You can find the most up-to-date technical documentation on the VMware Web site at:
http://www.vmware.com/support/
The VMware Web site also provides the latest product updates.
If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com
Index  67
About This Guide

*VMware Integrated OpenStack Installation and Configuration Guide* explains the process of deploying a working instance of standard OpenStack in your vCenter environment.

*VMware Integrated OpenStack Installation and Configuration Guide* also describes the prerequisites for preparing a dedicated vCenter instance, deploying the VMware Integrated OpenStack plug-in, and installing and configuring your VMware Integrated OpenStack cloud management infrastructure.

**Intended Audience**

This guide is for system administrators and developers who want to integrate their VMware® vSphere® deployment with OpenStack services by installing VMware Integrated OpenStack. To do so successfully, you should be familiar with VMware® vSphere® and the OpenStack components and functions. If you are deploying VMware Integrated OpenStack with VMware NSX for vSphere (NSX), you should be familiar with NSX administration. See the VMware technical documentation at https://www.vmware.com/support/pubs/nsx_pubs.html.

**VMware Technical Publications Glossary**

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.
Updated Information

This VMware Integrated OpenStack Installation and Configuration Guide is updated with each release of the product or when necessary.

This table provides the update history of the VMware Integrated OpenStack Installation and Configuration Guide.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1880-03  | - Updated for VMware Integrated OpenStack version 3.0 or 3.1.  
           - Updated for the Mitaka release of OpenStack.  
           - Updated installation procedures to reflect changes to the installer, including compact mode and multiple domain support. See Chapter 6, “Installing VMware Integrated OpenStack,” on page 35.  
           - Updated the software and hardware requirements to reflect new compact mode deployment. See “Hardware Requirements for Compact Mode Deployments,” on page 27.  
           - Added new procedures to prepare for compact mode deployment. See “Prepare the vCenter Instance for Compact Mode Deployment,” on page 29.  
           - Multiple minor revisions and updates as necessary. |
| 1880-02  | - Updated installation procedures to reflect changes to the installer. See Chapter 6, “Installing VMware Integrated OpenStack,” on page 35.  
           - Updated the post-installation configuration to show support for LBaaS v2.0. See “Configuring and Enabling LBaaS Using the CLI,” on page 49.  
           - Updated the software and hardware requirements to reflect streamlined architecture. See “VMware Integrated OpenStack System Requirements,” on page 16.  
           - Updated network and architecture diagrams to reflect changes.  
           - Add procedure for adding storage capacity to the Compute node. See “Add Storage to the Compute Node,” on page 64.  
           - Add procedure for adding storage capacity to the Image Service node. See “Add Storage to the Image Service,” on page 64.  
           - Added requirements for Python client and NSX licensing. See “Software Requirements for NSX Deployments,” on page 17. |
| 1880-01  | - Updated the software requirements for NSX deployments to include a link to the VMware Product Interoperability Matrix and with additional supported versions of vSphere and ESXi hosts. See “Software Requirements for NSX Deployments,” on page 17.  
           - Updated the software requirements for VDS deployments with additional supported versions of vSphere and ESXi hosts. See “Software Requirements for VDS Deployments,” on page 25.  
           - Expanded the VDS configuration options for NSX deployments. See “Prepare the vCenter Instance for NSX-Based Deployment,” on page 31.  
           - Corrected inaccurate link to the plugin registration page. See “Register the Integrated OpenStack Manager vApp,” on page 36. |
| 1880-00  | Initial release. |
About VMware Integrated OpenStack

With VMware Integrated OpenStack, you can implement OpenStack services on your existing VMware vSphere implementation.

You deploy VMware Integrated OpenStack through the Integrated OpenStack Manager vApp in vCenter. The Integrated OpenStack Manager provides a workflow that guides you through and completes the VMware Integrated OpenStack deployment process. With Integrated OpenStack Manager, you can specify your management and compute clusters, configure networking, and add resources. Post-deployment, you can use Integrated OpenStack Manager to add components or otherwise modify the configuration of your VMware Integrated OpenStack cloud infrastructure.

VMware Integrated OpenStack 3.x is based on the Mitaka release of OpenStack.

This chapter includes the following topics:

- “Internationalization,” on page 9
- “OpenStack Foundation Compliance,” on page 9
- “VMware Integrated OpenStack Architecture,” on page 10
- “Unicode UTF-8 and Special Character Support,” on page 10
- “NSX and VDS Feature Comparison,” on page 11
- “Customer Experience Improvement Program,” on page 11

Internationalization

VMware Integrated OpenStack 2.0 and greater is available in English and seven additional languages: Simplified Chinese, Traditional Chinese, Japanese, Korean, French, German, and Spanish.

ASCII characters must be used for all input and naming conventions of OpenStack resources (such as project names, usernames, image names, and so on) and for the underlying infrastructure components (such as ESXi hostnames, vSwitch port group names, data center names, datastore names, and so on).

OpenStack Foundation Compliance

Every new version of VMware Integrated OpenStack complies with the latest Guidelines created by the OpenStack Foundation DefCore Committee.

VMware Integrated OpenStack is designated as an OpenStack Powered Platform™ product and therefore provides proven interoperability with all other OpenStack Powered™ products.

For detailed information about the compatibility of VMware Integrated OpenStack with the OpenStack Powered Platform™, go to http://www.openstack.org/marketplace/distros/distribution/vmware/vmware-integrated-openstack.
VMware Integrated OpenStack Architecture

The VMware Integrated OpenStack architecture connects vSphere resources to the OpenStack Compute, Networking, Block Storage, Image Service, Identity Service, and Orchestration components.

VMware Integrated OpenStack is implemented as compute and management clusters in your vSphere environment.

The compute cluster handles all tenant workloads. Your VMware Integrated OpenStack deployment can have multiple compute clusters. Integrated OpenStack Manager creates one Compute driver instance in the management cluster for each compute cluster.

The management cluster contains the VMs that comprise your OpenStack cloud deployment. It also contains the load balancing, DHCP, and database services.

VMware Integrated OpenStack deployments can use NSX for the Networking component. You will require an additional cluster for the NSX Edge nodes.

Figure 1-1. VMware Integrated OpenStack with NSX in the SDDC context

Unicode UTF-8 and Special Character Support

VMware Integrated OpenStack supports internationalization (I18N) level 3. However, there are resources you specify that do not provide UTF-8 support. You can use only ASCII attribute names consisting of alphanumeric characters and underscores (_) for these resources.

VMware Integrated OpenStack Supports Unicode UTF-8

vCenter Server resources you specify using both the CLI and vSphere Web Client can be expressed with underscore (_), hyphen (-), blank spaces, and all letters and numbers from any language. For example, you can specify resources such as datastores labeled using non-English characters.

When using a Linux operating system, you should configure the system for use with UTF-8 encoding specific to your locale. For example, to use U.S. English, specify the following locale encoding: en_US.UTF-8. See your vendor’s documentation for information on configuring UTF-8 encoding for your Linux environment.
Resources Excluded From Unicode UTF-8 Support

The following resource names are excluded from UTF-8 support:

- VMware Integrated OpenStack manager name
- datacenter names
- cluster names
- networking port group names (both Standard vSwitch and VDS)
- NSX Transport Zone name
- datastore names (both local and shared NFS)

NSX and VDS Feature Comparison

You can deploy VMware Integrated OpenStack with either VDS- or NSX-based networking. The following table shows the differences between the two modalities.

<table>
<thead>
<tr>
<th>Supported Feature</th>
<th>VDS Mode</th>
<th>NSX Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider Networks leveraging VLANs</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>API/Management Plane High Availability</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DC-Wide Control Plane Scale</td>
<td>Limited</td>
<td>High</td>
</tr>
<tr>
<td>Layer 3/NAT High Availability &amp; Scale</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Neutron feature set:

- Private Logical Network Identifier Independent of VLANs
- Highly Available DHCP Service
- Security Groups
- Metadata Service Integration & Support
- L3 (centralized, distributed)
- NAT & Floating IP Support

<table>
<thead>
<tr>
<th>Enterprise Features</th>
<th>No</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Micro-segmentation with line-rate Stateful distributed firewall</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Provider-side security via Service Insertion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>In-kernel distributed routing</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

vRealize Operations & Log Insight Content Packs

| vRealize Operations & Log Insight Content Packs        | No       | Yes      |

Customer Experience Improvement Program

You can configure this product to collect data that can be used by the VMware Customer Experience Improvement Program.

This product participates in VMware’s Customer Experience Improvement Program (“CEIP”). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at [http://www.vmware.com/trustvmware/ceip.html](http://www.vmware.com/trustvmware/ceip.html)

To join or leave the CEIP for this product, please go to the Customer Experience Improvement Program page in the User Interface to change your participation in CEIP:

- During product deployment using the Integrated OpenStack Manager, participation in the CEIP is enabled by default, unless you choose not to participate.
After initial deployment, go to the Customer Experience Improvement Program page to modify your participation, if required.

- To join the CEIP, go to Home > Inventories, and click the VMware Integrated OpenStack icon. Then click the Manage tab and click the Settings tab. Finally click Enable to join.

- To leave the CEIP, go to Home > Inventories, and click the VMware Integrated OpenStack icon. Then click the Manage tab and click the Settings tab. Finally click Disable to leave the program.
You can deploy VMware Integrated OpenStack using NSX for the Neutron networking component.

This chapter includes the following topics:

- “Architectural Overview of NSX Deployments,” on page 13
- “VMware Integrated OpenStack System Requirements,” on page 16
- “Physical NSX Network,” on page 18

Architectural Overview of NSX Deployments

An VMware Integrated OpenStack NSX deployment includes management and compute clusters with four principal networks. You can also separate the NSX Edge node into a separate cluster.

Cluster and Component Architecture

When you deploy VMware Integrated OpenStack using NSX, you can use two different deployment modes:

- **Compact Mode** - Consists of a single ESXi host running two VMs and using a minimum of 120 GB of storage.

- **HA Mode** - Consists of 8 or more VMs using a minimum of 552 GB of storage.

A typical NSX deployment architecture in HA mode consists of three clusters and four VLANs. For details about the VLANs, see “Physical NSX Network,” on page 18.
The VMware Integrated OpenStack architecture includes the following clusters and components.

<table>
<thead>
<tr>
<th>Cluster or Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter instance</td>
<td>A dedicated vCenter instance is not required but optimizes deployment.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>For user authentication by the OpenStack Identity Service.</td>
</tr>
<tr>
<td>Management cluster</td>
<td>Contains all the deployed OpenStack component and management VMs. See “Management Cluster,” on page 22 below for a detailed description of the management cluster and its components.</td>
</tr>
<tr>
<td>Compute cluster</td>
<td>Compute resources for Nova. All tenant VMs are created on these compute clusters.</td>
</tr>
<tr>
<td>NSX Edge cluster</td>
<td>Contains Edge VMs that provide edge security and gateway services to logical networks, and provide DHCP, Floating IP (NAT), Security Groups and routing functions for the OpenStack Networking component.</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>The centralized network management component of NSX that provides an aggregated system view.</td>
</tr>
<tr>
<td>NSX Controllers</td>
<td>An advanced distributed state management system that controls virtual networks and overlay transport tunnels.</td>
</tr>
<tr>
<td>Management network</td>
<td>Carries traffic among the management components.</td>
</tr>
<tr>
<td>API access network</td>
<td>Exposes the VMware Integrated OpenStack dashboard and provides access for tenants to the OpenStack APIs and services.</td>
</tr>
<tr>
<td>Transport network</td>
<td>Connects the DHCP nodes in the Edge cluster with the compute clusters.</td>
</tr>
<tr>
<td>External Network</td>
<td>Provides external access for the instances created in VMware Integrated OpenStack.</td>
</tr>
</tbody>
</table>

The NSX Controller and NSX Manager nodes can be deployed on separate clusters or hosts. It is a best practice to deploy the NSX Controller and NSX Manager nodes in the Management Cluster.
**Management Cluster**

The Management Cluster contains all the deployed OpenStack component and management VMs.

*Figure 2-2. Management cluster in HA mode*

![Management Cluster Diagram](image)

*Figure 2-3. Management cluster in compact mode (to be provided)*

The management cluster contains the following components.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Balancers</td>
<td>Provide HA and enable horizontal scale-out architecture.</td>
<td>2 (1 active, 1 standby)</td>
</tr>
<tr>
<td>Databases (DBs)</td>
<td>Instances of MariaDB that store the OpenStack metadata. RabbitMQ, the message queue service used by all OpenStack services, also runs on the database nodes.</td>
<td>3 (1 active, 2 standby)</td>
</tr>
<tr>
<td>VMware Integrated OpenStack Controller</td>
<td>Contains all the OpenStack services, including Compute, Block Storage, Image Service, Identity Service, and Object Storage. The memcache service, which enables production-grade performance for the Identity Service, also runs on the controller nodes.</td>
<td>2 (both active)</td>
</tr>
<tr>
<td>Compute Driver</td>
<td>Contains a subset of Compute processes that interact with the compute clusters to manage VMs.</td>
<td>1 per compute cluster</td>
</tr>
<tr>
<td>VMware Integrated OpenStack Manager Service (OMS)</td>
<td>The vApp that you use to manage your VMware Integrated OpenStack vApp.</td>
<td>1</td>
</tr>
<tr>
<td>VMware Integrated OpenStack Template</td>
<td>Base template for creating all OpenStack service VMs.</td>
<td>1</td>
</tr>
<tr>
<td>Ceilometer Databases (optional)</td>
<td>Instances of MongoDB or NoSQL databases for use by Ceilometer.</td>
<td>3 (1 active, 2 standby)</td>
</tr>
</tbody>
</table>
VMware Integrated OpenStack System Requirements

Before you begin the VMware Integrated OpenStack deployment tasks, your system must comply with all hardware, software, networking, and storage requirements.

Hardware Requirements for NSX Deployments

The hardware requirements are based on the number of VMs used for each component. For example, two VMs are used for load balancing, each of which requires two vCPUs for a total requirement of four vCPUs.

Core VMware Integrated OpenStack Components

<table>
<thead>
<tr>
<th>Component</th>
<th>VMs</th>
<th>vCPU</th>
<th>vRAM (GB)</th>
<th>vDisk Space (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated OpenStack Manager</td>
<td>1</td>
<td>4 (4 per VM)</td>
<td>4 (4 per VM)</td>
<td>25</td>
</tr>
<tr>
<td>Load balancing service</td>
<td>2</td>
<td>4 (2 per VM)</td>
<td>8 (4 per VM)</td>
<td>40 (20 per VM)</td>
</tr>
<tr>
<td>Database service</td>
<td>3</td>
<td>12 (4 per VM)</td>
<td>48 (16 per VM)</td>
<td>240 (80 per VM)</td>
</tr>
<tr>
<td>Controllers</td>
<td>2</td>
<td>16 (8 per VM)</td>
<td>32 (16 per VM)</td>
<td>160 (80 per VM)</td>
</tr>
<tr>
<td>Compute service (Nova CPU)</td>
<td>1</td>
<td>2 (2 per VM)</td>
<td>4 (4 per VM)</td>
<td>20 (20 per VM)</td>
</tr>
<tr>
<td>Ceilometer</td>
<td>1</td>
<td>2 (2 per VM)</td>
<td>4 (4 per VM)</td>
<td>20 (20 per VM)</td>
</tr>
<tr>
<td>Database (MongoDB or NoSQL) for</td>
<td>3</td>
<td>6 (2 per VM)</td>
<td>12 (4 per VM)</td>
<td>60 (20 per VM)</td>
</tr>
<tr>
<td>Ceilometer (MongoDB or NoSQL) for Ceilometer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>46</td>
<td>112</td>
<td>565</td>
</tr>
</tbody>
</table>

Note: The optional Object Storage (Swift) is installed separately post-installation and is not included in the above requirements. See “Adding OpenStack Components and Features,” on page 54.

NSX Components

Additional CPU, RAM, and disk space is required for NSX components if they are deployed with VMware Integrated OpenStack. It is a best practice to deploy the NSX Manager and NSX Controller nodes in the Management cluster.

Table 2-1. NSX Components

<table>
<thead>
<tr>
<th>Component</th>
<th>VMs</th>
<th>vCPU</th>
<th>vRAM (GB)</th>
<th>vDisk Space (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Controller</td>
<td>3</td>
<td>12 (4 per VM)</td>
<td>12 (4 per VM)</td>
<td>60 (20 per VM)</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>1</td>
<td>4 (4 per VM)</td>
<td>12 (12 per VM)</td>
<td>60 (60 per VM)</td>
</tr>
<tr>
<td>NSX Edge (see note below)</td>
<td></td>
<td>1 per Edge DHCP VM,</td>
<td>0.5 per Edge DHCP VM,</td>
<td>0.5 per Edge DHCP VM,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 per Edge router VM</td>
<td>1 per Edge router VM</td>
<td>1 per Edge router VM</td>
</tr>
<tr>
<td>TOTAL</td>
<td>4 plus Edge requirements</td>
<td>16 plus Edge requirements</td>
<td>24 plus Edge requirements</td>
<td>120 plus Edge requirements</td>
</tr>
</tbody>
</table>

Note: When you create a logical subnet or logical router, a new Edge VM is dynamically created to serve this request if an existing Edge node cannot.
Software Requirements for NSX Deployments

Before you begin the VMware Integrated OpenStack deployment tasks, the software components must meet all of the version prerequisites for vSphere, ESXi hosts, and the NSX product. In a typical deployment, you require at least three ESXi hosts for the OpenStack management cluster and at least one ESXi host for the OpenStack compute cluster.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere version</td>
<td>Supported versions:</td>
</tr>
<tr>
<td></td>
<td>See the VMware Product Interoperability Matrix at</td>
</tr>
<tr>
<td></td>
<td><a href="http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php">http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php</a> for the</td>
</tr>
<tr>
<td></td>
<td>supported versions.</td>
</tr>
<tr>
<td>ESXi hosts</td>
<td>Supported versions:</td>
</tr>
<tr>
<td></td>
<td>See the VMware Product Interoperability Matrix at</td>
</tr>
<tr>
<td></td>
<td><a href="http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php">http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php</a> for the</td>
</tr>
<tr>
<td></td>
<td>supported versions.</td>
</tr>
<tr>
<td></td>
<td>Eight or more logical processors on each host.</td>
</tr>
<tr>
<td></td>
<td>The vCenter and all ESXi hosts intended for the VMware Integrated OpenStack</td>
</tr>
<tr>
<td></td>
<td>deployment must use the same Network Time Protocol (NTP) server. For details</td>
</tr>
<tr>
<td></td>
<td>about configuring NTP on ESXi servers, see the VMware knowledge base article</td>
</tr>
<tr>
<td></td>
<td>at <a href="http://kb.vmware.com/kb/1003063">http://kb.vmware.com/kb/1003063</a> and the vSphere documentation at</td>
</tr>
<tr>
<td></td>
<td>vcenterhost.doc%2FGUID-8756D419-A878-4AE0-9183-C6D5A91A8FB1.html.</td>
</tr>
<tr>
<td>NSX</td>
<td>NSX Advanced or Enterprise license.</td>
</tr>
<tr>
<td></td>
<td>See the VMware Product Interoperability Matrix at</td>
</tr>
<tr>
<td></td>
<td><a href="http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php">http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php</a> for the</td>
</tr>
<tr>
<td></td>
<td>preferred version.</td>
</tr>
<tr>
<td>OpenStack python-</td>
<td>OpenStack Mitaka version.</td>
</tr>
<tr>
<td>heatclient</td>
<td>See <a href="https://launchpad.net/python-heatclient/mitaka">https://launchpad.net/python-heatclient/mitaka</a>.</td>
</tr>
</tbody>
</table>

Required NSX Parameters

When you are deploying VMware Integrated OpenStack with NSX for the Networking component, you must configure the NSX nodes in advance.

When you install VMware Integrated OpenStack, you must provide the following information.

Starting with VMware Integrated OpenStack 3.1, if you use VMware NSX-T in your environment, you can use the native DHCP and metadata support. To be able to use these functionalities, you must create a DHCP profile and metadata proxy server for your NSX-T environment.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>User name for accessing the NSX Manager node.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for accessing the NSX Manager node.</td>
</tr>
<tr>
<td>Transport Zone</td>
<td>Name of the default transport zone.</td>
</tr>
<tr>
<td>Edge Cluster</td>
<td>The name of the cluster containing the Edge nodes.</td>
</tr>
<tr>
<td>Virtual Distributed Switch for</td>
<td>The VDS from the NSX configuration.</td>
</tr>
<tr>
<td>Edge VTEP</td>
<td></td>
</tr>
<tr>
<td>Port Group for External Network</td>
<td>The port group created on a VLAN specifically for the External network. You</td>
</tr>
<tr>
<td></td>
<td>created this port group as part of the process of preparing to deploy</td>
</tr>
<tr>
<td></td>
<td>VMware Integrated OpenStack with NSX.</td>
</tr>
<tr>
<td>(optional VMware NSX-T only)</td>
<td>To use native DHCP, configure a DHCP server profile for your NSX-T</td>
</tr>
<tr>
<td>DHCP profile</td>
<td>environment. For more information, see Create a DHCP Server Profile in the</td>
</tr>
<tr>
<td></td>
<td>NSX-T Administration Guide.</td>
</tr>
</tbody>
</table>
(optional VMware NSX-T only) Metadata proxy server

To use metadata support, configure a metadata proxy server for your NSX-T environment. For more information, see Add a Metadata Proxy Server in the NSX-T Administration Guide.

During the configuration, use the load balancer private IP of your OpenStack deployment for URL for the Nova server. For example: http://load_balancer_private_IP:8775/. Also keep the secret parameter, as you need it during the VMware Integrated OpenStack deployment.

### Physical NSX Network

For VMware Integrated OpenStack deployments based on NSX, the API access, Management, Transport, and External network each require a separate and dedicated VLAN.

Request that your network administrator prepare the necessary VLANs.

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Access network</td>
<td>Provides access for users to the OpenStack services through APIs or the VMware Integrated OpenStack dashboard.</td>
</tr>
<tr>
<td></td>
<td>■ Trunk all hosts in the Management cluster to this VLAN.</td>
</tr>
<tr>
<td></td>
<td>■ Make externally accessible.</td>
</tr>
<tr>
<td></td>
<td>■ Requires five or more continuous IP addresses.</td>
</tr>
<tr>
<td>External</td>
<td>Provides external user access to the instances.</td>
</tr>
<tr>
<td></td>
<td>■ Trunk all hosts in the NSX Edge cluster to this VLAN.</td>
</tr>
<tr>
<td>Management network</td>
<td>Carries traffic among the management components.</td>
</tr>
<tr>
<td></td>
<td>■ Trunk all hosts in the Management cluster to this VLAN.</td>
</tr>
<tr>
<td></td>
<td>■ Trunk all hosts in the Compute cluster to this VLAN.</td>
</tr>
<tr>
<td></td>
<td>■ Requires 18 or more continuous IP addresses. (21 if you add the Ceilometer component.)</td>
</tr>
<tr>
<td></td>
<td>■ Enable L2 or L3 access to this VLAN for the following components:</td>
</tr>
<tr>
<td></td>
<td>■ vCenter server</td>
</tr>
<tr>
<td></td>
<td>■ NSX Manager</td>
</tr>
<tr>
<td></td>
<td>■ NSX Controller</td>
</tr>
<tr>
<td></td>
<td>If you are deploying the NSX Manager and NSX Controller VMs on the Management cluster, you must trunk their hosts to the Management network.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Metadata-service</td>
<td>The metadata-service network enables new OpenStack instances to access and run customization</td>
</tr>
<tr>
<td></td>
<td>scripts made available by the Nova metadata service, which is hosted by the OpenStack controllers.</td>
</tr>
<tr>
<td>Transport</td>
<td>Carries traffic among the OpenStack instances.</td>
</tr>
<tr>
<td></td>
<td>▪ Trunk all hosts in the Compute cluster to this VLAN.</td>
</tr>
<tr>
<td></td>
<td>▪ Trunk all hosts in the NSX Edge cluster to this VLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>IMPORTANT</strong> The Maximum Transmission Unit (MTU) settings for the Transport VLAN must be</td>
</tr>
<tr>
<td></td>
<td>configured to support 1600 bytes. See the Knowledge Base at</td>
</tr>
</tbody>
</table>

**Figure 2-4.** Network Map for NSX Deployments
VMware Integrated OpenStack can use Virtual Distributed Switch (VDS) to provide basic L2 networking for tenant workloads.

In this model, the VMware Integrated OpenStack administrator creates a set of provider networks and shares them with tenants, who then connect their VMs to these networks.

This chapter includes the following topics:

- “Limitations of VDS Networking,” on page 21
- “Architectural Overview of VDS Deployments,” on page 21
- “VMware Integrated OpenStack System Requirements,” on page 24
- “Physical VDS Network Overview,” on page 25

**Limitations of VDS Networking**

VDS-based networking has limitations, including the inability of tenants to create their own private L2 networks, and the inability to deliver L3 and higher networking services such as virtual routers, security groups, and floating IPs.

If such features are important for your VMware Integrated OpenStack deployment, consider using NSX for Neutron networking.

**Architectural Overview of VDS Deployments**

A VMware Integrated OpenStack VDS deployment includes management and compute clusters with three principal networks.

**Cluster and Component Architecture**

A typical VDS deployment architecture consists of two clusters and three separate VLANs. For details about the VLANs, see “Physical VDS Network Overview,” on page 25.
The VMware Integrated OpenStack architecture includes the following clusters and components.

<table>
<thead>
<tr>
<th>Cluster or Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter instance</td>
<td>Configure a vCenter dedicated to your VMware Integrated OpenStack deployment. This is not required but optimizes deployment.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>For user authentication by the OpenStack Identity Service.</td>
</tr>
<tr>
<td>Management cluster</td>
<td>Contains all the deployed OpenStack component and management VMs. See the “Management Cluster,” on page 22 below for a detailed description of the management cluster and its components.</td>
</tr>
<tr>
<td>Compute cluster</td>
<td>Compute resources for Nova. All tenant VMs are created on these compute clusters.</td>
</tr>
<tr>
<td>Management network</td>
<td>Carries traffic among the management components.</td>
</tr>
<tr>
<td>API access network</td>
<td>Exposes the VMware Integrated OpenStack dashboard and provides access for tenants to the OpenStack APIs and services.</td>
</tr>
<tr>
<td>Provider network</td>
<td>Connects the DHCP nodes in the management cluster with the compute clusters. See “Management Cluster,” on page 22 below.</td>
</tr>
</tbody>
</table>

**Management Cluster**

The Management Cluster contains all the deployed OpenStack component and management VMs.

The DHCP nodes in the VDS-based deployment architecture are the principal distinction from a VDS-based deployment architecture. The DHCP nodes manage the IP addresses for tenant VMs and connect them to the Provider network.
The management cluster contains the following components.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Balancers</td>
<td>Provide HA and enable horizontal scale-out architecture.</td>
<td>2 (1 active, 1 standby)</td>
</tr>
<tr>
<td>Databases (DBs)</td>
<td>Instances of MariaDB that store the OpenStack metadata. RabbitMQ, the message queue service used by all OpenStack services, also runs on the database nodes.</td>
<td>3 (1 active, 2 standby)</td>
</tr>
<tr>
<td>VMware Integrated OpenStack Controller</td>
<td>Contains all the OpenStack services, including Compute, Block Storage, Image Service, Identity Service, and Object Storage. The memcache service, which enables production-grade performance for the Identity Service, also runs on the controller nodes.</td>
<td>2 (both active)</td>
</tr>
<tr>
<td>DHCP</td>
<td>Provide IP addresses to the instances connected to the Provider network.</td>
<td>2 (both active)</td>
</tr>
<tr>
<td>Compute Driver</td>
<td>Contains a subset of Compute processes that interact with the compute clusters to manage VMs.</td>
<td>1 per compute cluster</td>
</tr>
<tr>
<td>VMware Integrated OpenStack Manager Service (OMS)</td>
<td>The vApp that you use to manage your VMware Integrated OpenStack vApp.</td>
<td>1</td>
</tr>
<tr>
<td>VMware Integrated OpenStack Template</td>
<td>Template for redeploying failed OpenStack deployments. This template preserves the configuration settings to facilitate redeployment.</td>
<td>1</td>
</tr>
</tbody>
</table>

The DHCP nodes in the VDS-based deployment architecture are the principal distinction from a VDS-based deployment architecture. These DHCP nodes manage the IP addresses for tenant VMs and connect them to the Provider network.
VMware Integrated OpenStack System Requirements

Before you begin the VMware Integrated OpenStack deployment tasks, your system must comply with all hardware, software, networking, and storage requirements.

Hardware Requirements for VDS Deployments

The hardware requirements are based on the number of VMs used for each component. For example, two VMs are used for load balancing, each of which requires two vCPUs for a total requirement of four vCPUs.

Core VMware Integrated OpenStack Components

<table>
<thead>
<tr>
<th>Component</th>
<th>VMs</th>
<th>vCPU</th>
<th>vRAM (GB)</th>
<th>vDisk Space (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated OpenStack Manager</td>
<td>1</td>
<td>2 (2 per VM)</td>
<td>4 (4 per VM)</td>
<td>25</td>
</tr>
<tr>
<td>Load balancing service</td>
<td>2</td>
<td>4 (2 per VM)</td>
<td>8 (4 per VM)</td>
<td>40 (20 per VM)</td>
</tr>
<tr>
<td>Database service</td>
<td>3</td>
<td>12 (4 per VM)</td>
<td>48 (16 per VM)</td>
<td>240 (80 per VM)</td>
</tr>
<tr>
<td>Controllers</td>
<td>2</td>
<td>16 (8 per VM)</td>
<td>32 (16 per VM)</td>
<td>160 (80 per VM)</td>
</tr>
<tr>
<td>Compute service (Nova CPU)</td>
<td>1</td>
<td>2 (2 per VM)</td>
<td>4 (4 per VM)</td>
<td>20 (20 per VM)</td>
</tr>
<tr>
<td>DHCP service</td>
<td>2</td>
<td>8 (4 per VM)</td>
<td>32 (16 per VM)</td>
<td>40 (20 per VM)</td>
</tr>
<tr>
<td>Ceilometer</td>
<td>1</td>
<td>2 (2 per VM)</td>
<td>4 (4 per VM)</td>
<td>20 (20 per VM)</td>
</tr>
<tr>
<td>Database (MongoDB or NoSQL) for Ceilometer</td>
<td>3</td>
<td>6 (2 per VM)</td>
<td>12 (4 per VM)</td>
<td>60 (20 per VM)</td>
</tr>
</tbody>
</table>

**Note** The optional Object Storage (Swift) is installed separately post-installation and is not included in the above requirements. See “Adding OpenStack Components and Features,” on page 54.
Software Requirements for VDS Deployments

Before you begin the VMware Integrated OpenStack deployment tasks, the software components must meet all of the version prerequisites for vSphere, ESXi hosts. In a typical deployment, you require at least three ESXi hosts for the OpenStack management cluster and at least one ESXi host for the OpenStack compute cluster.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere version</td>
<td>Supported versions:</td>
</tr>
<tr>
<td></td>
<td>vSphere 6 Update 1 Enterprise Plus</td>
</tr>
<tr>
<td></td>
<td>vSphere 6 Enterprise Plus</td>
</tr>
<tr>
<td></td>
<td>vSphere 5.5 Update 3 Enterprise Plus</td>
</tr>
<tr>
<td></td>
<td>vSphere 5.5 Update 2 Enterprise Plus</td>
</tr>
<tr>
<td>ESXi hosts</td>
<td>Supported versions:</td>
</tr>
<tr>
<td></td>
<td>Version 6.0 Update 1</td>
</tr>
<tr>
<td></td>
<td>Version 6.0</td>
</tr>
<tr>
<td></td>
<td>Version 5.5 Update 3</td>
</tr>
<tr>
<td></td>
<td>Version 5.5 Update 2</td>
</tr>
<tr>
<td></td>
<td>Eight or more logical processors on each host.</td>
</tr>
</tbody>
</table>
|                  | The vCenter and all ESXi hosts intended for the VMware Integrated OpenStack deployment must use the same Network Time Protocol (NTP) server. For details about configuring NTP on ESX servers, see the VMware knowledge base article at http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003063.

Physical VDS Network Overview

A VMware Integrated OpenStack deployment with VDS networking requires three VLANs.

Request your network administrator to prepare the following VLANs.
<table>
<thead>
<tr>
<th>VLAN</th>
<th>Description</th>
</tr>
</thead>
</table>
| API Access network   | The API Access network provide access for users to the OpenStack services through APIs or the VMware Integrated OpenStack dashboard.  
  - Trunk all hosts in the Management cluster to this VLAN.  
  - Make externally accessible.  
  - Requires 5 or more continuous IP addresses. |
| Management network   | The Management network carries traffic among the management components.  
  - Trunk all hosts in the Management cluster to this VLAN.  
  - Trunk all hosts in the Compute cluster to this VLAN.  
  - The vCenter server needs to be connected to this network over L2 or L3.  
  - Requires 18 or more continuous IP addresses. (21 if you add the Ceilometer component.) |
| Provider             | The Provider network connects DHCP services with the OpenStack instances in the Compute cluster.  
  - Trunk all hosts in the Management cluster to this VLAN.  
  - Trunk all hosts in the Compute cluster to this VLAN. |

**Figure 3-1.** VMware Integrated OpenStack VDS Physical Network
You can deploy VMware Integrated OpenStack in compact deployment mode. Compact deployment mode requires significantly fewer hardware resources and memory than HA mode.

An VMware Integrated OpenStack deployment with compact architecture requires the least amount of resources to get started. The product architecture in compact mode requires one ESXi host and a minimum of 120 GB of storage.

As opposed to the HA architecture, the compact architecture has only one instance of controller, message queue, and database. As shown in the figure below, all of the components are deployed in two VMs.

**Figure 4-1. Management cluster in compact mode**

If you are comfortable protecting the virtual machine by making regular backups, then you can use compact architecture in production. If you are not comfortable making regular backups, the compact architecture is good for learning, proof of concept, and evaluating new versions of VIO.

**Hardware Requirements for Compact Mode Deployments**

The hardware requirements are based on the number of VMs used for each component.

**Core VMware Integrated OpenStack Components**

<table>
<thead>
<tr>
<th>Component</th>
<th>VMs</th>
<th>vCPU</th>
<th>vRAM (GB)</th>
<th>vDisk Space (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated OpenStack Manager</td>
<td>1</td>
<td>2 (2 per VM)</td>
<td>4 (4 per VM)</td>
<td>25</td>
</tr>
<tr>
<td>Controllers, Compute service (Nova CPU)</td>
<td>1</td>
<td>8 (8 per VM)</td>
<td>16 (16 per VM)</td>
<td>80 (80 per VM)</td>
</tr>
<tr>
<td>TOTAL</td>
<td>2</td>
<td>10</td>
<td>20 GB</td>
<td>120 GB</td>
</tr>
</tbody>
</table>
If you install Ceilometer, additional resources are required.

### Table 4-1. Additional requirements for Ceilometer

<table>
<thead>
<tr>
<th>Component</th>
<th>VMs</th>
<th>vCPU</th>
<th>vRAM (GB)</th>
<th>vDisk Space (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ceilometer</td>
<td>1</td>
<td>2 (2 per VM)</td>
<td>4 (4 per VM)</td>
<td>20 (20 per VM)</td>
</tr>
<tr>
<td>Database (MongoDB or NoSQL) for Ceilometer</td>
<td>3</td>
<td>6 (2 per VM)</td>
<td>12 (4 per VM)</td>
<td>60 (20 per VM)</td>
</tr>
<tr>
<td>TOTAL</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>80</td>
</tr>
</tbody>
</table>
Preparing the Dedicated vCenter Instance

Before you install and deploy VMware Integrated OpenStack, prepare your vCenter instance by setting up the necessary clusters, firewall, and network resources.

The procedure is different depending on whether you are using NSX or VDS for the Neutron networking component.

**Important** When preparing your vCenter instance, be aware that certain naming and character restrictions apply. See “Unicode UTF-8 and Special Character Support,” on page 10

This chapter includes the following topics:

- “Prepare the vCenter Instance for Compact Mode Deployment,” on page 29
- “Prepare the vCenter Instance for VDS Deployment,” on page 30
- “Prepare the vCenter Instance for NSX-Based Deployment,” on page 31

Prepare the vCenter Instance for Compact Mode Deployment

Before you install and deploy VMware Integrated OpenStack, prepare your vCenter instance by setting up the necessary clusters, firewall, and network resources.

For details about working with vCenter Server, see the vSphere documentation.

For details about working with data centers, see the vSphere documentation.

**Procedure**

1. (Optional) Configure a vCenter instance dedicated to your VMware Integrated OpenStack deployment.
   
   A dedicated vCenter instance is not required but optimizes deployment.

2. Create a vCenter Server.

3. Define a data center in vCenter.

4. Create a Virtual Distributed Switch.
5 Create the Management cluster.
   The management cluster contains VMware Integrated OpenStack management operations and the
   Integrated OpenStack Manager used to deploy and manage the Integrated OpenStack deployment.
   a Name the cluster.
   b Assign one host to the management cluster.
   c Attach one or more datastores to the management cluster to store images for the Image Service
      component.

6 Create the Compute cluster.
   a Name the cluster.
   b Assign at least one host to the compute cluster.
   c Attach one or more datastores to each Compute cluster.

7 Configure all clusters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSphere Distributed Resource Scheduler (DRS)</td>
<td>Enable.</td>
</tr>
<tr>
<td>Host Monitoring</td>
<td>Enable.</td>
</tr>
<tr>
<td>Admission Control</td>
<td>Enable and set the policy. The default policy is to tolerate one host failure.</td>
</tr>
<tr>
<td>Virtual machine restart policy</td>
<td>Set to High.</td>
</tr>
<tr>
<td>Virtual machine monitoring</td>
<td>Set to virtual machine and Application Monitoring.</td>
</tr>
<tr>
<td>Monitoring sensitivity</td>
<td>Set to High.</td>
</tr>
<tr>
<td>vMotion and Fault Tolerance Logging</td>
<td>Enable.</td>
</tr>
<tr>
<td>Hardware VT in the BIOS of all hosts in the cluster</td>
<td>Enable.</td>
</tr>
<tr>
<td>vMotion and Fault Tolerance Logging for the management network VMkernel port</td>
<td>Enable.</td>
</tr>
</tbody>
</table>

8 Create the Management port group on the VDS and tag it with the VLAN ID assigned to the
   Management network.

9 Create the API Access port group on the VDS and tag it with the VLAN ID assigned to the API Access
   network.

**Prepare the vCenter Instance for VDS Deployment**

Before you install and deploy VMware Integrated OpenStack, prepare your vCenter instance by setting up
the necessary clusters, firewall, and network resources.

For details about working with vCenter Server, see the vSphere documentation.

For details about working with data centers, see the vSphere documentation.

**Prerequisites**

Verify that the required VLANs are configured. See “Physical VDS Network Overview,” on page 25.

**Procedure**

1 (Optional) Configure a vCenter instance dedicated to your VMware Integrated OpenStack deployment.
   A dedicated vCenter instance is not required but optimizes deployment.
2 Create a vCenter Server.

3 Define a data center in vCenter.

4 Create a Virtual Distributed Switch.

5 Create the Management cluster.

   The management cluster contains VMware Integrated OpenStack management operations and the
   Integrated OpenStack Manager used to deploy and manage the Integrated OpenStack deployment.
   a Name the cluster.
   b Assign at least three hosts to the management cluster.
   c Attach one or more datastores to the management cluster to store images for the Image Service
   component.

6 Create the Compute cluster.

   a Name the cluster.
   b Assign at least one host to the compute cluster.
   c Attach one or more datastores to each Compute cluster.

7 Configure all clusters with the following settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSphere Distributed Resource Scheduler (DRS)</td>
<td>Enable.</td>
</tr>
<tr>
<td>Host Monitoring</td>
<td>Enable.</td>
</tr>
<tr>
<td>Admission Control</td>
<td>Enable and set the policy. The default policy is to tolerate one host failure.</td>
</tr>
<tr>
<td>Virtual machine restart policy</td>
<td>Set to High.</td>
</tr>
<tr>
<td>Virtual machine monitoring</td>
<td>Set to virtual machine and Application Monitoring.</td>
</tr>
<tr>
<td>Monitoring sensitivity</td>
<td>Set to High.</td>
</tr>
<tr>
<td>vMotion and Fault Tolerance Logging</td>
<td>Enable.</td>
</tr>
<tr>
<td>Hardware VT in the BIOS of all hosts in the cluster</td>
<td>Enable.</td>
</tr>
<tr>
<td>vMotion and Fault Tolerance Logging for the management network VMkernel port</td>
<td>Enable.</td>
</tr>
</tbody>
</table>

8 Create a VDS, and add all hosts in the Management and Compute clusters to this VDS.

9 Create the Management port group on the VDS and tag it with the VLAN ID assigned to the Management network.

10 Create the API Access port group on the VDS and tag it with the VLAN ID assigned to the API Access network.

**Prepare the vCenter Instance for NSX -Based Deployment**

Before you install and deploy VMware Integrated OpenStack, prepare your vCenter instance by setting up the necessary clusters, firewall, and network resources.

For details about working with vCenter Server, see the vSphere documentation.

For details about working with data centers, see the vSphere documentation.
Prerequisites

Verify that the required VLANs are configured. See “Physical NSX Network,” on page 18.

Procedure

1  (Optional) Configure a vCenter instance dedicated to your VMware Integrated OpenStack deployment.
    A dedicated vCenter instance is not required but optimizes deployment.

2  Create a vCenter Server.

3  Define a data center in the vCenter instance.

4  Create the Management cluster.

   The management cluster contains VMware Integrated OpenStack management operations and the
   Integrated OpenStack Manager used to deploy and manage the Integrated OpenStack deployment.
   a  Name the cluster.
   b  Assign at least three hosts to the management cluster.
   c  Attach one or more datastores to the management cluster to store images for the Image Service
      component.

5  Create the Compute cluster.
   a  Name the cluster.
   b  Assign at least one host to the compute cluster.
   c  Attach one or more datastores to each Compute cluster.

6  Create the Edge cluster.

   The recommended architecture separates the NSX Edge nodes into a dedicated cluster to ensure
   optimal performance. NSX Edge nodes provide DHCP and support for routing, and floating IP
   addresses.
   a  Name the cluster.
   b  Assign at least one host to the Edge cluster.
   c  Attach one or more datastores to the Edge cluster.

7  Configure all clusters with the following settings.
   ■ Enable VMware vSphere Distributed Resource Scheduler (DRS).
   ■ Enable Host Monitoring.
   ■ Enable Admission Control and set the policy. The default policy is to tolerate one host failure.
   ■ Set virtual machine restart policy to High.
   ■ Set virtual machine monitoring to virtual machine and Application Monitoring.
   ■ Set monitoring sensitivity to High.
   ■ Enable vMotion and Fault Tolerance Logging.
   ■ Enable Hardware VT enabled in the BIOS of all hosts in the cluster.
   ■ Enable vMotion and Fault Tolerance Logging for the management network VMkernel port.
8 Create and configure the Virtual Distributed Switch (VDS) appropriate to your physical implementation.

The VDS configuration depends on whether the Management, Edge, and Compute clusters are L2 adjacent. Clusters that are L2 adjacent can share the same VDS. Otherwise, create a separate VDS for each cluster.

Typically, there are three possible configurations:

- You add the Management, Edge, and Compute clusters to a shared VDS. (All three clusters are L2 adjacent.)

- You add the Management and Edge clusters to a shared VDS, and add the Compute cluster to a separate VDS. (The Management and Edge clusters are L2 adjacent.)

- You add the Management, Edge, and Compute clusters to separate VDS switches. (None of the clusters are L2 adjacent.)

9 Create a management port group on each VDS (Management, Edge, and Compute), and tag them with the VLAN ID assigned to the Management network.

10 Create the API Access port group on the Management VDS, and tag it with the VLAN ID assigned to the API Access network.

11 Create the External port group on the Edge VDS, and tag it with the VLAN ID assigned to the External network.
To install VMware Integrated OpenStack, you must obtain and install the VMware Integrated OpenStack OVA package in vSphere. You use the Integrated OpenStack Manager to configure your OpenStack components.

This chapter includes the following topics:

- “Deploy the VMware Integrated OpenStack OVA in the vSphere Web Client,” on page 35
- “Register the Integrated OpenStack Manager vApp,” on page 36
- “Deploy a New OpenStack Instance by Using the Integrated OpenStack Manager,” on page 37

### Deploy the VMware Integrated OpenStack OVA in the vSphere Web Client

Before you can install VMware Integrated OpenStack, you must deploy the VMware Integrated OpenStack OVA. The VMware Integrated OpenStack OVA installs the Integrated OpenStack Manager in the Inventories panel of the Home tab in your vSphere Web Client. The Integrated OpenStack Manager is the vApp through which you configure and implement an OpenStack cloud infrastructure integrated with your vSphere deployment.

**Prerequisites**

Verify that your vSphere instance is correctly prepared. See “Prepare the vCenter Instance for VDS Deployment,” on page 30.

- Install and configure vSphere. See “VMware Integrated OpenStack System Requirements,” on page 16.
- Obtain the VMware Integrated OpenStack OVA from VMware.

**Note** The OVA requires 4 GB on your local disk.

**Procedure**

1. Download the VMware Integrated OpenStack OVA file from the VMware Integrated OpenStack download page.
2. Login to the vSphere Web Client.
3. Go to the vCenter Hosts and Clusters view.
4. Choose the management cluster previously configured for the VMware Integrated OpenStack deployment.
5. Right-click the management cluster and select **Deploy OVF Template** from the pop-up menu.
6. Access the downloaded VMware Integrated OpenStack OVA.
7 Specify the destination and configure the OVA deployment.
   a (Optional) Specify a name for the Integrated OpenStack Manager vApp.
      The only valid characters for the Integrated OpenStack Manager vApp names are alphanumeric and underscores. The vApp name must be fewer than 60 characters. When you choose the vApp name, also consider how you will name your clusters. Together the vApp and cluster names can have a maximum of 80 characters.
   b Select the target datacenter created specifically for the VMware Integrated OpenStack OVA, and click Next.
   c Select your storage options and click Next.
   d To set up your networks, select the management port group for the OpenStack Manager Server and the previously configured management port group for the openstack-template Network 1 setting and click Next.
   e Customize the deployment properties by configuring the management server properties. This includes the option to create the default password for the management server.
8 Click Next.
9 Verify that the vApp can bind to the vService, and click Next.
10 Review the deployment settings and select Power on after deployment.
11 Click Finish to deploy the Integrated OpenStack Manager.
   The Integrated OpenStack Manager icon now appears in the Home Inventories panel.

   **NOTE** If the icon does not appear, log out of vCenter and log back in. The icon should appear.

What to do next
The icon for the Integrated OpenStack Manager might not appear after deploying the VMware Integrated OpenStack OVA. You must manually register the vApp plugin. See “Register the Integrated OpenStack Manager vApp,” on page 36.

Register the Integrated OpenStack Manager vApp
After you deploy the VMware Integrated OpenStack OVA as a plug-in, you must register the plug-in before you can access it in vSphere Web Client.
Until you complete this registration, the VMware Integrated OpenStack Manager icon will not appear in the Inventories tab in the vSphere Web Client.

Procedure
1 Navigate to https://[VMware Integrated OpenStack Manager Service IP Address]:8443/VIO.
2 Log in with the administrator credentials for the vCenter dedicated to the VMware Integrated OpenStack deployment.
3 Under Status, locate the red status indicator showing that the management server is not correctly connected to the vCenter.
4 Click Fix.
5 In the Certificate dialog box, verify the certificate and click OK.
6 Log out from the registration interface.
7 Log in to the vSphere Web Client and select **Home > Inventories**.
The VMware Integrated OpenStack Manager icon should now be visible on the Inventories tab in the vSphere Web Client.

What to do next

Use the Integrated OpenStack Manager to deploy OpenStack services in your vSphere environment. See “Deploy a New OpenStack Instance by Using the Integrated OpenStack Manager,” on page 37.

Deploy a New OpenStack Instance by Using the Integrated OpenStack Manager

You deploy the VMware Integrated OpenStack cloud by using the Integrated OpenStack Manager in your dedicated vCenter instance.

Prerequisites

Verify that you have prepared the required clusters and networks. See “Prepare the vCenter Instance for VDS Deployment,” on page 30.

Verify that the Integrated OpenStack Manager OVA was correctly deployed. See “Deploy the VMware Integrated OpenStack OVA in the vSphere Web Client,” on page 35.

Verify that the datastores required for the installation are available. The following conditions may prevent a datastore cluster from being available:

- The datastore is already configured for the current cluster.
- The datastore is not mounted to the current cluster.
- Ensure that the DNS server is set properly. The Active Directory domain relies on DNS to function properly.
- Ensure that the gateway/firewall forwards DNS requests in a private network.

Verify that the clusters required for the installation are available. The following conditions may prevent a cluster from being available:

- The cluster has no available datastores.
- The cluster has no reachable host.
- For Compute nodes: the cluster is already being consumed by another Compute node or NSX Edge node.

Procedure

1. In the vSphere Web Client, select Home > Inventories and click the Integrated OpenStack Manager icon.
2. Click Deploy OpenStack in the lower panel to start the deployment wizard.
3. On the Select a deployment method page, select the type of deployment.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use this wizard to configure a new OpenStack instance</strong></td>
<td>Deploys and configures a new OpenStack instance. You will require all the prerequisite information: network configurations, clusters, datastores, and so on.</td>
</tr>
<tr>
<td><strong>Use an exported template to pre-fill configuration settings in this wizard</strong></td>
<td>Populates the deployment wizard with settings by using a JSON template exported from an existing VMware Integrated OpenStack deployment.</td>
</tr>
</tbody>
</table>
| **Deployment type**                                | Choose the deployment type for the OpenStack Cloud. Select one of the following:  
- **HA** - Specifies an HA (high availability) deployment.  
  In a HA deployment, there are three or more VMs in the OpenStack instance.  
- **Compact** - Specifies a compact deployment.  
  With a compact deployment, the OpenStack instance contains two VMs. |

**NOTE** The rest of the procedure assumes this is a new OpenStack instance.

4. Click **Next**.

5. Review the deployment process and provide the administrator credentials for the vCenter Server instance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deployment name</strong></td>
<td>Enter a name for the current deployment. This value serves as a unique identifier for the deployment and can help facilitate in future upgrade processes.</td>
</tr>
<tr>
<td><strong>Use management vCenter Server as Compute vCenter Server</strong></td>
<td>Select this option to deploy on multiple vCenter servers. This option is supported on NSX deployments only.</td>
</tr>
<tr>
<td><strong>Management vCenter Server</strong></td>
<td>Enter the IP address or FQDN value for the vCenter instance to which the OpenStack management server is connected.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Enter the username for the vCenter Server administrator.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password for the vCenter Server administrator.</td>
</tr>
<tr>
<td><strong>Ignore the vCenter Server certificate validation</strong></td>
<td>Select this option to ignore the vCenter Server certificate validation. VMware Integrated OpenStack requires this authorization to access the vCenter Server for management services.</td>
</tr>
</tbody>
</table>

**NOTE** The rest of the procedure assumes this is a new OpenStack instance.

6. Click **Next**.
7 Select the cluster for the OpenStack management components.

**Note** If you choose Compact for the Deployment type setting, the Configure the load balancer step does not appear in the Integrated OpenStack Manager UI.

Select the Management cluster you created when you prepared the vCenter instance for the VMware Integrated OpenStack deployment.

**Figure 6-1. Select the management cluster**

![Select the management cluster](image)

8 Click Next.

9 In the Configure management networking screen, provide the following settings for the Management network and OpenStack API Access network.

You prepared the network settings and resources in advance. The Management network connects the OpenStack Manager and all OpenStack VMs with the vCenter Server. If applicable, all NSX Controller nodes also connect to this network. The API Access network is for user access to the OpenStack APIs and the OpenStack dashboard.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port group</td>
<td>Select a port group you configured in preparation for the VMware Integrated OpenStack deployment.</td>
</tr>
</tbody>
</table>
| IP range         | For the Management network setting, specify the range of IP addresses as determined during the network preparation:  
  - For Compact mode, the Management network requires a minimum of 4 contiguous IP addresses.  
  - For HA mode, the Management network requires a minimum of 11 contiguous IP addresses.  
  If you are configuring HA mode, then for the API access network setting, specify a minimum of two contiguous IP addresses. |
<p>| IP address       | If you are configuring Compact mode, then for the API access network, configure a single IP address. |
| Subnet mask      | Provide the subnet mask. |</p>
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway</td>
<td>Provide the gateway address.</td>
</tr>
<tr>
<td>DNS addresses</td>
<td>Provide the addresses for the domain name servers.</td>
</tr>
</tbody>
</table>

If you choose the **Compact** deployment mode, optionally enter the **Public hostname** for the API access network.

**Figure 6-2. Configure management networking**

10 Click Next.

11 If you chose **HA** deployment mode, an additional screen appears - the Configure the load balancer screen. If you specified **HA** deployment mode, provide the hostname and VIP settings for the load balancer service.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public hostname</td>
<td>FQDN value of the public VIP.</td>
</tr>
<tr>
<td>Public Virtual IP</td>
<td>Public VIP address.</td>
</tr>
</tbody>
</table>

**Note** The public VIP address for the load balancer VM also connects to the OpenStack API Access network.

12 Click Next.

13 Select the cluster for the Nova (Compute) component.

This is the Compute cluster you created when you prepared the vCenter instance for the VMware Integrated OpenStack deployment.

14 Click Next.
15 Select the datastores for the Nova (Compute) component to consume, and click **Next**.

**Figure 6-3. Add Nova datastores**

16 Select the datastores for the Glance (Image Service) component to consume, and click **Next**.
Configure the Neutron (Network) component.

You can select either Virtual Distributed Switch Networking or NSX Networking.

**IMPORTANT** After deploying VMware Integrated OpenStack, you cannot change this selection. For example, if you choose the Virtual Distributed Switch Networking option, you cannot later upgrade or modify to an NSX configuration without redeploying.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Distributed Switch</td>
<td>Select the dedicated VDS you previously configured for the VMware</td>
</tr>
<tr>
<td>Networking</td>
<td>Integrated OpenStack deployment. The port groups backing the provider</td>
</tr>
<tr>
<td></td>
<td>networks will map to this VDS.</td>
</tr>
<tr>
<td>NSX Networking</td>
<td>Complete the settings based on your NSX deployment.</td>
</tr>
<tr>
<td>Manager Address</td>
<td>IP address or FQDN of the NSX Manager.</td>
</tr>
<tr>
<td>Username</td>
<td>Username for the NSX Manager.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the NSX Manager.</td>
</tr>
<tr>
<td>Transport Zone</td>
<td>From the drop-down menu, select the Transport Zone that will carry</td>
</tr>
<tr>
<td></td>
<td>traffic between OpenStack instances.</td>
</tr>
<tr>
<td>Edge Cluster</td>
<td>From the drop-down menu, select the cluster where the NSX Edge</td>
</tr>
<tr>
<td></td>
<td>instances will be deployed.</td>
</tr>
<tr>
<td>Virtual Distributed Switch</td>
<td>From the drop-down menu, select the VDS from the NSX configuration.</td>
</tr>
<tr>
<td>External Network</td>
<td>From the drop-down menu, select the port group designated for the</td>
</tr>
<tr>
<td></td>
<td>external network. Instances can be uplinked to this external network</td>
</tr>
<tr>
<td></td>
<td>via a virtual router.</td>
</tr>
<tr>
<td>Router appliance size</td>
<td>From the drop-down menu, select the size for the NSX Edge server.</td>
</tr>
<tr>
<td>Enable Edge HA</td>
<td>Select this option to enable high availability for the NSX Edge server.</td>
</tr>
<tr>
<td>Metadata service network</td>
<td>Indicate the port group for the metadata service network.</td>
</tr>
</tbody>
</table>

**Note**

If you used the configuration recommended by VMware and described in this guide, select **Use the same port group...** option.

Click Next.
19 Set the VMware Integrated OpenStack authentication source.

   a Create and confirm the administrator credentials in the Setup OpenStack admin user panel. These are the credentials the OpenStack administrator will use to log into the VMware Integrated OpenStack dashboard.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenStack admin user</td>
<td>Define the OpenStack administrative user name. This is the default administrative user name for logging in to the VMware Integrated OpenStack dashboard.</td>
</tr>
<tr>
<td>OpenStack admin password</td>
<td>Define the OpenStack administrative user password. This is the default administrative user password for logging in to the VMware Integrated OpenStack dashboard.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>Reenter the password for confirmation.</td>
</tr>
</tbody>
</table>

   b (Optional) (Optional) If you want to configure Active Directory as an LDAP backend at this time, click Enable and complete the following settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Specify the full Active Directory domain name; for example, vmware.com.</td>
</tr>
<tr>
<td>Bind user</td>
<td>Provide the user name to bind to Active Directory for LDAP requests.</td>
</tr>
<tr>
<td>Bind password</td>
<td>Provide the password to allow the LDAP client access to the LDAP server.</td>
</tr>
<tr>
<td>Domain controllers</td>
<td>(Optional) VMware Integrated OpenStack automatically chooses the existing Active Directory domain controllers. However, you can specify a list of specific domain controllers to use. To do this, select the Domain controllers radio button and then enter the IP address of one or more domain controllers, separated by commas.</td>
</tr>
<tr>
<td>Site</td>
<td>(Optional) Optionally, you can limit LDAP searching to a specific deployment site within your organization; for example, sales.vmware.com. Do to this, select the Site radio button and enter the domain name of the site to search.</td>
</tr>
<tr>
<td>User Tree DN</td>
<td>(Optional) Enter the search base for users; for example, DC=vmware, DC=com. Defaults to the top of the user tree in most Active Directory deployments.</td>
</tr>
<tr>
<td>User Filter</td>
<td>(Optional) Enter an LDAP search filter for users.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>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 examples of filters, see <a href="https://msdn.microsoft.com/en-us/library/aa746475(v=vs.85).aspx">https://msdn.microsoft.com/en-us/library/aa746475(v=vs.85).aspx</a>.</td>
</tr>
</tbody>
</table>

**Figure 6-4. Configure authentication source**

20 (Optional) Provide the IP address for the Log Insight server to configure the syslog server, and click Next.

21 Choose to participate in the Customer Experience Improvement Program.

VMware’s Customer Experience Improvement Program (CEIP) provides VMware with information that enables VMware to improve its products and services and to fix problems. By choosing to participate in CEIP, you agree that VMware may collect technical information about your use of VMware products and services on a regular basis. This information does not personally identify you. See “Customer Experience Improvement Program,” on page 11. This option is enabled by default.

22 Click Next.

23 Review the configuration settings, and click Finish.

The deployment process can take several minutes to complete.

24 Confirm that VMware Integrated OpenStack deployed successfully.

a In the vSphere Web Client, go to the Home > Inventories panel, click the VMware Integrated OpenStack icon.

b Expand the Inventory view and click OpenStack Deployments.

The OpenStack Deployment tab shows the current status and if it is running.

c (Optional) Click the deployment name to view detailed status of each service node in the OpenStack deployment.
25 Confirm that you can access the VMware Integrated OpenStack dashboard.
   a In a Web browser, navigate to the VMware Integrated OpenStack dashboard. The URL is the Public Virtual IP address configured during the deployment process.
   b Log in as administrator to the VMware Integrated OpenStack dashboard. The default administrative username and password were configured during the deployment process.

   If the login is successful, VMware Integrated OpenStack was successfully deployed.

The Integrated OpenStack Manager implements the configuration to deploy your VMware Integrated OpenStack cloud. Optionally, you can review the deployment in vCenter by drilling down into the OpenStack Cluster.

**What to do next**

You can add OpenStack components, clusters, and datastores to your VMware Integrated OpenStack cloud deployment.

To complete the LDAP configuration, you must manually modify the default OpenStack domain configuration. See “Modify the Default Domain Configuration,” on page 47.

**Exclude the VMware Integrated OpenStack VMs from Firewall Protection**

For NSX based deployments, you must exclude the VMware Integrated OpenStack management VMs from firewall protection to ensure the free flow of traffic.

NSX Manager, NSX Controller, and NSX Edge VMs are excluded from firewall protection. You must manually exclude the VMware Integrated OpenStack and vCenter server VMs by placing them in the Exclusion List to allow traffic to flow freely.

The cluster that contains vCenter Server can be protected by a firewall, but the vCenter Server must also be in the exclusion list to avoid connectivity issues.

For more information about the exclusion list, see the NSX product documentation.

**Procedure**

1 In the vSphere Web Client, click **Networking & Security**.
2 In **Networking & Security Inventory**, click **NSX Managers**.
3 In the Name column, click the NSX Manager for VMware Integrated OpenStack.
4 Click the **Manage** tab and click the **Exclusion List** tab.
5 Click the **Add (+)** icon.
6 Select the OpenStack VMs in the Available Objects column and use the arrows buttons to move them to the Selected Objects column.
7 Click **OK** when you are finished.

If a VM has multiple vNICs, all of them are excluded from protection. If you add vNICs to a VM after it is added to the exclusion list, a firewall is deployed on the newly added vNICs. To exclude these vNICs from firewall protection, remove the VM from the exclusion list and add it back to the exclusion list.
Create the Provider Network in OpenStack

For VMware Integrated OpenStack deployments that use VDS for networking, you must complete the deployment process by creating the Provider network in OpenStack.

Prerequisites

Verify that VMware Integrated OpenStack was successfully deployed. You can do so by logging into the VMware Integrated OpenStack dashboard.

Procedure

1. In a Web browser, navigate to the VMware Integrated OpenStack dashboard. The URL is the Public Virtual IP address configured during the deployment process.
2. Log in as administrator. The default administrative username and password were configured during the deployment process.
3. Select the default admin project from the drop-down menu in the title bar.
4. Select Admin > System Panel > Networks. The Networks page lists the networks that are currently configured.
5. Click Create Network.
6. In the Create Network dialog box, configure the Provider network:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the network.</td>
</tr>
<tr>
<td>Project</td>
<td>Select the default admin project from the drop-down menu.</td>
</tr>
<tr>
<td>Provider Network Type</td>
<td>Select VLAN from the drop-down menu.</td>
</tr>
<tr>
<td>Physical Network</td>
<td>Enter dvs.</td>
</tr>
<tr>
<td>Segmentation ID</td>
<td>Enter the ID of the Provider VLAN. Contact your network administrator for this value.</td>
</tr>
</tbody>
</table>

7. Select the Admin State option.
8. Click Create Network.

The Provider network now appears on the Networks page. This completes the VMware Integrated OpenStack deployment process.

Monitor Your VMware Integrated OpenStack Deployment

After you finish installing VMware Integrated OpenStack, you can monitor your deployment configuration, including datastore sizes, network settings, and metadata service, among other details.

Procedure

1. In vCenter, select Home > VMware Integrated OpenStack.
2. Click the Monitor tab.
Modify the Default Domain Configuration

By default, the Identity Service component (Keystone) does not return users and groups to the default domain. The following procedure modifies the default configuration to ensure that users with administrative privileges can access and assign LDAP users to roles in OpenStack.

Prerequisites
- Verify that you have successfully deployed VMware Integrated OpenStack.
- Verify that VMware Integrated OpenStack is running.
- Verify that Active Directory is configured as the LDAP backend.

Procedure
1. Using SSH, log in to the VMware Integrated OpenStack deployment.
   This step varies depending on your mode of deployment.
   - If your deployment is using compact mode, log into the controller node.
   - If your deployment is high-availability mode, log into the load balancer node.
2. Switch to root user.
   sudo su -
   $ source ~/cloudadmin_v3.rc
4. Create the initial project in the default domain in OpenStack.
   $ openstack --os-identity-api-version 3 --os-username admin \
      --os-user-domain-name local --os-project-name admin --os-password admin \
      --os-region-name nova project create --domain default --description "Demo Project" --
or-show demo

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--os-username admin</td>
<td>Provides the administrative username for login, in this case admin.</td>
</tr>
<tr>
<td>--os-user-domain-name local</td>
<td>Specifies the domain, in this case local for the specified user.</td>
</tr>
<tr>
<td>--os-project-name admin</td>
<td>Specifies the admin OpenStack project.</td>
</tr>
<tr>
<td>--os-password admin</td>
<td>Provides the administrative password for login, in this case admin.</td>
</tr>
<tr>
<td>--os-region-name nova project create</td>
<td>Runs the nova project create command.</td>
</tr>
<tr>
<td>--domain default</td>
<td>This command specifies the domain where the new project is created, in this case the default domain.</td>
</tr>
<tr>
<td>--description &quot;Demo Project&quot;</td>
<td>This parameter names the new project, in this case Demo Project.</td>
</tr>
<tr>
<td>--or-show demo</td>
<td>Creates an alias for the new project.</td>
</tr>
</tbody>
</table>
5 Add an administrative user to the new project in the default domain.

```
$ openstack --os-identity-api-version 3 --os-username admin \
    --os-user-domain-name local --os-project-name admin --os-password admin \
    --os-region-name nova role add --project demo --project-domain default \
    --user SOMEUSER@vmware.com --user-domain default admin
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--os-username admin</td>
<td>Provides the administrative username for login, in this case admin.</td>
</tr>
<tr>
<td>--os-user-domain-name local</td>
<td>Specifies the domain, in this case local for the specified user.</td>
</tr>
<tr>
<td>--os-project-name admin</td>
<td>Specifies the admin OpenStack project.</td>
</tr>
<tr>
<td>--os-password admin</td>
<td>Provides the administrative password for login, in this case admin.</td>
</tr>
<tr>
<td>--os-region-name nova role add</td>
<td>Runs the nova role add command.</td>
</tr>
<tr>
<td>--project demo</td>
<td>Specifies the project to which the new administrative user is added.</td>
</tr>
<tr>
<td>--project-domain default</td>
<td>Specifies the project domain.</td>
</tr>
<tr>
<td>--user <a href="mailto:SOMEUSER@vmware.com">SOMEUSER@vmware.com</a></td>
<td>Specifies the new administrative user.</td>
</tr>
<tr>
<td>--user-domain default admin</td>
<td>Assigns the new user to the default admin domain.</td>
</tr>
</tbody>
</table>

**Note** If special characters are used for the user ID, you must modify the Keystone settings in the VMware Integrated OpenStack manager.

6 (Optional) If special characters are used for the administrative user ID, you must modify the Keystone settings in the VMware Integrated OpenStack manager.

a In the VMware Integrated OpenStack manager in vCenter, go to Manage > Settings > Configure Identity Source.

b Click Edit.

c Under Advanced Settings, modify the User ID value from `cn` to `userPrincipalName`.

You can now log in to the default domain in the VMware Integrated OpenStack dashboard using the administrative user name and password.
After completing installation of VMware Integrated OpenStack, you can integrate it with vRealize Operations Manager and the Endpoint Operations Management Agent, as well as add or extend other OpenStack components.

This chapter includes the following topics:

- “Configuring and Enabling LBaaS Using the CLI,” on page 49
- “Integrating OpenStack with the Endpoint Operations Management Agent,” on page 53
- “Adding OpenStack Components and Features,” on page 54
- “Adding Capacity in vSphere Web Client,” on page 63

Configuring and Enabling LBaaS Using the CLI

Load-Balancing-as-a-Service (LBaaS) enables Neutron, the networking component of OpenStack, to distribute incoming requests among designated instances. This distribution ensures that the workload is shared predictably among instances and enables more effective use of system resources. Because LBaaS supports proprietary and open source load balancing technologies, OpenStack administrators have more options when choosing which back-end technology to use for load balancing.

The current OpenStack release supports LBaaS v2.0. VMware Integrated OpenStack enables LBaaS v2.0 automatically.

**Note** VMware Integrated OpenStack does not support LBaaS v1.0.

Configuring LBaaS v2.0

VMware Integrated OpenStack 3.0 or 3.1 supports LBaaS v2.0. By default, you enable LBaaS v2.0 after you complete the VMware Integrated OpenStack installation or upgrade process.

This task includes creating a health monitor and associates it with the LBaaS pool that contains the LBaaS server instances. The health monitor is a Neutron service that checks if the instances are still running on the specified protocol-port.

**Prerequisites**

**Note** VMware Integrated OpenStack does not support LBaaS v1.0.

This task applies only to VMware Integrated OpenStack deployed with NSX.

**Procedure**

1. Using SSH, log in to the VMware Integrated OpenStack manager.
2 Switch to root user.
   sudo su -

3 Enable LBaaS v2.0.
   viocii lbaasv2-enable

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d DEPLOYMENT</td>
<td>Indicates the name of the VMware Integrated OpenStack deployment.</td>
</tr>
</tbody>
</table>

4 From the VMware Integrated OpenStack manager, use SSH to log in to the Neutron node.

5 Switch to root user.
   sudo su -

6 Create an exclusive router.
   neutron router-create --router_type=exclusive <router name>

7 Attach a subnet to the new router.
   neutron net-create <network name>
   neutron subnet-create <network name> <CIDR value> --name <subnet name>
   neutron router-interface-add <router name or id> <subnet name or id>
Create the load balancer.

This step includes creating the load balancer, creating the listener, and creating the load balancer pool.

a) Create the load balancer, specifying the load balancing VIP subnet.

```
neutron lbaas-loadbalancer-create --name LOAD_BALANCER_1_NAME <vip-subnet-id>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Provide a name for the new load balancer.</td>
</tr>
<tr>
<td>vip-subnet-id</td>
<td>Specify the VIP subnet for the new load balancer. Only members on this</td>
</tr>
<tr>
<td></td>
<td>subnet can be added to the pool.</td>
</tr>
</tbody>
</table>

b) Create a listener for the new load balancer.

```
neutron lbaas-listener-create \
--loadbalancer LOAD_BALANCER_1_NAME \ 
--protocol <protocol type> \ 
--protocol-port <protocol port> \ 
--name LISTENER_1_NAME
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loadbalancer</td>
<td>Specify the load balancer you created in the preceding substep.</td>
</tr>
<tr>
<td>protocol type</td>
<td>Specify the protocol type for the listener.</td>
</tr>
<tr>
<td>protocol port</td>
<td>Specify the protocol port.</td>
</tr>
<tr>
<td>name</td>
<td>Provide a name for the new listener.</td>
</tr>
</tbody>
</table>

c) Create an LBaaS pool.

```
neutron lbaas-pool-create \
--lb-algorithm <load balancing method> \ 
--listener LISTENER_1_NAME \ 
--protocol <protocol type> \ 
--name LB_POOL_1
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lb-algorithm</td>
<td>Specify a load balancing method:</td>
</tr>
<tr>
<td>IP_HASH</td>
<td>Selects a server based on a hash of the source and destination IP</td>
</tr>
<tr>
<td></td>
<td>address of each packet.</td>
</tr>
<tr>
<td>LEAST_CONN</td>
<td>Distributes client requests to multiple servers based on the number of</td>
</tr>
<tr>
<td></td>
<td>connections already on the server. New connections are sent to the server</td>
</tr>
<tr>
<td></td>
<td>with the fewest connections.</td>
</tr>
<tr>
<td>ROUND_ROBIN</td>
<td>Each server is used in turn according to the weight assigned to it.</td>
</tr>
<tr>
<td></td>
<td>This process is the smoothest and fairest algorithm when the server's</td>
</tr>
<tr>
<td></td>
<td>processing time remains equally distributed.</td>
</tr>
<tr>
<td>URI</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>listener</td>
<td>Specify the listener you created in the preceding substep.</td>
</tr>
<tr>
<td>protocol</td>
<td>Specify the protocol for members of the pool to use.</td>
</tr>
<tr>
<td></td>
<td>• TCP</td>
</tr>
<tr>
<td></td>
<td>• HTTP</td>
</tr>
<tr>
<td></td>
<td>• HTTPS</td>
</tr>
<tr>
<td>name</td>
<td>Provide a name for the new pool.</td>
</tr>
</tbody>
</table>

9. Create the instances for the servers and client.

```
nova boot --image <image-uuid> --flavor <flavor> <server 1 name>
nova boot --image <image-uuid> --flavor <flavor> <server 2 name>
nova boot --image <image-uuid> --flavor 1 <client name>
```

10. Add the server instances to the LBaaS pool that you created.

```
neutron lbos-member-create  \
--subnet <subnet-id> --address <server 1 IP> \ 
--protocol-port 80 <pool name>

neutron lbos-member-create  \
--subnet <subnet-id> --address <server 2 IP> \ 
--protocol-port 80 <pool name>
```

11. Set up the health monitor.

```
neutron lbos-healthmonitor-create  \
--delay DELAY_IN SECONDS --type [HTTP | TCP] --max-retries NUMBER \ 
--timeout TIMEOUT_IN SECONDS --pool LBAAS_POOL
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delay</td>
<td>Time in seconds between sending probes to members.</td>
</tr>
<tr>
<td>type</td>
<td>One of the predefined health monitor types. Specify HTTP or TCP.</td>
</tr>
<tr>
<td>max-retries</td>
<td>Number of permissible connection failures before changing the member status to INACTIVE.</td>
</tr>
<tr>
<td>timeout</td>
<td>Maximum number of seconds for a monitor to wait for a connection to be established before it times out.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The timeout value must be less than the delay value.</td>
</tr>
<tr>
<td>pool</td>
<td>Specify the LBaaS pool to be monitored.</td>
</tr>
</tbody>
</table>

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

   a. Create a test `index.html` file.
   b. From the same directory, run a simple request.
      ```
      # sudo python -m SimpleHTTPServer 80
      ```
   c. Log in to the client instance.
   d. Run the `wget` command to view whether your requests are being correctly load-balanced across the two servers in the pool.
      ```
      # wget -O - http://<vip-ip>
      ```
Integrating OpenStack with the Endpoint Operations Management Agent

After installing VMware Integrated OpenStack, you can integrate it with the Endpoint Operations Management Agent and vRealize Operations Manager.

Prerequisites

- Verify that vRealize Operations Manager is running.
- Verify that the vRealize Operations Management Pack for OpenStack 2.0 is installed. See the vRealize Operations Management Pack for OpenStack documentation.

Procedure

1. If you have not already, set up a vRealize Operations Manager server.
   Remember the user name, password, and IP address.
   See the vRealize Operations Manager documentation.

2. Using SSH, log in to the VMware Integrated OpenStack manager.

3. Obtain the Endpoint Operations Management Agent installation file and modify the agent properties file.
   b. Download the installation binary for End Point Operations Linux Agent - 64 bit.
      The complete download file name is vRealize-Endpoint-Operations-Management-Agent-x86-64-linux-6.2.1-3720494.tar.gz.

4. Modify the agent properties file.
   a. Untar the downloaded file.
   b. Copy the conf/agent.properties file.
   c. Modify the copy of the conf/agent.properties file to match your vRealize Operations Manager deployment.
      ```java
      agent.setup.serverIP=[vREALIZE OPERATIONS MANAGER SERVER ADDRESS]
      agent.setup.serverSSLP=Port=[vREALIZE OPERATIONS MANAGER SERVER SSL PORT]
      agent.setup.serverLogin=[vREALIZE OPERATIONS MANAGER ADMIN USER NAME]
      agent.setup.serverPword=[vREALIZE OPERATIONS MANAGER ADMIN PASSWORD]
      agent.setup.serverCertificateThumbprint=[vREALIZE OPERATIONS MANAGER SERVER THUMBPRINT]
      ```
      - The default for the agent.setup.serverSSLP parameter is 443.
      - For the agent.setup.serverCertificateThumbprint, specify either the SHA1 or SHA256 algorithm in hexadecimal format.
   d. Save the copy of the conf/agent.properties file.

5. Install the Endpoint Operations Management Agent in VMware Integrated OpenStack.
   ```bash
   sudo viocli epops install -s \
   vRealize-Endpoint-Operations-Management-Agent-x86-64-linux-6.2.1-3720494.tar.gz \
   -c agent.properties
   ```
6 Confirm the installation was successful.
   a Log in to your vRealize Operations Manager server.
   b In the left pane, select Administration > Inventory Explorer.
      You can identify the new OpenStack resources by their node names, such as controller 01, controller02, compute01, and so on.
   c In Inventory Explorer, select EP Ops Adapter Resources Group > Linux.
      You can identify the list of VMware Integrated OpenStack nodes: such as controller 01, controller02, and so on. If the VMware Integrated OpenStack nodes do not appear, ensure that the parameters in the agent.properties file are correct. If necessary, reconfigure the agent.
      
      ```
      sudo viocli epops reconfig -c your_agent.properties
      ```

### Adding OpenStack Components and Features

The deployment process installs a set of core OpenStack components. You can also install and configure the Object Storage (Swift) and Ceilometer components, and enable the LBaaS feature.

#### Adding the Object Storage Component

After you deploy your OpenStack cloud infrastructure by using the Integrated OpenStack Manager, you can add the optional Object Storage component. The optional Object Storage component is loaded when you deploy the Integrated OpenStack Manager vApp. It requires separate configuration to deploy it.

With OpenStack Object Storage, you can create redundant, scalable data storage by using clusters of standardized servers to store petabytes of accessible data. Object Storage uses a distributed architecture with no central point of control, providing greater scalability, redundancy, and permanence. Objects can be written to multiple hardware devices, with the OpenStack software responsible for ensuring data replication and integrity across the cluster. Storage clusters scale horizontally by adding new nodes. If a node fails, OpenStack replicates the content from other active nodes.

**Important** Although you can add the Object Storage component as an optional component to your VMware Integrated OpenStack deployment, VMware does not support it.

#### Set Up the Object Storage Environment

Before you can configure the Object Storage service for deployment, you must set up its environment to run OpenStack commands.

**Procedure**

1. Using SSH, log in to the VMware Integrated OpenStack manager.
2. From the VMware Integrated OpenStack manager, use SSH to log in to the controller01 node.
3. Switch to root user.
   ```
   sudo su -
   ```
4. Run the respective cloudadmin file.
   ```
   ```
   - For VMware Integrated OpenStack 3.0, run the cloudadmin_v3.rc file.
     ```
     source cloudadmin_v3.rc
     ```
   - For VMware Integrated OpenStack 3.1 and later, run the cloudadmin.rc file.
     ```
     source cloudadmin.rc
     ```
Configure the controller01 node to use the administrative password.

```bash
export OS_PASSWORD=ADMIN_PASSWORD
```

**What to do next**

You can now create the service user, the service, and the endpoint. See “Create the Object Storage User, Service, and End Point,” on page 55.

**Create the Object Storage User, Service, and End Point**

The optional Object Storage component is loaded when you deploy the Integrated OpenStack Manager vApp. It requires separate configuration to deploy it.

You configure and deploy the Object Storage component through the VM console.

**Prerequisites**

Configure and create your VMware Integrated OpenStack cloud.

**Procedure**

1. Open the console for the Identity Service component.

2. Create the administrative user for authentication by the Identity Service component.
   
   a. Use the `openstack user create` command to create the user.
   
   ```bash
   $ openstack user create
   --domain local
   --password password
   --email administrative_user_email
   swift
   
   b. Give the newly created user administrative privileges.
   
   ```bash
   $ openstack role add
   --project service
   --user swift
   admin
   
3. Create a service entry for the Object Storage service.

   ```bash
   $ keystone service-create
   --name=swift
   --type=object-store
   --description="VIO Object Storage"
   
   +-----------------+------------------+
   | Field           | Value            |
   +-----------------+------------------+
   | description      | VIO Object Storage|
   | enabled          | True             |
   | id               | eede9296683e4b5ebfa13f5166375ef6 |
   | name             | swift            |
   | type             | object-store     |
   +-----------------+------------------+

   The service id value is automatically generated.
Create an API end point for the Object Storage service.

Use the IP address of the controller in the commands.

```
openstack endpoint create \
  --region nova \n  object-store \n  public \n  http://controller01_IP_address:8080/v1/AUTH_%(tenant_id)s

openstack endpoint create \
  --region nova \n  object-store \n  internal \n  http://controller01_IP_address:8080/v1/AUTH_%(tenant_id)s

openstack endpoint create \
  --region nova \n  object-store \n  admin \n  http://controller01_IP_address:8080/v1
```

What to do next

After you deploy the Object Storage component, create the necessary configuration files. See “Create the Object Storage Configuration Files,” on page 56.

Create the Object Storage Configuration Files

When you deploy the Object Storage service, you must create or modify several configuration files.

Procedure

1. **Create the swift.conf File** on page 56
   
   The swift.conf file contains strings that prevent unauthorized access to your Object Storage content.

2. **Create and Configure the Loopback Device as Disk** on page 57
   
   The loopback device serves as a virtual disk to hold the Object Storage service data.

3. **Enable the rsync Service** on page 58
   
   To enable the rsync service for the Object Storage service, you must create the /etc/rsyncd.conf file, modify the default rsync configuration, and manually start the rsync service.

4. **Configure the Object Storage Proxy Server** on page 59
   
   The proxy server takes each request for an object and looks up locations for the account, container, or object, and routes the requests correctly. The proxy server also handles API requests.

5. **Create and Configure Object Storage Rings** on page 61
   
   Rings connect the account, container, and object services. Rings also provide load balancing and failover for services that are running on multiple nodes.

Create the swift.conf File

The swift.conf file contains strings that prevent unauthorized access to your Object Storage content.

Procedure

1. Using SSH, log in to the VMware Integrated OpenStack manager.

2. From the VMware Integrated OpenStack manager, use SSH to log in to the controller01 node.
3 Switch to root user.
   `sudo su -`

4 Create the swift directory.
   `mkdir -p /etc/swift`

5 Create the `swift.conf` file.

   Note: The `swift.conf` file contains prefix and suffix settings that provide an additional layer of security. You can use any unique value for these strings. Do not change or modify these values.

   ```
   [swift-hash]
   # random unique string that can never change (DO NOT LOSE)
   swift_hash_path_prefix = xrfuniounaqjnw
   swift_hash_path_suffix = fLIbertYgibbitZ
   ```

6 Save and close the `swift.conf` file.

What to do next

You can now create a loopback device as a disk to store the Object Storage service data. See “Create and Configure the Loopback Device as Disk,” on page 57.

Create and Configure the Loopback Device as Disk

The loopback device serves as a virtual disk to hold the Object Storage service data.

Procedure

1 If you are logged out, log back in to the Object Storage service.
   a Using SSH, log in to the VMware Integrated OpenStack manager.
   b From the VMware Integrated OpenStack manager, use SSH to log in to the controller01 node.
   c Switch to root user.
      `sudo su -`

2 Create the loopback device.
   `truncate -s 5GB /srv/swift-disk1`
   `mkfs.xfs /srv/swift-disk1`
   `truncate -s 5GB /srv/swift-disk2`
   `mkfs.xfs /srv/swift-disk2`
   `truncate -s 5GB /srv/swift-disk3`
   `mkfs.xfs /srv/swift-disk3`

3 Modify the `/etc/fstab` table file.
   `/srv/swift-disk1 /srv/node/sdb xfs loop,noatime,nodiratime,nobarrier,logbufs=8 0 0`
   `/srv/swift-disk2 /srv/node/sdc xfs loop,noatime,nodiratime,nobarrier,logbufs=8 0 0`
   `/srv/swift-disk3 /srv/node/sdd xfs loop,noatime,nodiratime,nobarrier,logbufs=8 0 0`

4 Mount the loopback device.
   `mkdir -p /srv/node/sdb`
   `mount /srv/node/sdb`
   `mkdir -p /srv/node/sdc`
   `mount /srv/node/sdc`
   `mkdir -p /srv/node/sdd`
   `mount /srv/node/sdd`
   `chown -R swift:swift /srv/node`
What to do next

You can now create the rsyncd.conf file to enable the rsync service. See “Enable the rsync Service,” on page 58.

Enable the rsync Service

To enable the rsync service for the Object Storage service, you must create the /etc/rsyncd.conf file, modify the default rsync configuration, and manually start the rsync service.

Procedure

1. If you are logged out, log back in to the Object Storage service.
   a. Using SSH, log in to the VMware Integrated OpenStack manager.
   b. From the VMware Integrated OpenStack manager, use SSH to log in to the controller01 node.
   c. Switch to root user.
      
      ```
sudo su -
      ```

2. Create the /etc/rsyncd.conf file.

   **Note**

   ```
   uid = swift  
gid = swift  
log file = /var/log/rsyncd.log  
pid file = /var/run/rsyncd.pid  
address = controller01 NODE IP ADDRESS  
[account]  
max connections = 2  
path = /srv/node/  
read only = false  
lock file = /var/lock/account.lock  
[container]  
max connections = 2  
path = /srv/node/  
read only = false  
lock file = /var/lock/container.lock  
[object]  
max connections = 2  
path = /srv/node/  
read only = false  
lock file = /var/lock/object.lock
   ```

3. For the address setting, provide the IP address of the controller01 node.

4. Change the RSYNC_ENABLE setting in the /etc/default/rsync file to true.

   ```
   RSYNC_ENABLE=true
   ```

5. Start the rsync service.

   ```
   service rsync start
   ```

6. Create the swift rcon cache directory

   ```
   mkdir -p /var/swift/recon  
   chown -R swift:swift /var/swift/recon
   ```
What to do next

You can now configure and start the Object Storage proxy service. See “Configure the Object Storage Proxy Server,” on page 59.

Configure the Object Storage Proxy Server

The proxy server takes each request for an object and looks up locations for the account, container, or object, and routes the requests correctly. The proxy server also handles API requests.

Procedure

1. If you are logged out, log back in to the Object Storage service.
   a. Using SSH, log in to the VMware Integrated OpenStack manager.
   b. From the VMware Integrated OpenStack manager, use SSH to log in to the controller01 node.
   c. Switch to root user.
      ```
      sudo su -
      ```
2. Create the `/etc/swift/proxy-server.conf` file.
   Enter the internal VIP in the commands.
   Configure the bind_port parameter according to your deployment mode.
   - For full deployments, set the bind_port parameter to 8080.
   - For compact mode deployments, set the bind_port parameter to a value within the defined local port range of the host.
   ```
   [DEFAULT]
   bind_port = BINDPORT
   user = swift
   swift_dir = /etc/swift
   
   [pipeline:main]
   pipeline = catch_errors gatekeeper healthcheck proxy-logging container_sync bulk \ 
   ratelimit authtoken keystonemiddleware.container-quotas account-quotas slo dlo \ 
   versioned_writes proxy-logging proxy-server
   
   [app:proxy-server]
   use = egg:swift#proxy
   account_autocreate = True
   
   [filter:tempauth]
   use = egg:swift#tempauth
   user_admin_admin = admin .admin .reseller_admin
   user_test_tester = testing .admin
   user_test2_tester2 = testing2 .admin
   user_test_tester3 = testing3
   user_test5_tester5 = testing5 service
   
   [filter:authtoken]
   paste.filter_factory = keystonemiddleware.auth_token:filter_factory
   auth_uri = http://INTERNAL_VIP:5000
   auth_url = http://INTERNAL_VIP:35357
   auth_type = password
   project_domain_name = local
   user_domain_name = local
   ```
project_name = admin
username = swift
password = password
delay_auth_decision = True

[filter:keystoneauth]
use = egg:swift#keystoneauth
operator_roles = _member_, admin

[filter:healthcheck]
use = egg:swift#healthcheck

[filter:cache]
use = egg:swift#memcache

[filter:ratelimit]
use = egg:swift#ratelimit

[filter:domain_remap]
use = egg:swift#domain_remap

[filter:catch_errors]
use = egg:swift#catch_errors

[filter:cname_lookup]
use = egg:swift#cname_lookup

[filter:staticweb]
use = egg:swift#staticweb

[filter:tempurl]
use = egg:swift#tempurl

[filter:formpost]
use = egg:swift#formpost

[filter:name_check]
use = egg:swift#name_check

[filter:list-endpoints]
use = egg:swift#list_endpoints

[filter:proxy-logging]
use = egg:swift#proxy_logging

[filter:bulk]
use = egg:swift#bulk

[filter:slo]
use = egg:swift#slo

[filter:dlo]
use = egg:swift#dlo

[filter:container-quotas]
What to do next

You can now create and configure the Object Storage rings. See “Create and Configure Object Storage Rings,” on page 61.

Create and Configure Object Storage Rings

Rings connect the account, container, and object services. Rings also provide load balancing and failover for services that are running on multiple nodes.

Procedure

1. If you are logged out, log back in to the controller01 node.
   a. Using SSH, log in to the VMware Integrated OpenStack manager.
   b. From the VMware Integrated OpenStack manager, use SSH to log in to the controller01 node.
   c. Switch to root user.
      ```
      sudo su -
      ```

2. Create the account, container, and object rings.
   ```
   cd /etc/swift
   swift-ring-builder account.builder create 18 3 1
   swift-ring-builder container.builder create 18 3 1
   swift-ring-builder object.builder create 18 3 1
   ```

3. Add a storage device to each ring.
   ```
   swift-ring-builder account.builder add --region 1 --zone 1 --ip controller01_node_IP_address
   --port 6002 --device sdb --weight 100
   swift-ring-builder account.builder add --region 1 --zone 1 --ip controller01_node_IP_address
   --port 6002 --device sdc --weight 100
   swift-ring-builder account.builder add --region 1 --zone 1 --ip controller01_node_IP_address
   --port 6002 --device sdd --weight 100
   ```
```
controller01_node_IP_address \
   --port 6001 --device sdc --weight 100
swift-ring-builder container.builder add --region 1 --zone 1 --ip
controller01_node_IP_address \
   --port 6001 --device sdd --weight 100
swift-ring-builder object.builder add --region 1 --zone 1 --ip controller01_node_IP_address \
   --port 6000 --device sdb --weight 100
swift-ring-builder object.builder add --region 1 --zone 1 --ip controller01_node_IP_address \
   --port 6000 --device sdc --weight 100
swift-ring-builder object.builder add --region 1 --zone 1 --ip controller01_node_IP_address \
   --port 6000 --device sdd --weight 100
```

4 Verify the ring contents for each ring.
   swift-ring-builder account.builder
   swift-ring-builder container.builder
   swift-ring-builder object.builder

5 Rebalance the rings.
   swift-ring-builder account.builder rebalance
   swift-ring-builder container.builder rebalance
   swift-ring-builder object.builder rebalance

6 Ensure that the swift user owns all of the configuration files.
   chown -R swift:swift /etc/swift

**Start the Swift Services**

After you create and modify the configuration files, you can start the Object Storage service.

**Procedure**

1 If you are logged out, log back in to the controller01 node.
   a Using SSH, log in to the VMware Integrated OpenStack manager.
   b From the VMware Integrated OpenStack manager, use SSH to log in to the controller01 node.
   c Switch to root user.
      sudo su -

2 Start the Object Storage service.
   service swift-proxy start

3 Start the swift account, container, and object service.
   swift-init all start

**Test the Object Storage Configuration**

After you start the Object Storage service, you can test the Object Storage configuration.

**Procedure**

1 Get current status.
   swift stat -v

2 Create a directory.
   swift post directory_name
Configure the Ceilometer Component

Ceilometer is the telemetric component of OpenStack that collects and persists data regarding the use of the physical and virtual resources in your OpenStack deployment.

You can enable Ceilometer after completing the VMware Integrated OpenStack deployment.

Procedure

1. In vCenter, select Home > VMware Integrated OpenStack > Manage.
2. Select the Settings tab.
3. Click Ceilometer.
4. Click Edit to modify the settings.
5. Select the Configure Ceilometer option.
6. Click OK to configure Ceilometer.

The vSphere Web Client might take a few minutes to update the OpenStack configuration.

Ceilometer is automatically enabled the first time you configure it. Afterwards, the Ceilometer settings show only Enable and Disable options.

Adding Capacity in vSphere Web Client

You can add compute clusters and datastores to an existing VMware Integrated OpenStack deployment.

Add a New Compute Cluster

You can increase the number of compute clusters in your VMware Integrated OpenStack deployment to increase CPU capacity.

Prerequisites

Prepare a cluster with at least one host.

Procedure

1. In vCenter, select Home > VMware Integrated OpenStack > Manage.
2. Select the Nova Compute tab.
3. Click the green plus-sign icon (+) at the top of the panel.
4 In the Add Nova cluster page of the Add Cluster to OpenStack dialog box, select the cluster you prepared as a prerequisite, and click Next. The cluster you select must contain at least one host.

5 On the Review proposed configuration page, select the existing management VM, and click Next.

6 Select the datastores for the tenants in the new cluster, and click Next.

7 Review the proposed configuration, and click Finish.

8 Confirm that the new cluster is added to the OpenStack deployment. The newly added cluster appears in the Nova Compute tab.

OpenStack capacity increases based on the resources available in the additional cluster.

**Add Storage to the Compute Node**

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

Adding a datastore to the Compute node causes the Nova service to restart, which might cause a temporary disruption to the OpenStack services in general.

**Prerequisites**

Verify that you have datastores available. See the vSphere Web Client documentation.

**Procedure**

1 In vCenter, select Home > VMware Integrated OpenStack > Manage.

2 Click the Nova Storage tab. This tab displays the datastores that are currently available, their status, and other details.

3 Click the green plus-sign icon (+) at the top of the panel.

4 On the Select a Nova node page of the Add Nova Datastores dialog box, select the cluster to which you want to add a datastore, and click Next.

5 On the Add Nova datastore page, select one or more datastores to add to the cluster, and click Next.

6 Review the proposed configuration, and click Finish.

The storage capacity for the selected Compute node increases accordingly with the size of the additional datastore.

**Add Storage to the Image Service**

You can increase the number of datastores available to the Image Service node in your VMware Integrated OpenStack deployment.

Adding a datastore to the Image Service node causes the Glance service to restart, which might cause a temporary disruption to the OpenStack services in general.

**Prerequisites**

Verify that you have datastores available. See the vSphere Web Client documentation.

**Procedure**

1 In vCenter, select Home > VMware Integrated OpenStack > Manage.
2 Click the **Glance Storage** tab.
   This tab displays the datastores that are currently available, their status, and other details.
3 Click the green plus-sign icon (+) at the top of the panel.
4 On the Add Glance datastore page, select one or more datastores to add to the cluster, and click **Next**.
5 Review the proposed configuration, and click **Finish**.

The storage capacity for the Image Service node increases accordingly with the size of the additional datastore.
Index

A
about this guide 5
architecture
   NSX 13
   VDS 21
available languages 9

C
capacity, adding 63
   Ceilometer, configuring clusters
      adding 63
      configuring 29
   compact mode 27
   components, adding 63
   Compute cluster, adding 63
   configuration, monitoring 46
   Customer Experience Improvement Program 11

D
default domain 47
deploying, a new OpenStack instance 37, 54
deployment, monitoring 46

E
   Endpoint Operations Management integration 53
   ESXi host requirements
      for NSX deployments 17
      for VDS deployments 25

F
   firewall, configuring 29
   firewall protection, removing VMs from 45
   firewall requirements
      for NSX deployments 17
      for VDS deployments 25

I
   implementation overview 9
   installation 35
   installing 37
   integration
      Endpoint Operations Management agent 53
      vRealize Operations Manager 53
   internationalization 9
   internationalization and localization 10

L
   LBaaS
      configuring 49
      enabling 49
      testing 49
   LBaaS v2
      configuring 49
      enabling 49
      testing 49
   Load Balancing as a Service, See LBaaS
   localization 9, 10
   loopback device 57

N
   networking, VLAN requirements 18, 25
   networks, setting up 29
   NSX, compared to VDS deployment 11
   NSX deployments, preparing for 13

O
   Object Storage
      configuring 56, 59
      deploying 55
      loopback device 57
      ring configuration 61
      starting 58, 62
      swift.conf file 56
      testing 62
   Object Storage component
      adding post-installation 54
      setting up environment 54
   OpenStack Foundation, compliance 9
   OpenStack components
      Compute cluster 63
      Compute storage 64
      Image Service storage 64
      Object Storage 54
   OpenStack Manager, deploying in vSphere 35

P
   post-installation configuration 49
   product overview 9
   provider network 46

R
   registering the vApp 36
software requirements for NSX deployments
ESXi host requirements for NSX deployments 17
firewall requirements for NSX deployments 17
vSphere requirements 17
software requirements for VDS deployments
ESXi host requirements for VDS deployments 25
firewall requirements for VDS deployments 25
vSphere requirements 25
special character support 10
storage
adding to Glance node 64
adding to Nova node 64
Object Storage component 54
system overview 9
system requirements
hardware 16, 24
hardware requirements for VDS deployments 24, 27
networking 16, 24
NSX 17
NSX hardware requirements 16
software 16, 24
software requirements 17, 25

telemetrics 63

unicode UTF-8 10
updated information 7

vApp, registering 36
vCenter
configuring for compact mode 29
configuring for NSX 31
configuring for VDS 30
preparing 29
VDS
compared to NSX deployment 11
limitations 21
VDS deployments, preparing for 21
vRealize Operations Manager integration 53
vSphere requirements
for NSX deployments 17
for VDS deployments 25