

VMware Integrated OpenStack Installation and Configuration Guide

Modified on 19 NOV 2020

VMware Integrated OpenStack 7.0

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

<https://docs.vmware.com/>

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

Copyright © 2015-2020 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1 VMware Integrated OpenStack Installation and Configuration Guide 5**
- 2 Introducing VMware Integrated OpenStack 6**
 - VMware Integrated OpenStack Architecture 6
 - Internationalization and Unicode Support 8
 - OpenStack Foundation Compliance 8
 - VMware Integrated OpenStack Licensing 9
 - Datastore Clusters in VMware Integrated OpenStack 9
 - First Class Disks in VMware Integrated OpenStack 10
- 3 Preparing Your Environment 12**
 - Hardware Requirements for VMware Integrated OpenStack 12
 - Software Requirements for VMware Integrated OpenStack 13
 - Required Network Ports 14
 - Configure vCenter Server for OpenStack 18
 - Configure NSX Data Center for vSphere for OpenStack 19
 - Configure NSX-T Data Center for OpenStack 20
- 4 Installing VMware Integrated OpenStack 27**
 - Install the VMware Integrated OpenStack Virtual Appliance 27
 - Create an OpenStack Deployment 30
 - Assign the VMware Integrated OpenStack License Key 35
- 5 Configuring Additional Components and Features 36**
 - Integrate VMware Integrated OpenStack with vRealize Operations Manager 36
 - Integrate VMware Integrated OpenStack with vRealize Log Insight 37
 - Forward Logs to an External Server 38
 - Enable the Designate Component 39
 - Enable Carrier Edition Features 43
 - Enable the Ceilometer Component 43
- 6 Upgrading VMware Integrated OpenStack 45**
 - Apply the VMware Integrated OpenStack 7.0.1 Patch 46
 - Remove the VMware Integrated OpenStack 7.0.1 patch 48
 - Upgrade VMware Integrated OpenStack 6.x to 7.0.1 49
 - Upgrade VMware Integrated OpenStack 5.1 to 7.0.1 50
 - Add IP Addresses to the Network Configuration 53
 - Install the New Virtual Appliance 53

Migrate to the New VMware Integrated OpenStack Deployment	56
Upgrade and Assign Your License Key	59
Delete the Old VMware Integrated OpenStack Deployment	60
Revert to a Previous VMware Integrated OpenStack Deployment	60

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 virtual appliance. The virtual appliance installs the Integrated OpenStack Manager, which streamlines the process of deploying OpenStack. After deployment, you can use the Integrated OpenStack Manager 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.

Introducing VMware Integrated OpenStack

2

VMware Integrated OpenStack is a distribution of OpenStack designed to run on a vSphere infrastructure.

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 Operations Manager and vRealize Log Insight

This chapter includes the following topics:

- [VMware Integrated OpenStack Architecture](#)
- [Internationalization and Unicode Support](#)
- [OpenStack Foundation Compliance](#)
- [VMware Integrated OpenStack Licensing](#)
- [Datastore Clusters in VMware Integrated OpenStack](#)
- [First Class Disks in VMware Integrated OpenStack](#)

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.

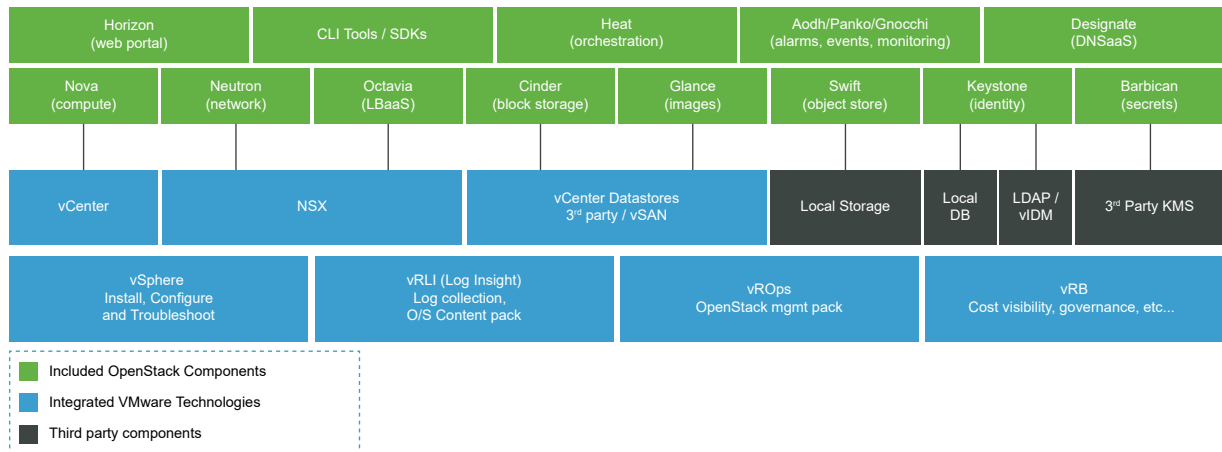
Keystone (identity management)

Authentication and authorization in OpenStack are managed by Keystone.

VMware Integrated OpenStack also provides the following OpenStack components:

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

Figure 2-1. Overview of VMware Integrated OpenStack 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 Linux to access VMware Integrated OpenStack, 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. Licenses are available for VMware Integrated OpenStack Data Center Edition and Carrier Edition

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 by assigning an evaluation license. When the evaluation license expires, all Carrier Edition features are disabled. 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.

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:

- Datastore clusters cannot be configured by using the Integrated OpenStack Manager web interface. To add a datastore cluster to your deployment, perform the following steps using the command-line interface.
 - a Specify the name of the Nova Compute server to update.

```
viocli update novacompute <novacompute_XXX>
```

- b Ensure that your datastore cluster is accessible to the Nova Compute server.

- c Assign the name of your datastore cluster to the `datastore_cluster` key.

```
conf:
  nova_compute:
    DEFAULT:
      default_schedule_zone: nova
      disk_allocation_ratio: 2
      host: compute01
  vmware:
    cluster_name: compute_cluster
    datastore_cluster: <your_datastore_cluster>
```

- d Wait for the Nova Compute server to restart.

When you use Nova to start a new compute instance, it is allocated to your datastore cluster.

- 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 only boot 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)

First Class Disks in VMware Integrated OpenStack

In VMware Integrated OpenStack 7.0.1, you can create Cinder volumes as First Class Disks (FCDs) instead of VMDKs.

An FCD, also known as an Improved Virtual Disk (IVD) or Managed Virtual Disk, is a named virtual disk independent of a virtual machine. Using FCDs for Cinder volumes eliminates the need for shadow virtual machines.

The FCD back end is offered in addition to the default VMDK back end. If you select FCD as the back-end driver for Cinder, you can use both FCD and VMDK volumes in the same deployment. You can also attach FCD and VMDK volumes to the same OpenStack instance.

To specify the back-end driver used for volume creation, create volume types with the `volume_backend_name` extra spec set to the name of the desired driver as in the following examples:

- For the VMDK driver, use **VMwareVcVmdkDriver**.
- For the FCD driver, use **VMwareVStorageObjectDriver**.

Then select the volume type when you create volumes.

Existing VMDK volumes cannot be automatically converted to FCD volumes. To convert a VMDK volume manually, detach the volume from all instances, unmanage it, and manage it again. For information, see "Manage a Volume" in the *VMware Integrated OpenStack Administration Guide*.

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

- vSphere 6.7 Update 2 or later is required to use FCD volumes.
- vSphere 6.7 Update 3 or later is required to perform the following operations on volumes that are attached to powered-on instances:
 - Creating a volume from a snapshot
 - Backing up a volume snapshot using a temporary volume created from a snapshot
- Storage DRS is not supported for FCD volumes.
- Volume multi-attach is not supported for FCD volumes.
- FCD volumes must be backed by a shared datastore.
- FCD volumes that are in use cannot be cloned, retyped, or extended.
- After you set a storage policy on an FCD volume, you cannot remove the storage policy from the volume. However, you can change the storage policy used by an unattached volume.
- Instances that have an FCD volume attached cannot be migrated. You must detach the volume before migrating the instance.
- FCD volumes with snapshots cannot be extended.
- FCD volumes do not support the import of a VM disk from vSphere.

Preparing Your Environment

3

Before deploying VMware Integrated OpenStack, ensure that your environment meets the system requirements and perform pre-installation tasks to prepare your networks and vSphere infrastructure.

This chapter includes the following topics:

- [Hardware Requirements for VMware Integrated OpenStack](#)
- [Software Requirements for VMware Integrated OpenStack](#)
- [Required Network Ports](#)
- [Configure vCenter Server for OpenStack](#)
- [Configure NSX Data Center for vSphere for OpenStack](#)
- [Configure NSX-T Data Center for OpenStack](#)

Hardware Requirements for VMware Integrated OpenStack

The specific hardware required to run VMware Integrated OpenStack depends on the scale of your deployment and size of controller that you select.

The Integrated OpenStack Manager requires the following hardware resources:

- 4 vCPUs
- 16 GB of memory
- One 40 GB hard disk and one 30 GB hard disk

A non-HA deployment requires between one and ten controllers. An HA deployment requires between three and ten controllers. The supported controller sizes are as follows:

- Small: 4 vCPUs, 16 GB of memory, and one 25 GB hard disk
- Medium: 8 vCPUs and 32 GB of memory, and one 50 GB hard disk
- Large: 12 vCPUs and 32 GB of memory, and one 75 GB hard disk

Note The small size can be used in HA deployments only. Non-HA deployments must use medium or large controllers.

The following persistent volumes are also required:

- MariaDB: one 60 GB hard disk for non-HA deployments or three 60 GB hard disks for HA deployments
- RabbitMQ: one 20 GB for non-HA deployments or three 20 GB hard disks for HA deployments
- Virtual Serial Port Concentrator (VSPC): one 2 GB hard disk per Nova compute instance

The following table lists minimum and maximum resource requirements for typical configurations.

Deployment Type	vCPUs	Memory	Disk Space (Non-Persistent)	Disk Space (Persistent)
Single-node non-HA deployment (minimum)	12 (4 + 8)	48 GB (16 + 32)	85 GB (30×2 + 25)	82 GB (60 + 20 + 2)
Single-node non-HA deployment (maximum)	16 (4 + 12)	48 GB (16 + 32)	135 GB (30×2 + 75)	82 GB (60 + 20 + 2)
Three-node HA deployment (minimum)	16 (4 + 4×3)	64 GB (16 + 16×3)	135 GB (30×2 + 25×3)	246 GB (60×3 + 20×3 + 2×3)
Three-node HA deployment (maximum)	40 (4 + 12×3)	112 GB (16 + 32×3)	285 GB (30×2 + 75×3)	246 GB (60×3 + 20×3 + 2×3)
Five-node HA deployment (minimum)	24 (4 + 4×5)	96 GB (16 + 16×5)	185 GB (30×2 + 25×5)	246 GB (60×3 + 20×3 + 2×3)
Five-node HA deployment (maximum)	64 (4 + 12×5)	176 GB (16 + 32×5)	435 GB (30×2 + 75×5)	246 GB (60×3 + 20×3 + 2×3)

Note If you want to enable Ceilometer, the CPUs on the ESXi host running the Integrated OpenStack Manager must support Advanced Vector Extensions (AVX).

If you want to deploy VMware Integrated OpenStack with NSX-T Data Center or NSX Data Center for vSphere networking, additional resources may be required.

- For NSX-T Data Center, see "System Requirements" in the *NSX-T Data Center Installation Guide*.
- For NSX Data Center for vSphere, see "System Requirements for NSX Data Center for vSphere" in the *NSX Installation Guide*.

Software Requirements for VMware Integrated OpenStack

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

VMware Integrated OpenStack 7.0.1 requires the following products:

- vSphere Enterprise Plus Edition.
- (NSX-T Data Center deployments only) NSX-T Data Center Advanced Edition
- (NSX Data Center for vSphere deployments only) NSX Data Center for vSphere

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 7.0.1 is also compatible with the following products:

- vSAN
- VMware Identity Manager
- vRealize Log Insight
- vRealize Operations Manager with vRealize Operations Management Pack for VMware Integrated OpenStack

The Integrated OpenStack Manager web interface supports the following web browsers:

- Google Chrome version 50 and later
- Mozilla Firefox version 45 and later
- (Windows only) Microsoft Edge version 38 and later

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.

Required Network Ports

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

All ports listed are TCP unless otherwise specified.

Object	Port Number	Protocol	Network	Service or Product	Description
Manager and Controllers	22		Internal	SSH	SSH
Manager	53	TCP or UDP	Internal	DNS	FQDN resolution
Controllers	53	TCP or UDP	Public and Internal	DNS	FQDN resolution
Manager	443		Internal	VIO Web UI	VIO Web UI service

Object	Port Number	Protocol	Network	Service or Product	Description
Controllers	443		Public and Internal	OpenStack dashboard service	VMware Integrated OpenStack dashboard
ESXi hosts	443		Internal	ESXi hosts	ESXi API endpoint
NSX Manager	443		Internal	NSX Manager	NSX Manager endpoint
vCenter Server Appliance	443		Internal	vCenter Server	vCenter Server API endpoint
Manager	2379		Internal	Etcd Server	Etcd API endpoint
Manager	2380		Internal	Etcd Server	Etcd API endpoint
Controllers	3306		Internal	OpenStack database	Database cluster
Controllers	4567		Internal	OpenStack database	MariaDB Galera replication traffic
Manager	5000		Internal	Docker Registry	Docker Registry service endpoint
Controllers	5000		Public and Internal	OpenStack API services	Keystone API endpoint
Controllers	5672		Internal	OpenStack RPC bus	RabbitMQ message bus
Controllers	6090		Public and Internal	OpenStack console services	MKS proxy
Manager	6443		Internal	Kubernetes apiserver	Kubernetes apiserver endpoint
Controllers	8000		Public and Internal	OpenStack API services	Heat CloudFormation API endpoint
Controllers	8004		Public and Internal	OpenStack API services	Heat API endpoint
Manager	8443		Internal	VIO API	VIO API endpoint
Controllers	8774		Public and Internal	OpenStack API services	Nova API endpoint
Controllers	8775		Internal	OpenStack metadata	Metadata service (required unless config drive is used)

Object	Port Number	Protocol	Network	Service or Product	Description
Controllers	8776		Public and Internal	OpenStack API services	Cinder API endpoint
Controllers	8778		Public and Internal	OpenStack API services	Nova Placement API endpoint
Manager	8879		Internal	Helm Repo Server	Helm Repo service endpoint
Manager	9000		Internal	VIO Web UI Authentication Proxy	VIO Web UI Authentication Proxy
Manager	9090		Internal	VIO API swagger	VIO API swagger endpoint
Manager and Controllers	9099		Internal	Calico CNI	Calico CNI
Controllers	9292		Public and Internal	OpenStack API services	Glance API endpoint
Controllers	9311		Public and Internal	OpenStack API services	Barbican API endpoint
vCenter Server Appliance	9443		Internal	vCenter Server	vCenter Server
Manager	9449		Internal	vAPI	vAPI
Controllers	9696		Public and Internal	OpenStack API services	Neutron API endpoint
Controllers	9876		Public and Internal	OpenStack API services	Octavia API endpoint
Manager and Controllers	10250		Internal	Kubernetes kubelet	Kubernetes kubelet
Manager	10251		Internal	Kubernetes scheduler	Kubernetes scheduler
Manager	10252		Internal	Kubernetes controller manager	Kubernetes controller manager
Controllers	11211		Internal	OpenStack control plane cache	Memory cache services for controller nodes
Controllers	35357		Public and Internal	OpenStack API services	Keystone administrator API endpoint
Manager and Controllers	44134		Internal	Tiller Server	Tiller service 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	9000 (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
Controllers	8041	Public and Internal	OpenStack API services	Gnocchi API endpoint services
Controllers	8042	Public and Internal	OpenStack API services	Aodh API endpoint services
Controllers	8779	Public and Internal	OpenStack API services	Panko API endpoint services

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

Object	Port Number	Network	Service or Product	Description
Controllers	53 (UDP)	Public and Internal	DNS	Designate MiniDNS service
Controllers	9001	Public and Internal	OpenStack API services	Designate endpoint services

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

Object	Port Number	Network	Service or Product	Description
Controllers	8080	Public and Internal	OpenStack API services	Swift endpoint services

Configure vCenter Server for OpenStack

Before installing the VMware Integrated OpenStack OVA, configure your environment as described in the following procedure.

Prerequisites

- Deploy vCenter Server and all ESXi hosts.
- Enable NTP on vCenter Server and on all ESXi hosts. Configure vCenter Server and ESXi hosts to use the same NTP time source, and ensure that the time source is highly available. For information about configuring NTP in vSphere, see "Synchronizing Clocks on the vSphere Network" in the *vSphere Security* guide.
- Create a PTR record associating the IP address planned for the Integrated OpenStack Manager with its FQDN, and ensure that the Integrated OpenStack Manager can connect to a DNS server.

Procedure

- 1 In vCenter Server, create a data center for VMware Integrated OpenStack.
- 2 In the data center, create the management cluster and compute cluster.
- 3 If you want to use NSX networking, create the edge cluster.
- 4 Enable DRS and vSphere HA on the management cluster.

Note After deploying OpenStack, disable vSphere HA on all controller nodes.

- 5 Create a resource pool in the management cluster.
- 6 For NSX Data Center for vSphere deployments, create a resource pool in the edge cluster.
- 7 If you want to use datastore clusters for compute nodes, enable Storage DRS on the datastore clusters and set the **Cluster automation level** to **No Automation (Manual Mode)**.
- 8 In your data center, create one or more distributed switches for your management, compute, and edge clusters.
- 9 On each distributed switch, set the maximum transmission unit (MTU) to 1600 or higher.
- 10 Plan the management network and assign a dedicated VLAN to it.
 - If you do not want to use DHCP, ensure that the management network has at least five contiguous IP addresses available.
 - Ensure that the management network can 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.
 - For NSX-T Data Center deployments, ensure that the vCenter Server, NSX Manager, and NSX Controller instances can access the management network on Layer 2 or Layer 3.

- For NSX Data Center for vSphere deployments, if you want to use the management network for metadata service, ensure that the management network has an additional two contiguous IP addresses available. This is not required for deployments with an independent metadata service network.
- 11 Plan the API access network and assign a dedicated VLAN to it.
- Create the port group for the API access network on the distributed switches for your management, compute, and edge clusters. The network must be externally accessible.
 - If you do not want to use DHCP, ensure that the API access network has at least four contiguous IP addresses available.
 - Ensure that the API access network can 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.
- 12 For NSX Data Center for vSphere deployments, create the port group for the external network on the distributed switch for the edge cluster.
- 13 (Optional) For NSX Data Center for vSphere deployments, plan the metadata service network.
- Ensure that the metadata service network has at least two contiguous IP addresses available. If you do not create an independent metadata service network, ensure that your management network has two additional IP addresses available for the metadata service.
 - Ensure that the metadata service network can communicate with the management network.

What to do next

If you want to use NSX networking, deploy and configure your networking back end.

- [Configure NSX Data Center for vSphere for OpenStack](#)
- [Configure NSX-T Data Center for OpenStack](#)

Configure NSX Data Center for vSphere for OpenStack

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

Procedure

- ◆ Install NSX Data Center for vSphere as described in the [NSX Installation Guide](#).

Note the following:

- The NSX Manager must be installed on the compute vCenter Server instance used by VMware Integrated OpenStack. Cross-vCenter Server installation is not supported.
- Ensure that the maximum transmission unit (MTU) on the transport network is set to 1600 or higher.

What to do next

Install VMware Integrated OpenStack. See [Chapter 4 Installing VMware Integrated OpenStack](#).

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.

Note For NSX-T Data Center to work with vSphere Distributed Switch (VDS) version 7.0, vSphere 7.0 and NSX-T 3.0 or later must be installed. Before deploying and configuring NSX-T Data Center, see "Prepare a vSphere Distributed Switch for NSX-T" in the *NSX-T Data Center Installation Guide*.

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 If you are using NSX-T Data Center 2.3.1, controllers must be deployed separately. See "NSX Controller Installation and Clustering" in the *NSX-T Data Center Installation Guide*.
 - c Add your vCenter Server instance as a compute manager. See "Add a Compute Manager" in the *NSX-T Data Center Installation Guide*.
 - d 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.

- e Deploy NSX Edge nodes. See "Installing NSX Edge" in the *NSX-T Data Center Installation Guide*.
 - f If you are running vSphere 7.0 or later, add a new compute manager. See "Add a Compute Manager" in the [NSX-T Data Center Installation Guide](#).
- Generate the NSX-T root CA certificate using the cluster virtual IP. See "Generating and Registering the NSX Manager Certificate for Enterprise PKS" in the [VMware Enterprise PKS product documentation](#).

Procedure

- 1 Log in to the NSX Manager as an administrator.

2 Create an overlay transport zone.

- a On the **System** tab, 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 is used for the N-VDS that is installed on transport nodes added to this transport zone.
- c If provided with the option, select **Standard** or **Enhanced Datapath** for the N-VDS mode.
- d Select **Overlay** for the traffic type.
- e Click **Add**.

3 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 is 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**.

4 Create an uplink profile.

- a On the **System** tab, select **Fabric > Profiles**.
- b On 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, define a custom uplink name.
If you are using a physical link on an ESXi host, you can also define a standby uplink name.
- g In the **Transport VLAN** text box, enter the VLAN ID of the physical network.
- h Enter a maximum transmission unit (MTU) of 1600 or higher.
- i Click **Add**.

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

- a On the **System** tab, select **Fabric > Profiles**.
- b On 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 Click **Add**.
- 6 Create an IP address pool for tunnel endpoints.
- a On the **Advanced Networking & Security** tab, select **Inventory > Groups**.
 - b On 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**.
- 7 Add the ESXi hosts in your compute cluster to the NSX-T Data Center fabric.
- a On the **System** tab, select **Fabric > Nodes**.
 - b On the **Host Transport Nodes** tab, click **Add**.
 - If you are running vSphere 7.0 or later, select the compute manager that you added to the NSX-T Data Center and select the node with OS Type `ESXi 7.0.0`.
 - If you are running vSphere 6.x or earlier, 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 prompts you to use the default thumbprint provided by the host.
 - c Click **Next**.
 - d From the **Transport Zone** drop-down menu, select the overlay transport zone.
 - e From the **N-VDS Name** drop-down menu, select the N-VDS for the overlay transport zone.
 - If you are running vSphere 7.0 or later, select **VDS**.
 - If you are using a standard N-VDS, select the NIOC profile that you created in this procedure.
 - f From the **Uplink Profile** drop-down menu, select the uplink profile that you created in this procedure.
 - g From the **LLDP Profile** drop-down menu, select the desired LLDP profile.
 - h From the **IP Assignment** drop-down menu, select **Use IP Pool**.

- i From the **IP Pool** drop-down menu, select the tunnel endpoint IP address pool that you created in this procedure.
 - j In the **Physical NICs** field, enter the name of an unused NIC on your host.
 - k From the drop-down menu, select the uplink name that you defined in the uplink profile.
 - l Click **Add**.
- 8 Add the NSX Edge nodes in your edge cluster to the NSX-T Data Center fabric.
- a On the **System** tab, select **Fabric > Nodes**.
 - b On the **Edge Transport Nodes** tab, click **Add Edge VM**.
 - c Enter the name, FQDN, and description of the transport node.
 - d Select a form factor for the edge virtual machine and click **Next**.
 - e Enter the credentials for the NSX Edge virtual machine and click **Next**.
 - f Select the compute manager that you configured in this procedure.
 - g Select the cluster, resource pool or host, and datastore for the NSX Edge virtual machine and click **Next**.
 - h Select whether to use DHCP or a static IP address for the NSX Edge virtual machine.
If you select **Static**, enter the management IP address and default gateway.
 - i From the **Management Interface** drop-down menu, select the management network.
 - j Click **Next**.
 - k From the **Transport Zone** drop-down menu, select the overlay and VLAN transport zones.
 - l From the **Edge Switch Name** drop-down menu, select the N-VDS for the overlay transport zone.
 - m From the **Uplink Profile** drop-down menu, select the uplink profile that you created in this procedure.
 - n From the **IP Assignment** drop-down menu, select **Use IP Pool**.
 - o From the **IP Pool** drop-down menu, select the tunnel endpoint IP address pool that you created in this procedure.
 - p From the **DPDK Fastpath Interfaces** drop-down menu, select the uplink name that you defined in the uplink profile.
 - q Click **Select Interface**.
 - r Select the management network and click **Save**.
 - s Click **Add N-VDS**.
 - t From the **Edge Switch Name** drop-down menu, select the N-VDS for the VLAN transport zone.

- u From the **Uplink Profile** drop-down menu, select the uplink profile that you created in this procedure.
 - v From the **DPDK Fastpath Interfaces** drop-down menu, select the uplink name that you defined in the uplink profile.
 - w Click **Select Interface**.
 - x Select the management network and click **Save**.
- 9 Create an edge cluster and add NSX Edge nodes to it.
- a On the **System** tab, select **Fabric > Nodes**.
 - b On 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 menu.
 - e From the **Member Type** drop-down menu, 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 **Add**.
- 10 Create a logical switch.
- a On the **Advanced Networking & Security** tab, 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 Select an uplink teaming policy.
 - f Specify the VLAN ID of the network.
 - g Click **Add**.
- 11 Create a tier-0 router.
- a On the **Advanced Networking & Security** tab, select **Networking > Routers**.
 - b On 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**.

- 12 Create a port on the tier-0 router to associate with the upstream physical router.
 - a On the **Advanced Networking & Security** tab, select **Networking > Routers**.
 - b On 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 Enter a maximum transmission unit (MTU) of 1600 or higher.
 - g From the **Transport Node** drop-down menu, select a member of the edge cluster.
 - h From the **Logical Switch** drop-down menu, select the switch that you created in this procedure.
 - i Select **Attach to new switch port** and enter a name for the switch port.
 - j Under **Subnets**, click **Add**.
 - k Enter the IP address of the router port and its prefix length in bits.

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

- l Click **Add**.
- 13 Create a DHCP server profile.
 - a On the **Advanced Networking & Security** tab, select **Networking > DHCP**.
 - b On the **Server Profiles** tab, click **Add**.
 - c Enter a name and description for the profile.
 - d Select the edge cluster that you created in this procedure.
 - e Click **Add**.
 - 14 Create a metadata proxy server.
 - a On the **Advanced Networking & Security** tab, select **Networking > DHCP**.
 - b On the **Metadata Proxies** tab, click **Add**.
 - c Enter a name and description for the metadata proxy server.
 - d In the **Nova Server URL** field, enter the planned private OpenStack endpoint of your VMware Integrated OpenStack deployment.

VMware Integrated OpenStack uses the first IP address in the management network as the private OpenStack endpoint. If you are not certain which IP address will be used, you can enter a placeholder IP address and update this setting after you have deployed VMware Integrated OpenStack.
 - e In the **Secret** field, enter a password to pair with your VMware Integrated OpenStack deployment.

- f Select the edge cluster that you created in this procedure.
- g Click **Add**.

What to do next

Install VMware Integrated OpenStack. See [Chapter 4 Installing VMware Integrated OpenStack](#).

Installing VMware Integrated OpenStack

4

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

Procedure

1 Install the VMware Integrated OpenStack Virtual Appliance

You deploy the VMware Integrated OpenStack virtual appliance on your vCenter Server instance. This appliance includes the OpenStack Management Server, through which you deploy and maintain your OpenStack cloud infrastructure.

2 Create an OpenStack Deployment

You deploy OpenStack by using the Integrated OpenStack Manager web interface.

3 Assign the VMware Integrated OpenStack License Key

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

Install the VMware Integrated OpenStack Virtual Appliance

You deploy the VMware Integrated OpenStack virtual appliance on your vCenter Server instance. This appliance includes the OpenStack Management Server, through which you deploy and maintain your OpenStack cloud infrastructure.

This procedure describes how to install the VMware Integrated OpenStack using the vSphere Client. If you want to use the OVF Tool to install the virtual appliance, you must include the `--allowExtraConfig` parameter.

Prerequisites

- Deploy or upgrade vSphere and any other VMware products that you want to use with VMware Integrated OpenStack.
- Verify that your hardware, networks, and vCenter Server instance are correctly prepared. See [Chapter 3 Preparing Your Environment](#).
- Verify that DRS has been enabled on the management cluster for VMware Integrated OpenStack.

- Obtain the VMware Integrated OpenStack 7.0 OVA file from the product download page at https://my.vmware.com/en/group/vmware/info?slug=infrastructure_operations_management/vmware_integrated_openstack/7_0. The file requires approximately 6 GB of storage space.

Procedure

- 1 Log in to the vSphere Client and select the **Hosts and Clusters** view.
- 2 Edit the settings of the management cluster previously configured for VMware Integrated OpenStack and set **DRS Automation** to **Manual**.

Important Do not use Storage vMotion to migrate VMware Integrated OpenStack vApp and controller virtual machines, which will rename the vmdk files for Kubernetes Persistent Volume and break the function.

- 3 Right-click the management cluster previously configured for VMware Integrated OpenStack and select **Deploy OVF Template...** from the pop-up menu.
- 4 Provide the path to the VMware Integrated OpenStack OVA and click **Next**.
- 5 Enter a name for the VMware Integrated OpenStack vApp, select the data center that you defined during preparation, and click **Next**.
- 6 Select the cluster on which to run the vApp and click **Next**.
- 7 Review the details of the template to be installed and click **Next**.
- 8 Read the license agreements and select **I accept all license agreements**. Then click **Next**.
- 9 Specify a provisioning format and storage policy, select the datastore for vApp files storage, and click **Next**.

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

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

- 11 On the **Customize template** page, enter additional settings for VMware Integrated OpenStack.
- a Under **Network properties**, you can enter static IP addresses for the Integrated OpenStack Manager virtual machine and DNS server.
 - If you want to use DHCP, leave all fields blank. If you enter a static IP address for the Integrated OpenStack Manager, you must also enter the subnet mask, default gateway, and DNS server. For the default gateway, use the eth1 interface.
 - If you enter the Integrated OpenStack Manager FQDN, alphanumeric letters must be lowercase and match the DNS record on the DNS server. For example, "viomgr01".
 - b Under **System**, enter an initial password for the administrator accounts on the Integrated OpenStack Manager.

This password is used for the `admin` account on the web interface and the `root` user on the Integrated OpenStack Manager virtual machine. The following rules apply to the password:

 - The password must contain between 8 and 128 characters.
 - The password must contain at least one uppercase letter, one lowercase letter, one digit, and one special character.
 - The password cannot contain simplistic patterns, common words, or words derived from the name of the account.
 - c For **Permit Root Logon**, select **true**.
 - d Under **Internal Network**, enter the network address of the Kubernetes service network, the network address of the Kubernetes pod network, and the domain name suffix of the service network.

Important

- The network settings cannot be changed after deployment. Ensure that each network is large enough to support your deployment, including future expansion.

The pod network must contain enough IP addresses so that each manager and controller node in the deployment can be assigned a /24 CIDR block. For example, the network 192.168.0.0/22 can support a maximum of four nodes, and the network 192.168.0.0/21 can support a maximum of eight nodes.
 - The service and pod networks must be valid private networks as defined by RFC 1918.
 - The service and pod networks must not overlap each other or any existing networks.
 - The service network domain suffix must not overlap any existing domains. For example, if your current domain is named `corp.local`, you cannot use `cluster.local` as your service network domain. Use a different domain suffix, such as `cluster.example`.
-

- e (Optional) Under **Log Management**, enter the IP address and port number of your log analytics server.

You can add or update the log analytics server information after the deployment is finished.

- f Under **Time Management**, enter one or more NTP servers to use for time synchronization.

All VMware Integrated OpenStack virtual machines must use a single, highly available time source. You must enter an NTP server in this field.

- 12 Once `All properties have valid values` is displayed in the upper left of the page, 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 virtual appliance.

- 14 Right-click the name of the VMware Integrated OpenStack virtual appliance and select **Power > Power On**.

- 15 Select the Integrated OpenStack Manager virtual machine in the virtual appliance and record its IP address.

You can access this IP address to log in to the Integrated OpenStack Manager through the web interface or SSH.

What to do next

[Apply the VMware Integrated OpenStack 7.0.1 Patch](#) then use the Integrated OpenStack Manager web interface to create an OpenStack deployment and assign a license key.

Create an OpenStack Deployment

You deploy OpenStack by using the Integrated OpenStack Manager web interface.

Prerequisites

- Prepare your networks and vCenter Server environment. See [Chapter 3 Preparing Your Environment](#).
- Install VMware Integrated OpenStack on your vCenter Server instance. See [Install the VMware Integrated OpenStack Virtual Appliance](#).
- In vSphere, take a snapshot of the Integrated OpenStack Manager virtual machine. This snapshot is needed if you want to delete and recreate your deployment.
- Verify that all required clusters and datastores are available. If you add any resources to your vSphere environment after starting the deployment wizard, you must close and reopen the wizard before your changes can be displayed.
- Verify that the DNS server is set correctly and that the network gateway or firewall forwards DNS requests on private networks.

- For NSX-T Data Center deployments, obtain the values of the following parameters:
 - 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
 - Metadata proxy server and secret
- For NSX Data Center for vSphere deployments, obtain the values of the following parameters:
 - FQDN or IP address of the NSX Manager
 - Username and password to access the NSX Manager
 - Transport zone
 - Edge cluster
 - Resource pool and datastore for the edge cluster
 - Distributed switch for NSX Data Center for vSphere
 - Port group for the external network
 - Port group for the metadata service network (if independent from the management network)

Procedure

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

You can access the web interface by opening the IP address of the Integrated OpenStack Manager in a web browser. To find the IP address, select the Integrated OpenStack Manager virtual machine in the vSphere Client and view the **Summary** tab.

- 2 Select **OpenStack Deployment** and click **Add**.
- 3 Select whether you want to create a deployment or use an exported template to populate settings.

Note

- Passwords are not saved in exported templates. You must enter each password and validate it before additional settings can be populated.
 - Additional vCenter Server instances are not saved in exported templates. You must add vCenter Server instances manually before their settings can be populated.
-

- 4 Specify the deployment name, deployment mode, number of controllers, and controller size.
For non-HA mode, you can deploy with one medium or large controller. For HA mode, you can deploy with three or five controllers of any size.

After deployment, you can scale out your control plane and convert non-HA deployments to HA mode. However, you cannot scale in your control plane or convert HA deployments to non-HA mode.

- 5 Click **Next**.
- 6 Enter the FQDN or IP address of your management vCenter Server instance and specify its administrator credentials.

Note If you want to deploy VMware Integrated OpenStack with NSX Data Center for vSphere networking, you must enter the location of the vCenter Server instance in the format in which it was registered with NSX Manager. To find the correct format, log in to NSX Manager, click **Manage vCenter Registration**, and view the **vCenter Server** section. Ensure that the value entered in VMware Integrated OpenStack is the same as the value displayed in the **vCenter Server** section in NSX Manager.

- 7 If the Integrated OpenStack Manager connects to the vCenter Server instance over a private, secure network and you need to disable certificate validation, select the **Ignore vCenter Server certificate validation** check box.
- 8 Click **Next**.
- 9 Under **Management network**, select the management network from the drop-down menu, choose whether to enable DHCP, and specify an IP address for the private OpenStack endpoint.

Note The following conditions apply:

- If you disable DHCP, you must enter:
 - One or more IP address ranges for the network
 - The subnet mask for those ranges
 - The gateway address
 - One or more DNS servers
 - The IP address of the private OpenStack endpoint cannot be included in any IP address range specified for the management network.
-

- 10 Under **API network**, select the API access network from the drop-down menu, choose whether to enable DHCP, specify an IP address for the public OpenStack endpoint and optionally specify a public hostname.

Note The following conditions apply:

- If you disable DHCP, you must enter:
 - One or more IP address ranges for the network
 - The subnet mask for those ranges
 - The gateway address
 - One or more DNS servers
- The IP address of the public OpenStack endpoint cannot be included in any IP address range specified for the API access network.
- After the initial deployment, the public hostname for the public OpenStack endpoint cannot be changed.

-
- 11 Under **Control plane resources**, select the vSphere data center, resource pool, and datastore that you want to use for the OpenStack control plane.

Note The datastore cannot be changed after the control plane has been deployed.

-
- 12 Under **Persistent storage**, select a datastore and click **Next**.

- 13 Select a networking mode from the drop-down menu.

Important You cannot change the networking mode after deploying OpenStack. To switch to a different networking mode, you must redeploy.

-
- 14 Enter the parameters for your networking back end.

- If you selected **NSX Policy**, perform the following steps:
 - a Enter the FQDN or IP address of the NSX Manager and its administrator credentials, and click **Validate**.

Note If you have deployed an NSX Manager cluster, specify only the parent NSX Manager node. 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*.

- b Select the default transport zones, tier-0 router, DHCP server profile, and metadata proxy server from the drop-down menus.
 - c Enter the secret for the metadata proxy server and click **Next**.
- If you selected **DVS**, specify the distributed switch and trunk network to use for OpenStack and click **Next**.

15 Under **Nova configuration**, click **Add** and select the vCenter Server instance containing your compute cluster.

16 Enter a Nova availability zone for the instances in the target cluster.

17 Select the desired cluster and datastore and click **Submit**.

You can click **Add** again to include multiple compute clusters in your deployment.

18 Confirm your compute settings and click **Next**.

19 Under **Glance configuration**, click **Add** and select the vCenter Server instance containing the datastore that you want to use to store images.

20 Select one or more datastores and click **OK**.

21 Confirm your image datastore settings and click **Next**.

22 Under **Cinder configuration**, click **Add** and select the vCenter Server instance containing the cluster that you want to use for the block storage.

23 Select **VMDK** or **FCD** as the backend driver.

24 Enter an availability zone for the target cluster.

25 Select one or more clusters and click **OK**.

26 Confirm your block storage settings and click **Next**.

27 Under **Local admin user**, enter the password of the OpenStack administrator account and click **Next**.

This password is used to authenticate with OpenStack and the VMware Integrated OpenStack dashboard as the cloud administrator.

Important Do not select **Configure identity source** and configure LDAP. For new deployments of VMware Integrated OpenStack 7.0.1, you can configure LDAP only after the deployment has finished. For instructions, see "Configure LDAP Authentication" in the *VMware Integrated OpenStack Administration Guide*.

28 Select whether you want to enable VMware Integrated OpenStack Carrier Edition and click **Next**.

29 Under **Barbican configuration**, select **Simple Crypto** or **KMIP** as the plugin for secret management.

If you select **KMIP**, you must enter the hostname and credentials for your KMIP server.

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

Results

The Integrated OpenStack Manager begins to deploy your OpenStack cloud, and the status of the deployment is displayed as `Provisioning`. When the status changes to `Running`, the deployment is finished.

Note Do not scale out the deployment or add components (such as Designate) while the deployment is in the `Provisioning` state.

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 by logging in to My VMware <https://my.vmware.com/group/vmware/home>.

Procedure

- 1 Log in to the OpenStack Management Server web interface as the `admin` user.
- 2 Select **Licenses** and click **Add**.
- 3 Enter a name for your license key.

The name cannot exceed 253 characters. It can only contain letters, digits, spaces, hyphens (-), and periods (.) and must start and end with a letter or digit.
- 4 Enter your license key and click **OK**.
- 5 Select your license key, click **Assign**, and click **OK**.

Results

Your license key is displayed in the table with related information. You can repeat this procedure to add more licenses as needed for your deployment.

Configuring Additional Components and Features

5

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](#)
- [Integrate VMware Integrated OpenStack with vRealize Log Insight](#)
- [Forward Logs to an External Server](#)
- [Enable the Designate Component](#)
- [Enable Carrier Edition Features](#)
- [Enable the Ceilometer Component](#)

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 vRealize Operations Management Pack for Container Monitoring.

Prerequisites

If you have already installed the vRealize Operations Management Pack for NSX-T version 2.0, uninstall the management pack before proceeding. You can reinstall version 2.0 after the vRealize Operations Management Pack for VMware Integrated OpenStack has been installed.

Procedure

- 1 Deploy and configure vRealize Operations Manager.
See [VMware vRealize Operations Manager Help](#).
- 2 Install and configure 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.

3 Configure the OpenStack instance.

See "Configure the OpenStack Instance" in the *VMware vRealize Operations Management Pack for VMware Integrated OpenStack* document.

Results

You can view VMware Integrated OpenStack objects on the dashboards displayed in vRealize Operations Manager.

What to do next

Configure the vCenter Adapter. For information, see "VMware vSphere Solution in vRealize Operations Manager" in the *vRealize Operations Manager Help* document.

For NSX deployments, you can also configure the vRealize Operations Management Pack for NSX-T or vRealize Operations Management Pack for NSX for vSphere.

- For information about the vRealize Operations Management Pack for NSX-T, see the *VMware vRealize Operations Management Pack for NSX-T* document.
- For information about the vRealize Operations Management Pack for NSX for vSphere, see documentation under the **Resources** tab on the vRealize Operations Management Pack for NSX for vSphere page on VMware Solution Exchange at <https://marketplace.vmware.com/vsx/solutions/management-pack-for-nsx-for-vsphere>.

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.cloud.vmware.com/services/details/vmware-integrated-openstack-content-pack-7-0?slug=true>.

Note By default, vRealize Log Insight 8.1.1 or later, port 9543, is used for the HTTPS connection. If you use port 9000 for the HTTP connection, disable **Require SSL Connection** in **SSL Configuration** of vRealize Log Insight.

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 Log in to the Integrated OpenStack Manager web interface as the `admin` user.
 - b In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.
 - c On the **Settings** tab, select **Log Management** and click **Edit**.
 - d Enter the IP address and port of your vRealize Log Insight syslog server and click **OK**.

Results

You can monitor the OpenStack data in vRealize Log Insight on the dashboards under **Content Pack Dashboards > OpenStack**. You can select the status of your log analytics integration by running the `viocli get deployment` command.

Forward Logs to an External Server

If you did not configure a syslog server when deploying VMware Integrated OpenStack, you can modify your deployment to send logs to a remote syslog server. You can also modify your deployment if you no longer want to send logs to vRealize Log Insight.

The procedure to forward logs to a remote server depends upon your deployment configuration.

- If you have never configured a syslog server, you enable the Fluentd Cluster Logging Custom Resource (CR) by creating a `custom-fluentd-cr.yml` file and using the Kubernetes command-line utility to apply the file.
- If you specified a vRealize Log Insight server and want to change the syslog server, you disable fluentd CR using the Kubernetes command-line utility or by removing the vRealize Log Insight IP from the VMware Integrated OpenStack UI. Then you edit the `custom-fluentd-cr.yml` file and run the file to reenables fluentd CR.

Prerequisites

Verify that a remote syslog server such as Rsyslog is installed and configured.

Procedure

- 1 (Optional) If you configured your deployment to send logs to vRealize Log Insight, disable fluentd CR.
 - To disable fluentd CR using the VMware Integrated OpenStack UI, remove the IP address that you specified for the vRealize Log Insight syslog server. See [Integrate VMware Integrated OpenStack with vRealize Log Insight](#).
 - To disable fluentd CR using the Kubernetes command-line utility, type the command:

```
osctl delete fluentd fluentd1
```

- 2 Create the custom-fluentd-cr.yml file with a valid remote syslog server IP and port.

If fluentd CR was previously enabled, you update your existing custom-fluentd-cr.yml file.

```
apiVersion: vio.vmware.com/v1alpha1
kind: Fluentd
metadata:
  name: fluentd1
  labels:
    app: lcm
    StatusController: ""
spec:
  loginsight:
    type: remote_syslog
    ip: <remote_server_ip>
    port: <remote_server_port>
```

- 3 Enable fluentd CR.

```
osctl apply -f custom-fluentd-cr.yml
```

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.

For more information about Designate, see the OpenStack Designate documentation at <https://docs.openstack.org/designate/train>.

Prerequisites

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

Infoblox:

- 1 Ensure that the DNS server can communicate with the VMware Integrated OpenStack API access network.
- 2 On the Infoblox server, create a user for Designate to use.
- 3 Create one name server group to serve Designate zones.
 - a Set the Designate mDNS servers as external primaries.
 - b Set all IP addresses on the eth1 interface of the load balancer node as external primaries.
 - c Add a grid member as a grid secondary and select the `Lead Secondary` option for this member.
 - d Add additional grid secondaries as needed.

Bind9:

- 1 Ensure that the DNS server can communicate with the VMware Integrated OpenStack API access network.
- 2 Enable `rndc addzone` and `rndc delzone` functionality to allow receipt of a NOTIFY message from a secondary node. Open `named.conf.options` or `named.conf` in a text editor and add the following lines in the `options` section:

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

- 3 Restart the Bind9 server.

PowerDNS:

- 1 Ensure that the DNS server can communicate with the VMware Integrated OpenStack API access network.
- 2 Enable the API in the `pdns.conf` file.
- 3 In the `pdns.conf` file, add the `trusted-notification-proxy` parameter and set its value to the IP address of the `eth1` interface of each controller node, separated by commas:

```
trusted-notification-proxy=controller1-eth1-ip,...
```

Microsoft DNS:

- 1 Ensure that the DNS server can communicate with the VMware Integrated OpenStack API access network.
- 2 On the Microsoft DNS server, add inbound rules allowing communication on port 5358 over TCP and UDP.
- 3 Install Python 2.7, the Microsoft Visual C++ Compiler for Python 2.7, and the pip package installer.

4 Install Designate version 8.0.0.

```
pip install designate==8.0.0
```

5 Write the following information to a file named `designate.conf`:

```
[service:agent]
backend_driver = msdns
masters = mgmt-server-ip:53
```

6 Open Command Prompt as an administrator and start the Designate agent using the `designate.conf` file:

```
designate-agent --config-file path/designate.conf
```

The Designate agent must remain open while Designate is in use.

Procedure

- 1 Log in to the Integrated OpenStack Manager web interface as the `admin` user.
- 2 In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.
- 3 On the **Settings** tab, select **Configure Designate** and click **Enable**.
- 4 Select your back end and enter the required parameters.

- Infoblox back end

Option	Description
DNS server	Enter the IP address of the Infoblox server.
DNS port	Enter the port on the Infoblox server for the DNS service. The default value is 53.
WAPI URL	Enter the Infoblox WAPI URL. The default is <code>https://<infoblox-server>/wapi/v<wapi-version-major.minor>/</code> . For example: <code>https://infoblox-server-example/wapi/v3.4/</code>
	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.
Confirm password	Confirm the password for the Infoblox username.
NS group	Specify the name server group to serve Designate zones.

- Bind9 back end

Option	Description
DNS server	Enter the IP address of the Bind9 server.
DNS port	Enter the port on the Bind9 server for the DNS service. The default value is 53.
RNDC host	Enter the IP address of the Remote Name Daemon Control (RNDC) server. The default value is the IP address of the Bind9 server.
RNDC port	Enter the port for the RNDC service. The default value is 953.
RNDC key	Enter the contents of the <code>/etc/bind/rndc.key</code> file.

- PowerDNS back end

Option	Description
DNS server	Enter the IP address of the PowerDNS server.
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 <code>http://powerdns-server/8081</code> .
API key	Enter the value of <code>api-key</code> in the <code>/etc/powerdns/pdns.conf</code> file.

- Microsoft DNS back end

Option	Description
DNS server	Enter the IP address of the Microsoft DNS server.
DNS port	Enter the port on the Microsoft DNS server for the DNS service. The default value is 53.
Agent server	Enter the IP address of the host where the Designate agent is running.
Agent port	Enter the port to use for the Designate agent service. The default value is 5358.

5 Click **Validate**. Once validation has finished, click **OK**.

Results

Tenants can now create DNS zones using the VMware Integrated OpenStack dashboard. For instructions, see "Create a DNS Zone" in the *VMware Integrated OpenStack Administration Guide*.

Enable Carrier Edition Features

You can enable VMware Integrated OpenStack Carrier Edition features through the Integrated OpenStack Manager web interface.

Prerequisites

Assign a Carrier Edition license to your VMware Integrated OpenStack deployment. See [Assign the VMware Integrated OpenStack License Key](#).

For information about licensing, see [VMware Integrated OpenStack Licensing](#).

Procedure

- 1 Log in to the Integrated OpenStack Manager web interface as the `admin` user.
- 2 In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.
- 3 On the **Settings** tab, select **Configure Carrier Edition** and click **Enable**.

Results

You can now configure your deployment to use Carrier Edition features.

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.

For more information about Ceilometer, see the OpenStack Ceilometer documentation at <https://docs.openstack.org/ceilometer/train>.

Prerequisites

Verify that the CPUs on the ESXi host running the Integrated OpenStack Manager support Advanced Vector Extensions (AVX).

Procedure

- 1 Log in to the Integrated OpenStack Manager web interface as the `admin` user.
- 2 In **OpenStack Deployment**, click the name of your deployment and open the **Manage** tab.
- 3 On the **Settings** tab, select **Configure Ceilometer** and click **Enable**.

Results

The Kubernetes pods required by Ceilometer are created and the services are enabled.

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.

Upgrading VMware Integrated OpenStack

6

Your upgrade path to VMware Integrated OpenStack 7.0.1 depends upon the version that you are migrating from.

To upgrade from VMware Integrated OpenStack 6.0 to VMware Integrated OpenStack 7.0.1, you follow instructions to [Upgrade VMware Integrated OpenStack 6.x to 7.0.1](#). If you are running an older version, follow instructions to [Upgrade VMware Integrated OpenStack 5.1 to 7.0.1](#).

As part of either upgrade path, you follow instructions to [Apply the VMware Integrated OpenStack 7.0.1 Patch](#) to your VMware Integrated OpenStack 7.0 OVA.

Before starting any upgrade, verify that your environment meets the requirements for VMware Integrated OpenStack 7.0.1. See [Hardware Requirements for VMware Integrated OpenStack](#) and [Software Requirements for VMware Integrated OpenStack](#).

If you have enabled Ceilometer, verify that the CPUs on the ESXi host support Advanced Vector Extensions (AVX). If AVX is not supported, disable Ceilometer before upgrading.

In the procedure to upgrade from VMware Integrated OpenStack 5.1, you create a VMware Integrated OpenStack 7.0.1 deployment and migrate your existing deployment to it. This procedure requires that you have sufficient hardware and IP address resources to support two deployments temporarily.

Note the following differences between a new VMware Integrated OpenStack 7.0.1 deployment and a deployment that has been upgraded from a previous version:

- The OpenStack region name of a new VMware Integrated OpenStack 7.0.1 deployment is `RegionOne`. The OpenStack region name of an upgraded deployment is `nova`.
- The names of Nova compute nodes in a new VMware Integrated OpenStack 7.0.1 deployment are in the following format: `compute-vcenter-id-cluster-moid`. The names of Nova compute nodes in an upgraded deployment are in the following format: `nova-compute-number`. After the deployment is upgraded, new Nova compute nodes use the new naming format, including nodes that are deleted and recreated.
- A new VMware Integrated OpenStack 7.0.1 deployment includes the `service` and `default` domains only. The `service` domain contains accounts used by OpenStack services, and the `Default` domain contains accounts used by OpenStack users, including the `admin` account. An upgraded deployment also contains the `local` domain for backward compatibility.

This chapter includes the following topics:

- [Apply the VMware Integrated OpenStack 7.0.1 Patch](#)
- [Remove the VMware Integrated OpenStack 7.0.1 patch](#)
- [Upgrade VMware Integrated OpenStack 6.x to 7.0.1](#)
- [Upgrade VMware Integrated OpenStack 5.1 to 7.0.1](#)

Apply the VMware Integrated OpenStack 7.0.1 Patch

To upgrade to VMware Integrated OpenStack 7.0.1, you apply a patch.

This procedure uses the `viocli` to apply the patch on a VM. You can apply the patch to an existing VMware Integrated OpenStack 7.0 deployment or apply it to a freshly installed VIO 7.0 OVA. For a freshly installed VMware Integrated OpenStack 7.0 OVA, you apply the patch as follows:

- If you are installing VMware Integrated OpenStack 7.0 and have not configured an OpenStack deployment, you apply the patch after installing the VMware Integrated OpenStack virtual appliance. See [Install the VMware Integrated OpenStack Virtual Appliance](#).
- If you are upgrading from VMware Integrated OpenStack 6.x or earlier, you install the VMware Integrated OpenStack 7.0 OVA as part of the upgrade process, then apply the patch on a VM without an OpenStack deployment. Follow the procedure to install the VMware Integrated OpenStack 7.0 OVA for the version of VMware Integrated OpenStack that you are upgrading:
 - [Upgrade VMware Integrated OpenStack 6.x to 7.0.1](#)
 - [Upgrade VMware Integrated OpenStack 5.1 to 7.0.1](#)

Prerequisites

- Download both the VMware Integrated OpenStack 7.0.1 patch and `viocli` packages from the product download page at https://my.vmware.com/en/group/vmware/info?slug=infrastructure_operations_management/vmware_integrated_openstack/7_0.
- Verify that no patches have been previously applied. For example, if the VMware Integrated OpenStack patch was previously applied, remove it before applying the patch again. See [Remove the VMware Integrated OpenStack 7.0.1 patch](#).
- If you have an existing VMware Integrated OpenStack 7.0 with an OpenStack deployment, create a backup of your existing deployment. See [Back Up Your Deployment](#)

Procedure

- 1 Log in to the Integrated OpenStack Manager in the VMware Integrated OpenStack environment.

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

- 2 Update the `viocli` binary for the VMware Integrated OpenStack 7.0 virtual machine and change access permissions.

```
tar -xvf viocli.tar.gz
```

```
cp ./export/cli/viocli /usr/bin
```

```
chmod -R a+x /usr/bin/viocli
```

- 3 Add the patch to VMware Integrated OpenStack 7.0.

```
viocli patch add -l <VIO_7.0.1_patch_tar_path>
```

Where `VIO_7.0.1_patch_tar_path` is `patch-7.0.1.0-17200834.tar.gz`.

- 4 Verify that the patch has been added.

```
viocli patch list
```

If properly added, the state of the patch appears as: `ADDED`.

- 5 Install the patch.

```
viocli patch install -p <VIO_7.0.1_patch_name>
```

Where `VIO_7.0.1_patch_name` is `patch-7.0.1.0-17200834`.

- 6 Verify that the patch has been installed.

```
viocli patch list
```

- If properly installed on an existing VMware Integrated OpenStack 7.0 deployment, the state of the patch appears as: `APPLIED`.
- If properly installed on a freshly installed VMware Integrated OpenStack 7.0 OVA, such as with an upgrade or new installation, the state of the patch appears as: `APPLYING`.

- 7 (Optional) If you are applying the patch on an existing VMware Integrated OpenStack 7.0 deployment, check the patch deployment status.

```
viocli get deployment
```

If the deployment is stable, the state of the patch appears as: `RUNNING`, indicating that all OpenStack services have been patched.

Note If an error occurs or the deployment does not remain stable, retain the support bundle for tracking.

What to do next

If you applied the patch to a freshly installed VMware Integrated OpenStack 7.0 OVA, continue with the process for your new VMware Integrated OpenStack installation or upgrade:

- If performing a fresh install of VMware Integrated OpenStack 7.0, continue in the process with [Create an OpenStack Deployment](#).
- If upgrading from VMware Integrated OpenStack 6.x, return to [Upgrade VMware Integrated OpenStack 6.x to 7.0.1](#) and restore your backup.
- If upgrading from VMware Integrated OpenStack 5.1, continue in the upgrade process with [Migrate to the New VMware Integrated OpenStack Deployment](#).

Remove the VMware Integrated OpenStack 7.0.1 patch

If you do not want to use VMware Integrated OpenStack 7.0.1, you can remove the patch and revert to version 7.0.

Procedure

- 1 Remove the VMware Integrated OpenStack 7.0.1 patch.

```
viocli patch delete -p <VIO_7.0.1_patch_name>
```

- 2 (Optional) If you are removing the patch from an existing VMware Integrated OpenStack 7.0 deployment, check the OpenStack deployment status.

```
viocli get deployment
```

If the deployment is stable, the state of the patch appears as: `RUNNING`. The state of the patch should remain `RUNNING`, indicating that all OpenStack services have been rolled back to version 7.0.

- 3 To manually revert three core services: `vio-operator`, `vio-api`, and `nginx-ingress`, enter the following four commands.

```
helm repo update
```

```
helm upgrade --install vio-ingress-ctl vio/nginx-ingress --version=1.6.0 --values /vio/config/input/mgmt-ingress-ctl-values.yml
```

```
helm upgrade --install vio-operator vio/vio-operator --version=1.0.0 --values /vio/config/input/vio-api-ctl-values.yml
```

```
helm upgrade --install vio-api vio/vio-api --version=1.0.0 --values /vio/config/input/vio-api-ctl-values.yml
```

Note If an error occurs, retain the support bundle for tracking.

Upgrade VMware Integrated OpenStack 6.x to 7.0.1

You follow this procedure to upgrade from VMware Integrated OpenStack 6.x to 7.0.1.

Prerequisites

- Download the VMware Integrated OpenStack 7.0 OVA from the product download page at https://my.vmware.com/en/group/vmware/info?slug=infrastructure_operations_management/vmware_integrated_openstack/7_0.
- Ensure that your current deployment is running VMware Integrated OpenStack 6.0 or later. If you are running an older version, follow the procedure described in [Upgrade VMware Integrated OpenStack 5.1 to 7.0.1](#).

Procedure

- 1 Log in to the Integrated OpenStack Manager in the existing VMware Integrated OpenStack environment.

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

- 2 Run the `ovfenv` command to determine the OVF configuration for your existing VMware Integrated OpenStack environment.

```
ovfenv
```

Record the output of this command for later use.

- 3 Create a backup of your existing VMware Integrated OpenStack environment.
For instructions, see [Back Up Your Deployment](#).
- 4 Export the configuration for your existing VMware Integrated OpenStack deployment.
 - a Log in to the Integrated OpenStack Manager web interface of your existing VMware Integrated OpenStack deployment.
 - b Click **OpenStack Deployment**.
 - c Select your deployment and click **Export Template**.

Save the exported template for later use.

- 5 Install the OVA on your vCenter Server instance.

Important

- Ensure that all aspects of the OVF configuration are consistent with your existing VMware Integrated OpenStack environment. To determine the correct configuration, refer to the output of the `ovfenv` command in Step 2.
 - Do not power on the newly installed VMware Integrated OpenStack virtual appliance at this time.
-

For more information, see [Install the VMware Integrated OpenStack Virtual Appliance](#).

- 6 Stop the existing VMware Integrated OpenStack deployment.
 - a In the vSphere Client, power off the Integrated OpenStack Manager virtual machine.
 - b Take a snapshot of the Integrated OpenStack Manager virtual machine.
 - c Power off all OpenStack controller virtual machines.
- 7 Power on the new VMware Integrated OpenStack virtual appliance.
- 8 Patch the freshly installed VMware Integrated OpenStack 7.0 OVA. See [Apply the VMware Integrated OpenStack 7.0.1 Patch](#).
- 9 Restore the backup that you created in Step 3 on the new VMware Integrated OpenStack installation.

When restoring the backup, you must use the configuration file template for restoring VMware Integrated OpenStack on a new control plane. For instructions, see [Restore Your Deployment from a Backup](#).

To determine the correct values for the required parameters, refer to the exported template in Step 4.

Results

Your existing environment is migrated to VMware Integrated OpenStack 7.0.1. When the status of your OpenStack deployment is displayed as `Running`, the upgrade process is finished. You can check the status of your deployment by running the `viocli get deployment` command.

After the new deployment is in the `Running` status, you can safely delete the manager and controller virtual machines for the old deployment.

Upgrade VMware Integrated OpenStack 5.1 to 7.0.1

You upgrade from VMware Integrated OpenStack 5.1 to 7.0.1 by installing the new version and migrating your existing deployment.

Prerequisites

- Verify that your current deployment is running VMware Integrated OpenStack 5.1. If you are running an older version, upgrade to version 5.1 first.
- Verify that there is a user named `admin` in the local domain in the VMware Integrated OpenStack 5.x deployment. This user is needed if the default domain is configured as LDAP during the upgrade. If there is no user named `admin`, manually create a user with that name in the 5.x environment.

Note If the `admin` password has been updated from the OpenStack side, the `admin` password extracted by the upgrade script may differ from the actual password. If so, you need to edit `data.admin_password` of `secret/managedpasswords` in `cluster.yml` with the actual password.

- If the VMware Integrated OpenStack 5.1 deployment includes multiple load balancers, disable the LDAP load balancer.
- If a domain is configured with LDAP, ensure that the domain name is appended to the bind user.
- Check the nova_api cell_mappings table for a row with a NULL name. If found, correct the name to ensure that schema migrations run correctly.

a From the OpenStack Management Server, log in to any database node on the VIO 5.1 control plane.

b Switch to the root user.

```
sudo su -
```

c To start the MariaDB client, run the `mysql` command.

d To access the nova_api database, run the SQL command: `use nova_api`

e Run the SQL command: `select id,name from cell_mappings;`

f Examine the output. Look for any row with NULL in the name column. In the following example, NULL appears in the row with id=9.

```
+-----+-----+
| id | name |
+-----+-----+
| 6 | cell0 |
| 9 | NULL |
+-----+-----+
```

g With the ID of the row that has NULL in the name column, run the SQL command to correct the name.

```
update cell_mappings set name='cell1' where id=<ID_of_row_with_NULL>;
```

h Run the SQL command: `select id,name from cell_mappings;`

i Examine the output. In the following example, cell1 replaces NULL in the row with id=9.

```
+-----+-----+
| id | name |
+-----+-----+
| 6 | cell0 |
| 9 | cell1 |
+-----+-----+
```

- Download the VMware Integrated OpenStack 7.0 OVA, the 7.0.1 patch, upgrade, and viocli packages from the product download page at https://my.vmware.com/en/group/vmware/info?slug=infrastructure_operations_management/vmware_integrated_openstack/7_0. The files require approximately 6 GB of storage space.

- Record any custom changes made to the OpenStack deployment outside of the `custom.yml` and `custom-playbook.yml` files. Customizations outside of these files must be reconfigured on the new deployment once the upgrade is complete.
- If you have configured identity federation with VMware Identity Manager using the OIDC protocol, delete the configured identity provider before upgrading. You can add the identity provider again once the upgrade is complete.

To delete the provider, run the `openstack identity provider delete idp-name` command.

- If you have configured VMware Integrated OpenStack to use an NSX Manager cluster, remove this configuration before upgrading. To do so, change the value of the `nsxv3_api_managers` parameter to include only the IP address of the parent NSX Manager. You can add the other managers in your cluster once the upgrade is complete.
- If you have deployed Swift, record your cluster configuration. Swift clusters cannot be upgraded to VMware Integrated OpenStack 7.0, and the Swift configuration is not preserved. If you want to continue using Swift, you can recreate your cluster after the upgrade is complete.
- Verify that no internal OpenStack management workloads are running.

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 Virtual Appliance](#)

You install the VMware Integrated OpenStack 7.0 virtual appliance and apply the 7.0.1 patch on your existing vCenter Server instance.

3 [Migrate to the New VMware Integrated OpenStack Deployment](#)

You run an upgrade conversion script on your old deployment to generate the files required for upgrade. Then you apply the upgrade files on your new deployment to complete the migration process.

4 [Upgrade and Assign Your License Key](#)

After you upgrade to VMware Integrated OpenStack 7.0.1, you must upgrade your license key in My VMware and assign it to your new deployment.

5 [Delete the Old VMware Integrated OpenStack Deployment](#)

After you upgrade VMware Integrated OpenStack, you can delete virtual machines from the previous version to release resources.

6 [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.

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.

In VMware Integrated OpenStack 7.0.1, each worker node requires one IP address on the management network and one IP address on the API access network. This means that the management and API access networks require at least three available IP addresses each for HA deployments and at least one available IP address each for non-HA deployments.

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 Integrated OpenStack Manager in the management network IP range. If you have already allocated additional IP addresses for upgrades, assign the first available IP address to the Integrated OpenStack Manager 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.
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.
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 Virtual Appliance

You install the VMware Integrated OpenStack 7.0 virtual appliance and apply the 7.0.1 patch on your existing vCenter Server instance.

This procedure describes how to install the VMware Integrated OpenStack using the vSphere Client. If you want to use the OVF Tool to install the virtual appliance, you must include the `--allowExtraConfig` parameter.

Prerequisites

Confirm that your management and API access networks include sufficient IP addresses for the new installation. See [Add IP Addresses to the Network Configuration](#).

Procedure

- 1 Log in to the vSphere Client and select the **Hosts and Clusters** view.
- 2 Edit the settings of the management cluster previously configured for VMware Integrated OpenStack and set **DRS Automation** to **Manual**.

Important Do not use Storage vMotion to migrate VMware Integrated OpenStack vApp and controller VMs, which will rename the vmdk files for Kubernetes Persistent Volume and break the function.

- 3 Right-click the management cluster and select **Deploy OVF Template...** from the pop-up menu.
- 4 Provide the path to the VMware Integrated OpenStack OVA and click **Next**.
- 5 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.

- 6 Select the cluster on which to run the vApp and click **Next**.
- 7 Review the details of the template to be installed and click **Next**.
- 8 Read the license agreements and select **I accept all license agreements**. Then click **Next**.
- 9 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*.

- 10 In the **Destination Network** column, select the existing management network and click **Next**.

- 11 On the **Customize template** page, enter additional settings for VMware Integrated OpenStack.
 - a Under **Network properties**, you can enter static IP addresses for the Integrated OpenStack Manager virtual machine and DNS server.

If you want to use DHCP, leave all fields blank. If you enter a static IP address for the Integrated OpenStack Manager, you must also enter the subnet mask, default gateway, and DNS server.
 - b Under **System**, enter an initial password for the administrator accounts on the Integrated OpenStack Manager.

This password is used for the `admin` account on the web interface and the `root` user on the Integrated OpenStack Manager virtual machine. The following rules apply to the password:

 - The password must contain between 8 and 128 characters.
 - The password must contain at least 1 uppercase letter, 1 lowercase letter, 1 digit, and 1 special character.
 - The password cannot contain simplistic patterns, common words, or words derived from the name of the account.
 - c For **Permit Root Logon**, select **true**.
 - d Under **Internal Network**, enter the network address of the Kubernetes service network, the network address of the Kubernetes pod network, and the domain name suffix of the service network.

Note The service and pod networks must not overlap each other or any existing networks. The service network domain suffix must not overlap any existing domains.

For example, if your current domain is named `corp.local`, you cannot use `cluster.local` as your service network domain. Use a different domain suffix, such as `cluster.example`.

- e (Optional) Under **Log Management**, enter the IP address and port number of your log analytics server.

You can add or update the log analytics server information after the deployment is finished.
 - f (Optional) Under **Time Management**, enter one or more NTP servers to use for time synchronization.

All VMware Integrated OpenStack virtual machines must use a single, highly available time source. If you cannot configure a time source on all ESXi hosts, you must enter an NTP server in this field.
- 12 Once `All properties have valid values` is displayed in the upper left of the page, 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 Right-click the name of the VMware Integrated OpenStack vApp and select **Power > Power On**.
- 15 Select the new Integrated OpenStack Manager virtual machine in the vApp and record its IP address.

You can access this IP address to log in to the new Integrated OpenStack Manager through the web interface or SSH.

What to do next

[Apply the VMware Integrated OpenStack 7.0.1 Patch](#)

Migrate to the New VMware Integrated OpenStack Deployment

You run an upgrade conversion script on your old deployment to generate the files required for upgrade. Then you apply the upgrade files on your new deployment to complete the migration process.

Prerequisites

- Install the VMware Integrated OpenStack 7.0 virtual appliance and apply the 7.0.1 patch. See [Install the New Virtual Appliance](#).
- Confirm that your existing VMware Integrated OpenStack deployment is running properly. On the old OpenStack Management Server, run the `viocli deployment status` command.
- Verify that the backup functionality on the existing VMware Integrated OpenStack deployment works properly and that the disk is not full.
- Transfer the upgrade conversion script to the old OpenStack Management Server.

Procedure

- 1 Log in to the old OpenStack Management Server as `viouser`.
- 2 Switch to the `root` user.

```
sudo su -
```

- 3 Decompress and run the upgrade conversion script.

```
tar -xzf vio-upgrade-7.0.1.0-build-number.tar.gz
```


Before running the script, change the current working directory to the directory containing the script.

```
cd upgrade
```

```
./upgrade.sh
```

When prompted, enter the password for the `viouser` account.

The script collects a support bundle, backs up the OpenStack database, and generates the following files:

- `/tmp/pre_upgrade/upgrade.tar.gz`
 - `./cluster.yaml`
 - `./restore.yaml`
 - `./themes.tar` (only if you have previously customized the VMware Integrated OpenStack dashboard theme)
- 4 (Optional) The upgrade migrates your old deployment to a new medium-sized deployment by default. To change the size of the new deployment, edit the `cluster.yaml` file and change the size of the VMware Integrated OpenStack manager and controller nodes.

The following example `cluster.yaml` file shows the size of the manager and controller nodes set to large.

```
apiVersion: vio.vmware.com/v1alpha1
kind: VIOMachineSet
metadata:
  labels:
    app: lcm
    clusterController: "true"
  name: manager1
spec:
  count: 1
  providerConfig:
    value:
      machineSpec:
        datacenter: sanity_dc
        datastore: datastore-nfs
        resourcePool: VIO_resource_pool
  size: large
  vmware_insecure: .VCenter:vcenter1:spec.insecure
  vmware_server_host: .VCenter:vcenter1:spec.hostname
  vmware_server_password: .VCenter:vcenter1:spec.password
  vmware_server_username: .VCenter:vcenter1:spec.username
---
apiVersion: vio.vmware.com/v1alpha1
kind: VIOMachineSet
metadata:
  labels:
    app: lcm
```

```

clusterController: "true"
name: controller1
spec:
  count: 3
  providerConfig:
    value:
      machineSpec:
        datacenter: sanity_dc
        datastore: datastore-nfs
        resourcePool: VIO_resource_pool
  size: large
vmware_insecure: .VCenter:vcenter1:spec.insecure
vmware_server_host: .VCenter:vcenter1:spec.hostname
vmware_server_password: .VCenter:vcenter1:spec.password
vmware_server_username: .VCenter:vcenter1:spec.username

```

- 5 Stop the old VMware Integrated OpenStack deployment.

```
sudo viocli deployment stop
```

Note OpenStack services are unavailable until the migration process is finished.

- 6 In the vSphere Client, create a content library named **VIO**.
- 7 Upload the `/tmp/pre_upgrade/upgrade.tar.gz` file to the content library.

If the `themes.tar` file was generated, upload the file to the content library also.

Note Before clicking **Import**, verify the names of the files that appear. If `upgrade.tar.gz` is missing the `.gz` extension, add it. If `themes.tar` is missing the `.tar` extension, add it.

- 8 Transfer the `cluster.yaml` and `restore.yaml` files to the new Integrated OpenStack Manager.
- 9 Log in to the new Integrated OpenStack Manager as the `root` user.
- 10 Apply the cluster configuration file to the new VMware Integrated OpenStack deployment.

```
kubectl -n openstack create -f cluster.yaml
```

- 11 Apply the upgrade configuration file to the new VMware Integrated OpenStack deployment.

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

Results

OpenStack services are now provided by the new deployment.

What to do next

- Assign your VMware Integrated OpenStack license key to the new deployment. See [Upgrade and Assign Your License Key](#).

- 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 private OpenStack endpoint of the new deployment.

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](#).

Upgrade and Assign Your License Key

After you upgrade to VMware Integrated OpenStack 7.0.1, you must upgrade your license key in My VMware and assign it to your new deployment.

Procedure

- 1 Upgrade your license key as described in [KB 2006974](#).
- 2 Log in to the OpenStack Management Server web interface (Do not use the VMware Integrated OpenStack plugin in vCenter) as the `admin` user.
- 3 Select **Licenses** and click **Add**.
- 4 Enter a name for your license key.
The name cannot exceed 253 characters. It can only contain letters, digits, spaces, hyphens (-), and periods (.) and must start and end with a letter or digit.
- 5 Enter your license key and click **OK**.
- 6 Select your license key, click **Assign**, and click **OK**.

Results

Your license key is displayed in the table with related information. You can repeat this procedure to add more licenses as needed for your deployment.

Delete the Old VMware Integrated OpenStack Deployment

After you upgrade VMware Integrated OpenStack, you can delete virtual machines from the previous version to release resources.

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.
- Do not use the VMware Integrated OpenStack plugin in vCenter Server to delete the deployment.
- For NSX Data Center for vSphere deployments, do not remove edge nodes from the edge cluster.

Procedure

- 1 In the vSphere Client (Do not use the VMware Integrated OpenStack plugin in vCenter), delete the VMware Integrated OpenStack controller virtual machines.
- 2 Delete the Integrated OpenStack Manager virtual machine.

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, power off and delete the new VMware Integrated OpenStack virtual appliance and any virtual machines generated by the new deployment.
- 2 Log in to the old OpenStack Management Server as `viouser`.
- 3 Start the previous OpenStack deployment.

```
sudo viocli deployment start
```

- 4 Delete the upgrade conversion script files from the OpenStack Management Server.