VMware Integrated OpenStack Installation and Configuration Guide

Modified on 29 AUG 2019

VMware Integrated OpenStack 5.1

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

https://docs.vmware.com/

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

VMware Integrated OpenStack Installation and Configuration Guide

1

The *VMware Integrated OpenStack Installation and Configuration Guide* explains the process of deploying OpenStack in your VMware vSphere® environment.

Before installing VMware Integrated OpenStack, review the deployment and networking modes described in this guide and ensure that your environment meets the stated requirements. Once you are ready, prepare your vCenter Server® instance and deploy the VMware Integrated OpenStack vApp. The vApp provides a workflow that guides you through the rest of the deployment process, allowing you to specify your management and compute clusters, configure networking, and add resources. After deployment, you can use the vApp to add components or otherwise modify the configuration of your OpenStack cloud infrastructure.

Intended Audience

This guide is for system administrators and developers who want to integrate their vSphere deployment with OpenStack services. To do so successfully, you should be familiar with vSphere and the OpenStack components and functions. If you are deploying VMware Integrated OpenStack with VMware NSX® Data Center for vSphere® or NSX-T™ Data Center, you should also be familiar with the administration of those products.

Terminology

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

Introducing VMware Integrated OpenStack

2

VMware Integrated OpenStack is a distribution of OpenStack designed to run on a vSphere infrastructure. VMware Integrated OpenStack 5.1 is based on the OpenStack Queens release.

VMware Integrated OpenStack makes use of your existing infrastructure for the hypervisor, networking, and storage components for OpenStack, simplifying installation and operations and offering better performance and stability.

VMware Integrated OpenStack offers a variety of unique features:

- vCenter Server cluster as the compute node for reduced management complexity
- Distributed Resource Scheduler (DRS) and Storage DRS for workload rebalancing and datastore load balancing
- vSphere high availability (HA) to protect and automatically restart workloads
- Support for importing vSphere virtual machines and templates into OpenStack
- Advanced networking functionality through NSX
- Integration with products such as vRealize Automation, vRealize Operations Manager, and vRealize Log Insight

This chapter includes the following topics:

VMware Integrated OpenStack Architecture

VMware Integrated OpenStack connects vSphere resources to OpenStack components.

VMware Integrated OpenStack is implemented as compute and management clusters in your vSphere environment. The compute clusters handle tenant workloads, while the management cluster contains OpenStack components and other services such as load balancing, database, and DHCP.

The core OpenStack projects included in VMware Integrated OpenStack are as follows:

Nova (compute) Compute clusters in vSphere are used as Nova compute nodes. Nova creates instances as virtual machines in these clusters, and vSphere uses DRS to place the virtual machines.

Neutron (networking) Neutron implements networking functions by communicating with the NSX Manager (for NSX-T Data Center or NSX Data Center for vSphere deployments) or with vCenter Server (for VDS-only deployments).

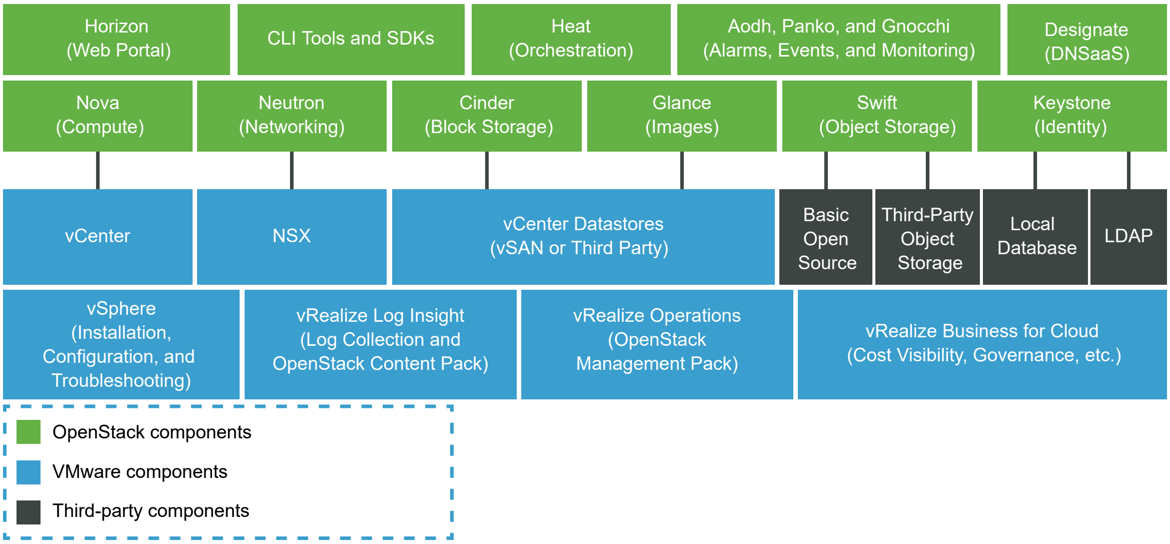
Cinder (block storage) Cinder executes block volume operations through the VMDK driver, causing the desired volumes to be created in vSphere.

Glance (image service) Glance images are stored and cached in a dedicated image service datastore when the virtual machines that use them are booted.

VMware Integrated OpenStack also provides the following OpenStack components:

- Barbican (secret management)
- Ceilometer (telemetry), including Aodh (alarming), Panko (event storage), and Gnocchi (time series database)
- Designate (DNS)
- Heat (orchestration)
- Horizon (user interface)
- Keystone (identity management)
- Swift (object storage) - technical preview only

Figure 2-1. Overview of VMware Integrated OpenStack Components


Horizon (Web Portal)
CLI Tools and SDKs
Heat (Orchestration)
Aodh, Panko, and Gnocchi (Alarms, Events, and Monitoring)
Designate (DNSaaS)
Nova (Compute)
Neutron (Networking)
Cinder (Block Storage)
Glance (Images)
Swift (Object Storage)
Keystone (Identity)
vCenter
NSX
vCenter Datastores (vSAN or Third Party)
Basic Open Source
Third-Party Object Storage
Local Database
LDAP
vSphere (Installation, Configuration, and Troubleshooting)
vRealize Log Insight (Log Collection and OpenStack Content Pack)
vRealize Operations (OpenStack Management Pack)
vRealize Business for Cloud (Cost Visibility, Governance, etc.)
OpenStack components
VMware components
Third-party components

Internationalization and Unicode Support

VMware Integrated OpenStack supports UTF-8 character encoding, and its interface and documentation are available in English, French, German, Spanish, Japanese, Korean, Simplified Chinese, and Traditional Chinese.

If you are using vCenter Server for Windows, you must set the system locale (language for non-Unicode programs) to `English (United States)`.

If you are using Linux, configure the system to use the UTF-8 encoding specific to your locale. For example, to use U.S. English, specify the `en_US.UTF-8` locale. For more information, see the documentation for your operating system.

Important Although VMware Integrated OpenStack supports Unicode, the following items must only contain ASCII characters:

- Names of OpenStack resources (such as project, users, and images)
- Names of infrastructure components (such as ESXi hosts, port groups, data centers, and datastores)
- LDAP and Active Directory attributes

OpenStack Foundation Compliance

Every new version of VMware Integrated OpenStack complies with the most recent interoperability guidelines available at the time of release.

Interoperability guidelines are created in the OpenStack community by the Interop Working Group and are approved by the OpenStack Foundation Board of Directors.

As an OpenStack Powered Platform product, VMware Integrated OpenStack provides proven interoperability with all other OpenStack Powered products. For more information, see the VMware Integrated OpenStack page on OpenStack Marketplace at https://www.openstack.org/marketplace/distros/distribution/vmware/vmware-integrated-openstack.

VMware Integrated OpenStack Licensing

VMware Integrated OpenStack requires a license key to provide functionality.

VMware Integrated OpenStack licenses are available for Data Center Edition and Carrier Edition.

Data Center Edition is available as a standalone product or as part of VMware vRealize Suite. It is designed for enterprises that want to build a private cloud based on OpenStack.

Carrier Edition is part of the VMware vCloud NFV bundle. It is designed for telecommunications companies and communication service providers that want to build a network functions virtualization (NFV) cloud. In addition to all features of Data Center Edition, it supports the following:

- SR-IOV
- Tenant data centers
- Enhanced Platform Awareness (EPA), including virtual CPU pinning and NUMA awareness
- NSX-managed virtual distributed switch (N-VDS) in enhanced data path mode

To obtain licenses or additional information, see the VMware Integrated OpenStack product page at https://www.vmware.com/products/openstack.html or contact your VMware sales representative.

You can use VMware Integrated OpenStack in evaluation mode for 60 days without assigning a license key. When the evaluation license expires, all NFV features are disabled, and you cannot run vRealize Automation workflows. Obtain and assign your VMware Integrated OpenStack license key as soon as possible after installing VMware Integrated OpenStack.

In addition to the VMware Integrated OpenStack license, you will also need sufficient licenses for vSphere and for any other VMware components that you deploy, such as NSX-T Data Center.

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

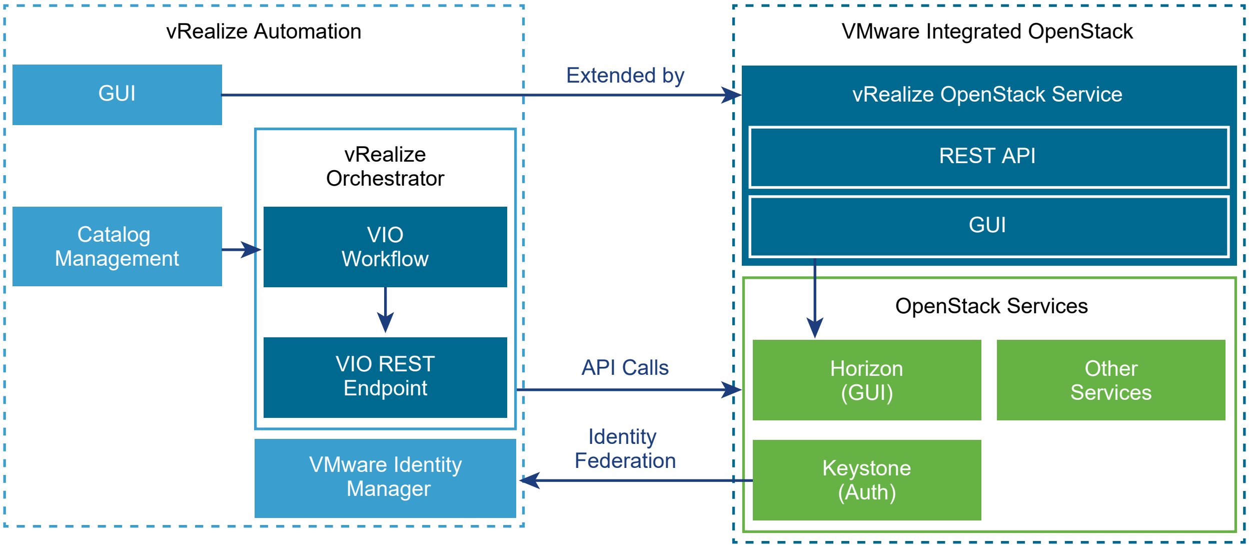
You can join or leave the CEIP at any time after deploying VMware Integrated OpenStack. In the vSphere Client, select **Menu > VMware Integrated OpenStack** and click **OpenStack Deployments**. Open the **Manage** tab, then click the **Settings** tab, and select **Customer Experience Improvement Program**. On the page displayed, you can join or leave the CEIP.

Integration with vRealize Automation

When you integrate VMware Integrated OpenStack with vRealize Automation, you can benefit from the following features:

- Securely use existing credentials to access cloud resources through integration with VMware Identity Manager.
- Manage all your OpenStack deployments from a single GUI through the VMware Integrated OpenStack tab that appears in the vRealize Automation portal.
- Consume VMware Integrated OpenStack based infrastructure through vRealize Automation XaaS blueprints.
- Run OpenStack Heat workflows that provide on-demand network capabilities on OpenStack based resource pools.
- Run workflows to manage VMs, projects, and networks.
- Create custom OpenStack workflows through the OpenStack API.

Figure 2-2. Integration Architecture



VMware Identity Manager Integration

By integrating VMware Integrated OpenStack with VMware Identity Manager you achieve a way to use existing credentials securely when accessing cloud resources such as servers, volumes, and databases, across multiple endpoints provided in multiple authorized clouds. You have a single set of credentials, without having to provision additional identities or log in multiple times. The user's Identity Provider maintains the credential.

Managing OpenStack Deployments Through the vRealize Automation Portal

If you have enabled the VMware Identity Manager integration, you can use the VMware Integrated OpenStack tab that appears in the vRealize Automation portal. This tab embeds the VMware Integrated OpenStack dashboard in the vRealize Automation portal to allow for cloud administrators to manage OpenStack deployments from a single GUI. vRealize Automation administrator must enable the new tab and configure mappings to associate users to their respective projects. When a user who is associated with a project, logs in to the vRealize Automation portal, the **VIO** tab is visible.

vRealize Automation XaaS Blueprints Design

To consume vRealize Automation blueprints, you must install the vRealize Orchestrator Plug-in for OpenStack. vRealize Automation administrators can design and publish OpenStack blueprints. An approval chain and entitlement can also be configured. vRealize Automation users can request OpenStack catalog items that can be either approved or denied by users with assigned approval role.

vRealize Orchestrator Workflows

After you design vRealize Automation XaaS Blueprints, you consume them through the vRealize Orchestrator workflows that allow cloud administrators to automate user on-boarding and application deployment to OpenStack.

For information about using vRealize Automation with OpenStack, see *Using the vRealize Orchestrator VMware Integrated OpenStack Plug-In 2.0*.

Datastore Clusters in VMware Integrated OpenStack

You can use datastore clusters in the ESXi clusters that host VMware Integrated OpenStack compute workloads.

A datastore cluster is a collection of datastores with shared resources and a shared management interface. You can use vSphere Storage DRS to manage the resources in a datastore cluster. For information about creating and configuring datastore clusters, see "Creating a Datastore Cluster" in *vSphere Resource Management*.

If you want to use datastore clusters with VMware Integrated OpenStack, be aware of the following:

- When you deploy OpenStack using the VMware Integrated OpenStack vApp, you cannot select a datastore cluster for the compute or block storage component to consume. To specify a datastore cluster for the compute or block storage component during deployment, deploy OpenStack using the API.
- During deployment, if you specify a datastore cluster for the compute component to consume, you cannot use `custom.yml` to specify other datastore clusters for any compute node after deployment. If you do so, the compute nodes with datastore clusters specified during deployment will not function properly.

- If you use `custom.yml` to add compute nodes with datastore clusters after deployment, note the following limitations:
  - Only one datastore cluster can be used for each vCenter Server instance.
  - If your environment has multiple vCenter Server instances, the name of the datastore cluster used by VMware Integrated OpenStack in each instance must be the same.
- Swift nodes do not support datastore clusters.
- You can boot only images backed by virtual machines. Sparse and preallocated images cannot be booted on datastore clusters.
- You must enable Storage DRS on your datastore clusters and set the **Cluster automation level** to **No Automation (Manual Mode)**. Automatic migrations are not supported.
- Only the following provisioning operations use Storage DRS:
  - Booting from a Glance template image
  - Creating raw Cinder volumes
  - Creating a volume from another volume (full clones and linked clones)
  - Cloning snapshots in COW format (full clones and linked clones)

VMware Integrated OpenStack Deployment Modes

3

You can deploy VMware Integrated OpenStack in high availability (HA), compact, or tiny mode.

This chapter includes the following topics:

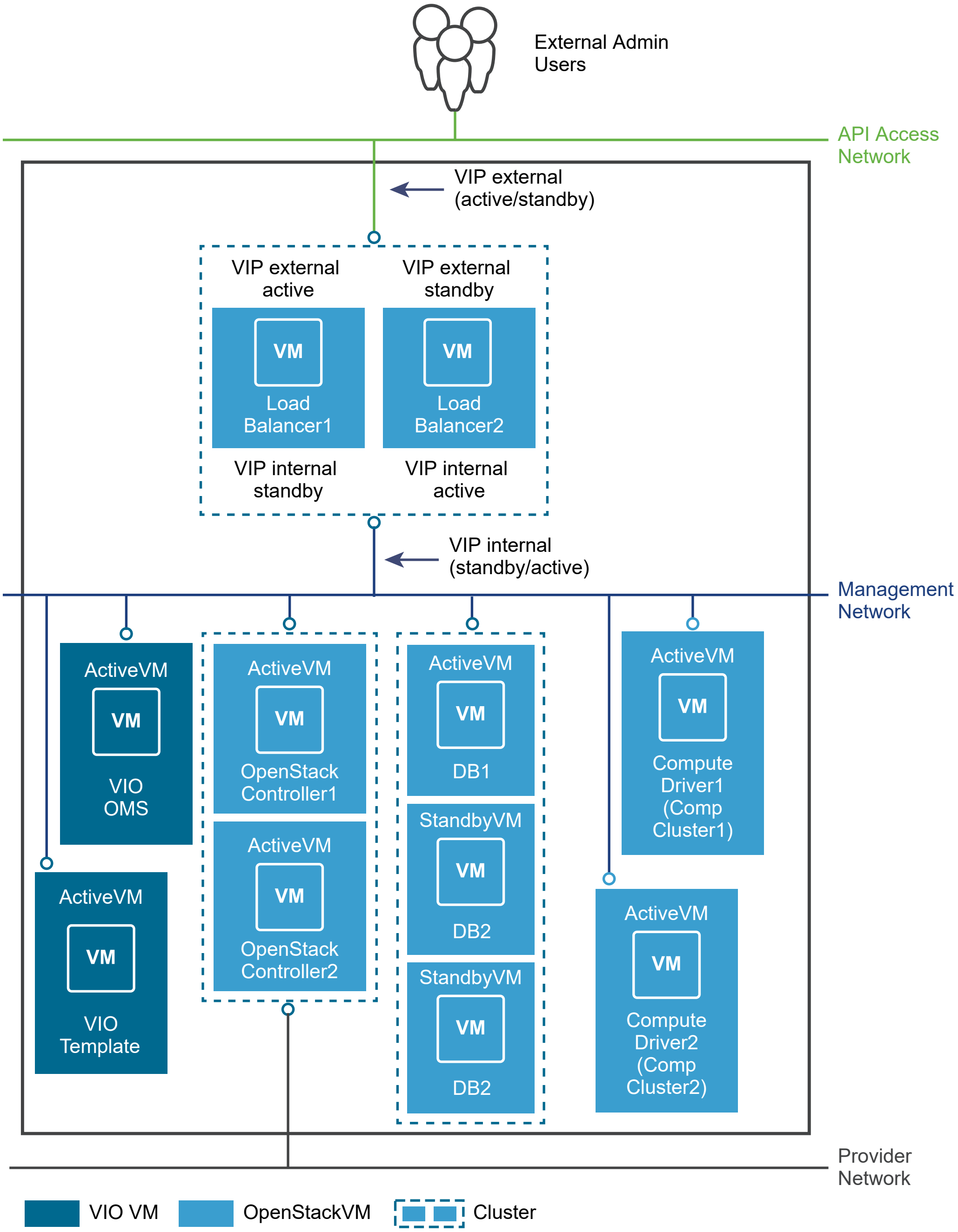
- VMware Integrated OpenStack Deployment in HA Mode
- VMware Integrated OpenStack Deployment in Compact Mode
- VMware Integrated OpenStack Deployment in Tiny Mode

VMware Integrated OpenStack Deployment in HA Mode

High availability (HA) deployment mode includes active and standby nodes to ensure that services are not interrupted.

An HA deployment runs on three ESXi hosts and includes at least nine virtual machines. These include two load balancers, three database nodes, two controllers, the OpenStack Management Server, and at least one compute driver. An additional compute driver is created for each compute cluster that you add to your deployment.

Figure 3-1. Management Cluster in HA Mode



To deploy in HA mode, at least 11 contiguous IP addresses must be available on the management network. Each of the preceding virtual machines requires one IP address, and two additional IP addresses are required for private OpenStack endpoints. At least two contiguous IP addresses must be available on the API access network, both of which are used as public OpenStack endpoints.

Note

- In VDS networking mode, an additional two virtual machines are required for DHCP.
- If you want to deploy Ceilometer, an additional five virtual machines are required. These virtual machines each require one IP address on the management network.

To ensure that you can upgrade VMware Integrated OpenStack successfully, plan management and API access networks that include twice the number of IP addresses required for your deployment. The extra IP addresses will be used during the upgrade procedure.

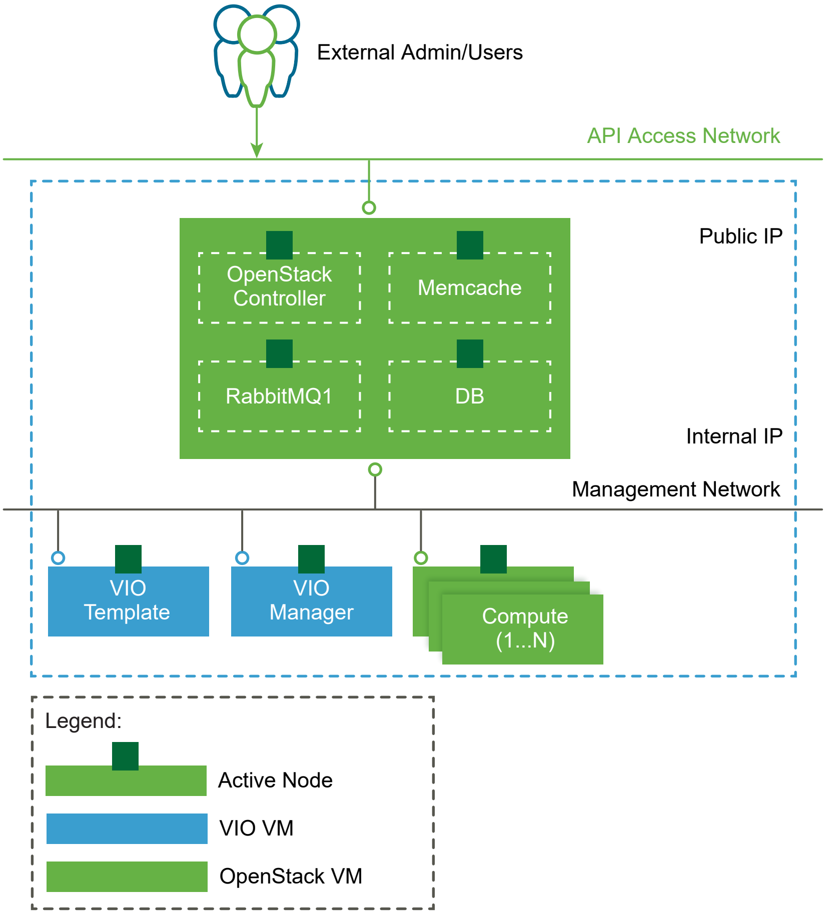
VMware Integrated OpenStack Deployment in Compact Mode

Compact deployment mode requires fewer hardware resources and less memory than HA mode. All control plane instances are deployed on a single virtual machine, and only one controller, message queue, and database instance are included.

Compact deployment mode is suitable for evaluation and proof of concept testing. If you make regular backups of your virtual machines, it can also be used in production environments.

A compact deployment runs on one ESXi host and includes at least three virtual machines. These include the OpenStack Management Server, the unified control plane node, and at least one compute driver node. An additional compute driver is created for each compute cluster that you add to your deployment.

Figure 3-2. Management Cluster in Compact Mode



To deploy in compact mode, at least four contiguous IP addresses must be available on the management network. Each of the preceding virtual machines requires one IP address, and one additional IP address is required for the private OpenStack endpoint. At least one IP address must be available on the API access network to be used as the public OpenStack endpoint.

Note If you want to deploy Ceilometer, an additional five virtual machines are required. These virtual machines each require one IP address on the management network.

To ensure that you can upgrade VMware Integrated OpenStack successfully, plan management and API access networks that include twice the number of IP addresses required for your deployment. The extra IP addresses will be used during the upgrade procedure.

HA in Compact Mode

With vSphere HA, VM monitoring, and vSAN, you can enable certain HA features on a compact deployment.

- By enabling vSphere HA on the management cluster, you can provide fault tolerance in the event that an ESXi host stops functioning, loses network connectivity with the master host, or enters the `Network Isolated` state.

- By enabling vSphere HA and VM monitoring on the management cluster, you can provide fault tolerance in the event that a control plane virtual machine, compute virtual machine, or OpenStack service stops functioning.
- By using vSAN on the management cluster, you can provide fault tolerance for storage components.

If you want to enable these HA features on a compact deployment, your management cluster must include at least three ESXi hosts.

If you are deploying OpenStack using the public API, you can enable HA by including the following attribute:

```
"control_plane_ha_enabled": "true"
```

This attribute will automatically enable vSphere HA and VM monitoring on the management cluster.

VMware Integrated OpenStack Deployment in Tiny Mode

Tiny deployment mode consolidates all OpenStack control plane and compute driver nodes.

To deploy OpenStack in tiny mode, you must use the VMware Integrated OpenStack API. Deployment using the vApp is not supported.

In tiny mode, the same virtual machine comprises the management and compute clusters. Because tiny mode involves only a single virtual machine, you cannot add compute clusters.

A tiny deployment runs on one ESXi host and includes two virtual machines. These include the OpenStack Management Server and the unified control plane and compute driver node.

To deploy in tiny mode, at least three contiguous IP addresses must be available on the management network. Each of the preceding virtual machines requires one IP address, and one additional IP address is required for the private OpenStack endpoint. At least one IP address must be available on the API access network to be used as the public OpenStack endpoint.

Note If you want to deploy Ceilometer, an additional five virtual machines are required. These virtual machines each require one IP address on the management network.

To ensure that you can upgrade VMware Integrated OpenStack successfully, plan management and API access networks that include twice the number of IP addresses required for your deployment. The extra IP addresses will be used during the upgrade procedure.

VMware Integrated OpenStack Networking Modes

4

You can deploy VMware Integrated OpenStack with NSX-T Data Center, NSX Data Center for vSphere, or vSphere Distributed Switch (VDS) as the networking back end.

This chapter includes the following topics:

- VMware Integrated OpenStack Deployments with NSX
- VMware Integrated OpenStack Deployments with VDS
- Comparison of NSX and VDS Features

VMware Integrated OpenStack Deployments with NSX

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

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.

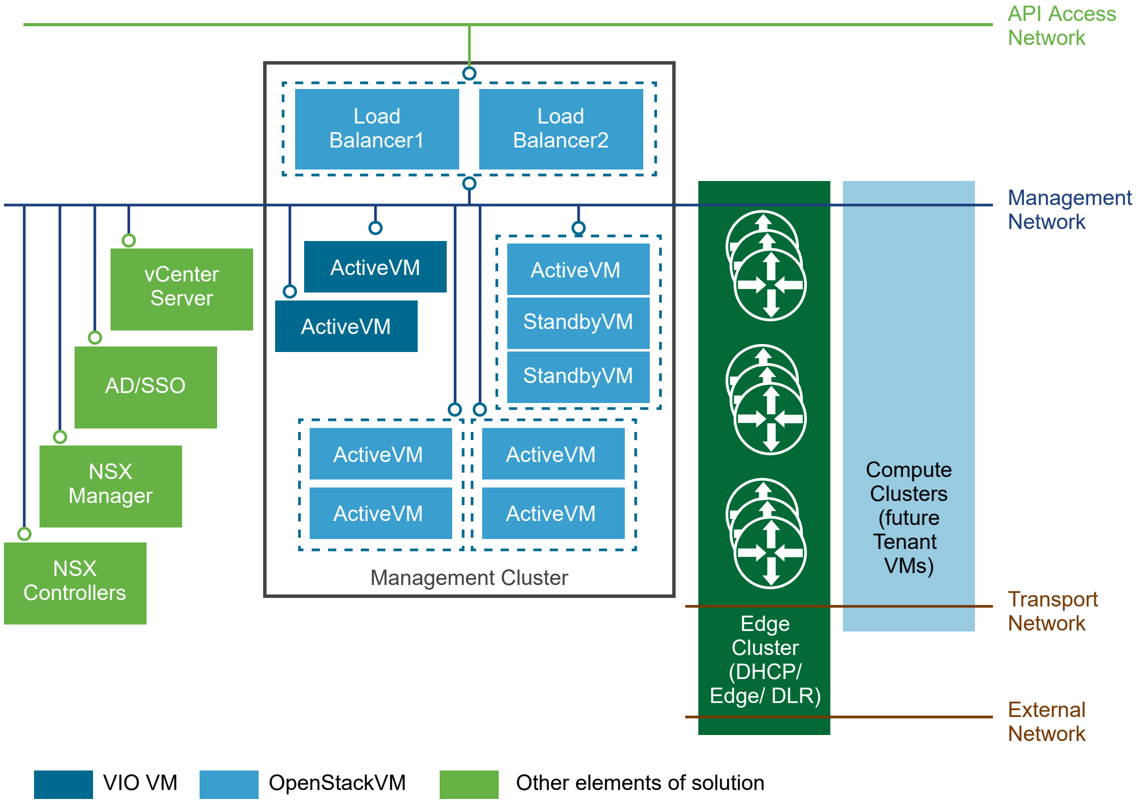
Cluster and Component Architecture

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.

Figure 4-1. NSX deployment in HA mode



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

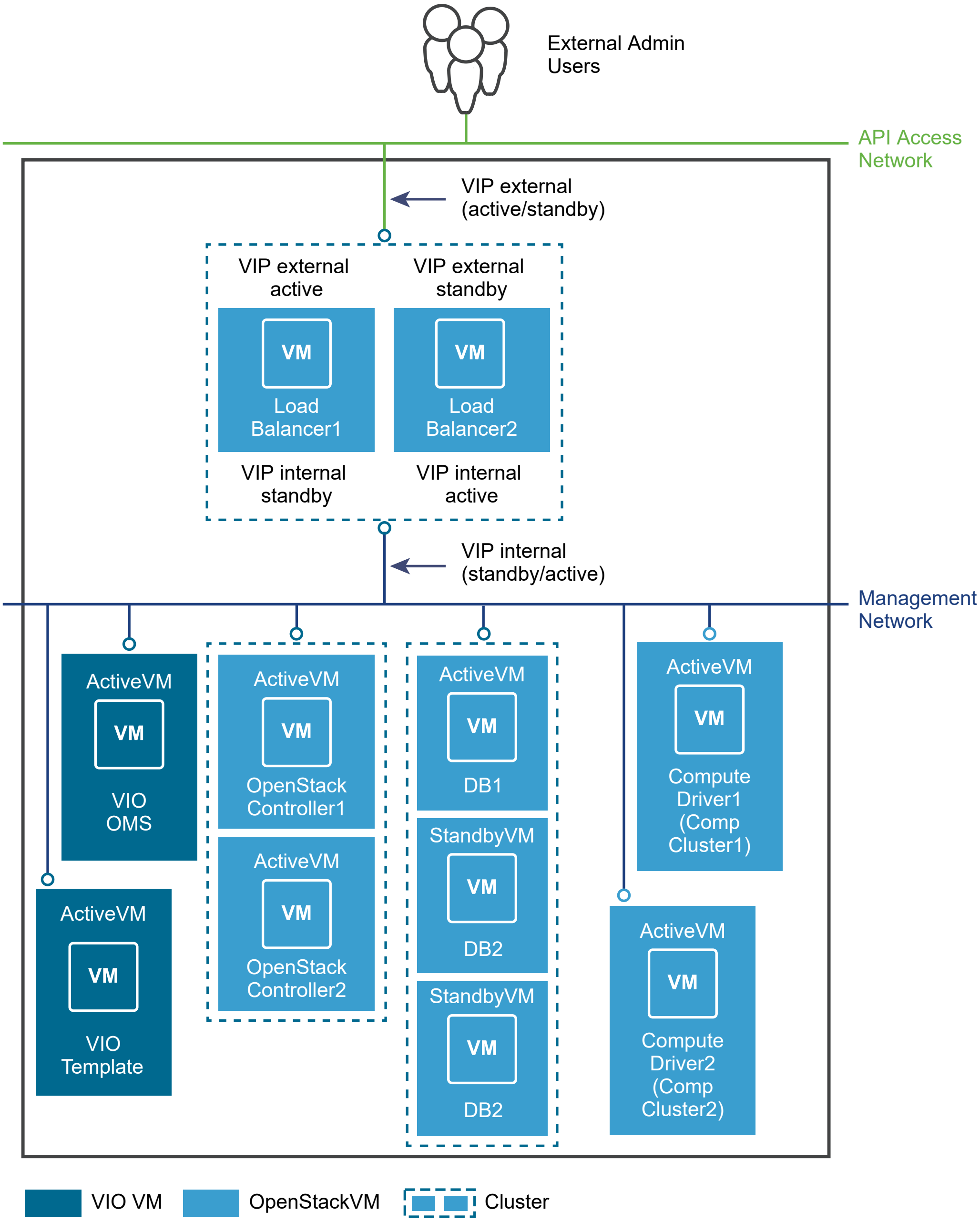
Cluster or Component	Description
vCenter Server instance	A dedicated vCenter Server instance is not required but optimizes deployment.
Active Directory	For user authentication by the OpenStack Identity Service.
Management cluster	Contains all the deployed OpenStack component and management VMs. See Management Cluster 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 VMware Integrated OpenStack deployments.

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 4-2. Management cluster in HA mode



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)

Physical NSX Network

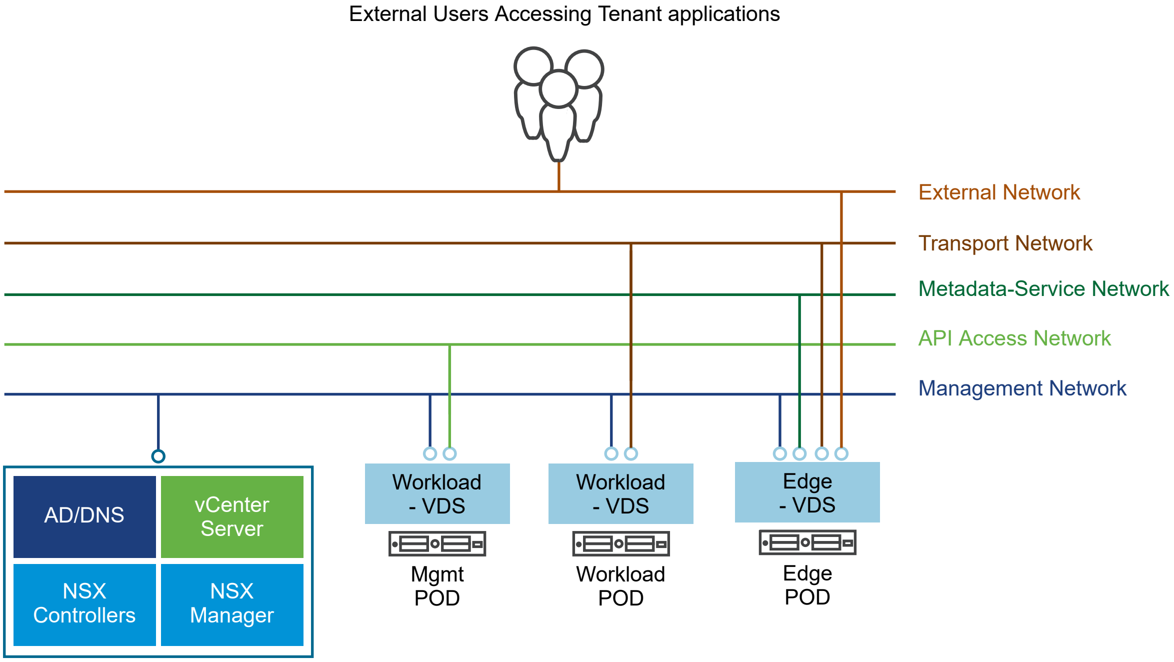
For VMware Integrated OpenStack deployments based on NSX, the API access, Management, Transport, and External network each require a separate and dedicated VLAN.

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. ■ Include at least 2 contiguous IP addresses for HA deployments or 1 IP address for compact or tiny deployments.
External	Provides external user access to deployments. ■ Trunk all hosts in the NSX Edge cluster to this VLAN.
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. ■ Include at least 11 contiguous IP addresses for HA deployments or 4 contiguous IP addresses for compact or tiny deployments. An additional 5 contiguous IP addresses are required if you want to deploy Ceilometer. ■ 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.

VLAN	Description
Metadata-service	The metadata-service network enables new OpenStack deployments 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 deployments. ■ 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 4-3. Network Map for NSX Deployments



VMware Integrated OpenStack Deployments with VDS

VMware Integrated OpenStack can use vSphere Distributed Switch (VDS) to provide basic L2 networking for tenant workloads.

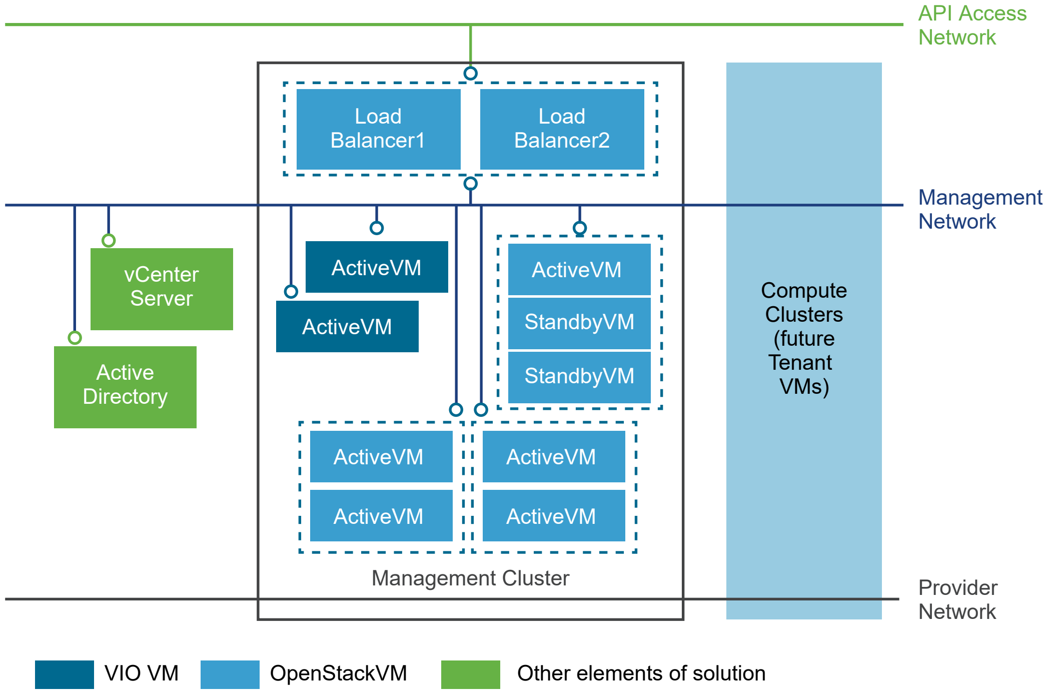
In this model, the VMware Integrated OpenStack administrator creates a set of provider networks and shares them with tenants, who then connect their VMs to these networks.

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.



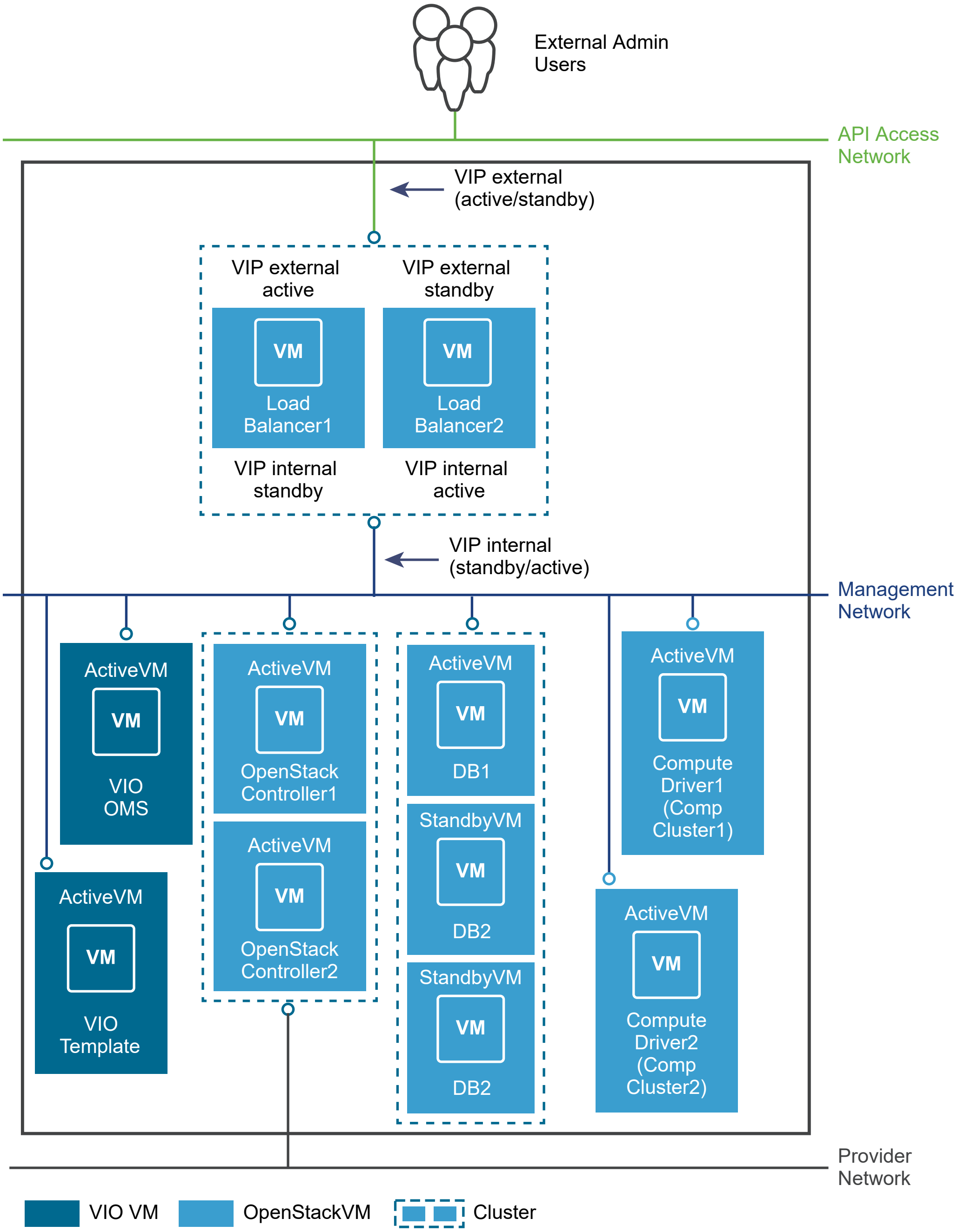
The VMware Integrated OpenStack architecture includes the following clusters and components.

Cluster or Component	Description
vCenter Server instance	Configure a vCenter Server 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 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 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)

Component	Description	Nodes
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)
DHCP	Provide IP addresses to the virtual machines 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.

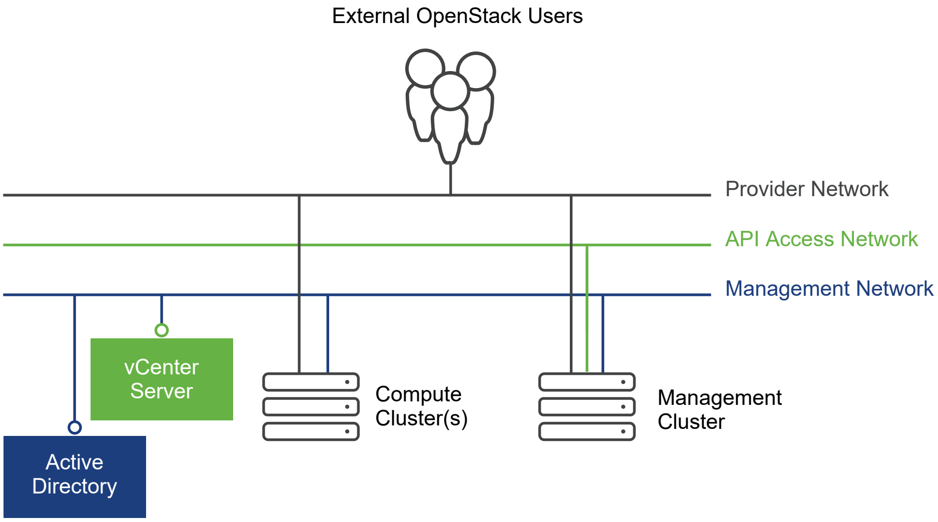
Physical VDS Network Overview

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. ■ Include at least 2 contiguous IP addresses for HA deployments or 1 IP address for compact or tiny deployments.
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. ■ Include at least 11 contiguous IP addresses for HA deployments or 4 contiguous IP addresses for compact or tiny deployments. An additional 5 contiguous IP addresses are required if you want to deploy Ceilometer.
Provider	The Provider network connects DHCP services with the OpenStack deployments 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 4-4. VMware Integrated OpenStack VDS Physical Network



Comparison of NSX and VDS Features

VMware Integrated OpenStack offers different features depending on whether you deploy with VDS or NSX networking.

Supported Feature	VDS	NSX
Provider networks leveraging VLANs	Yes	Yes
High availability for the API/management plane	Yes	Yes
DC-wide control plane scale	Limited	High
Layer 3/NAT high availability and scale	No	Yes
Neutron feature set: ■ Private logical network identifier independent of VLANs ■ Highly available DHCP service ■ Security groups ■ Virtual routers ■ Integration and support of metadata service ■ Centralized or distributed Layer 3 ■ NAT and floating IP address 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
Tenant creation of private Layer 2 networks	No	Yes
Content packs for vRealize Operations Manager and vRealize Log Insight	No	Yes

Preparing Your Environment 5

You prepare your network and vCenter Server instance before installing VMware Integrated OpenStack.

The specific procedure for preparing your environment depends on the networking mode you have chosen.

This chapter includes the following topics:

Software Requirements for VMware Integrated OpenStack

VMware Integrated OpenStack works together with various software products to provide functionality.

VMware Integrated OpenStack 5.1 requires the following products:

- vSphere 6.5 or later, including:
  - vCenter Server 6.5 or later
  - ESXi 6.5 or later
- (NSX-T Data Center deployments only) NSX-T Data Center 2.1.0 or later
- (NSX Data Center for vSphere deployments only) NSX Data Center for vSphere 6.3.6 or 6.4.1 or later

Note If you want to deploy VMware Integrated OpenStack with VDS networking only, NSX is not required.

You can optimize performance by using a separate vCenter Server instance dedicated to VMware Integrated OpenStack.

VMware Integrated OpenStack 5.1 is also compatible with the following products:

- vSAN 6.6.1 Update 2 or later
- vRealize Automation 7.5 or later
- vRealize Log Insight 4.6.1 or later with VMware OpenStack Content Pack 1.2

- vRealize Operations Manager 6.7 or later with vRealize Operations Management Pack for VMware Integrated OpenStack 5.0

For the most current information about supported versions, see the VMware Product Interoperability Matrices at https://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Hardware Requirements for VMware Integrated OpenStack

The specific hardware required to run VMware Integrated OpenStack depends on the type of deployment and networking that you select.

Note Each ESXi host used for VMware Integrated OpenStack must have at least eight logical processors.

HA Deployments

Three ESXi hosts are required to deploy the following virtual machines:

Component	Virtual Machines	vCPUs	vRAM (GB)	Disk Space (GB)
OpenStack Management Server	1	VDS: 2 (2 per VM) NSX: 4 (4 per VM)	4 (4 per VM)	25 (25 per VM)
OpenStack template	1	2 (2 per VM)	4 (4 per VM)	20 (20 per VM)
Load balancer	2	4 (2 per VM)	8 (4 per VM)	40 (20 per VM)
Database	3	12 (4 per VM)	48 (16 per VM)	240 (80 per VM)
Controller	2	16 (8 per VM)	32 (16 per VM)	160 (80 per VM)
Compute driver	1	2 (2 per VM)	4 (4 per VM)	20 (20 per VM)
TOTAL	10	VDS: 38 NSX: 40	100	505

An additional compute driver virtual machine with the same specifications is created for each compute cluster that you add to the deployment.

Compact Deployments

One ESXi host is required to deploy the following virtual machines:

Component	Virtual Machines	vCPUs	vRAM (GB)	Disk Space (GB)
OpenStack Management Server	1	2	4	25
OpenStack template	1	2	4	20
Control plane	1	8	16	80
Compute driver	1	2	4	20
TOTAL	4	14	28	145

An additional compute driver virtual machine with the same specifications is created for each compute cluster that you add to the deployment.

Tiny Deployments

One ESXi host is required to deploy the following virtual machines:

Component	Virtual Machines	vCPUs	vRAM (GB)	Disk Space (GB)
OpenStack Management Server	1	2	4	25
OpenStack template	1	2	4	20
Control and compute	1	8	24	80 (20 + 60)
TOTAL	3	12	32	125

VDS Networking

For HA deployments with VDS networking, the following resources are also required.

Component	Virtual Machines	vCPUs	vRAM (GB)	Disk Space (GB)
DHCP	2	8 (4 per VM)	32 (16 per VM)	40 (20 per VM)

For compact and tiny deployments with VDS networking, the DHCP service runs on the controller node and does not require independent virtual machines.

NSX Data Center for vSphere Networking

See "System Requirements for NSX Data Center for vSphere" in the *NSX Installation Guide*.

NSX-T Data Center Networking

See "System Requirements" in the *NSX-T Installation Guide*.

Additional Components

If you want to use Ceilometer, the following resources are also required.

Component	Virtual Machines	vCPUs	vRAM (GB)	Disk Space (GB)
Ceilometer	1	4 (4 per VM)	4 (4 per VM)	20 + 60 (20 + 60 per VM)
Gnocchi storage	1	4 (4 per VM)	4 (4 per VM)	20 (20 per VM)
Gnocchi compute	3	12 (4 per VM)	12 (4 per VM)	60 (20 per VM)
TOTAL	5	20	20	160

If you want to use Swift, additional resources are required based on the scale of your deployment. The following table lists only the resources required by default.

Component	Virtual Machines	vCPUs	vRAM (GB)	Disk Space (GB)
Swift proxy	2	16 (8 per VM)	32 (16 per VM)	40 (20 per VM)
Swift storage	3	6 (2 per VM)	6 (2 per VM)	60 + 6144 (20 + 2048 per VM)
TOTAL	5	22	38	6244

When you create your Swift cluster, you can specify the number and disk size of storage and proxy nodes in it. You can also add nodes after the cluster is created.

If you need to change the number of vCPUs or amount of vRAM used for proxy or storage nodes, modify the following parameters in the `/opt/vmware/vio/etc/omjs.properties` file and restart the OpenStack Management Server service.

```
oms.vmsize.cpu.swift_proxy
oms.vmsize.cpu.swift_storage
oms.vmsize.memory.swift_proxy
oms.vmsize.memory.swift_storage
```

The size of the root disk of each node is fixed at 20 GB.

Required Network Ports

You open required ports on your firewall to ensure that VMware Integrated OpenStack can operate properly.

Note In a compact deployment, controller, load balancer, and database nodes are deployed as a single virtual machine. In a tiny deployment, controller, load balancer, database, and compute nodes are deployed as a single virtual machine.

All ports listed are TCP unless otherwise specified.

Object	Port Number	Network	Service or Product	Description
Load balancer, controller, database, and compute nodes	22	Internal	SSH	SSH (used by Ansible)
OpenStack Management Server	53 (TCP or UDP)	Internal	DNS	FQDN resolution
OpenStack Management Server	123 (UDP)	Internal	NTP	NTP service
Load balancer nodes	443	Public and internal	OpenStack dashboard service	VMware Integrated OpenStack dashboard
OpenStack Management Server	443	Internal	OpenStack Management Server	OpenStack Management Server
ESXi hosts	443	Internal	ESXi hosts	ESXi API endpoint
NSX Manager	443	Internal	NSX Manager	NSX Manager endpoint

Object	Port Number	Network	Service or Product	Description
vCenter Server Appliance	443	Internal	vCenter Server	vCenter Server API endpoint
Load balancer nodes	1993	Internal	OpenStack load balancer UI	HAProxy web UI
Load balancer and database nodes	3306	Public and internal	OpenStack API services	Database cluster
Database nodes	4369	Internal	OpenStack RPC bus	RabbitMQ port mapper daemon (epmd) service
Database nodes	4444	Internal	OpenStack database	MariaDB Galera state snapshot transfers
Database nodes	4567	Internal	OpenStack database	MariaDB Galera replication traffic
Database nodes	4568	Internal	OpenStack database	MariaDB Galera incremental state transfers
Load balancer and controller nodes	5000	Public and internal	OpenStack API services	Keystone API endpoint
Database nodes	5672	Internal	OpenStack RPC bus	RabbitMQ message bus
Load balancer and controller nodes	6080	Public and internal	OpenStack console services	novnc proxy
Load balancer and controller nodes	6083	Public and internal	OpenStack console services	Serial proxy
Load balancer and controller nodes	6090	Public and internal	OpenStack console services	MKS proxy
Load balancer and controller nodes	8000	Public and internal	OpenStack API services	Heat CloudFormation API endpoint
Load balancer and controller nodes	8004	Public and internal	OpenStack API services	Heat API endpoint
OpenStack Management Server	8088	Internal	OpenStack Management Server	Jarvis
OpenStack Management Server	8443	Internal	OpenStack Management Server	OpenStack Management Server OpenAPI documentation
Load balancer and controller nodes	8774	Public and internal	OpenStack API services	Nova API endpoint
Controller nodes	8775	Internal	OpenStack metadata	Metadata service (required unless config drive is used)
Load balancer and controller nodes	8776	Public and internal	OpenStack API services	Cinder API endpoint
Load balancer and controller nodes	8778	Public and internal	OpenStack API services	Nova placement API

Object	Port Number	Network	Service or Product	Description
Load balancer and controller nodes	9191	Internal	OpenStack API services	Glance registry endpoint
Load balancer and controller nodes	9292	Public and internal	OpenStack API services	Glance API endpoint
Load balancer and controller nodes	9311	Public and internal	OpenStack API services	Barbican API endpoint
vCenter Server appliance	9443	Internal	vCenter Server	vCenter Server
OpenStack Management Server	9449	Internal	vAPI	vAPI
Load balancer and controller nodes	9696	Public and internal	OpenStack API services	Neutron API endpoint
Database nodes	11211	Internal	OpenStack control plane cache	Memory cache services for controller nodes
Load balancer and controller nodes	35357	Public and internal	OpenStack API services	Keystone administrator API endpoint

If you want to use LDAP or Active Directory, the following ports must also be open.

Object	Port Number	Network	Service or Product	Description
Active Directory or LDAP hosts	389	Internal	Domain controller or LDAP server	Serving LDAP requests (non-secured)
Active Directory or LDAP hosts	636	Internal	Domain controller or LDAP server (LDAPS)	Serving LDAP requests (secured)
Active Directory or LDAP hosts	3268	Internal	Domain controller	Serving LDAP requests with global catalog (non-secured)
Active Directory or LDAP hosts	3269	Internal	Domain controller (LDAPS)	Serving LDAP requests with global catalog (secured)

If you want to forward logs to vRealize Log Insight, the following port must also be open.

Object	Port Number	Network	Service or Product	Description
vRealize Log Insight syslog server	514 (TCP or UDP)	Internal	Syslog server	Syslog service

If you deploy Ceilometer, the following ports must also be open.

Object	Port Number	Network	Service or Product	Description
Ceilometer and Gnocchi storage nodes	22	Internal	SSH	SSH (used by Ansible)
Load balancer and Gnocchi storage nodes	8041	Public and internal	OpenStack API services	Gnocchi API endpoint

Object	Port Number	Network	Service or Product	Description
Load balancer and Ceilometer nodes	8042	Public and internal	OpenStack API services	Aodh API endpoint
Load balancer and Ceilometer nodes	8779	Public and internal	OpenStack API services	Panko API endpoint

If you deploy Designate, the following ports must also be open.

Object	Port Number	Network	Service or Product	Description
Load balancer nodes	53 (UDP)	Public	DNS	Designate MiniDNS service
Load balancer and controller nodes	9001	Public and internal	OpenStack API services	Designate endpoint

If you deploy Swift, the following port must also be open.

Object	Port Number	Network	Service or Product	Description
Load balancer nodes	8080	Public	OpenStack API services	Swift endpoint

Configure NSX-T Data Center for OpenStack

If you want to use NSX-T Data Center as the networking solution for VMware Integrated OpenStack, deploy and configure NSX-T Data Center as described in the following procedure.

Prerequisites

- Deploy vSphere, including vCenter Server and all ESXi hosts.
- Install NSX-T Data Center.

  a Deploy NSX Manager. See "NSX Manager Installation" in the *NSX-T Data Center Installation Guide*.

  b Deploy NSX Controller instances. See "NSX Controller Installation and Clustering" in the *NSX-T Data Center Installation Guide*.

  c Join each NSX Controller with the NSX Manager. See "Join NSX Controllers with the NSX Manager" in the *NSX-T Data Center Installation Guide*.

  d Initialize the control cluster. See "Initialize the Control Cluster to Create a Control Cluster Master" in the *NSX-T Data Center Installation Guide*.

  e If you deployed multiple NSX Controller instances, join them to the cluster. See "Join Additional NSX Controllers with the Cluster Master" in the *NSX-T Data Center Installation Guide*.

  f (Optional) Add your vCenter Server instance as a compute manager. See "Add a Compute Manager" in the *NSX-T Data Center Installation Guide*.

g (NSX-T Data Center 2.4 or later) If you want to use an NSX Manager cluster, deploy additional NSX Manager nodes. See "Deploy NSX Manager Nodes to Form a Cluster from UI" in the *NSX-T Data Center Installation Guide*.

Note An NSX Manager cluster provides high availability for a single NSX-T Data Center instance. Multiple instances of NSX-T Data Center cannot be used with the same VMware Integrated OpenStack deployment.

h Deploy NSX Edge nodes. See "NSX Edge Installation" in the *NSX-T Data Center Installation Guide*.

Procedure

1 Log in to the NSX Manager as an administrator.

2 Add your ESXi hosts to the NSX-T Data Center fabric.

a Select **Fabric > Nodes**.

b In the **Hosts** tab, click **Add**.

c Enter the name, management IP address, user name, and password of the host.

You can also enter a host thumbprint. If you do not enter a thumbprint, NSX-T Data Center will prompt you to use the default thumbprint provided by the host.

d Click **Add**.

3 Create an IP address pool for tunnel endpoints.

a Select **Inventory > Groups**.

b In the **IP Pools** tab, click **Add**.

c Enter a name and description for the IP address pool.

d Under **Subnets**, click **Add**.

e Click the first entry under each column and specify the IP address range, gateway, and network address.

You can also specify DNS servers (separated by commas) and a DNS suffix.

f Click **Add**.

4 Create an overlay transport zone.

a Select **Fabric > Transport Zones** and click **Add**.

b Enter a name, description, and N-VDS name for the overlay transport zone.

The N-VDS name will be used for the N-VDS that is installed on transport nodes added to this transport zone.

c Select **Standard** or **Enhanced Datapath** for the N-VDS mode.

   d Select **Overlay** for the traffic type.

   e Click **Add**.

5 Create a VLAN transport zone.

   a Select **Fabric > Transport Zones** and click **Add**.

   b Enter a name, description, and N-VDS name for the overlay transport zone.

   The N-VDS name will be used for the N-VDS that is installed on transport nodes added to this transport zone.

   c Select **Standard** or **Enhanced Datapath** for the N-VDS mode.

   d Select **VLAN** for the traffic type.

   e Click **Add**.

6 Create an uplink profile.

   a Select **Fabric > Profiles**.

   b In the **Uplink Profiles** tab, click **Add**.

   Note If you are using a physical link on an ESXi host, you can modify the default policy instead of creating a new one.

   c Enter a name and description for the profile.

   d (Optional) Under **LAGs**, add and configure one or more link aggregation groups (LAGs).

   e Under **Teamings**, add a new teaming policy or configure the default policy.

   f In the **Active Uplinks** column, specify a physical link on your ESXi host or NSX Edge node.

   The link must be up and available.

   If you are using a physical link on an ESXi host, you can also specify a standby uplink if desired.

   g In the **Transport VLAN** text box, enter the VLAN ID of the physical network.

   h Retain the default MTU value of 1600.

   i Click **Add**.

7 If you want to use N-VDS in standard mode, create a Network I/O Control (NIOC) profile.

   a Select **Fabric > Profiles**.

   b In the **NIOC Profiles** tab, click **Add**.

   c Enter a name and description for the profile.

   d Set **Status** to **Enabled**.

   e Under **Host Infra Traffic Resource**, specify the desired traffic types and bandwidth allocations.

   f Retain the default MTU value of 1600.

   g Click **Add**.

8 Add the ESXi hosts in your compute cluster to the overlay transport zone.

   a Select **Fabric > Nodes**.

   b In the **Transport Nodes** tab, click **Add**.

   c Enter a name for the transport node.

   d From the **Node** drop-down list, select the desired ESXi host.

   e Under **Transport Zones**, select the overlay transport zone in the **Available** column and click the left arrow to move it to the **Selected** column.

   f Open the **N-VDS** tab.

   g Select the N-VDS for the overlay transport zone and the uplink profile that you created in this procedure.

     If you are using a standard N-VDS, select the NIOC profile also.

   h From the **IP Assignment** drop-down list, select **Use IP Pool**.

   i From the **IP Pool** drop-down list, select the tunnel endpoint IP address pool that you created in this procedure.

   j From the **Physical NICs** drop-down lists, select an unused NIC and uplink.

   k Click **Add**.

9 Add NSX Edge nodes to the overlay and VLAN transport zones.

   a Select **Fabric > Nodes**.

   b In the **Transport Nodes** tab, click **Add**.

   c Enter a name for the transport node.

   d From the **Node** drop-down list, select the desired NSX Edge node.

   e Under **Transport Zones**, select the overlay and VLAN transport zones in the **Available** column and click the left arrow to move them to the **Selected** column.

   f Open the **N-VDS** tab.

   g Select the N-VDS for the overlay transport zone and the uplink profile that you created in this procedure.

     If you are using a standard N-VDS, select the NIOC profile also.

   h From the **IP Assignment** drop-down list, select **Use IP Pool**.

   i From the **IP Pool** drop-down list, select the tunnel endpoint IP address pool that you created in this procedure.

   j From the **Virtual NICs** drop-down lists, select an unused NIC and uplink.

   k Click **Add N-VDS**.

l Select the N-VDS for the VLAN transport zone and the uplink profile that you created in this procedure.

If you are using a standard N-VDS, select the NIOC profile also.

m From the **IP Assignment** drop-down list, select **Use DHCP**.

n From the **Virtual NICs** drop-down lists, select an unused NIC and uplink.

o Click **Add**.

10 Create an edge cluster and add NSX Edge nodes to it.

a Select **Fabric > Nodes**.

b In the **Edge Clusters** tab, click **Add**.

c Enter a name and description for the cluster.

d Select an edge cluster profile from the drop-down list.

e From the **Member Type** drop-down list, select **Edge Node**.

f Select the NSX Edge nodes in the **Available** column and click the left arrow to move them to the **Selected** column.

g Click **OK** and click **Add**.

11 Create a logical switch.

a Select **Networking > Switching**.

b In the **Switches** tab, click **Add**.

c Enter a name and description for the switch.

d Select the VLAN transport zone.

e Specify the VLAN ID of the network.

f Click **Add**.

12 Create a tier-0 router.

a Select **Networking > Routers**.

b In the **Routers** tab, click **Add > Tier-0 Router**.

c Enter a name and description for the router.

d Select the edge cluster that you created in this procedure.

e Select **Active-Active** or **Active-Standby** as the high availability mode.

f If you want to use **Active-Standby** mode, select **Preemptive** or **Non-Preemptive** as the failover mode and select a preferred member from the edge cluster.

g Click **Add**.

13 Create a port on the tier-0 router to associate with the upstream physical router.

   a Select **Networking > Routers**.

   b In the **Routers** tab, click the name of your tier-0 router.

   c Select **Configuration > Router Ports** and click **Add**.

   d Enter a name and description for the port.

   e In the **Type** field, select **Uplink**.

   f From the **Transport Node** drop-down list, select a member of the edge cluster.

   g From the **Logical Switch** drop-down list, select the switch that you created in this procedure.

   h Select **Attach to new switch port** and enter a name for the switch port.

   i Enter the IP address of the router port in CIDR format (for example, 192.0.2.20/24).

   Note This IP address cannot be within the subnet of any OpenStack external network.

   j Click **Add**.

14 Enable BGP on the tier-0 router and add BGP neighbors.

   a Select **Networking > Routers**.

   b In the **Routers** tab, click the name of your tier-0 router.

   c Select **Routing > BGP** and click **Edit**.

   d Toggle **Status** to **Enabled**.

   e Enter your AS number and click **Save**.

   f Under **Neighbors**, click **Add**.

   g Enter the IP address and a description of the BGP neighbor.

   h Enter the remote AS number for the neighbor.

   i Open the **Local Address** tab.

   j From the **Type** drop-down list, select **Uplink**.

   k Select the uplink ports in the **Available** column and click the left arrow to move them to the **Selected** column.

   l Click **Add**.

What to do next

Prepare your vSphere environment to install VMware Integrated OpenStack.

VMware Integrated OpenStack can generate a new DHCP profile and metadata proxy server for your deployment. You are no longer required to configure these items in advance.

If you want to manually configure a metadata proxy server in NSX-T Data Center before deployment, specify the first IP address in the VMware Integrated OpenStack management network IP range as the URL for the Nova server.

Prepare to Install VMware Integrated OpenStack with NSX-T Data Center

If you have chosen to deploy VMware Integrated OpenStack with NSX-T Data Center, configure your environment as described in the following procedure.

Prerequisites

- Deploy vCenter Server and all ESXi hosts.
- Deploy and configure NSX-T Data Center and all related nodes. See Configure NSX-T Data Center for OpenStack.

  Note VMware Integrated OpenStack can generate a new DHCP profile and metadata proxy server for your deployment. You are no longer required to configure these items in advance.

  If you want to manually configure a metadata proxy server in NSX-T Data Center before deployment, specify the first IP address in the VMware Integrated OpenStack management network IP range as the URL for the Nova server.
- Open the TCP and UDP ports required by VMware Integrated OpenStack. See Required Network Ports.
- Create a PTR record associating the IP address planned for the OpenStack Management Server with its FQDN, and ensure that the OpenStack Management Server can connect to a DNS server.
- Obtain the following NSX-T Data Center parameters. You configured these parameters when deploying NSX-T Data Center.
  - FQDN or IP address of the NSX Manager
  - Username and password to access the NSX Manager
  - Overlay transport zone
  - VLAN transport zone
  - Tier-0 router
  - DHCP profile (if configured in NSX-T Data Center)
  - Metadata proxy server and value of the `secret` parameter (if configured in NSX-T Data Center)

Procedure

1 Configure the management, API access, transport, and external networks and assign a dedicated VLAN to each.

a Ensure that the management and API access networks have sufficient IP addresses to support your deployment.

The required size of these networks depends on the deployment mode and on whether you want to deploy Ceilometer.

Deployment Mode	IP Address Requirements
HA	■ Management network: 11 contiguous IP addresses ■ API access network: 2 contiguous IP addresses
HA with Ceilometer	■ Management network: 16 contiguous IP addresses ■ API access network: 2 contiguous IP addresses
Compact or tiny	■ Management network: 4 contiguous IP addresses ■ API access network: 1 IP address
Compact or tiny with Ceilometer	■ Management network: 9 contiguous IP addresses ■ API access network: 1 IP address

Important Ensure that the management network and API access network can each be expanded to twice the original number of IP addresses during upgrades. When upgrading VMware Integrated OpenStack, you will temporarily require sufficient IP addresses to support two deployments.

b Ensure that the vCenter Server, NSX Manager, and NSX Controller instances can access the management network on Layer 2 or Layer 3.

c Ensure that the API access network is externally accessible.

d On the transport network, set the Maximum Transmission Unit (MTU) to 1600 bytes.

2 On your vCenter Server instance, create a data center.

3 In the data center, create the management cluster.

- For HA deployments, the cluster must contain at least three hosts and at least one datastore.
- For compact or tiny deployments, the cluster must contain at least one host and at least one datastore.

4 Create the compute cluster.

The compute cluster must contain at least one host and at least one datastore.

5 (Optional) Create the edge cluster.

If you create an edge cluster, it must contain at least one host and at least one datastore.

6 On the management and compute clusters, click the **Configure** tab and modify cluster parameters.

   a On the **vSphere DRS** page, click the **Edit...** button.

   b Enable **vSphere DRS** and click **OK**.

   c On the **vSphere Availability** page, click the **Edit...** button.

   d Enable **vSphere HA**.

   e On the **Failures and Responses** tab, select **Enable Host Monitoring**.

   f Expand the **Host Failure Response** section and set **Default VM Restart Priority** to **High**.

   g Expand the **VM Monitoring** section, select **VM and Application Monitoring** and set **VM monitoring sensitivity** to **High**.

   h On the **Admission Control** tab, ensure that admission control is enabled and click **OK**.

7 On each host in each cluster, enable virtualization hardware extensions in the BIOS.

8 On the VMkernel adapter for the management network, enable **vMotion**.

9 If you want to use datastore clusters, enable Storage DRS on the datastore clusters and set the **Cluster automation level** to **No Automation (Manual Mode)**.

10 In your data center, create one or more distributed switches for your management, compute, and edge clusters.

   A distributed switch can be shared among clusters that are Layer 2 adjacent. Create a separate distributed switch for any cluster that is not Layer 2 adjacent to the other clusters.

11 On each distributed switch created, create the management port group and tag it with the VLAN ID assigned to the management network.

12 On the distributed switch for the management nodes, create the API access port group and tag it with the VLAN ID assigned to the API access network.

13 On the distributed switch for the edge nodes, create the external port group and tag it with the VLAN ID assigned to the external network.

What to do next

After you have prepared your environment, you can install VMware Integrated OpenStack. See Chapter 6 Installing VMware Integrated OpenStack.

Installing VMware Integrated OpenStack

6

You obtain the VMware Integrated OpenStack OVA package, install it in vSphere, and then create an OpenStack deployment.

Procedure

1. Install VMware Integrated OpenStack

   You deploy VMware Integrated OpenStack on your vCenter Server instance. This installs the OpenStack Management Server, through which you configure and implement an OpenStack cloud infrastructure integrated with your vSphere deployment.

2. Create an OpenStack Deployment

   You can deploy OpenStack by using the VMware Integrated OpenStack vApp or the OpenStack Management Server API.

3. Assign the VMware Integrated OpenStack License Key

   You assign a license key for VMware Integrated OpenStack to enable its features.

4. Verify Your OpenStack Deployment

   You verify your OpenStack deployment to ensure that it is functioning properly.

Install VMware Integrated OpenStack

You deploy VMware Integrated OpenStack on your vCenter Server instance. This installs the OpenStack Management Server, through which you configure and implement an OpenStack cloud infrastructure integrated with your vSphere deployment.

Important The VMware Integrated OpenStack OVA cannot be installed in the HTML5 vSphere Client. Use the Flex-based vSphere Web Client for this procedure.

Prerequisites

- Deploy or upgrade vSphere and any other VMware products that you want to use with VMware Integrated OpenStack.
- Verify that your vCenter Server instance is correctly prepared. See Chapter 5 Preparing Your Environment.

- Obtain the VMware Integrated OpenStack 5.1 OVA file from the product download page at https://my.vmware.com/en/group/vmware/info?slug=infrastructure_operations_management/vmware_integrated_openstack/5_1. The file requires approximately 6 GB of storage space.

Procedure

1 Log in to the vSphere Web Client and select the **Hosts and Clusters** view.

2 Right-click the management cluster previously configured for VMware Integrated OpenStack and select **Deploy OVF Template...** from the pop-up menu.

3 Provide the path to the VMware Integrated OpenStack OVA and click **Next**.

4 Enter a name for the VMware Integrated OpenStack vApp, select the data center that you defined during preparation, and click **Next**.

> **Note** The name of the VMware Integrated OpenStack vApp can contain only letters, numbers, and underscores (_). The name cannot exceed 60 characters, and the combination of the vApp name and cluster name cannot exceed 80 characters.

5 Select the cluster on which to run the vApp and click **Next**.

6 Review the details of the template to be installed and click **Next**.

7 Read the license agreements and click **Accept**. Then click **Next**.

8 Specify a provisioning format and storage policy, select the datastore on which the vApp files will be stored, and click **Next**.

For more information about provisioning formats, see "About Virtual Disk Provisioning Policies" in *vSphere Virtual Machine Administration*.

9 In the **Destination Network** column, select the management network defined during preparation and click **Next**.

10 On the **Customize template** page, enter a password for the `viouser` account on the OpenStack Management Server.

You can also expand the other properties and configure parameters for the OpenStack Management Server, NTP server, and syslog server.

11 Once `All properties have valid values` is displayed in the upper left of the page, click **Next**.

12 Verify that the vApp can bind to the vService and click **Next**.

13 On the **Ready to complete** page, review your settings. When you are satisfied that the settings are correct, click **Finish** to install the vApp.

14 Select **Home > Global Inventory Lists** and click **vApps**.

15 Right-click the name of the VMware Integrated OpenStack vApp and select **Power > Power On**.

The vApp powers on and the VMware Integrated OpenStack icon appears in the main menu.

If the icon for VMware Integrated OpenStack does not appear, see "Display the VMware Integrated OpenStack vApp" in the *VMware Integrated OpenStack Administration Guide*.

What to do next

Use the vApp or API to create an OpenStack deployment.

Create an OpenStack Deployment

You can deploy OpenStack by using the VMware Integrated OpenStack vApp or the OpenStack Management Server API.

Create an OpenStack Deployment Using the Virtual Appliance

You can deploy OpenStack by using the VMware Integrated OpenStack virtual appliance on your vCenter Server instance.

Note The vApp deployment procedure does not support the following options:

- Deployment in tiny mode
- Datastore clusters

If you want to use these options, see Create an OpenStack Deployment Using the API.

Prerequisites

- Prepare your networks and vCenter Server environment. See Chapter 5 Preparing Your Environment.
- Install VMware Integrated OpenStack on your vCenter Server instance. See Install VMware Integrated OpenStack.
- Verify that all required clusters and datastores are available.
  - Clusters must include the required number of hosts and datastores and must not be consumed by another node.
  - Datastores must be mounted to the correct cluster and must not be already configured.
- Verify that the DNS server is set correctly and that the network gateway or firewall forwards DNS requests on private networks.

Procedure

1. In the vSphere Client, select **Menu > VMware Integrated OpenStack**.
2. Under **Basic Tasks**, click **Connect to an OpenStack management server**.
3. Select the OpenStack Management Server and click **OK**.
4. Click **Deploy OpenStack**.
5. Select whether you want to create a new deployment or use an exported template to populate settings.
6. Select **HA** or **Compact** from the **Deployment type** drop-down menu and click **Next**.
7. Enter a name for the deployment.

8. If you want to use multiple vCenter Server instances, deselect the **Use management vCenter Server as Compute vCenter Server** check box and enter the FQDN or IP address, administrator credentials, and availability zone of the compute vCenter Server instance.

   Otherwise, select the check box and enter the FQDN or IP address, administrator credentials, and availability zone of your vCenter Server instance.

9. If the OpenStack Management Server connects to the vCenter Server instance over a private, secure network and you need to disable certificate validation, select the **Ignore the vCenter Server certificate validation** check box.

10. Click **Next**.

11. Select the management cluster that you created during preparation and click **Next**.

12. Provide the settings for the management network and API access network that you defined during preparation and click **Next**.

    If you are deploying in compact mode, you can also enter a public hostname for the API access network.

    Important The management and API access networks cannot include more than 100 IP addresses each.

13. If you are deploying in HA mode, enter the hostname and public virtual IP address of the load balancer service and click **Next**.

14. Select the compute cluster that you created during preparation and click **Next**.

15. Select one or more datastores for the compute component to consume and click **Next**.

    The selected datastores are used to create instances.

16. Select one or more datastores for the image service component to consume and click **Next**.

    The selected datastores are used to store images.

17. Select a networking mode.

    - If you want to deploy with VDS only, click **Virtual Distributed Switch Networking** and select the VDS on which to create the port groups backing the provider network.
    - If you want to deploy with NSX Data Center for vSphere networking, click **NSX-V Networking** and specify the FQDN or IP address and administrator credentials of your NSX Manager. After the credentials are validated, select the other parameters for your NSX Data Center for vSphere deployment from the drop-down lists. You can also choose whether to enable HA for edge nodes and whether to use an independent metadata service network.

- If you want to deploy with NSX-T Data Center networking, click **NSX-T Networking** and specify the FQDN or IP address and administrator credentials of your NSX Manager. After the credentials are validated, select the other parameters for your NSX-T Data Center deployment from the drop-down lists.

  Note If you have deployed an NSX Manager cluster, specify only the parent NSX Manager node at this time. After OpenStack is deployed, specify the additional nodes as described in Configure VMware Integrated OpenStack with an NSX Manager Cluster" in the *VMware Integrated OpenStack Administration Guide*.

  You can choose to generate a new metadata proxy server and DHCP profile for VMware Integrated OpenStack by selecting the check boxes. Metadata proxy servers and DHCP profiles generated in this manner are automatically removed when the deployment is deleted.

Important You cannot change the networking mode after deploying VMware Integrated OpenStack. If you need to switch to a different networking mode, you must redeploy.

18 Click **Next**.

19 Enter the username and password for the administrator account on the VMware Integrated OpenStack dashboard.

20 If you want to configure LDAP authentication for a single domain, select the **Enable** check box in the lower pane and click the **Add** (plus sign) icon.

Important

- If you configure an LDAP domain in this step, you cannot specify additional LDAP domains later. To use multiple LDAP domains in your deployment, configure the domains after deploying OpenStack.
- If you do not specify an LDAP admin user, you must manually specify a project and administrator after deployment. For instructions, see "Configure LDAP Authentication" in the *VMware Integrated OpenStack Administration Guide*.

21 Click **Next**.

22 If you want to use vRealize Log Insight to manage logs, enter the parameters of your vRealize Log Insight syslog server.

23 Click **Next**.

24 Select whether you want to participate in the Customer Experience Improvement Program and click **Next**.

For more information, see Customer Experience Improvement Program.

25 Review your settings. When you are satisfied that the settings are correct, click **Finish**.

The VMware Integrated OpenStack vApp begins to deploy your OpenStack cloud.

The status of the deployment is displayed as `Provisioning`. When the status changes to `Running`, the deployment is complete.

What to do next

Assign a license key for VMware Integrated OpenStack.

Create an OpenStack Deployment Using the API

You can deploy OpenStack by using the OpenStack Management Server API.

For more information about APIs, see the VMware Integrated OpenStack API reference at https://code.vmware.com/apis/448.

Prerequisites

- Prepare your networks and vCenter Server environment. See Chapter 5 Preparing Your Environment.
- Install VMware Integrated OpenStack on your vCenter Server instance. See Install VMware Integrated OpenStack.
- Verify that all required clusters and datastores are available.
  - Clusters must include the required number of hosts and datastores and must not be consumed by another node.
  - Datastores must be mounted to the correct cluster and must not be already configured.
- Verify that the DNS server is set correctly and that the network gateway or firewall forwards DNS requests on private networks.

Procedure

1. In the vSphere Client, select **Menu > VMware Integrated OpenStack**.
2. Under **Basic Tasks**, click **Connect to an OpenStack management server**.
3. Select the OpenStack Management Server and click **OK**.
4. Using an HTTP client, authenticate with the OpenStack Management Server API endpoint using the administrator credentials for your vCenter Server instance.

   This procedure uses cURL as an example.

   ```
   curl -X POST https://mgmt-server-ip:8443/login -d "username=vcenter-user&password=vcenter-
   password" -v
   ```

5. Deploy OpenStack with your specifications.

   ```
   curl -X POST https://mgmt-server-ip:8443/v1/clusters -b JSESSIONID=session-id -d
   "{specifications}"
   ```

   The value of `JSESSIONID` is displayed in the output from Step 1.

   The schema is as follows:

```
{
  "attributes": {},
  "deployment_type": "{LARGE | SINGLEVM | TINY}",
  "management_cluster": {
    "moid": "mgmt-cluster-moid",
    "name": "mgmt-cluster-name"
  },
  "name": "deployment-name",
  "network_mapping": {
    "data_network": "api-access-network-name",
    "external_network": "external-network-name",
    "management_network": "mgmt-network-name",
    "metadata_network": "metadata-network-name"
  },
  "networkings": [
    {
      "dns1": "dns-server-ip1",
      "dns2": "dns-server-ip2",
      "gateway": "gateway-ip",
      "ip_blocks": [
        {
          "begin_ip": "ip-range-start",
          "end_ip": "ip-range-end"
        }
      ],
      "name": "network-name",
      "netmask": "subnet-mask",
      "portgroup_moref": "port-group-moid",
      "portgroup_name": "port-group-name"
    }
  ],
  "openstack_info": {
    "attributes": {},
    "availability_zones": [
      {
        "attributes": {},
        "name": "az-name"
      }
    ],
    "compute": {
      "attributes": {},
      "compute_clusters": [
        {
          "attributes": {},
          "availability_zone_name": "compute-cluster-
az",
          "cluster_moid": "compute-cluster-moid",
          "cluster_name": "compute-cluster-name",
          "datastore_regex": "compute-datastores",
          "esxi_netmask": "host-subnet-mask",
          "vcenter_ip": "compute-vcserver-ip"
        }
      ]
    },
    "identity": {
      "ad_domains": [
        {
          "attributes": {},
          "bind_password": "ldap-ad-user-password",
          "bind_user": "ldap-ad-user",
          "force_ldaps": {true | false},
          "ldap_admin_user": "ldap-admin",
          "ldap_certificates": [
            "cert-content"
```

`deployment_type`: Enter **LARGE** for an HA deployment, **SINGLEVM** for a compact deployment, or **TINY** for a tiny deployment.

`networkings`: Create a copy of the contents of the `networkings` section for each network that you want to configure. Ensure that the value of the `name` parameter for each network is the name of the corresponding network in the `network_mapping` section.

`netmask`: Enter the value of `netmask` as a network address (for example, `255.255.255.0`).

`availability_zones`: Create a copy of the contents of the `availability_zones` section for each availability zone that you want to create.

`compute_clusters`: Create a copy of the contents of the `compute_clusters` section for each compute cluster that you want to configure. To specify a datastore cluster for a compute cluster to consume, include the following parameter inside the `attributes` section:

`"nova_datastore_cluster": "ds-cluster-name"`

`datastore_regex`: You can enter a regular expression to add all matching datastores.

Important Configuring an LDAP domain is optional. If you configure an LDAP domain through this API, you cannot specify additional LDAP domains later. To use multiple LDAP domains in your deployment, configure the domains after deploying OpenStack.

```
          ],
          "ldap_group_desc_attribute": "group-
description",
          "ldap_group_filter": "group-search-filter",
          "ldap_group_id_attribute": "group-id",
          "ldap_group_member_attribute": "group-
member",
          "ldap_group_name_attribute": "group-name",
          "ldap_group_objectclass": "group-object-
class",
          "ldap_group_tree_dn": "group-tree-dn",
          "ldap_search_scope": "search-scope",
          "ldap_url": "ldap-url",
          "ldap_use_start_tls": {true | false},
          "ldap_user_enabled_attribute": "enabled-
attribute",
          "ldap_user_filter": "user-search-filter",
          "ldap_user_id_attribute": "user-id",
          "ldap_user_mail_attribute": "user-email",
          "ldap_user_name_attribute": "user-name",
          "ldap_user_objectclass": "user-object-
class",
          "ldap_user_pass_attribute": "user-password",
          "ldap_user_tree_dn": "user-tree-dn"
        }
      ],
      "admin_project_name": "admin-project-name",
      "attributes": {},
      "sql_domain": {
        "admin_password": "admin-password",
        "admin_user": "admin-username",
        "attributes": {}
      },
      "token_expiration_time": "token-expiration-
seconds"
    },
    "image": {
      "datastores": [
        {
          "datastores": "glance-datastore",
          "vcenter_ip": "glance-vcserver-ip"
        }
      ],
      "glance_folder": "image-folder"
    },
    "network": {
      "attributes": {},
      "dvs": {},
      "neutron_backend": "{DVS | NSXV | NSXV3}",
      "nsxv": {
        "nsxv_dvs_moref": "nsxv-vds-moid",
        "nsxv_dvs_name": "nsxv-vds-name",
        "nsxv_edge_cluster_moref": "edge-cluster-
moid",
        "nsxv_edge_cluster_name": "edge-cluster-name",
        "nsxv_edge_ha": "{TRUE | FALSE}",
        "nsxv_exclusive_router_appliance_size":
"string",
        "nsxv_external_network_name": "external-
network-name",
        "nsxv_manager": "nsx-manager-ip",
        "nsxv_password": "nsx-manager-password",
        "nsxv_username": "nsx-manager-username",
        "nsxv_vdn_scope_moref": "vdn-scope-moid"
      },
```

`neutron_backend`: Enter **DVS** for VDS networking, **NSXV** for NSX Data Center for vSphere networking, or **NSXV3** for NSX-T Data Center networking.

The fields in the `nsxv` section apply only to deployments with NSX Data Center for vSphere networking. The fields in the `nsxv3` section apply only to deployments with NSX-T Data Center networking. The values of these fields will be ignored in other deployments.

```
       "nsxv3": {
         "nsxv3_api_managers": "nsx-manager-ip",
         "nsxv3_api_password": "nsx-manager-password",
         "nsxv3_api_username": "nsx-manager-username",
         "nsxv3_default_overlay_tz": "nsx-overlay-
zone",
         "nsxv3_default_tier0_router": "t0-router",
         "nsxv3_default_vlan_tz": "nsx-vlan-zone",
         "nsxv3_edge_cluster_name": "edge-cluster-
name",
         "nsxv3_edge_cluster_uuid": "edge-cluster-
uuid",
         "nsxv3_md_shared_password": "metadata-proxy-
secret",
         "nsxv3_native_dhcp_profile": "dhcp-profile",
         "nsxv3_native_dhcp_profile_oms_create":
"{true | false}",
         "nsxv3_native_md_proxy": "metadata-proxy-ip"
         "nsxv3_native_md_proxy_oms_create": "{true |
false}"
       }
     },
     "region_name": "openstack-region",
     "syslog": {
       "port": "port-number",
       "protocol": "{UDP | TCP}",
       "server": "syslog-server-ip",
       "tag": "string"
     },
     "vcenter_insecure": "{true | false}",
     "volumn": {
       "attributes": {},
       "cinder_folder": "cinder-folder"
     }
   },
   "public_access": {
     "public_hostname": "public-api-hostname",
     "public_vip": "public-api-vip"
   },
   "root_ca_certificates": [
     "root-ca-content"
   ],
   "vcenters": [
     {
       "attributes": {},
       "hostname": "vcserver-hostname",
       "password": "vcserver-admin-password",
       "username": "vcserver-admin-user"
     }
   ],
   "version": "v1"
}
```

`nsxv3_native_dhcp_profile_oms_create`: Enter **`true`** to automatically generate a DHCP profile for OpenStack. The `nsxv3_native_dhcp_profile` parameter will then be ignored.

`nsxv3_native_md_proxy_oms_create`: Enter **`true`** to automatically generate a metadata proxy server for OpenStack. The `nsxv3_native_md_proxy` parameter will then be ignored.

Note To specify a datastore cluster for block storage to consume, include the following parameters inside the `attributes` section under `volumn`:

```
"cinder_vmware_datastore_cluster": "ds-
cluster-name",
"cinder_vmware_sdrs_default_cluster_name":
"compute-cluster-name"
```

Set the value of `cinder_vmware_datastore_cluster` to the datastore cluster that you want to use for block storage. Set the value of `cinder_vmware_sdrs_default_cluster_name` to the compute cluster used to create raw Cinder volumes.

What to do next

Assign a license key for VMware Integrated OpenStack.

Assign the VMware Integrated OpenStack License Key

You assign a license key for VMware Integrated OpenStack to enable its features.

For more information about licensing, see VMware Integrated OpenStack Licensing.

Prerequisites

- Install VMware Integrated OpenStack.
- Obtain your VMware Integrated OpenStack license key from the license portal at https://my.vmware.com/group/vmware/my-licenses.

Procedure

1. In the vSphere Client, select **Menu > Administration**.
2. Under **Licensing**, click **Licenses**.
3. Open the **Assets** tab and select **Solutions**.
4. Select **VMware Integrated OpenStack 5.0** and click **Assign License**.
5. Click **New License** and enter your VMware Integrated OpenStack license key and name.
6. Review the license information and click **OK**.

What to do next

Verify that OpenStack has been successfully deployed.

Verify Your OpenStack Deployment

You verify your OpenStack deployment to ensure that it is functioning properly.

Procedure

1. In the vSphere Client, select **Menu > VMware Integrated OpenStack** and click **OpenStack Deployments**.
2. In the **Deployment List** tab, confirm that the status of your deployment is `Running`.
3. Click the name of the deployment and confirm that the status of all nodes is `Service Ready`.
4. In a web browser, enter the first IP address in the API access network and confirm that you can access the VMware Integrated OpenStack dashboard.
5. Log in with the user name and password that you configured during deployment.

If you can successfully perform the preceding actions, this indicates that the OpenStack deployment has been created successfully.

What to do next

You have successfully installed VMware Integrated OpenStack. See Chapter 7 Configuring Additional Components and Features to add features and integration to your deployment. See the *VMware Integrated OpenStack Administration Guide* for information about managing your deployment.

Configuring Additional Components and Features 7

After installing VMware Integrated OpenStack, you can configure additional OpenStack components and integrate your deployment with vRealize Operations Manager.

This chapter includes the following topics:

Integrate VMware Integrated OpenStack with vRealize Operations Manager

You can monitor OpenStack resources in vRealize Operations Manager by installing the vRealize Operations Management Pack for VMware Integrated OpenStack and the End Point Operations Management agent.

Prerequisites

- Deploy vRealize Operations Manager. See *VMware vRealize Operations Manager Help*.
- Install the vRealize Operations Management Pack for VMware Integrated OpenStack. See "Installing and Configuring the Management Pack for VMware Integrated OpenStack" in the *VMware vRealize Operations Management Pack for VMware Integrated OpenStack* document.

Procedure

1 Obtain the End Point Operations Management agent installation file for Linux in GZ format.

   a Go to the vRealize Operations Manager download page at https://my.vmware.com/en/group/vmware/info/slug/infrastructure_operations_management/vmware_vrealize_operations/7_0 and select your version of vRealize Operations Manager.

   b Under **Product Downloads**, find your edition of vRealize Operations Manager and click **Go to Downloads**.

   c Find `End Point Operations Linux Agent - 64 bit (gz file)` and click **Download Now**.

2 Transfer the End Point Operations Management agent installation file to the OpenStack Management Server and decompress it to a temporary directory.

3 In the temporary directory, open the `conf/agent.properties` file and modify the following parameters to match your vRealize Operations Manager deployment.

```
agent.setup.serverIP=vrops-server-ip
agent.setup.serverSSLPort=vrops-server-ssl-port
agent.setup.serverLogin=vrops-admin-username
agent.setup.serverPword=vrops-admin-password
agent.setup.serverCertificateThumbprint=vrops-server-cert-thumbprint
```

4 Install the End Point Operations Management agent in VMware Integrated OpenStack.

```
sudo viocli epops install -s epops-install-file.tar.gz -c epops-dir/conf/agent.properties
```

VMware Integrated OpenStack objects are displayed in the vRealize Operations Manager **Inventory Explorer** in the **EP Ops Adapter Resources Group**.

What to do next

If you need to reconfigure the End Point Operations Management agent, modify the `agent.properties` file and run the following command:

```
sudo viocli epops reconfig -c epops-dir/conf/agent.properties
```

For more information about command-line parameters, see "viocli epops Command" in the *VMware Integrated OpenStack Administration Guide*.

Integrate VMware Integrated OpenStack with vRealize Log Insight

You can monitor OpenStack data in vRealize Log Insight using dashboards provided by the VMware OpenStack Content Pack.

For more information about the VMware OpenStack Content Pack, see the VMware OpenStack Content Pack page at https://marketplace.vmware.com/vsx/solutions/openstack-content-pack.

Prerequisites

Deploy vRealize Log Insight. See the *Getting Started* document for your version of vRealize Log Insight.

Procedure

1 Install the VMware OpenStack Content Pack in vRealize Log Insight.

   a Log in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission.

   b From the drop-down menu on the upper right, select **Content Packs**.

   c Click **Marketplace** under **Content Pack Marketplace** on the left.

   d Click **OpenStack**.

   e Select the check box to agree to the terms of the license agreement.

   f Click **Install**.

   For more information about vRealize Log Insight content packs, see "Working with Content Packs" in the *Using vRealize Log Insight* document for your version.

2 If you did not configure a syslog server when deploying OpenStack, modify your deployment configuration to send logs to vRealize Log Insight.

   a In the vSphere Client, select **Menu > VMware Integrated OpenStack**.

   b Click **OpenStack Deployments** and open the **Manage** tab.

   c On the **Settings** tab, click **Syslog Server** and click **Edit**.

   d Enter the IP address, port, and protocol of your vRealize Log Insight syslog server and click **OK**.

You can monitor OpenStack data in vRealize Log Insight on the dashboards under **Content Pack Dashboards > OpenStack**.

Integrate VMware Integrated OpenStack with vRealize Automation

You can integrate VMware Integrated OpenStack with vRealize Automation through vRealize Orchestrator to enforce control and governance, manage OpenStack deployments as resource pools, and manage VMware Integrated OpenStack from the vRealize Automation portal.

You integrate the two solutions by enabling Keystone federation, configuring the vRealize Automation tenant FQDN through the OpenStack Management Server, and installing the vRealize Orchestrator OpenStack plug-in.

Prerequisites

- Deploy and configure vRealize Automation. See the *Installing or Upgrading vRealize Automation* document for your version.
- Deploy and configure vRealize Orchestrator. See the *Installing and Configuring VMware vRealize Orchestrator* document for your version.

Procedure

1 Log in to the OpenStack Management Server.

2 Add vRealize Automation as a Keystone identity provider.

```
sudo viocli federation identity-provider add --type vidm
```

You are prompted to enter the following information.

Option	Description
Identity provider name [None]:	Name of the identity provider
Identity provider display name (for Horizon) [VMware Identity Manager]:	Name of the identity provider to be displayed on the VMware Integrated OpenStack dashboard
Description [None]:	Custom description for this identity provider
vIDM endpoint address [None]:	IP address of your VMware Identity Manager endpoint in the format `https://`*`vidm-endpoint-ip`*`.eng.vmware.com`
vIDM admin user [admin]:	Username of the VMware Identity Manager administrator
vIDM admin password:	Password for the VMware Identity Manager administrator
Do not verify certificates when establishing TLS/SSL connections [False]:	Enter `true` to disable certificate verification or `false` to enable certificate verification.
vIDM tenant name []:	Enter `vsphere.local`
Enter the name of the domain that federated users associate with [Default]:	Domain to which all federated users belong. If the specified domain does not exist, it will be created.
Enter the name to the groups that federated users associate with (separated by commas ",") []:	Groups to which all federated users belong. If the specified groups do not exist, they will be created. **Note** Include all groups defined in your custom mappings.
Do you want to change advanced settings? (Y/N)	Enter `N`

3 Update the deployment configuration.

```
sudo viocli identity configure
```

This command causes your VMware Integrated OpenStack deployment to go down temporarily.

4 Configure the VMware Integrated OpenStack tab for your vRealize Automation tenant.

```
sudo viocli vros enable -vt vra-tenant-name -vh vra-ip -va vra-admin -vrs mgmt-server-ip
```

Note Enter the `vra-tenant-name` value in all uppercase letters.

5 Deploy the vRealize Orchestrator OpenStack Plug-In.

See "Deploy the vRealize Orchestrator OpenStack Plug-In" in the *Using the vRealize Orchestrator OpenStack Plug-In 2.0* document.

You can now manage VMware Integrated OpenStack through the vRealize Automation portal and design and consume blueprints.

For more information, see *Using the vRealize Orchestrator OpenStack Plug-In*.

Configure the Barbican Component

Barbican is a component of OpenStack that stores, provisions, and manages secret data. It acts as the key manager for VMware Integrated OpenStack.

Barbican is enabled and configured with the simple crypto plugin when you install or upgrade to VMware Integrated OpenStack 5.1. After deployment, you can modify the configuration to use Key Management Interoperability Protocol (KMIP).

Note With Barbican, tenants must explicitly grant the `barbican` user access to the certificates, keys, and TLS containers for their projects in your deployment. If you do not want tenants to configure the ACL, you can modify `custom-playbook.yml` to grant the `barbican` user access to all objects stored in Barbican. Because tenants may store objects unrelated to LBaaS in Barbican, ensure that you understand and accept the security implications of this action before proceeding.

To grant the `barbican` user access to all objects stored in Barbican, specify `"rule:all_users"` as the value of `secret:get` and `container:get` in the `/etc/barbican/policy.json` file.

Procedure

1 Log in to the OpenStack Management Server.

2 Configure Barbican to use the KMIP plugin.

```
sudo viocli barbican --secret-store-plugin KMIP --host kmip-server --port kmip-port --ca-certs ca-cert-file [--certfile local-cert-file --keyfile local-key-file --user kmip-user --password kmip-password]
```

Depending on the implementation of KMIP in your environment, you may need to include the `--certfile` and `--keyfile` parameters only, the `--user` and `--password` parameters only, or all four of these parameters.

Barbican uses KMIP instead of simple crypto.

Note If the payload of a secret is in plaintext, tenants must now include the `--secret-type passphrase` parameter when creating the secret.

What to do next

Tenants can now configure LBaaS v2.0. For instructions, see "Configuring LBaaS v2.0" in the *VMware Integrated OpenStack User's Guide*.

Enable the Ceilometer Component

Ceilometer is a component of OpenStack that polls, collects, and publishes OpenStack service data.

The VMware Integrated OpenStack implementation of Ceilometer includes the Aodh, Panko, and Gnocchi projects.

After deploying VMware Integrated OpenStack, you can enable Ceilometer to perform telemetry functions. Enabling or disabling Ceilometer may temporarily affect other OpenStack services.

Prerequisites

Ensure that your environment has been prepared for Ceilometer, including five extra contiguous IP addresses on the management network. For other requirements, see the Additional Components section of Hardware Requirements for VMware Integrated OpenStack and the relevant table in Required Network Ports.

Procedure

1 In the vSphere Client, select **Menu > VMware Integrated OpenStack**.

2 Click **OpenStack Deployments** and open the **Manage** tab.

3 On the **Settings** tab, click **Ceilometer** and click **Enable**.

The virtual machines required by Ceilometer are created and the service is enabled.

If Ceilometer does not enter the enabled state, this indicates that an error occurred. Confirm that your environment meets the hardware requirements for Ceilometer and check `/var/log/oms/oms.log` on the OpenStack Management Server to determine the nature of the error.

What to do next

If you no longer want to use Ceilometer, you can disable it on this page. This will stop the Ceilometer service and remove all Ceilometer nodes.

Enable the Designate Component

Designate is a component of OpenStack that provides DNS as a service, including domain name registration and zone and record set management for OpenStack clouds.

After deploying VMware Integrated OpenStack, you can enable Designate to provide DNS functions. Enabling or disabling Designate may temporarily affect other OpenStack services.

Enable the Designate Component Using the GUI

You can enable Designate by using the VMware Integrated OpenStack vApp.

Prerequisites

VMware Integrated OpenStack supports Infoblox, Bind9, and PowerDNS back-end servers for Designate. The prerequisites for each type of back-end server are listed as follows.

Infoblox:

- Install the Infoblox back end on a network that is connected to a public network in VMware Integrated OpenStack.
- Create a user for Designate to use.
- Create one name server group to serve Designate zones.
  - Set the Designate mDNS servers as external primaries. Set all IP addresses on the eth1 interface of the load balancer node as external primaries.
  - Add a grid member as a grid secondary and select the `Lead Secondary` option for this member.
  - Add additional grid secondaries as needed.

Bind9:

- Install the Bind9 back end on a network that is connected to a public network in VMware Integrated OpenStack.
- Enable `rndc addzone` or `rndc delzone` functionality to allow receipt of a NOTIFY message from a non-master node. Open `named.conf.options` or `named.conf` in a text editor and add the following lines under options:

  ```
  allow-new-zones yes;
  allow-notify{any;};
  ```

PowerDNS:

- Install PowerDNS on a network that is connected to a public network in VMware Integrated OpenStack.
- Enable the API in the `pdns.conf` file.

Procedure

1. In the vSphere Client, select **Menu > VMware Integrated OpenStack**.
2. Click **OpenStack Deployments** and open the **Manage** tab.
3. On the **Settings** tab, select **Configure Designate** and click **Edit**.
4. Specify the options for your back end and click **Configure**.
   - Infoblox back end

Option	Description
Type	Select **Infoblox**.
DNS server	Enter the Infoblox server IP address.
DNS port	Enter the port on the Infoblox server for the DNS service. The default value is `53`.

Option	Description
WAPI URL	Enter the Infoblox WAPI URL. The default is `https://`*`infoblox-server`*`/wapi/`*`wapi-version`*`/`. **Note** The URL must end with a slash (/).
Username	Enter the username for Designate to access the Infoblox API.
Password	Enter the password for the Infoblox username.
NS group	Specify the name server group to serve Designate zones.

- Bind9 back end

Option	Description
Type	Select **Bind9**.
DNS server	Enter the Bind9 server IP address.
DNS port	Enter the port on the Bind9 server for the DNS service. The default value is `53`.
RNDC host	Enter the RNDC server IP address. The default value is the Bind9 server IP address.
RNDC port	Enter the RNDC port. The default value is 953.
RNDC key	Enter the contents of the `/etc/bind/rndc.key` file.

- PowerDNS back end

Option	Description
Type	Select **PowerDNS**.
DNS server	Enter the PowerDNS server IP address.
DNS port	Enter the port on the PowerDNS server for the DNS service. The default value is `53`.
API endpoint	Enter the PowerDNS API endpoint URL. The default value is `http://`*`powerdns-server`*`/8081`.
API key	Enter the value of `api-key` in the `/etc/powerdns/pdns.conf` file.

5 If you are running VMware Integrated OpenStack 5.1, modify the Designate database to prevent duplicate entries.

   This step is not necessary if you have patched your deployment to version 5.1.0.1.

   a Log in to the active database node and switch to the `root` user.

   ```
   sudo su –
   ```

   b Open the Designate database.

   ```
   mysql
   use designate
   ```

   c Modify the database to prevent duplicate entries.

   ```
   ALTER TABLE service_statuses
   ADD UNIQUE (`hostname`, `service_name`);
   ```

Your tenants can now create DNS zones using the VMware Integrated OpenStack dashboard. For instructions, see "Create a DNS Zone" in the *VMware Integrated OpenStack User's Guide*.

What to do next

See the OpenStack Designate CLI documentation at https://docs.openstack.org/python-designateclient/queens/user/shell-v2.html for information on how to use Designate.

Important VMware Integrated OpenStack supports only the v2 API. To perform command-line operations, use the `openstack` command instead of the `designate` command.

Enable the Designate Component Using the CLI

You can enable Designate by modifying the `custom.yml` file in your environment.

Prerequisites

VMware Integrated OpenStack supports Infoblox, Bind9, and PowerDNS back-end servers for Designate. The prerequisites for each type of back-end server are listed as follows.

Infoblox:

- Install the Infoblox back end on a network that is connected to a public network in VMware Integrated OpenStack.
- Create a user for Designate to use.
- Create one name server group to serve Designate zones.
  - Set the Designate mDNS servers as external primaries. Set all IP addresses on the eth1 interface of the load balancer node as external primaries.
  - Add a grid member as a grid secondary and select the `Lead Secondary` option for this member.
  - Add additional grid secondaries as needed.

Bind9:

- Install the Bind9 back end on a network that is connected to a public network in VMware Integrated OpenStack.
- Enable `rndc addzone` or `rndc delzone` functionality to allow receipt of a NOTIFY message from a non-master node. Open `named.conf.options` or `named.conf` in a text editor and add the following lines under options:

  ```
  allow-new-zones yes;
  allow-notify{any;};
  ```

PowerDNS:

- Install PowerDNS on a network that is connected to a public network in VMware Integrated OpenStack.
- Enable the API in the `pdns.conf` file.

Procedure

1. Log in to the VMware Integrated OpenStack dashboard as a cloud administrator.
2. Select the **admin** project from the drop-down menu in the title bar.
3. Log in to the VMware Integrated OpenStack dashboard.
4. Select your project from the drop-down menu in the title bar.
5. Log in to the OpenStack Management Server as `viouser`.
6. If your deployment is not using a `custom.yml` file, copy the template `custom.yml` file to the `/opt/vmware/vio/custom` directory.

   ```
   sudo mkdir -p /opt/vmware/vio/custom
   sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
   ```

7. Open the `/opt/vmware/vio/custom/custom.yml` file in a text editor.
8. Uncomment the `designate_enabled`, `designate_type`, `designate_dns_server`, and `designate_dns_port` parameters and configure them.

Option	Description
designate_enabled	Enter `true`.
designate_type	Enter `infoblox`, `bind9`, or `powerdns`.
designate_dns_server	Enter the IP address of your DNS server.
designate_dns_port	Enter the port number for the DNS service.

9 Uncomment the parameters specific to your back end and configure them.

- Infoblox back end

Option	Description
`designate_infoblox_wapi_url`	Enter the Infoblox WAPI URL. The default is `https://`*`infoblox-server`*`/wapi/`*`wapi-version`*`/`. **Note** The URL must end with a slash (/).
`designate_infoblox_password`	Enter the password for the Infoblox username.
`designate_infoblox_username`	Enter the username for Designate to access the Infoblox API.
`designate_ns_group`	Specify the name server group to serve Designate zones.

- Bind9 back end

Option	Description
`designate_rndc_host`	Enter the RNDC server IP address. The default value is the Bind9 server IP address.
`designate_rndc_port`	Enter the RNDC port. The default value is 953.
`designate_rndc_key`	Enter the contents of the `/etc/bind/rndc.key` file.

- PowerDNS back end

Option	Description
`designate_pdns_api_endpoint`	Enter the PowerDNS API endpoint URL. The default value is `http://`*`powerdns-server`*`/8081`. .
`designate_pdns_api_key`	Enter the value of `api-key` in the `/etc/powerdns/pdns.conf` file.

10 Deploy the updated configuration.

```
sudo viocli deployment configure
```

Deploying the configuration briefly interrupts OpenStack services.

11 If you are running VMware Integrated OpenStack 5.1, modify the Designate database to prevent duplicate entries.

   This step is not necessary if you have patched your deployment to version 5.1.0.1.

   a Log in to the active database node and switch to the `root` user.

   ```
   sudo su -
   ```

   b Open the Designate database.

   ```
   mysql
   use designate
   ```

   c Modify the database to prevent duplicate entries.

   ```
   ALTER TABLE service_statuses
   ADD UNIQUE (`hostname`, `service_name`);
   ```

Your tenants can now create DNS zones using the VMware Integrated OpenStack dashboard. For instructions, see "Create a DNS Zone" in the *VMware Integrated OpenStack User's Guide*.

What to do next

See the OpenStack Designate CLI documentation at https://docs.openstack.org/python-designateclient/queens/user/shell-v2.html for information on how to use Designate.

Important VMware Integrated OpenStack supports only the v2 API. To perform command-line operations, use the `openstack` command instead of the `designate` command.

Add the Swift Component

Swift is a component of OpenStack that provides distributed object storage.

Important In VMware Integrated OpenStack 5.1, Swift is provided as a technical preview only. Running production workloads is not currently supported.

Note The nodes in a Swift cluster cannot be deleted. If you want to remove nodes from your cluster, you must delete the entire cluster and create it again.

For more information about Swift, see the OpenStack Swift documentation at https://docs.openstack.org/swift/queens/.

Prerequisites

- Ensure that you have sufficient resources available to deploy Swift. The resources required depend on the scale of your deployment. For minimum requirements, see the Additional Components section of Hardware Requirements for VMware Integrated OpenStack.
- Ensure that your network has been prepared for Swift. See the relevant table in Required Network Ports.

Procedure

1 In the vSphere Client, create a new cluster for Swift and add at least one host and datastore.

Swift must be deployed in a dedicated cluster.

- Ensure that the Swift cluster can communicate with the management cluster over the management network.
- Ensure that all hosts in the Swift cluster use a local datastore.

2 Log in to the OpenStack Management Server as `viouser`.

3 Create the Swift cluster.

```
sudo viocli swift create-cluster --cluster-moid swift-cluster --datastores swift-ds [--storage-node-count storage-nodes] [--proxy-node-count proxy-nodes] [--disk-size GB] [--swift-partition-power-count part-power] [--swift-replica-count replicas] [--swift-min-part-hours time]
```

Option	Description
--cluster-moid	Enter the managed object identifier (MOID) of the vSphere cluster that you want to use for Swift.
--datastores	Specify one or more datastores that you want to use for Swift storage. Separate multiple entries with commas. **Important** Swift does not support datastore clusters.
--storage-node-count	(Optional) Enter the number of Swift storage nodes to create. The default value is `3`.
--proxy-node-count	(Optional) Enter the number of Swift proxy nodes to create. The default value is `2`.
--disk-size	(Optional) Enter the disk size in gigabytes for Swift storage nodes. The default value is `2048`.
--swift-partition-power-count	Specify the partition power of the Swift ring. The number of partitions managed by the ring is equal to 2 raised to the partition power. The default value is `10`.
--swift-replica-count	Enter the number of replicas to create for objects stored in Swift. The default value is `3`. **Note** The number of replicas cannot exceed the number of storage nodes in the deployment.
--swift-min-part-hours	Specify the time in hours before a partition can be assigned to another storage node. The default value is `1`.

Alternatively, you can prepare the desired specifications in JSON format and run `sudo viocli swift create-cluster -f` *`spec-file.json`* to create the cluster. For information about the required format, see "viocli swift Command" in the *VMware Integrated OpenStack Administration Guide*.

The virtual machines required for your Swift cluster are created and the service is enabled.

What to do next

You can add storage and proxy nodes to your cluster to scale out your deployment. For more information, see "Add Nodes to Your Swift Cluster" in the*VMware Integrated OpenStack Administration Guide*.

By default, users with the admin or _member_ role can perform Swift operations. To add or change the roles, uncomment the swift_operator_roles parameter in custom.yml and modify the value of the parameter to include the roles that you want. Then run viocli deployment configure --tags add_proxy_node --limit swift_proxy,swift_storage to deploy the updated configuration.

Upgrading VMware Integrated OpenStack 8

You upgrade to VMware Integrated OpenStack 5.1 by migrating to a new deployment or by applying a patch. The upgrade path depends on the version of VMware Integrated OpenStack that you are currently running.

You can upgrade from VMware Integrated OpenStack 4.0, 4.1, or 5.0 to VMware Integrated OpenStack 5.1. If you are running a version older than 4.0, first upgrade to 4.1 and then upgrade to 5.1.

To upgrade from VMware Integrated OpenStack 4.0 or 4.1, follow the procedure described in Upgrade VMware Integrated OpenStack. In this procedure, you create a VMware Integrated OpenStack 5.1 deployment and migrate your 4.0 or 4.1 deployment to it. This procedure requires that you have sufficient hardware and IP address resources to support two deployments temporarily.

To upgrade from VMware Integrated OpenStack 5.0, follow the procedure described in Patch VMware Integrated OpenStack. In this procedure, you use the `viopatch` utility to install the 5.1 patch on your existing deployment.

You can revert to the pre-upgrade version if the upgrade is not successful or if you no longer want to use version 5.1. To revert an upgrade, see Revert to a Previous VMware Integrated OpenStack Deployment . To roll back a patch, see Roll Back a VMware Integrated OpenStack Patch.

This chapter includes the following topics:

Upgrade VMware Integrated OpenStack

You upgrade to VMware Integrated OpenStack 5.1 by installing the new version and migrating your existing deployment.

Prerequisites

- Download the VMware Integrated OpenStack 5.1 OVA from the product download page at https://my.vmware.com/en/group/vmware/info?slug=infrastructure_operations_management/vmware_integrated_openstack/5_1. The file requires approximately 6 GB of storage space.

- Verify that your environment meets the requirements for VMware Integrated OpenStack 5.1. See Hardware Requirements for VMware Integrated OpenStack and Software Requirements for VMware Integrated OpenStack.
- Verify that the network ports required for VMware Integrated OpenStack 5.1 are open. See Required Network Ports.

  Important The HAProxy web UI now uses port 1993. Update your firewall configuration accordingly.
- Prepare sufficient resources to make a duplicate of every node in your current deployment. If you want to upgrade a compact deployment to an HA deployment, you will need additional resources. See Hardware Requirements for VMware Integrated OpenStack.
- Record any custom changes made to the OpenStack deployment outside of the `custom.yml` and `custom-playbook.yml` files. Any customizations not included in these files will not take effect on the new version and must be configured again on the new deployment once the upgrade is complete.
- If you have enabled Ceilometer, disable it before upgrading. You can enable Ceilometer again after the upgrade process is finished.
- For NSX-T Data Center deployments, if you do not want to use Barbican as your key manager, modify your `custom.yml` file as follows:

  a Under Barbican options, uncomment `cert_manager_type`.

  b Set its value to **`vmware_nsxv3`**.
- Ensure that no internal OpenStack management workloads are running.
- Ensure that your current deployment is running VMware Integrated OpenStack 4.0 or 4.1. If you are running an older version, upgrade to version 4.1 first. If you are running VMware Integrated OpenStack 5.0, follow the procedure described in Patch VMware Integrated OpenStack.

Procedure

1 Add IP Addresses to the Network Configuration

Before upgrading, ensure that your management and API access networks include sufficient IP addresses to support the existing and new deployments concurrently.

2 Install the New Version

You install VMware Integrated OpenStack 5.1 on your existing vCenter Server instance.

3 Migrate to the New VMware Integrated OpenStack Deployment

You back up your existing data to the new deployment and then migrate to the new deployment. This procedure starts the new deployment and stops the old deployment.

4 Delete the Old VMware Integrated OpenStack Deployment

After you upgrade VMware Integrated OpenStack, you can delete the deployment from the previous version.

Add IP Addresses to the Network Configuration

Before upgrading, ensure that your management and API access networks include sufficient IP addresses to support the existing and new deployments concurrently.

Note IP addresses from other networks segments cannot be added to the management or API access networks.

The IP addresses that you configure in this procedure are permanent. After you migrate to the new deployment, these IP addresses will be used instead of the IP addresses assigned to your existing deployment. You will need to update any DNS entries or other references to VMware Integrated OpenStack IP addresses once the upgrade is finished.

Important Do not include the IP address of the OpenStack Management Server in the management network IP range. If you have already allocated additional IP addresses for upgrades, assign the first available IP address to the OpenStack Management Server and remove it from the management network IP range.

Procedure

1. In the vSphere Client, select **Menu > VMware Integrated OpenStack**.
2. Click **OpenStack Deployments** and open the **Manage** tab.
3. On the **Networks** tab, click the **Options** (three dots) icon next to the management network and select **Add IP Range**.
4. Specify an IP address range for the management network of the new deployment.

   Note

   - The new IP address range must have at least the same number of IP addresses as the existing management network.
   - The management network cannot include more than 100 IP addresses.
5. Click the **Options** (three dots) icon next to the API access network and select **Add IP Range**.
6. Specify an IP address range for the API access network of the new deployment.

   Note

   - The new IP address range must have at least the same number of IP addresses as the existing API access network.
   - The API access network cannot include more than 100 IP addresses.

What to do next

Install the new version of VMware Integrated OpenStack on your vCenter Server instance.

Install the New Version

You install VMware Integrated OpenStack 5.1 on your existing vCenter Server instance.

Important The VMware Integrated OpenStack OVA cannot be installed in the HTML5 vSphere Client. Use the Flex-based vSphere Web Client for this procedure.

Prerequisites

Add IP address ranges for the new installation. See Add IP Addresses to the Network Configuration.

Procedure

1 In the vSphere Web Client, edit the settings of the management cluster and set **DRS Automation** to **Manual**.

2 Right-click the management cluster and select **Deploy OVF Template...** from the pop-up menu.

3 Provide the path to the VMware Integrated OpenStack OVA and click **Next**.

4 Enter a name for the new VMware Integrated OpenStack vApp, select your data center, and click **Next**.

   Note The name of the VMware Integrated OpenStack vApp can contain only letters, numbers, and underscores (_). The name cannot exceed 60 characters, and the combination of the vApp name and cluster name cannot exceed 80 characters.

5 Select the cluster on which to run the vApp and click **Next**.

6 Review the details of the template to be installed and click **Next**.

7 Read the license agreements and click **Accept**. Then click **Next**.

8 Specify a provisioning format and storage policy, select the datastore on which the vApp files will be stored, and click **Next**.

   For more information about provisioning formats, see "About Virtual Disk Provisioning Policies" in *vSphere Virtual Machine Administration*.

9 In the **Destination Network** column, select the management network and click **Next**.

10 On the **Customize template** page, enter a password for the `viouser` account on the OpenStack Management Server.

   You can also expand the other properties and configure parameters for the OpenStack Management Server, NTP server, and syslog server.

11 Once `All properties have valid values` is displayed in the upper left of the page, click **Next**.

12 Verify that the vApp can bind to the vService and click **Next**.

13 On the **Ready to complete** page, review your settings. When you are satisfied that the settings are correct, click **Finish** to install the vApp.

14 Select **Home > Global Inventory Lists** and click **vApps**.

15 Right-click the name of the new VMware Integrated OpenStack vApp and select **Power > Power On**.

What to do next

Migrate your deployment to the new version.

Migrate to the New VMware Integrated OpenStack Deployment

You back up your existing data to the new deployment and then migrate to the new deployment. This procedure starts the new deployment and stops the old deployment.

Prerequisites

- Install VMware Integrated OpenStack 5.1. See Install the New Version.
- On the new OpenStack Management Server, apply the latest patch to VMware Integrated OpenStack 5.1. For instructions, see the release notes for the latest patch.

  Note If you have upgraded your deployment from version 3.1 or earlier, you must patch to version 5.1.0.1 or later before proceeding.
- If you have enabled Ceilometer, disable it before upgrading.
  - a In the vSphere Client, select **Menu > VMware Integrated OpenStack**.
  - b Click **OpenStack Deployments** and open the **Manage** tab.
  - c On the **Settings** tab, click **Ceilometer** and click **Disable**.
- Mount a remote NFS server to the new OpenStack Management Server. This server is used to back up data from the old deployment and transfer that data to the new deployment.

Procedure

1 Log in to the new OpenStack Management Server and prepare a directory to store the backup.

```
sudo viocli upgrade prepare old-mgmt-server-ip /nfs-server-folder
```

2 Log in to the old OpenStack Management Server and back up its data to the prepared directory.

```
sudo viocli backup mgmt_server new-mgmt-server-ip:/nfs-server-folder
```

3 Log in to the new OpenStack Management Server again and reconfigure the new installation using the data backed up from the old installation.

```
sudo viocli upgrade mgmt_server backup-directory new-mgmt-server-ip:/nfs-server-folder
```

The backup directory name is in the format `vio_ms_`*`timestamp`*.

4 Log out of the vSphere Client and log back in.

This refreshes the interface so that the new deployment is displayed.

5 In the vSphere Client, select **Menu > VMware Integrated OpenStack**.

6 Click **OpenStack Deployments** and open the **Summary** tab.

7 Verify that the **Version Information** table shows the version of the new VMware Integrated OpenStack installation.

8 Under **Connected Server**, click **Connect Server...**.

9 Select the new OpenStack Management Server and click **OK**.

10 Open the **Manage** tab and click the **Upgrades** tab.

11 In the table displayed, right-click the current deployment and select **Upgrade**.

   a Enter a name for the new deployment.

   This name must be different from the name of the current deployment.

   b If you are upgrading from a compact deployment, select a deployment type for your new deployment in the **Deployment type** drop-down menu.

   During the upgrade process, you can change a compact deployment to an HA deployment if desired.

   c Click **Next**, review the upgrade configuration, and click **Finish**

   The status of the current deployment is `Running`, and the status of the new deployment is `Provisioning`.

12 After the status of the new deployment changes to `Prepared`, right-click the name of the old deployment and select **Migrate Data**.

   Important This action will stop OpenStack services. Services will be down until the upgrade finishes.

   When the migration process finishes, the status of the new deployment changes to `Migrated`.

13 Right-click the name of the old deployment and select **Switch to New Deployment**.

   When the migration process finishes, the status of the new deployment changes to `Running`, and the status of the previous deployment changes to `Stopped`.

OpenStack services are now provided by the new deployment.

Important Do not perform any operation that adds or removes nodes until you have completed the process described in Delete the Old VMware Integrated OpenStack Deployment. These operations include the following:

- Enabling Ceilometer
- Adding or removing compute clusters
- Adding or removing Swift clusters or nodes

What to do next

- Upgrade your license key in My VMware. See KB 2006974.

- Update any DNS entries to use the IP addresses of the new VMware Integrated OpenStack deployment.
- For NSX-T Data Center deployments, update the metadata proxy configuration in NSX Manager to use the IP address of the new OpenStack Management Server.
- If you integrated your deployment with vRealize Automation, perform the integration procedure again. See Integrate VMware Integrated OpenStack with vRealize Automation.
- If you integrated your deployment with VMware Identity Manager, remove the existing configuration from `custom.yml` and reconfigure integration using the new procedure. See "Configure VMware Identity Manager Federation" in the *VMware Integrated OpenStack Administration Guide*.

If the upgrade is unsuccessful or you do not want to use the new version, you can revert to your previous VMware Integrated OpenStack deployment. See Revert to a Previous VMware Integrated OpenStack Deployment .

If the upgrade is successful, you can delete the old VMware Integrated OpenStack deployment. See Delete the Old VMware Integrated OpenStack Deployment.

Delete the Old VMware Integrated OpenStack Deployment

After you upgrade VMware Integrated OpenStack, you can delete the deployment from the previous version.

Important After you delete the deployment, you cannot revert to the previous version. Do not delete the deployment until all validation tasks have been completed and you are certain that you will not need to revert to the previous version.

Procedure

1. In the vSphere Client, select **Menu > VMware Integrated OpenStack**.
2. Click **OpenStack Deployments** and open the **Manage** tab.
3. On the **Upgrades** tab, verify that the status of the new deployment is `Running` and the status of the old deployment is `Stopped`.
4. Click the **Options** (three dots) icon next to the old deployment and select **Delete**.
5. At the prompt, confirm the deletion.

The deployment no longer appears on the **Upgrades** tab or in the **OpenStack Deployments** list. The upgrade process is now finished.

What to do next

If you want to enable Ceilometer, you can do so at this time. See Enable the Ceilometer Component.

Revert to a Previous VMware Integrated OpenStack Deployment

You can revert to the previous VMware Integrated OpenStack deployment if the upgrade failed or if you do not want to use the new version.

Important The old deployment is required for reversion. If you have already deleted the old deployment, you cannot revert to the previous version.

Procedure

1 In the vSphere Client, select **Menu > VMware Integrated OpenStack** and click **OpenStack Deployments**.

2 In the **Deployment List** tab, click the **Options** (three dots) icon next to the new deployment and select **Delete OpenStack Deployment**.

  If you want to retain the new deployment for further testing, you can select **Stop OpenStack Services** instead.

  Note After you switch to the old OpenStack Management Server, the **Delete OpenStack Deployment** option is no longer available. You can manually delete the virtual machines associated with the new deployment in the vSphere Client.

3 Log in to the OpenStack Management Server of the old deployment and restart the OpenStack Management Server service.

```
service oms restart
```

4 Log in to the vCenter Server virtual machine, stop the vSphere Client service, delete residual files, and restart the service.

```
service-control --stop vsphere-ui
cd /etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/
rm -rf *
cd /usr/lib/vmware-vsphere-client/server/work
rm -rf *
service-control --start vsphere-ui
```

5 Log out of the vSphere Client and log back in.

6 In the vSphere Client, select **Home > VMware Integrated OpenStack** and click **OpenStack Deployments**.

7 In the **Summary** tab, click the **Change Server...** button.

8 Click **OK** and select the OpenStack Management Server of the old deployment.

9 In the **Deployment List** tab, click the **Options** (three dots) icon next to the old deployment and select **Start OpenStack Services**.

What to do next

If you chose to stop services instead of deleting the new deployment, you can manually remove its virtual machines in the vSphere Client. If you deleted the new deployment, its virtual machines are removed automatically.

Patch VMware Integrated OpenStack

You install the VMware Integrated OpenStack 5.1 patch by using the `viopatch` utility.

Important The `viopatch uninstall` action is deprecated and cannot be used to revert to the previous version. The snapshots created in this process are therefore necessary for reversion. Do not remove these snapshots until all validation tasks have been completed and you are certain that you will not need to revert to the previous version.

Prerequisites

- Download the VMware Integrated OpenStack 5.1 patch from the product download page at https://my.vmware.com/en/group/vmware/info?slug=infrastructure_operations_management/vmware_integrated_openstack/5_1. The patch is delivered as a DEB file.
- Verify that your environment meets the requirements for VMware Integrated OpenStack 5.1. See Hardware Requirements for VMware Integrated OpenStack and Software Requirements for VMware Integrated OpenStack.
- Verify that the network ports required for VMware Integrated OpenStack 5.1 are open. See Required Network Ports.

  Important The HAProxy web UI now uses port 1993. Update your firewall configuration accordingly.
- For NSX-T Data Center deployments, if you do not want to use Barbican as your key manager, modify your `custom.yml` file as follows:

  a Under Barbican options, uncomment `cert_manager_type`.

  b Set its value to **`vmware_nsxv3`**.
- Ensure that your current deployment is running VMware Integrated OpenStack 5.0. If you are running an older version, follow the procedure described in Upgrade VMware Integrated OpenStack.

Procedure

1 If you have already deployed OpenStack, take snapshots of the OpenStack Management Server and the deployment.

Note Do not perform this step if you have not yet deployed OpenStack on the current environment.

a In the vSphere Client, take a snapshot of the OpenStack Management Server virtual machine.

b Log in to the OpenStack Management Server and take a snapshot.

```
sudo viopatch snapshot take
```

Note This command stops OpenStack services. Services will be started again when the patch is installed.

2 Transfer the VMware Integrated OpenStack 5.1 patch file to the OpenStack Management Server virtual machine.

3 Add and install the patch file.

```
sudo viopatch add -l path/vio-patch-5.1_5.1.0.10738236_all.deb
sudo viopatch install -p vio-patch-5.1 -v 5.1.0.10738236
```

You can run the `sudo viopatch list` command at any time to display all added patches and the corresponding version.

What to do next

After you have validated that the patched version is operating correctly, you can run `sudo viopatch snapshot remove` to delete the snapshot. This action is destructive and cannot be reversed. You cannot roll back after deleting the snapshot.

If you need to roll back to the previous version, see Roll Back a VMware Integrated OpenStack Patch.

Roll Back a VMware Integrated OpenStack Patch

You can roll back a VMware Integrated OpenStack patch if the upgrade failed or if you do not want to use the new version.

Prerequisites

- Verify that you retained the snapshot of the OpenStack Management Server taken in vSphere before the patch.
- Verify that you retained the snapshot of your deployment taken with the `viopatch` utility. You can run `sudo viopatch snapshot list` to confirm whether `viopatch` has a snapshot of the nodes in your deployment.

Procedure

1 In the vSphere Client, revert the OpenStack Management Server to the previous snapshot.

2. Log in to the OpenStack Management Server virtual machine and restart the OpenStack service.

   ```
   sudo service oms restart
   ```

3. Revert the deployment to the previous snapshot.

   ```
   sudo viopatch snapshot revert
   ```

4. On the vCenter Server virtual machine, stop the vSphere Client service, delete residual files, and restart the service.

   ```
   service-control --stop vsphere-ui
   cd /etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/
   rm -rf *
   cd /usr/lib/vmware-vsphere-client/server/work
   rm -rf *
   service-control --start vsphere-ui
   ```

5. Log out of the vSphere Client and log back in.