VMware Integrated OpenStack Installation and Configuration Guide

Modified on 19 SEP 2017

VMware Integrated OpenStack 4.0

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

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

Contents

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.

About VMware Integrated OpenStack 1

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 4.x is based on the Ocata release of OpenStack.

This chapter includes the following topics:

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 Licensing

After you install VMware Integrated OpenStack, it remains in evaluation mode for 60 days until you install a VMware Integrated OpenStack license key.

After the evaluation license expires, all NFV features are disabled, you can not add vCenter Server instances, and run vRealize Automation workflows, until you obtain and assign a valid VMware Integrated OpenStack license key. Obtain and assign VMware Integrated OpenStack license keys as soon as possible after installing VMware Integrated OpenStack.

VMware Integrated OpenStack licenses allow you to use different functionalities as per the license type that you select. To obtain VMware Integrated OpenStack license keys, go to the VMware Integrated OpenStack Product Licensing Center at https://www.vmware.com/products/openstack.html, or contact your VMware sales representative.

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.

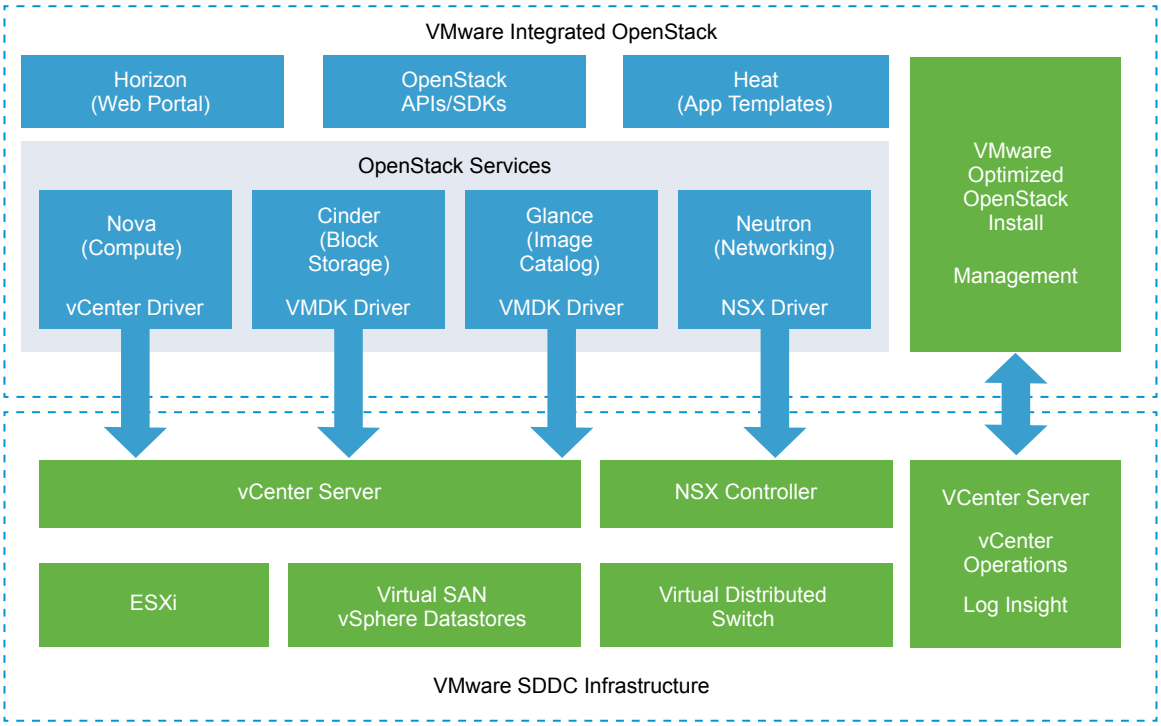
VMware Integrated OpenStack is implemented as compute and management clusters in your vSphere environment.

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.

Supported Feature	VDS Mode	NSX Mode
Provider Networks leveraging VLANs	Yes	Yes
API/Management Plane High Availability	Yes	Yes
DC-Wide Control Plane Scale	Limited	High
Layer 3/NAT High Availability & Scale	No	Yes
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	No	Yes
Enterprise Features ■ Micro-segmentation with line-rate Stateful distributed firewall ■ Provider-side security via Service Insertion ■ In-kernel distributed routing	No	Yes
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

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.

VMware Integrated OpenStack Deployments with NSX 2

You can deploy VMware Integrated OpenStack using NSX for the Neutron networking component.

This chapter includes the following topics:

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.

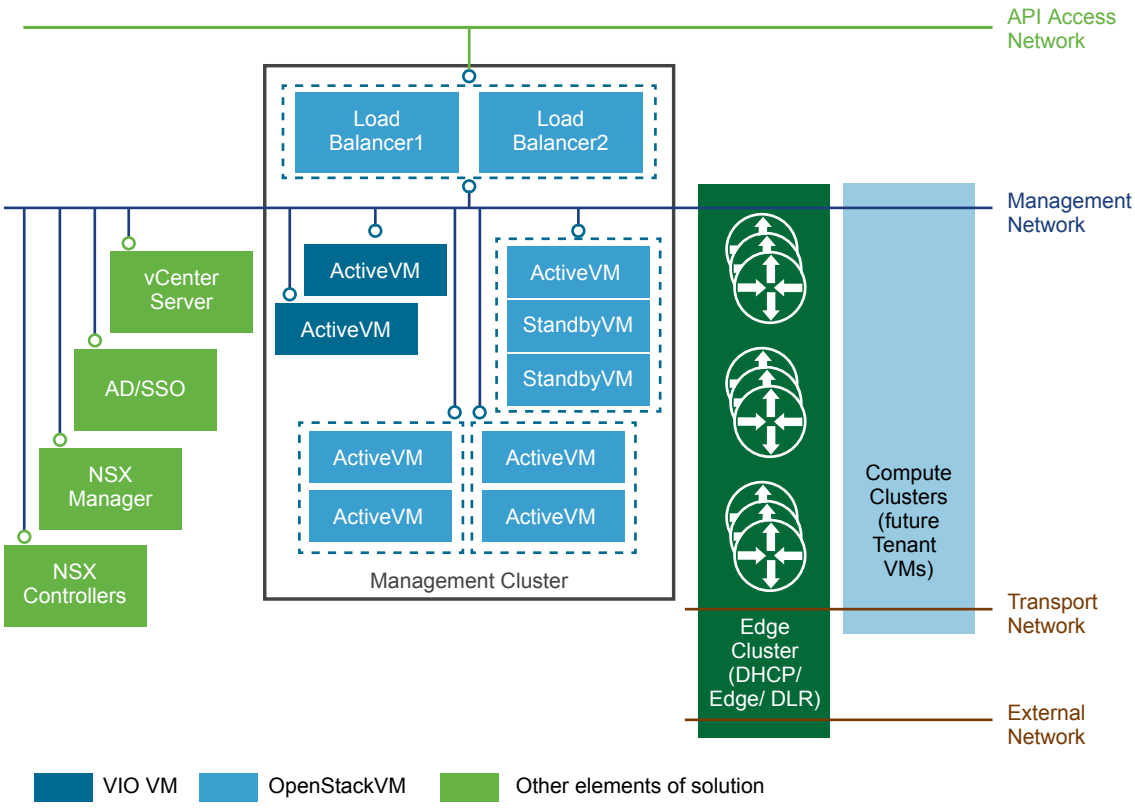
Cluster and Component Architecture

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 16.

Figure 2-1. NSX deployment in HA mode



The VMware Integrated OpenStack architecture includes the following clusters and components.

Cluster or Component	Description
vCenter instance	A dedicated vCenter instance is not required but optimizes deployment.
Active Directory	For user authentication by the OpenStack Identity Service.
Management cluster	Contains all the deployed OpenStack component and management VMs. See "Management Cluster," on page 20 below for a detailed description of the management cluster and its components.
Compute cluster	Compute resources for Nova. All tenant VMs are created on these compute clusters.
NSX Edge cluster	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.
NSX Manager	The centralized network management component of NSX that provides an aggregated system view.
NSX Controllers	An advanced distributed state management system that controls virtual networks and overlay transport tunnels.
Management network	Carries traffic among the management components.
API access network	Exposes the VMware Integrated OpenStack dashboard and provides access for tenants to the OpenStack APIs and services.
Transport network	Connects the DHCP nodes in the Edge cluster with the compute clusters.
External Network	Provides external access for the instances created in VMware Integrated OpenStack.

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

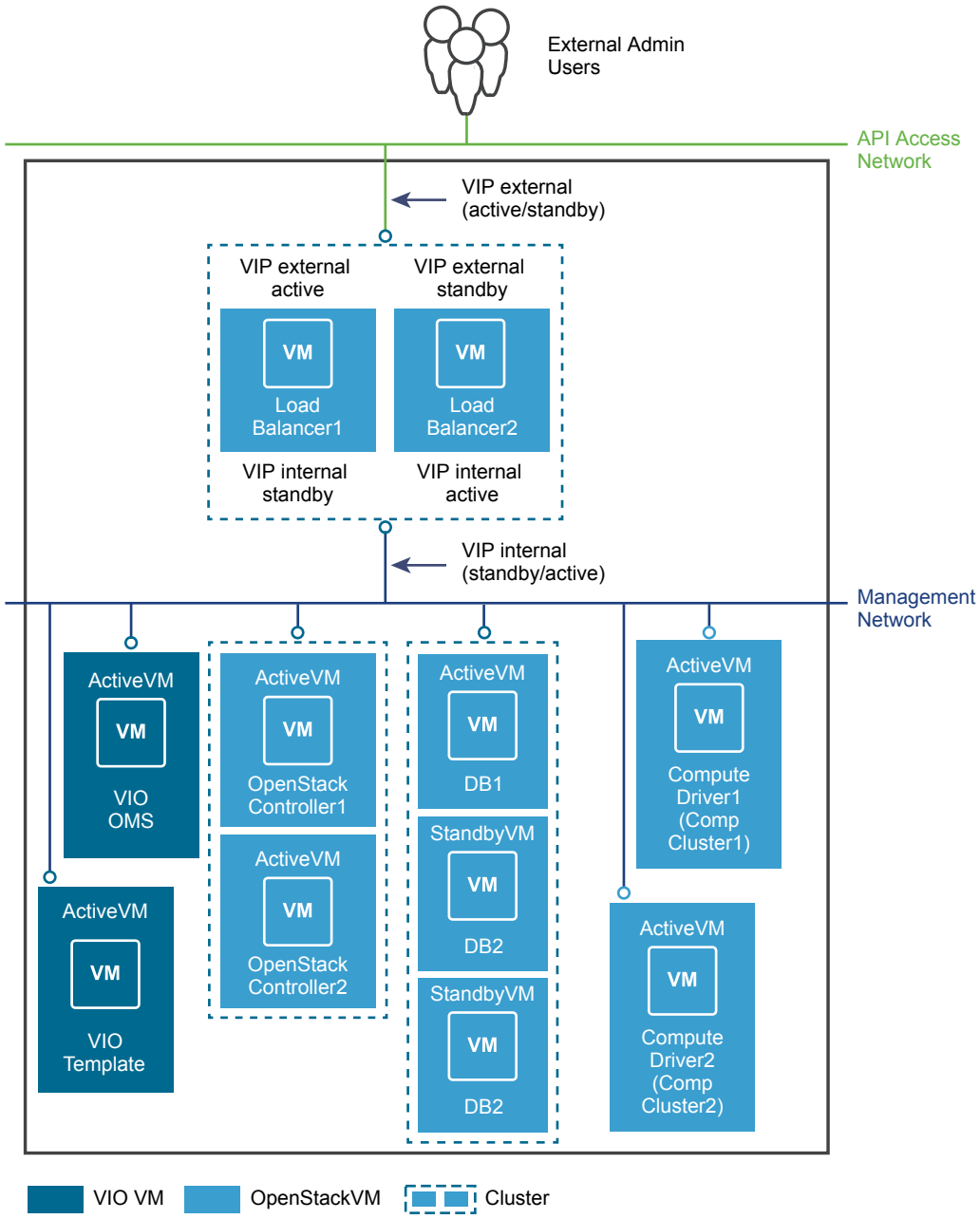


Figure 2-3. Management cluster in compact mode (to be provided)

The management cluster contains the following components.

Component	Description	Nodes
Load Balancers	Provide HA and enable horizontal scale-out architecture.	2 (1 active, 1 standby)
Databases (DBs)	Instances of MariaDB that store the OpenStack metadata. RabbitMQ, the message queue service used by all OpenStack services, also runs on the database nodes.	3 (1 active, 2 standby)
VMware Integrated OpenStack Controller	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.	2 (both active)
Compute Driver	Contains a subset of Compute processes that interact with the compute clusters to manage VMs.	1 per compute cluster
VMware Integrated OpenStack Manager Service (OMS)	The vApp that you use to manage your VMware Integrated OpenStack vApp.	1
VMware Integrated OpenStack Template	Base template for creating all OpenStack service VMs.	1
Ceilometer Databases (optional)	Instances of MongoDB or NoSQL databases for use by Ceilometer.	3 (1 active, 2 standby)

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

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

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 52.

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

Component	VMs	vCPU	vRAM (GB)	vDisk Space (GB)
NSX Controller	3	12 (4 per VM)	12 (4 per VM)	60 (20 per VM)
NSX Manager	1	4 (4 per VM)	12 (12 per VM)	60 (60 per VM)
NSX Edge (see note below)	Varies: created on demand.	1 per Edge DHCP VM, 2 per Edge router VM	0.5 per Edge DHCP VM, 1 per Edge router VM	0.5 per Edge DHCP VM, 1 per Edge router VM
TOTAL	4 plus Edge requirements	16 plus Edge requirements	24 plus Edge requirements	120 plus Edge requirements

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.

Requirement	Description
vSphere version	■ Supported versions: See the VMware Product Interoperability Matrix at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php for the supported versions.
ESXi hosts	■ Supported versions: See the VMware Product Interoperability Matrix at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php for the supported versions. ■ Eight or more logical processors on each host. ■ 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/kb/1003063 and the vSphere documentation at Edit Time Configuration for a Host.
NSX	NSX Advanced or Enterprise license. See the VMware Product Interoperability Matrix at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php for the preferred version.
OpenStack python-heatclient	OpenStack Ocata version. See https://launchpad.net/python-heatclient/ocata.

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.

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

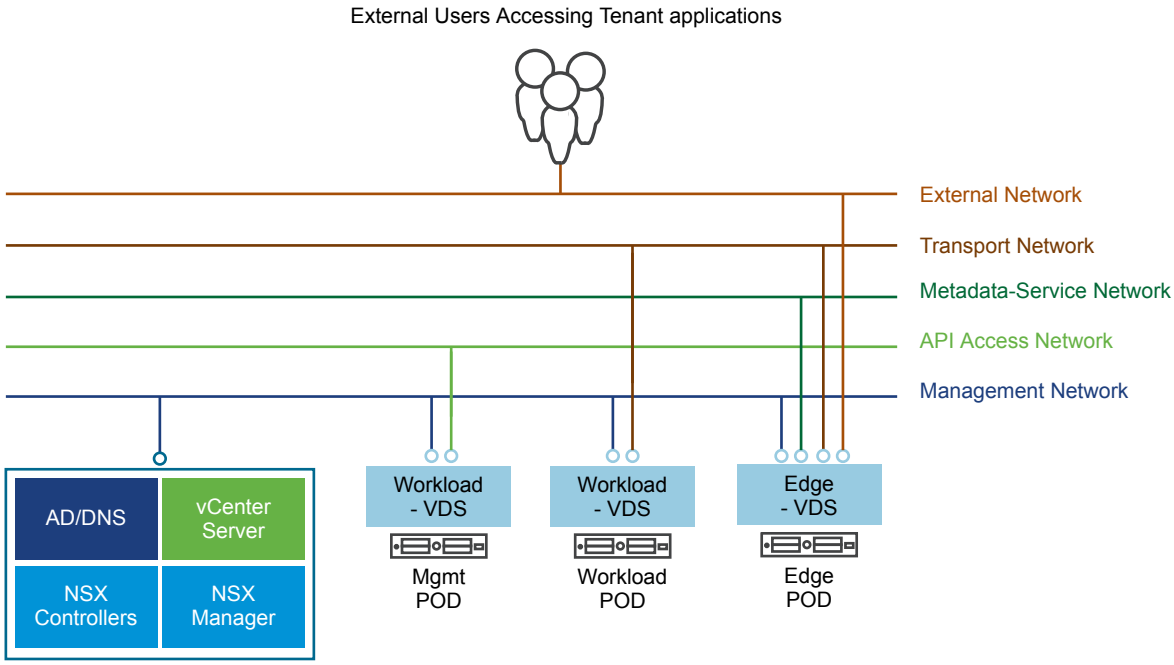
VLAN	Description
API Access network	Provides access for users to the OpenStack services through APIs or the VMware Integrated OpenStack dashboard. ■ Trunk all hosts in the Management cluster to this VLAN. ■ Make externally accessible. ■ Requires five or more continuous IP addresses.
External	Provides external user access to the instances. ■ Trunk all hosts in the NSX Edge cluster to this VLAN.

VLAN	Description

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.
	■ Requires 18 or more continuous IP addresses. (21 if you add the Ceilometer component.)
	■ Enable L2 or L3 access to this VLAN for the following components:
	  ■ vCenter server
	  ■ NSX Manager
	  ■ NSX Controller
	If you are deploying the NSX Manager and NSX Controller VMs on the Management cluster, you must trunk their hosts to the Management network.

Metadata-service	The metadata-service network enables new OpenStack instances to access and run customization scripts made available by the Nova metadata service, which is hosted by the OpenStack controllers.
Transport	Carries traffic among the OpenStack instances. ■ Trunk all hosts in the Compute cluster to this VLAN. ■ Trunk all hosts in the NSX Edge cluster to this VLAN. **IMPORTANT** The Maximum Transmission Unit (MTU) settings for the Transport VLAN must be configured to support 1600 bytes. See the Knowledge Base at http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2093324.

Figure 2-4. Network Map for NSX Deployments



VMware Integrated OpenStack Deployments with VDS 3

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

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.

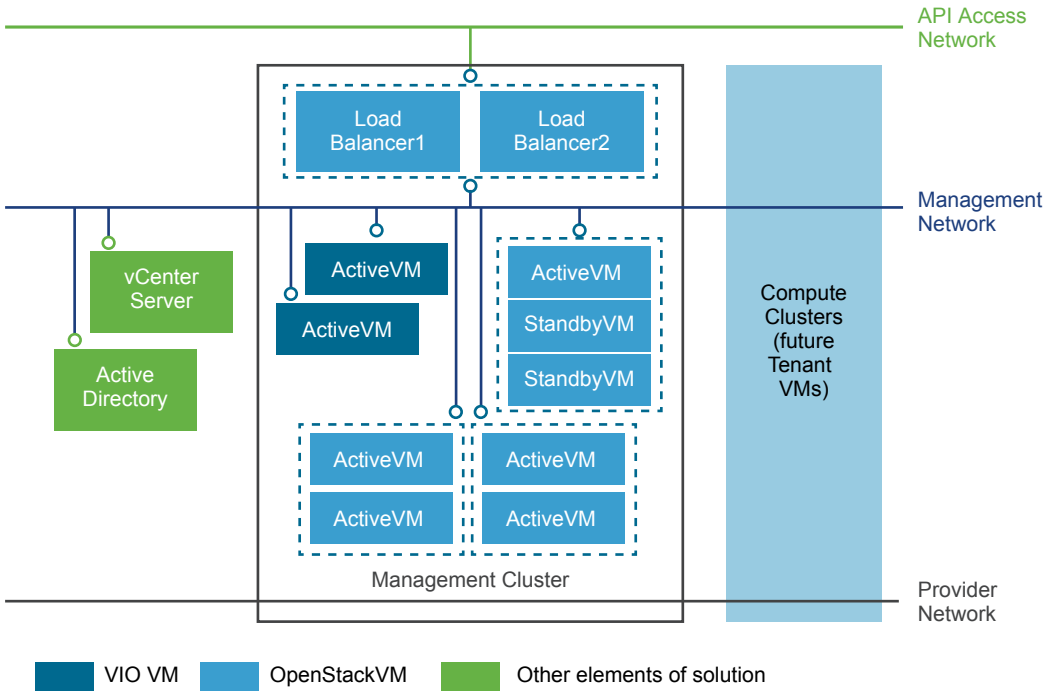
If such features are important for your VMware Integrated OpenStack deployment, consider using NSX for Neutron networking.

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 23.



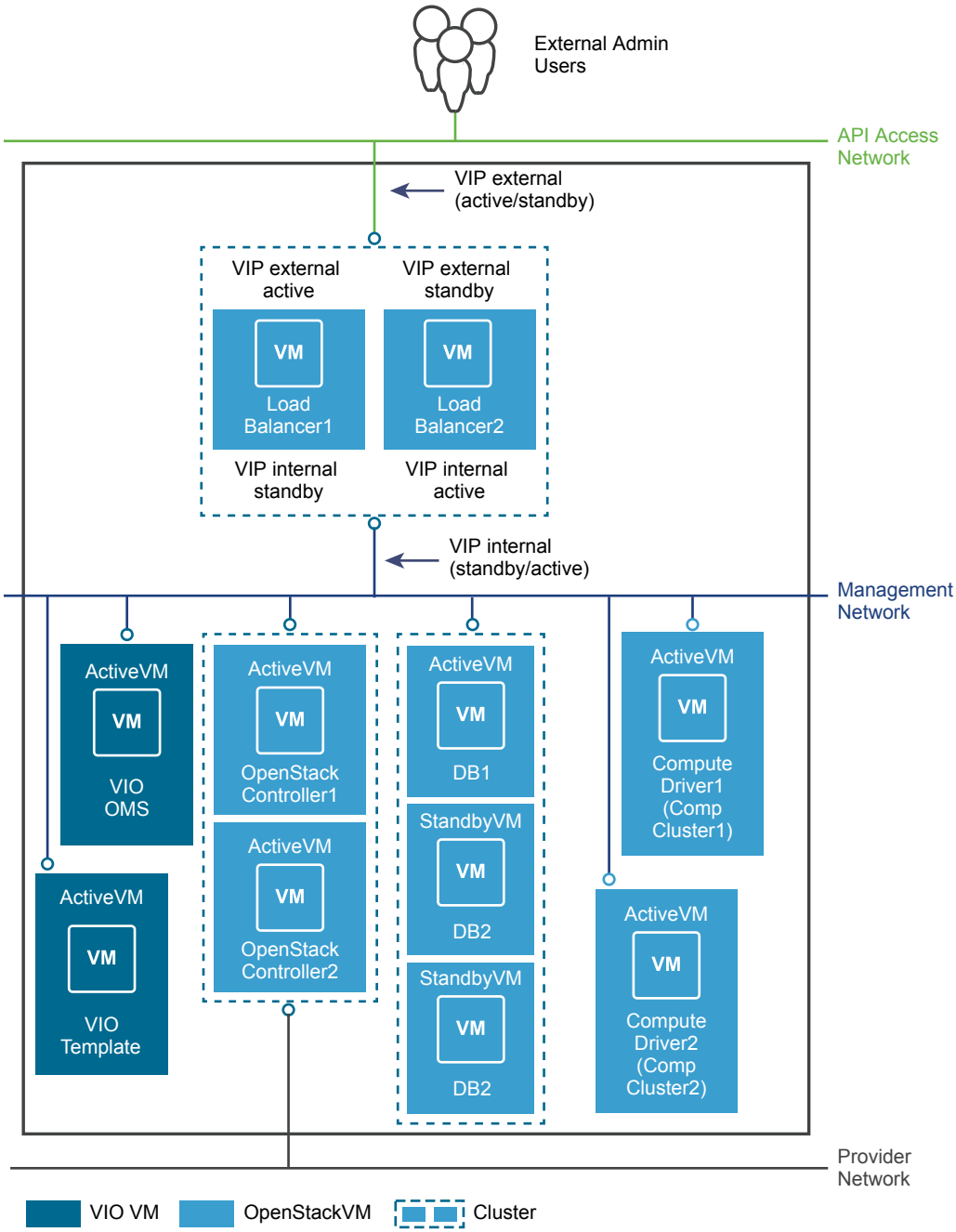
The VMware Integrated OpenStack architecture includes the following clusters and components.

Cluster or Component	Description
vCenter instance	Configure a vCenter dedicated to your VMware Integrated OpenStack deployment. This is not required but optimizes deployment.
Active Directory	For user authentication by the OpenStack Identity Service.
Management cluster	Contains all the deployed OpenStack component and management VMs. See the "Management Cluster," on page 20 below for a detailed description of the management cluster and its components.
Compute cluster	Compute resources for Nova. All tenant VMs are created on these compute clusters.
Management network	Carries traffic among the management components.
API access network	Exposes the VMware Integrated OpenStack dashboard and provides access for tenants to the OpenStack APIs and services.
Provider network	Connects the DHCP nodes in the management cluster with the compute clusters. See "Management Cluster," on page 20 below.

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.

Component	Description	Nodes
Load Balancers	Provide HA and enable horizontal scale-out architecture.	2 (1 active, 1 standby)
Databases (DBs)	Instances of MariaDB that store the OpenStack metadata. RabbitMQ, the message queue service used by all OpenStack services, also runs on the database nodes.	3 (1 active, 2 standby)
VMware Integrated OpenStack Controller	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.	2 (both active)

Component	Description	Nodes
DHCP	Provide IP addresses to the instances connected to the Provider network.	2 (both active)
Compute Driver	Contains a subset of Compute processes that interact with the compute clusters to manage VMs.	1 per compute cluster
VMware Integrated OpenStack Manager Service (OMS)	The vApp that you use to manage your VMware Integrated OpenStack vApp.	1
VMware Integrated OpenStack Template	Template for redeploying failed OpenStack deployments. This template preserves the configuration settings to facilitate redeployment.	1

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

Component	VMs	vCPU	vRAM (GB)	vDisk Space (GB)
Integrated OpenStack Manager	1	2 (2 per VM)	4 (4 per VM)	25
Load balancing service	2	4 (2 per VM)	8 (4 per VM)	40 (20 per VM)
Database service	3	12 (4 per VM)	48 (16 per VM)	240 (80 per VM)
Controllers	2	16 (8 per VM)	32 (16 per VM)	160 (80 per VM)
Compute service (Nova CPU)	1	2 (2 per VM)	4 (4 per VM)	20 (20 per VM)
DHCP service	2	8 (4 per VM)	32 (16 per VM)	40 (20 per VM)
Ceilometer	1	2 (2 per VM)	4 (4 per VM)	20 (20 per VM)
Database (MongoDB or NoSQL) for Ceilometer	3	6 (2 per VM)	12 (4 per VM)	60 (20 per VM)
TOTAL	15	52	144	605

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 52.

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.

Requirement	Description
vSphere version	Supported versions: ■ vSphere 6 Update 1 Enterprise Plus ■ vSphere 6 Enterprise Plus ■ vSphere 5.5 Update 3 Enterprise Plus ■ vSphere 5.5 Update 2 Enterprise Plus

ESXi hosts	■ Supported versions:
	  ■ Version 6.0 Update 1
	  ■ Version 6.0
	  ■ Version 5.5 Update 3
	  ■ Version 5.5 Update 2
	■ Eight or more logical processors on each host.
	■ 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.

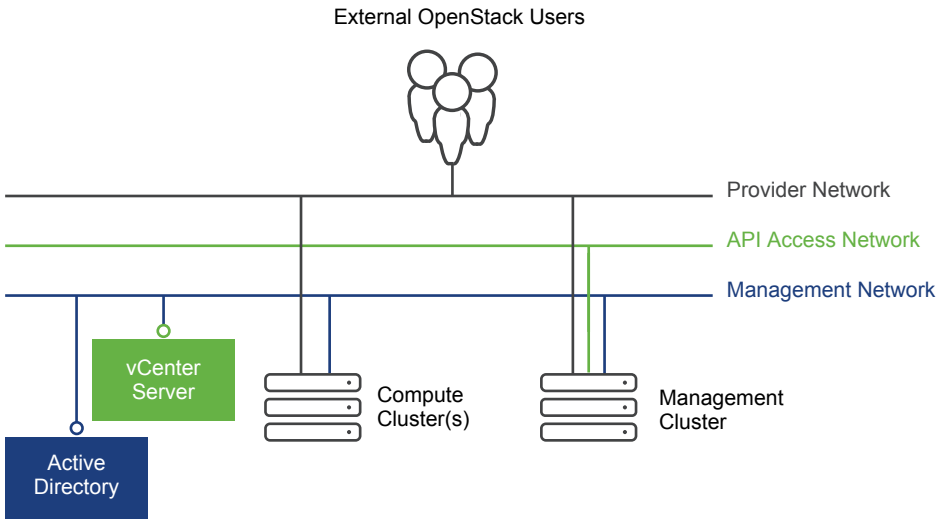
Physical VDS Network Overview

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

Request your network administrator to prepare the following VLANs.

VLAN	Description
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



VMware Integrated OpenStack Deployment in Compact Mode

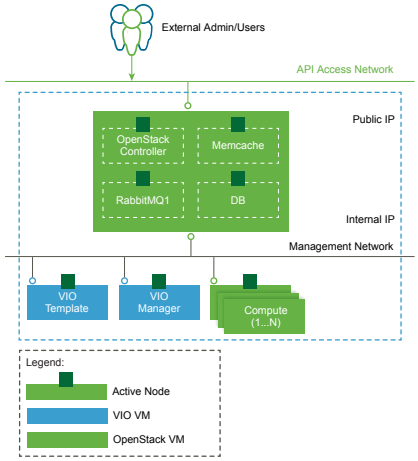
4

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

Component	VMs	vCPU	vRAM (GB)	vDisk Space (GB)
Integrated OpenStack Manager	1	2 (2 per VM)	4 (4 per VM)	25
Controllers, Compute service (Nova CPU)	1	8 (8 per VM)	16 (16 per VM)	80 (80 per VM)
TOTAL	2	10	20 GB	120 GB

If you install Ceilometer, additional resources are required.

Table 4-1. Additional requirements for Ceilometer

Component	VMs	vCPU	vRAM (GB)	vDisk Space (GB)
Ceilometer	1	2 (2 per VM)	4 (4 per VM)	20 (20 per VM)
Database (MongoDB or NoSQL) for Ceilometer	3	6 (2 per VM)	12 (4 per VM)	60 (20 per VM)
TOTAL	4	8	16	80

Preparing the Dedicated vCenter Instance 5

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 9

.

This chapter includes the following topics:

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.

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

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 23.

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.

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

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 16.

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.

Installing VMware Integrated OpenStack 6

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

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 28.

- Install and configure vSphere. See "VMware Integrated OpenStack System Requirements," on page 14.
- 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 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 the vSphere Web Client 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 34.

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 35.

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 28.

Verify that the Integrated OpenStack Manager OVA was correctly deployed. See "Deploy the VMware Integrated OpenStack OVA in the vSphere Web Client," on page 33.

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.

Option	Description
Use this wizard to configure a new OpenStack instance	Deploys and configures a new OpenStack instance. You will require all the prerequisite information: network configurations, clusters, datastores, and so on.
Use an exported template to pre-fill configuration settings in this wizard	Populates the deployment wizard with settings by using a JSON template exported from an existing VMware Integrated OpenStack deployment.
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.

Option	Description
Deployment name	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.
Use management vCenter Server as Compute vCenter Server	Select this option to deploy on multiple vCenter servers. This option is supported on NSX deployments only.
Management vCenter Server	Enter the IP address or FQDN value for the vCenter instance to which the OpenStack management server is connected.
Username	Enter the username for the vCenter Server administrator.
Password	Enter the password for the vCenter Server administrator.
Ignore the vCenter Server certificate validation	Select this option to ignore the vCenter Server certificate validation.

VMware Integrated OpenStack requires this authorization to access the vCenter Server for management services.

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

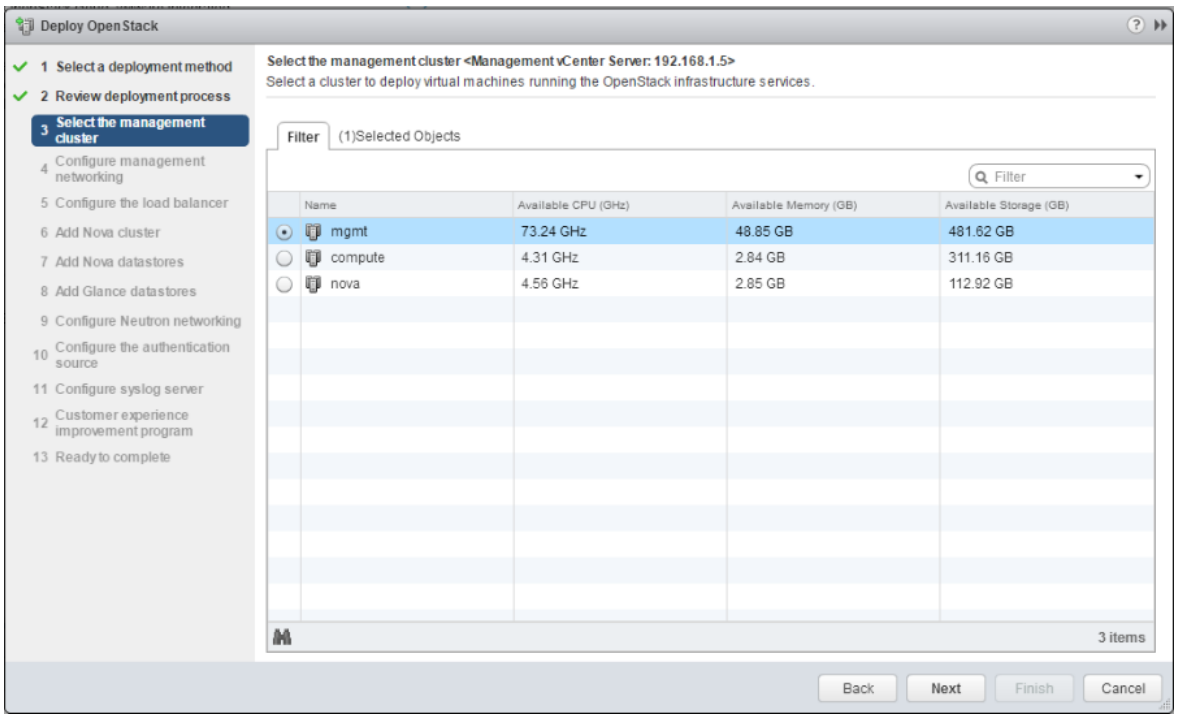
6 Click **Next**.

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



8 Click **Next**.

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

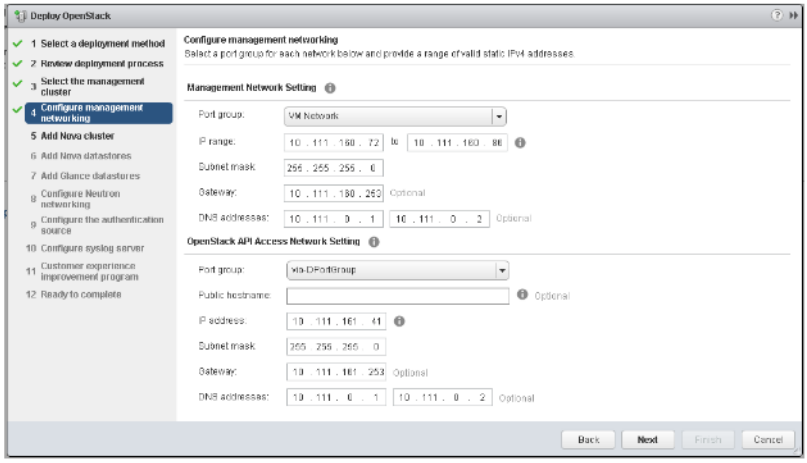
You prepared the network settings and resources in advance. The Management network connects the OpenStack Manager and all OpenStack VMs with the vCenter Server. If applicable, all NSX Controller nodes also connect to this network. The API Access network is for user access to the OpenStack APIs and the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

Setting	Description
Port group	Select a port group you configured in preparation for the VMware Integrated OpenStack deployment.
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.
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.

Setting	Description
Gateway	Provide the gateway address..
DNS addresses	Provide the addresses for the domain name servers.

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.

Option	Description
Public hostname	FQDN value of the public VIP.
Public Virtual IP	Public VIP address.

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

12 Click **Next**.

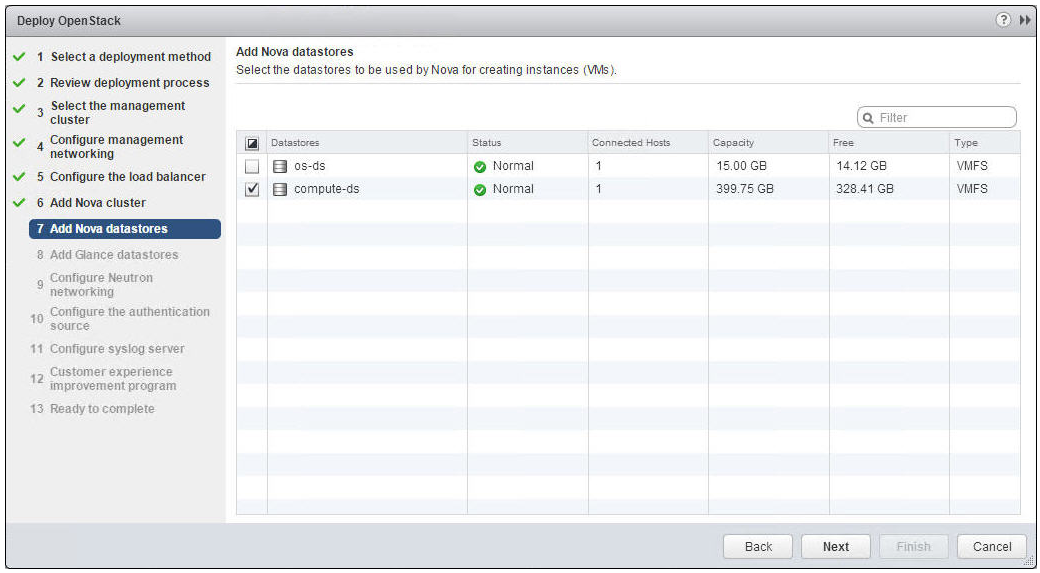
13 Select the cluster for the Nova (Compute) component.

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**.

17 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.

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

18 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.

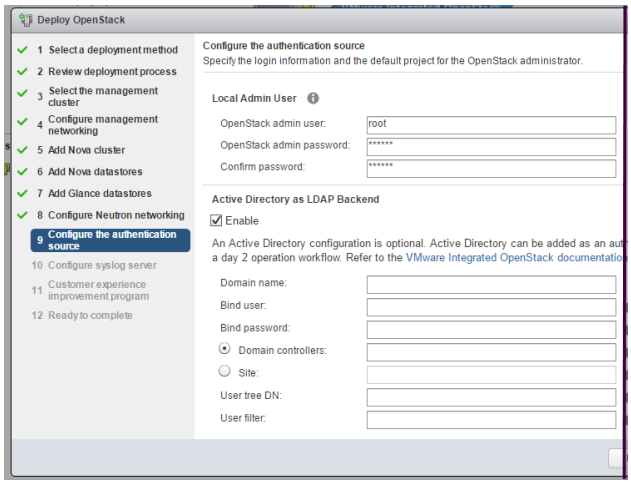
Option	Description
OpenStack admin user	Define the OpenStack administrative user name. This is the default administrative user name for logging in to the VMware Integrated OpenStack dashboard.
OpenStack admin password	Define the OpenStack administrative user password. This is the default administrative user password for logging in to the VMware Integrated OpenStack dashboard.
Confirm password	Reenter the password for confirmation.

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

Option	Description
Domain Name	Specify the full Active Directory domain name; for example, vmware.com.
Bind user	Provide the user name to bind to Active Directory for LDAP requests.
Bind password	Provide the password to allow the LDAP client access to the LDAP server.
Domain controllers	(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 controller**s radio button and then enter the IP address of one or more domain controllers, separated by commas.
Site	(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.
User Tree DN	(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.
User Filter	(Optional) Enter an LDAP search filter for users.

Option	Description
	Important If your directory contains more than 1,000 objects (users and groups), you must apply a filter to ensure that fewer than 1,000 objects are returned. For examples of filters, see https://msdn.microsoft.com/en-us/library/aa746475(v=vs.85).aspx.

Figure 6-4. Configure authentication source



c Click **Next**.

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 10.

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 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 45.

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 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

Option	Description
Name	Enter a name for the network.
Project	Select the default admin project from the drop-down menu.
Provider Network Type	Select **VLAN** from the drop-down menu.
Physical Network	Enter **dvs**.
Segmentation ID	Enter the ID of the Provider VLAN. Contact your network administrator for this value.

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 -
```

3 Execute the `cloudadmin_v3.rc` file.

```
$ 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
```

Parameter	Description
`--os-identity-api-version 3`	Specifies the API version, in this case, version **3**.
`--os-username admin`	Provides the administrative username for login, in this case **admin**.
`--os-user-domain-name local`	Specifies the domain, in this case **local** for the specified user.
`--os-project-name admin`	Specifies the admin OpenStack project.
`--os-password admin`	Provides the administrative password for login, in this case **admin**.
`--os-region-name nova project create`	Runs the `nova project create` command.
`--domain default`	This command specifies the domain where the new project is created, in this case the **default** domain.
`--description "Demo Project"`	This parameter names the new project, in this case **Demo Project**.
`--or-show demo`	Creates an alias for the new project.

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
```

Parameter	Description
`--os-identity-api-version 3`	Specifies the API version, in this case, version **3**.
`--os-username admin`	Provides the administrative username for login, in this case **admin**.
`--os-user-domain-name local`	Specifies the domain, in this case **local** for the specified user.
`--os-project-name admin`	Specifies the admin OpenStack project.
`--os-password admin`	Provides the administrative password for login, in this case **admin**.
`--os-region-name nova role add`	Runs the `nova role add` command.
`--project demo`	Specifies the project to which the new administrative user is added.
`--project-domain default`	Specifies the project domain.
`--user SOMEUSER@vmware.com`	Specifies the new administrative user.
`--user-domain default admin`	Assigns the new user to the default admin domain.

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.

Post-Installation Configuration and Options 7

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

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

4 Switch to root user.

```
sudo su –
```

5 Create an exclusive router.

```
neutron router-create --router_type=exclusive <router name>
```

6 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>
```

7 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>
```

Parameter	Description
name	Provide a name for the new load balancer.
vip-subnet-id	Specify the VIP subnet for the new load balancer. Only members on this subnet can be added to the pool.

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
```

Parameter	Description
loadbalancer	Specify the load balancer you created in the preceding substep.
protocol type	Specify the protocol type for the listener. ■ TCP ■ HTTP ■ HTTPS
protocol port	Specify the protocol port.
name	Provide a name for the new listener.

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
```

Parameter	Description
lb-algorithm	Specify a load balancing method: ■ IP_HASH Selects a server based on a hash of the source and destination IP address of each packet. ■ LEAST_CONN Distributes client requests to multiple servers based on the number of connections already on the server. New connections are sent to the server with the fewest connections. ■ ROUND_ROBIN Each server is used in turn according to the weight assigned to it. This process is the smoothest and fairest algorithm when the server's processing time remains equally distributed. ■ URI

Parameter	Description
	The left part of the URI, before the question mark, is hashed and divided by the total weight of the running servers. The result designates which server receives the request, ensuring that a request is always directed to the same server as long as all servers remain available.
listener	Specify the listener you created in the preceding substep.
protocol	Specify the protocol for members of the pool to use. ■ TCP ■ HTTP ■ HTTPS
name	Provide a name for the new pool.

8 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>
```

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

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

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

10 Set up the health monitor.

```
neutron lbaas-healthmonitor-create \
--delay DELAY_IN_SECONDS --type [HTTP | TCP] --max-retries NUMBER \
--timeout TIMEOUT_IN_SECONDS --pool LBAAS_POOL
```

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

11 (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.
   a. Go to https://my.vmware.com/web/vmware/details?downloadGroup=VROPS-621&productId=563&rPId=11131.
   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.

      ```
      agent.setup.serverIP=[vREALIZE OPERATIONS MANAGER SERVER ADDRESS]
      agent.setup.serverSSLPort=[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.serverSSLPort` 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.

   ```
   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
```

5 Configure the controller01 node to use the administrative password.

```
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 53.

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 `user-create` command to create the user.

```
$ openstack user create \
  --domain local \
     --password password \
  --email administrative_user_email
  swift
```

b Give the newly created user administrative privileges.

```
$ openstack role add \
  --project service \
  --user swift \
  admin
```

3 Create a service entry for the Object Storage service.

```
$ 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.

4 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 \
object-store \
public \
http://controller01_IP_address:8080/v1/AUTH_%\(tenant_id\)s

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

openstack endpoint create \
--region nova \
object-store \
admin \
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 54.

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 54

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 55

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

3 Enable the rsync Service on page 56

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 57

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 59

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 = xrfuniounenqjnw
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 55.

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 en able the rsync service. See "Enable the rsync Service," on page 56.

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 57.

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 keystoneauth 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]
```

```
use = egg:swift#container_quotas

[filter:account-quotas]
use = egg:swift#account_quotas

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

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

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

[filter:versioned_writes]
use = egg:swift#versioned_writes
```

What to do next

You can now create and configure the Object Storage rings. See "Create and Configure Object Storage Rings," on page 59.

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
swift-ring-builder container.builder add --region 1 --zone 1 --ip
controller01_node_IP_address \
     --port 6001 --device sdb --weight 100
swift-ring-builder container.builder add --region 1 --zone 1 --ip
```

```
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
```

3 Return a list of directories.

```
swift list
```

4 Upload a file.

```
swift upload directory_name myfile.txt
```

5 List the files in a directory.

```
swift list directory_name
```

6 Download the files in a directory.

```
swift download 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**.

The Ceilometer panel displays the current status and configuration.

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 the vSphere Web Client

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

Adding Compute Resources from Multiple vCenter Server Instances

You can add multiple vCenter Server instances to your VMware Integrated OpenStack deployment, if you use VMware NSX-T as virtual network provider. By adding more instances, you improve scalability and resiliency for your OpenStack infrastructure.

Requirements for Adding Compute Resources from Multiple vCenter Server Instances

You can add multiple vCenter Server instances, if the following requirements are met:

- High Availability deployments only, not available for compact mode deployments.
- Virtual network must be provided by VMware NSX-T, not available for deployments that use vSphere Distributed Switch or VMware NSX for vSphere .
- You can have only one availability zone per vCenter Server instance.

Add New Compute Clusters for an OpenStack Deployment from Multiple vCenter Server Instances

You can increase the number of compute clusters in your VMware Integrated OpenStack deployment to increase CPU capacity. You can select compute clusters from all Compute vCenter Server instances in your data center.

Prerequisites

Prepare a cluster with at least one host.

Procedure

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

2 (Optional) Add additional vCenter Server instances for use in VMware Integrated OpenStack.

   a Select the **Compute vCenter Server** tab.

   b Click the green plus-sign icon (+) at the top of the panel to add a new instance.

   c In the Add Compute vCenter Server dialog box, enter the FQDN of the instance, credentials with administrative privileges, and click **OK**.

3 Select the **Nova Compute** tab.

   This tab displays the current Nova Compute clusters and their status.

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

5 On the Select a Compute vCenter Server page, select the instance and the availability zone for the compute cluster that you need and click **Next**.

6 On the Add Nova cluster page, select the cluster that you prepared as a prerequisite, and click **Next**.

   The cluster you select must contain at least one host.

7 On the Add Nova datastores page, select the datastores for the tenants in the new cluster, and click **Next**.

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

9 Review the proposed configuration, and click **Finish**.

10 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.

Install the VMware Integrated OpenStack License Key

VMware Integrated OpenStack requires a license key to operate. Install a VMware Integrated OpenStack license key as soon as possible after you install VMware Integrated OpenStack.

Prerequisites

VMware Integrated OpenStack uses the vSphere licensing infrastructure for license management. Ensure that you have sufficient vSphere licenses for vCenter Server to be able to use the vSphere Distributed Switch feature.

Procedure

1 In a Web browser, log in to the vSphere Web Client to administrate your vCenter Server instance on which VMware Integrated OpenStack is installed.

2 On the vSphere Web Client **Home** tab, click **Licensing**.

3 Click the plus sign on the **Licenses** tab.

4 Enter the VMware Integrated OpenStack license key in the **License Keys** text box and click **Next**.

5 Update the license name, review the details of the license, and click **Finish**.

6 Click the **Assets** tab and click **Solutions**.

7 Right-click the VMware Integrated OpenStack deployment and select **Assign License**.

8 Select the license from the list of available licenses, and click **OK**.

Index