop-down menu.

   c Click **Add**.

   d On the **Filter** tab, select virtual machines to add to the group.

   e Click **OK**.

4 Create a host group.

   a Click **Add**.

   b Enter a name and select **Host Group** from the **Type** drop-down menu.

   c Click **Add**.

   d On the **Filter** tab, select hosts to add to the group.

   e Click **OK**.

What to do next

Create a rule that determines how OpenStack instances assigned to the VM group are distributed on the hosts in the host group.

Create a DRS Rule for OpenStack Instance Placement

You create a DRS rule to manage the distribution of OpenStack instances in a VM group to a specific host group.

Prerequisites

- Define at least one VM group and at least one host group. See Define VM and Host Groups for Placing OpenStack Instances.
- On the compute cluster, enable DRS and set **DRS Automation** to **Partially automated** or **Fully automated**.
- On the compute cluster, set **Power Management** to **Off**.

Procedure

1 In the vSphere Client, click the compute cluster and select **Configure**.

2 Under **Configuration**, click **VM/Host Rules**.

3 Click the **Add...** button.

4 Enter a name for the rule and select the **Enable rule** option.

5 In the **Type** drop-down menu, select **Virtual Machines to Hosts**.

6 In the **VM Group** drop-down menu, select the VM group that contains the OpenStack instances you want to place.

7 In the next drop-down menu, select a specification for the rule.

Option	Description
Must run on hosts in group	OpenStack instances in the specified VM group must run on hosts in the specified host group.
Should run on hosts in group	OpenStack instances in the specified VM group should, but are not required, to run on hosts in the specified host group.

Option	Description
Must not run on hosts in group	OpenStack instances in the specified VM group must never run on hosts in the specified host group.
Should not run on hosts in group	OpenStack instances in the specified VM group should not, but may, run on hosts in the specified host group.

8 In the **Host Group** drop-down menu, select the host group that contains the hosts on which the OpenStack instances will be placed and click **OK**.

What to do next

In the VMware Integrated OpenStack dashboard, modify the metadata for a specific image to ensure that all instances generated from that image are automatically included in the VM group and therefore subject to the DRS rule.

Apply VM Group Settings to Image Metadata

You modify the metadata of a source image to automatically place instances into VM groups. DRS rules then determine the host groups on which these instances will be created.

Prerequisites

Configure a VM group and host group for the compute cluster.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

2 Select the **admin** project from the drop-down menu in the title bar.

3 Select **Admin > Compute > Images**.

4 Create a new image or choose an existing image.

5 Click the down arrow next to the flavor that you want to use and select **Update Metadata**.

6 In the **Available Metadata** pane, expand **VMware Policies** and click the **Add** (plus sign) icon next to **DRS VM group**.

7 Enter the desired VM group name as the value of the `vmware_vm_group` parameter and click **Save**.

Results

All OpenStack instances generated from this source image will be automatically assigned to the specified VM group and governed by its DRS rules.

Configure Device Passthrough

You can configure passthrough for networking, non-networking, and NVIDIA GRID vGPUs.

Networking Devices

You can configure a port to allow SR-IOV passthrough and then create OpenStack instances that use physical network adapters.

If you want to create multiple ports with different SR-IOV physical NICs to provide network redundancy for a VM, perform the optional steps in the following procedure.

Prerequisites

- Enable SR-IOV in vSphere. See "Enable SR-IOV on a Host Physical Adapter" in *vSphere Networking*.
- Create a dedicated compute cluster for SR-IOV devices. DRS rules do not apply to these devices.
- To persist the MAC address of a physical device, add its cluster as a compute node before enabling passthrough on the device. If passthrough has already been enabled, you can disable it, restart the cluster, and enable direct passthrough again.
- Enable VMware Integrated OpenStack Carrier Edition features. See "Enable Carrier Edition Features" in the *VMware Integrated OpenStack Installation and Configuration Guide*.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Edit the Nova compute configuration.

```
viocli update nova-compute
```

3 Add the following information in the `nova_compute` section.

```
pci:
  passthrough_whitelist:
    type: multistring
    values:
    - '{"product_id": "*", "vendor_id": "*", "physical_network": "*"}'
```

4 If you are using a DVS or NSX-T Data Center deployment, add the `dvs_moid` parameter in the `vmware` section.

```
dvs_moid: sriov-vds-moid
```

Set the value of `dvs_moid` to the managed object identifier (MOID) of the distributed switch associated with the compute cluster for SR-IOV devices.

5 Open the toolbox and set the password for the `admin` account.

```
toolbox
export OS_PASSWORD=admin-password
```

6 (Optional) If you want to configure port redundancy, create a VM flavor with the isolate property.

The isolate property ensures that the SR-IOV ports are by different physical NICs in the ESXi server host as required for port redundancy.

```
openstack flavor set <FLAVOR_ID> --property group_policy=isolate
```

FLAVOR_ID is the UUID of the Nova flavor to be used for the VMs with isolated SR-IOV ports.

7 Create a provider network for SR-IOV devices.

- For NSX Data Center for vSphere deployments, create a VLAN or port group network.
- For NSX-T Data Center deployments, create a VLAN or opaque network.
- For DVS deployments, create a VLAN network.

```
neutron net-create network-name --tenant-id project-uuid --provider:network_type {vlan |
portgroup | nsx-net} --provider:physical_network physical-id [--provider:segmentation_id
vlan-id]
```

Option	Description
network-name	Enter a name for the network.
`--tenant-id`	Specify the UUID of the project for which to create the port. You can find the UUID of a project by running the `openstack project list` command.
`--provider:network_type`	Enter **`vlan`** for a VLAN network, **`portgroup`** for a port group network, or **`nsx-net`** for an opaque network.
`--provider:physical_network`	■ For a VLAN network in NSX Data Center for vSphere, specify the MOID of the distributed switch. ■ For a VLAN network in NSX-T Data Center, specify the UUID of the VLAN transport zone. ■ For a VLAN network in a DVS deployment, specify the name of the distributed vSwitch. ■ For a port group network, specify the name of the port group. The network name must match the port group name. ■ For an opaque network, specify the UUID of the logical switch.
`--provider:segmentation_id`	If you want to create a VLAN-based network, enter the VLAN ID.

8 Create a subnet on the network.

```
neutron subnet-create network-id --tenant-id project-uuid --name subnet-name
```

Option	Description
network-id	Specify the UUID of the network on which to create the subnet. You can find the UUID of a network by running the `openstack network list` command.
--tenant-id	Specify the UUID of the project for which to create the subnet.
--name	Enter a name for the subnet.

9 Create a passthrough-enabled port by using the `--vnic_type direct` parameter.

```
neutron port-create network-id --tenant-id project-uuid --name port-name --vnic_type direct
```

Option	Description
network-id	Specify the UUID of the network on which to create the port. You can find the UUID of a network by running the `openstack network list` command.
--tenant-id	Specify the UUID of the project for which to create the port.
--name	Enter a name for the port.

Note Port security is not supported for passthrough-enabled ports and is automatically disabled for the port created.

To provide your OpenStack instance with access to physical network adapters, configure your instance with this single port. Or to deploy a VM with multiple ports that provide redundancy, note the port ID in the output and repeat this step to create a second direct port.

10 (Optional) Deploy a VM with the VM flavor and two direct ports.

```
nova boot --flavor <FLAVOR_ID> --image <IMAGE_ID> --nic port-id=<port1-id> --nic port-
id=<port2-id> <VM_NAME>
```

Option	Description
FLAVOR_ID	Specify the flavor created in Step 6.
--nic	Enter the port ID created with each direct port.

Non-Networking Devices

You can configure a flavor to allow passthrough and then create OpenStack instances that use physical hardware interfaces.

This procedure does not apply to NVIDIA GRID vGPUs. To configure an NVIDIA GRID vGPU, see NVIDIA GRID vGPU.

Prerequisites

- Enable SR-IOV or DirectPath I/O in vSphere:
  - To enable SR-IOV, see "Enable SR-IOV on a Host Physical Adapter" in *vSphere Networking*.
  - To enable DirectPath I/O, see "Enable Passthrough for a Network Device on a Host" in *vSphere Networking*.
- Create a dedicated compute cluster for SR-IOV devices. DRS rules do not apply to these devices.
- Verify that the `vmware_extra_config` metadata is not configured on the image that you want to use for passthrough.
- To persist the MAC address of a physical device, add its cluster as a compute node before enabling direct passthrough on the device. If direct passthrough has already been enabled, you can disable it, restart the cluster, and enable direct passthrough again.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Edit the Nova configuration.

```
viocli update nova
```

3 In the `nova` section, create the `DEFAULT` section. In the `DEFAULT` section, create the `pci_alias` section.

4 In the `pci_alias` section, add the `type` parameter and set its value to `multistring`.

5 Add the `values` parameter and set its value to match your device.

Use the following format:

```
values:
- '{"device_type": "type-PF", "vendor_id": "vendor-id", "name": "physical-name"}'
- '{"device_type": "type-VF", "vendor_id": "vendor-id", "name": "virtual-name"}'
```

Option	Description
vendor-id	Enter the four-character vendor ID for your device. Enter all letters in lowercase.
physical-name	Enter an alias for the physical device.
virtual-name	Enter an alias for the virtual device.

6 In the `vmware` section, add the `generic_passthrough` parameter and set its value to **`true`**.

The configuration file now looks similar to the following.

```
conf:
  nova:
    vmware:
      [...]
      generic_passthrough: true
    DEFAULT:
      pci_alias:
        type: multistring
        values:
        - '{"device_type": "type-PF", "vendor_id": "vendor-id", "name": "physical-name"}'
        - '{"device_type": "type-VF", "vendor_id": "vendor-id", "name": "virtual-name"}'
```

7 Edit the Nova compute configuration.

```
viocli update nova-compute
```

8 In the `vmware` section, add the `generic_passthrough` parameter and set its value to **`true`**.

The configuration file now looks similar to the following.

```
conf:
  nova_compute:
    DEFAULT:
      [...]
    vmware:
      [...]
      generic_passthrough: true
```

9 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

10 Select the **admin** project from the drop-down menu in the title bar.

11 Select **Admin > Compute > Flavors**.

12 Create a new flavor or choose an existing flavor to use for passthrough.

13 Select **Update Metadata** next to the flavor that you want to use.

14 In the **Custom** field under **Available Metadata**, type **`vmware_extra_config`** and click the **Add** (plus sign) icon.

15 Set the value of `vmware:extra_config` to **`{"pciPassthru.use64bitMMIO":"TRUE"}`**.

16 In the **Custom** field under **Available Metadata**, type **`pci_passthrough:alias`** and click the **Add** (plus sign) icon.

17 Set the value of `pci_passthrough:alias` to *`virtual-device-name:device-count`*.

Option	Description
virtual-device-name	Enter the virtual device name that you specified in this procedure.
device-count	Specify the number of virtual functions that can be called in one request. This value can range from 1 to 10.

18 Expand **VMware Quota** and click the **Add** (plus sign) icon next to `Quota: Memory Reservation`.

19 Set the value of `quota:memory_reservation` to **100** and click **Save**.

Results

You can now deploy passthrough-enabled virtual machines by configuring them with the flavor that you modified during this procedure.

NVIDIA GRID vGPU

You can allow an OpenStack instance to use an NVIDIA GRID vGPU device on its ESXi host.

For more information about cleaning the stale resource provider and vGPU trait, see Clean Stale vGPU Resource.

Note

- Only one vGPU is supported per OpenStack instance.
- The same vGPU profile is used for all OpenStack instances.

Prerequisites

Verify that the driver for your vGPU device is installed on the ESXi host.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Edit the Nova compute configuration.

```
viocli update nova-compute
```

3 In the `vmware` section, add the `gpu_profile` parameter and set its value to the vGPU profile that you want to use.

4 Add the `profile_fb_size_kb` parameter and set its value to the size of the vGPU frame buffer in kilobytes (KB).

   For example, enter `profile_fb_size_kb: 4096` to indicate a frame buffer of 4096 KB.

```
conf:
  nova_compute:
    vmware:
      gpu_profile: grid_t4-2q
      profile_fb_size_kb: 4096
```

   For more information about frame buffers, see the NVIDIA Virtual GPU Software User Guide at https://docs.nvidia.com/grid/latest/grid-vgpu-user-guide/index.html.

5 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

6 Select the **admin** project from the drop-down menu in the title bar.

7 Select **Admin > Compute > Flavors**.

8 Create a new flavor or choose an existing flavor to use for NVIDIA GRID vGPU passthrough.

9 Select **Update Metadata** next to the flavor that you want to use.

10 In the **Available Metadata** pane, expand **VMware Driver Options for Flavors** and click the **Add** (plus sign) icon next to **VMware vGPU**.

11 Set the value of `vmware:vgpu` to `1` and click **Save**.

What to do next

You can now configure an instance to use an NVIDIA GRID vGPU by configuring the instance with the flavor that you modified in this procedure.

Clean Stale vGPU Resource

You can use the `nova-manage` command for cleaning the stale resource providers and traits for vGPU.

If you remove an ESXi host from compute node, some stale resource providers and traits can still be present in the placement database. The presence of these stale resource providers and traits can cause instance creation failure. So, use the `nova-manage` command for cleaning the stale resources and traits.

Note If you have instances created with the vGPU profile, you cannot delete the associated resource providers and the traits.

Procedure

1 Before removing the ESXi host, record the moid of the ESXi host.

2 Log in to the `nova-osapi` pod.

```
osctl exec -it nova-api-osapi-5c786c7469-5z4jh bash
```

`compute-13350e6f-c17` is the name of the compute node.

`host -15757` is the moid of the removed ESXi host.

3 Run the `nova-manage` command.

```
nova-manage placement purge_stale_trait_and_provider --host compute-13350e6f-c17 --esxi
host-15757 --fix true
```

If you do not specify the `--fix true` parameter, the command can only list the resource providers. Otherwise, you can delete the listed resource providers.

Results

After applying the `nova-manage` command, you can see that there are no stale resource providers, and traits present in the placement database.

Configure Resource QoS

You can control resource allocations for CPU, memory, disk IOPS, and virtual network interfaces by modifying a flavor or image.

Note Configuring virtual interface quotas is not supported in NSX-T Data Center. The VIF limit, reservation, and shares settings cannot be used with NSX-T Data Center deployments.

To configure QoS for NSX-T Data Center, create a Network I/O Control (NIOC) profile and apply it to the N-VDS for the transport nodes in your deployment. See "Configure Network I/O Control Profiles" in the *NSX-T Data Center Installation Guide*.

QoS resource allocation can also be specified by flavor extra specs or image metadata. If flavor and image settings conflict, the image metadata configuration takes precedence.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

2 Select the **admin** project from the drop-down menu in the title bar.

3 Specify a flavor or image to use for QoS.

- To use flavor extra specs for QoS configuration, perform the following steps:
  a Select **Admin > Compute > Flavors**.
  b Create a new flavor or choose an existing flavor to use for QoS.
  c Select **Update Metadata** next to the flavor that you want to use.
- To use image metadata for QoS configuration, perform the following steps:
  a Select **Admin > Compute > Images**.
  b Create a new image or choose an existing image to use for QoS.

c Click the down arrow next to the image that you want to use and select **Update Metadata**.

4 In the **Available Metadata** pane, expand **VMware Quota**.

5 Click the **Add** (plus sign) icon next to the item that you want to use.

Option	Description
Quota: CPU Limit	Specify the maximum CPU allocation in megahertz. The value `0` indicates that CPU usage is not limited.
Quota: CPU Reservation	Specify the guaranteed CPU allocation in megahertz.
Quota: CPU Reservation in Percentage	Specify the guaranteed CPU allocation as a percentage of total CPU cycles.
Quota: CPU Shares Level	Specify the level of CPU shares allocated. You can enter **`custom`** and add the **Quota: CPU Shares Value** metadata to provide a custom value.
Quota: CPU Shares Value	Specify the number of CPU shares allocated. If the **Quota: CPU Shares Level** metadata is not set to `custom`, this value is ignored.
Quota: Disk IO Limit	Specify the maximum disk transaction allocation in IOPS. The value `0` indicates that disk transactions are not limited.
Quota: Disk IO Reservation	Specify the guaranteed disk transaction allocation in IOPS.
Quota: Disk IO Shares Level	Specify the level of disk transaction shares allocated. You can enter **`custom`** and add the **Quota: Disk IO Shares Value** metadata to provide a custom value.
Quota: Disk IO Shares Value	Specify the number of disk transaction shares allocated. If the **Quota: Disk IO Shares Level** metadata is not set to `custom`, this value is ignored.
Quota: Memory Limit	Specify the maximum memory allocation in megabytes. The value `0` indicates that memory usage is not limited.
Quota: Memory Reservation	Specify the guaranteed memory allocation in megabytes.
Quota: Memory Reservation in Percentage	Specify the guaranteed memory allocation as a percentage of total memory.
Quota: Memory Shares Level	Specify the level of memory shares allocated. You can enter **`custom`** and add the **Quota: Memory Shares Value** metadata to provide a custom value.
Quota: Memory Shares Value	Specify the number of memory shares allocated. If the **Quota: Memory Shares Level** metadata is not set to `custom`, this value is ignored.
Quota: VIF Limit	Specify the maximum virtual interface bandwidth allocation in megabits per second (Mbps). The value `0` indicates that virtual interface bandwidth is not limited.
Quota: VIF Reservation	Specify the guaranteed virtual interface bandwidth allocation in Mbps.

Option	Description
Quota: VIF Shares Level	Specify the level of virtual interface bandwidth shares allocated. You can enter **`custom`** and the **Quota: VIF Shares Value** metadata to provide a custom value.
Quota: VIF Shares Value	Specify the number of virtual interface bandwidth shares allocated. If the **Quota: VIF Shares Level** metadata is not set to `custom`, this value is ignored.

6 Click **Save**.

Results

You can now deploy QoS-enabled instances by configuring them with the flavor or image that you modified in this procedure.

To apply QoS settings to an existing instance, resize the instance and select the flavor with the desired QoS settings. The specified settings take effect after the resize process is complete.

Import Virtual Machines into VMware Integrated OpenStack

You can import virtual machines into VMware Integrated OpenStack using NSX-V, NSX-T, and non-default domain.

VMware Integrated OpenStack with NSX Data Center for vSphere

You can import virtual machines from vSphere into your VMware Integrated OpenStack deployment and manage them as OpenStack instances.

This procedure applies to deployments with VDS or NSX Data Center for vSphere networking. For NSX-T Data Center deployments, see VMware Integrated OpenStack with NSX-T Data Center.

The following conditions apply to imported virtual machines:

- If a virtual machine has multiple disks, the disks are imported as Cinder volumes.
- Existing networks are imported as port group-based provider networks with access restricted to the specified project.
- After a virtual machine with a specific network backing is imported, the same network cannot be imported to a different project.
- Neutron subnets are automatically created with DHCP disabled.
- Neutron ports are automatically created based on the IP and MAC address of the network interface card on the virtual machine.

Note If the DHCP server cannot maintain the same IP address during lease renewal, the instance information in OpenStack will show the incorrect IP address. To avoid this problem, use static DHCP bindings on existing DHCP servers and do not run new OpenStack instances on imported networks.

You import virtual machines using the Data Center Command-Line Interface (DCLI) in the Integrated OpenStack Manager toolbox.

Prerequisites

Verify that the virtual machines that you want to import are in the same vCenter Server instance.

Procedure

1 Add the clusters containing the desired virtual machines as compute clusters in your VMware Integrated OpenStack deployment.

For instructions, see Add Compute Clusters to Your Deployment.

2 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

3 If you want to prevent imported virtual machines from being relocated or renamed, update your deployment configuration.

a Modify the Nova compute configuration.

```
viocli update nova-compute
```

b In the `vmware` section, add the `import_vm_relocate` parameter and set its value to `false`.

If you do not perform this step, imported virtual machines are modified as follows:

- The names of imported virtual machines are changed to the following format: *`original-name (instance-uuid)`*
- Imported virtual machines are placed in the following folder in vSphere: *`datacenter`* > *`root-VM-folder`* > `OpenStack > Project (`*`project-uuid`*`)`

4 Open the toolbox and connect to the VMware Integrated OpenStack vAPI endpoint.

The endpoint is located at the private OpenStack endpoint of your deployment.

```
toolbox
dcli +server https://internal-vip:9449/api +i
```

5 Import unmanaged virtual machines into VMware Integrated OpenStack.

Note When you execute a command, DCLI prompts you to enter the administrator credentials for your vCenter Server instance. You can save these credentials to avoid entering your username and password every time.

- Run the following command to import all unmanaged virtual machines:

```
com vmware vio vm unmanaged importall --cluster cluster-name [--tenant-mapping {FOLDER
| RESOURCE_POOL} [--root-folder root-folder | --root-resource-pool root-resource-pool]]
```

Option	Description
`--cluster`	Enter the compute cluster that contains the virtual machines that you want to import.
`--tenant-mapping {FOLDER | RESOURCE_POOL}`	Specify whether to map imported virtual machines to OpenStack projects based on their location in folders or resource pools. If you do not include this parameter, all imported VMs will become instances in the **import_service** project by default.
`--root-folder`	If you specified **`FOLDER`** for the `--tenant-mapping` parameter, you can provide the name of the root folder containing the virtual machines to be imported. All virtual machines in the specified folder or any of its subfolders are imported as instances into an OpenStack project with the same name as the folder in which they are located. **Note** If you specify `--tenant-mapping FOLDER` but do not specify `--root-folder`, the name of the top-level folder in the cluster is used by default.
`--root-resource-pool`	If you specified **`RESOURCE_POOL`** for the `--tenant-mapping` parameter, you can provide the name of the root resource pool containing the virtual machines to be imported. All virtual machines in the specified resource pool or any of its child resource pools are imported as instances into an OpenStack project with the same name as the resource pool in which they are located.

- Run the following command to import a specified virtual machine:

```
com vmware vio vm unmanaged importvm --vm vm-id [--tenant project-name] [--nic-mac-address nic-mac --nic-ipv4-address nic-ip] [--root-disk root-disk-path] [--nics specifications]
```

Option	Description
`--vm`	Enter the identifier of the virtual machine that you want to import. You can view the ID values of all unmanaged virtual machines by running the `com vmware vio vm unmanaged list` command.
`--tenant`	Specify the OpenStack project into which you want to import the virtual machine. If you do not include this parameter, the `import_service` project is used by default.
`--nic-mac-address`	Enter the MAC address of the network interface card on the virtual machine. If you do not include this parameter, the import process attempts to discover the MAC and IP addresses automatically. **Note** If you include this parameter, you must also include the `nic_ipv4_address` parameter.
`--nic-ipv4-address`	Enter the IP address and prefix for the network interface card on the virtual machine. Enter the value in CIDR notation (for example, 10.10.1.1/24). This parameter must be used together with the `--nic-mac-address` parameter.
`--root-disk`	For a virtual machine with multiple disks, specify the root disk datastore path in the following format: **`--root-disk '[datastore1] dir/disk_1.vmdk'`**
`--nics`	For a virtual machine with multiple NICs, specify the MAC and IP addresses of each NIC in JSON format. Use the following key-value pairs: ■ mac_address: MAC address of the NIC in standard format ■ ipv4_address: IPv4 address in CIDR notation For example: `--nics '[{"mac_address": "00:50:56:9a:f5:7b", "ipv4_address": "192.0.2.10/24"}, {"mac_address": "00:50:56:9a:ee:be", "ipv4_address": "192.0.2.11/24"}]'`

Results

The specified virtual machines are imported into your OpenStack deployment and can be managed as OpenStack instances.

VMware Integrated OpenStack with NSX-T Data Center

You can import virtual machines from vSphere into your VMware Integrated OpenStack deployment and manage them like OpenStack instances.

This procedure applies to deployments with NSX-T Data Center networking. For VDS or NSX Data Center for vSphere deployments, see VMware Integrated OpenStack with NSX Data Center for vSphere.

The following conditions apply to imported virtual machines:

- If a virtual machine has multiple disks, the disks are imported as Cinder volumes.
- After a virtual machine with a specific network backing is imported, the same network cannot be imported to a different project. If you want to use a network for multiple projects, configure it as a shared network.

You import virtual machines using the Data Center Command-Line Interface (DCLI) in the Integrated OpenStack Manager toolbox.

Prerequisites

Verify that the virtual machines that you want to import are in the same vCenter Server instance.

Procedure

1. Add the clusters containing the desired virtual machines as compute clusters in your VMware Integrated OpenStack deployment.

   For instructions, see Add Compute Clusters to Your Deployment.

2. Connect the virtual machine to a Neutron network.

   You can use a provider network or a tenant network for this procedure.

   a. In the vSphere Client, open the **Hosts and Clusters** view.

   b. Right-click each virtual machine that you want to import and select **Edit Settings...**.

   c. From the drop-down list next to the network adapter, select the Neutron network that you want to use.

   d. Expand the network adapter settings and record its MAC address.

3. Create a temporary opaque network for the virtual machine.

   - For NSX-T 2.5, you create a Logical Switch. See "Create a Logical Switch" in the *NSX-T Data Center Administration Guide*, then perform the following steps to obtain the logical switch ID.

     a. In the **Logical Switch** column, cllick the name of the switch that you created.

b Record the ID of the switch as displayed in the **Overview** column.

- For NSX-T 3.0, you create a segment. Follow instructions in "Add a Segment" in the *NSX-T Data Center Administration Guide* and record the name of the segment you added.

4 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

5 Edit the Nova compute configuration.

```
viocli update nova-compute
```

6 In the `vmware` section, add the `import_net_id` parameter and set its value to the ID of the switch or the name of the segment that you added in.

7 If you want to prevent imported virtual machines from being relocated or renamed, add the `import_vm_relocate` parameter and set its value to `false`.

8 Open the toolbox and set the password for the `admin` account.

```
toolbox
export OS_PASSWORD=admin-account-password
```

9 Create a Neutron port that uses the MAC address of the virtual machine's network adapter.

```
neutron port-create network --name port --tenant-id project-id --mac-address vm-mac [--
fixed-ip ip_address=vm-ip]
```

Option	Description
network	Enter the name of the Neutron network to which you connected the virtual machine.
`--name`	Enter a name for the port.
`--tenant-id`	Specify the UUID of the project for which to create the port.
`--mac-address`	Enter the MAC address of the virtual machine's network adapter recorded in Step 2d.
`--fixed-ip`	Enter the IP address of the virtual machine. If the virtual machine does not have an IP address or you do not want to retain the existing IP address, you can omit this parameter.

10 Connect to the VMware Integrated OpenStack vAPI endpoint.

The endpoint is located at the private OpenStack endpoint of your deployment.

```
dcli +server http://internal-vip:9449/api +i
```

11 Import the virtual machine into VMware Integrated OpenStack.

```
com vmware vio vm unmanaged importvm --vm vm-moid --nic-net-id network-uuid --nic-port-id
port-uuid [--tenant project-name] [--root-disk root-disk-path]
```

Option	Description
--vm	Enter the managed object identifier (MOID) of the virtual machine that you want to import. You can view the MOIDs of all unmanaged virtual machines by running the `com vmware vio vm unmanaged list` command.
--nic-net-id	Enter the UUID of the Neutron network to which you connected the virtual machine.
--nic-port-id	Enter the UUID of the port that you created for the virtual machine.
--tenant	Specify the OpenStack project into which you want to import the virtual machine. If you do not include this parameter, the `import_service` project is used by default.
--root-disk	For a virtual machine with multiple disks, specify the root disk datastore path in the following format: **`--root-disk '[datastore1] dir/disk_1.vmdk'`**

Note When you execute a command, DCLI prompts you to enter the administrator credentials for your vCenter Server instance. You can save these credentials to avoid entering your username and password every time.

Results

The specified virtual machine is imported into your OpenStack deployment and can be managed as an OpenStack instance.

VMware Integrated OpenStack with Non-Default Domain

You can import virtual machines to a non-default domain from vSphere into your VMware Integrated OpenStack deployment and manage them like OpenStack instances.

This procedure applies to deployments with a non-default domain. For NSX-T Data Center deployments, see VMware Integrated OpenStack with NSX-T Data Center.

The following conditions apply to imported virtual machines:

- If a virtual machine has multiple disks, the disks are imported as Cinder volumes.
- After importing a virtual machine with a specific network backing, you cannot use the same network to import a different project. If you want to use a network for multiple projects, configure the provider VLAN (Virtual LAN) network as the shared network.

You import virtual machines using the Data Center Command-Line Interface (DCLI) in the Integrated OpenStack Manager toolbox.

Prerequisites

Verify that the virtual machines that you want to import are in the same vCenter Server instance.

Procedure

1 Add the clusters containing the desired virtual machines as compute clusters in your VMware Integrated OpenStack deployment.

   For instructions, see Add Compute Clusters to Your Deployment.

2 Connect the virtual machine to a Neutron network.

   a In the vSphere Client, open the **Hosts and Clusters** view.

   b Right-click each virtual machine that you want to import and select **Edit Settings...**.

   c From the drop-down list next to the network adapter, select the Neutron network that you want to use.

   d Expand the network adapter settings and record its MAC address.

3 Create a temporary opaque network for the virtual machine.

   - For NSX-T 2.5, you create a Logical Switch. See "Create a Logical Switch" in the *NSX-T Data Center Administration Guide*, then perform the following steps to obtain the logical switch ID.

     a In the **Logical Switch** column, cllick the name of the switch that you created.

     b Record the ID of the switch as displayed in the **Overview** column.

   - For NSX-T 3.0, you create a segment. Follow instructions in "Add a Segment" in the *NSX-T Data Center Administration Guide* and record the name of the segment you added.

4 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

5 Edit the Nova compute configuration.

```
viocli update nova-compute
```

6 In the `vmware` section, add the `import_net_id` parameter and set its value to the recorded switch ID or the segment name.

7 If you want to prevent imported virtual machines from being relocated or renamed, add the `import_vm_relocate` parameter and set its value to `false`.

8 To import virtual machines to a non-default domain, you must create a user and project in this domain and set the `default_tenant_domain_name` parameter in the `vioshim` pod.

```
domain name: import-domain
admin user in import-domain: import-domain
a new project in import-domain: import-proj2
```

```
viocli update vioshim
conf:
  vioshim:
    DEFAULT:
      default_tenant_domain_name: import-domain
```

To verify, you can login to the following pod.

```
osctl exec -it vioadmin1-vioshim-6855dd94b4-s5vzk -c vioshim bash
```

To check the content of `/etc/viocli/viocli.conf`, you can use the following line of code:

```
default_tenant_domain_name = import-domain
```

9 Set the password for the `admin` account.

```
export OS_PASSWORD=admin-account-password
```

10 Export variables in the toolbox.

The password given in the following code is for reference. For exporting variables in the toolbox, you must specify your password.

```
[root@vioadmin1-vioshim-6855dd94b4-s5vzk /]# export OS_PROJECT_NAME=import-proj2
[root@vioadmin1-vioshim-6855dd94b4-s5vzk /]# export OS_PROJECT_DOMAIN_NAME=import-domain
[root@vioadmin1-vioshim-6855dd94b4-s5vzk /]# export OS_USER_DOMAIN_NAME=import-domain
[root@vioadmin1-vioshim-6855dd94b4-s5vzk /]# export OS_PASSWORD=*****
[root@vioadmin1-vioshim-6855dd94b4-s5vzk /]# export OS_USERNAME=import-admin
```

You can also import virtual machines using a default project `import-service` and export variables in the toolbox.

```
[root@vioadmin1-vioshim-56f9ddc779-wc4lc /]#
[root@vioadmin1-vioshim-56f9ddc779-wc4lc /]# export OS_PASSWORD=*****
[root@vioadmin1-vioshim-56f9ddc779-wc4lc /]#  env | grep -i project
OS_PROJECT_NAME=import-service
OS_PROJECT_DOMAIN_NAME=default
[root@vioadmin1-vioshim-56f9ddc779-wc4lc /]# export OS_PROJECT_NAME=admin
```

11 Create a Neutron port in the specified project.

You can create a Neutron port in the specified project. The project `import-proj2` uses the shared provider network, and you must specify the `--tenant-id` for the port to avoid the PortNotUsable issue.

```
neutron port-create network --name port --tenant-id <project id of import-proj2> --mac-address vm-mac --fixed-ip ip_address=vm-ip
```

```
neutron port-create network --name port --tenant-id project id --mac-address vm-mac --fixed-ip ip_address=vm-ip
```

Option	Description
network	Enter the name of the Neutron network to which you connected the virtual machine.
`--name`	Enter a name for the port.
`--tenant-id`	Specify the UUID of the project for which to create the port.
`--mac-address`	Enter the MAC address of the virtual machine's network adapter.
`--fixed-ip`	Enter the IP address of the virtual machine. If the virtual machine does not have an IP address or you do not want to retain the existing IP address, you can omit this parameter.

12 Connect to the VMware Integrated OpenStack vAPI endpoint.

The endpoint is located at the private OpenStack endpoint of your deployment.

```
dcli +server https://internal-vip:9449/api +i
```

13 Import the virtual machine, specifying the tenant name.

To import virtual machines, you must specify the `--tenant` name. However, if no `--tenant` name is specified, VMware Integrated OpenStack will use a default `--tenant` name `import-service`.

```
com vmware vio vm unmanaged importvm --vm vm-moid --nic-net-id network-uuid --nic-port-id port-uuid --tenant import-proj2
```

```
com vmware vio vm unmanaged importvm --vm vm-moid --nic-net-id network-uuid --nic-port-id port-uuid --tenant import-service
```

Option	Description
`--vm`	Enter the managed object identifier (MOID) of the virtual machine that you want to import. You can view the MOIDs of all unmanaged virtual machines by running the `com vmware vio vm unmanaged list` command.
`--nic-net-id`	Enter the UUID of the Neutron network to which you connected the virtual machine.

Option	Description
--nic-port-id	Enter the UUID of the port that you created for the virtual machine.
--tenant	Specify the OpenStack project into which you want to import the virtual machine.
--root-disk	For a virtual machine with multiple disks, specify the root disk datastore path in the following format: **--root-disk '[datastore1] dir/disk_1.vmdk'**

Note When you execute a command, DCLI prompts you to enter the administrator credentials for your vCenter Server instance. You can save these credentials to avoid entering your username and password every time.

Results

The specified virtual machines are imported into your OpenStack deployment and can be managed as OpenStack instances.

Supported Extra Specs for Flavor

Flavor extra specs are used for the advanced configuration of compute instances. VMware Integrated OpenStack exposes additional capabilities through flavor extra specs.

Note Configuring virtual interface quotas is not supported in NSX-T Data Center. The following extra specs cannot be used with NSX-T Data Center deployments:

- `quota:vif_limit`
- `quota:vif_reservation`
- `quota:vif_shares_level`
- `quota:vif_shares_share`

However, vSphere 7.0, when used with the new VDS and NSX-T Data Center, certainly supports the additional capabilities of the preceding extra specs.

To configure QoS for NSX-T Data Center, create a Network I/O Control (NIOC) profile and apply it to the N-VDS for the transport nodes in your deployment. See "Configure Network I/O Control Profiles" in the *NSX-T Data Center Installation Guide*.

If an image metadata and flavor extra spec conflict, the image metadata takes precedence over the flavor extra spec.

Table 5-1. Flavor Extra Specs in VMware Integrated OpenStack

Extra Spec	Description
`hw:vifs_multi_thread`	Specify **`true`** to provide each virtual interface with its own transmit thread.
`quota:cpu_limit`	Specify the maximum CPU allocation in MHz. The value `0` indicates that CPU usage is not limited.

Table 5-1. Flavor Extra Specs in VMware Integrated OpenStack (continued)

Extra Spec	Description
quota:cpu_reservation	Specify the guaranteed CPU allocation in MHz.
quota:cpu_reservation_percent	Specify the guaranteed CPU allocation as a percentage of the actual CPU speed of the instance. This parameter takes precedence over the cpu_reservation parameter.
quota:cpu_shares_level	Specify the level of CPU shares allocated. You can enter **custom** and add the cpu_shares_share parameter to provide a custom value.
quota:cpu_shares_share	Specify the number of CPU shares allocated. If the cpu_shares_level parameter is not set to custom, this value is ignored.
quota:disk_io_limit	Specify the maximum disk transaction allocation in IOPS. The value 0 indicates that disk transactions are not limited.
quota:disk_io_reservation	Specify the guaranteed disk transaction allocation in IOPS.
quota:disk_io_shares_level	Specify the level of disk transaction shares allocated. You can enter **custom** and add the disk_io_shares_share parameter to provide a custom value.
quota:disk_io_shares_share	Specify the number of disk transaction shares allocated. If the disk_io_shares_level parameter is not set to custom, this value is ignored.
quota:memory_limit	Specify the maximum memory allocation in MB. The value 0 indicates that memory usage is not limited.
quota:memory_reservation	Specify the guaranteed memory allocation in MB.
quota:memory_reservation_percent	Specify the guaranteed memory allocation as a percentage of the actual memory of the instance. The value 100 indicates that guest memory is also fully reserved. This parameter takes precedence over the memory_reservation parameter.
quota:memory_shares_level	Specify the level of memory shares allocated. You can enter **custom** and add the memory_shares_share parameter to provide a custom value.
quota:memory_shares_share	Specify the number of memory shares allocated. If the memory_shares_level parameter is not set to custom, this value is ignored.
quota:vif_limit	Specify the maximum virtual interface bandwidth allocation in Mbps. The value 0 indicates that virtual interface bandwidth is not limited.
quota:vif_reservation	Specify the guaranteed virtual interface bandwidth allocation in Mbps.

Table 5-1. Flavor Extra Specs in VMware Integrated OpenStack (continued)

Extra Spec	Description
quota:vif_shares_level	Specify the level of virtual interface bandwidth shares allocated. You can enter **custom** and add the vif_shares_share parameter to provide a custom value.
quota:vif_shares_share	Specify the number of virtual interface bandwidth shares allocated. If the vif_shares_level parameter is not set to custom, this value is ignored.
vmware:boot_efi_secure_boot	Specify **true** to perform signature checks on any EFI images loaded during startup.
vmware:boot_enter_bios	Specify **true** to make virtual machines enter the BIOS configuration on next startup. Virtual machines automatically reset this parameter after the next startup.
vmware:boot_retry	Specify the delay in milliseconds before the boot sequence is started.
vmware:boot_retry_delay	Specify the delay in milliseconds before the boot sequence is retried. If the boot_retry_enabled parameter is set to false, this value is ignored.
vmware:boot_retry_enabled	Specify **true** to retry the boot sequence if a boot failure occurs.
vmware:cpu_affinity	Specify a list of CPUs that instances can use.
vmware:extra_config	Specify custom configurations in the JSON format. For example, '{"acpi.smbiosVersion2.7":"FALSE"}'.
vmware:hw_version	Specify the hardware version used to create images. In an environment with different host versions, you can use this parameter to place instances on the correct hosts.
vmware:latency_sensitivity_level	Specify the latency sensitivity level for virtual machines.
vmware:latency_sensitivity_per_cpu_high	Specify the high latency sensitivity level for selected virtual CPUs within a virtual machine. Use the OpenStack CLI to specify this option. For example,vmware:latency_sensitivity_per_cpu_high="1, 3" configures high latency sensitivity for vcpu1 and vcpu3 within your virtual machine.
vmware:resource_pool	Specify the resource pool on which to place new instances. If the name of the project containing the instance matches the name of a resource pool in your environment, the instance is placed in that resource pool by default. Setting this parameter overrides the default behavior and forces the instance to be placed in the specified resource pool.
vmware:set_bios_uuid	Specify **true** to use the Nova UUID of instances as the device UUID.

Table 5-1. Flavor Extra Specs in VMware Integrated OpenStack (continued)

Extra Spec	Description
vmware:storage_policy	Specify the storage policy used for new instances. If Storage Policy-Based Management (SPBM) is not enabled, this parameter is ignored.
vmware:tenant_vdc	Specify the UUID of the tenant virtual data center in which to place instances.
vmware:vgpu	Specify the number of shared vGPUs to attach to the instance.
vmware:vm_group	Specify the DRS VM group in which virtual machines will be placed. If the specified VM group does not exist, instances fail to power on.

Cinder Volumes

6

Volumes are block storage devices that you attach to instances to enable persistent storage.

As a cloud administrator, you can manage volumes and volume types for users in various projects. Cloud users can attach a volume to a running instance or detach a volume and attach it to another instance.

For more information about Cinder, see the OpenStack Cinder documentation at https://docs.openstack.org/cinder/train.

This chapter includes the following topics:

Create Volume Type

You can create volume types and expose them to one or more tenants for use in volume creation. Volume types can define a vSphere storage profile and default adapter type.

Note Barbican encryption is not supported for volumes or volume types.

Procedure

1. Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.
2. Select the **admin** project from the drop-down menu in the title bar.
3. Select **Admin > Volume > Volume Types** and click **Create Volume Type**.
4. Enter a name and description for the volume type.

5 If you want to make the volume type available to certain projects only, deselect **Public**.

You can configure access to the volume type after it is created.

6 Click **Create Volume Type**

The new volume type is displayed in the **Volume Types** list.

7 If you want to associate a vSphere storage profile with the volume type, perform the following steps:

a In the **Actions** column, select **View Extra Specs**.

b Click **Create**.

c Enter **`vmware:storage_profile`** in the **Key** text box.

d Enter the name of the vSphere storage profile in the **Value** text box.

e Click **Create**.

8 If you want to set a default adapter for the volume type, perform the following steps:

a In the **Actions** column, select **View Extra Specs**.

b Click **Create**.

c Enter **`vmware:adapter_type`** in the **Key** text box.

d Enter the adapter type in the **Value** text box.

The following values are supported: **`lsiLogic`**, **`busLogic`**, **`lsiLogicsas`**, **`paraVirtual`**, and **`ide`**.

e Click **Create**.

9 If your volume type is not public, select **Edit Access** in the **Actions** column and specify the projects that can use the volume type.

If you do not specify any projects, the volume type is visible only to cloud administrators.

Results

Tenants can select a volume type when creating a volume or modifying an existing volume. The settings defined by the specified volume type are then applied to the new volume.

What to do next

If you want to change the name or description of a volume type, click **Edit Volume Type** in the **Actions** column and make the desired changes. To delete unneeded volume types, select them in the **Volume Types** table and click **Delete Volume Types**.

Create Volume

You create volumes and attach them to instances to provide persistent storage.

Prerequisites

- If you want to create a volume from an image, upload the desired image. See Import an Image.
- If you want to create an FCD-backed volume, verify that you have added at least one Cinder host using the FCD back end. Then create a volume type and set its `volume_backend_name` extra spec to the name of the FCD back end which is **`VMwareVStorageObjectDriver`**. Select this volume type during the volume creation process. For information about volume types, see Create Volume Type.

Procedure

1. Log in to the VMware Integrated OpenStack dashboard.
2. Select your project from the drop-down menu in the title bar.
3. Select **Project > Volumes > Volumes**.
4. Click **Create Volume** and enter the desired configuration.

Option	Description
Volume Name	Enter a name for the new volume.
Description	Enter a description for the volume.
Volume Source	Select **No source, empty volume**, **Snapshot**, **Image**, or **Volume**. If you select **Snapshot**, **Image**, or **Volume**, specify the desired object from the next drop-down menu.
Type	If you selected **No source, empty volume** or **Image** as the volume source, select a volume type for the volume. For volumes whose source is a volume snapshot or another volume, the volume type is inherited from the source.
Size (GiB)	Enter the size of the volume in gibibytes.
Availability Zone	If you selected **No source, empty volume** or **Image** as the volume source, specify the availability zone in which to create the volume. For volumes whose source is a volume snapshot or another volume, the availability zone is inherited from the source.

5. Click **Create Volume**.

What to do next

In the **Actions** column to the right of the volume, you can perform the following actions:

- Click **Edit Volume** to modify the name and description of the volume and whether it is bootable.
- Click **Extend Volume** to increase the size of an unattached volume.
- Click **Launch as Instance** to create an instance using an unattached volume.
- Click **Manage Attachments** to attach the volume to or detach the volume from an instance.

- Click **Create Snapshot** to take a snapshot of the volume.

  Note Creating a snapshot of a volume attached to an instance can result in a corrupted snapshot. If possible, detach the volume before creating the snapshot.

- Click **Change Volume Type** to modify the volume type and migration policy.
- Click **Upload to Image** to upload the volume to Glance as an image.
- Click **Create Transfer** to assign ownership of an unattached volume to a different project. For details, see Transfer Volume.
- Click **Update Metadata** to add, remove, or change volume metadata.

You can also select one or more unattached volumes and click **Delete Volumes** to remove them.

Transfer Volume

You can assign ownership of an unattached volume to another project.

Prerequisites

Ensure that the volume that you want to transfer is not attached to an instance.

Procedure

- To initiate a transfer, perform the following steps:
  a. Log in to the VMware Integrated OpenStack dashboard.
  b. Select your project from the drop-down menu in the title bar.
  c. Select **Project > Compute > Volumes**.
  d. In the **Actions** column next to the volume that you want to transfer, click **Create Transfer**.
  e. Enter a name for the transfer task and click **Create Volume Transfer**.
  f. Record or download the transfer ID and authorization key displayed on the **Volume Transfer Details** page and send this information to the user who will accept the transfer.

     Important After you close the **Volume Transfer Details** page, the transfer ID and authorization key can no longer be retrieved. If the transfer ID or authorization key are lost, you must cancel the transfer and initiate it again.

- To receive a transfer, perform the following steps:
  a. Log in to the VMware Integrated OpenStack dashboard.
  b. Select your project from the drop-down menu in the title bar.
  c. Select **Project > Compute > Volumes** and click **Accept Transfer**.

d Enter the transfer ID and authorization key that you received from the user who initiated the transfer.

e Click **Accept Volume Transfer**.

Manage Volume

You can manage non-OpenStack volumes on the Cinder hosts in your deployment. Managing a volume makes it usable in your OpenStack deployment.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.

2 Select the **admin** project from the drop-down menu in the title bar.

3 Select **Admin > Volume > Volumes**.

4 Click **Manage Volume** and enter the desired configuration.

Option	Description
Identifier	Enter the name or identifier for the source volume. **Note** To migrate a volume from the VMDK back end to the FCD back end, enter the ID of the existing VMDK volume.
Identifier Type	Select **Name** or **ID**. **Note** To migrate a volume from the VMDK back end to the FCD back end, select **ID**.
Host	Enter the Cinder host that contains the existing volume. Use the following format: *`host:backend-name@pool`*.
Volume Name	Enter a name for the volume.
Description	Enter a description of the volume.
Metadata	Enter metadata as key-value pairs. For example, `img_config_drive=mandatory`.
Volume Type	Select a volume type for the volume.
Availability Zone	Select an availability zone in which to place the volume.
Bootable	Select the checkbox to allow instances to boot from the volume.

5 Click **Manage**.

Results

The specified volume is managed by Cinder and visible in OpenStack.

Multi-Attach Volume

With Cinder multi-attach, you can simultaneously attach volumes to multiple instances.

Prerequisites

If you want to use multi-attach volumes, be aware of the following limitations:

- Hardware acceleration is required for NFS datastores that back multi-attach volumes.
- Multi-attach volumes cannot be relocated while they are in use. To avoid the effects of this limitation, create multi-attach volumes on a shared datastore.

  You can specify datastores for multi-attach volumes by using a storage profile. Create the desired storage profile in vSphere and assign it to the volume type defined in this procedure using the `vmware:storage_profile` extra spec.
- Multi-attach volumes must use thick provision eager zeroed as the provisioning format.
- Multi-attach volumes must use VMDK as the back-end driver. FCD volumes do not support multi-attach.
- To prevent data corruption, format multi-attach volumes with a cluster-aware file system.
- You cannot clone, back up, or take snapshots of multi-attach volumes while those volumes are attached.
- If more than eight ESXi hosts attempt to access a single multi-attach volume simulaneously, attaching the volume will fail.
- You cannot perform live migration on an instance to which a multi-attach volume is attached.
- The `viocli prepare datastore` command does not support multi-attach volumes. Detach multi-attach volumes before migrating them to another datastore.

Procedure

1. Create a new volume type or choose an existing volume type to use for multi-attach.

   For instructions, see Create Volume Type.
2. Select **View Extra Specs** next to the volume type that you want to use.
3. Click **Create**.
4. In the **Key** field, enter **`multiattach`**.
5. In the **Value** field, enter **`<is> True`**.
6. Click **Create**.
7. On the **Volume Type Extra Specs** page, click **Create**.
8. In the **Key** field, enter **`vmware:vmdk_type`**.
9. In the **Value** field, enter **`eagerZeroedThick`**.
10. Click **Create**.

11 (Optional) Specify a storage profile to ensure that multi-attach volumes are created on supported datastores.

a On the **Volume Type Extra Specs** page, click **Create**.

b In the **Key** field, enter **`vmware:storage_profile`**.

c In the **Value** field, enter the name of the desired storage profile.

d Click **Create**.

Results

A multi-attach-capable volume type is created. To create multi-attach volumes, select this volume type when creating or retyping volumes. Note that retyping a volume to enable or disable multi-attach is only supported when the volume is unattached.

Migrate Volume

You can safely migrate Cinder volumes between datastores. This enables you to replace datastores, increase resources and capacity, and preserve volumes without taking them offline.

Note You cannot migrate a volume that has snapshots attached. You must detach all snapshots before migrating a volume.

Migrate All Volumes from a Datastore

You can quickly evacuate all volumes from a specified datastore, automatically migrating them to other datastores in the same datastore cluster.

Prerequisites

- Verify that the specified datastore is part of a datastore cluster.
- On the datastore cluster, enable Storage DRS and set it to **No Automation (Manual Mode)**.
- Detach all snapshots from all volumes on the datastore.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Prepare the volumes in the datastore for migration.

```
viocli prepare datastore dc-name ds-name
```

Option	Description
dc-name	Enter the name of the data center that contains the desired datastore.
ds-name	Enter the name of the datastore.

3 Place the datastore in maintenance mode.

See "Place a Datastore in Maintenance Mode" in the *vSphere Resource Management* document.

Results

When you place the datastore in maintenance mode, the datastore is evacuated and the volumes automatically migrate to other datastores in the same datastore cluster.

Migrate Unattached Cinder Volumes

You can migrate Cinder volumes that are unattached to instances to specified target datastores.

Prerequisites

Detach all snapshots from the volumes that you want to migrate.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Migrate the volumes.

- To migrate all volumes from a datastore, run the following command:

```
viocli migrate volume --source-dc src-dc-name --source-ds src-ds-name dest-dc-name
dest-ds-name [--ignore-storage-policy]
```

- To migrate specified volumes from a datastore, run the following command:

```
viocli migrate volume --volume-ids UUID1 dest-dc-name dest-ds-name [--ignore-storage-
policy]
```

Option	Description
--source-dc	Enter the data center containing the volumes that you want to migrate. This parameter must be used together with the `--source-ds` parameter. If you want to migrate specified volumes only, do not include this parameter.
--source-ds	Enter the datastore containing the volumes that you want to migrate. This parameter must be used together with the `--source-dc` parameter. If you want to migrate specified volumes only, do not include this parameter.
--volume-ids	Enter the UUID of the volume that you want to migrate. You can include multiple UUIDs separated by commas (,). If you want to migrate all volumes from a datastore, use the `--source-dc` and `--source-ds` parameters instead of this parameter.
dest-dc-name	Enter the name of the data center that contains the datastore to which you want to migrate volumes.

Option	Description
dest-ds-name	Enter the name of the datastore to which you want to migrate volumes.
`--ignore-storage-policy`	Include this parameter to migrate volumes to the target datastore even if the datastore does not comply with the storage policy of the volume.

Results

The specified volumes are migrated to the target datastore.

Migrate Attached Cinder Volumes

You can migrate Cinder volumes that are attached to an OpenStack instance by migrating the corresponding virtual machine to a different datastore.

Note

- Multi-attach volumes cannot be migrated while attached. Detach multi-attach volumes before migrating them to another datastore.
- After the OpenStack instance to which the volume is attached is migrated, the corresponding shadow virtual machine has no disk. When you detach the volume, the disk will be re-attached to the shadow virtual machine.

Prerequisites

Detach all snapshots from the volumes that you want to migrate.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Open the toolbox.

```
toolbox
```

3 Migrate the instance to which the volume is attached.

```
openstack server migrate compute-name instance-uuid --live
```

- To find the name of a compute node, run the `openstack host list` command and view the **Host Name** column.
- To find the UUID of the instance, run the `openstack server list` command and view the **ID** column.

For more information, see Migrate Instance.

4 In the vSphere Client, migrate the shadow virtual machine that corresponds to the OpenStack volume.

   For information, see "Migrate a Virtual Machine to New Storage in the vSphere Web Client" in the *vCenter Server and Host Management* document.

5 If you want to migrate the shadow virtual machine to a cluster in a different availability zone, update the Cinder host for the volume.

   a Get a list of cinder-api pods on the LCM node.

   ```
   osctl get pods | grep cinder-api
   ```

   b Using the name of one of the cinder-api pods listed, start a bash session on the pod.

   ```
   osctl exec -it <cinder-api-pod-name> bash
   ```

   c In the new session, get a list of Cinder hosts.

   ```
   cinder-manage host list
   ```

   The list includes hosts and zones of Cinder volumes.

   d Modify the attributes of the volume you want to move. Set the host and zone values to the Cinder volume host in the AZ where you want to move the shadow VM.

   ```
   cinder-manage volume update volume_host --volume_id <volume-uuid> --newhost <new-volume-host> --zone <availability-zone>
   ```

   Where:

   - *volume-uuid* is the Cinder volume UUID of the shadow VM you want to move
   - *new-volumne-host* is the Cinder hostname in the destination AZ.
   - *availability-zone* is the destination AZ.

Results

The Cinder volume and the disk of the corresponding shadow virtual machine are migrated to the new datastore.

Cinder Volume Backup

You can configure Cinder to back up volumes to a network file system (NFS) server.

Prerequisites

- Create a shared NFS directory dedicated to storing Cinder backups.
- Verify that the owner of the NFS share folder is the `root` user (UID 0).

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Edit the Cinder configuration.

```
viocli update cinder
```

3 In the `conf` section, create the `cinder` section. In the `cinder` section, create the `DEFAULT` section.

4 In the `DEFAULT` section, add the `backup_driver` parameter and set its value to `cinder.backup.drivers.nfs.NFSBackupDriver`.

The configuration file now looks similar to the following.

```
conf:
  backends:
    [...]
  cinder:
    DEFAULT:
      backup_driver: cinder.backup.drivers.nfs.NFSBackupDriver
```

5 Add the `backup_mount_options` parameter and set its value to your version of NFS.

For example, enter **`vers=4`** to support NFS version 4.

6 Add the `backup_share` parameter and set its value to the location of the shared NFS directory.

Use the format *nfs-host:path*. For example, `192.0.2.100:/cinder`.

7 Create the `manifests` section.

8 In the `manifests` section, add the `statefulset_backup` parameter and set its value to **`true`**.

9 Add the `job_backup_storage_init` parameter and set its value to **`true`**.

The configuration file now looks similar to the following.

```
conf:
  backends:
    [...]
  cinder:
    DEFAULT:
      backup_driver: cinder.backup.drivers.nfs.NFSBackupDriver
      backup_mount_options: nfs-version
      backup_share: nfs-host:path
manifests:
  statefulset_backup: true
  job_backup_storage_init: true
```

Results

You can now use the `cinder backup-create` command to back up your Cinder volumes.

Supported Extra Specs for Volume Type

Volume type extra specs are used for advanced configuration of Cinder volumes. VMware Integrated OpenStack exposes additional capabilities through volume type extra specs.

Table 6-1. Volume Type Extra Specs in VMware Integrated OpenStack

Extra Spec	Description
`vmware:vmdk_type`	Specify the provisioning format of Cinder volumes in vSphere. You can specify the following formats ■ Thin provision: `thin` ■ Thick provision lazy zeroed: `thick` ■ Thick provision eager zeroed: `eagerZeroedThick`
`vmware:clone_type`	Specify the clone type. You can specify the following types: ■ Full clone: `full` ■ Linked clone: `linked`
`vmware:storage_profile`	Enter the name of the storage policy to use for new volumes.
`vmware:adapter_type`	Specify the adapter type used to attach the volume. You can specify the following types: ■ IDE: `ide` ■ LSI Logic: `lsiLogic` ■ LSI Logic SAS: `lsiLogicsas` ■ BusLogic Parallel: `busLogic` ■ VMware Paravirtual SCSI: `paraVirtual`

Glance Images 7

In the OpenStack context, an image is a file that contains a virtual disk from which you can install an operating system on a virtual machine. You create an instance in your OpenStack cloud by using one of the images available.

The VMware Integrated OpenStack image service component natively supports images that are packaged in the ISO, OVA, and VMDK formats. You can also import RAW, QCOW2, VDI, and VHD images, which are automatically converted to the VMDK format during the image creation process.

VMware Integrated OpenStack only support the **`openstack image save`** and **`glance image-download`** commands for VMDK format image.

This chapter includes the following topics:

Import an Image

You can import an image file into your VMware Integrated OpenStack deployment and use it to launch instances.

The following image formats are supported:

- VMDK
- ISO
- OVA
- RAW
- QCOW2
- VDI

- VHD

Note ISO images cannot be used for creating volumes.

Procedure

1 To create an image in the horizon, log in to the VMware Integrated OpenStack dashboard.

2 Select your project from the drop-down menu in the title bar.

3 Select **Project > Compute > Images**.

4 Click **Create Image** and enter the desired configuration.

Option	Action
Image Name	Enter a name for the image.
Image Description	Enter a description for the image.
Image Source	Click **Browse** and select the image file.
Format	Select **ISO** or **VMDK**. For images in OVA, RAW, QCOW2, VDI, or VHD formats, select **VMDK** as the disk format.
Disk Adapter Type	For VMDK images, select the adapter type.
Minimum Disk (GB)	Specify the minimum disk size for the image in gigabytes.
Minimum RAM (MB)	Specify the minimum RAM for the image in megabytes.
Visibility	(Cloud administrators only) Select **Public** to make the image available to all projects or **Private** to make the image available only to the current project.
Protected	Select **Yes** to prevent the image from being deleted.

5 (Optional) Click **Next** and configure metadata for the image.

6 Click **Create Image**.

7 (Optional) Create Image using OpenStack CLI.

You can also create an image using the OpenStack CLI for uploading the local image file to VMware Integrated OpenStack.

For example, a simple command for uploading the local `vmdk` file.

```
openstack image create --disk-format vmdk --file local.vmdk \
--property vmware_adaptertype=paraVirtual \
--property vmware_disktype=streamOptimized \
--property vmware_create_template=false \
--property vmware_template_disk_type=thick \
--property vmdk_skip_conversion=true \
imagename
```

The following options are used for creating the `openstack image create` command.

Option	Description
`image-name`	Enter the name of the image.
`--disk-format`	Enter the disk format of the image. You must use `vmdk`.
`--file`	Specify the image file for uploading.
`{--public | private}`	To make the image available to all the users, include the parameter `--public`. To make the image available only to the current user, include the parameter `--private`.
`--property vmware_adaptertype`	Specify the adapter type of the VMDK disk. If you do not include this parameter, the adapter type is determined by introspection. **Note** ■ For disks using paravirtual adapters, include this parameter and set it to **`paraVirtual`**. ■ For disks using LSI Logic SAS adapters, include this parameter and set it to **`lsiLogicsas`**.
`--property vmware_disktype`	Specify **`sparse`** as the disk type. Otherwise, you can use **`streamOptimized`**. If you do not include this parameter, the disk type is determined by introspection. **Note** **`streamOptimized`** is the only supported disk type for vSAN datastore.
`--property vmware_create_template`	If `true`, VMware Integrated OpenStack can convert the image as a vSphere VM template for Nova instances creation. `True` is the recommended option. **Note** As the image file is converted to vSphere VM template, you cannot download the image as checksum changed. If `false`, VMware Integrated OpenStack can use the `vmdk` file as a glance image. With this option, the image can be downloaded using `openstack image save`.
`--property vmware_template_disk_type`	Specify the provisioning format for the image in vSphere. You can enter **`thin`** for thin provision or **`thick`** for thick provision lazy zeroed. If you do not include this parameter, thin provision is used by default.
`--property vmdk_skip_conversion`	Specify `true` for skipping the auto image conversion when uploading it by using the `openstack image create` command. The default value is `false`.

What to do next

You can now launch instances from the image. In the **Actions** column next to an image, you can edit or delete the image, update its metadata, launch an instance from the image, or create a volume from the image.

Import a VM Template as Image

You can add virtual machine templates to your VMware Integrated OpenStack deployment as Glance images.

Prerequisites

- Verify that the virtual machine template is located in the same vCenter Server instance as your VMware Integrated OpenStack deployment.
- Verify that the virtual machine template does not have multiple disks, a CD-ROM drive, or a floppy drive.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Open the toolbox and set the password for the `admin` account.

```
toolbox
export OS_PASSWORD=admin-account-password
```

3 Create an empty Glance image in VMDK format.

```
glance image-create --name image-name --disk-format vmdk --container-format bare
```

4 Add the location of the virtual machine template to the image.

```
glance location-add image-uuid --url vi://vcserver-ip/datacenter-name/vm/folder-name/
template-name
```

You can check the **VM and Templates View** in the vSphere Client to confirm the location of the template.

Results

The specified virtual machine template is imported as an image. You can launch OpenStack instances from the image or configure additional settings, such as image metadata.

Migrate an Image

You can migrate an image to another datastore while preserving its UUID and metadata.

Prerequisites

Determine the UUID of the image that you want to migrate and of the project containing the image. You can use the `openstack image list` command to display the UUID of each image and the `openstack image show` command to display the UUID of the project that contains a specified image.

Procedure

1. In the vSphere Client, open the **VMs and Templates** view and locate the image that you want to migrate.

   The image is located in the folder for the project that contains it.
2. Right-click the image and select **Clone to Template**.
3. Enter a new name for the image and click **Next**.
4. Select the desired compute resource and click **Next**.
5. Select the desired datastore and click **Next**.
6. Click **Finish**.
7. Record the name of the original image as shown in vSphere.
8. Delete the original image.
9. Rename the cloned image to the name of the original image.

Results

The image is moved to the new datastore. You can continue to launch instances from it normally.

Customize Windows Image

You can configure images for Windows guest customization by applying guest customization metadata.

Windows guest customization is an alternative to Cloudbase-Init. Do not use Windows guest customization metadata and Cloudbase-Init on the same image.

Prerequisites

- Install the appropriate version of Microsoft System Preparation (Sysprep) for each guest operating system that you want to customize.
- Install VMware Tools on the source image.

Procedure

1. Log in to the VMware Integrated OpenStack dashboard.
2. Select your project from the drop-down menu in the title bar.
3. Select **Project > Compute > Images**.

4 Create a new Windows image or choose an existing image to customize.

5 Select **Update Metadata** next to the image that you want to use.

6 In the **Available Metadata** pane, expand **Guest Customization Options**.

7 Click the **Add** (plus sign) icon next to the metadata that you want to configure.

Option	Description
Auto logon count	Enter the number of times that the machine can be automatically logged in to as Administrator. You can increase this value above 1 if your configuration requires multiple reboots. This value might be determined by the list of commands executed by the `GuiRunOnce` command.
Automatic logon	Select the checkbox to automatically log in to the VM as Administrator.
Maximum number of connections	Enter the number of client licenses purchased for the Windows server being installed. **Note** This parameter is used only if the server licensing mode is set to `PerServer`.
Product Key	Enter the serial number to include in the answer file when mini-setup runs. **Note** If the guest operating system was installed using a volume-licensed CD, this parameter is not required.
Server licensing mode	Select **PerServer** or **PerSeat** as the server licensing mode.
Windows workgroup to join	Select the workgroup that the virtual machine will join.

8 Click **Save**.

Results

When you launch instances from the image, the specified Windows guest customization options are applied.

Supported Image Metadata

Image metadata is used for advanced configuration of Glance images. VMware Integrated OpenStack exposes additional capabilities through image metadata.

Note Configuring virtual interface quotas is not supported in NSX-T Data Center. The following metadata cannot be used with NSX-T Data Center deployments:

- `quota_vif_limit`
- `quota_vif_reservation`
- `quota_vif_shares_level`
- `quota_vif_shares_share`

To configure QoS for NSX-T Data Center, create a Network I/O Control (NIOC) profile and apply it to the N-VDS for the transport nodes in your deployment. See "Configure Network I/O Control Profiles" in the *NSX-T Data Center Installation Guide*.

If an image metadata and flavor extra spec conflict, the image metadata takes precedence over the flavor extra spec.

Table 7-1. Image Metadata in VMware Integrated OpenStack

Extra Spec	Description
`quota_cpu_limit`	Specify the maximum CPU allocation in MHz. The value `0` indicates that CPU usage is not limited.
`quota_cpu_reservation`	Specify the guaranteed CPU allocation in MHz.
`quota_cpu_reservation_percent`	Specify the guaranteed CPU allocation as a percentage of the actual CPU speed of the instance. This parameter takes precedence over the `cpu_reservation` parameter.
`quota_cpu_shares_level`	Specify the level of CPU shares allocated. You can enter **`custom`** and add the `cpu_shares_share` parameter to provide a custom value.
`quota_cpu_shares_share`	Specify the number of CPU shares allocated. If the `cpu_shares_level` parameter is not set to `custom`, this value is ignored.
`quota_disk_io_limit`	Specify the maximum disk transaction allocation in IOPS. The value `0` indicates that disk transactions are not limited.
`quota_disk_io_reservation`	Specify the guaranteed disk transaction allocation in IOPS.
`quota_disk_io_shares_level`	Specify the level of disk transaction shares allocated. You can enter **`custom`** and add the `disk_io_shares_share` parameter to provide a custom value.
`quota_disk_io_shares_share`	Specify the number of disk transaction shares allocated. If the `disk_io_shares_level` parameter is not set to `custom`, this value is ignored.

Table 7-1. Image Metadata in VMware Integrated OpenStack (continued)

Extra Spec	Description
quota_memory_limit	Specify the maximum memory allocation in MB. The value 0 indicates that memory usage is not limited.
quota_memory_reservation	Specify the guaranteed memory allocation in MB.
quota_memory_reservation_percent	Specify the guaranteed memory allocation as a percentage of the actual memory of the instance. The value 100 indicates that guest memory is also fully reserved. This parameter takes precedence over the memory_reservation parameter.
quota_memory_shares_level	Specify the level of memory shares allocated. You can enter **custom** and add the memory_shares_share parameter to provide a custom value.
quota_memory_shares_share	Specify the number of memory shares allocated. If the memory_shares_level parameter is not set to custom, this value is ignored.
quota_vif_limit	Specify the maximum virtual interface bandwidth allocation in Mbps. The value 0 indicates that virtual interface bandwidth is not limited.
quota_vif_reservation	Specify the guaranteed virtual interface bandwidth allocation in Mbps.
quota_vif_shares_level	Specify the level of virtual interface bandwidth shares allocated. You can enter **custom** and add the vif_shares_share parameter to provide a custom value.
quota_vif_shares_share	Specify the number of virtual interface bandwidth shares allocated. If the disk_io_shares_level parameter is not set to custom, this value is ignored.
vmware_boot_efi_secure_boot	Specify **true** to perform signature checks on any EFI images loaded during startup.
vmware_boot_enter_bios	Specify **true** to make virtual machines enter the BIOS configuration on next startup. Virtual machines automatically reset this parameter after the next startup.
vmware_boot_retry	Specify the delay in milliseconds before the boot sequence is started.
vmware_boot_retry_delay	Specify the delay in milliseconds before the boot sequence is retried. If the boot_retry_enabled parameter is set to false, this value is ignored.
vmware_boot_retry_enabled	Specify **true** to retry the boot sequence if a boot failure occurs.
vmware_cpu_affinity	Specify a list of CPUs that instances can use. Use , to connect multiple values in the list. For example, [0,1,2].

Table 7-1. Image Metadata in VMware Integrated OpenStack (continued)

Extra Spec	Description
vmware_extra_config	Specify custom configurations in JSON format. For example, '{"acpi.smbiosVersion2.7":"FALSE"}'.
vmware_latency_sensitivity_level	Specify the latency sensitivity level for virtual machines. Setting this key will adjust certain settings on virtual machines.
vmware_resource_pool	Specify the resource pool on which to place new instances. If the name of the project containing the instance matches the name of a resource pool in your environment, the instance is placed in that resource pool by default. Setting this parameter overrides the default behavior and forces the instance to be placed in the specified resource pool.
vmware_storage_policy	Specify the storage policy used for new instances. If Storage Policy-Based Management (SPBM) is not enabled, this parameter is ignored.
vmware_tenant_vdc	Specify the UUID of the tenant virtual data center in which to place instances.
vmware_vgpu	Specify the number of shared vGPUs to attach to the instance.
vmware_vm_group	Specify the DRS VM group in which virtual machines will be placed. If the specified VM group does not exist, instances will fail to power on.

Heat Stacks

8

You can use Heat stacks to automate the deployment of infrastructure, services, and applications.

A stack can configure the automated creation of most OpenStack resources, including instances, floating IP addresses, volumes, security groups, and users. To create a stack, you use an orchestration template that defines the parameters for automating the deployment of infrastructure, services, and applications.

You can also create a stack that combines an orchestration template with an environment file. An environment file supplies a unique set of values to the parameters defined by the template. By using environment files with templates, you can create many unique stacks from a single template.

VMware Integrated OpenStack supports the native OpenStack Heat Orchestration Template (HOT) format through a REST API and the Amazon Web Services (AWS) CloudFormation template format through a Query API that is compatible with CloudFormation.

For information about how to create template and environment files for your Heat stacks, see "Template Guide" in the OpenStack documentation at https://docs.openstack.org/heat/train/template_guide/index.html.

This chapter includes the following topics:

Generate a Heat Template

You can use the Template Generator to create orchestration templates through a drag-and-drop interface.

The following are the supported resource types:

- `OS::Aodh::CompositeAlarm`
- `OS::Aodh::EventAlarm`
- `OS::Aodh::GnocchiAggregationByMetricsAlarm`
- `OS::Aodh::GnocchiAggregationByResourcesAlarm`
- `OS::Aodh::GnocchiResourcesAlarm`

- OS::Barbican::CertificateContainer
- OS::Barbican::GenericContainer
- OS::Barbican::Order
- OS::Barbican::RSAContainer
- OS::Barbican::Secret
- OS::Cinder::Quota
- OS::Cinder::Volume
- OS::Cinder::VolumeAttachment
- OS::Cinder::VolumeType
- OS::Designate::RecordSet
- OS::Designate::Zone
- OS::Heat::AccessPolicy
- OS::Heat::AutoScalingGroup
- OS::Heat::CloudConfig
- OS::Heat::DeployedServer
- OS::Heat::InstanceGroup
- OS::Heat::MultipartMime
- OS::Heat::None
- OS::Heat::RandomString
- OS::Heat::ResourceChain
- OS::Heat::ResourceGroup
- OS::Heat::ScalingPolicy
- OS::Heat::SoftwareComponent
- OS::Heat::SoftwareConfig
- OS::Heat::SoftwareDeployment
- OS::Heat::SoftwareDeploymentGroup
- OS::Heat::Stack
- OS::Heat::StructuredConfig
- OS::Heat::StructuredDeployment
- OS::Heat::StructuredDeploymentGroup
- OS::Heat::TestResource

- OS::Heat::UpdateWaitConditionHandle
- OS::Heat::Value
- OS::Heat::WaitCondition
- OS::Heat::WaitConditionHandle
- OS::Keystone::Domain
- OS::Keystone::Endpoint
- OS::Keystone::Group
- OS::Keystone::GroupRoleAssignment
- OS::Keystone::Project
- OS::Keystone::Region
- OS::Keystone::Role
- OS::Keystone::Service
- OS::Keystone::User
- OS::Keystone::UserRoleAssignment
- OS::Neutron::Firewall
- OS::Neutron::FirewallPolicy
- OS::Neutron::FirewallRule
- OS::Neutron::FloatingIP
- OS::Neutron::FloatingIPAssociation
- OS::Neutron::Net
- OS::Neutron::Port
- OS::Neutron::ProviderNet
- OS::Neutron::QoSBandwidthLimitRule
- OS::Neutron::QoSDscpMarkingRule
- OS::Neutron::QoSPolicy
- OS::Neutron::Quota
- OS::Neutron::RBACPolicy
- OS::Neutron::Router
- OS::Neutron::RouterInterface
- OS::Neutron::SecurityGroup
- OS::Neutron::SecurityGroupRule

- `OS::Neutron::Segment`
- `OS::Neutron::Subnet`
- `OS::Neutron::Trunk`
- `OS::Nova::Flavor`
- `OS::Nova::HostAggregate`
- `OS::Nova::KeyPair`
- `OS::Nova::Quota`
- `OS::Nova::Server`
- `OS::Nova::ServerGroup`
- `OS::Octavia::HealthMonitor`
- `OS::Octavia::L7Policy`
- `OS::Octavia::L7Rule`
- `OS::Octavia::Listener`
- `OS::Octavia::LoadBalancer`
- `OS::Octavia::Pool`
- `OS::Octavia::PoolMember`

Procedure

1. Log in to the VMware Integrated OpenStack dashboard.
2. Select your project from the drop-down menu in the title bar.
3. Select **Project > Orchestration > Template Generator**.
4. From the **Template Version** drop-down menu, select the desired Heat version.
5. Drag the icons for the desired resource types onto the canvas.
6. Click each icon to set parameters and dependencies and click **Save**.
7. When you have added and configured all desired resources, click the **Template Generator** icon.
8. Review the configuration and click **Download** to download the generated template or **Create Stack** to launch a stack using the generated template.

Launch a Stack

With orchestration stacks, you can launch and manage multiple composite cloud applications.

Prerequisites

Create the orchestration template for your stack. For more information, see "Template Guide" in the OpenStack documentation at https://docs.openstack.org/heat/train/template_guide/index.html.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard.

2 Select your project from the drop-down menu in the title bar.

3 Select **Project > Orchestration > Stacks**.

4 Click **Launch Stack** and enter your orchestration template.

Option	Description
Template Source	Select **File**, **Direct Input**, or **URL**. ■ If you select **File**, click **Choose File** and upload your orchestration template. ■ If you select **Direct Input**, enter your orchestration template in the **Template Data** field. ■ If you select **URL**, enter the URL where your orchestration template is located.
Environment Source	Select **File** or **Direct Input**. ■ If you select **File**, click **Choose File** and upload your environment file. ■ If you select **Direct Input**, enter your environment file in the **Environment Data** field.

5 Click **Next** and enter the configuration for your stack.

Option	Description
Stack Name	Enter a name for the stack.
Creation Timeout (minutes)	Enter the time in minutes after which stack creation will time out.
Rollback on Failure	Select the check box to roll back changes if the stack fails to launch.
Password for user "admin"	Enter the password for the `admin` user. This password is required to perform orchestration operations.

6 Click **Launch**.

What to do next

In the **Actions** column, you can suspend, resume, or delete your stack. You can also validate the stack or change its orchestration template and environment file.

Swift Object Storage

9

Swift is a component of OpenStack that provides distributed object storage.

Important In VMware Integrated OpenStack 7.1, Swift is provided as a technical preview only. Running production workloads is not currently supported.

For more information about Swift, see the OpenStack Swift documentation at https://docs.openstack.org/swift/train.

This chapter includes the following topics:

- Create the Swift Cluster
- Add Nodes to Your Swift Cluster
- Store Objects in Swift

Create the Swift Cluster

Creating the Swift cluster starts the Swift services and generates the necessary nodes.

Important In VMware Integrated OpenStack 7.1, Swift is provided as a technical preview only. Running production workloads is not currently supported.

Prerequisites

- Ensure that you have sufficient resources available to deploy Swift. The resources required depend on the scale of your deployment.
- Ensure that all hosts in the Swift cluster use a shared datastore (vSAN or NFS). Local datastores are not supported for Swift.
- Verify that all datastores included in the Swift cluster are available to all controller nodes in your deployment.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 In a text editor, create the Swift cluster configuration file in YAML format.

The configuration file must define three Swift nodes. Use the following template:

```
---
nodes:
- datastore: node1-datastore
  disk_size: node1-disksize-GB
  name: node1-name
  zone: node1-zone
- datastore: node2-datastore
  disk_size: node2-disksize-GB
  name: node2-name
  zone: node2-zone
- datastore: node3-datastore
  disk_size: node3-disksize-GB
  name: node3-name
  zone: node3-zone
```

Option	Description
node-datastore	Enter the name of the datastore for the specified Swift node.
node-disksize-GB	Enter the desired disk size in gigabytes.
node-name	Enter a name for the specified Swift node. The name of each node must be unique.
node-zone	Enter the Swift zone number for the specified Swift node. The zone number must be an integer.

3 Create the Swift cluster using the configuration file defined in the previous step.

```
viocli create swift -f swift-config-file
```

Results

The pods required for your Swift cluster are created and the service is enabled.

What to do next

To scale out your cluster, see Add Nodes to Your Swift Cluster.

To delete your Swift cluster, run the `viocli delete swift` command.

Add Nodes to Your Swift Cluster

You can add nodes to scale out your Swift cluster.

Important In VMware Integrated OpenStack 7.1, Swift is provided as a technical preview only. Running production workloads is not currently supported.

The nodes in a Swift cluster cannot be deleted. If you want to remove nodes from your cluster, you must delete the entire cluster and create it again.

Prerequisites

Deploy Swift. See Create the Swift Cluster.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Add a node to your cluster.

```
viocli add swiftnode --name node-name --datastore node-datastore --zone node-zone --disk-size node-disksize-gb
```

Option	Description
node-name	Enter a name for the Swift node. The name of each node must be unique.
node-datastore	Enter the name of the datastore for the node. Only shared datastores (vSAN or NFS) are supported. Swift nodes cannot be created on local datastores.
node-zone	Enter the Swift zone number for the node. The zone number must be an integer.
node-disksize-gb	Enter the desired disk size in gigabytes.

Store Objects in Swift

You can create containers in Swift and upload objects to them.

Important In VMware Integrated OpenStack 7.1, Swift is provided as a technical preview only. Running production workloads is not currently supported.

Prerequisites

Deploy Swift. See Create the Swift Cluster.

Procedure

1 Log in to the VMware Integrated OpenStack dashboard.

2 Select your project from the drop-down menu in the title bar.

3 Select **Project > Object Store > Containers** and click **Container**.

4 Enter a name, and click **Submit**.

The name of a container cannot include slashes (/).

5 Click the name of the container to open it.

6 (Optional) Click the **Folder** button to create a folder.

7 Click the **Upload** (up arrow) button to upload a file to the container.

What to do next

You can download or delete the files in your container. You can also click the down arrow next to any file to view details or select **Edit** to replace it with a different file.

Backup and Restore 10

You can back up your VMware Integrated OpenStack installation to ensure that you can restore from errors that may occur.

This chapter includes the following topics:

Back Up Your Deployment

You can use the command line to back up your OpenStack deployment.

Important The temporary configuration file created in this procedure contains the vCenter Server credentials in plaintext. For security purposes, delete this file after the backup is finished.

The following items are backed up:

- Configurations for OpenStack components
- OpenStack control plane database
- Deployment secrets

For information about backing up Cinder, see Cinder Volume Backup.

Prerequisites

Create a content library in your vCenter Server instance. For information about content libraries, see "Using Content Libraries" in *vSphere Virtual Machine Administration*.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 In a text editor, create the configuration file for the backup in YAML format.

Use the following template:

```
---
name: backup-name
description: backup-description
target:
   kind: contentLibrary
   contentLibrary:
      name: content-library-name
```

Option	Description
backup-name	Enter a name for the backup. The alphanumeric string can include special characters (-) and (_).
backup-description	Enter a description of the backup.
content-library-name	Enter the name of the Content Library for the backup save.

3 Specify the vCenter Server for the backup.

```
viocli create vcenter --vc_hostname <hostname> --vc_password <password> --vc_username
<username>
```

Or use an alias for the Kubernetes command-line utility to get the vCenter Server from the deployment.

```
osctl get vcenter
```

4 Create the backup with the configuration file and the vCenter Server.

```
viocli create backup -f <configuration-file> --content-vcenter <vcenter-name>
```

Results

A backup of your deployment is saved to the content library that you specified in the backup configuration file.

Scheduled Backup

You can configure your deployment to be automatically backed up on a regular schedule.

The following items are backed up:

- Configurations for OpenStack components
- OpenStack control plane database
- Deployment secrets

For information about backing up Cinder, see Cinder Volume Backup.

Prerequisites

Create a content library in your vCenter Server instance. For information about content libraries, see "Using Content Libraries" in *vSphere Virtual Machine Administration*.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 In a text editor, create the configuration file for the scheduled backup in YAML format.

Use the following template:

```
---
namePrefix: backup-name-prefix
description: backup-description
backupSchedule: backup-schedule
retentionPolicy:
  maximumNumberOfBackup: max-backups
target:
   kind: contentLibrary
   contentLibrary:
      name:content-library-name
```

Option	Description
backup-name-prefix	Enter a prefix for the backup files. The alphanumeric string can include the special character (-).
backup-description	Enter a description of the backup.
backup-schedule	Specify the backup schedule as a five-field cron expression. For example, enter **`"5 0 * * *"`** to back up every day at 00:05.
max-backups	The maximum number of backups to retain. Enter an integer greater than 0.
content-library-name	Enter the name of the Content Library for the backup save.

3 Specify the vCenter Server for the scheduled backup.

```
viocli create vcenter --vc_hostname <hostname> --vc_password <password> --vc_username
<username>
```

Or use an alias for the Kubernetes command-line utility to get the vCenter Server from the deployment.

```
osctl get vcenter
```

4 Create the backup task with the configuration file and the vCenter Server.

```
viocli create backupschedule -f <configuration-file> --content-vcenter <vcenter-name>
```

The backup task is created, and backups of your deployment are saved to the content library according to the specified schedule.

5 Verify the backup schedule.

```
viocli get backupschedule
```

Detail information about the backup cronjob is present in the output when you check scheduled backups.

Example output:

```
SCHEDULE NAME       STATUS    CREATION DATE                  NAME PREFIX   MAX BACKUPS
RETAINED   KIND             LOCATION                          DESCRIPTION
backupschedule322   Unknown   Wed Jun 17 13:53:42 UTC 2020   vio7-backup
2                     ContentLibrary   192.168.111.29:backupcontentlib   Backups for VIO7
deployment
```

6 To change the configurations of a scheduled backup, perform the following:

a Edit the backup schedule.

```
osctl edit backupschedule <backup_schedule_name>
```

b If you want to change `backupSchedule` frequency, change `backupSchedule` field under spec to target frequency.

```
spec:
  backupSchedule: <target-frequency>
```

c If you want to change `retentionPolicy`, change `maximumNumberOfBackup` field under spec to target number.

```
spec:
  retentionPolicy:
    maximumNumberOfBackup: <target-num>
```

d If you want to change content library name, change name field under `contentLibrary` to target name.

```
spec:
  target:
    contentLibrary:
      name: <target-contentLibrary-name>
    kind: contentLibrary
```

e Save the change and exit.

Note Do not change any other field not mentioned here.

Results

To delete a scheduled backup: `viocli delete backupschedule <backup_schedule_name>`.

Delete the command using the schedule name from the example: `viocli delete backupschedule backupschedule322`.

Restore Deployment

You can restore your VMware Integrated OpenStack deployment from a backup.

Important

- The temporary configuration file created in this procedure contains the vCenter Server credentials in plaintext. For security purposes, delete this file after the backup is finished.
- Do not perform multiple restore operations concurrently. If a restore operation is incorrectly configured, wait until the operation fails or times out before trying again.
- Unless the current database is corrupted, or there exists other paramount reasons that requires an earlier version, the current database should be backed up and used for restoration for the control plane. Restoration from an earlier version of backup could cause potential data loss.

Prerequisites

- Verify that you have a backup available. See Back Up Your Deployment or Scheduled Backup.
- If you are not performing an upgrade, verify that the VMware Integrated OpenStack versions are identical for restore and backup operations.

Procedure

1. Log in to the Integrated OpenStack Manager as the `root` user.

   ```
   ssh root@mgmt-server-ip
   ```

2. In a text editor, create the restoration configuration file in YAML format.
   - If you want to restore your VMware Integrated OpenStack on an existing control plane, use the following template:

     ```
     ---
     name: backup-file-name
     description: restore-description
     source:
        kind: contentLibrary
        contentLibrary:
           name: content-library-name
     datastore: control-plane-storage
     ```

The parameters are described as follows.

Option	Description
backup-file-name	Enter the name of the backup file to restore.
restore-description	Enter a description for the restoration task.
content-library-name	Enter the name of the content library containing the backup file.
control-plane-storage	(Optional) Enter the name of a datastore on which to store control plane information.

- If you want to restore your VMware Integrated OpenStack on a new control plane, use the following template:

```
---
cluster:
  network_info:
  - networkName: mgmt-network-name
    type: management
    static_config:
      ip_ranges:
      - mgmt-ip-range-begin, mgmt-ip-range-end
      netmask: mgmt-subnet-mask
      gateway: mgmt-gateway-address
      dns:
      - mgmt-dns-server
  - networkName: api-network-name
    type: api
    static_config:
      ip_ranges:
      - api-ip-range-begin, api-ip-range-end
      netmask: api-subnet-mask
      gateway: api-gateway-address
      dns:
      - api-dns-server
  - networkName: trunk-network-name
    type: dvs_trunk_network
    static_config:
      ip_ranges:
      - trunk-ip-range-begin, trunk-ip-range-end
---
datacenter: datacenter-name
datastore: datastore-name
resourcePool: resource-pool-name
count: controller-count
size: controller-size
---
name: backup-file-name
description: restore-description
source:
```

```
   kind: contentLibrary
   contentLibrary:
      name: content-library-name
datastore: control-plane-storage
```

The parameters are described as follows.

Table 10-1. Management Network Configuration

Option	Description
mgmt-network-name	Enter the name of the management network.

If your management network uses static IP addresses instead of DHCP, enter the following values. These values are not required for DHCP networks.

Option	Description
mgmt-ip-range-begin, *mgmt-ip-range-end*	Enter the IP address ranges on your management network in dotted-decimal format, separated by commas. For example, **`192.0.2.10, 192.0.2.50`**.
mgmt-subnet-mask	Enter the subnet mask for the management network.
mgmt-gateway-address	Enter the IP address of the network gateway for the management network.

mgmt-dns-server	Enter the IP address of one or more DNS servers for the management network. Enter each IP address on a separate line. For example:
	`- 192.0.2.1`
	`- 192.0.2.100`

Table 10-2. API Access Network Configuration

Option	Description
api-network-name	Enter the name of the API access network.

If your API access network uses static IP addresses instead of DHCP, enter the following values. These values are not required for DHCP networks.

Option	Description
api-ip-range-begin, *api-ip-range-end*	Enter the IP address ranges on your API access network in dotted-decimal format, separated by commas. For example, **`198.51.100.10, 198.51.100.50`**.
api-subnet-mask	Enter the subnet mask for the API access network.

Option	Description
api-gateway-address	Enter the IP address of the network gateway for the API access network.

api-dns-server	Enter the IP address of one or more DNS servers for the API access network. Enter each IP address on a separate line. For example:
	`- 198.51.100.1`
	`- 198.51.100.100`

If your deployment uses VDS networking, enter the following values. These values is not required for NSX deployments.

Table 10-3. Trunk Network Configuration

Option	Description
trunk-network-name	Enter the name of the trunk network.
trunk-ip-range-begin, *trunk-ip-range-end*	Enter the IP address ranges on your trunk network in dotted-decimal format, separated by commas. For example, **`169.254.0.1,169.254.0.254`**.

Enter the following information for all deployment types.

Table 10-4. Control Plane Configuration

Option	Description
datacenter-name	Enter the name of the vSphere data center in which to create the VMware Integrated OpenStack control plane.
datastore-name	Enter the name of the datastore for the VMware Integrated OpenStack control plane.
resource-pool-name	Enter the name of the resource pool for the VMware Integrated OpenStack control plane.

Table 10-4. Control Plane Configuration (continued)

Option	Description
controller-count	Specify the number of controllers to create.
controller-size	Specify the size of the controllers. The following values are accepted: ■ **`small`** (4 vCPUs and 16 GB of RAM) ■ **`medium`** (8 vCPUs and 32 GB of RAM) ■ **`large`** (12 vCPUs and 32 GB of RAM)

Table 10-5. Backup Configuration

Option	Description
backup-file-name	Enter the name of the backup file to restore.
restore-description	Enter a description for the restoration task.
content-library-name	Enter the name of the content library containing the backup file.

If your content library and VMware Integrated OpenStack are located in separate vCenter Server instances, enter the configuration for the vCenter Server instance containing the content library. The following values are not required if your content library and control plane are located in the same vCenter Server instance.

Table 10-6. Content Library Configuration

Option	Description
control-plane-storage	(Optional) Enter the name of a datastore on which to store control plane information.

3 Specify the vCenter Server for the VMware Integrated OpenStack deployment restoration.

```
viocli create vcenter --vc_hostname <host> --vc_password <password> --vc_username <user>
```

Or use an alias for the Kubernetes command-line utility to get the vCenter Server from the deployment.

```
osctl get vcenter
```

4 Restore your deployment with the configuration file, specifying the destination vCenter Server where you want to restore the deployment.

```
viocli restore deployment -f <configuration-file> --destination-vcenter=<vcenter-name> [--
skip-control-plane] [--content-vcenter=<vcenter-name>]
```

If the `--skip-control-plane` flag is set, restore your deployment by including the vCenter Server that contains the backup image for restoring.

```
viocli restore deployment -f <configuration-file> --destination-vcenter=<vcenter-name> --
skip-control-plane --content-vcenter=<vcenter-name>
```

For example, the following code shows restoring deployment by loading the file `backup_vio_edge_scale` to the directory `/var/lib/restore`.

```
body:
  {"value":

{"bytes_transferred":0,"size":19756648,"name":"backup_vio_edge_scale","download_endpoint":
      {"uri":"https://10.155.21.175:443/cls/data/853ecee5-ad10-492e-afe6-52a62728f5fb/
backup_vio_edge_scale"
      },"status":"PREPARED"
    }
  }
```

After you finish the backup, file `backup_vio_edge_scale` is successfully loaded from content library `bak_vio_edge` to directory `/var/lib/restore`.

If restore is successful, the message appears as: `download completed`, `prepare running`, and `restore succeeded`.

Results

The OpenStack deployment is restored to the state of the backup.

Note Because you use restoration function for deployment upgrade, you cannot restore the VMware Integrated OpenStack license and CA-signed certificate in the new deployment from the old deployment.

1 For restoring a certificate, you must resign and reapply for a certificate after restoration. Or you must perform the following steps:

   a Save the certs secret from the original deployment.

   ```
   osctl get secret certs -oyaml > certs.yaml
   ```

   b After restoration, in the new VMware Integrated OpenStack deployment, replace the `private_key` and the `vio_certificate` value in certs secret with the data from the previous step.

   c Stop and start services with `viocli`.

2 For restoring license, see Assign the VMware Integrated OpenStack License Key in *VMware Integrated OpenStack Installation Guide.*.

Disaster Recovery

11

Starting from VMware Integrated OpenStack 7.1, you can follow the validated procedure for recovering the VMware Integrated OpenStack management plane in another site when disaster occurs. After the recovery, you can use the VMware Integrated OpenStack for managing the protected instances, volumes, and networks in the recovery site.

This chapter includes the following topics:

Overview and Limitations

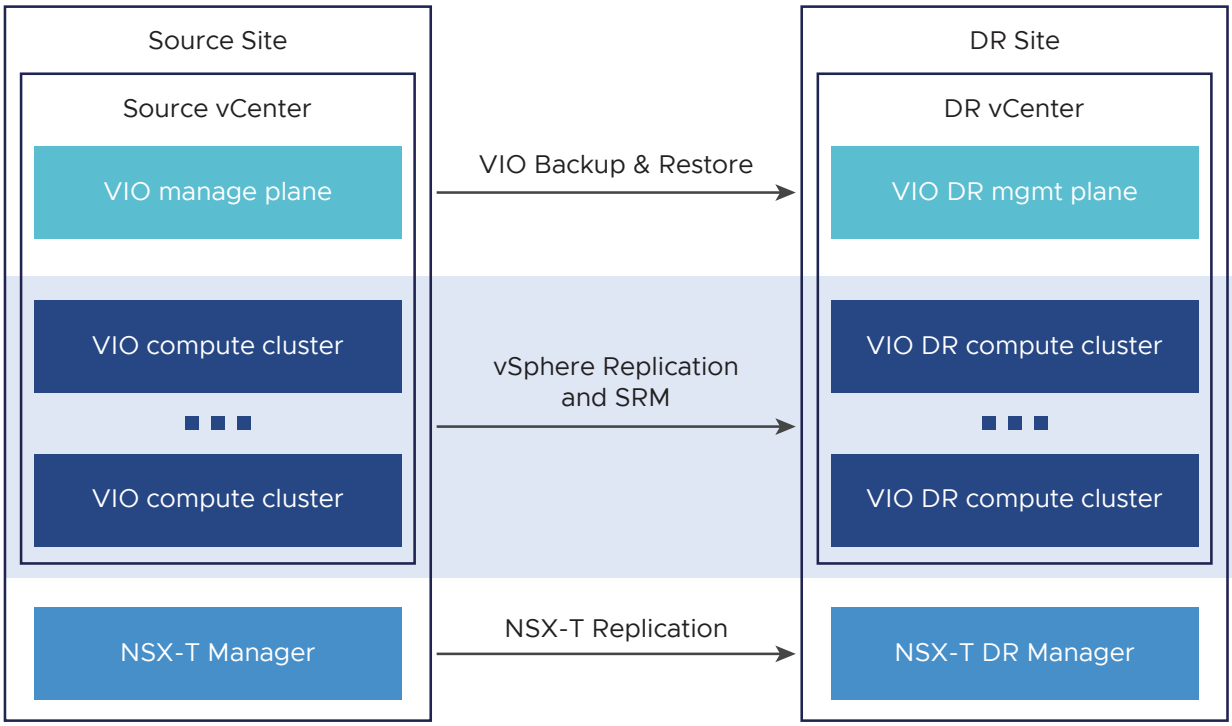
VMware Integrated OpenStack 7.1 supports and validates disaster recovery procedure. The disaster recovery procedure is validated with vSphere 7.0 u2 and NSX-T 3.1.1, SRM 8.4, and vSphere Replication 8.4.

For data plane disaster recovery, VMware Integrated OpenStack leverages the SRM and the vSphere Replication for protecting Nova instances, Cinder volumes, and leverages NSX-T for protecting Neutron networks.

For management plane disaster recovery, VIO leverages backup or restore procedure for recovering the VIO manager and the controller nodes in the recovery site.

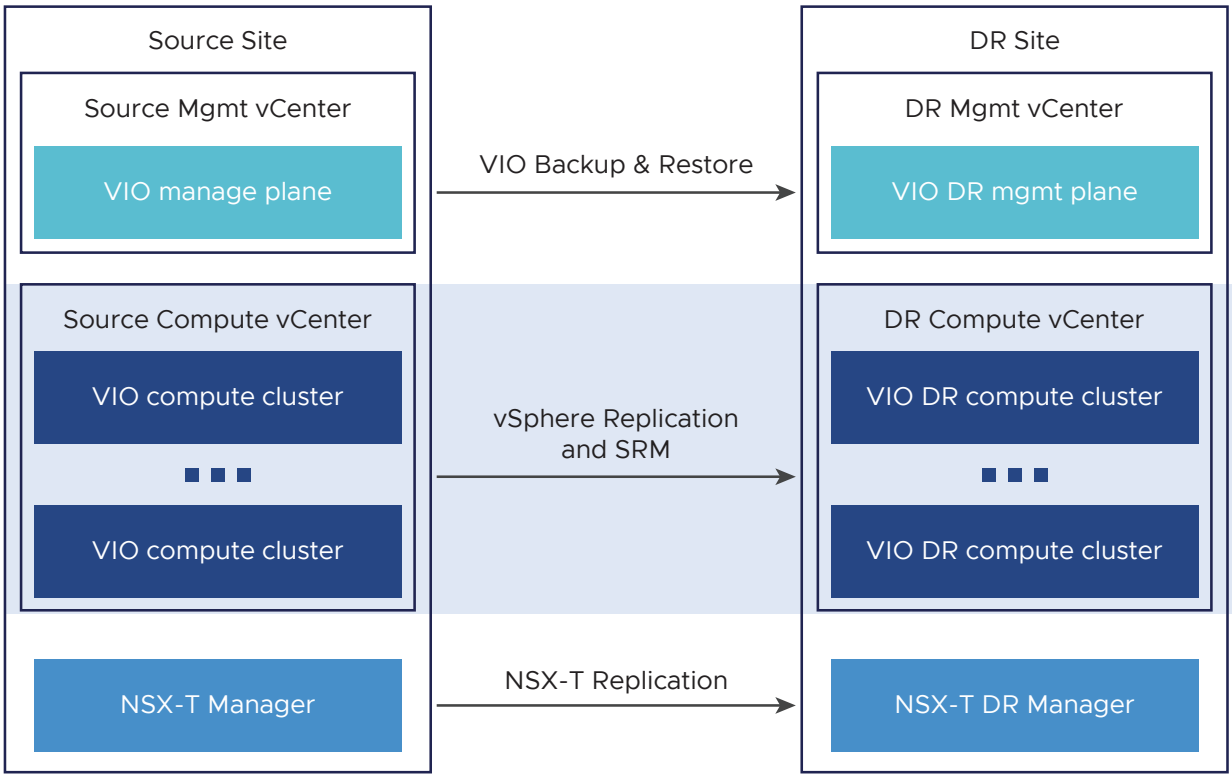
VMware Integrated OpenStack 7.1 supports Single vCenter and Multiple vCenter mode topologies. In the single vCenter topology, the management cluster and compute clusters are in the same vCenter for both the source and the target site as shown in the illustration.

Figure 11-1. Single vCenter Mode.



In the multiple vCenter topology, the management cluster is in vCenter1 and all compute clusters are in vCenter2 for the source and the target site as shown in the illustration.

Figure 11-2. Multiple vCenter Mode.



In VMware Integrated OpenStack 7.1, the disaster recovery procedure has the following limitations:

- The admin must manually configure the SRM and the vSphere Replication, and NSX-T for data plane protection and recovery.
- Supports one vCenter for management, and one vCenter for compute.
- Supports multiple compute clusters under the same vCenter for compute.
- Supports one to one mapping between source compute clusters and target compute clusters.
- Does not support instances with the SR-IOV and the vGPU devices.
- Does not support Cinder volume with the FCD driver.
- Does not support tenant VDC.
- Does not support OpenStack images.
- Does not support replicating instances with the protection group and the test plan. Otherwise, the volume attach and volume detach features can fail.

Data Plane Backup

Replicate Instances and Volumes

VMware Integrated OpenStack 7.1 leverages SRM and vSphere Replication for Nova and Cinder backup and recovery.

Before the disaster, you can use vSphere Replication for replicating instances and volumes from the source site to the target site.

Prerequisites

- Verify that you have the vSphere Replication is installed and configured in your environment. For more information see, Installing and Setting Up vSphere Replication.
- Verify that you have the VMware Site Recovery Manager installed and configured in your environment. For more information, see VMware Site Recovery Installation and Configuration.
- After installing the VMware Site Recovery Manager, log in to the SRM for configuring the replication servers, folder mappings, resource mappings, and placeholder datastores.

  Note When configuring the replication settings, you must have a one-to-one mapping from the source cluster to the target cluster.

Procedure

1 Replicate Nova instances:

   a In the vSphere Web Client, right click the virtual machine.

   b Select **All Site Recovery actions > Configure Replication**.

   c Follow the wizard to finish the configuration.

   In **Target site**, select the target site for VM replication.

   In **VM validation**, verify that you have configured the VMs.

   In **Target datastore**, select the datastore for the replicated files.

   In **Replication settings**, select the replication settings.

   Note If you select **Enable point in time instances**, the volume detach feature from Nova instances can fail at the target site.

   In **Protection group**, select **Do not add to protection group now**.

   In **Ready to complete**, review your settings, and click **Finish**.

2 Replicate Cinder volumes:

   a VMware Integrated OpenStack creates shadow VMs as the placeholder for OpenStack volumes. You must replicate shadow VM of Cinder volumes.

   b Verify volume status is `attached` or `available` by using the OpenStack command or Horizon UI.

c For volume in `available` status, you must replicate the shadow VM as Nova instances.

d For volume in the `attached` status, you must replicate the shadow VM as Nova instances.

Ensure that you select **Add to new protection group** and select **Do not add to recovery plan now**.

Replicate Networks

VMware Integrated OpenStack 7.1 leverages the NSX-T for network backup and recovery.

For more information about NSX-T Multisite, see NSX-T Data Center Multisite.

With VMware Integrated OpenStack 7.1, the disaster recovery procedure is validated with NSX-T Multiple Site Manual or Scripted Recovery of the Management Plane steps.

Prerequisites

Verify that you have NSX-T configured with continuous backup. For more information about configuring NSX-T, see NSX-T Configuration with Continuous Backup.

Procedure

1. There is no further configuration needed if the network objects created by VMware Integrated OpenStack Neutron are protected and backup by the NSX-T backup procedure.
2. Create Tier-0 Gateways, DHCP profile, and Metadata Proxy with the new edge cluster in the disaster recovery site. These resources can be used for network recovery when disaster occurs in the primary location.
3. (Optional) Before the disaster, create a pre-installed NSX Manager Cluster in the target disaster recovery site to save recovery time.

Data Plane Recovery

Recover Networks

When a disaster occurs on the primary location, you can recover the NSX-T deployment in the disaster recovery site with the backup data.

Prerequisites

- Verify that you have NSX-T configured with continuous backup.
- Verify that the NSX-T is deployed and configured with disaster recovery vCenter as compute manager in the disaster recovery site.
- Verify that the edge cluster, transport nodes, tier-0 gateway, DHCP profile, metadata proxy is created and configured with NSX-T in the disaster recovery site.

Procedure

1 Restore the NSX-T manager. For more information about restoring the NSX-T manager, see Restore NSX-T Manager.

2 Verify that the VMware Integrated OpenStack objects are recovered successfully.

3 For each recovered tier-1 router, update the edge cluster and linked tier-0 gateway.

4 For each recovered segment, update the new metadata proxy in the disaster recovery site.

5 For DHCP profile, update the new edge cluster in the disaster recovery site.

Recover Instances and Volumes

When a disaster occurs on primary location, you recover the Nova instances and Cinder volumes in the target disaster recovery site using SRM.

Note You do not have to recover virtual machine of the Cinder volume in attached status.

Procedure

1 Log in to the Site Recovery manager in the target site.

2 Under **Replications**, select the virtual machine and click **RECOVER**.

3 Under **Recover virtual machine**, select **Recovery options**.

   a Select **Synchronize recent changes**.

   b Unselect **Power on the virtual machine after recovery**.

   c Click **Next**.

4 In the **Folder** section, specify a folder for the virtual machine at the recovery site and click **Next**.

5 In the **Resource** section, specify the resource for the virtual machine at the recovery site and click **Next**.

   Note The target cluster must have one-to-one mapping with the source compute cluster.

6 In the **Ready to complete** section, review your selected settings and click **Finish**.

7 For Nova instance VM, select the network from the **Network adapter 1** tab and select **Connect At Power On**. For Cinder volume shadow VM, you can skip this step.

8 Power on the Nova instance VMs. For Cinder volume shadow VM, leave it as power off.

Management Plane Backup

Before disaster, you can configure `viocli` backup scheduler and duplicate the backup file to another vCenter.

Create VMware Integrated OpenStack Scheduled Backup Task

You can automatically backup your VMware Integrated OpenStack deployment on a regular schedule. For more information about creating a scheduled backup task, see Scheduled Backup.

Save Backup Data Outside the Source Site

You must save the backup data outside the source site. For example, you can download the backup data from the content library and upload it to a file server in a third site. The vSphere Content Library has its own built-in native replication mechanism which allows you for publishing and subscribing the libraries between two different vCenter servers. You can leverage this option for saving the backup data out of the source site. For more information about backing up data out of the source site, see VMware vSphere Virtual Machine documentation.

Management Plane Recovery

To recover your VMware Integrated OpenStack deployment, you must deploy VMware Integrated OpenStack virtual appliance, and use `viocli create drrecover` for updating the VMware Integrated OpenStack backup data, and then use restore procedure for recovering the deployment in the disaster recovery site.

Prerequisites

- Verify that you deploy VMware Integrated OpenStack 7.1 OpenStack virtual appliance in the disaster recovery target site.
- Verify that there is a VMware Integrated OpenStack backup package in the vCenter content library in the disaster recovery target site.
- Before disaster, you must prepare the disaster recovery YAML file.

Procedure

1. Create the vCenter and the NSX CR in target site.
   a. Create CR for management and compute vCenter servers.

   ```
   viocli create vcenter -n 10.155.20.126 -u administrator@vsphere.local -p 'xxxxxx'
   ```

   b. Create CR for NSX manager.

   ```
   viocli create nsx -n nsxmgr01.violab.com -u admin -p 'xxxxxx!xxxxxx'
   ```

c Retreive the vCenter and NSX CR names.

```
viocli get vcenter
NAME              CREATION DATE            VALIDATION
vcenter155        2021-04-28 14:03:17      Success
vcenter388        2021-04-28 14:02:12      Success
viocli get nsx
NAME              CREATION DATE            VALIDATION
nsx950            2021-04-28 14:05:10      Success
```

d Calculate Nova compute name in the target site.

- Log in to the management vCenter or compute vCenter.
- Click each `nova-compute` cluster for obtaining the URL from the address bar. For example:

  ```
  https://<vcenter_server>/ui/app/cluster;nav=h/
  urn:vmomi:ClusterComputeResource:domain-c8:7e8d8b50-09e4-4cbf-ba52-cab4ae78eba6/
  summary
  ```

- Extract the string `ClusterComputeResource:domain-cx:xxxxxxxx` from the http URL for each compute cluster for reforming compute node name.

  For example, for `ClusterComputeResource:domain-c8:7e8d8b50`, compute node name is `compute-7e8d8b50-c8`.

2 Create the disaster recovery template and edit the source and target site information.

```
viocli create drrecover -o > drrecover.yaml
```

3 Edit the disaster recovery template YAML file with the necessary configuration information.

Note Ensure that you configure the backup package disaster recovery vCenter content library in the backup configuration section in YAML.

4 Generate a disaster recovery package in vCenter content library using the `drrecover` command.

```
viocli create drrecover -f drrecover.yaml
```

Verify that there is a new backup package generated in the disaster recovery vCenter content library, for example: `backup125-DR-625849`.

5 Use the new generated backup package `backup125-DR-625849` for restoring the VMware Integrated OpenStack deployment in the disaster recovery vCenter. For more information, see Restore Deployment.

6 After restore procedure, your deployment is recovered in the disaster recovery site. You can use it to manage the recovered instances, volumes, and networks.

Following are the examples for the disaster recovery tempate. You can check the details for the configurations.

Target site configuration:

```
# Target site deployment configurations
# vCenter name to create control plane and the backup data from source site must be in
content library of this vcenter
# Could use osctl get vCenter to retreive and config vCenter_name: vcenter293
vcenter_name:
```

OpenStack Configuration:

```
# OpenStack deployment configurations
osdeployment:
  openstack_endpoints:
    # Should be in the same network segment with management network
    private_vip: 10.155.20.136
    # Should be in the same network segment with API network
    public_vip: 10.155.21.96
  # Storage policy daatstore to create persistent volume
  datastore: ds-vio
```

Neutron Configuration:

```
# Neutron configurations
neutron:
  conf:
    dns:
      designate_enabled: true
    plugins:
      nsx:
      # Support nsx policy neutron driver
        nsx_p:
          # default overlay transport zone id
          deafult_overlay_tz: 4f12b507-e5b5-40fc-91dc-1943b9f63ea7
          # default vlan transport zone id
          default_vlan_tz: 7c33e81e-7b21-474b-89d4-b0312649e3fd
          # default tier0 router name
          default_tier0_router: dr-tier0-gateway
          # dhcp_profile id
          dhcp_profile: vio-dhcp-profile-dr
          # metadata proxy id
          metadata_proxy: vio-md-proxy-dr-ts
          # nsx object for target site
          nsx_name: nsx718
```

OpenStack service configuration for management server:

```
# OpenStack service configurations for mgmt vcenter
- vcenter_name: vcenter293
  mgmt: true
  novacomputes:
  # Replicate following fields for each novacompute
```

```
  # Source site nova compute name i.e. compute-xxxxxx-cxx. Could get from "viocli get
novacompute"
  - source_compute_name:
    # Target site nova compute name i.e. compute-yyyyyy-cyy.
    target_compute_name:
    # Target site nova compute cluster name
    cluster_name:
    datastore_regex:
    # Fill in the dvs moid for each novacompute if CarrierEdition and SRIOV enabled
    # dvs_moid:
  glance:
  # Replicate following fields for each glance backend
  - vmware_datastores:
  cinder:
  # Replicate following fields for each cinder backend
  # Source site cinder backend name i.e. nova-xx.xx.xx.xx-vmdk-1. Could get from
spec.conf.backends section in "osctl get cinder -oyaml"
  - source_backend_name:
    # List each compute cluster from the next line after "vmware_cluster_name:", one for
each line.
    # Do not add anything after "vmware_cluster_name:".
    vmware_cluster_name:
    # Replicate following field for each cluster
```

OpenStack service configuration for compute vCenter:

```
compute vcenter
- vcenter_name: vcenter187
  mgmt: false
  novacomputes:
  # Replicate following fields for each novacompute
  # Source site nova compute name i.e. compute-xxxxxx-cxx. Could get from "viocli get
novacompute"
  - source_compute_name: compute-5479e7cb-c8
    # Target site nova compute name i.e. compute-yyyyyy-cyy.
    target_compute_name: compute-8f710e32-c8
    # Target site nova compute cluster name
    cluster_name: domain-c8
    datastore_regex: ds26\-2
    # Fill in the dvs moid for each novacompute if Carrier Edition and SRIOV enabled
    # dvs_moid:
  - source_compute_name: compute-5479e7cb-c1014
    # Target site nova compute name i.e. compute-yyyyyy-cyy.
    target_compute_name: compute-8f710e32-c1009
    # Target site nova compute cluster name
    cluster_name: domain-c1009
    datastore_regex: ds9\-1
    # Fill in the dvs moid for each novacompute if CarrierEdition and SRIOV enabled
    # dvs_moid:
  glance:
  # Replicate following fields for each glance backend
  - vmware_datastores: ds26-1
  cinder:
  # Replicate following fields for each cinder backend
  # Source site cinder backend name i.e. nova-xx.xx.xx.xx-vmdk-1. Could get from
```

```
spec.conf.backends section in "osctl get cinder -oyaml"
  - source_backend_name: cinder1-10.155.20.145-vmdk-1
    # List each compute cluster from the next line after "vmware_cluster_name:", one for
each line.
    # Do not add anything after "vmware_cluster_name:".
    vmware_cluster_name:
    # Replicate following field for each cluster
    - compute01
  - source_backend_name: cinder1-10.155.20.145-vmdk-2
    # List each compute cluster from the next line after "vmware_cluster_name:", one for
each line.
    # Do not add anything after "vmware_cluster_name:".
    vmware_cluster_name:
    # Replicate following field for each cluster
    - compute02
```

Backup Configuration:

```
# Backup configurations from source site
# Name of the backup file
name: backup125
source:
  kind: contentLibrary
  contentLibrary:
    # Name of the content library containing
    name: VIO
# Optional, specified the datastore to be us
datastore: ds-vio
```

Post Recovery Configuration

After you recover the VMware Integrated OpenStack deployment from a disaster, you can use the post disaster recovery command for updating the OpenStack database.

Procedure

1 Update the OpenStack Nova compute database.

```
vio-post-dr
```

`vio-post-dr` command updates the OpenStack Nova compute DB.

For example, if `compute-5479e7cb-c1014` in source site is mapped to `compute-8f710e32-c1009` in target site, run the following command:

```
vio-post-dr compute-5479e7cb-c1014 compute-8f710e32-1009 fix
```

2 Clean stale Glance images.

Since the images replication is not supported, as a result, the images in the target site are no longer useful and you must run the Glance command for removing the stale resources.

```
osctl exec -ti mariadb-server-0 -- mysql --defaults-file=/etc/mysql/admin_user.cnf -e
"delete from glance.image_members; delete from glance.image_properties; delete from
glance.image_tags; delete from glance.image_locations; delete from glance.images;"
```

3 Update Neutron external network.

You must update the OpenStack Neutron external network to point to the new tier-0 gateway in disaster recovery target site.

```
openstack network set --provider-physical-network dr-site-t0-gateway external-network-name
```

Configuration Options

12

VMware Integrated OpenStack admin can configure each service components such as the Keystone, Nova, Cinder, and so on, by using the `viocli update` command.

The `viocli update` command accepts the YAML input format. VMware Integrated OpenStack can convert the YAML format to the OpenStack community compliant format.

For more information about OpenStack options, see the OpenStack train configuration at https://docs.openstack.org/train/configuration/.

Note If the parameter value is not correct, it can cause the services to not startup. You can receive the corresponding pod error or a crashloop message.

Use the following YAML format for the `viocli update` command.

```
conf:
  service:      # nova, keystone, neutron, cinder
    section1:   # example: default
      key1: value1
    section2:   # example: ldap
      key2: value2
    section3:   # example: backend
      key3: value3
```

VMware Integrated OpenStack can convert the YAML format to the classic OpenStack configuration files for the corresponding service components.

```
[section1] # [DEFAULT]
key1 = value1
[section2]      # [ldap]
key2 = value2
[section3]      # [backend]
key3 = value3
```

After the update is complete, wait for few minutes for the pods being recreated, then you can confirm that your change is effective within the service pod.

For example, the `viocli update heat` updates the heat.conf in the heat engine pod. To confirm the status of your configuration, you can use the heat engine command.

```
# osctl get pods | grep heat-engine | grep Running
heat-engine-7bbbbbf787-r9kq7                                        1/1     Running
0          3m57s
# osctl exec -it heat-engine-7bbbbbf787-r9kq7  -- cat /etc/heat/heat.conf
```

This chapter includes the following topics:

viocli update Keystone Command

You can update certain parameters in your Keystone service configuration by using the `viocli update keystone` command.

For more information about Keystone configuration, see the Openstack Keystone configuration documentation at https://docs.openstack.org/keystone/train/configuration/config-options.html#configuration.

For more information about Keystone service configuration examples, see the OpenStack Keystone configuration examples at https://docs.openstack.org/keystone/train/configuration/samples/keystone-conf.html.

Configuration options example using `viocli update keystone`.

```
conf:
  keystone:
    DEFAULT:
      list_limit: 100
    token:
      expiration: 7200

  ks_domains:
    <keystone domain name>:
      ldap:
        user_enabled_invert: false
        user_enabled_mask: 2
```

```
        user_enabled_default: true
        chase_referrals: false
        debug_level: 4095
        pool_retry_max: 20
        pool_size: 200
        pool_retry_delay: 0.1
        pool_connection_timeout: -1
        pool_connection_lifetime: 600
        use_auth_pool: true
        auth_pool_size: 100
        auth_pool_connection_lifetime: 60
        user_enabled_attribute: userAccountControl
        lockout_failure_attempts = 6
        lockout_duration = 1800
```

Table 12-1. viocli update Keystone Parameters

Parameter	Default Value	Description
`list_limit`	`none`	Enter the maximum number of entities that can be returned in a collection.
`expiration`	Minimum value: `0` Maximum value: `9223372036854775807`	Enter the amount of time the token can take to remain valid. Drastically increasing this value can increase load on the driver and drastically decreasing this value can break the long running operations.
`ks_domains`		Enter the Keystone domain name.
`user_enabled_invert`	`false`	Enter `true` to disable the account. Setting `keystone_ldap_user_enabled_invert: true` can allow you to use the lock attributes.
`user_enabled_mask`	`0`	Enter `2` to set the mask value. A value of `0` indicates that you cannot use the mask.
`user_enabled_default`	`true`	Enter `true` to enable the keystone LDAP users. However, if this is not `true`, the typical value is `512`.
`chase_referrals`	`none`	Enter the systems default referral chasing behavior boolean value for queries.
`debug_level`	`none`	Enter the LDAP debugging level value for LDAP calls. The minimum value is `-1`. A value of `0` indicates that you cannot enable debugging.
`pool_retry_max`	`3`	Enter the maximum number of times to attempt reconnecting to the LDAP server. The minimum value is `0`.
`pool_size`	`10`	Enter the size of the LDAP connection pool. The minimum value is `0`.
`pool_retry_delay`	`0.1`	Enter the number of seconds to wait before attempting to reconnect to the LDAP server.

Table 12-1. viocli update Keystone Parameters (continued)

Parameter	Default Value	Description
pool_connection_timeout	-1	Enter the connection timeout value to use when pooling LDAP connections. A value of -1 indicates that connection can never timeout.
pool_connection_lifetime	600	Enter the maximum connection lifetime to the LDAP server in seconds. The minimum value is 1.
use_auth_pool	true	Enter true to enable LDAP connection pooling for end-user authentication.
auth_pool_size	100	Enter the size of the connection pool to use for end-user authentication. The minimum value is 1.
auth_pool_connection_lifetime	60	Enter the maximum end-user authentication connection lifetime value in seconds. The minimum value is 1.
user_enabled_attribute	enabled	Enter the LDAP attribute that you can map to user-enabled flag.
lockout_failure_attempts	5	Configures the maximum number of failed authentication attempts.
lockout_duration	1800	Configures the number of seconds an account is locked out after you reach lockout_failure_attempts. If set to 0, accounts are locked permanently until specifically unlocked from CLI/API.

viocli update Nova Command

You can update certain parameters in your Nova service configuration by using the `viocli update nova` command.

For more information about Nova configuration, see the Openstack Nova configuration documentation at https://docs.openstack.org/nova/train/configuration/config.html.

For more information about Nova service configuration examples, see the OpenStack Nova configuration examples at https://docs.openstack.org/nova/train/configuration/sample-config.html.

Configuration options example using `viocli update nova`.

```
conf:
  nova:
    DEFAULT:
      force_config_drive: false
      rpc_response_timeout: 6000
      executor_thread_pool_size: 64

    conductor:
      workers: 2
```

```
    vmware:
      network_passthrough: false
      tenant_vdc: false

    filter_scheduler:
      max_instance_per_host: 50
      max_io_ops_per_host: 8
      available_filters: nova.scheduler.filters.all_filters
      enabled_filters:
AvailabilityZoneFilter,ComputeFilter,ComputeCapabilitiesFilter,ImagePropertiesFilter,

ServerGroupAntiAffinityFilter,ServerGroupAffinityFilter,PciPassthroughFilter,AggregateInstance
ExtraSpecsFilter

    pci:
      alias: [{"device_type": "type-VF", "name": "sriov"}, {"vendor_id":"8086",
"product_id":"1520",
      "device_type": "type-PF", "name":"fpt"}]
      passthrough_whitelist: [{"vendor_id": "*", "product_id": "*"}]

    cinder:
      cross_az_attach: true

    scheduler:
      max_attempts: 3

    database:
      max_pool_size: 50
```

Table 12-2. viocli update Nova Parameters

Parameter	Default Value	Description
force_config_drive	false	Enter true to force enable the configuration drive functionality. However, you can still enable the configuration drives through the REST API or image metadata properties.
rpc_response_timeout	60	Enter the value in seconds to wait for a response from a call.
executor_thread_pool_size	64	Enter the size of the executor thread pool for the executor to thread or eventlet.
workers	none	Enter the number of workers for the OpenStack Conductor service.
max_instances_per_host	50	Enter the maximum number of instances that can exist on a host.
max_io_ops_per_host	8	Enter the maximum number of instances that can actively perform input and output operation on a host.

Table 12-2. viocli update Nova Parameters (continued)

Parameter	Default Value	Description
available_filters	nova.scheduler.filters.all_filters	Enter filters that a scheduler can use.
enabled_filters		Enter filters that a scheduler must use. Supported filters: AvailabilityZoneFilter, ComputeFilter,, ImagePropertiesFilter,, ServerGroupAffinityFilter PciPassthroughFilter, AggregateInstanceExtraSpecs Filter, AggregateMultiTenancyIsolation
alias	''	Enter the aliasfor the PCI passthrough device requirement.
passthrough_whitelist	''	Enter the allowlist of peripheral component interconnect devices available to virtual machines.
cross_az_attach	true	Enter the attach between instance and volume in different availability zones. If this value is false, volumes attached to an instance must be in the same availibility zone in Cinder as the instance availibility zone in Nova.
max_attempt	3	Enter the maximum number of schedule attempts for a chosen host.
max_pool_size	none	Enter the maximum number of SQL connections to keep open in a pool. A value of 0 indicates no limit.

viocli update Nova Compute Command

You can update certain parameters in your Nova Compute service configuration by using the `viocli update nova-compute` command.

Configuration options example using `viocli update nova-compute`.

```
conf:
  nova_compute:
    DEFAULT:
      debug: true
      default_schedule_zone: nova1
      host: compute-7e8d8b50-c8
      cpu_allocation_ratio: 16
      ram_allocation_ratio: 1.5
      disk_allocation_ratio: 0.0
```

```
    max_concurrent_builds: 20
    always_resize_on_same_host: False
    sync_power_state_interval: 600
    sync_power_state_action: dbsync
    use_hypervisor_stats: true
    update_resources_interval: 0
    # Options of the interval (in second) to schedule the cache image cleanup worker thread
    image_cache_manager_interval: 2400
    # Options of the expiration (in second) for unused image cache to be deleted
    remove_unused_original_minimum_age_seconds: 86400

  vmware:
    host_ip: .VCenter:vcenter1:spec.hostname
    host_password: .VCenter:vcenter1:spec.password
    host_username: .VCenter:vcenter1:spec.username
    insecure: .VCenter:vcenter1:spec.insecure
    cluster_name: domain-c8
    datastore_regex: sharedVmfs\-1|sharedVmfs\-0
    network_passthrough: false
    tenant_vdc: false
    pbm_enabled: true
    pbm_default_policy: <policy_name>
    set_asset_tag: <value>
    import_vm_enabled: true
    import_vm_relocate: true
    datastore_selection_policy: max_free_space
    import_net_id: None
    datastore_cluster: dsc
    shared_datastore_regex: sharedVmfs\-1|sharedVmfs\-0

    dvs_moid:
    # compute01: dvs-35
    # compute02: dvs-36
    default_vif_model: vmxnet3
    gpu_profile: grid_p100-4a
    profile_fb_size_kb: 4096
```

Table 12-3. viocli update Nova Compute Parameters

Parameter	Default Value	Description
`debug`	`false`	Enter `true` to set the logging level to `debug` rather than the default INFO level.
`default_schedule_zone`	`none`	Enter the default availability zone fot instances.
`host`	`<current_hostname>`	Enter the hostname, FQDN, or IP address of this host.
`cpu_allocation_ratio`	`none`	Enter the virtual CPU to physical CPU allocation ratio.
`ram_allocation_ratio`	`none`	Enter the virtual RAM to physical RAM allocation ratio.

Table 12-3. viocli update Nova Compute Parameters (continued)

Parameter	Default Value	Description
disk_allocation_ratio	none	Enter the virtual disk to physical disk allocation ratio.
max_concurrent_builds	10	Enter the the maximum number of instance builds to run concurrently by nova-compute.
always_resize_on_same_host		Enter the force destination node to match source for resize.
sync_power_state_interval	600	Enter the interval to sync power states between the database and the hypervisor.
sync_power_state_action		The action to take when there is an inconsistency with the database instance state and the actual state of the instance.
use_hypervisor_stats		This option specifies whether to use vCenter stats or rely on nova resource tracking.
update_resources_interval	0	This option specifies how often the update_available_resources periodic task is run.
image_cache_manager_interval	2400	This option specifies the interval in seconds to schedule the cache image cleanup worker thread.
remove_unused_original_minimum_age_seconds	86400	This option specifies the expiration in seconds for unused image cache to be deleted..
host_ip	none	Enter the hostname or IP address for connection to VMware vCenter host.
host_password	none	Enter the password for connection to VMware vCenter host.
host_username	none	Enter the username for connection to VMware vCenter host
insecure	false	Verify the HTTPS connection.
cluster_name	none	Enter the name of the VMware Cluster ComputeResource.
datastore_regex	none	Enter the regular expression setting, which specifies the datastores to use with compute.
network_passthrough		Flag to enable or disable network passthrough features.
tenant_vdc		Flag to enable or disable tenant vdc.

Table 12-3. viocli update Nova Compute Parameters (continued)

Parameter	Default Value	Description
pbm_enabled	false	This option enables or disables storage policy based placement of instances.
pbm_default_policy	none	This option specifies the default policy to be used.
use_linked_clone	true	Enter the linked clone.
set_asset_tag		This option is to provide a workaround to bug.
import_vm_enabled		Flag to enable or disable import vm.
import_vm_relocate		This option can reorganize imported virtual machines to follow the default naming convention and folder placement as per VMware driver.
datastore_selection_policy	max_connected_hosts	Enter the nova datastore selection policy.
import_net_id		Enter the NSXT switch UUID required for enabling the virtual machine to be plugged into the correct neutron port.
datastore_cluster		Enter the name or moid of a datastore cluster.
shared_datastore_regex		Enter the regular expression for shared datastores for CD-ROM.
default_vif_model		Enter the default vnic model.
gpu_profile		Enter the profile for GPU passthrough devices.
profile_fb_size_kb		Enter the GPU profile frame buffer size in kilobytes.

viocli update Cinder Command

You can update certain parameters in your Cinder service configuration by using the `viocli update cinder` command.

For more information about Cinder configuration, see the Openstack Cinder configuration documentation at https://docs.openstack.org/cinder/train/configuration/block-storage/drivers/vmware-vmdk-driver.html.

For more information about Cinder service configuration examples, see the OpenStack cinder configuration examples at https://docs.openstack.org/cinder/train/_static/cinder.conf.sample.

Configuration options example using `viocli update cinder`.

```
conf:
  backends:
    nova1-10.185.245.206-vmdk-1:
      backend_availability_zone: nova1
      vmware_cluster_name:
        type: multistring
        values:
        - nova.Prod.100
        - nova.Prod.200
      vmware_host_ip: .VCenter:vcenter1:spec.hostname
      vmware_host_password: .VCenter:vcenter1:spec.password
      vmware_host_username: .VCenter:vcenter1:spec.username
      vmware_image_format: template
      vmware_insecure: .VCenter:vcenter1:spec.insecure
      volume_driver: cinder.volume.drivers.vmware.vmdk.VMwareVcVmdkDriver
      vmware_adapter_type: <type-name> #available value: ide, busLogic, lsiLogicsas,
paraVirtual. Recommend use paraVirtual.
      vmware_tmp_dir: /tmp
      vmware_snapshot_format: template
      vmware_lazy_create: true
      vmware_disable_backing_ref_cache: false
      vmware_datastore_regex:
      vmware_verify_requirements: true
      vmware_datastore_cluster:
      vmware_sdrs_default_cluster_name:
      vmware_snapshot_quiesce: true
      vmware_image_transfer_timeout_secs: 7200


  cinder:
    DEFAULT:
      default_availability_zone: nova1
      enabled_backends: nova1-10.185.245.206-vmdk-1
      vmware_adapter_type: <type-name> #available value: ide, busLogic, lsiLogicsas,
paraVirtual. Recommend use paraVirtual.
      default_volume_type: __DEFAULT__
      default_availability_zone:
      storage_availability_zone: nova
      backup_driver: cinder.backup.drivers.nfs.NFSBackupDriver
      backup_mount_options: vers=4
      backup_share: nfs-host:path
      backup_workers: 1
      backup_executor_thread_pool_size: 4
      backup_rpc_response_timeout: 600
      backup_file_size: 1999994880
      backup_sha_block_size_bytes: 32768
      backup_compression_algorithm: zlib
      rpc_response_timeout: 60
      executor_thread_pool_size: 64
    database:
      max_pool_size: 5
```

```
manifests:
  statefulset_backup: true
  job_backup_storage_init: true
```

Table 12-4. viocli update Cinder Parameters

Parameter	Default Value	Description
backend_availability_zone	none	Enter the availability zone for the volume backend.
vmware_cluster_name		Enter the name of a vCenter compute cluster where you can create volumes.
vmware_host_ip	none	Enter the IP address for connecting to VMware vCenter Server.
vmware_host_password	none	Enter the password for authenticating with VMware vCenter Server.
vmware_host_username	none	Enter the username for authenticating with VMware vCenter Server.
vmware_image_format		Enter the image format to use for uploading volume to the image service.
vmware_insecure	false	If true, the vCenter certificate is not verified.
volume_driver	cinder.volume.drivers.vmware.vmdk.VMwareVcVmdkDriver	Enter the driver to use for volume creation.
vmware_adapter_type	lsilogic	Enter the adapter type used for attaching volumes.
vmware_tmp_dir	/tmp	Enter the directory where virtual disks are stored during volume backup and restore.
vmware_snapshot_format		Enter the volume snapshot format in vCenter Server.
vmware_lazy_create	true	If true, the backend volume in vCenter Server is created lazily when the volume is created without any source.
vmware_disable_backing_ref_cache	false	If true, the caching of vCenter references of legacy volume backends are disabled and queried by volume name rather than volume ID.
vmware_datastore_regex	none	Enter the regular expression pattern to match the name of the datastores where you can create backend volumes.
vmware_verify_requirements	novalocal	If true, the space and storage policy requirements verification takes place during raw volume creation.

Table 12-4. viocli update Cinder Parameters (continued)

Parameter	Default Value	Description
vmware_datastore_cluster		Enter the name or moid of datastore cluster where you can provision volume.
vmware_sdrs_default_cluster_name		Enter the default cluster for raw volume creation using vSphereStorage DRS. If you specify vmware_datastore_cluster, you must set this option.
vmware_snapshot_quiesce	none	If true, you can enable quiescing for backend snapshots created during snapshot or clone of a volume attached to a powered-on instance.
vmware_image_transfer_timeout_secs	7200	Enter the timeout in seconds for VMDK volume transfer between cinder and glance.
enabled_backends	none	Enter the list of backend names to use.
default_volume_type	none	Enter the default volume type to use.
default_availability_zone	nova	Enter the default availability zone of this node.
storage_availability_zone	nova	Enter the availability zone of this node.
backup_driver	cinder.backup.drivers.nfs.NFSBackupDriver	Configure this option to use the cinder backup feature.
backup_mount_options	none	Enter the mount options passed to the NFS client. See NFS man page for details.
backup_share	none	Enter the NFS server path with format.
backup_workers	1	Enter the number of backup processes to launch.
backup_executor_thread_pool_size		Enter the size of executor thread pool for backup restore operations.
backup_rpc_response_timeout		Enter the number of seconds to wait for a response from a long running RPC call during backup and restore.
backup_file_size	1999994880	Enter the maximum size in bytes of the file used to hold backups.
backup_sha_block_size_bytes	32768	Enter the size in bytes that track changes for incremental backups.
backup_compression_algorithm	zlib	Enter the name of the compression algorithm to use.

Table 12-4. viocli update Cinder Parameters (continued)

Parameter	Default Value	Description
rpc_response_timeout	60	Enter the value in seconds to wait for a response from a call.
executor_thread_pool_size	64	Enter the size of the executor thread pool when executor is threading or eventlet.
max_pool_size	5	Enter the number of SQL connections to keep open in a pool.
statefulset_backup		Create the manifests section if using the cinder backup feature.
job_backup_storage_init		Create the manifests section if using the cinder backup feature.

viocli update Glance Command

You can update certain parameters in your Glance service configuration by using the `viocli update glance` command.

Configuration options example using `viocli update glance`.

```
conf:
  glance:
    DEFAULT:
      client_socket_timeout: 1800

  backends:
    vmware0:
      vmware_datastores: DC.vio.001:sharedVmfs-1:100,DC.vio.001:sharedVmfs-0:100
      vmware_insecure: .VCenter:vcenter1:spec.insecure
      vmware_server_host: .VCenter:vcenter1:spec.hostname
      vmware_server_password: .VCenter:vcenter1:spec.password
      vmware_server_username: .VCenter:vcenter1:spec.username
      vmware_store_image_dir: /images
      vmware_create_template: true
      bypass_vcenter: true
```

Table 12-5. viocli update Glance Parameters

Parameter	Default Value	Description
client_socket_timeout	900	Enter the timeout for client connections socket operations.
vmware_create_template	true	Enter `true` if the uploaded image is a virtual template.
bypass_vcenter		Enter `true` to upload images directly to ESXi server or through vCenter.

Table 12-5. viocli update Glance Parameters (continued)

Parameter	Default Value	Description
vmware_store_image_dir	/openstack_glance	Enter the path to store vmdk images in the datastore. This works when vmware_create_template is false.
vmware_datastores	''	Enter the datastore for storing images.
vmware_insecure	false	Set the verification of the ESX/ vCenter server certificate.
vmware_server_host		Enter the address of the ESX/ESXi or vCenter target system.
vmware_server_password		Enter the server password.
vmware_server_username		Enter the server username.

viocli update Neutron Command

You can update certain parameters in your Neutron service configuration by using the `viocli update neutron` command.

Configuration options example using `viocli update neutron`.

```
conf:
  neutron:
    DEFAULT:
      api_workers: 8
      rpc_workers: 1
      max_allowed_address_pair: 10

    quotas:
      quota_network: 100
      quota_subnet: 100
      quota_port: 500
      quota_router: 10
      quota_floatingip: 50
      quota_security_group: 10
      quota_security_group_rule: 100

    plugins:
      nsx:
        nsxv:
          # (ListOpt) Ordered list of router_types to allocate as tenant routers.
          tenant_router_types: shared, distributed, exclusive
          # This option is supported starting from VIO 7.1.
          # default_edge_size = <purpose>:<edge size>[,...]
          # Supported purpose are router, dhcp, lb.
          # Supported sizes are compact, large, xlarge, quadlarge.
          default_edge_size: dhcp:compact, router:large, lb:quadlarge
```

```
        nsx_p:
          default_overlay_tz: 10096ec5-9ec4-4f2e-841d-80167c8d3005
          default_tier0_router: first_tier0_router
          default_vlan_tz: bf86b52f-a629-4c07-a8bd-14b4b46ba384
          dhcp_profile: openstack_dhcp_profile
          ens_support: true
          insecure: .NSX:nsx1:spec.insecure
          metadata_proxy: openstack_md_proxy

metadata_proxy_shared_secret: .Secret:managedencryptedpasswords:data.metadata_proxy_shared_sec
ret

nsx_api_managers: .NSX:nsx1:spec.hostname,.NSX:nsx2:spec.hostname,.NSX:nsx3:spec.hostname
          nsx_api_password: .NSX:nsx1:spec.password
          nsx_api_user: .NSX:nsx1:spec.username
          # if the default CGNAT range in NSX-T is updated, below values must be updated to
the same.
          transit_networks: 100.64.0.0/16, fc3d:e3c3:7b93::/48
```

Table 12-6. viocli update Neutron Parameters

Parameter	Default Value	Description
api_workers	none	Enter the number of separate API worker processes for service.
rpc_workers	none	Enter the number of RPC worker processes for service.
max_allowed_address_pair	10	Enter the maximum number of allowed address pairs.
dns_domain	openstacklocal	Enter the domain to use for building the hostnames.
quota_network	100	Enter the number of networks allowed per tenant.
quota_subnet	100	Enter the number of subnets allowed per tenant.
quota_port	500	Enter the number of ports allowed per tenant.
quota_router	10	Enter the number of routers allowed per tenant.
quota_floatingip	50	Enter the number of floating IPs allowed per tenant.
quota_security_group	10	Enter the number of security groups allowed per tenant.
quota_security_group_rule	100	Enter the number of security rules allowed per tenant.

Table 12-6. viocli update Neutron Parameters (continued)

Parameter	Default Value	Description
`default_edge_size`		This option is supported starting from VIO 7.1 with NSX-V. Supported purpose are `router`, `dhcp`, snd `lb`. Supported sizes are `compact`, `large`, `xlarge`, and `quadlarge`. `default_edge_size`: *<purpose>:<edge size>[,..]*
`tenant_router_types`		You can enter `exclusive`, `shared`, `distributed`, or any combination separated by `(,)`.
`default_overlay_tz`		The default overlay transport zone in NSX-T.
`default_tier0_router`		The default T0 Gateway in NSX-T.
`default_vlan_tz`		The default vLAN transport zone in NSX-T.
`dhcp_profile`		The default DHCP profile in NSX-T.
`ens_support`	`false`	Enter `true` if enable the enhanced data path feature.
`metadata_proxy`		Enter the profile name or UUID. This is a mandatory option.
`transit_networks`		If the default CGNAT range in NSX-T is updated, transit network values must be updated to the same. `transit_networks`: `IPv4CIDR`, `IPv6CIDR`

viocli update Heat Command

You can update certain parameters in your Heat service configuration by using the `viocli update heat` command.

For more information about Heat configuration, see the Openstack Heat configuration documentation at https://docs.openstack.org/heat/train/configuration/config-options.html.

Configuration options example using `viocli update heat`.

```
conf:
  heat:
    DEFAULT:
      max_resources_per_stack: 1000
      max_stacks_per_tenant: 100
      event_purge_batch_size: 200
      max_events_per_stack: 1000
```

```
      encrypt_parameters_and_properties: false
      max_nested_stack_depth: 5
      max_interface_check_attempts: 60
      convergence_engine: true
      observe_on_update: false
      max_template_size: 524288
      stack_action_timeout: 3600
      max_pool_size: 5
      max_overflow: 50
      rpc_response_timeout: 60
      client_retry_limit: 2
```

You can also update heat parameters in a non-interactive mode as given in the following example:

```
kubectl -n openstack patch heat heat1 --type=merge --patch '{"spec":{"conf":{"heat":
{"DEFAULT":{"rpc_response_timeout":360}}}}}'
```

Updating heat parameters in a non-interactive mode yields the same result as the `viocli update heat` command.

Table 12-7. viocli update Heat Parameters

Parameter	Default Value	Description
max_resources_per_stack	1000	Enter the maximum number of resources that a heat stack can use.
max_stacks_per_tenant	100	Enter the maximum number of heat stacks that each project can create.
event_purge_batch_size	200	Enter the size of the stack events purged.
max_events_per_stack	1000	Enter the number of maximum events that are available per stack.
encrypt_parameters_and_properties	false	Encrypt template parameters that are marked as hidden and also all the resource properties before storing them in database.
max_nested_stack_depth	5	Enter the maximum number of times to check whether an interface has been attached or detached.
max_interface_check_attempts	10	Enter the number of times to check whether an interface has been attached or detached
convergence_engine	true	This option enables the engine with convergence architecture.
observe_on_update	false	On update enables heat to collect existing resource properties from reality and converge to updated template
max_template_size	524288	Enter the maximum file size in bytes of a heat template.

Table 12-7. viocli update Heat Parameters (continued)

Parameter	Default Value	Description
stack_action_timeout	3600	Enter the timeout in seconds for heat stack actions.
max_pool_size	5	Enter the maximum number of SQL connections to keep open in a pool.
max_overflow	50	If set, enter the maximum value with SQLAlchemy.
rpc_response_timeout	60	Enter the seconds to wait for a response from a call.
client_retry_limit	2	Enter the number of times to retry when a client encounters an expected intermittent error.

viocli update MariaDB Command

You can update certain parameters in your MariaDB service configuration by using the `viocli update mariadb` command.

Configuration options example using `viocli update mariadb`.

```
conf:
  connect_timeout: 5
  max_connections: 5000
  net_read_timeout: 1200
  net_write_timeout: 1200
  ingress:
    proxy-read-timeout: "1200"
    proxy-send-timeout: "1200"
    proxy-stream-timeout: 3600s
```

Table 12-8. viocli update MariaDB Parameters

Parameter	Default Value	Description
connect_timeout	10	Enter the number of seconds the `mysqld` server is waiting for a packet.
proxy_read_timeout	60	Enter the timeout for reading a response from the proxied server.
proxy_send_timeout	60	Enter the timeout for transmitting a request to the proxied server.
max_connections	151	This option determines the number of connections the `mysql/mariadb` accepts.

Table 12-8. viocli update MariaDB Parameters (continued)

Parameter	Default Value	Description
net_read_timeout	30	Enter the number of connections to wait for more data from a connection before aborting the read.
net_write_timeout	30	Enter the number of seconds to wait for more data from a connection before aborting the read.

Update Policies for Services

You can add `policy` section for controlling RBAC policy for specific services.

Each OpenStack service, such as identity, compute, networking, and so on, has its own role-based access policies. These policies determine which objects you can access and they are defined in the services policy configuration file. For VMware Integrated OpenStack deployment, you must use `viocli update` command for editing the corresponding services policy configuration.

Note For VIO 7.x, Keystone has a default reader and member role. It is not functional by default. You must edit the corresponding services policy for using the role explicitly to meet your permission control requirements. For more information about user and role management, see Keystone User and Role Management.

Syntax:

Use `viocli update <service>` command for adding RBAC policy for specified services.

You can use `project_id`, `user_id`, `domain_id`, or `role` for creating the user scoping conditions. Use the following operators for general scopes combination:

- **!**: No user can perform the operation.
- @ or **""**: Any users can perform the operation.
- **not**, **and**, **or**: The operator for combining multiple scope.

The following sample code shows the different operators for general scopes combination:

```
conf:
  policy:
    "alias_1": "is_admin:True or project_id:%(project_id)s"
    "alias_2": "role:reader"
    "alias_3": "other user scope definition"
    "operation_1": "!"
    "operation_2": "@"
    "operation_3": "rule:alias_1 or (rule:alias_2 and rule:alias_3)"
```

Example:

You can define certain rules like the `power_user` and the `read_user` within your policy configuration file. For example, in the following code the `read_user` calls the APIs for server index, show, and details, but it cannot create, delete, start, and stop Nova instances.

```
conf:
  nova:
    vmware:
      #some configurations for VIO
  policy:
    power_user: (role:member) and project_id:%(project_id)s
    read_user: (role:reader) and project_id:%(project_id)s
    os_compute_api:servers:detail: rule:read_user
    os_compute_api:servers:index: rule:read_user
    os_compute_api:servers:show: rule:read_user
    os_compute_api:servers:start: rule:power_user
    os_compute_api:servers:stop: rule:power_user
    os_compute_api:servers:create: rule:power_user
    os_compute_api:servers:delete: rule:power_user
```

Review the full policies:

You must find the service pod and then review the policy file content. Use the following commands for reviewing the full Nova policy:

```
# osctl get pod | grep nova-api-osapi
nova-api-osapi-7d7978fb44-b24rl                                   2/2     Running
0          3d23h

# osctl exec -it nova-api-osapi-7d7978fb44-b24rl /bin/bash
Defaulting container name to nova-osapi.
Use 'kubectl describe pod/nova-api-osapi-7d7978fb44-b24rl -n openstack' to see all of the
containers in this pod.

[root@nova-api-osapi-7d7978fb44-b24rl /]# cat /etc/nova/policy.yaml

os_compute_api:os-simple-tenant-usage:discoverable: '@'
......
```

For more information about policies for different services, see the following OpenStack community documents:

Keystone: Keystone Policy

Nova: Nova Policy

Cinder: Cinder Policy

Glance: Glance Policy

Neutron: Neutron Policy

Command Reference

13

VMware Integrated OpenStack includes the `viocli` utility to configure and manage your deployment on the command line. To use `viocli`, connect to the Integrated OpenStack Manager over SSH and log in as the `root` user.

For NSX deployments, the `nsxadmin` utility is also provided to perform certain network-related operations. You must log in to a Neutron server pod to use `nsxadmin`. For information about `nsxadmin` commands, see the `nsxadmin` documentation at https://opendev.org/x/vmware-nsx/src/branch/master/doc/source/admin_util.rst.

The Kubernetes `kubectl` command-line utility may be required for some operations. For more information about `kubectl`, see the official Kubernetes documentation.

The following aliases are provided to improve user experience for operators.

Alias	Kubectl Command
`osctl`	`kubectl -n openstack`
`osapply`	`kubectl -n openstack apply`
`osctlw`	`kubectl -n openstack --watch`
`osdel`	`kubectl -n openstack delete`
`osedit`	`kubectl -n openstack edit`
`osget`	`kubectl -n openstack get`
`oslog`	`kubectl -n openstack logs`

In addition, the `viossh` *`controller-node-name`* alias allows you to log in to a controller node.

This chapter includes the following topics:

Comparison of Command-Line Operations

In VMware Integrated OpenStack 7.1, the command-line utilities have been refactored. The following table lists the command-line operations in VMware Integrated OpenStack 5.1 and their equivalents in version 7.1.

Table 13-1. Comparison of Command-Line Operations

VMware Integrated OpenStack 5.1 Command	VMware Integrated OpenStack 7.1 Command
`viocli backup`	`viocli create backup`
`viocli barbican`	This command has been deprecated. Use the Integrated OpenStack Manager web interface to configure Barbican.
`viocli certificate add`	`viocli import certificate`
`viocli certificate list`	`viocli get certificates`
`viocli certificate remove`	This command has been deprecated. Use the `viocli import certificate` command to replace incorrect or expired certificates.
`viocli certificate show`	`viocli get certificates`
`viocli dbverify`	This command has been deprecated.
`viocli deployment cert-req-create`	`viocli create csr`
`viocli deployment cert-update`	`viocli import certificate`
`viocli deployment configure`	This command has been deprecated. When you use the `viocli update` command to configure your deployment, the changes are applied immediately.

Table 13-1. Comparison of Command-Line Operations (continued)

VMware Integrated OpenStack 5.1 Command	VMware Integrated OpenStack 7.1 Command
`viocli deployment default`	This command has been deprecated.
`viocli deployment getlogs`	`viocli generate supportbundle`
`viocli deployment pause`	This command has been deprecated.
`viocli deployment post-deploy`	This command has been deprecated.
`viocli deployment reset_status`	This command has been deprecated.
`viocli deployment resume`	This command has been deprecated.
`viocli deployment run-custom-playbook`	This command has been deprecated.
`viocli deployment start`	This command has been deprecated.
`viocli deployment status`	`viocli get deployment`
`viocli deployment stop`	This command has been deprecated.
`viocli ds-migrate-prep`	`viocli prepare datastore`
`viocli enable-tvd`	`viocli add tvd`
`viocli epops`	This command has been deprecated. End Point Operations Management agents are no longer used for integration with vRealize Operations Manager.
`viocli federation`	This command has been deprecated. Use the Integrated OpenStack Manager web interface to configure identity federation.
`viocli identity`	This command has been deprecated. Use the Integrated OpenStack Manager web interface to configure authentication.
`viocli inventory-admin clean-instance-vms`	`viocli delete orphaned-managed-vms`
`viocli inventory-admin clean-instances`	`viocli delete orphaned-instances`
`viocli inventory-admin clean-shadow-vms`	`viocli delete orphaned-shadow-vms`
`viocli inventory-admin create-tenant-vdc`	`viocli create tenant-vdc`
`viocli inventory-admin delete-tenant-vdc`	`viocli delete tenant-vdc`
`viocli inventory-admin list-tenant-vdcs`	`viocli get tenant-vdcs`
`viocli inventory-admin reset-instances-state`	`viocli reset instances`
`viocli inventory-admin show-availability-zones`	`viocli get availability-zones`
`viocli inventory-admin show-hypervisors`	`viocli get hypervisors`
`viocli inventory-admin show-instance-vms`	`viocli get managed-vms`

Table 13-1. Comparison of Command-Line Operations (continued)

VMware Integrated OpenStack 5.1 Command	VMware Integrated OpenStack 7.1 Command
`viocli inventory-admin show-instances`	`viocli get instances`
`viocli inventory-admin show-shadow-vms`	`viocli get shadow-vms`
`viocli inventory-admin show-tenant-vdc`	`viocli get tenant-vdcs`
`viocli inventory-admin sync-availability-zones`	This command has been deprecated. Synchronizing availability zones is no longer necessary.
`viocli inventory-admin update-tenant-vdc`	`viocli update tenant-vdc`
`viocli lbaasv2-enable`	This command has been deprecated.
`viocli recover`	This command has been deprecated. Nodes are automatically recovered.
`viocli restore`	`viocli restore deployment`
`viocli rollback`	This command has been deprecated.
`viocli services start`	`viocli start services`
`viocli services stop`	`viocli stop services`
`viocli show`	`viocli get controllers`
`viocli swift add-proxy`	`viocli add swiftnode`
`viocli swift add-storage`	`viocli add swiftnode`
`viocli swift create-cluster`	`viocli create swift`
`viocli swift delete-cluster`	`viocli delete swift`
`viocli swift list-datastore-zone-mapping`	This command has been deprecated.
`viocli upgrade`	This command has been deprecated.
`viocli volume-migrate`	`viocli migrate volume`
`viocli vros`	This command has been deprecated. Integration with vRealize Automation is no longer supported.
`viopatch add`	These commands have been deprecated. Patching is not supported in VMware Integrated OpenStack 7.1.
`viopatch install`	
`viopatch list`	
`viopatch snapshot`	
`viopatch uninstall`	
`viopatch version`	`viocli version`

VMware Integrated OpenStack Toolbox

VMware Integrated OpenStack includes a toolbox container in which you can run OpenStack command-line clients and other utilities.

To access the toolbox, log in to the Integrated OpenStack Manager as the `root` user and run the `toolbox` command.

OpenStack Client

The toolbox includes the following OpenStack clients:

- Aodh
- Barbican
- Cinder
- Designate
- Glance
- Gnocchi
- Heat
- Keystone
- Neutron
- Nova
- Swift

The toolbox is automatically configured with the settings for the `admin` user in your OpenStack deployment. To log in as another user, download the RC file from the VMware Integrated OpenStack dashboard and apply it to the toolbox container.

1 Log in to the VMware Integrated OpenStack dashboard.

2 From the menu in the top-right corner, select **OpenStack RC File**.

3 Transfer the file to the VMware Integrated OpenStack toolbox container.

4 Apply the settings by running the `source` *`rc-file`* command.

Other Utilities

In addition to the OpenStack clients, the toolbox includes the Data Center Command-Line Interface (DCLI). To use DCLI, run the `dcli` command and specify the private OpenStack endpoint of your deployment.

```
dcli +server https://internal-vip:9449/api +i
```

For more information, see the VMware Data Center CLI page at https://code.vmware.com/web/tool/2.12.0/vmware-datacenter-cli.

Note The `nsxadmin` utility cannot be run from the toolbox. To use `nsxadmin`, open a shell to the Neutron server container:

```
kubectl -n openstack exec -it neutron-server-pod-name -- /bin/bash
```

viocli add Command

Use the `viocli add` command to add plugins and resources to your VMware Integrated OpenStack deployment.

The `viocli add` command supports a variety of actions to perform different tasks. The following parameters apply to all actions.

Parameter	Mandatory or Optional	Description
`-v` or `--verbose`	Optional	Displays output in verbose mode.

You can run `viocli add -h` or `viocli add --help` to display the parameters for the command. You can also use the `-h` or `--help` option on any action to display parameters for the action. For example, `viocli add swiftnode -h` will show parameters for the `swiftnode` action.

The actions that `viocli add` supports are listed as follows.

`viocli add swiftnode --name` *`node-name`* `--datastore` *`ds-name`* `--zone` *`swift-zone`* `--disk-size` *`size-gb`* `[-v]`

Adds a node to the Swift cluster.

Parameter	Mandatory or Optional	Description
`--name` *node-name*	Mandatory	Specifies the name of the new node.
`--datastore` *ds-name*	Mandatory	Specifies the datastore on which to create the node.
`--zone` *swift-zone*	Mandatory	Specifies the Swift zone in which to place the node.
`--disk-size` *size-gb*	Mandatory	Specifies the disk size in gigabytes for the node.

`viocli add tvd -m manager-ip -u nsx-username -p nsx-password --insecure {true | false} --overlay-tz overlay-tz --vlan-tz vlan-tz --tier-0-router t0-router --dhcp-profile dhcp-profile --md-proxy md-proxy --md-proxy-secret shared-secret [-v]`

Adds NSX-T Data Center networking support to a VMware Integrated OpenStack deployment that was deployed with NSX Data Center for vSphere.

Parameter	Mandatory or Optional	Description
`-m` *manager-ip* or `--manager` *manager-ip*	Mandatory	IP address of the NSX Manager of your NSX-T Data Center deployment.
`-u` *nsx-username* or `--username` *nsx-username*	Mandatory	User name of the NSX Manager administrator.
`-p` *nsx-password* or `--password` *nsx-password*	Mandatory	Password for the NSX Manager administrator.
`--insecure {true | false}`	Optional	Specifies whether to verify the certificate of the NSX Manager. If you do not include this option, `true` is used by default.
`--overlay-tz` *overlay-tz*	Mandatory	Name or UUID of the default NSX-T Data Center overlay transport zone used for creating tunneled isolated Neutron networks.
`--vlan-tz` *vlan-tz*	Mandatory	Name or UUID of the default NSX-T Data Center VLAN transport zone used for bridging between Neutron networks if no physical network has been specified.
`--tier-0-router` *t0-router*	Mandatory	Name or UUID of the default tier-0 router used to connect to tier-1 logical routers and configure external networks.
`--dhcp-profile` *dhcp-profile*	Mandatory	Name or UUID of the DHCP server profile used to enable native DHCP service. You must create the profile in NSX-T Data Center before using the plugin.
`--md-proxy` *md-proxy*	Mandatory	Name or UUID of the metadata proxy server used to enable native metadata service. You must create the metadata proxy server in NSX-T Data Center before using the plugin.
`--md-proxy-secret`	Mandatory	Shared secret for metadata proxy requests.

viocli create Command

Use the `viocli create` command to create backups, scheduled backups, certificate signing requests (CSRs), and Swift clusters and nodes.

The `viocli create` command supports a variety of actions to perform different tasks. The following parameters apply to all actions.

Parameter	Mandatory or Optional	Description
`-f` *config-file* or `--file` *config-file*	Optional	Runs the command using a specified configuration file.
`-i` or `--interactive`	Optional	Opens the configuration template in a text editor so that you can enter the required information interactively. After entering the information, save and quit the text editor to run the command.
`-o` or `--out`	Optional	Runs the command without prompting for confirmation.
`-v` or `--verbose`	Optional	Displays output in verbose mode.

To display the parameters for the command, run `viocli create -h` or `viocli create --help`. You can also use the `-h` or `--help` option to display parameters for any action. For example, `viocli create backup -h` shows parameters for the `backup` action.

Use `viocli create` to perform the following actions.

`viocli create backup {-f config-file | -i | -o} --content-vcenter <vcenter-name> [-t timeout] [-v]`

Creates a backup of your OpenStack deployment. The following additional parameters apply to the `backup` action.

Parameter	Mandatory or Optional	Description
`-t` *timeout* or `--timeout` *timeout*	Optional	Specifies the time in seconds for which `viocli` will display the progress of the backup operation. If you do not include this parameter, the default value of 1800 seconds will be used.

For more information, see Back Up Your Deployment.

`viocli create backupschedule {-f config-file | -i | -o} --content-vcenter <vcenter-name> [-t timeout] [-v]`

Creates a scheduled backup of your OpenStack deployment. For more information, see Scheduled Backup.

viocli create csr -c *country-code* -t *state-name* -l *city-name* -o *org-name* -u *org-unit* [-s *service-name*] [-d *output-dir*] [-f *config-file* | -i | -o] [-v]

Creates a certificate signing request to send to a certificate authority. The following additional parameters apply to the `csr` action.

Parameter	Mandatory or Optional	Description
`-c` *country-code* or `--countries` *country-code*	Mandatory	Two-letter ISO country code in which the organization applying for the certificate is located.
`-t` *state-name* or `--states` *state-name*	Mandatory	Full name of the state or province.
`-l` *city-name* or `--localities` *city-name*	Mandatory	Name of the town or city.
`-n` *org-name* or `--org-names` *org-name*	Mandatory	Legal name of the organization.
`-u` *org-unit* or `--org-units` *org-unit*	Mandatory	Name of the department or organizational unit.
`-s` *service-name* or `--services` *service-name*	Optional	Name of one or more VMware Integrated OpenStack services for which to generate the CSR. Separate multiple names with commas (,). If you do not include this parameter, a CSR is generated for every VMware Integrated OpenStack service.
`-d` *output-dir* or `--output` *output-dir*	Optional	Directory to which CSRs are saved. If you do not include this parameter, CSRs are saved to the `./csr` directory.

viocli create swift {-f *config-file* | -i | -o} [-v]

Creates a Swift cluster. For more information, see "Add the Swift Component" in the *VMware Integrated OpenStack Installation and Configuration Guide*.

viocli create tenant-vdc --compute *compute-node* --name *vdc-name* --project-id *project-uuid* [--cpu-reserve *cpu-min*] [--cpu-limit *cpu-max*] [--mem-reserve *memory-min*] [--mem-limit *memory-max*] [-f *config-file* | -i | -o] [-v]

Creates a tenant virtual data center (VDC) with the specified settings. The following additional parameters apply to the `tenant-vdc` action.

Parameter	Mandatory or Optional	Description
`--compute` *compute-node*	Mandatory	Compute node on which to create the tenant VDC. You can find the names of compute nodes by running the `openstack compute service list` command.
`--name` *vdc-name*	Mandatory	Name of the tenant VDC.
`--project-id` *project-uuid*	Mandatory	UUID of the project under which to create the tenant VDC.
`--cpu-reserve` *cpu-min*	Optional	CPU cycles in megahertz to reserve for the VDC. If you do not enter a value, `0` is used by default.
`--cpu-limit` *cpu-max*	Optional	Maximum limit for CPU usage on the VDC (in megahertz). If you do not enter a value, CPU usage is not limited.
`--mem-reserve` *memory-min*	Optional	Memory in megabytes to reserve for the VDC. If you do not enter a value, `0` is used by default.
`--mem-limit` *memory-max*	Optional	Maximum limit for memory consumption on the VDC (in megabytes). If you do not enter a value, memory consumption is not limited.

viocli create vcenter --vc_hostname <*hostname*> --vc_password <*password*> --vc_username <*username*>

Creates a new vCenter for backup, restoration, or other requests. The following additional parameters apply to the `vcenter` action.

Parameter	Mandatory or Optional	Description
`-n` *hostname* or `--vc_hostname` *hostname*	Mandatory	vCenter hostname or IP address of new object.
`-p` *password* or `--vc_password` *password*	Mandatory	vCenter password required to create the new object.
`-u` *username* or `--vc_username` *username*	Mandatory	vCenter username required to create the new object.

viocli delete Command

Use the `viocli delete` command to remove resources from your VMware Integrated OpenStack deployment.

The `viocli delete` command supports a variety of actions to perform different tasks. The following parameters apply to all actions.

Parameter	Mandatory or Optional	Description
`--force`	Optional	Runs the command without confirmation.
`-v` or `--verbose`	Optional	Displays output in verbose mode.

You can run `viocli delete -h` or `viocli delete --help` to display the parameters for the command. You can also use the `-h` or `--help` option on any action to display parameters for the action. For example, `viocli delete tenant-vdc -h` will show parameters for the `tenant` action.

The actions that `viocli delete` supports are listed as follows.

`viocli delete orphaned-instances [--no-grace-period] [--force] [-v]`

Deletes orphaned OpenStack instances.

Parameter	Mandatory or Optional	Description
`--no-grace-period`	Optional	Ignores the grace period when determining whether objects are orphaned. Objects modified in the past 30 minutes are included in the results only when this parameter is set.

`viocli delete orphaned-managed-vms [--no-grace-period] [--force] [-v]`

Deletes orphaned virtual machines that are managed by OpenStack.

Parameter	Mandatory or Optional	Description
`--no-grace-period`	Optional	Ignores the grace period when determining whether objects are orphaned. Objects modified in the past 30 minutes are included in the results only when this parameter is set.

`viocli delete orphaned-shadow-vms [--no-grace-period] [--force] [-v]`

Deletes orphaned shadow virtual machines.

Parameter	Mandatory or Optional	Description
`--no-grace-period`	Optional	Ignores the grace period when determining whether objects are orphaned. Objects modified in the past 30 minutes are included in the results only when this parameter is set.

`viocli delete swift [--force] [-v]`

Deletes the Swift cluster.

`viocli delete tenant-vdc` *`tvdc-id`* `[--compute` *`compute-node`*`] [--force] [-v]`

Deletes orphaned shadow virtual machines.

Parameter	Mandatory or Optional	Description
tvdc-id	Mandatory	ID of the tenant VDC to delete.
`--compute` *compute-node*	Optional	Compute node from which to delete the tenant VDC. If you do not include this parameter, the tenant VDC is deleted from all compute nodes.

viocli generate Command

Use the `viocli generate` command to generate a support bundle for your VMware Integrated OpenStack deployment.

The `viocli generate` command uses the following syntax.

```
viocli generate supportbundle [--path file-path] [--recent={true | false] [-u] [-v]
```

Parameter	Mandatory or Optional	Description
`--path` *file-path*	Optional	Directory to which the support bundle is saved. If you do not include this parameter, the support bundle is saved to the `/var/log` directory.
`--recent={true | false}`	Optional	If **`true`**, creates VIO logs for the past 24 hours. Default value is **`false`**.
`-u` or `--uncompressed`	Optional	Saves the support bundle as uncompressed files. If you do not include this parameter, the support bundle is saved as a compressed TAR archive.
`-v` or `--verbose`	Optional	Displays output in verbose mode.

You can also run `viocli generate -h` or `viocli generate --help` to display the parameters for the command.

viocli get Command

Use the `viocli get` command to view the resources in your deployment.

The `viocli get` command supports various actions to perform different tasks. The following parameter applies to all actions.

Parameter	Mandatory or Optional	Description
`-v` or `--verbose`	Optional	Displays output in verbose mode.

To display the parameters for the command, run `viocli get -h` or `viocli get --help`. You can also use the `-h` or `--help` option to display parameters for any action. For example, `viocli get controllers -h` shows parameters for the `controller` action.

Use `viocli get` to perform the following actions.

`viocli get controllers [-v]`

Displays information about all controllers in your deployment. You can include the `-v` parameter to display the validation results of the control plane.

`viocli get deployment [-v]`

Displays detailed information about your deployment, including its overall status, the status of your log analytics integration (if configured), and the status of each node.

`viocli get drivers`

Displays driver types for OpenStack Cinder and OpenStack Neutron.

`viocli get resources`

Displays a list of all resource types in your deployment.

`viocli get <resource-type> <resource-name>`

Displays all resources of a certain type. When displaying resources of the `instances` type, the following additional parameters apply.

Parameter	Mandatory or Optional	Description
`--nova-state {ERROR | SHUTOFF}`	Optional	Displays OpenStack instances in the `ERROR` or `SHUTOFF` state only.
`--vc-state {poweredOn | poweredOff | suspended}`	Optional	Displays OpenStack instances in the specified state that are powered on, powered off, or suspended in vCenter Server.

`viocli get` *resource-typeresource-name*

Displays information about a specific resource. When displaying information about a specific resource, the following additional parameter applies.

Parameter	Mandatory or Optional	Description
`--history`	Optional	Displays the configuration changes for the specified resource.

viocli import Command

Use the `viocli import` command to import certificates into your deployment.

The `viocli import` command uses the following syntax.

```
viocli import certificate -d cert-dir [-v]
```

Parameter	Mandatory or Optional	Description
`-d` *cert-dir* or `--folder` *cert-dir*	Mandatory	Directory containing the certificates that you want to import.
`-v` or `--verbose`	Optional	Displays output in verbose mode.

You can also run `viocli import -h` or `viocli import --help` to display the parameters for the command.

viocli migrate Command

Use the `viocli volume-migrate` command to migrate resources in your deployment.

The following parameter applies to the `viocli volume-migrate` command.

Parameter	Mandatory or Optional	Description
`-v` or `--verbose`	Optional	Displays output in verbose mode.

You can run `viocli volume-migrate -h` or `viocli volume-migrate --help` to display the parameters for the command.

`viocli volume-migrate {--volume-ids` *`volume1-uuid...`* `| --source-dc` *`src-dc-name`* `--source-ds` *`src-ds-name`*`] `*`dest-dc-name dest-ds-name`* `[--ignore-storage-policy] [-v]`

Migrates unattached Cinder volumes to another datastore.

Parameter	Mandatory or Optional	Description
`--volume-ids`	Mandatory if `--source-dc` and `--source-ds` are not used.	UUID of the volume that you want to migrate. You can include multiple UUIDs separated by commas (,). If you want to migrate all volumes from a datastore, use the `--source-dc` and `--source-ds` parameters instead of this parameter.
`--source-dc` *src-dc-name*	Mandatory if `--volume-ids` is not used.	Name of the data center containing the volumes that you want to migrate. This parameter must be used together with the `--source-ds` parameter. If you want to migrate specified volumes only, do not include this parameter.
`--source-ds` *src-ds-name*	Mandatory if `--volume-ids` is not used.	Name of the datastore containing the volumes that you want to migrate. This parameter must be used together with the `--source-dc` parameter. If you want to migrate specified volumes only, do not include this parameter.
dest-dc-name	Mandatory	Name of the data center that contains the datastore to which you want to migrate volumes.
dest-ds-name	Mandatory	Name of the datastore to which you want to migrate volumes.
`--ignore-storage-policy`	Optional	Migrates volumes to the target datastore even if the datastore does not comply with the storage policy of the volume.

viocli patch Command

Use the `viocli patch` command to manage patches in your VMware Integrated OpenStack deployment.

The `viocli patch` command supports a variety of actions to perform different tasks. The following parameters apply to all actions.

Parameter	Mandatory or Optional	Description
`-v` or `--verbose`	Optional	Displays output in verbose mode.

To display the parameters for the command, run `viocli patch -h` or `viocli patch --help`.

Use `viocli patch` to perform the following actions.

`viocli patch list`

Displays detailed information about all VMware Integrated OpenStack patches, including overall status.

`viocli patch add -l | –location <patch-path>`

Adds a patch to your deployment. Copies new Helm charts and Docker images into the target location `/opt/vmware/data` on the manager node.

`viocli patch install -p | –patch <patch-name>`

Installs a VMware Integrated OpenStack patch. Applies the patch custom resource and executes run.sh to restart the Helm repository and Docker registry pods.

`viocli patch delete -p | –patch <patch-name>`

Removes a patch cleanly.

viocli prepare Command

Use the `viocli prepare` command to prepare datastores for migration.

Note This command does not support multi-attach volumes.

The `viocli prepare` command uses the following syntax.

```
viocli prepare datastore dc-name ds-name [-v]
```

Parameter	Mandatory or Optional	Description
dc-name	Mandatory	Name of the data center containing the desired volumes.
ds-name	Mandatory	Name of the datastore containing the desired volumes.
`-v` or `--verbose`	Optional	Displays output in verbose mode.

You can also run `viocli prepare -h` or `viocli prepare --help` to display the parameters for the command.

viocli reset Command

Use the `viocli reset` command to reset passwords or instances in your deployment.

The `viocli reset` command uses the following syntax to reset VMware Integrated OpenStack UI and API admin passwords.

```
viocli reset password [--force] [-v]
```

The `viocli reset` command uses the following syntax to reset instances.

```
viocli reset instances --nova-state {ERROR | SHUTOFF} [--force] [-v]
```

Parameter	Mandatory or Optional	Description
`--nova-state {ERROR | SHUTOFF}`	Mandatory	Resets OpenStack instances in the `ERROR` or `SHUTOFF` state.
`--force`	Optional	Runs the command without confirmation.
`-v` or `--verbose`	Optional	Displays output in verbose mode.

You can also run `viocli reset -h` or `viocli reset --help` to display the parameters for the command.

viocli restore Command

Use the `viocli restore` command to restore a deployment from a backup file previously created by using the `viocli create backup` command.

For more information, see Restore Deployment.

The `viocli restore` command uses the following syntax.

```
viocli restore deployment {-f config-file | -i | -o} [--skip-control-plane] [-t timeout] [-v]
```

Parameter	Mandatory or Optional	Description
`-f` *config-file* or `--file` *config-file*	Optional	Runs the command using a specified configuration file.
`-i` or `--interactive`	Optional	Opens the configuration template in a text editor so that you can enter the required information interactively. After entering the information, save and quit the text editor to run the command.
`-o` or `--out`	Optional	Runs the command without prompting for confirmation.

Parameter	Mandatory or Optional	Description
`--skip-control-plane`	Optional	Restores the OpenStack deployment only and does not alter the current control plane configuration.
`-t` *timeout* or `--timeout` *timeout*	Optional	Specifies the time in seconds for which `viocli` will display the progress of the restore operation. If you do not include this parameter, the default value of 1800 seconds will be used.
`-v` or `--verbose`	Optional	Displays output in verbose mode.

You can also run `viocli restore -h` or `viocli restore --help` to display the parameters for the command.

viocli start Command

Use the `viocli start` command to start services in your deployment.

The `viocli start` command supports various actions to perform different tasks. The following parameters apply to all actions.

Parameter	Mandatory or Optional	Description
`-t` *timeout* or `--timeout` *timeout*	Optional	Specifies the time in seconds for which `viocli` will display the progress of the start operation. If you do not include this parameter, the default value of 900 seconds will be used.
`-v` or `--verbose`	Optional	Displays output in verbose mode.

To display the parameters for the command, run `viocli start -h` or `viocli start --help`.

Use `viocli start` to perform the following actions.

`viocli start services [-t timeout] [-v]`

Starts services in your VMware Integrated OpenStack deployment.

`viocli start service <service-name> <instance-name> [-t timeout]`

Starts an individual service with a specific name.

viocli stop Command

Use the `viocli stop` command to stop services in your deployment.

The `viocli stop` command supports various actions to perform different tasks. The following parameters apply to all actions.

Parameter	Mandatory or Optional	Description
`-t` *timeout* or `--timeout` *timeout*	Optional	Specifies the time in seconds for which `viocli` will display the progress of the stop operation. If you do not include this parameter, the default value of 900 seconds will be used.
`-v` or `--verbose`	Optional	Displays output in verbose mode.

To display the parameters for the command, run `viocli stop -h` or `viocli stop --help`.

Use `viocli stop` to perform the following actions.

`viocli stop services [-t timeout] [-v]`

Stops all services in your VMware Integrated OpenStack deployment.

`viocli stop service <service-name> <instance-name> [-t timeout]`

Stops an individual service with a specific name.

viocli update Command

Use the `viocli update` command to update the configuration of resources in your deployment. The configuration is loaded in the default text editor for you to modify.

The `viocli update` command uses the following syntax.

```
viocli update resource-type [resource-name] [--live-debug={true | false}] [--force] [-v]
```

Parameter	Mandatory or Optional	Description
resource-type	Mandatory	Type of resource that you want to update. The following values are accepted: ■ `aodh` ■ `barbican` ■ `ceilometer` ■ `ceilometeragent` ■ `cinder` ■ `deployment` ■ `designate` ■ `glance` ■ `gnocchi` ■ `heat` ■ `horizon` ■ `keystone` ■ `mariadb` ■ `memcached` ■ `neutron` ■ `nova` ■ `novacompute` ■ `panko` ■ `rabbitmq` ■ `swift` ■ `tenant-vdc`
resource-name	Optional	Name of the resource that you want to update. If only one instance of the desired resource is running, this parameter is not required.
`--live-debug={true | false}`	Optional	Used mostly by R&D during development to enable live debug mode on the specified resource. To allow for debugging, starts the resource pod with "sleep infinity" rather than starting the core process. **Note** Live debug causes a control plane outage of the services being debugged. To return to normal operations, use viocli to disable live debug and wait for the pods to restart. Customers are advised to use this feature only under the direction of VMware technical services.
`--force`	Optional	Runs the command without confirmation.
`-v` or `--verbose`	Optional	Displays output in verbose mode.

The following additional parameter applies to the `deployment` resource.

Parameter	Mandatory or Optional	Description
`--enable-ha`	Mandatory	Enables high availability (HA) mode on your deployment.

The following additional parameters apply to the `tenant-vdc` resource.

Parameter	Mandatory or Optional	Description
`--compute` *compute-node*	Mandatory	Compute node that contains the tenant VDC.
`--id` *vdc-id*	Mandatory	Identifier of the tenant VDC.
`--cpu-reserve` *cpu-min*	Optional	CPU cycles in megahertz to reserve for the VDC. If you do not enter a value, `0` is used by default.
`--cpu-limit` *cpu-max*	Optional	Maximum limit for CPU usage on the VDC (in megahertz). If you do not enter a value, CPU usage is not limited.
`--mem-reserve` *memory-min*	Optional	Memory in megabytes to reserve for the VDC. If you do not enter a value, `0` is used by default.
`--mem-limit` *memory-max*	Optional	Maximum limit for memory consumption on the VDC (in megabytes). If you do not enter a value, memory consumption is not limited.

You can also run `viocli update -h` or `viocli update --help` to display the parameters for the command.

viocli version Command

Use the `viocli version` command to display the current version of VMware Integrated OpenStack.

The `viocli version` command uses the following syntax.

```
viocli version [-v]
```

Parameter	Mandatory or Optional	Description
`-v` or `--verbose`	Optional	Displays output in verbose mode.

You can also run `viocli version -h` or `viocli version --help` to display the parameters for the command.

Troubleshooting

14

If errors occur, you can perform troubleshooting actions to restore your OpenStack deployment to operating status.

This chapter includes the following topics:

Create a Support Bundle

You can generate a support bundle that includes logs from your VMware Integrated OpenStack deployment for assisting you in troubleshooting.

Procedure

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Generate a support bundle.

```
viocli generate supportbundle
```

Results

The log files are collected into a support bundle. You can use this for troubleshooting or provide it to technical support staff when requesting assistance.

Auto-Generated Log Backups

Starting from VMware Integrated OpenStack 7.1, VMware Integrated OpenStack logs are automatically backed up on a daily basis to increase log retention for a maximum of seven days. The retention days can vary according to free space on the vio-manager virtual machine. The log backups are stored in `/var/log/vio_daily_log` on the vio-manager virtual machine. For troubleshooting purposes, you can upload the auto-generated log backups present in that folder.

VMware Integrated OpenStack Virtual Appliance Fails to Deploy

When you install the VMware Integrated OpenStack OVA, you receive the error message `The operation is not supported on the object.`

Cause

This error occurs when DRS is disabled on the management cluster where you are installing the VMware Integrated OpenStack OVA.

Solution

1. In the vSphere Client, select the management cluster.
2. On the **Configure** tab, select **Services > vSphere DRS**.
3. Click **Edit** and enable **vSphere DRS**.

Synchronize OpenStack Instance State

You can reset OpenStack instances in the `ERROR` or `SHUTOFF` state that are powered on in vCenter Server.

Problem

An OpenStack instance may remain in the `ERROR` or `SHUTOFF` state even after the virtual machine corresponding to the instance is powered on in vCenter Server.

Solution

1. Log in to the Integrated OpenStack Manager as the `root` user.

   ```
   ssh root@mgmt-server-ip
   ```

2. Display OpenStack instances in the `ERROR` or `SHUTOFF` state that are listed as powered on in vCenter Server.

   ```
   viocli get instances --nova-state {ERROR | SHUTOFF} --vc-state poweredOn
   ```

3. Reset powered-on instances in the `ERROR` or `SHUTOFF` state.

   ```
   viocli reset instances --nova-state {ERROR | SHUTOFF}
   ```

Project Instance Table Is Slow to Display

In large-scale environments, the VMware Integrated OpenStack dashboard might be slow to display the instance table for an OpenStack project.

Problem

When you log in to the VMware Integrated OpenStack dashboard and select **Project > Compute > Instances**, the dashboard takes longer than expected to display the list of instances.

To address this issue, you can configure the dashboard to obtain instance IP address information from Nova instead of Neutron. This improves the performance of the instance page, but IP address information on that page may not be displayed immediately.

Solution

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Modify the Horizon configuration.

```
viocli update horizon
```

3 In the `config` section, add the `horizon_instance_retrieve_ip_address` parameter and set its value to `false`.

The configuration file now looks similar to the following.

```
conf:
  horizon:
    local_settings:
      config:
        horizon_instance_retrieve_ip_address: false
        openstack_neutron_network:
          neutron_backend: network-mode
```

User Deletion Intermittently Fails

In high-concurrency scenarios, deleting OpenStack users may intermittently fail.

Problem

When you attempt to delete an OpenStack user, an error message appears:

```
Failed to consume a task from the queue: Gateway Timeout (HTTP 504): GatewayTimeout: Gateway
Timeout (HTTP 504)
```

To resolve this problem, modify the lock wait timeout of the database.

Solution

1 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

2 Modify the MariaDB configuration.

```
viocli update mariadb
```

3 In the `conf` section, add the `innodb_lock_wait_timeout` parameter and set its value to `1000`.

The configuration file includes:

```
conf:
  innodb_lock_wait_timeout: 1000
```

Cinder Backup Fails Under High Concurrency

The default VMware Integrated OpenStack configuration may be insufficient for Cinder backup operations with high concurrency or large volumes.

Problem

When you increase the concurrency of Cinder backup operations or the size of Cinder volumes, operations may fail and `GetResourceFailure` errors may be displayed in the logs.

Solution

1 Scale out the control plane and number of Cinder backup pods.

Each controller node can contain only one Cinder backup pod.

a Increase the number of controller nodes in your deployment.

See Add Controller Nodes to Your Deployment.

b Increase the number of Cinder backup pods in your deployment.

See Scale OpenStack Services.

2 Log in to the Integrated OpenStack Manager as the `root` user.

```
ssh root@mgmt-server-ip
```

3 Update the RPC response timeout and executor thread pool size for Cinder.

a Modify the Cinder configuration.

```
viocli update cinder
```

b In the `DEFAULT` section, add the `rpc_response_timeout` parameter and set its value to `6000`.

c Add the `executor_thread_pool_size` parameter and set its value to `640`.

The configuration file now looks similar to the following.

```
conf:
  backends:
    [...]
  cinder:
    DEFAULT:
      [...]
      rpc_response_timeout: 6000
      executor_thread_pool_size: 640
```

4 Update the database timeout and maximum connection parameters.

a Modify the MariaDB configuration.

```
viocli update mariadb
```

b In the `conf` section, add the `connect_timeout` parameter and set its value to `5`.

c Add the `max_connections` parameter and set its value to `5000`.

d Add the `net_read_timeout` parameter and set its value to `1200`.

e Add the `net_write_timeout` parameter and set its value to `1200`.

f In the `conf` section, add the `ingress` section.

g In the `ingress` section, add the `proxy-read-timeout` parameter and set its value to `1200`.

h Add the `proxy-send-timeout` parameter and set its value to `1200`.

i Add the `proxy-stream-timeout` parameter and set its value to `3600s`.

The configuration file now looks similar to the following.

```
conf:
  connect_timeout: 5
  max_connections: 5000
  net_read_timeout: 1200
  net_write_timeout: 1200
  ingress:
    proxy-read-timeout: "1200"
    proxy-send-timeout: "1200"
    proxy-stream-timeout: 3600s
```

5 Update the pool sizes and allocation ratios for Nova.

a Modify the Nova configuration.

```
viocli update nova
```

b In the `nova` section, add the `DEFAULT` section.

c In the `DEFAULT` section, add the `cpu_allocation_ratio` parameter and set its value to `30`.

d Add the `executor_thread_pool_size` parameter and set its value to `640`.

e Add the `ram_allocation_ratio` parameter and set its value to `6`.

f In the `nova` section, add the `database` section.

g In the `database` section, add the `max_pool_size` parameter and set its value to `50`.

The configuration file now looks similar to the following.

```
conf:
  nova:
    DEFAULT:
      cpu_allocation_ratio: 30
      executor_thread_pool_size: 640
      ram_allocation_ratio: 6
    database:
      max_pool_size: 50
```

6 Update the token expiration and Web Server Gateway Interface (WSGI) parameters for Keystone.

a Modify the Keystone configuration.

```
viocli update keystone
```

b In the `conf` section, add the `keystone` section.

c In the `keystone` section, add the `wsgi_processes` parameter and set its value to `8`.

d Add the `wsgi_threads` parameter and set its value to `15`.

e In the `keystone` section, add the `token` section.

f In the `token` section, add the `expiration` parameter and set its value to `28800`.

The configuration file now looks similar to the following.

```
conf:
  keystone:
    wsgi_processes: 8
    wsgi_threads: 15
      token:
        expiration: 28800
```