

# VMware Cloud Foundation Operations and Administration Guide

09 FEB 2021

VMware Cloud Foundation 4.2

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](http://www.vmware.com)

Copyright © 2015-2021 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

About the VMware Cloud Foundation Operations and Administration Guide	8
<b>1 Administering VMware Cloud Foundation Systems</b>	<b>9</b>
VMware Software Components Deployed in a Typical VMware Cloud Foundation System	10
Web Interfaces Used When Administering Your VMware Cloud Foundation System	10
<b>2 Getting Started with SDDC Manager</b>	<b>12</b>
Log in to the SDDC Manager Dashboard	12
Tour of the SDDC Manager User Interface	13
Log out of the SDDC Manager Dashboard	15
<b>3 Configuring Customer Experience Improvement Program</b>	<b>17</b>
<b>4 Certificate Management</b>	<b>19</b>
View Certificate Information	20
Configure a Microsoft Certificate Authority	21
Add OpenSSL CA support	22
Install Certificates with the Microsoft Certificate Authority or OpenSSL Certificate Authority	23
Install Certificates with External or Third-Party Certificate Authorities	25
Clean Out Old or Unused Certificates	29
<b>5 License Management</b>	<b>30</b>
Add License Keys for the Software in Your VMware Cloud Foundation System	30
Edit License Description	31
Delete License Key	31
<b>6 Prepare ESXi Hosts for VMware Cloud Foundation</b>	<b>32</b>
Create a Custom ISO Image for ESXi	33
Create a Custom ESXi ISO Image Using VMware PowerCLI	33
Create a Custom ESXi ISO Image Using vSphere Lifecycle Manager	34
Install ESXi Interactively and Configure Hosts for VMware Cloud Foundation	35
Install ESXi on VMware Cloud Foundation Hosts Using the ISO	36
Configure the Network on VMware Cloud Foundation Hosts	36
Configure the Virtual Machine Network Port Group on VMware Cloud Foundation Hosts	37
Configure SSH and NTP on VMware Cloud Foundation Hosts	38
Install ESXi Using the VMware Imaging Appliance	38
Download ESXi Software and VIBs	40
Provide Network Information for Imaging	40

Upload ISOs and VIBs to the VMware Imaging Appliance service	41
Image Servers with ESXi and VIBs	42
Post-Imaging Tasks	44
Regenerate the Self-Signed Certificate on All Hosts	45
Configure ESXi Hosts with Signed Certificates	46

## 7 Host Management 47

Network Pool Management	47
Size a Network Pool	48
Create a Network Pool	49
View Network Pool Details	50
Edit a Network Pool	51
Rename a Network Pool	51
Delete a Network Pool	51
Enable Additional pNICs on Hosts	52
Commission Hosts	52
Decommission Hosts	57
View Host Inventory	57
Normal Lockdown Mode	59

## 8 vSphere Lifecycle Manager Image Management 60

Create a Cluster Image	62
Making a Cluster Image Available in VMware Cloud Foundation	63
Export a vSphere Lifecycle Manager Image	64
Extract a vSphere Lifecycle Manager Image	65
View vSphere Lifecycle Manager Images	66
Firmware Updates	66

## 9 Storage Management 67

Sharing Remote Datastores with HCI Mesh for VI Workload Domains	69
vVols Storage for VI Workload Domains	69
Add a VASA Provider	70
View a VASA Provider	70
Edit a VASA Provider	70
Delete a VASA Provider	71

## 10 Working with Workload Domains 72

Adding Virtual Machines to the Management Domain	74
About VI Workload Domains	75
Prerequisites for a Workload Domain	76
Start the VI Configuration Wizard	79

Specify Names and vSphere Lifecycle Manager Method	79
Specify vSphere Cluster Details	80
Specify Compute Details	80
Specify Networking Details	80
Select the vSAN Parameters	82
Specify the VMFS on FC Datastore	82
Specify vVols Storage Details	83
Select Hosts	83
Specify NFS Storage Details	84
Select Licenses	84
View Object Names	85
Review Details and Start the Creation Workflow	85
Deploying a VI Workload Domain with a Remote Cluster	86
Deploying NSX-T Edge Clusters	87
Create an NSX-T Edge Cluster	88
View Workload Domain Details	93
Delete a VI Workload Domain	93
View vSphere Cluster Details	95
Rename a Cluster	95
Shrink a Workload Domain	96
Remove a Host from a vSphere Cluster in a Workload Domain	96
Delete a vSphere Cluster from a Workload Domain	97
Expand a Workload Domain	98
Add a Host to a vSphere Cluster in a Workload Domain	98
Add a vSphere Cluster to a Workload Domain	100
Rename a Workload Domain	103
<b>11 Working with Workload Management</b>	<b>104</b>
Sizing Compute and Storage Resources for VMware Cloud Foundation with Tanzu	104
Enable Workload Management	105
View Workload Management Cluster Details	106
Update Workload Management License	107
<b>12 vRealize Suite Lifecycle Manager in Cloud Foundation</b>	<b>108</b>
Deploy vRealize Suite Lifecycle Manager in Cloud Foundation	109
Connect vRealize Suite Products to Workload Domains in VMware Cloud Foundation	111
<b>13 Download an Install Bundle</b>	<b>113</b>
<b>14 Multi-Instance Management</b>	<b>114</b>
About the Multi-Instance Management Dashboard	116

Create a Federation	119
Invite a VMware Cloud Foundation Instance to Join a Federation	121
Join a Federation	122
Join a Federation by Clicking an Invitation	122
Join a Federation through the Multi-Instance Management Dashboard	123
Leave a Federation	124
Dismantle a Federation	124
Certificate Rotation	125
<b>15 Stretching Clusters</b>	<b>126</b>
About Availability Zones and Regions	127
Stretched Cluster Requirements	127
Deploy and Configure vSAN Witness Host	130
Stretch a Cluster	130
Expand a Stretched Cluster	137
Unstretch a Cluster	140
Replace a Failed Host in a Stretched Cluster	141
Change the vSAN Witness Host in a Stretched Cluster	143
<b>16 Composability Management</b>	<b>144</b>
Configure Translation Layer	144
Compose a Server	146
View Composability Information	147
Add Storage	147
Remove Storage	147
Decompose a Server	148
<b>17 Monitoring Capabilities in the VMware Cloud Foundation System</b>	<b>149</b>
Viewing Tasks and Task Details	149
<b>18 Updating Cloud Foundation DNS and NTP Servers</b>	<b>151</b>
Update DNS Server Configuration	151
Update NTP Server Configuration	154
<b>19 Supportability and Serviceability (SoS) Utility</b>	<b>158</b>
SoS Utility Options	158
Collect Logs for Your VMware Cloud Foundation System	162
Component Log Files Collected by the SoS Utility	164
<b>20 Replacing Host Components</b>	<b>167</b>
Avoiding Unintentional Downtime	167

- Replacing Components of a Host Running in Degraded Mode 168
  - Replace Components of an Assigned Host Running in Degraded Mode 168
  - Replace Components of an Unassigned Host Running in Degraded Mode 169
- Replace a Dead Host 169
- Replace Boot Disk on a Host 170

## **21 User and Group Management 171**

- Add a User or Group to VMware Cloud Foundation 171
- Remove a User or Group 172
- Create a Local Account 172
- Create an Automation Account 174

## **22 Password Management 178**

- Rotate Passwords 179
- Manually Update Passwords 180
- Remediate Passwords 182
- Look Up Account Credentials 183
- Updating SDDC Manager Passwords 184
  - Update SDDC Manager Root and Super User Passwords 185
  - Update SDDC Manager REST API Account Password 185
  - Update SDDC Manager Local Account Password 186
  - Update Expired SDDC Manager root Password 186

## **23 Backing Up and Restoring SDDC Manager and NSX Manager 188**

- Image-Based Backup and Restore 188
- File-Based Backup and Restore 189
  - Configure an External SFTP Server for File-Based Backups 189
  - Configure a Backup Schedule for SDDC Manager VM 191
  - Restore SDDC Manager 193

## **24 VMware Cloud Foundation Glossary 194**

# About the VMware Cloud Foundation Operations and Administration Guide

The *VMware VMware Cloud Foundation Operations and Administration Guide* provides information about managing a VMware Cloud Foundation™ system, including managing the system's virtual infrastructure, managing users, configuring and deploying service offerings, and upgrading and monitoring the system.

## Intended Audience

The *VMware VMware Cloud Foundation Operations and Administration Guide* is intended for cloud architects, infrastructure administrators, and cloud administrators who are familiar with and want to use VMware software to quickly deploy and manage an SDDC. The information in this document is written for experienced data center system administrators who are familiar with:

- Concepts of virtualization, software-defined data centers, virtual infrastructure (VI), and virtual desktop infrastructure (VDI)
- VMware virtualization technologies, such as VMware ESXi™, the hypervisor
- Software-defined networking using VMware NSX-T™ Data Center
- Software-defined storage using VMware vSAN™
- IP networks

Additionally, you should be familiar with these VMware software products, software components, and their features:

## Related Publications

The *Introducing VMware Cloud Foundation* document provides a high-level overview of the VMware Cloud Foundation product.

The *Planning and Preparation Workbook* provides detailed information about the software, tools, and external services that are required for VMware Cloud Foundation.

The *VMware VMware Cloud Foundation Deployment Guide* contains detailed information about a VMware Cloud Foundation system, its components, and the network topology of a deployed system.

The *VMware Cloud Foundation Lifecycle Management* document describes how to manage the lifecycle of a Cloud Foundation environment.



# Administering VMware Cloud Foundation Systems

# 1

As an SDDC administrator, you use the information in the *VMware Cloud Foundation Operations and Administration* document to understand how to administer and operate your installed VMware Cloud Foundation system.

An administrator of a VMware Cloud Foundation system performs tasks such as:

- Manage certificates and passwords.
- Add capacity to your system.
- Configure and provision the systems and the workload domains that are used to provide service offerings.
- Manage provisioned workload domains.
- Monitor alerts and the health of the system.
- Troubleshoot issues and prevent problems across the physical and virtual infrastructure.
- Perform life cycle management on the VMware Cloud Foundation software components.

---

**Note** Perform all VMware Cloud Foundation operations in the SDDC Manager UI. Do not use the vSphere Client/Web Client or VMware Host Client to modify or delete resources which VMware Cloud Foundation has deployed and configured, unless specifically instructed to do so in the VMware Cloud Foundation documentation.

---

See the *Introducing VMware Cloud Foundation* document for a high-level overview of the VMware Cloud Foundation product and the *VMware VMware Cloud Foundation Deployment Guide* for information on deploying the product.

This chapter includes the following topics:

- [VMware Software Components Deployed in a Typical VMware Cloud Foundation System](#)
- [Web Interfaces Used When Administering Your VMware Cloud Foundation System](#)

## VMware Software Components Deployed in a Typical VMware Cloud Foundation System

In a typical VMware Cloud Foundation system, you encounter specific VMware software that SDDC Manager deploys in the system.

---

**Note** For information about which specific editions of each VMware product are licensed for use with the VMware Cloud Foundation license, use the information resources at the VMware Cloud Foundation product information page at <http://www.vmware.com/products/cloud-foundation.html>.

---

For the exact version numbers of the VMware products that you will see in your VMware Cloud Foundation system after the initial bring-up process, see the *Release Notes* document for your VMware Cloud Foundation version. If the system has been updated after the initial bring-up process using the Life Cycle Management features, see "View Upgrade History" in the *VMware Cloud Foundation Upgrade Guide* for details on how to view the versions of the VMware software components that are within your system.

---

**Caution** Do not manually change any of the settings that SDDC Manager sets automatically. If you change the generated settings, like names of VMs, port groups, virtual switches, or resource pools, unpredictable results might occur. Do not change settings for the resources that are automatically created and deployed during workflows, the workload domain processes, assigned IP addresses or names, and so on.

---

You can find the documentation for the following VMware software products and components at [docs.vmware.com](https://docs.vmware.com):

- vSphere (vCenter Server and ESXi)
- vSAN
- NSX-T Data Center
- vRealize Suite

## Web Interfaces Used When Administering Your VMware Cloud Foundation System

You use SDDC Manager loaded in a browser for the single-point-of-control management of your VMware Cloud Foundation system. This user interface provides centralized access to and an integrated view of the physical and virtual infrastructure of your system.

In addition to using the SDDC Manager Dashboard, you can use the following user interfaces for administration tasks involving their associated VMware software components that are part of a VMware SDDC. All these interfaces run in a browser, and you can launch them from within the SDDC Manager Dashboard.

Launch links are typically identified in the user interface by the launch icon: .

VMware SDDC Web Interfaces	Description	Launch Link Location in SDDC Manager Dashboard
vSphere Client	This interface provides direct management of resources managed by the vCenter Server instances, for identity management, and for management of the NSX resources that provide the software-defined networking capabilities of the SDDC. You can also manage object level storage policies for distributed software-defined storage provided by vSAN.	<ol style="list-style-type: none"> <li>1 On the SDDC Manager Dashboard, click <b>Inventory &gt; Workload Domains</b>.</li> <li>2 Click <b>View Details</b> for a workload domain.</li> <li>3 In the Domain column, click the domain name.</li> <li>4 Click the <b>Services</b> tab.</li> <li>5 Click the vCenter Server launch link.</li> </ol>
NSX-T Manager Web interface		<ol style="list-style-type: none"> <li>1 On the SDDC Manager Dashboard, click <b>Inventory &gt; Workload Domains</b>.</li> <li>2 Click <b>View Details</b> for a workload domain.</li> <li>3 In the Domain column, click the domain name.</li> <li>4 Click the <b>Services</b> tab.</li> <li>5 Click the NSX-T Cluster launch link.</li> </ol>

# Getting Started with SDDC Manager

## 2

You use SDDC Manager to perform administration tasks on your VMware Cloud Foundation system. This user interface provides an integrated view of the physical and virtual infrastructure and centralized access to manage the physical and logical resources.

You work with the SDDC Manager Dashboard by loading it in a web browser. For the list of supported browsers and versions, see the *Release Notes*.

---

**Note** When performing out-of-band (OOB) troubleshooting of hardware, some vendors may use Java-based consoles. Refer to the vendor documentation for supported browsers.

---

This chapter includes the following topics:

- [Log in to the SDDC Manager Dashboard](#)
- [Tour of the SDDC Manager User Interface](#)
- [Log out of the SDDC Manager Dashboard](#)

## Log in to the SDDC Manager Dashboard

You access SDDC Manager through the SDDC Manager Dashboard in a supported browser.

### Prerequisites

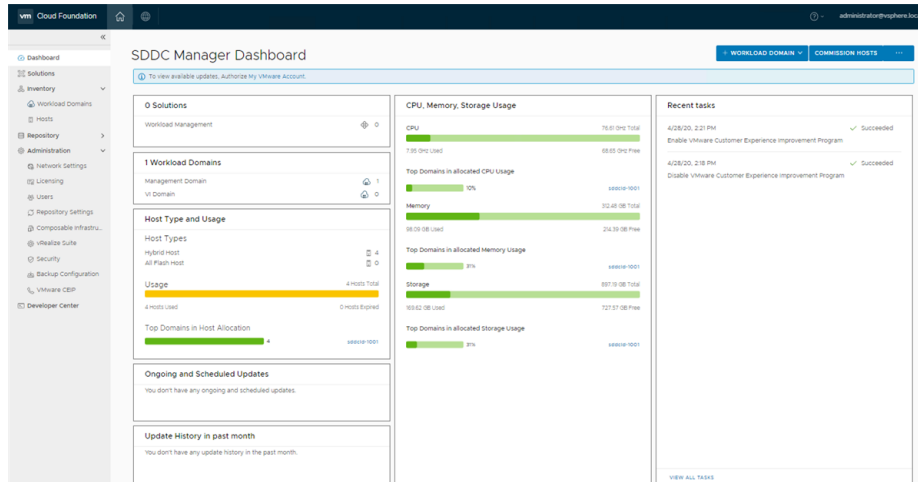
To log in, you need the SDDC Manager IP address or FQDN and the password for the single-sign on user (for example **administrator@vsphere.local**). You added this information to the deployment parameter workbook before bring-up.

### Procedure

- 1 In a browser, type one of the following:
  - `https://FQDN` where *FQDN* is the host name of the SDDC Manager.
  - `https://IP_address` where *IP\_address* is the IP address of the SDDC Manager.
- 2 Log in with the single-sign on user credentials.

### Results

You are logged in to SDDC Manager and the Dashboard page appears in the browser.



## Tour of the SDDC Manager User Interface

The the SDDC Manager Dashboard provides a single point of control for managing and monitoring your VMware Cloud Foundation instance and for provisioning workload domains.

You use the navigation bar to move between the main areas of the user interface.

### Navigation Bar

The navigation bar is available on the left side of the interface and provides a hierarchy for navigating to the corresponding pages.

Category	Functional Areas
Dashboard	<p>The Dashboard provides the high-level administrative view for SDDC Manager in the form of widgets. There are widgets for Solutions; Workload Domains; Host Types and Usage; Ongoing and Scheduled Updates; Update History; CPU, Memory, Storage Usage; and Recent Tasks.</p> <p>You can control the widgets that are displayed and how they are arranged on the dashboard.</p> <ul style="list-style-type: none"> <li>■ To rearrange widgets, click the heading of the widget and drag it to the desired position.</li> <li>■ To hide a widget, hover the mouse anywhere over the widget to reveal the <b>X</b> in the upper-right corner, and click the <b>X</b>.</li> <li>■ To add a widget, click the three dots in the upper right corner of the page and select <b>Add New Widgets</b>. This displays all hidden widgets. Select a widget and click <b>Add</b>.</li> </ul>
Solutions	<p>Solutions include the following section:</p> <ul style="list-style-type: none"> <li>■ Kubernetes - Workload Management enables you to start a Workload Management deployment and view Workload Management cluster details.</li> </ul>

Category	Functional Areas
Inventory	<p>Inventory includes the following sections:</p> <ul style="list-style-type: none"> <li>■ <b>Workload Domains</b> takes you to the Workload Domains page, which displays and provides access to all workload domains.</li> </ul> <p>This page includes summary information about all workload domains, including domain type, storage usage, configuration status, owner, clusters, hosts and update availability. It also displays CPU, memory, and storage utilization for each workload domain, and collectively across all domains.</p> <ul style="list-style-type: none"> <li>■ <b>Hosts</b> takes you to the Hosts page, which displays and provides access to current hosts and controls for managing hosts.</li> </ul> <p>This page includes detailed information about all hosts, including FQDN, host IP, network pool, configuration status, host state, cluster, and storage type. It also displays CPU and memory utilization for each host, and collectively across all hosts.</p>
Lifecycle Management	<p>Lifecycle Management includes the following sections:</p> <ul style="list-style-type: none"> <li>■ <b>Release Versions</b> displays the versions in your environment and the associated component versions in that release.</li> <li>■ <b>Bundle Management</b> displays the available install, update, and upgrade bundles for your environment, and your bundle download history.</li> </ul> <hr/> <p><b>Note</b> To access bundles, you must be logged in to your My VMware account through the <b>Administration &gt; Repository Settings</b> page.</p> <hr/> <ul style="list-style-type: none"> <li>■ <b>Image Management</b> enables you to import a vSphere Lifecycle Manager cluster image from vCenter Server and view the available images. This is an alternative way of managing the life cycle of ESXi hosts.</li> </ul>

Category	Functional Areas
Administration	<p>Administration includes the following sections:</p> <ul style="list-style-type: none"> <li>■ <b>Network Settings</b> enables you to configure, view, and manage network pool settings. You can create new network pools, and view and modify existing network pools.</li> <li>■ <b>Storage Settings</b> enables you to add new VASA providers, view, edit, and delete existing VASA providers.</li> <li>■ <b>Licensing</b> enables you to manage VMware product licenses. You can also add licenses for the component products in your VMware Cloud Foundation deployment.</li> <li>■ <b>Users</b> enables you to manage VMware Cloud Foundation users and groups, including adding users and groups and assigning roles.</li> <li>■ <b>Repository Settings</b> enables you to log in to your My VMware account.</li> <li>■ <b>Composable Infrastructure</b> enables you to configure composable servers to meet the needs of your workloads without physically moving any hardware components.</li> <li>■ <b>vRealize Suite</b> enables you to deploy vRealize Suite Lifecycle Manager.</li> <li>■ <b>Security</b> enables you to integrate with your Microsoft Certificate Authority Server and perform password management actions, such as rotation, updates and remediation.</li> <li>■ <b>Backup</b> enables you to register an external SFTP server with SDDC Manager for backing up SDDC Manager and NSX Managers. You can also configure the backup schedule for SDDC Manager.</li> <li>■ <b>VMware CEIP</b> to join or leave the VMware Customer Experience Improvement Program.</li> </ul>
Developer Center	<p>The VMware Cloud Foundation Developer Center includes the following sections:</p> <ul style="list-style-type: none"> <li>■ <b>Overview:</b> API reference documentation. Includes information and steps for all the Public APIs supported by VMware Cloud Foundation.</li> <li>■ <b>API Explorer:</b> Lists the APIs and allows you to invoke them directly on your VMware Cloud Foundation system.</li> <li>■ <b>Code Samples:</b> Sample code to manage a VMware Cloud Foundation instance.</li> </ul>

## Log out of the SDDC Manager Dashboard

Log out of SDDC Manager when you have completed your tasks.

## Procedure

- 1 In the SDDC Manager Dashboard, open the logged-in account menu by clicking the down arrow next to the account name in the upper right corner.
- 2 Click the menu choice to log out.



# Configuring Customer Experience Improvement Program

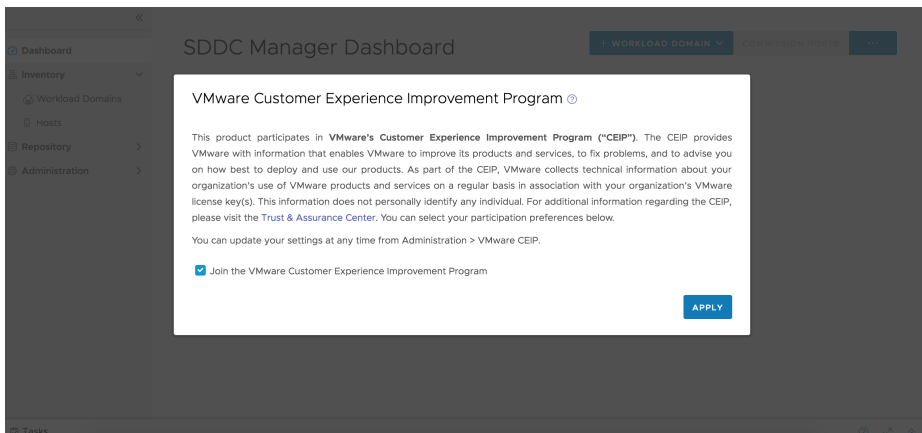
## 3

This product participates in VMware Customer Experience Improvement Program (CEIP).

The CEIP provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects the technical information about your organization's use of the VMware products and services regularly in association with your organization's VMware license keys. This information does not personally identify any individual. For additional information regarding the CEIP, refer to the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>.

You can turn CEIP on or off across all the SDDC components deployed in VMware Cloud Foundation by the following methods:

- When you log into SDDC Manager for the first time, a pop-up window appears. The **Join the VMware Customer Experience Program** option is selected by default. Deselect this option if you do not want to enable CEIP. Click **Apply**.



- You can turn CEIP on or off from the Administration tab on the SDDC Manager dashboard.

**Note** When you join CEIP, the **Enable VMware Customer Experience Improvement Program** task is shown in the floating task bar of the SDDC dashboard. Similarly, when you leave CEIP, the **Disable VMware Customer Experience Improvement Program** task is displayed. This task bar is available on all the screens of VMware Cloud Foundation.

To turn CEIP on or off from the **Administration** tab, perform the following steps:

## Procedure

- 1 On the SDDC Manager Dashboard, click **Administration > VMware CEIP**.
- 2 To turn CEIP on, select the **Join the VMware Customer Experience Improve Program** option.
- 3 To turn CEIP off, deselect the **Join the VMware Customer Experience Improve Program** option.

# Certificate Management

# 4

You can manage certificates for all external-facing VMware Cloud Foundation component resources, including configuring a certificate authority, generating and downloading CSRs, and installing them. This section provides instructions for using either the built-in OpenSSL Certificate Authority, which is part of SDDC Manager, or a Microsoft Certificate Authority.

You can manage the certificates for the following components.

- vCenter Server
- NSX Manager
- SDDC Manager
- vRealize Suite Lifecycle Manager

---

**Note** VMware Cloud Foundation does not manage certificates for ESXi hosts. By default, ESXi hosts use VMCA-signed certificates, but they can also use external CA-signed certificates. If ESXi hosts are using VMCA-signed certificates, VMCA manages the certificates and certificate rotation. If ESXi hosts are using external certificates, you are responsible for managing the certificates. For more information about external certificates, see [Configure ESXi Hosts with Signed Certificates](#).

---

You replace certificates for the following reasons:

- Certificate has expired or is close to expiring.
- Certificate has been revoked.
- You do not want to use the default VMCA certificate.
- Optionally, when you create a new workload domain.

However, it is recommended that you replace all certificates right after deploying VMware Cloud Foundation. After you create new workload domains, you can replace certificates for the appropriate components as needed.

## Procedure

### 1 [View Certificate Information](#)

You can view details of a currently active certificate for a component resource directly in the SDDC Manager Dashboard.

## 2 Configure a Microsoft Certificate Authority

Before you can generate and install certificates, you must configure a certificate authority (CA).

## 3 Install Certificates with the Microsoft Certificate Authority or OpenSSL Certificate Authority

You can generate a CSR and signed certificates and install them for selected resource components directly in the SDDC Manager Dashboard.

## 4 Install Certificates with External or Third-Party Certificate Authorities

If you intend to generate and install external or third-party certificates, you must download the certificate signing request (CSR) from the SDDC Manager Dashboard and have it manually signed by a third-party CA. You can then use the controls in the SDDC Manager Dashboard to install the certificate.

## 5 Clean Out Old or Unused Certificates

Old or unused certificates are stored in a trust store in SDDC Manager. You can delete old certificates through the SDDC Manager VM.

# View Certificate Information

You can view details of a currently active certificate for a component resource directly in the SDDC Manager Dashboard.

### Procedure

- 1 In the SDDC Manager Dashboard, click **Inventory > Workload Domains**.

The Workload Domains page displays information for all workload domains.

- 2 In the list of domains, click the name of the workload domain to open the details page for that domain.

The workload domain details page displays CPU, memory, and storage allocated to the domain.

- 3 Select the **Security Tab**.

This tab lists the certificates for each resource component associated with the workload domain. It displays the following details:

- Resource type
- Issuer, the certificate authority name
- Resource host name
- Valid from and valid to dates
- Certificate status: *Active*, *Expiring* (will expire within 15 days), or *Expired*.
- Certificate operation status.

- 4 To view certificate details, expand the resource to view the certificate details In the Resource Type column.

The expanded field displays certificate details including signature algorithm, public key, public key algorithm, certificate string, and more.

## Configure a Microsoft Certificate Authority

Before you can generate and install certificates, you must configure a certificate authority (CA).

### Prerequisites

- Verify that the Microsoft Certificate Authority Server has the correct roles installed. See [Install Microsoft Certificate Authority Roles](#).
- Verify the Microsoft Certificate Authority Server has been configured for basic authentication. See [Configure the Microsoft Certificate Authority for Basic Authentication](#).
- Verify a valid certificate template has been configured on the Microsoft Certificate Authority. See [Create and Add a Microsoft Certificate Authority Template](#).
- Verify least privileged service account has been configured on the Microsoft Certificate Authority Server and Template. See [Assign Certificate Management Privileges to the SDDC Manager Service Account](#).
- Verify that time is synchronized between the Microsoft Certificate Authority and the SDDC Manager appliance. Each system can be configured with a different timezone, but it is recommended that they receive their time from the same NTP source.

---

**Note** If the CA Web server and CA are on different machines, you must perform the steps mentioned in <https://blogs.technet.microsoft.com/askds/2009/04/22/how-to-configure-the-windows-server-2008-ca-web-enrollment-proxy/> in addition to the following steps.

---

### Procedure

- 1 Navigate to **Administration > Security > Certificate Management** to open the Configure Certificate Authority page.
- 2 Click **Edit** and complete the following configuration settings.

Option	Description
Certificate Authority	Select the CA from the drop-down menu. The default is <b>Microsoft</b> .
CA Server URL	Specify the URL for the CA address server. This address must begin with <b>https://</b> and end with <b>certsrv</b> , for example <b>https://www.mymicrosoftca.com/certsrv</b>
Username	Provide a valid user name to enable access to the address server.

Option	Description
<b>Password</b>	Provide a valid password to enable access to the address server.
<b>Template Name</b>	Enter the certsrv template name. You must create this template in Microsoft Certificate Authority.

### 3 Click **Save**.

A dialog box appears, asking you to review and confirm the CA server certificate details.

### 4 Click **Accept** to complete the configuration.

## Results

The Microsoft CA is now available for use in generating and installing a certificate.

## Add OpenSSL CA support

To generate OpenSSL Certificate Authority (CA) signed certificates for the VMware Cloud Foundation environment:

### Procedure

- 1 To configure the OpenSSL CA settings before generating the certificates, navigate to **Administration > Security > Certificate Management**.
- 2 In the Configure Certificate Authority page, select **OpenSSL** for **Certificate Authority**. Provide the required information.

Attribute	Description
Common Name	Enter the issuer name.
Organizational Unit	Use this field to differentiate between divisions within your organization with which this certificate is associated.
Organization	Specify the name under which your company is legally registered. The listed organization must be the legal registrant of the domain name in the certificate request.
Locality	Specify the city or the locality where your company is legally registered.
State	Enter the full name (do not abbreviate) of the state, province, region, or territory where your company is legally registered.
Country	Select the country where your company is legally registered.

Click **Save**.

- 3 To generate the OpenSSL CA signed certificates, navigate to **Inventory > Workload Domains > Select Domain**.

- 4 Under the **Security** tab, click **Generate Signed Certificates**.
- 5 The **Generate Signed Certificates** pop-up appears. Select **OpenSSL** as the Certificate Authority.
- 6 Click **Generate Certificates**.

## Install Certificates with the Microsoft Certificate Authority or OpenSSL Certificate Authority

You can generate a CSR and signed certificates and install them for selected resource components directly in the SDDC Manager Dashboard.

### Prerequisites

- Verify that the bring-up process is complete and successful.
- Verify that you have configured the Certificate Authority, as described in [Configure a Microsoft Certificate Authority](#).

### Procedure

- 1 In the SDDC Manager Dashboard, click **Inventory > Workload Domains**.

The Workload Domains page displays information for all workload domains.

- 2 In the list of domains, click the name of the workload domain to open the details page for that domain.

The workload domain details page displays CPU, memory, and storage allocated to the domain.

- 3 Select the **Security Tab**.

This tab lists the default certificates, among other details, for the Cloud Foundation resource components. It also provides controls for working with certificates.

---

**Note** You can view the current certificate and key information for a component by clicking the down-arrow icon next to the name.

---

- 4 Generate the CSR.
  - a Use the check boxes to select the resource components for which you want to generate the CSR.
  - b Click **Generate CSRS**.

The Generate CSRs dialog box opens.

- c Configure the following settings for the CSR.

Option	Description
<b>Algorithm</b>	Select the key type for the certificate. RSA (the default) is typically used. The key type defines the encryption algorithm for communication between the hosts.
<b>Key Size</b>	Select the key size (2048 bit, 3072 bit, or 4096 bit) from the drop-down menu.
<b>Email</b>	Optionally, enter a contact email address.
<b>Organizational Unit</b>	Use this field to differentiate between divisions within your organization with which this certificate is associated.
<b>Organization</b>	Type name under which your company is legally registered. The listed organization must be the legal registrant of the domain name in the certificate request.
<b>Locality</b>	Type the city or locality where your company is legally registered.
<b>State or Province Name</b>	Type the full name (do not abbreviate) of the state, province, region, or territory where your company is legally registered.
<b>Country</b>	Type the country name where your company is legally registered. This value must use the ISO 3166 country code.

- d Click **Generate CSR**.

The Generate CSRs dialog box closes. The Security tab displays a status of `CSR Generation is in progress`. When the CSR generation completes, the **Generate Signed Certificates** button becomes active.

## 5 Generate the signed certificates.

- a Leave all the resource components selected.
- b Click **Generate Signed Certificates**.

The Generate Signed Certificates dialog box appears, listing the selected components.

- c For the Select Certificate Authority, select the desired authority, and click **Generate Certificate**.

The Generate Signed Certificates dialog box closes. The Security tab displays a status of `Certificates Generation is in progress`. When the certificate generation completes, the **Install Certificates** button becomes active.



## 6 Click **Install Certificates**.

The Security tab displays a status of `Certificates Installation is in progress`.

---

**Note** As installation completes, the Certificates Installation Status column for each selected resource component in the list changes to `Successful` with a green check mark.

---

**Important** If you selected SDDC Manager as one of the resource components, you must manually restart SDDC Manager services to reflect the new certificate and to establish a successful connection between VMware Cloud Foundation services and other resources in the management domain.

---

## 7 Restart all services using the provided `sddcmanager_restart_services.sh` script.

To restart the service:

- a Using SSH, log in to the SDDC Manager VM with the following credentials:

User name: **vcf**

Password: use the password specified in the deployment parameter workbook.

- b Enter **su** to switch to the root user.

- c Run the following command:

```
sh /opt/vmware/vcf/operationsmanager/scripts/cli/sddcmanager_restart_services.sh
```

# Install Certificates with External or Third-Party Certificate Authorities

If you intend to generate and install external or third-party certificates, you must download the certificate signing request (CSR) from the SDDC Manager Dashboard and have it manually signed by a third-party CA. You can then use the controls in the SDDC Manager Dashboard to install the certificate.

## Prerequisites

Verify that you have configured and packaged your certificate authority configuration files in the form of a `<domain_name>.tar.gz` file. The contents of this archive must adhere to the following structure:

- The name of the top-level directory must exactly match the name of the domain as it appears in the list on the **Inventory > Workload Domains** page. For example, `MGMT`.
- The PEM-encoded root CA certificate chain file (`rootca.crt`) must reside inside this top-level directory.

The `rootca.crt` file contains a root certificate authority and can have *N* number of intermediate certificates. The file structure of the `rootca.crt` file must look like the following example:

```
-----BEGIN CERTIFICATE-----
<Intermediate1 certificate content>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate2 certificate content>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root certificate content>
-----END CERTIFICATE-----
```

In the above example, there are two intermediate certificates, `intermediate1` and `intermediate2`, and a root certificate. `intermediate1` must use the certificate issued by `intermediate2` and `intermediate2` must use the certificate issued by Root CA.

- This directory must contain one sub-directory for each component resource.

The name of each sub-directory must exactly match the resource hostname of a corresponding component as it appears in the Resource Hostname column in the **Workload Domains > Security** tab.

For example, `nsxManager.vrack.vsphere.local`, `vcenter-1.vrack.vsphere.local`, and so on.

- Each sub-directory must contain a corresponding `.crt` file, whose name must exactly match the resource as it appears in the Resource Hostname column in the **Workload Domains > Security** tab. The content of the `.crt` file must end with a newline character. All certificates including `rootca.crt` must be in UNIX file format.

For example, the `nsxManager.vrack.vsphere.local` sub-directory would contain the `nsxManager.vrack.vsphere.local.crt` file.

- Additional requirements for NSX-T certificates are listed below.
  - Server certificate (`NSXT_FQDN.crt`) must contain the `Basic Constraints` field with value `CA:FALSE`.
  - Root CA certificate chain file (`rootca.crt`), intermediate certificates, and root certificate must contain the `Basic Constraints` field with value `CA:TRUE`.
  - If the NSX-T certificate contains HTTP or HTTPS based CRL Distribution Point it must be reachable from the server.
  - The extended key usage (EKU) of the generated certificate must contain the EKU of the CSR generated.

---

**Note** All resource and hostname values can be found in the list on the **Inventory > Workload Domains > Security** tab.

---

## Procedure

- 1 In the SDDC Manager Dashboard, navigate to **Inventory > Workload Domains**.

The Workload Domains page displays information for all workload domains.

- 2 In the list of domains, click the name of the workload domain to open the details page for that domain.

The workload domain details page displays CPU, memory, and storage allocated to the domain.

- 3 Select the **Security Tab**.

This tab lists the default certificates, among other details, for the Cloud Foundation resource components. It also provides controls for working with certificates.

---

**Note** You can view the current certificate and key information for a component by clicking the down-arrow icon next to the name.

---

- 4 Generate the CSR.

- a Use the check boxes to select the resource components for which you want to generate the CSR.

- b Click **Generate CSR**.

The Generate CSRs dialog box opens.

- c Configure the following settings for the CSR.

Option	Description
<b>Algorithm</b>	Select the key type for the certificate. RSA (the default) is typically used. The key type defines the encryption algorithm for communication between the hosts.
<b>Key Size</b>	Select the key size (2048 bit, 3072 bit, or 4096 bit) from the drop-down menu.
<b>Email</b>	Optionally, enter a contact email address.
<b>Organizational Unit</b>	Use this field to differentiate between divisions within your organization with which this certificate is associated.
<b>Organization</b>	Type name under which your company is legally registered. The listed organization must be the legal registrant of the domain name in the certificate request.
<b>Locality</b>	Type the city or locality where your company is legally registered.
<b>State or Province Name</b>	Type the full name (do not abbreviate) of the state, province, region, or territory where your company is legally registered.
<b>Country</b>	Type the country name where your company is legally registered. This value must use the ISO 3166 country code.

- d Click **Generate CSR**.

The Generate CSRs dialog box closes. The Security tab displays a status of `CSR Generation is in progress`. When CSR generation is complete, the **Download CSR** button becomes active.

- 5 Click **Download CSR** to download and save the CSR files to the directory structure described in the Prerequisites section above.
- 6 External to the SDDC Manager Dashboard, complete the following tasks:
  - a Verify that the different `.csr` files have successfully generated and are allocated in the required file structure.
  - b Get the certificate requests signed.  
This will create the corresponding `.crt` files.
  - c Verify that the newly acquired `.crt` files are correctly named and allocated in the required file structure.
  - d Package the file structure as `<domain name>.tar.gz`. The `<domain name>` folder must include the `rootca.crt` file.
- 7 Click **Upload and Install**.
- 8 In the Upload and Install Certificates dialog box, click **Browse** to locate and select the newly created `<domain name>.tar.gz` file.

After you select the file, the **Upload** button becomes active.

- 9 Click **Upload**.

When upload is complete, the **Install Certificate** button becomes active.

- 10 Click **Install Certificate**.

The Security tab displays a status of `Certificates Installation is in progress`.

---

**Note** As installation completes, the Certificates Installation Status column for the affected components in the list changes to `Successful` with a green check mark.

---

**Important** If you selected SDDC Manager as one of the resource components, you must manually restart SDDC Manager services to reflect the new certificate and to establish a successful connection between VMware Cloud Foundation services and other resources in the management domain.

---

- 11 Restart all services using the provided `sddcmanager_restart_services.sh` script.

To restart the service:

- a Using SSH, log in to the SDDC Manager VM with the following credentials:

User name: **vcf**

Password: use the password specified in the deployment parameter workbook.

- b Enter **su** to switch to the root user.
- c Run the following command:

```
sh /opt/vmware/vcf/operationsmanager/scripts/cli/sddcmanager_restart_services.sh
```

## Clean Out Old or Unused Certificates

Old or unused certificates are stored in a trust store in SDDC Manager. You can delete old certificates through the SDDC Manager VM.

### Procedure

- 1 Using SSH, log in to the SDDC Manager VM with the following credentials:

Username: **vcf**

Password: use the password specified in the deployment parameter workbook.

- 2 Enter **su** to switch to the root user.
- 3 Change to the `/opt/vmware/vcf/operationsmanager/scripts/cli` directory.

```
cd /opt/vmware/vcf/operationsmanager/scripts/cli
```

- 4 From the `/opt/vmware/vcf/operationsmanager/scripts/cli` directory, use the following script and command to discover the names of the certificates in the trust store.

```
sddcmanager-ssl-util.sh -list
```

- 5 Using the name of the certificate, delete the old or unused certificate.

```
sddcmanager-ssl-util.sh -delete <certificate alias name from list>
```

- 6 (Optional) Clean out root certificates in VMware Endpoint Certificate Store from the Platform Services Controller node.

See [Explore Certificate Stores from the vSphere Client](#) in the vSphere product documentation.

# License Management

# 5

In the deployment parameter workbook that you completed before bring-up, you entered license keys for the following components:

- VMware vSphere
- VMware vSAN
- VMware NSX-T Data Center
- VMware vCenter Server

After bring-up, these license keys appear in the Licensing screen of the SDDC Manager Dashboard.

You must have adequate license units available before you create a VI workload domain, add a host to a cluster, or add a cluster to a workload domain. Add license keys as appropriate before you begin any of these tasks.

This chapter includes the following topics:

- [Add License Keys for the Software in Your VMware Cloud Foundation System](#)
- [Edit License Description](#)
- [Delete License Key](#)

## Add License Keys for the Software in Your VMware Cloud Foundation System

You can add licenses to the VMware Cloud Foundation license inventory.

### Procedure

- 1 On the SDDC Manager Dashboard, navigate to **Administration > Licensing**.
- 2 Click **+ License Key**.
- 3 Select the product key for which you are entering a license key.
- 4 Type the license key.

- 5 Type a description for the license.

A description can help in identifying the license.

- 6 Click **Add**.

#### What to do next

If you want to replace an existing license with a newly added license, you must add and assign the new license in the management UI (for example, vSphere Client or NSX Manager) of the component whose license you are replacing.

## Edit License Description

If you have multiple license keys for a product, the description can help in identifying the license. For example, you may want to use one license for high-performance workload domains and the other license for regular workload domains.

#### Procedure

- 1 On the SDDC Manager Dashboard, navigate to **Administration > Licensing**.
- 2 Hover your mouse in the license row that you want to edit.  
A set of three dots appears on the left of the product name.
- 3 Click the dots and then click **Edit Description**.
- 4 On the Edit License Key Description window, edit the description as appropriate.
- 5 Click **Save**.

## Delete License Key

Deleting a license key removes the license from the VMware Cloud Foundation license inventory. If the license has been applied to any workload domain, host, or cluster, the license is not removed from them, but it cannot be applied to new workload domains, hosts, or clusters.

#### Procedure

- 1 On the SDDC Manager Dashboard, navigate to **Administration > Licensing**.
- 2 Hover your mouse in the license row that you want to edit.  
A set of three dots appears on the left of the product name.
- 3 Click the dots and then click **Remove Key**.
- 4 On the Remove Key dialog box, click **Remove**.

#### Results

The license is removed from the VMware Cloud Foundation license inventory

# Prepare ESXi Hosts for VMware Cloud Foundation

## 6

Before you can begin the process of deploying VMware Cloud Foundation you must prepare a minimum of four ESXi hosts that will form the management domain. To create a new VI workload domain, you must prepare a minimum of three ESXi hosts.

Preparing the ESXi hosts involves installing the correct version of ESXi and performing some basic configuration tasks. VMware Cloud Foundation supports two methods for preparing these ESXi hosts, either interactively or through the use of the VMware Imaging Appliance service (VIA) which is bundled within VMware Cloud Builder. For the supported ESXi version, see the Bill of Materials (BOM) section of the *VMware Cloud Foundation Release Notes*.

- [Create a Custom ISO Image for ESXi](#)

When your environment requires a custom ISO file for ESXi, you can create one using VMware PowerCLI or vSphere Lifecycle Manager.

- [Install ESXi Interactively and Configure Hosts for VMware Cloud Foundation](#)

You can interactively install ESXi on all the hosts that will form the first cluster in the management domain, then you configure the management network, DNS, NTP, and SSH services. You can use the same process to add more hosts to the management domain later, or to install and configure hosts for VI workload domains.

- [Install ESXi Using the VMware Imaging Appliance](#)

You can use the VMware Imaging Appliance service (VIA) included with the VMware Cloud Builder appliance to image servers for use in the management domain and VI workload domains. For the supported ESXi version, see the BOM section of the *VMware Cloud Foundation Release Notes*.

- [Regenerate the Self-Signed Certificate on All Hosts](#)

Once you have configured the ESXi hosts' identity by providing a hostname you must regenerate the self-signed certificate to ensure the correct common name is defined.

- [Configure ESXi Hosts with Signed Certificates](#)

If corporate policy requires that you use external CA-signed certificates instead of VMCA-signed certificates for ESXi hosts, you can manually add external certificates to the hosts.



## Create a Custom ISO Image for ESXi

When your environment requires a custom ISO file for ESXi, you can create one using VMware PowerCLI or vSphere Lifecycle Manager.

You might need to create a custom ISO image for ESXi in the following situations:

- The ESXi version specified in the VMware Cloud Foundation BOM does not have an associated ISO file on VMware Customer Connect. This can be the case for ESXi patch releases.
- You need an async patch version of ESXi.
- You need a vendor-specific (OEM) ISO file.

### Prerequisites

Download the zip files for the following:

- ESXi patch for the ESXi version specified in the VMware Cloud Foundation BOM or in the list of supported sync patches in [KB 88287](#). You can download patches from <https://customerconnect.vmware.com/patch#search>.
- OEM add-on for ESXi from VMware Customer Connect. If the ESXi version specified in the BOM is not available in the **Select Version** drop-down menu, contact your vendor to determine which OEM add-on version to use.

## Create a Custom ESXi ISO Image Using VMware PowerCLI

You can use VMware Power CLI to create a custom ISO.

### Prerequisites

VMware PowerCLI 12.0 or later.

### Procedure

- 1 Gather the required information for the software spec that is used to create the custom ISO.
  - a In VMware PowerCLI, use the `Get-DepotBaseImages` cmdlet to get the base image version from the zip file for the ESXi patch that you downloaded from the patches portal.

For example:

```
Get-DepotBaseImages "c:\temp\VMware-ESXi-7.0U1d-17551050-depot.zip"
```

- b Use the `Get-DepotAddons` cmdlet to get the add-on name and version from the zip file for the OEM add-on for ESXi that you downloaded from My VMware. (if applicable)

For example:

```
Get-DepotAddons "c:\temp\HPE-701.0.0.10.6.5.12-Jan2021-Synergy-Addon-depot.zip"
```

- 2 Create the software spec using the information you gathered in step 1.

The software spec is a JSON file that contains information about the ESXi version and vendor add-on (if applicable). For example:

```
{
  "add_on": {
    "name": "HPE-Custom-Syn-AddOn",
    "version": "701.0.0.10.6.5-12"
  },
  "base_image": {
    "version": "7.0.1-0.30.17551050"
  },
  "components": null,
  "hardware_support": null,
  "solutions": null
}
```

- 3 In VMware PowerCLI, use the `New-ISOImage` cmdlet to generate a custom ISO.

For example:

```
New-ISOImage -SoftwareSpec "c:\temp\HPE-70Uld-custom.JSON" -Depots "c:\temp\VMware-ESXi-7.0Uld-17551050-depot.zip" , "c:\temp\HPE-701.0.0.10.6.5.12-Jan2021-Synergy-Addon-depot.zip" -Destination "c:\temp\HPE-70Uld-custom.iso"
```

Provide the path to the software spec you created in step 2.

The depot(s) include the path to the zip files for the supported ESXi version and vendor add-on.

The destination include the path and file name for the custom ISO file.

For more information about the `New-ISOImage` cmdlet, see <https://code.vmware.com/docs/11794/cmdletreference/doc/New-ISOImage.html>.

## Create a Custom ESXi ISO Image Using vSphere Lifecycle Manager

If you have access to a vCenter Server 7.0 environment, you can use vSphere Lifecycle Manager to create and export a custom ISO.

### Prerequisites

Import the ESXi patch and vendor add-on (if applicable) zip files to the vSphere Lifecycle Manager depot. See [Import Updates to the vSphere Lifecycle Manager Depot](#).

### Procedure

- 1 Log in to vCenter Server using the vSphere Client.
- 2 Create a new temporary cluster, selecting the **Manage all hosts in the cluster with a single image** check box.
- 3 Select the ESXi version and vendor add-on (optional) and click **OK**.

- 4 Export the vSphere Lifecycle Manager image as an ISO.

See [Export an Image](#).

- 5 Delete the temporary cluster.

## Install ESXi Interactively and Configure Hosts for VMware Cloud Foundation

You can interactively install ESXi on all the hosts that will form the first cluster in the management domain, then you configure the management network, DNS, NTP, and SSH services. You can use the same process to add more hosts to the management domain later, or to install and configure hosts for VI workload domains.

### Prerequisites

- Download the ESXi ISO from My VMware. For the supported ESXi version, see the Bill of Materials (BOM) section of the *VMware Cloud Foundation Release Notes*. If the required version of ESXi does not have an ISO available on My VMware, you can create one. See [Create a Custom ISO Image for ESXi](#).
- Make sure that you have a host machine for SDDC access. You use this host to connect to the data center and perform configuration steps.
- Verify that you have the completed *Planning and Preparation Workbook*.
- Verify the Prerequisite Checklist sheet in the *Planning and Preparation Workbook*.

### Procedure

#### 1 [Install ESXi on VMware Cloud Foundation Hosts Using the ISO](#)

Install ESXi on all hosts in the first cluster in the management domain interactively. You can use the same process to install ESXi on additional hosts for the management domain, or on hosts for a VI workload domain.

#### 2 [Configure the Network on VMware Cloud Foundation Hosts](#)

After the initial boot, use the ESXi Direct Console User Interface (DCUI) for host network configuration and administrative access.

#### 3 [Configure the Virtual Machine Network Port Group on VMware Cloud Foundation Hosts](#)

You perform configuration of the Virtual Machine Network port group for each ESXi host by using the VMware Host Client.

#### 4 [Configure SSH and NTP on VMware Cloud Foundation Hosts](#)

Complete the initial configuration of all ESXi hosts by enabling the TSM-SSH service and configuring the NTP service to avoid time synchronization issues in the SDDC.

## Install ESXi on VMware Cloud Foundation Hosts Using the ISO

Install ESXi on all hosts in the first cluster in the management domain interactively. You can use the same process to install ESXi on additional hosts for the management domain, or on hosts for a VI workload domain.

Repeat this procedure for each host in the cluster that you want to add to a workload domain.

### Procedure

- 1 Power on the ESXi host.
- 2 Mount and boot from ESXi ISO.
- 3 On the **Welcome to the VMware ESXi Installation** screen, press Enter to start the installation.
- 4 On the **End User License Agreement (EULA)** screen, press F11 to accept the EULA.
- 5 On the **Select a Disk to Install or Upgrade** screen, select the internal disk to install ESXi on and press Enter.
- 6 On the **Please select a keyboard layout** screen, select the keyboard layout and press Enter.
- 7 On the **Enter a root password** screen enter the `esxi_root_user_password`, enter the password a second time to confirm the spelling, and press Enter.
- 8 On the **Confirm Install** screen, press F11 to start the installation.
- 9 On the **Installation Complete** screen, press Enter to reboot the host.
- 10 Repeat this procedure for all remaining hosts.

## Configure the Network on VMware Cloud Foundation Hosts

After the initial boot, use the ESXi Direct Console User Interface (DCUI) for host network configuration and administrative access.

Perform the following tasks to configure the host network settings:

- Configure the network adapter (vmk0) and VLAN ID for the Management Network.
- Configure the IP address, subnet mask, gateway, DNS server, and FQDN for the ESXi host.

Repeat this procedure for all the hosts that you are adding to the workload domain.

### Procedure

- 1 Open the DCUI of the ESXi host.
  - a Open a console window to the host.
  - b Press F2 to enter the DCUI.
  - c Log in by using the `esxi_root_user_password`.

- 2 Configure the network.
  - a Select **Configure Management Network** and press Enter.
  - b Select **VLAN (Optional)** and press Enter.
  - c Enter the VLAN ID for the Management Network and press Enter.
  - d Select **IPv4 Configuration** and press Enter.
  - e Select **Set static IPv4 address and network configuration** and press the Space bar.
  - f Enter the IPv4 Address, Subnet Mask and Default Gateway and press Enter.
  - g Select **DNS Configuration** and press Enter.
  - h Select **Use the following DNS Server address and hostname** and press the Space bar.
  - i Enter the Primary DNS Server, Alternate DNS Server and Hostname and press Enter.
  - j Select **Custom DNS Suffixes** and press Enter.
  - k Ensure that there are no suffixes listed and press Enter.
- 3 Press Escape to exit and press Y to confirm the changes.
- 4 Repeat this procedure for all remaining hosts.

## Configure the Virtual Machine Network Port Group on VMware Cloud Foundation Hosts

You perform configuration of the Virtual Machine Network port group for each ESXi host by using the VMware Host Client.

You configure the VLAN ID of the VM Network port group on the vSphere Standard Switch. This configuration provides connectivity to the Management network to allow communication to the vCenter Server Appliance during the automated deployment.

Repeat this procedure for each host that you are adding to the workload domain.

### Procedure

- 1 In a web browser, log in to the ESXi host using the VMware Host Client.
- 2 Click **OK** to join the Customer Experience Improvement Program.
- 3 Configure a VLAN for the VM Network port group.
  - a In the navigation pane, click **Networking**.
  - b Click the **Port groups** tab, select the **VM network** port group, and click **Edit Settings**.
  - c On the **Edit port group - VM network** page, enter the Management Network VLAN ID, and click **Save**.
- 4 Repeat this procedure for all remaining hosts.

## Configure SSH and NTP on VMware Cloud Foundation Hosts

Complete the initial configuration of all ESXi hosts by enabling the TSM-SSH service and configuring the NTP service to avoid time synchronization issues in the SDDC.

Repeat this procedure for all the hosts that you are adding to the workload domain.

### Procedure

- 1 In a web browser, log in to the ESXi host using the VMware Host Client.
- 2 Configure and start the TSM-SSH service.
  - a In the navigation pane, click **Manage** and click the **Services** tab.
  - b Select the **TSM-SSH** service, and click the **Actions** menu.
  - c Select **Policy** and click **Start and stop with host**.
  - d To start the service, click **Start**.
- 3 Configure and start the NTP service.
  - a In the navigation pane, click **Manage**, and click the **System** tab.
  - b Click **Time & date** and click **Edit NTP Settings**.
  - c On the **Edit NTP Settings** page, select the **Use Network Time Protocol (enable NTP client)** radio button, and change the NTP service startup policy to **Start and stop with host**.
  - d In the **NTP servers** text box, enter the NTP Server FQDN or IP Address, and click **Save**.
  - e To start the service, click **Actions**, select **NTP service**, and click **Start**.
- 4 Repeat this procedure for all remaining hosts.

## Install ESXi Using the VMware Imaging Appliance

You can use the VMware Imaging Appliance service (VIA) included with the VMware Cloud Builder appliance to image servers for use in the management domain and VI workload domains. For the supported ESXi version, see the BOM section of the *VMware Cloud Foundation Release Notes*.

You must have access to the VMware Cloud Builder appliance to use the VMware Imaging Appliance service. If you deleted the VMware Cloud Builder after bring-up, you can redeploy it as described in "Deploy Cloud Foundation Builder Appliance" in the *VMware Cloud Foundation Deployment Guide*.

The default root credentials for servers imaged with VIA are user **root**, password **EvoSddc!2016**.

### Prerequisites

The servers that you image must meet certain prerequisites:

- PXE Boot is configured as primary boot option

- Install device is configured as the second boot option
- Legacy boot mode configured in BIOS

---

**Note** Although the VMware Imaging Appliance service does not support UEFI boot mode, VMware Cloud Foundation does support it for servers configured outside of VIA.

---

- Servers are in the same L2 domain as the VMware Cloud Builder appliance
- Servers are reachable over an untagged VLAN/Network (VLAN ID 0)
- The VMware Cloud Builder appliance is deployed on an untagged VLAN/Network
- Server hardware/firmware should be configured for virtualization and vSAN and match the VMware Cloud Foundation BOM as described in the Release Notes
- Physical hardware health status should be "healthy" without any errors
- Any onboard NICs are inactive on the servers and only the two 10 GbE NICs reserved for use with VMware Cloud Foundation are active in BIOS

## Procedure

### 1 Download ESXi Software and VIBs

In order to image your servers, you need to download an ESXi ISO and any vSphere Installation Bundles (VIBs) required to get the servers to a supported version of ESXi. See the BOM section of the VMware Cloud Foundation Release Notes for information about ESXi support.

### 2 Provide Network Information for Imaging

You must provide the VMware Imaging Appliance service with certain network information specific to your environment before you can image your servers. This information is contained in the `via.properties` file on the VMware Cloud Builder appliance.

### 3 Upload ISOs and VIBs to the VMware Imaging Appliance service

After you have downloaded the required software and updated `via.properties` with your network information, you can upload ISOs and VIBs to the VMware Imaging Appliance service.

### 4 Image Servers with ESXi and VIBs

Once you have uploaded the required ESXi and VIB packages to the VMware Imaging Appliance service, you can begin imaging servers. You can image an individual server, or multiple servers at the same time.

### 5 Post-Imaging Tasks

After you image your servers with ESXi and VIBs, you must perform some post-imaging tasks, depending on whether you use an untagged or a tagged management VLAN.

## Download ESXi Software and VIBs

In order to image your servers, you need to download an ESXi ISO and any vSphere Installation Bundles (VIBs) required to get the servers to a supported version of ESXi. See the BOM section of the VMware Cloud Foundation Release Notes for information about ESXi support.

You can download the ISO and VIBs from My VMware (<https://my.vmware.com>) to any location on the Windows machine that is connected to the VMware Cloud Builder appliance. Make sure to record the MD5 or SHA-1 checksums. You will need them when you upload the ISO/VIB to the VMware Imaging Appliance service.

If the required version of ESXi does not have an ISO available on My VMware, you can create one. See [Create a Custom ISO Image for ESXi](#). In order to upload a user-created custom ISO for use with the VMware Imaging Appliance, you must provide an MD5 checksum. You can use an MD5 utility to generate a checksum for user-created custom ISOs.

## Provide Network Information for Imaging

You must provide the VMware Imaging Appliance service with certain network information specific to your environment before you can image your servers. This information is contained in the `via.properties` file on the VMware Cloud Builder appliance.

### Procedure

- 1 SSH into the VMware Cloud Builder appliance using the credentials specified when you deployed the VM. See "Deploy Cloud Foundation Builder Appliance" in the *VMware Cloud Foundation Deployment Guide*.
- 2 Type `su` to switch to the root user.
- 3 Navigate to the `/opt/vmware/evorack-imaging/config/` directory.



#### 4 Update the `via.properties` file with your network information.

- a If the VMware Cloud Builder appliance is using the `eth0` interface (default), then you do not need to modify any of the properties in Section A. If the VMware Cloud Builder appliance has multiple network interfaces and is not using `eth0`, you must update the following properties.

Property	Description
<code>via.network.interface</code>	Interface of the VMware Cloud Builder appliance configured in management network.
<code>via.web.url</code>	The IP address used to access the VMware Imaging Appliance service UI. Update this with the IP address of VMware Cloud Builder appliance in the management network.
<code>via.network.ifaceaddr</code>	Update this with the IP address of VMware Cloud Builder appliance in the management network.
<code>via.dhcp.esxi.tftpServer</code>	IP address of the server where TFTP is running. Update this with the IP address of VMware Cloud Builder appliance in the management network.
<code>via.config.remote.pxe=false</code>	Do not modify.

- b Update Section B with the network information for your environment.

Property	Description
<code>via.dhcp.netmask</code>	Netmask of the management network.
<code>via.dhcp.subnet</code>	Subnet of the management network.
<code>via.dhcp.routers</code>	Gateway IP of the management network.
<code>via.esxi.firewall.allowed.network</code>	CIDR notation for subnet IP of the management network.

#### 5 Type `systemctl restart imaging.service` to restart the imaging service.

Wait for the imaging service to restart.

#### 6 Type `systemctl status imaging.service` to verify that the imaging service is running.

#### What to do next

Log in to the VMware Imaging Appliance service and upload software.

## Upload ISOs and VIBs to the VMware Imaging Appliance service

After you have downloaded the required software and updated `via.properties` with your network information, you can upload ISOs and VIBs to the VMware Imaging Appliance service.

#### Procedure

- 1 In a web browser on the Windows machine that is connected to the VMware Cloud Builder appliance, navigate to `https://Cloud_Builder_VM_IP:8445/via`.

The VMware Imaging Appliance service page displays.

- 2 Enter the admin credentials you provided when you deployed the VMware Cloud Builder appliance and click Log in.
- 3 Click **Bundle** and then click the **ESXi ISOs** tab.
- 4 Click **Browse** to locate and select the ISO.

- 5 Select the checksum type and enter the checksum.  
If you are uploading a user-created custom ISO, you can use an MD5 utility to generate a checksum to enter here.
- 6 Click **Upload ISO**.
- 7 When the uploaded ISO appears, select **Activate** to use the ISO for imaging servers.
- 8 Click the **Modify ViBs** tab.  
The steps for uploading ViBs are optional.
- 9 Click **Browse** to locate and select the ViB.

- 10 Click **Upload ViB**.
- 11 When the uploaded ViB appears, select **In use** to use the ViB for imaging servers.

#### What to do next

Use the selected ISO and ViB(s) to image servers for use with VMware Cloud Foundation.

## Image Servers with ESXi and ViBs

Once you have uploaded the required ESXi and ViB packages to the VMware Imaging Appliance service, you can begin imaging servers. You can image an individual server, or multiple servers at the same time.

You can use VIA to image servers for use in the management domain and VI workload domains. The management domain requires a minimum of four servers. See the *Planning and Preparation Workbook* for more information about requirements.

**Note** When you image servers, VIA uses the ESXi ISO that you activated and the VIB(s) that you marked as **In use**.

## Procedure

- 1 In a web browser on the Windows machine that is connected to the VMware Cloud Builder appliance, navigate to `https://Cloud_Builder_VM_IP:8445/via`.

The VMware Imaging Appliance service page displays.

- 2 Enter the admin credentials you provided when you deployed the VMware Cloud Builder appliance and click Log in.
- 3 Click Imaging.
- 4 Enter the required information.

Name

MGMT Domain

Description

Servers for the management domain

NOTE : Please ensure that the user guidelines and pre requisites are followed as per product documentation before proceeding.

ESXI SERVER

NTP Server: 10.0.0.250

Number: 4

1 IP: 10.0.0.100 MAC: 00:50:56:ad:7a:1b Host FQDN: esxi-1.vrack.vsphere.local

2 IP: 10.0.0.101 MAC: 00:50:56:ad:75:26 Host FQDN: esxi-2.vrack.vsphere.local

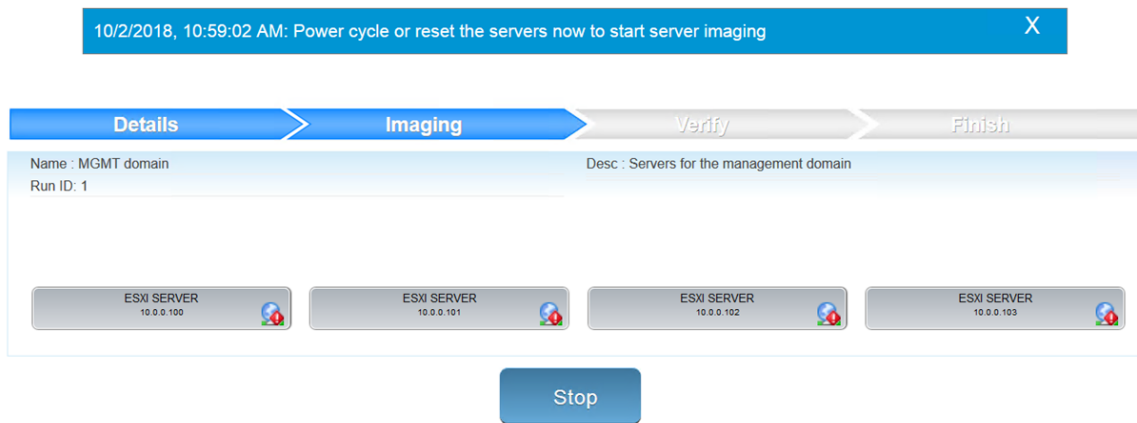
3 IP: 10.0.0.102 MAC: 00:50:56:ad:28:35 Host FQDN: esxi-3.vrack.vsphere.local

4 IP: 10.0.0.103 MAC: 00:50:56:ad:24:18 Host FQDN: esxi-4.vrack.vsphere.local

Option	Description
Name	Enter a name for the imaging job.
Description	Enter a description for the imaging job.
NTP Server	Enter the IP address for the NTP server.
Number	Enter the number of servers you want to image with the selected ISO and VIBs.
IP	Enter the IP address for the server.
MAC	Enter the MAC address for the server.
Host FQDN	Enter the FQDN for the server.

- 5 Click **Start Imaging**.

- 6 When prompted, power cycle the server(s) to continue imaging.



VIA displays information about the progress of imaging. Click a server to view details. Once imaging is complete, VIA performs verification of the servers.

- 7 When verification is finished, click **Complete**.

#### What to do next

Perform post-imaging tasks.

## Post-Imaging Tasks

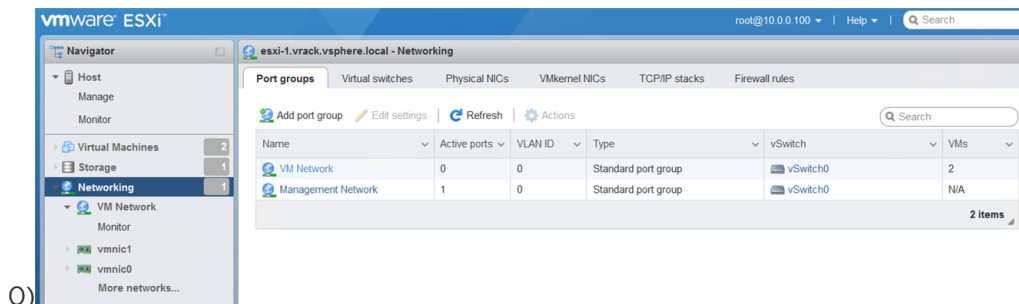
After you image your servers with ESXi and VIBs, you must perform some post-imaging tasks, depending on whether you use an untagged or a tagged management VLAN.

For imaging servers, the VMware Imaging Appliance service requires an untagged VLAN. You can continue to use an untagged VLAN for management, or you can use a tagged VLAN.

### Untagged Management VLAN

In this scenario, you use the same network for provisioning and management.

- Ensure that the Management Network and VM Network port groups on each host use the untagged VLAN (VLAN ID



- Verify that your DNS and NTP server are routable to the management network and ESXi hosts can reach them. To configure a default gateway or static routes on your ESXi hosts, see <https://kb.vmware.com/kb/2001426>.

## Tagged Management VLAN

In this scenario, you use an untagged VLAN for provisioning and a tagged VLAN for management.

- Modify the Management Network and VM Network port groups on each host to use the tagged VLAN
- Migrate the hosts from the provisioning network to the management network on the TOR switches
- Verify that your DNS and NTP server are routable to the management network and ESXi hosts can reach them. To configure a default gateway or static routes on your ESXi hosts, see <https://kb.vmware.com/kb/2001426>.

## Regenerate the Self-Signed Certificate on All Hosts

Once you have configured the ESXi hosts' identity by providing a hostname you must regenerate the self-signed certificate to ensure the correct common name is defined.

During the installation of ESXi, the installer generates a self-signed certificate for each ESXi host but the process is performed prior to the ESXi identity being configured. This means all ESXi hosts have a common name in their self-signed certificate of `localhost.localdomain`. All communication between VMware Cloud Builder and the ESXi hosts is performed securely over HTTPS and as a result it validates the identity when making a connection by comparing the common name of the certificate against the FQDN provided within the VMware Cloud Builder configuration file.

To ensure that the connection attempts and validation does not fail, you must manually regenerate the self-signed certificate after hostname has been configured.

---

**Note** VMware Cloud Foundation supports the use of signed certificates. If your organization's security policy mandates that all ESXi hosts must be configured with a CA-signed certificate, see [Configure ESXi Hosts with Signed Certificates](#).

---

### Procedure

- 1 Log in to the ESXi host using an SSH client such as Putty.
- 2 Regenerate the self-signed certificate by executing the following command:

```
/sbin/generate-certificates
```

- 3 Restart the `hostd` and `vpixd` services by executing the following command:

```
/etc/init.d/hostd restart && /etc/init.d/vpxd restart
```

- 4 Repeat this procedure for all remaining hosts.

## Configure ESXi Hosts with Signed Certificates

If corporate policy requires that you use external CA-signed certificates instead of VMCA-signed certificates for ESXi hosts, you can manually add external certificates to the hosts.

When you install ESXi software on a server to create an ESXi host, the host initially has an autogenerated certificate. By default, when the host is added to a vCenter Server system during bring-up of the management domain or other operations involving hosts (for example, host commissioning, VI workload domain creation, and so on), the autogenerated certificate is replaced with a certificate that is signed by the VMware Certificate Authority (VMCA).

When you use external certificates during bring-up, they are not replaced by VMCA-signed certificates. Once you perform bring-up with external certificates for ESXi hosts, all future hosts added to VMware Cloud Foundation must also use external certificates. You cannot use external certificates for ESXi hosts in a VI workload domain unless you used external certificates to create the management domain during bring-up.

### Prerequisites

External CA-signed certificate and key are available.

### Procedure

- 1 Log in to the ESXi Shell for the first host, either directly from the DCUI or from an SSH client, as a user with administrator privileges.
- 2 In the directory `/etc/vmware/ssl`, rename the existing certificates using the following commands:

```
mv rui.crt orig.rui.crt
```

```
mv rui.key orig.rui.key
```

- 3 Copy the external certificate and key that you want to use to `/etc/vmware/ssl`.
- 4 Rename the external certificate and key to `rui.crt` and `rui.key`.
- 5 Restart the host management agents by running the following commands:

```
/etc/init.d/hostd restart
```

```
/etc/init.d/vpxa restart
```

- 6 Repeat for all the ESXi hosts that you are adding to VMware Cloud Foundation.

# Host Management

# 7

To add hosts to the VMware Cloud Foundation inventory, you must first create a network pool or expand the default network pool created during bring-up. If you want to isolate VMkernel traffic (management, vSAN, vMotion, or overlay) across multiple physical NICs (pNICs) on the hosts, you must enable the additional pNICs before adding them to VMware Cloud Foundation.

For information on network pools, see [Network Pool Management](#). For information on enabling additional pNICs, see [Enable Additional pNICs on Hosts](#).

You then commission hosts to VMware Cloud Foundation. During the commissioning process, you associate hosts with a network pool. Commissioned hosts are added to the VMware Cloud Foundation inventory. You can add these hosts to the management domain or to a VI workload domain. When a host is added to a workload domain, an IP address from the network pool's IP inclusion range is assigned to it.

See [VMware Configuration Maximums](#) for information about the maximum number of hosts per SDDC Manager instance.

This chapter includes the following topics:

- [Network Pool Management](#)
- [Enable Additional pNICs on Hosts](#)
- [Commission Hosts](#)
- [Decommission Hosts](#)
- [View Host Inventory](#)
- [Normal Lockdown Mode](#)

## Network Pool Management

When you create a VI workload domain or add a host or vSphere cluster to a workload domain, you do not need to enter IP addresses manually. Network pools automatically assign static IP addresses to vSAN, NFS, iSCSI, and vMotion VMkernel ports.

A network pool is a collection of a set of subnets within an L2 domain. Depending on the storage option, it includes information about subnets reserved for the vMotion and vSAN, NFS, or iSCSI networks that are required for adding a host to the VMware Cloud Foundation inventory.

**Table 7-1. Information Required for a Network Pool**

Storage Being Used	Required Networks in Network Pool
vSAN	vMotion and vSAN
NFS	vMotion and NFS
vSAN and NFS	vMotion, vSAN, and NFS
VMFS on FC	vMotion only or vMotion and NFS
vVols on FC	vMotion only or vMotion and NFS
vVols on iSCSI	vMotion and iSCSI
vVols on NFS	vMotion and NFS

The network pool also contains a range of IP addresses, called an inclusion range. IP addresses from the inclusion ranges are assigned to the vMotion and vSAN, NFS, or iSCSI VMkernel ports on the host. The use of inclusion ranges allows you to limit the IP addresses that are consumed from a given subnet. You can add more inclusion ranges to expand the use of the provided subnet.

A default network pool is created during bring-up. This network pool is automatically associated with the management domain. Network information for this network pool is based on the deployment parameter workbook you provided during bring-up. This network pool contains vMotion and vSAN networks only - an NFS network is not supported in this network pool. If the vSAN and vMotion networks in your management domain are in the same L2 domain, you can expand the default network pool. You can also expand the default network pool if you expand the management domain by adding a host.

To create a workload domain with hosts in a different L2 domain than the management domain, you must create a new network pool. Also, if you want to use external NFS or VMFS on FC storage, you must create a new network pool. A network pool can contain both vSAN and NFS networks. For NSX-T workload domains, you can use the Cloud Foundation API to select hosts from different network pools, if those network pools have the same VLAN ID and MTU settings.

You can also create a workload domain with multiple vSphere clusters, each with its own network pool. You can have multiple vSphere clusters within a workload domain to provide a separate fail over domains (a VM only fails over between hosts in a cluster). Multiple vSphere clusters also provide isolation for security reasons and are also useful for grouping servers of a particular type of configuration together. Multiple vSphere clusters can also be used to handle the growth. Original servers used in the first cluster can get outdated at some point. Newer server models can then be added in a new cluster to the workload domain and workloads can be migrated at a leisurely pace.

## Size a Network Pool

Properly sizing a network pool is critical to prevent future issues in the environment due to insufficient IP addresses. Care must be taken when defining the subnets for a network pool as the subnet cannot be changed after it is deployed. The scope of IP addresses used from the defined



subnet can be limited by the definition of one or more inclusion ranges. Thus, it is recommended that you begin with defining a larger subnet than what is initially required and utilize the inclusion ranges to limit use. This will provide you the capability to grow with demand as needed.

You begin sizing a network pool by determining the number of hosts that you will have in each vSphere cluster. A workload domain must contain a minimum of one vSphere cluster, with a minimum number of three hosts. The exception to this rule is the management workload domain, which requires a minimum of four hosts. This allows for an additional level of availability for the critical infrastructure components. A vSphere cluster can be expanded to the maximum number of hosts supported by vCenter, which is currently 64 hosts.

Allocate a minimum of one IP address per host plus enough additional IP addresses to account for growth and expansion of the environment. Ensure that the subnet defined provides enough unused IP addresses and that appropriate inclusion ranges are defined. Note that some of the IP addresses within the subnet will be used for other purposes, such as defining the gateway address, firewalls, or other entities. Use care not to conflict with these addresses.

Here are some important considerations for determining the size of your network pool:

- Type of network architecture
- Physical switch details
  - Are they managed or non-managed
    - Do they support L3 (this may require a license)
    - Number of ports
- Where the network switches are placed (at the top of the rack or at the end of a row)
- Where the default gateway is created
- Number of hosts that can be placed in each rack or L2 domain
- Number of hosts required in a vSphere cluster
- Whether the network switches will be shared with non-VMware Cloud Foundation hosts
- Number of workload domains you plan on creating

## Create a Network Pool

A network pool must include the vMotion network information. Depending on the type of storage you are using, you must provide network information for vSAN, NFS, and iSCSI.

The subnet in a network pool cannot overlap the subnet of another pool.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Administration > Network Settings**.
- 2 Click **Create Network Pool**.
- 3 Enter a name for the network pool.

#### 4 Select the network type(s).

- For vSAN and NFS, you can include both vSAN and NFS network information in the same network pool or create separate network pools for vSAN and NFS.
- For VMFS on FC storage, select vMotion only or vMotion and NFS.
- For vVols on FC storage, select vMotion only or vMotion and NFS.
- For vVols on iSCSI storage, select vMotion and iSCSI.
- For vVols on NFS storage, select vMotion and NFS.

#### 5 Provide the following network information for the selected network type(s).

- a Enter a VLAN ID between 1 and 4094.
- b Enter an MTU between 1500 and 9000.
- c In the **Network** text box, enter a subnet IP address.
- d Enter the subnet mask.
- e Enter the default gateway.
- f Enter an IP address range from which an IP address can be assigned to hosts that are associated with this network pool.

The IP address range must be from within the specified subnet. You cannot include the IP address of the default gateway in the IP address range. You can enter multiple IP address ranges.

---

**Note** Ensure that you have entered the correct IP address range. IP ranges cannot be edited after the network pool is created.

---

#### 6 Click **Save**.

## View Network Pool Details

You can view vSAN and vMotion network details for a network pool as well as the total number of used and available IP addresses.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Administration > Network Settings**.
- 2 Click the arrow to the left of the pool name.

A high-level summary of the network pool's vSAN and vMotion network information is displayed.

- 3 Click the name of a network pool.

Network pool details are displayed.

## Edit a Network Pool

You can add an IP inclusion range to a network pool. No other parameters can be modified.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Administration > Network Settings**.
- 2 Click the vertical ellipsis (three dots) in the network pool row you want to edit and then click **Edit**.
- 3 Enter an IP inclusion range and click **Add**.
- 4 Click **Save**.

## Rename a Network Pool

You can rename an existing network pool.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Administration > Network Settings**.
- 2 Click the vertical ellipsis (three dots) in the network pool row you want to rename and then click **Rename Network Pool**.
- 3 Enter a new name for the network pool.
- 4 Click **Rename**.

## Delete a Network Pool

You can delete a network pool if none of the hosts with an IP address from this pool belong to a workload domain. The default pool created during bring-up cannot be deleted.

### Prerequisites

Ensure that the hosts in the network pool are not assigned to a workload domain. To verify this, navigate to **Administration > Network Settings** and confirm that the **Used IPs** for the network pool is 0.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Administration > Network Settings**.
- 2 Click the vertical ellipsis (three dots) in the network pool row that you want to delete and click **Delete**.

The Delete Network Pool dialog box appears.

- 3 Click **Delete**.

## Enable Additional pNICs on Hosts

You can isolate VMkernel traffic (management, vSAN, vMotion, or overlay) across multiple physical NICs (pNICs). Each vSphere distributed switch supports two or more pNICs, so you must define additional vSphere distributed switches and map traffic per vDS as appropriate.

Traffic isolation across physical NICs is not supported through the UI. You must enable the additional pNICs on hosts before commissioning them to VMware Cloud Foundation. You can then update the API spec to map traffic flow to reflect your physical topology. For information on using APIs, see *VMware Cloud Foundation API Reference Guide*.

---

**Note** Management and VI Workload domains can have hosts with multiple pNICs and vSphere Distributed Switches (vDS) that can scale up to the vSphere maximums supported in the vSphere version included in the VMware Cloud Foundation Bill of Materials (BOM). See the *VMware Cloud Foundation Release Notes* for the BOM.

---

## Commission Hosts

Adding hosts to the VMware Cloud Foundation inventory is called commissioning. You can add hosts individually or use a JSON template to add multiple hosts at once.

The hosts that you want to commission must meet a set of criteria. After you specify host details and select the network pool to associate a host with, VMware Cloud Foundation validates and commissions each host. Each host is added to the free pool and is available for the workload domain creation.

- Hosts that use vSAN storage can only be used with vSAN-based workload domains.
- Hosts that use NFS storage can only be used with NFS-based workload domains.
- Hosts that use VMFS on FC storage can only be used with VMFS on FC-based workload domains.
- Hosts that use vVols storage can only be used with vVols-based workload domains.

---

**Note** The management domain can only include hosts that use the vSAN storage.

---

See [VMware Configuration Maximums](#) for information about the maximum number of hosts you can commission at one time.

Ensure that a network pool supports the storage type you select for a host (vSAN, NFS, VMFS on FC, vVols).

- For vSAN and NFS, you can include both vSAN and NFS network information in the same network pool or create separate network pools for vSAN and NFS.
- For VMFS on FC storage, select vMotion only or vMotion and NFS.
- For vVols on FC storage, select vMotion only or vMotion and NFS.
- For vVols on iSCSI storage, select vMotion and iSCSI.

- For vVols on NFS storage, select vMotion and NFS.

If you used hosts with certificates generated by an external CA for bring-up, hosts used for expanding workload domains (management or VI) or for creating VI workload domains must also use certificates generated by an external CA. See [Configure ESXi Hosts with Signed Certificates](#).

### Prerequisites

Ensure that each host you are commissioning meets the following criteria:

- Hosts for vSAN-based workload domains are vSAN-compliant and certified on the VMware Hardware Compatibility Guide.
- Hosts for NFS-based workload domains are certified on the VMware Hardware Compatibility Guide.
- Hosts for VMFS on FC-based workload domains are certified on the VMware Compatibility Guide. In addition, the hosts must have supported FC cards (Host Bus Adapters) and drivers installed and configured. For compatible FC cards, see the VMware Compatibility Guide.
- Hosts for vVols-based workload domains are certified on the VMware Hardware Compatibility Guide.
  - For vVols on FC-based workload domains, ensure that all ESXi hosts have access to the FC array before launching the workflow.
  - For vVols on NFS-based workload domains, ensure that all ESXi hosts must be able to reach the NFS server from the NFS network assigned in the IP pool.
  - For vVols on iSCSI-based workload domains, ensure that the iSCSI software initiator must be enabled on each ESXi host and the VASA provider URL must be listed as the dynamic target.
- Two NIC ports with a minimum 10 Gbps speed. One port must be free, and the other port must be configured on a standard switch. This switch must be restricted to the management port group.

You can commission hosts with more than two NICs using the VMware Cloud Foundation API.

- Host has the drivers and firmware versions specified in the VMware Hardware Compatibility Guide.
- A supported version of ESXi is installed on the host. See the *VMware Cloud Foundation Release Notes* for information about supported versions.
- SSH and syslog are enabled.
- DNS is configured for forward and reverse lookup and FQDN.
- Host name must be same as the FQDN.
- Management IP address is configured on the first NIC port.
- Host has a standard switch and configured with 10 GB speed default uplinks starting with vmnic0 and increasing sequentially.

- Hardware health status is healthy without any errors.
- All disk partitions on HDD and SSD are deleted.
- Network pool must be created and available before host commissioning.
- Hosts for the vSAN-based workload domain must be associated with the vSAN enabled network pool.
- Hosts for the NFS-based workload domain are associated with the NFS enabled network pool.
- Host is configured with an appropriate gateway. The gateway must be part of the management subnet.

#### Procedure

- 1 On the SDDC Manager Dashboard, click **Inventory > Hosts**.
- 2 Click **Commission Hosts**.
- 3 Confirm that hosts to be commissioned meet each criterion in the checklist and select the check boxes.
- 4 Click **Proceed**.

- 5 Select whether you want to add hosts one at a time or import a JSON file to add multiple hosts at once.

Option	Description
<b>Add new</b>	<p>Manually enter the following information for the host you want to add:</p> <ul style="list-style-type: none"> <li>■ FQDN</li> </ul> <p>The FQDN must match the host name (including capitalization) provided during DNS configuration.</p> <ul style="list-style-type: none"> <li>■ Storage type (vSAN, NFS, VMFS on FC, or vVol)</li> </ul> <p><b>Note</b> vVols storage protocol type (FC, iSCSI, or NFS) appears only when you select vVols as the storage type</p> <ul style="list-style-type: none"> <li>■ Network pool (select an existing network pool from the list)</li> <li>■ User name and password (root credentials)</li> </ul> <p>Host Addition and Validation ⓘ</p> <hr/> <p>▼ Add Hosts</p> <p>You can either choose to add host one at a time or download <a href="#">JSON</a> template and perform bulk commission.</p> <p><input checked="" type="radio"/> Add new <input type="radio"/> Import</p> <p>Host FQDN <input type="text" value="esxi-5.vrack.vsphere.local"/></p> <p>Storage Type <input type="radio"/> vSAN <input type="radio"/> NFS <input type="radio"/> VMFS on FC <input checked="" type="radio"/> vVol</p> <p>vVol Storage Protocol Type <input type="text" value="iSCSI"/> ⓘ</p> <p>Network Pool Name ⓘ <input type="text" value="vvol-iscsi-np"/></p> <p>User Name <input type="text" value="root"/></p> <p>Password <input type="password" value="*****"/> ⓘ</p> <p><b>ADD</b></p>

Click **Add**.

You can now add more hosts or proceed to the next step.

#### Import


- To download the JSON template, click the link.
- Open the JSON template file and enter information about the hosts to add.
  - FQDN
  - User name and password (root credentials)
  - Storage type (vSAN, NFS, FC, or VVol)
  - Network pool name

**Note** vVols storage protocol type (FC, iSCSI, or NFS) appears only when you select vVols as the storage type

Option	Description
	 <pre> 1 { 2   "hostsSpec": 3   { 4     "hostfqdn": "esxi-1.vrack.vsphere.local", 5     "username": "root", 6     "storageType": "VVOL", 7     "password": "EvoSddc!2016", 8     "networkPoolName": "vvol-iscsi-np", 9     "vVolStorageProtocolType": "ISCSI" 10  }, 11  { 12    "hostfqdn": "esxi-2.vrack.vsphere.local", 13    "username": "root", 14    "storageType": "VVOL", 15    "password": "EvoSddc!2016", 16    "networkPoolName": "vvol-iscsi-np", 17    "vVolStorageProtocolType": "ISCSI" 18  } 19  ] 20 }</pre>

- c To locate and select the JSON file containing host information, click **Browse**.
- d Click **Upload**.

The host or hosts appear in the **Hosts Added** section.

- 6 Verify that the server fingerprint is correct for each host and then click the confirm fingerprint icon .
- 7 Click **Validate All**.

VMware Cloud Foundation validates the host information you provided. Each host is marked as **Valid** or **Invalid**.

For invalid hosts, you can correct the problem and validate again, or select the host and click **Remove** to proceed with commissioning the valid hosts.

- 8 Click **Next** to review the host information and then click **Commission** to begin commissioning.

The Hosts page appears, and the status of the commission task is displayed. To display the task bar, click **View Status in Task**.

**Note** Multiple VMKs are created to test the vMotion network, which may cause changes in the MAC addresses and IP address relations. If MAC address filtering is enabled on your physical infrastructure, this may cause issues such as vMotion network connectivity validation failure.

## Results

The commissioned hosts are added to the host table. The host belongs to a free pool until you assign it to a workload domain.



## Decommission Hosts

Removing hosts from the VMware Cloud Foundation inventory is called decommissioning. If you want to re-use a host in a different workload domain, you must decommission the host and re-image it up before adding it to the workload domain.

See [VMware Configuration Maximums](#) for information about the maximum number of hosts you can decommission at one time.

### Prerequisites

The hosts that you want to decommission must not be assigned to a workload domain. If a host is assigned to a workload domain, you must remove it before you can decommission it. See [Remove a Host from a vSphere Cluster in a Workload Domain](#).

### Procedure

- 1 On the SDDC Manager Dashboard, click **Inventory > Hosts**.
- 2 Click **Unassigned Hosts**.
- 3 In the hosts table, select the host(s) you want to decommission.
- 4 Click **Decommission Selected Hosts**.
- 5 Click **Confirm**.

The Hosts page appears and the status of the decommission task is displayed. Click **View Status in Task** to display the task bar.

### What to do next

Re-image the decommissioned host before adding it to a workload domain.

## View Host Inventory

The Hosts page displays details about all the hosts in your VMware Cloud Foundation system, including CPU utilization and memory usage across all hosts, as well as the total number of hosts used and unallocated.

For each host, the Hosts page displays the following information:

- FQDN name
- IP address
- The network pool to which the host belongs
- Current status
- Host state, or the workload domain to which it is allocated
- Cluster or more specifically, the domain cluster to which it is assigned
- Host-specific CPU and memory usage

- Storage type

The Hosts page also provides controls for commissioning hosts.

#### Procedure

- 1 From the SDDC Manager Dashboard, navigate to **Inventory > Hosts**.

The Hosts page appears.

- 2 Navigate directly to pages related to a specific host.

For example:

- To jump to the details page for the domain to which a listed host belongs, click the domain name link in the Host State column. For information about viewing workload domains, see [View Workload Domain Details](#).
- To jump to the details page for the domain cluster to which a listed host belongs, click the cluster name in the Cluster column. For information about clusters, see [Expand a Workload Domain](#).
- To quickly view network assignment details for a specific host, click the info icon next to the value in the Network Pool column.

- 3 To view the details of a specific host, click the FQDN name in the list.

The host details page appears, displaying the following information:

- A chart showing total and used CPU capacity.
- A chart showing total and used memory capacity.
- A summary of the networks (vSAN, vMotion, and Management) to which the host belongs and its IP address on those networks.
- The manufacturer and model of the host.
- Storage information including capacity and cache tiers.

---

**Note** Below the page title, the host details page also provides quick links to the network pool and the workload domain cluster to which the host belongs.

---

- 4 (Optional) To decommission the host from the host details page, click **Actions** near the page name and select **Decommission**.

For details, see [Decommission Hosts](#).

- 5 (Optional) To view host VM details, click **Actions** near the page name and select **Open in ESXi Client**.

The ESXi Client opens.

## Normal Lockdown Mode

You can activate or deactivate normal lockdown mode in VMware Cloud Foundation to increase the security of your hosts.

To activate or deactivate normal lockdown mode in VMware Cloud Foundation, you must perform operations through the vCenter Server. For information on how to activate or deactivate normal lockdown mode, see "Lockdown Mode" in *vSphere Security* at <https://docs.vmware.com/en/VMware-vSphere/index.html>.

You can enable normal lockdown mode on a host after the host is added to workload domain. VMware Cloud Foundation creates service accounts that can be used to access the hosts. Service accounts are added to the Exception Users list during the bring-up or host commissioning. You can rotate the passwords for the service accounts using the password management functionality in the the SDDC Manager Dashboard. See [Chapter 22 Password Management](#).

# vSphere Lifecycle Manager Image Management



A vSphere Lifecycle Manager image represents a desired software specification to be applied to all ESXi hosts in a vSphere cluster. When you set up a vSphere Lifecycle Manager image, you define the full software stack that you want to run on the ESXi hosts in a vSphere cluster: the ESXi version, additional VMware software, and vendor and third-party software such as firmware and drivers. Using a single image to manage all ESXi hosts in a vSphere cluster ensures cluster-wide host image homogeneity.

vSphere Lifecycle Manager images are made available by leveraging vSphere Lifecycle Manager, a vCenter Server service. This service is integrated with VMware Cloud Foundation and enables centralized and simplified lifecycle management of ESXi hosts. When you use vSphere Lifecycle Manager images, you follow one workflow and use the same ESXi image for all software life cycle related operations: install, upgrade, update, and patching, which significantly simplifies the life cycle management process for a VI workload domain.

For more information on vSphere Lifecycle Manager images, see [vSphere Lifecycle Manager Images](#).

## vSphere Lifecycle Manager Image Components

A vSphere Lifecycle Manager image can include four elements.

- ESXi base image

The base image contains an image of VMware ESXi Server and additional components, such as drivers and adapters that are necessary to boot a server. Base images have a user-readable name and a unique version.

- Vendor Add-On

A vendor add-on is a collection of software components that OEMs create and distribute for ESXi hosts. The vendor add-on can contain drivers, patches, and solutions.

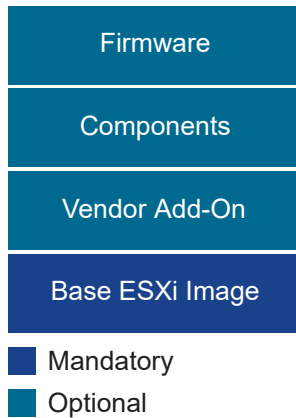
- Component

A component is the smallest discrete unit in an image, created and published by third-party software vendors.

- Firmware

Firmware refers to firmware and drivers add-on, a special type of vendor add-on designed to assist in the firmware update process. It contains firmware for a specific server type and corresponding drivers. To add a firmware and drivers add-on to your image, you must install the hardware support manager plug-in provided by the hardware vendor for the hosts in the respective cluster.

The ESXi base image is required for setting up a vSphere Lifecycle Manager image. All other elements are optional.



## vSphere Lifecycle Manager Images in VMware Cloud Foundation

vSphere Lifecycle Manager images must be created in vSphere and then imported to VMware Cloud Foundation. Unlike vSphere where images are managed per cluster, VMware Cloud Foundation allows you to manage all images in a single place and re-use them for clusters across workload domains.

You can create an image either on the management domain vCenter Server, or a vCenter Server external to VMware Cloud Foundation. Since an image is created for a cluster of hosts, you must create a cluster enabled for vSphere Lifecycle Manager images and then create an image for that cluster. While creating the image, you specify the ESXi version and can also select vendor add-ons, components, or firmware for the image.

If you created the image in a vCenter Server managed by VMware Cloud Foundation, you can extract the image from the vSphere cluster and apply it to a VI workload domain. If you created the image in an external vCenter Server, you export the image specification and component files from vSphere to your local computer. You then import these files to VMware Cloud Foundation so that you can apply the image to a VI workload domain.

After you import an image to VMware Cloud Foundation, it can be customized when it is applied to a cluster. For example, say your image included only the base ESXi image. When you use this image to create a VI workload domain, NSX-T components are added to the default cluster during the domain creation. You may also add vendor-adds, components, or firmware to the workload domain cluster. You can now extract the updated image from this cluster and reuse it for other similar clusters in this workload domain or in other workload domains.

## vSphere Lifecycle Manager Image Workflow



## vSphere Lifecycle Manager Options for Workload Domains

You have two vSphere Lifecycle Manager options for VI workload domains. You select an option while creating a workload domain. All clusters in the workload domain are managed using the selected option.

- vSphere Lifecycle Manager images automate the lifecycle management of your VMware Cloud Foundation environment including firmware by using cluster images.
- vSphere Lifecycle Manager baselines also automates the lifecycle management of your VMware Cloud Foundation environment, but firmware updates are manual.

The management domain uses vSphere Lifecycle Manager baselines.

This chapter includes the following topics:

- [Create a Cluster Image](#)
- [Making a Cluster Image Available in VMware Cloud Foundation](#)
- [View vSphere Lifecycle Manager Images](#)
- [Firmware Updates](#)

## Create a Cluster Image

Cluster images are created in vSphere 7.0. You can create an image either on the management domain vCenter Server, or a vCenter Server external to VMware Cloud Foundation.

You first create an empty cluster in vSphere and then set up an image on that cluster. During the creation of an image, you define the ESXi version and can optionally add vendor add-ons, components, and firmware.

---

**Note** The default cluster in the management domain is not vLCM-enabled, so you cannot use this for creating an image.

---

### Prerequisites

If you want to add firmware to the cluster image, you must install the Hardware Support Manager from your vendor. See [Firmware Updates](#).

### Procedure

- 1 Look up the ESXi version supported by your VMware Cloud Foundation release by referring to the BOM section in the *VMware Cloud Foundation Release Notes*.
- 2 Download the ESXi base image for this version and upload it to vSphere Client. See *VMware ESXi Installation and Setup*.
- 3 Create an empty cluster in the vCenter Server where you want to create a cluster image. You do not need to add any hosts to this cluster.
  - a In the vSphere Client, select **Actions > New Cluster**.
  - b As a best practice, name this cluster *ClusterForImage*.  
You can keep this cluster for creating additional cluster images for upgrades.
  - c Select **Manage all hosts in this cluster with a single image**.
  - d In the **Image Setup** section, select the ESXi software you uploaded in step 2. Optionally, you can also select a vendor add-on and components.
  - e If you have the vendor Hardware Support Manager installed, you can select firmware. This step is optional.
  - f Click **OK**.

The new cluster and cluster image are created.

### What to do next

Import the cluster image to VMware Cloud Foundation. See [Export a vSphere Lifecycle Manager Image](#).

## Making a Cluster Image Available in VMware Cloud Foundation

A cluster image must be made available in VMware Cloud Foundation before it can be applied to a VI workload domain or cluster. You can either import a cluster image from vSphere 7.0 or extract an image from a vLCM-enabled workload domain cluster in SDDC Manager.

## Export a vSphere Lifecycle Manager Image

If you created a vSphere Lifecycle Manager image in an external vCenter Server, you export the image from vCenter Server to your local computer.

The following files need to be exported from vCenter Server.

Format	Content
JSON	Image specification
JSON	Cluster specification
ISO	ESXi image (optional) You can use the ISO file for imaging additional hosts that you bring into VMware Cloud Foundation.
ZIP	Image components

### Prerequisites

A vSphere Lifecycle Manager image must have been created in vSphere 7.0. For more information, see [Create a Cluster Image](#).

### Procedure

- 1 Log in to the vSphere Client of the vCenter Server where you had created the vSphere Lifecycle Manager image.
- 2 Export the image specification JSON, ISO, and ZIP files from vSphere to your local computer.
  - a In the vSphere Client, click **Host and Clusters**.
  - b In the navigation pane, expand **vCenter > Datacenter** and select the vSphere Lifecycle Manager image you want to export.
  - c On the Updates tab, click **Hosts > Image**.
  - d Click the horizontal ellipsis icon and select **Export**.
  - e Click **JSON** and then click **Export**.

This downloads the image specification JSON file.

- f Repeat steps c and d for the ISO and ZIP file formats.

You can use the ISO file for imaging additional hosts that you bring into VMware Cloud Foundation. Exporting this file is optional.

---

**Note** Do not rename these files.

---

- 3 Retrieve the vSphere cluster ID using vSphere APIs.
  - a Click **Menu > Developer Center**.
  - b Click the **API Explorer** tab.



- c Ensure that **Select Endpoint** has the local vCenter Server selected and **Select API** is set to vcenter.
  - d Expand the **cluster** section.
  - e Expand **GET /api/vcenter/cluster** and click **Execute**.
  - f Under Response, expand **VcenterClusterSummary (...)** for the cluster where you created the image and copy the `cluster` value.
- 4 Retrieve the cluster JSON specification and download to the local computer using vSphere APIs.
- a In the **API Explorer** tab of the vCenter Server, ensure that **Select Endpoint** has the local vCenter Server selected and **Select API** is set to esx.
  - b Expand the **settings/clusters/software** section.
  - c Expand **GET /api/esx/settings/clusters/{cluster}/software**.
  - d In the cluster parameter area, paste the `cluster` value you had retrieved in step 3 and click **Execute**.
  - e Under Response next to EsxSettingsSoftwareInfo, click the download arrow to download the JSON specification.

## Extract a vSphere Lifecycle Manager Image

You can extract a vSphere Lifecycle Manager image from a vCenter Server managed by VMware Cloud Foundation.

### Prerequisites

A vSphere Lifecycle Manager image must have been created in vSphere 7.0. For more information, see [Create a Cluster Image](#).

### Procedure

- 1 From the navigation bar, click **Lifecycle Management > Image Management**.
- 2 Click the **Import Image** tab.
- 3 In the Option 1 section, select a workload domain.
- 4 Select the cluster from which you want to extract the vSphere Lifecycle Manager image.
- 5 Click **Extract Cluster Image**.

### Results

The extracted cluster image is displayed in the Available Images tab and can be used for a new VI workload domain or a new cluster in a VI workload domain enabled for vSphere Lifecycle Manager images.

## View vSphere Lifecycle Manager Images

You can view the cluster images available in VMware Cloud Foundation.

### Procedure

- 1 From the navigation bar, click **Lifecycle Management > Image Management**.
- 2 Click the **Available Images** tab.

All vSphere Lifecycle Manager images available in your VMware Cloud Foundation environment are displayed. You can search by image name, or filter by ESXi version or vendor.

## Firmware Updates

You can use cluster images to perform firmware updates on the ESXi hosts in a cluster. Using cluster images simplifies the host update operation. With a single operation, you update both the software and the firmware on the host.

To apply firmware updates to hosts in a cluster, you must deploy and configure a vendor provided software module called hardware support manager. The deployment method and the management of a hardware support manager is determined by the respective OEM. For example, the hardware support manager that Dell EMC provides is part of their host management solution, OpenManage Integration for VMware vCenter (OMIVV), which you deploy as an appliance.

You must deploy the hardware support manager appliance on a host with sufficient disk space. After you deploy the appliance, you must power on the appliance virtual machine, log in to the appliance as an administrator, and register the appliance as a vCenter Server extension. Each hardware support manager has its own mechanism of managing firmware packages and making firmware add-ons available for you to choose.

For detailed information about deploying, configuring, and managing hardware support managers, refer to the vendor-provided documentation.

# Storage Management

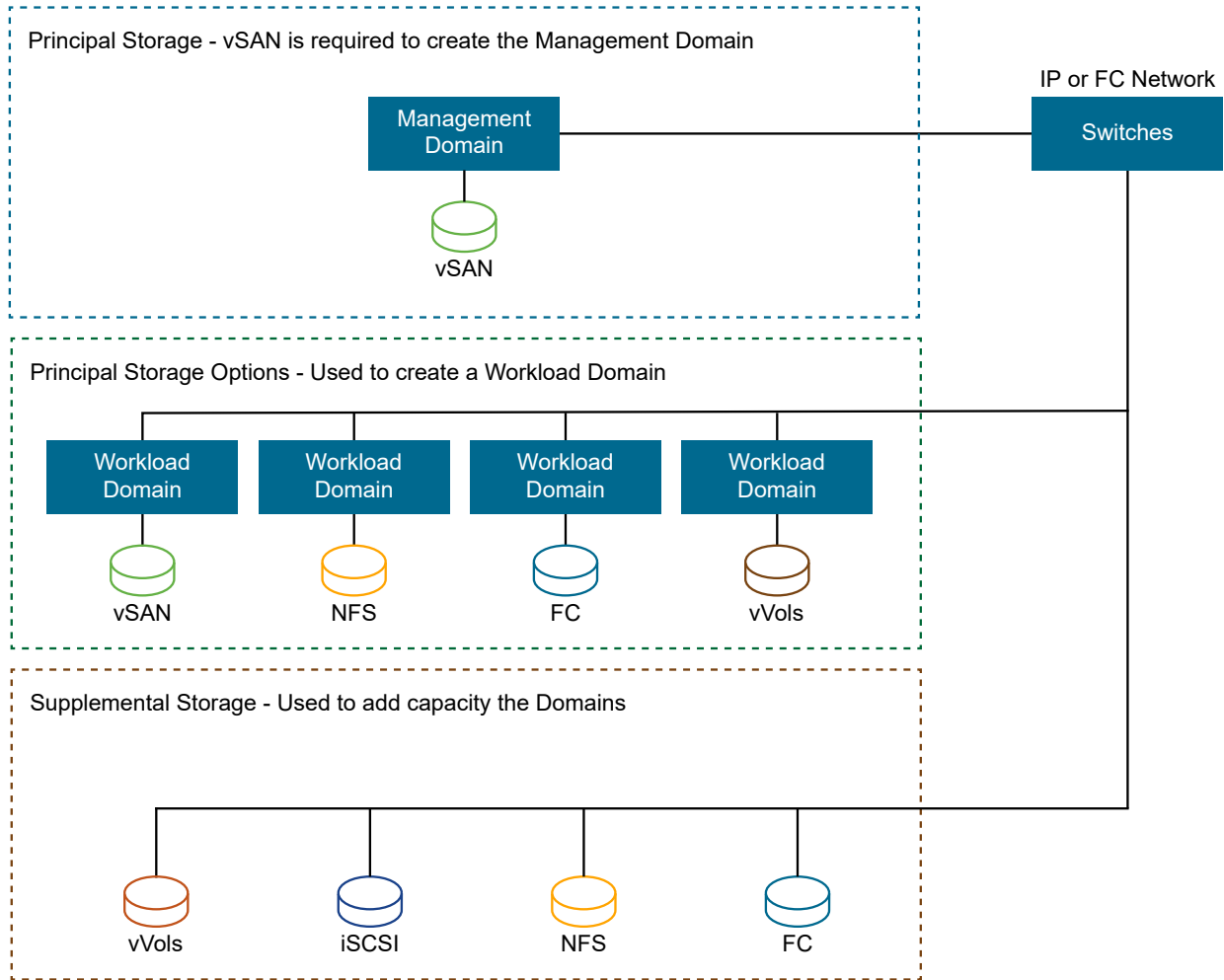
## 9

To create and manage a workload domain, VMware Cloud Foundation requires a principal storage service for all ESXi hosts within the workload domain. When a principal storage service has been provisioned and the workload domain has been created, supplemental storage can be provided to the workload domain using the vSphere Client.

VMware Cloud Foundation uses and is validated against vSAN, NFS v3, VMFS on FC, and vVols for the principal storage. The management domain requires vSAN for the principal storage. You can use vSAN, NFS v3, VMFS on FC, or vVols for the principal storage with VI workload domains. The type of principal storage used by the initial vSphere cluster in a VI workload domain is defined when the VI workload domain is created. For VI workload domains, you can add vSphere clusters that use a different type of principal storage than the type selected for the initial cluster when the VI workload domain was created. After a vSphere cluster has been deployed, you cannot change to another storage type.

Using vSAN as the principal storage for all VI workload domains uses the benefits of managing and maintaining a full software-defined stack. vSAN is also updated and patched through the SDDC Manager lifecycle management. Updating and patching non-vSAN storage is a manual task and falls outside of the SDDC Manager lifecycle management. To ensure the supportability, non-vSAN storage and HBAs must be validated against the vSphere HCL.

Supplemental storage can be added to the management domain or a VI workload domain for the purposes of workload migration, backup and archive purposes. VMware Cloud Foundation supports vVols, iSCSI, NFS (v3 or v4.1), and VMFS on FC as the supplemental storage. See [vSphere Storage](#) for information about adding these storage types.



Both the principal and supplemental storage must be listed in the VMware Compatibility Guide for vSphere Storage and validated by the storage vendor as a VMware Cloud Foundation supplemental storage solution. SDDC Manager processes do not manage or integrate the supplemental storage. VMware Cloud Foundation manages lifecycle processes automatically and without direct intervention, any storage provided to a workload domain must not modify the workload domain hosts in such a way that maintenance mode or graceful guest shutdown requests are prevented or dependent upon another separate process or action. The workload domains can be scaled up or down by adding or removing ESXi hosts, any storage provided to a workload domain must not prevent the processes used by SDDC Manager to add or remove hosts in vSphere clusters.

Storage requiring the use of VMware Installation Bundles (VIBs) is supported, provided the storage presented is vSAN, NFS, VMFS on FC, or vVols. However, VMware Cloud Foundation does not manage or maintain VIBs which must be installed or upgraded after deploying or upgrading ESXi. Work with your storage vendor to manage these VIBs.

VMware Cloud Foundation supports stretched clusters with clusters that use external (non-vSAN) storage. Contact your storage vendor for more information.

This chapter includes the following topics:

- [Sharing Remote Datastores with HCI Mesh for VI Workload Domains](#)
- [vVols Storage for VI Workload Domains](#)

## Sharing Remote Datastores with HCI Mesh for VI Workload Domains

HCI Mesh is a software-based approach for disaggregation of compute and storage resources in vSAN. HCI Mesh brings together multiple independent vSAN clusters by enabling cross-cluster utilization of remote datastore capacity within vCenter Server. HCI Mesh enables you to efficiently utilize and consume data center resources, which provides simple storage management at scale.

VMware Cloud Foundation 4.2 supports sharing remote datastores with HCI Mesh for VI workload domains.

You can create HCI Mesh by mounting remote vSAN datastores on vSAN clusters and enable data sharing from the vCenter Server. It can take up to 5 minutes for the mounted remote vSAN datastores to appear on the SDDC Manager Dashboard.

It is recommended that you do not mount or configure remote vSAN datastores for vSAN clusters in the management domain.

For more information on sharing remote datastores with HCI Mesh, see "Sharing Remote Datastores with HCI Mesh" in *Administering VMware vSAN 7.0* at <https://docs.vmware.com/en/VMware-vSphere/index.html>.

---

**Note** You cannot mount remote vSAN datastores on stretched clusters.

---

## vVols Storage for VI Workload Domains

Virtual Volumes (vVols) is a storage type for VI workload domains in VMware Cloud Foundation. vVols virtualizes SAN and NAS devices by abstracting physical hardware resources into logical pools of capacity. The vVols functionality changes the storage management paradigm from managing space inside datastores to managing abstract storage objects handled by storage arrays.

With vVols, an individual virtual machine becomes a unit of storage management. The storage hardware gains control over the virtual disk content, layout, and management.

vVols storage provides protocol endpoints that are discoverable on the physical storage fabric. ESXi hosts use the protocol endpoints to connect to virtual volumes on the storage. vVols supports NFS, iSCSI, and Fibre Channel (FC). No matter which storage protocol is used, protocol endpoints provide a uniform access to both SAN and NAS storage.

You must configure VMware APIs for Storage Awareness (VASA) provider to manage all aspects of vVols storage. VASA provider delivers information from the underlying storage container.

For more information on vVols storage, see [vSphere Storage](#).

## Add a VASA Provider

To use vVols storage in VMware Cloud Foundation, add a VASA provider .

### Prerequisites

Before you add the VASA provider details in VMware Cloud Foundation, ensure that you have set up the VASA provider. For information about setting up a VASA provider, see *Before You Enable vVols* topic in [vSphere Storage](#).

### Procedure

- 1 On the SDDC Manager Dashboard, click **Administration > Storage Settings**.
- 2 Click **Add VASA Provider**.
- 3 Enter a name for the VASA provider.
- 4 Enter a URL for the VASA provider.
- 5 Enter VASA provider user credentials.
  - VASA provider user name
  - VASA provider password
- 6 Enter VASA provider storage container details.
  - Storage container name
  - Storage container type (FC, iSCSI, or NFS)
- 7 Click **Save**.

---

**Note** You can add additional VASA user credentials and storage containers.

---

## View a VASA Provider

You can view the VASA provider details in SDDC Manager.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Administration > Storage Settings**.
- 2 In the VASA provider table, click the name of the VASA provider.

### Results

VASA provider details are displayed.

---

**Note** You can also edit the VASA provider details by clicking **Edit**.

---

## Edit a VASA Provider

You can edit the existing VASA provider details.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Administration > Storage Settings**.

- 2 Hover your mouse in the VASA provider row that you want to edit.

A set of three dots appears on the left of the VASA provider name. Click these dots and then click **Edit**.

- 3 Edit the VASA provider details.

You can also remove existing storage containers. To remove a storage container from the VASA provider, ensure that the storage container is free and not used by any workload domain or cluster.

---

**Note** You must enter the VASA provider password each time you edit the VASA provider details.

---

- 4 Click **Save**.

## Delete a VASA Provider

You can delete a VASA provider through the SDDC Manager.

### Prerequisites

Ensure that the VASA provider storage containers are free and not used by any cluster or workload domain.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Administration > Storage Settings**.

- 2 Hover the mouse on the VASA provider row that you want to delete.

A set of three dots appears on the left of the VASA provider name. Click the dots and then click **Delete**.

- 3 Confirm your choice by once again clicking **Delete**.

# Working with Workload Domains

# 10

Workload domains are logical units that carve up the compute, network, and storage resources of the VMware Cloud Foundation system. The logical units are groups of ESXi hosts managed by vCenter Server instances with specific characteristics for redundancy and VMware best practices.

The first workload domain, referred to as the management domain, is created by default during bring-up. The VMware Cloud Foundation software stack is deployed within the management domain. Additional infrastructure virtual machines which provide common services, such as backup or security appliances, can also be deployed in the management domain.

All workload domains include these VMware capabilities by default:

## **VMware vSphere® High Availability (HA)**

This feature leverages multiple ESXi hosts configured as a cluster to provide rapid recovery from outages and cost-effective high availability for applications running in virtual machines. By default, VMware Cloud Foundation provides a highly available environment for workload domains with minimal configuration. There may be additional settings (not set by default) that can increase availability of virtual machines further. For more information about vSphere HA, see the [vSphere Availability documentation](#).

## **VMware vSphere® Distributed Resource Scheduler™ (DRS)**

This feature dynamically allocates and balances computing capacity across a group of hardware resources aggregated into logical resource pools or clusters. Clusters are the primary unit of operation in VMware Cloud Foundation. DRS continuously monitors use across resource pools and allocates available resources among the virtual machines based on predefined rules that reflect business needs and changing priorities. When a virtual machine experiences an increased load, vSphere DRS automatically allocates additional resources by redistributing virtual machines among the physical servers in the resource pool. For more information about DRS, see the *vSphere Resource Management* documentation at <https://docs.vmware.com/en/VMware-vSphere/>.

## **VMware vSAN®**

This component aggregates local storage disks in a group of ESXi hosts to create a storage pool shared across all hosts in that group. For more information about vSAN, see the *VMware vSAN* documentation at <https://docs.vmware.com/en/VMware-vSAN/>.

## **VMware NSX Manager Automated Backup**



It is crucial to take backups of all NSX-T Data Center components to restore the system to its working state in the event of a failure. Until you register an external SFTP server, the NSX-T backups are taken on the SFTP server that is built into SDDC Manager. It is recommended that you register an external SFTP server soon after you upgrade or deploy VMware Cloud Foundation. See [Configure an External SFTP Server for File-Based Backups](#).

You can restore an NSX-T Data Center configuration back to the state that is captured in any of the backups.

Each VMware Cloud Foundation instance is one SSO domain to which all vCenter Servers are joined. See [VMware Configuration Maximums](#) for information about the maximum number of supported workload domains.

---

**Note** If you use cross vCenter vMotion between two VI workload domains with dissimilar hardware, you must enable EVC on the corresponding clusters. See [Enable EVC on an Existing Cluster](#) in the vSphere product documentation. You can enable EVC on the management domain by selecting the appropriate value in the Deploy Parameters tab of the deployment parameter workbook. For more information, see the *VMware Cloud Foundation Deployment Guide*.

---

## Procedure

### 1 Adding Virtual Machines to the Management Domain

If you deployed VMware Cloud Foundation using a consolidated architecture, you can add user VMs to the management domain. To prevent resource conflicts between the core VMware Cloud Foundation services, these additional virtual machines should be added to the resource pool created for this purpose during bring-up (Resource Pool User VM).

### 2 About VI Workload Domains

### 3 Deploying NSX-T Edge Clusters

You can deploy NSX-T Edge clusters with 2-tier routing to provide north-south routing and network services in the management domain and VI workload domains.

### 4 View Workload Domain Details

The Workload Domains page displays high level information about the workload domains in the VMware Cloud Foundation system. CPU, memory, and storage utilized by the workload domain is also displayed here.

### 5 Delete a VI Workload Domain

You can delete a VI workload domain from the SDDC Manager Dashboard.

### 6 View vSphere Cluster Details

The cluster page displays high level information about the vSphere cluster as well as the hosts that form that cluster. CPU, memory, and storage utilization are also displayed.

### 7 Rename a Cluster

You can use the vSphere Client to rename a cluster managed by VMware Cloud Foundation. The SDDC Manager UI is updated with the new name.

## 8 Shrink a Workload Domain

You can reduce the management domain or a VI workload domain by removing a host from a vSphere cluster in the workload domain or by deleting a vSphere cluster.

## 9 Expand a Workload Domain

You can expand the management domain or a VI workload domain to add resources to support additional workloads or availability.

## 10 Rename a Workload Domain

You can rename an existing workload domain.

# Adding Virtual Machines to the Management Domain

If you deployed VMware Cloud Foundation using a consolidated architecture, you can add user VMs to the management domain. To prevent resource conflicts between the core VMware Cloud Foundation services, these additional virtual machines should be added to the resource pool created for this purpose during bring-up (Resource Pool User VM).

---

**Note** You must be careful when adding virtual machines to the management domain. You do not want to consume excessive resources that would obstruct standard operations. Excess capacity consumption can cause failures of virtual machine fail overs in the event of a host failure or maintenance action.

---

You can add capacity to the management domain by adding a host(s) in order to expand the management workload domain. To expand the management domain, see [Expand a Workload Domain](#).

### Procedure

- 1 On the SDDC Manager Dashboard, navigate to **Inventory > Workload Domains**.
- 2 In the workload domains table, click the name of the management domain.
- 3 Click the **Services** tab.
- 4 Click the vCenter Server link.

This opens the vSphere Client for the management domain.

- 5 Create a VM.

See *Create a New Virtual Machine* in *vSphere Resource Management*.

---

**Note** Do not move any of the VMware Cloud Foundation management VMs into the resource pool.

---

## 6 Move the VM to the resource pool for user virtual machines.

See *Add a Virtual Machine to a Resource Pool* in *vSphere Resource Management*.

---

**Note** Do not move any of the VMware Cloud Foundation management VMs to the newly created resource pool.

---

## About VI Workload Domains

In the VI Configuration wizard, you specify the storage, name, compute, and networking details for the VI workload domain. Based on the selected storage, you provide vSAN parameters, NFS share details, VMFS on FC datastore information, or vVols storage details. You then select the hosts and licenses for the workload domain and start the creation workflow.

The workflow automatically:

- Deploys an extra vCenter Server Appliance for the new workload domain within the management domain.  
  
By using a separate vCenter Server instance per workload domain, software updates can be applied without impacting other workload domains. It also allows for each workload domain to have an additional isolation as needed.
- Connects the specified ESXi servers to this vCenter Server instance and groups them into a cluster. Each host is configured with the port groups applicable for the workload domain.
- Configures networking on each host.
- Configures vSAN, NFS, VMFS on FC, or vVols storage on the ESXi hosts.
- For the first VI workload domain, the workflow deploys a cluster of three NSX Managers in the management domain and configures a virtual IP (VIP) address for the NSX Manager cluster. The workflow also configures an anti-affinity rule between the NSX Manager VMs to prevent them from being on the same host for High Availability. Subsequent VI workload domains can share an existing NSX Manager cluster or deploy a new one. To share an NSX Manager cluster, the workload domains must use the same update method. The workload domains must both use vSphere Lifecycle Manager (vLCM) images, or they must both use vLCM baselines.
- During the bring-up with application virtual networks (AVNs), VMware Cloud Foundation creates a two-node NSX Edge cluster on the management domain for use by the vRealize Suite components. You can add additional NSX Edge clusters on the management domain. By default, workload domains do not include any NSX Edge clusters and are isolated. To provide north-south routing and network services, add one or more Edge clusters to a workload domain. See [Deploying NSX-T Edge Clusters](#).

---

**Note** Multiple Edge clusters cannot reside on the same vSphere cluster.

---

- To periodically get backed up to an SFTP server, NSX Managers deployed as part of a VI workload domain are configured. By default, these backups are written to an SFTP server built into SDDC Manager, but you can register an external SFTP server for better protection against failures. See [Configure an External SFTP Server for File-Based Backups](#). SDDC Manager uses either the built-in or external SFTP server with all currently deployed NSX Managers and when deploying additional NSX Managers.
- Licenses and integrates the deployed components with the appropriate pieces in the VMware Cloud Foundation software stack.

The result is a workload-ready SDDC environment.

---

**Note** You can only perform one workload domain operation at a time. For example, when you create a new workload domain, you cannot add a cluster to any other workload domain.

---

## Procedure

### 1 Prerequisites for a Workload Domain

This section lists pre-requisites for a VI workload domain.

### 2 Start the VI Configuration Wizard

Start the VI Configuration wizard and select the storage type for the workload domain.

### 3 Deploying a VI Workload Domain with a Remote Cluster

With Cloud Foundation Remote Clusters, you can deploy a VI workload domain that has its vSphere cluster at a remote location. You can also enable VMware Cloud Foundation with Tanzu on a cluster deployed at a remote site. The remote cluster is managed by the VMware Cloud Foundation instance at the central site. You can perform a full-stack life cycle management for the remote sites from the central the SDDC Manager Dashboard.

## Prerequisites for a Workload Domain

This section lists pre-requisites for a VI workload domain.

- If you plan to use DHCP for the Host Overlay Network TEPs, a DHCP server must be configured on the NSX-T host overlay (Host TEP) VLAN of the workload domain. When NSX-T creates Edge Tunnel End Points (TEPs) for the VI workload domain, they are assigned IP addresses from the DHCP server.

---

**Note** If you do not plan to use DHCP, you can use a static IP pool for the Host Overlay Network TEPs. The static IP pool is created or selected as part of workload domain creation.

---

- A minimum of three hosts marked with the appropriate storage must be available in your VMware Cloud Foundation inventory.
  - To create a VI workload domain with NFS storage, the hosts must be commissioned with NFS as the storage type and must be associated with an NFS network pool.
  - To create a VI workload domain with vSAN storage, the hosts must be commissioned with vSAN as the storage type and must be associated with an vSAN network pool.

- To create a VI workload domain with VMFS on FC storage, the hosts must be commissioned with VMFS on FC as the storage type and must be associated with a vMotion only or vMotion and NFS network pool.
- To create a VI workload domain with vVols on FC, the hosts must be commissioned with vVols on FC as the storage protocol type and must be associated with vMotion only or vMotion and NFS.
- To create a VI workload domain with vVols on iSCSI, the hosts must be commissioned with vVols on iSCSI as the storage protocol type and must be associated with vMotion and iSCSI.
- To create a VI workload domain with vVols on NFS, the hosts must be commissioned with vVols on NFS as the storage protocol type and must be associated with vMotion and NFS.

---

**Note** VASA provider must be added to create a VI workload domain with vVols storage.

---

For information on adding hosts to your inventory, see [Chapter 7 Host Management](#).

- There must be a free pNIC on each host to be used for the workload domain.
- To create a VI workload domain that uses vSphere Lifecycle Manager to apply cluster images to all hosts in the cluster, you must have a cluster image available. See [Chapter 8 vSphere Lifecycle Manager Image Management](#).
- If the management domain in your environment has been upgraded to a version different from the original installed version, you must download a VI workload domain install bundle for the current version before you can create a VI workload domain. See [Chapter 13 Download an Install Bundle](#).
- Decide on a name for your VI workload domain. Each VI workload domain must have a unique name. It is good practice to include the region and site information in the name because resource object names (such as host and vCenter names) are generated based on the VI workload domain name. The name can be three to 20 characters long and can contain any combination of the following:
  - Lowercase alphabetic characters
  - Uppercase alphabetic characters
  - Numbers

---

**Note** Spaces are not allowed in any of the names you specify when creating a VI workload domain.

---

- Decide on the following passwords:
  - vCenter Server root password
  - NSX-T Manager admin password

Although the individual VMware Cloud Foundation components support different password requirements, you must set passwords following a common set of requirements across all components:

- Minimum length: 12
- Maximum length: 16
- At least one lowercase letter, one uppercase letter, a number, and one of the following special characters: ! @ # \$ ^ \*
- Must NOT include:
  - A dictionary word
  - A palindrome
  - More than four monotonic character sequences
  - Three of the same consecutive characters
- Gather the information that you need for the workload domain creation workflow.

**Table 10-1. Information Required**

vCenter IP address and FQDN
Three NSX Managers IP addresses and FQDNs
NSX Manager Virtual IP (VIP) address and FQDN

- The IP addresses and Fully Qualified Domain Names (FQDNs) for the vCenter and NSX Manager instances must be resolvable by DNS.
- If you are using NFS storage for the workload domain, you need the following information:
  - Datastore name
  - Path to the NFS share
  - IP address of the NFS server

The NFS share and server must be accessible from the VMware Cloud Foundation network. You must have read/write permission to the NFS share.

- If you are using VMFS on FC storage for the workload domain, you must create the datastore on the hosts and configure zoning and mounting of associated volumes.
- You must have valid license keys for the following products:
  - NSX-T Data Center
  - vSAN (No license required for NFS or VMFS on FC)
  - vSphere

Because vSphere and vSAN licenses are per CPU, ensure that you have sufficient licenses for the ESXi hosts to be used for the workload domain. See [Chapter 5 License Management](#).

## Start the VI Configuration Wizard

Start the VI Configuration wizard and select the storage type for the workload domain.

### Procedure

- 1 On the SDDC Manager Dashboard, click **+ Workload Domain** and then click **VI Virtual Infrastructure**.
- 2 Select the storage type and click **Begin**.

## Specify Names and vSphere Lifecycle Manager Method

Provide names for the VI workload domain and organization and select whether the VI workload domain will use vSphere Lifecycle Manager (vLCM) images or baselines.

### Prerequisites

Verify that you have met the prerequisites described in [About VI Workload Domains](#).

### Procedure

- 1 Type a name for the VI workload domain, such as **sf001**. The name must contain between 3 and 20 characters.

It is good practice to include location information in the name since resource object names (such as host and vCenter names) are generated based on the VI workload domain name.

- 2 (Optional) Type a name for the organization that requested or will use the virtual infrastructure, such as **Finance**. The name must contain between 3 and 20 characters.
- 3 Choose the update method for the workload domain.

The method that you select for the workload domain cannot be changed later.

Option	Description
<b>Enable vSphere Lifecycle Manager Baselines</b>	This is the default option. This option is required for Kubernetes- Workload Management. See <a href="#">Chapter 11 Working with Workload Management</a> . If you enable vLCM baselines, you cannot use cluster images for firmware upgrades.
<b>Enable vSphere Lifecycle Manager Images</b>	Enable vLCM images to use cluster images for firmware upgrades. A cluster image represents a desired software specification to be applied to all hosts in a cluster. See <a href="#">Chapter 8 vSphere Lifecycle Manager Image Management</a> . Workload domains with vLCM images enabled do not support Kubernetes-Workload Management.

- 4 Click **Next**.

## Specify vSphere Cluster Details

Provide a name for the workload domain vSphere cluster. If you selected vSphere Lifecycle Manager, select a cluster image to apply to the hosts.

### Prerequisites

You must have a cluster image available if the workload domain is using vSphere Lifecycle Manager. See [Chapter 8 vSphere Lifecycle Manager Image Management](#).

### Procedure

- 1 Enter a vSphere cluster name.
- 2 Select a cluster image from the drop-down menu.

The option is only available for workload domains that use vSphere Lifecycle Manager.

## Specify Compute Details

Specify the details for the vCenter Server that gets deployed for the workload domain.

### Procedure

- 1 Enter an FQDN for the workload domain's vCenter Server.
- 2 Enter and confirm a vCenter Server root password.
- 3 Click **Next**.

## Specify Networking Details

Provide information about the NSX Manager cluster to use with the VI workload domain. If you already have an NSX Manager cluster for a different VI workload domain, you can reuse that NSX Manager cluster or create a new one.

Do not share an NSX Manager cluster between workload domains catering to different use cases that would require different NSX-T Edge cluster specifications and configurations.

See [VMware Configuration Maximums](#) for information about the maximum number of workload domains that can be managed by a single NSX Manager instance.

### Procedure

- 1 On the Networking page of the wizard, choose to create a new NSX Manager cluster or reuse an existing one.

For the first VI workload domain, you must create an NSX Manager cluster.



- 2 If you are reusing an existing NSX Manager cluster, select the cluster.

The networking information for the selected cluster will display and cannot be edited. Skip to step 5.

---

**Note** In order to share an NSX Manager cluster, the workload domains must use the same update method. The workload domains must both use vSphere Lifecycle Manager (vLCM) baselines or they must both use vLCM images.

---

- 3 Provide the NSX Manager cluster details:
  - NSX Manager cluster FQDN
  - FQDNs for three NSX Managers (nodes)
  - NSX Manager Admin password
- 4 If you are creating a new NSX Manager cluster, enter the VLAN ID for the NSX-T host overlay (host TEP) network.
- 5 Select the IP allocation method.

---

**Note** You can only use a static IP pool for VI workload domains with uniform L2 clusters. For L3 aware or stretch clusters, DHCP is required for Host Overlay Network TEP IP assignment.

---

Option	Description
DHCP	<p>With this option VMware Cloud Foundation uses DHCP for the Host Overlay Network TEPs.</p> <p>A DHCP server must be configured on the NSX-T host overlay (Host TEP) VLAN. When NSX creates TEPs for the VI workload domain, they are assigned IP addresses from the DHCP server.</p>
Static IP Pool	<p>With this option VMware Cloud Foundation uses a static IP pool for the Host Overlay Network TEPs. You can re-use an existing IP pool or create a new one.</p> <p>To create a new static IP Pool provide the following information:</p> <ul style="list-style-type: none"> <li>■ Pool Name</li> <li>■ Description</li> <li>■ CIDR</li> <li>■ IP Range.</li> <li>■ Gateway IP</li> </ul> <p>Make sure the IP range includes enough IP addresses for the number of hosts that will use the static IP Pool. The number of IP addresses required depends on the number of pNICs on the ESXi hosts that are used for the vSphere Distributed Switch that handles host overlay networking. For example, a host with four pNICs that uses two pNICs for host overlay traffic requires two IP addresses in the static IP pool.</p> <hr/> <p><b>Note</b> You cannot stretch a cluster that uses static IP addresses for the NSX-T Host Overlay Network TEPs.</p>

- 6 Click **Next**.

## Select the vSAN Parameters

At the Storage step of the creation wizard, specify the availability you want provisioned for the VI workload domain. This page appears only if you are using vSAN storage for this workload domain.

Based on your selections, SDDC Manager will determine:

- The minimum number of hosts that it needs to fulfill those selections
- The specific hosts in your environment that are available and appropriate to fulfill those selections
- The virtual infrastructure features and their specific configurations that are needed to fulfill those selections

**Note** You can modify the vSAN configuration in vSphere without negatively affecting the VMware Cloud Foundation configuration.

### Procedure

- 1 Specify the level of availability you want configured for this virtual environment.

The availability level determines the level of redundancy that is set for the assigned resources. For more information, see *Managing Fault Domains in Virtual SAN Clusters* in *Administering VMware Virtual SAN*.

Option	Description
0	<p>With this choice, the following vSAN parameters are used:</p> <ul style="list-style-type: none"> <li>■ Number of failures to tolerate: zero (0).</li> </ul> <p>Because vSAN requires a minimum of three hosts by default, three hosts are assigned to the virtual infrastructure.</p>
1	<p>With this choice, the following vSAN parameters are used:</p> <ul style="list-style-type: none"> <li>■ Number of failures to tolerate: one (1).</li> </ul> <p>Because vSAN requires a minimum of four hosts by default, four hosts are assigned to the virtual infrastructure. This is the default value.</p>
2	<p>With this choice, the following vSAN parameters are used:</p> <ul style="list-style-type: none"> <li>■ Number of failures to tolerate: two (2).</li> </ul> <p>Because vSAN requires a minimum of five hosts by default for this setting, five hosts are assigned to the virtual infrastructure.</p>

- 2 Click **Next**.

## Specify the VMFS on FC Datastore

If you are using VMFS on FC storage for the workload domain, you must specify the VMFS on FC datastore name.

### Procedure

- 1 On the Storage page, enter the name of the VMFS on FC datastore.
- 2 Click **Next**.

## Specify vVols Storage Details

If you use vVols storage for the workload domain, you must specify the vVols storage details.

### Procedure

- 1 Select a VASA protocol type.  
vVols supports FC, NFS, and iSCSI storage protocol types.
- 2 Select a VASA provider name.
- 3 Select a storage container.
- 4 Select a VASA user.
- 5 Enter a datastore name.
- 6 Click **Next**.

## Select Hosts

The Host Selection page displays available hosts along with hosts details. Hosts that are powered off, cannot be accessed via SSH, or have not been properly commissioned are not displayed.

- Select only healthy hosts.

To check a host's health, SSH in to the SDDC Manager VM using the **vcf** administrative user account and type the following command:

```
sudo /opt/vmware/sddc-support/sos --health-check
```

When prompted, enter the **vcf** user password. For more information, see [Chapter 19 Supportability and Serviceability \(SoS\) Utility](#)

- For optimum performance, you must select hosts that are identical in terms of memory, CPU types, and disks.

If you select unbalanced hosts, the UI displays a warning message, but you can proceed with the workload domain creation.

- You cannot select hosts that are in a dirty state. A host is in a dirty state when it has been removed from a cluster in a workload domain.

To clean a dirty host, re-image the host.

- For NSX for vSphere workload domains, all hosts in a cluster must be associated with the same network pool. For NSX-T workload domains, you can use the Cloud Foundation API to select hosts from different network pools, as long as those network pools have the same VLAN ID and MTU settings.

## Procedure

- 1 Select the hosts for creating the VI workload domain.

For a vSAN VI workload domain with 0 or 1 availability, a minimum of three hosts is required. For a VI workload domain with 2 availability, a minimum of five hosts is required. When you select hosts with sufficient storage to form a VI cluster, the **Next** button is enabled.

You can add hosts with multiple active pNICs to the workload domain using the VMware Cloud Foundation API.

The total resources based on the selected hosts are displayed.

- 2 Click **Next**.

## Specify NFS Storage Details

If you are using NFS storage for this workload domain, you must provide the NFS share folder and IP address of the NFS server.

## Procedure

- 1 On the NFS Storage page, enter a name for the NFS datastore name.
- 2 Enter the path to the NFS share.
- 3 Enter the IP address of the NFS server.

---

**Note** When creating additional datastores for an NFS share and server, use the same datastore name. If you use a different datastore name, vCenter overwrites the datastore name provided earlier.

---

- 4 Click **Next**.

## Select Licenses

On the Licenses page select an available license for NSX-T, vSAN, and vSphere.

## Prerequisites

You must have added valid license keys for the following products:

- VMware vSAN (if using vSAN as the storage option)  
NFS does not require a license
- VMware NSX-T Data Center
- VMware vSphere

Since vSphere and vSAN licenses are per CPU, ensure that you have sufficient licenses for the ESXi hosts to be used for the workload domain.

For information on adding license keys, see [Add License Keys for the Software in Your VMware Cloud Foundation System](#).

**Procedure**

- 1 Select a license key for each of the components in the VI workload domain.
- 2 Click **Next**.

**View Object Names**

The Object Names page displays the vSphere objects that will be generated for the VI workload domain. Object names are based on the VI workload domain name.

**Procedure**

- 1 Review the syntax that will be used for the vSphere objects generated for this domain.
- 2 Click **Next**.

**Review Details and Start the Creation Workflow**

At the Review step of the wizard, review the information about the workload domain and start the creation workflow. You can also print the information or download a printable version to print later. It can take up to two hours for the domain to be created.

The Review page displays information about the resources and their configurations that are deployed when the workflow creates and deploys the virtual infrastructure for this workload domain.

The hosts that will be added to the workload domain are listed along with information such as the network pool they belong to, memory, CPU, and so on.

**Procedure**

- 1 Scroll down the page to review the information.
- 2 Click **Finish** to begin the creation process.

The Workload Domains page appears, and a notification is displayed letting you know that VI workload domain is being added. Click **View Task Status** to view the domain creation tasks and sub tasks.

If a task fails, you can fix the issue and rerun the task. If the workload domain creation fails, contact VMware Support.

---

**Note** Multiple VMKs are created to test the vMotion network, which may cause changes in the MAC addresses and IP address relations. If MAC address filtering is enabled on your physical infrastructure, this may cause issues such as vMotion network connectivity validation failure.

---

**Results**

When the VI workload domain is created, it is added to the workload domains table.

The default end-state for a workload domain includes a network fabric with the following configuration

- Two NSX-T transport zones (one for VLAN and one for overlay) for each host

- NIOC and uplink profiles
- Four segments (previously known as logical networks); one each for management, vSAN, vMotion, and host overlay (host TEP)
- Some empty vDS and port groups  
Do not edit or delete these.

#### What to do next

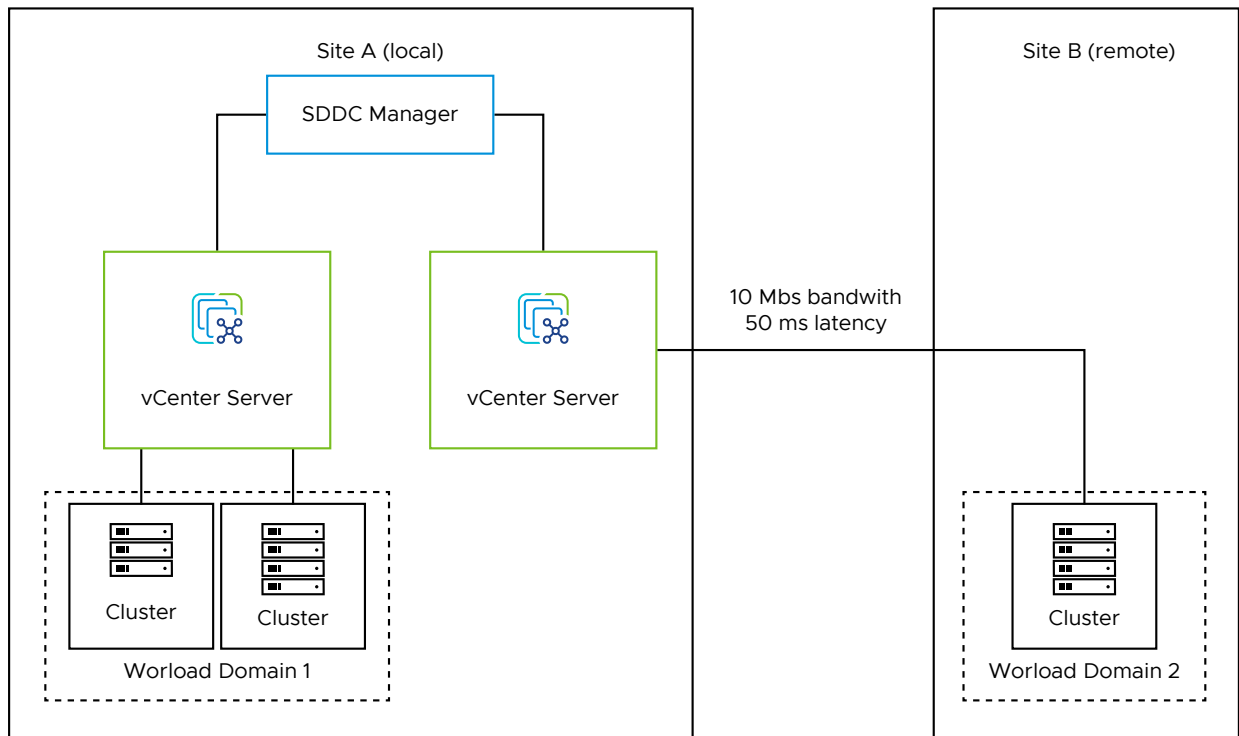
Deploy and configure an NSX-T Edge cluster. See [Deploying NSX-T Edge Clusters](#).

## Deploying a VI Workload Domain with a Remote Cluster

With Cloud Foundation Remote Clusters, you can deploy a VI workload domain that has its vSphere cluster at a remote location. You can also enable VMware Cloud Foundation with Tanzu on a cluster deployed at a remote site. The remote cluster is managed by the VMware Cloud Foundation instance at the central site. You can perform a full-stack life cycle management for the remote sites from the central the SDDC Manager Dashboard.

Cloud Foundation Remote Clusters have the following limitations:

- VMware Cloud Foundation supports a single remote cluster per VMware Cloud Foundation instance.
- A VI workload domain can include local clusters or a remote cluster, but not both.



The prerequisites for deploying a VI workload domain with a remote cluster are:

- Ensure that you meet the general prerequisites for deploying a VI workload domain. See [Prerequisites for a Workload Domain](#).
- Cloud Foundation Remote Clusters supports a minimum of 3 and maximum of 4 hosts.
- Dedicated WAN connectivity is required between central site and Cloud Foundation Remote Clusters site.
- Primary and secondary active WAN links are recommended for connectivity from the central site to the Cloud Foundation Remote Clusters site. The absence of WAN links can lead to two-failure states, WAN link failure, or NSX Edge node failure, which can result in unrecoverable VMs and application failure at the Cloud Foundation Remote Clusters site.
- Minimum bandwidth of 10 Mbps and latency of 50 Ms is required between the central VMware Cloud Foundation instance and Cloud Foundation Remote Clusters site.
- The network at the Cloud Foundation Remote Clusters site must be able to reach the management network at the central site.
- DNS and NTP server must be available locally at or reachable from the Cloud Foundation Remote Clusters site

For information on enabling VMware Cloud Foundation with Tanzu on a cluster deployed at a remote site, see [Chapter 11 Working with Workload Management](#).

## Deploying NSX-T Edge Clusters

You can deploy NSX-T Edge clusters with 2-tier routing to provide north-south routing and network services in the management domain and VI workload domains.

An NSX-T Edge cluster is a logical grouping of NSX-T Edge nodes run on a vSphere cluster. NSX-T Data Center supports a 2-tier routing model. In the top tier is the tier-0 logical router. Northbound, the tier-0 logical router connects to one or more physical routers or layer 3 switches and serves as a gateway to the physical infrastructure. Southbound, the tier-0 logical router connects to one or more tier-1 logical routers or directly to one or more logical switches. In the bottom tier is the tier-1 logical router. Northbound, the tier-1 logical router connects to a tier-0 logical router. Southbound, it connects to one or more logical switches.

During bring-up with application virtual networks (AVNs), VMware Cloud Foundation creates a two-node NSX-T Edge cluster on the management domain for use by the vRealize Suite components. You can add additional NSX-T Edge clusters on the management domain to scale out or if you need custom configured services.

By default, workload domains do not include any NSX-T Edge clusters and are isolated. Add one or more Edge clusters to a workload domain to provide routing and network services.

You can add multiple NSX-T Edge clusters to the management or workload domains for scalability and resiliency.

VMware Cloud Foundation supports creating a maximum of 16 Edge clusters per NSX Manager cluster and 8 Edge clusters per vSphere cluster for Edge clusters deployed through SDDC Manager or the VMware Cloud Foundation API. For scaling beyond these limits, you can deploy additional edge clusters through NSX-T Manager and scale up-to the NSX-T supported maximums limits.

The north-south routing and network services provided by an NSX-T Edge cluster created for a workload domain are shared with all other workload domains that use the same NSX Manager cluster.

## Create an NSX-T Edge Cluster

You can add an NSX-T Edge cluster with 2-tier routing to the management domain or a workload domain to provide north-south routing and network services.

SDDC Manager does not enforce rack failure resiliency for Edge clusters. Make sure that the number of Edge nodes that you add to an NSX-T Edge cluster, and the vSphere clusters to which you deploy the Edge nodes, enable the Edge cluster to continue to provide Edge routing services in case of rack failure.

After you create an NSX-T Edge cluster, SDDC Manager does not support expanding or shrinking it by adding or deleting Edge nodes. If you need to expand or shrink an NSX-T Edge cluster, contact VMware Support.

This procedure describes how to use SDDC Manager to create an NSX-T Edge cluster with NSX-T Edge node virtual appliances. If you have latency intensive applications in your environment, you can deploy NSX Edge nodes on bare-metal servers. See [Deployment of VMware NSX-T Edge Nodes on Bare-Metal Hardware for VMware Cloud Foundation 4.0.x](#).

### Prerequisites

- Separate VLANs and subnets are available for NSX-T Host Overlay (Host TEP) VLAN and NSX-T Edge Overlay (Edge TEP) VLAN. You cannot use DHCP for the NSX-T Edge Overlay (Edge TEP) VLAN.
- NSX-T Host Overlay (Host TEP) VLAN and NSX-T Edge Overlay (Edge TEP) VLAN are routed to each other.
- For dynamic routing, set up two Border Gateway Protocol (BGP) Peers on Top of Rack (ToR) switches with an interface IP, BGP autonomous system number (ASN), and BGP password.
- Reserve a BGP ASN to use for the NSX-T Edge cluster's Tier-0 gateway.
- DNS entries for the NSX-T Edge nodes are populated in the customer-managed DNS server.
- The vSphere cluster hosting an NSX-T Edge cluster must include hosts with identical management, uplink, host TEP, and Edge TEP networks (L2 uniform).
- You cannot deploy an Edge cluster on a vSphere cluster that is stretched. You can stretch an L2 uniform vSphere cluster that hosts an Edge cluster.



- The management network and management network gateway for the Edge nodes must be reachable.
- In Cloud Foundation 4.0, Workload Management supports one Tier-0 gateway per transport zone. When creating an Edge cluster for Workload Management, ensure that its overlay transport zone does not have other Edge clusters (with Tier-0 gateways) connected to it. Starting from Cloud Foundation 4.0.1, this limitation has been removed.

#### Procedure

- 1 On the SDDC Manager Dashboard, click **Inventory > Workload Domains**.
- 2 In the **Workload Domains** page, click a domain name in the Domain column.
- 3 Select **Actions > Add Edge Cluster**.
- 4 Verify the prerequisites, select **Select All**, and click **Begin**.
- 5 Enter information for the NSX-T Edge cluster and click **Next**.

Setting	Description
Edge Cluster Name	Enter a name for the Edge cluster.
MTU	Enter the MTU for the Edge cluster. The MTU can be 1600-9000.
ASN	Enter the BGP ASN for the Edge cluster.
Tier 0 Name	Enter a name for the tier-0 gateway.
Tier 1 name	Enter a name for the tier-1 gateway.
Edge Cluster Profile Type	Select <b>Default</b> or, if your environment requires specific Bidirectional Forwarding Detection (BFD) configuration, select <b>Custom</b> .
Edge Cluster Profile Name	Enter an NSX Edge cluster profile name. (Custom Edge cluster profile only)
BFD Allowed Hop	Enter the number of multi-hop Bidirectional Forwarding Detection (BFD) sessions allowed for the profile. (Custom Edge cluster profile only)
BFD Declare Dead Multiple	Enter the number of number of times the BFD packet is not received before the session is flagged as down. (Custom Edge cluster profile only)
BFD Probe Interval (milliseconds)	BFD is detection protocol used to identify the forwarding path failures. Enter a number to set the interval timing for BFD to detect a forwarding path failure. (Custom Edge cluster profile only)
Standby Relocation Threshold (minutes)	Enter a standby relocation threshold in minutes. (Custom Edge cluster profile only)
Edge Root Password	Enter and confirm a password.
Edge Admin Password	Enter and confirm a password.
Edge Audit Password	Enter and confirm a password.

Edge cluster passwords must meet the following requirements:

- At least 12 characters
- At least one lower-case letter

- At least one upper-case letter
- At least one digit
- At least one special character (!, @, ^, =, \*, +)
- At least five different characters
- No dictionary words
- No palindromes
- More than four monotonic character sequence is not allowed

6 Specify the use case details and click **Next**.

Setting	Description
Use Case	Select <b>Workload Management</b> to create an Edge cluster that complies with the requirements for running Workload Management. See <a href="#">Chapter 11 Working with Workload Management</a> . If you select this option, you cannot modify the Edge form factor or Tier-0 service high availability settings. Select <b>Custom</b> if you want to modify those settings.
Edge Form Factor	<p>The default setting is <b>Large</b>.</p> <ul style="list-style-type: none"> <li>■ Small: 4 GB memory, 2 vCPU, 200 GB disk space. The NSX Edge Small VM appliance size is suitable for lab and proof-of-concept deployments.</li> <li>■ Medium: 8 GB memory, 4 vCPU, 200 GB disk space. The NSX Edge Medium appliance size is suitable for production environments with load balancing.</li> <li>■ Large: 32 GB memory, 8 vCPU, 200 GB disk space. The NSX Edge Large appliance size is suitable for production environments with load balancing..</li> <li>■ XLarge: 64 GB memory, 16 vCPU, 200 GB disk space. The NSX Edge Extra Large appliance size is suitable for production environments with load balancing.</li> </ul> <p>Workload management requires <b>Large</b>.</p>
Tier-0 Service High Availability	In the active-active mode, traffic is load balanced across all members. In active-standby mode, all traffic is processed by an elected active member. If the active member fails, another member is elected to be active. Workload Management requires <b>Active-Active</b> . Some services are only supported in <b>Active-Standby</b> : NAT, load balancing, stateful firewall, and VPN. If you select <b>Active-Standby</b> , use exactly two Edge nodes in the Edge cluster.
Tier-0 Routing Type	Select <b>Static</b> or <b>EBGP</b> to determine the route distribution mechanism for the tier-0 gateway. If you select <b>Static</b> , you must manually configure the required static routes in NSX Manager. If you select <b>EBGP</b> , Cloud Foundation configures eBGP settings to allow dynamic route distribution.

7 Enter the NSX-T Edge node details for the first node and click **Add Edge Node**.

Setting	Description
Edge Node Name (FQDN)	Enter the FQDN for the Edge node. Each node must have a unique FQDN.
Management IP (CIDR)	Enter the CIDR for the management network. Each node must have a unique management IP.

Setting	Description
Management Gateway	Enter the IP address for the management network gateway.
Edge TEP 1 IP (CIDR)	Enter the CIDR for the first Edge TEP. Each node must have a unique Edge TEP 1 IP.
Edge TEP 2 IP (CIDR)	Enter the CIDR for the second Edge TEP. Each node must have a unique Edge TEP 2 IP. The Edge TEP 2 IP must be different than the Edge TEP 1 IP.
Edge TEP Gateway	Enter the IP address for the Edge TEP gateway.
Edge TEP VLAN	Enter the Edge TEP VLAN ID.
Cluster	Select a vSphere cluster to host the Edge node.
Cluster Type	<p>Select <b>L2 Uniform</b> if all hosts in the vSphere cluster have identical management, uplink, host TEP, and Edge TEP networks.</p> <p>Select <b>L2 non-uniform and L3</b> if any of the hosts in the vSphere cluster have different networks.</p> <p><b>Important</b> VMware Cloud Foundation does not support Edge cluster creation on <b>L2 non-uniform and L3</b> vSphere clusters.</p>
First Uplink VLAN	<p>Enter the VLAN ID for the first uplink.</p> <p>This is a link from the NSX-T Edge node to the first uplink network.</p>
First Uplink Interface IP (CIDR)	Enter the CIDR for the first uplink. Each node must have unique uplink interface IPs.
Peer IP (CIDR)	Enter the CIDR for the first uplink peer. (EBGP only)
ASN Peer	Enter the ASN for the first uplink peer. (EBGP only)
BGP Peer Password	Enter and confirm the BGP password. (EBGP only). A BGP password is required.
Second Uplink VLAN	<p>Enter the VLAN ID for the second uplink.</p> <p>This is a link from the NSX-T Edge node to the second uplink network.</p>
Second Uplink Interface IP(CIDR)	Enter the CIDR for the second uplink. Each node must have unique uplink interface IPs. The second uplink interface IP must be different than the first uplink interface IP.
Peer IP (CIDR)	Enter the CIDR for the second uplink peer. (EBGP only)
ASN Peer	Enter the ASN for the second uplink peer. (EBGP only)
BGP Peer Password	Enter and confirm the BGP password. (EBGP only). A BGP password is required.

- 8 Click **Add More Edge Nodes** and enter the Edge node details.

A minimum of two NSX-T Edge nodes is required. Edge cluster creation allows up to 8 Edge nodes if the Tier-0 Service High Availability is Active-Active and two Edge nodes per Edge cluster if the Tier-0 Service High Availability is Active-Standby.

- 9 When you are done adding NSX-T Edge nodes, click **Next**.

- 10 Review the summary and click Next.

SDDC Manager validates the NSX-T Edge node information.

- 11 If validation fails, use the **Back** button to edit your settings and try again.

To edit or delete any of the Edge nodes, click the three vertical dots next to an Edge node in the table and select an option from the menu.

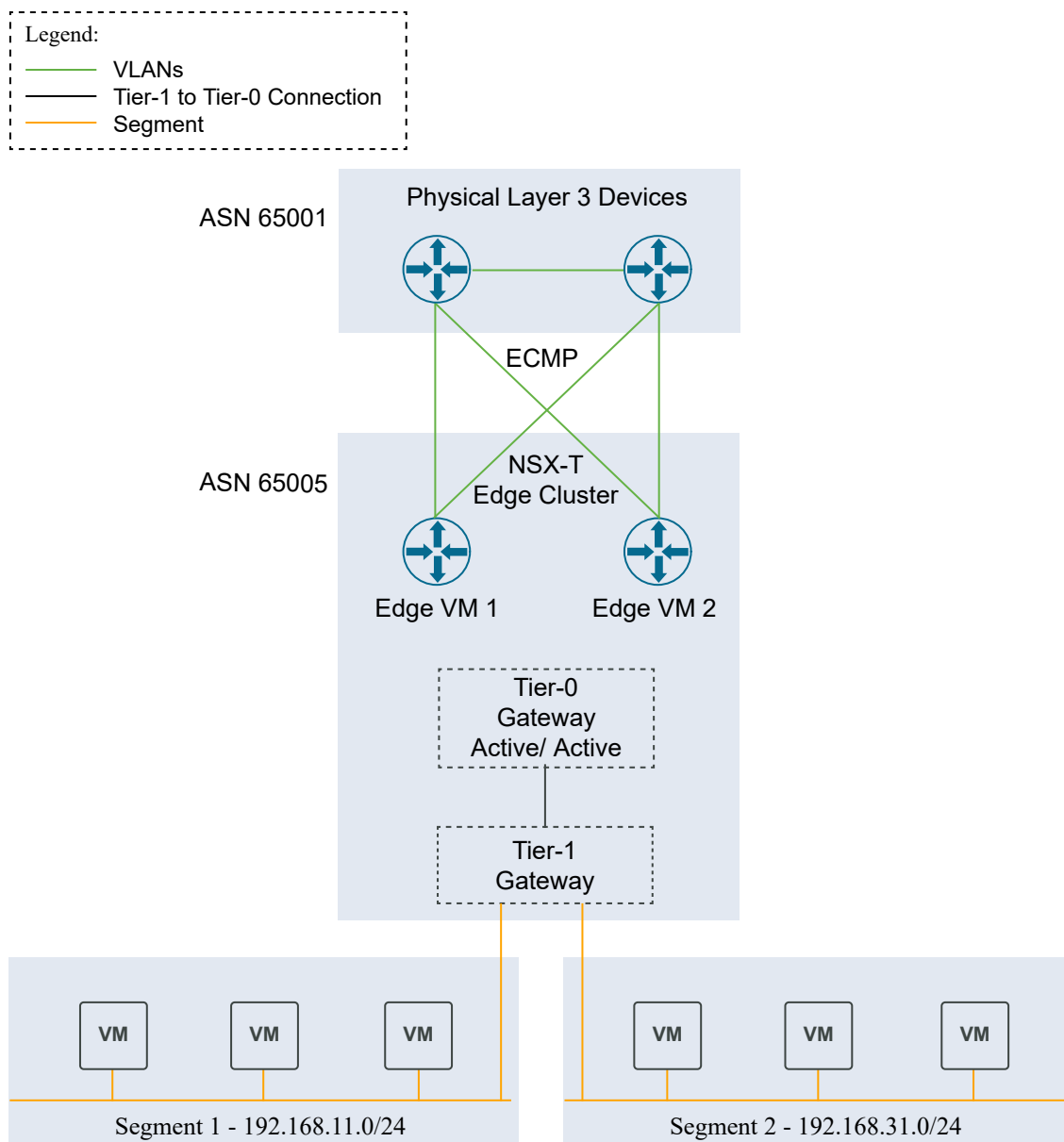
- 12 If validation succeeds, click **Finish** to create the NSX Edge cluster.

You can monitor progress in the Tasks panel.

### Example

The following example shows a scenario with sample data. You can use the example to guide you in creating NSX-T Edge clusters in your environment.

**Figure 10-1. Two-node NSX-T Edge cluster in a single rack**



### What to do next

In NSX Manager, you can create segments connected to the NSX-T Edge cluster's tier-1 gateway. You can connect workload VMs to these segments to provide north-south and east-west connectivity.

## View Workload Domain Details

The Workload Domains page displays high level information about the workload domains in the VMware Cloud Foundation system. CPU, memory, and storage utilized by the workload domain is also displayed here.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Inventory > Workload Domains**.
- 2 In the workload domains table, click the name of the workload domain.

The domain details page displays CPU, memory, and storage allocated to the domain. The tabs on the page display additional information as described in the table below.

Tab	Information Displayed
Summary	Clusters in the workload domain and availability level for each cluster.
Services	<p>SDDC software stack components deployed for the workload domain's virtual environment and their IP addresses. Click a component name to navigate to that aspect of the virtual environment. For example, click vCenter to reach the vSphere Web Client for that workload domain.</p> <p>All the capabilities of a VMware SDDC are available to you in the VI workload domain's environment, such as creating, provisioning, and deploying virtual machines, configuring the software-defined networking features, and so on.</p>
Updates/Patches	Available updates for the workload domain.
Update History	Updates applied to this workload domain.
Hosts	Names, IP addresses, status, associated clusters, and capacity utilization of the hosts in the workload domain and the network pool they are associated with.
Clusters	Names of the clusters, number of hosts in the clusters, and their capacity utilization.
Security	Default certificates for the VMware Cloud Foundation components. For more information, see <a href="#">Chapter 4 Certificate Management</a> .

### What to do next

You can add a cluster to the workload domain from this page.

## Delete a VI Workload Domain

You can delete a VI workload domain from the SDDC Manager Dashboard.

When you delete a workload domain, the clusters within that workload domain are deleted and the hosts are returned to the free pool.

Deleting a VI workload domain also removes the components associated with the workload domain from the management domain. This includes the vCenter Server instance and the NSX Manager cluster.

---

**Note** If the NSX Manager cluster is shared with any other VI workload domains, it cannot be deleted.

---

The network pools used by the workload domain are not deleted as part of the workload domain deletion process and must be deleted separately.

---

**Caution** Deleting a workload domain is an irreversible operation. All clusters and VMs within the workload domain are deleted and the underlying datastores are destroyed.

---

It can take up to 20 minutes for a workload domain to be deleted. During this process, you cannot perform any operations on workload domains.

#### Prerequisites

- If remote vSAN datastores are mounted on a cluster in the workload domain, the workload domain cannot be deleted. To delete such workload domains, you must first migrate any VMs from the remote datastore to the local datastore and then unmount the remote vSAN datastores from vCenter Server.
- Back up the data on the workload domain. The datastores on the workload domain are destroyed when the workload domain is deleted.
- Migrate the VMs that you want to keep to another workload domain.
- Delete any workload VMs created outside VMware Cloud Foundation before deleting the workload domain.
- Delete any NSX Edge clusters hosted on the workload domain. See [KB 78635](#).

#### Procedure

- 1 On the SDDC Manager Dashboard, click **Inventory > Workload Domains**.

The Workload Domains page displays information for all workload domains.

- 2 Click the vertical ellipsis (three dots) next to the workload domain you want to remove and click **Delete Domain**.

A confirmation window appears with details about the impact of deleting the workload domain, including how many hosts will be returned to the free pool.

- 3 On the Delete Workload Domain dialog box, click **Delete Workload Domain**.

The details page for the workload domain appears with a message indicating that the workload domain is being deleted. When the removal process is complete, the workload domain is removed from the domains table.

## View vSphere Cluster Details

The cluster page displays high level information about the vSphere cluster as well as the hosts that form that cluster. CPU, memory, and storage utilization are also displayed.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Inventory > Workload Domain**.
- 2 In the workload domains table, click the name of a workload domain.
- 3 Click the **Clusters** tab.
- 4 In the clusters table, click the name of a vSphere cluster.

The cluster detail page appears. The tabs on the page display additional information as described in the table below.

Tab	Information Displayed
Summary	Organization, vSAN storage parameters, and overlay networking VLAN ID.
Hosts	Details about each host in the vSphere cluster. You can click a name in the FQDN column to access the host details page.

### What to do next

You can add or remove a host, or access the vSphere Client from this page.

## Rename a Cluster

You can use the vSphere Client to rename a cluster managed by VMware Cloud Foundation. The SDDC Manager UI is updated with the new name.

### Prerequisites

Ensure that you do not rename a cluster in the following conditions:

- When the cluster belongs to a workflow that is in progress.
- When the cluster belongs to a failed VI workflow, cluster workflow or host workflow. If you try to rename a cluster that belongs to a failed workflow, restart of the failed workflow will not be supported.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Inventory > Workload Domains**.
- 2 Click a workload domain.
- 3 Under the **Clusters** tab, click a cluster you want to rename.
- 4 On the right of the cluster name, click **Actions** and then click **Open in vSphere Client**.
- 5 In the vSphere Client, click **Actions** and then click **Rename**.

- 6 Enter a new name for the cluster.
- 7 Click **OK**.

---

**Note** It takes up to two minutes for the new name to appear on the SDDC Manager UI.

---

## Shrink a Workload Domain

You can reduce the management domain or a VI workload domain by removing a host from a vSphere cluster in the workload domain or by deleting a vSphere cluster.

### Remove a Host from a vSphere Cluster in a Workload Domain

You can remove a host from a vSphere cluster in the management domain or a VI workload domain through the Workload Domains page in the SDDC Manager Dashboard.

Before you remove a host from a vSphere cluster, ensure that you have enough hosts remaining to facilitate the configured vSAN availability. Failure to do so might result in the datastore being marked as read-only or in data loss.

#### Prerequisites

- Delete any workload VMs created outside VMware Cloud Foundation or move them to another host.
- You cannot remove a host from a vSphere cluster if that vSphere cluster is hosting an Edge node.
  - Move the Edge node to another host in the same vSphere cluster. You cannot move an Edge node to a host that already hosts another Edge node.
  - If you cannot move the Edge node, delete the Edge node on the host. You cannot delete Edge nodes if doing so would result in an Edge cluster with fewer than two Edge nodes.
- You cannot remove a host from a vSphere cluster if that vSphere cluster was selected for Edge node placement and the Edge node deployment is still in pending state.

#### Procedure

- 1 On the SDDC Manager Dashboard, click **Inventory > Workload Domains**.  
The Workload Domains page displays information for all workload domains.
- 2 In the workload domains table, click the name of the workload domain that you want to modify.  
The detail page for the selected workload domain appears.
- 3 Click the **Clusters** tab.
- 4 Click the name of the cluster from which you want to remove a host.
- 5 Click the **Hosts** tab.



## 6 Select the host to remove and click **Remove Selected Hosts**.

An alert appears, asking you to confirm or cancel the action. If the removal results in the number of hosts in the cluster being less than the minimum number of required hosts, you must click **Force Remove** to remove the host.

## 7 Click **Remove** to confirm the action.

The details page for the cluster appears with a message indicating that the host is being removed. When the removal process is complete, the host is removed from the hosts table.

### Results

The host is removed from the workload domain and added to the free pool.

### What to do next

Decommission the host. See [Decommission Hosts](#). After you decommission a host, you must re-image it and commission it before you can use it again.

## Delete a vSphere Cluster from a Workload Domain

You can delete a vSphere cluster from the management domain or from a VI workload domain. Datastores on the ESXi hosts in the deleted cluster are destroyed.

You cannot delete the last cluster in a workload domain. Instead, delete the workload domain. See [Delete a VI Workload Domain](#).

### Prerequisites

- If remote vSAN datastores are mounted on the cluster, the cluster cannot be deleted. To delete such clusters, you must first migrate any VMs from the remote datastore to the local datastore and then unmount the vSAN remote datastores from vCenter Server.
- Delete any workload VMs created outside VMware Cloud Foundation before deleting the cluster.
- Migrate or backup the VMs and data on the datastore associated with the cluster to another location.
- Delete the NSX Edge clusters hosted on the vSphere cluster or shrink the NSX Edge cluster by deleting Edge nodes hosted on the vSphere cluster. You cannot delete Edge nodes if doing so would result in an Edge cluster with fewer than two Edge nodes. For information about deleting an NSX Edge cluster, see [KB 78635](#).

### Procedure

#### 1 On the SDDC Manager Dashboard, click **Inventory > Workload Domains**.

The Workload Domains page displays information for all workload domains.

#### 2 Click the name of the workload domain that contains the cluster you want to delete.

#### 3 Click the **Clusters** tab to view the clusters in the workload domain.

- 4 Hover your mouse in the cluster row you want to delete.
- 5 Click the three dots next to the cluster name and click **Delete Cluster**.
- 6 Click **Delete Cluster** to confirm that you want to delete the cluster.

The details page for the workload domain appears with a message indicating that the cluster is being deleted. When the removal process is complete, the cluster is removed from the clusters table.

## Expand a Workload Domain

You can expand the management domain or a VI workload domain to add resources to support additional workloads or availability.

To expand a domain, you can:

- Add a host from the VMware Cloud Foundation inventory to a vSphere cluster.  
By adding an individual host to an existing workload domain, you can expand the amount of resources contained within an existing vSphere cluster.
- Add a new vSphere cluster to a workload domain.  
As workload domains support multiple vSphere clusters, you can add an additional cluster to an existing workload domain to provide for increased capacity and VM failover isolation.

## Add a Host to a vSphere Cluster in a Workload Domain

Adding an individual host to the management domain or a VI workload domain adds the resources of that host to the domain. You can add multiple hosts at a time to a domain.

### Prerequisites

- There must be a host available in the VMware Cloud Foundation inventory. For information on adding a host to VMware Cloud Foundation, see [Commission Hosts](#).
- Ensure that the host you want to add is in an active state.
- You must have a valid vSphere license specified in the Licensing tab of the SDDC Manager Dashboard with adequate sockets available for the host to be added. For more information, see [Add License Keys for the Software in Your VMware Cloud Foundation System](#).
- Verify that the host to be added matches the configuration of the hosts already in the vSphere cluster. This allows the vSphere cluster configuration to remain balanced. If the host to be added does not match the pre-existing hosts in the vSphere cluster, the cluster will be unbalanced and a warning is displayed. The warning does not prevent the expansion and can be dismissed if needed.
- The host you are adding must have the same type of principal storage as the existing hosts in the cluster. For the management domain, the host must use vSAN for principal storage. For VI workload domains, the host can use vSAN, NFS, VMFS on FC, or vVols for principal storage. A host using NFS for principal storage will automatically use the same NFS configuration as

the other hosts in the cluster. For a host using VMFS on FC, you must create the datastore on the host and configure zoning and mounting of associated volumes before adding the host to a vSphere cluster. A host using vVols for principal storage will automatically use the same vVols configuration as the other hosts in the cluster.

- If the vSphere cluster hosts an NSX-T Edge cluster, you can only add new hosts with the same management, uplink, host TEP, and Edge TEP networks (L2 uniform) as the existing hosts.
- If the vSphere cluster to which you are adding hosts uses a static IP pool for the Host Overlay Network TEPs, that pool must include enough IP addresses for the hosts you are adding. The number of IP addresses required depends on the number of pNICs on the ESXi hosts that are used for the vSphere Distributed Switch that handles host overlay networking. For example, a host with four pNICs that uses two pNICs for host overlay traffic requires two IP addresses in the static IP pool.

#### Procedure

- 1 On the SDDC Manager Dashboard, click **Inventory > Workload Domains**.

The Workload Domains page displays information for all workload domains.

- 2 In the workload domains table, click the name of the workload domain that you want to expand.

The detail page for the selected workload domain appears.

- 3 Click the **Clusters** tab.
- 4 Click the name of the vSphere cluster where you want to add a host.
- 5 Click **Actions > Add Host**.

The Add Hosts wizard appears.

- 6 Select the cluster expansion type.

This option only appears if the vSphere cluster hosts an NSX-T Edge cluster.

Option	Description
<b>L2 Uniform</b>	Select if all hosts you are adding to the vSphere cluster have the same management, uplink, host TEP, and Edge TEP networks as the existing hosts in the vSphere cluster.
<b>L2 non-uniform and L3</b>	Select if any of the hosts you are adding to the vSphere cluster have different networks than the existing hosts in the vSphere cluster.
	<b>Important</b> VMware Cloud Foundation does not support adding hosts to <b>L2 non-uniform and L3</b> vSphere clusters that host an NSX-T Edge cluster.

- 7 Select the host you want to add to the vSphere cluster.

When you use the SDDC Manager UI to add a host, it must be associated with the same network pool as the other hosts in the cluster. The Cloud Foundation API supports adding hosts from different network pools to NSX-T workload domain clusters, if those network pools have the same VLAN ID and MTU settings.

For optimum performance, you must select hosts that are identical in terms of memory, CPU types, and disks to the other hosts in the vSphere cluster. If you select unbalanced hosts, the UI displays a warning message, but you can proceed with the workload domain creation.

You can add a host with multiple active pNICs to a multi pNIC-aware cluster using APIs.

- 8 Click **Next**.
- 9 Select the vSphere license you want to apply to the host.
- 10 Click **Next**.
- 11 Review the host and license details and click **Finish**.

The details page for the vSphere cluster appears with a message indicating that the host is being added. Wait until the action is complete before performing additional workload domain tasks.

## Add a vSphere Cluster to a Workload Domain

You can add a vSphere cluster to the management domain or to a VI workload domain through the Workload Domains page in the SDDC Manager Dashboard.

For the management domain, all vSphere clusters must use vSAN for principal storage. For VI workload domains, vSphere clusters can use vSAN, NFS, VMFS on FC, or vVols for principal storage. If a VI workload domain has multiple clusters, each clusters can use a different type of principal storage, as long as all hosts within a vSphere cluster use the same type.

### Prerequisites

- There must be at least three hosts available in the VMware Cloud Foundation inventory. For information on adding a host to VMware Cloud Foundation, see [Commission Hosts](#).
- Ensure that the hosts you want to add to the vSphere cluster are in an active state.
- You must have a valid vSphere and vSAN (if using vSAN storage) license specified in the Licensing tab of the SDDC Manager Dashboard with adequate sockets available for the host to be added. For more information, see [Add License Keys for the Software in Your VMware Cloud Foundation System](#).
- If you are using DHCP for the Host Overlay Network TEPs, a DHCP server must be configured on the NSX-T host overlay (Host TEP) VLAN of the management domain. When NSX creates TEPs for the VI workload domain, they are assigned IP addresses from the DHCP server.
- From the UI, you can only select hosts on which pNICs 0 and 1 are active.

## Procedure

- 1 On the SDDC Manager Dashboard, click **Inventory > Workload Domains**.

The Workload Domains page displays information for all workload domains.

- 2 Use one of the following methods to get started.

- ◆ From the workload domain page:

- a Hover your mouse in the workload domain row that where you want to add a cluster.

A set of three dots appear on the left of the workload domain name.

- b Click these dots and then click **Add Cluster**.

The Add Cluster wizard appears.

- ◆ From the workload domain details page:

- a Click the name of the workload domain to go to the details page for that workload domain.

- b Click **Actions > Add Cluster**.

The Add Cluster wizard appears.

- 3 Select the storage type for the vSphere cluster and click **Begin**.

- 4 Enter a name for the vSphere cluster and click **Next**.

- 5 Select the cluster image to be applied to the vSphere cluster.

You can select a cluster image only if you are adding a vSphere cluster to a vLCM-enabled VI workload domain.

- 6 On the Networking page, enter the NSX-T host overlay (Host TEP) VLAN of the management domain.

- 7 Select the IP allocation method, provide the required information, and click **Next**.

**Note** You can only use a static IP pool for the management domain and VI workload domains with uniform L2 clusters. For L3 aware or stretch clusters, DHCP is required for Host Overlay Network TEP IP assignment.

Option	Description
DHCP	With this option VMware Cloud Foundation uses DHCP for the Host Overlay Network TEPs.
Static IP Pool	<p>With this option VMware Cloud Foundation uses a static IP pool for the Host Overlay Network TEPs. You can re-use an existing IP pool or create a new one.</p> <p>To create a new static IP Pool provide the following information:</p> <ul style="list-style-type: none"> <li>■ Pool Name</li> <li>■ Description</li> <li>■ CIDR</li> <li>■ IP Range.</li> <li>■ Gateway IP</li> </ul> <p>Make sure the IP range includes enough IP addresses for the number of hosts that will use the static IP Pool. The number of IP addresses required depends on the number of pNICs on the ESXi hosts that are used for the vSphere Distributed Switch that handles host overlay networking. For example, a host with four pNICs that uses two pNICs for host overlay traffic requires two IP addresses in the static IP pool.</p> <p><b>Note</b> You cannot stretch a cluster that uses static IP addresses for the NSX-T Host Overlay Network.</p>

- 8 If you selected vSAN storage for the vSphere cluster, the vSAN parameters page appears. Specify the level of availability you want configured for this cluster. The specified Failures To Tolerate (FTT) value determines the number of hosts required the cluster.
- 9 If you selected VMFS on FC storage for the vSphere cluster, enter the VMFS on FC datastore name.
- 10 If you selected vVols storage for the vSphere cluster, the vVols storage page appears. Enter the VASA storage protocol type, VASA provider name, VASA container name, VASA user name, and datastore name.
- 11 Click **Next**.
- 12 On the Object Names page, review the syntax that will be used for the vSphere objects generated for this cluster and click **Next**.
- 13 On the Host Selection page, select hosts for the vSphere cluster.

When you use the SDDC Manager UI to add a cluster, all hosts must be associated with the same network pool. The Cloud Foundation API supports adding hosts from different network pools to NSX-T workload domain clusters, as long as those network pools have the same VLAN ID and MTU settings.

You can add hosts with multiple active pNICs to the vSphere cluster using APIs.

When you have selected the minimum number of hosts required for this cluster, the **Next** button is enabled.

- 14 Click **Next**.
- 15 If you selected NFS storage for the vSphere cluster, the NFS Storage page appears. Enter the datastore name, NFS share folder, and NFS server IP address.
- 16 Click **Next**.
- 17 On the Licenses page, select the vSphere and vSAN (if using vSAN storage) license to apply to this cluster.
- 18 Click **Next**.
- 19 On the Review page, review the vSphere cluster details and click **Finish**.

---

**Note** Multiple VMKs are created to test the vMotion network, which may cause changes in the MAC addresses and IP address relations. If MAC address filtering is enabled on your physical infrastructure, this may cause issues such as vMotion network connectivity validation failure.

---

The details page for the workload domain appears with the following message: `Adding a new cluster is in progress`. When this process completes, the vSphere cluster appears in the Clusters tab in the details page for the workload domain.

## Rename a Workload Domain

You can rename an existing workload domain.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Inventory > Workload Domains**.
- 2 Hover your mouse in the workload domain row that you want to rename.

A set of three dots appears on the left of the workload domain name. Click these dots and then click **Rename Domain**.

- 3 Enter a new name for the workload domain.
- 4 Click **Rename**.

# Working with Workload Management

# 11

VMware Cloud Foundation™ with VMware Tanzu™ enables you to deploy and operate the compute, networking, and storage infrastructure for vSphere with Tanzu workloads. vSphere with Tanzu transforms vSphere to a platform for running Kubernetes workloads natively on the hypervisor layer. When enabled on a vSphere cluster, vSphere with Tanzu provides the capability to run Kubernetes workloads directly on ESXi hosts and to create upstream Kubernetes clusters within dedicated resource pools. vSphere with Tanzu can also be enabled on the management domain default cluster.

You validate the underlying infrastructure for VMware Cloud Foundation with Tanzu on the Cloud Foundation UI and then complete the deployment in the vSphere UI. The UI refers to the VMware Cloud Foundation with Tanzu functionality as Kubernetes - Workload Management.

For more information on vSphere with Tanzu, see [What Is vSphere with Tanzu?](#).

This chapter includes the following topics:

- [Sizing Compute and Storage Resources for VMware Cloud Foundation with Tanzu](#)
- [Enable Workload Management](#)
- [View Workload Management Cluster Details](#)
- [Update Workload Management License](#)

## Sizing Compute and Storage Resources for VMware Cloud Foundation with Tanzu

Compute and storage requirements for each component are key considerations when you size the solution.

Virtual Machine	Nodes	Total vCPUs	Total Memory	Total Storage
Supervisor Cluster control plane (small nodes - up to 2000 pods per Supervisor cluster)	3	12	48 GB	200 GB
Registry Service	N/A	7	7 GB	200 GB
Tanzu Kubernetes Cluster control plane (small nodes)	3 (per cluster)	6	12 GB	48 GB



Virtual Machine	Nodes	Total vCPUs	Total Memory	Total Storage
Tanzu Kubernetes Cluster worker nodes (small nodes)	3 (per cluster)	6	12 GB	48 GB
VMware NSX-T Edge node	2	16	64 GB	400 GB

## Enable Workload Management

With Workload Management, you validate the underlying infrastructure for vSphere with Tanzu. You then complete the deployment in vSphere.

The UI refers to the VMware Cloud Foundation with Tanzu functionality as Kubernetes - Workload Management.

### Prerequisites

- A Workload Management ready NSX-T VI workload domain must have been deployed  
For a Workload Management ready NSX-T VI workload domain, you must have selected the **Enable vSphere Lifecycle Manager Baselines** option on the Name page of the VI Configuration wizard. For more information, see [Specify Names and vSphere Lifecycle Manager Method](#).
- An NSX-T Edge cluster must have been deployed on the workload domain.  
Workload Management must have been selected on the Use Case page of the Add Edge Cluster wizard. See step 6 in [Create an NSX-T Edge Cluster](#).
- All hosts in the cluster where you want to enable Workload Management must have a vSphere with Tanzu license.
- The following IP addresses must have been defined. You must provide them when you complete Workload Management deployment in the vCenter UI.
  - Non-routable subnet for pod networking
  - Non-routable subnet for service IP addresses
  - Routable subnet for ingress
  - Routable subnet for egress

### Procedure

- 1 From the navigation bar, select **Solutions**.
- 2 In the Kubernetes - Workload Management section, click **Deploy**.

The Workload Domains drop-down menu displays all Workload Management ready workload domains, including the management domain.

- 3 Select the workload domain associated with the cluster where you want to enable Workload Management.

Clusters in the selected workload domain that are compatible with Workload Management are displayed in the Compatible section. Incompatible clusters are displayed in the Incompatible section, along with the reason for the incompatibility. If you want to get an incompatible cluster to a usable state, you can exit the Workload Management deployment wizard while you resolve the issue.

- 4 From the list of compatible clusters on the workload domain, select the cluster where you want to enable Workload Management.

- 5 Click **Next**.

On the Validation page, the following validations are performed.

- vCenter details (vCenter connectivity, objects, and version)
- Network validation (NSX-T details and version)
- Workload Management cluster compatibility

- 6 Click **Next**.

The Review page displays information about the VI workload domain associated with the cluster where you are enabling Workload Management. The remaining deployment is to be completed on the vSphere UI. Note down the values for the following fields as you have to enter these values in the vSphere UI. These fields are marked with a check box on the UI.

- Cluster where you are enabling Workload Management
- DNS server for the cluster
- NTP server for the cluster
- Edge cluster on the workload domain where you are enabling Workload Management
- vSphere Distributed Switch for the workload domain

- 7 Click **Complete in vSphere**.

The page in the vSphere UI is displayed. The vSphere Center associated with the cluster where you are enabling Workload Management is selected by default. Continue the process here.

See [Create and Configure a Supervisor Namespace](#).

#### What to do next

Once you enable Workload Management on a cluster, you must assign a Tanzu edition license to the cluster before the evaluation license expires. See [Update Workload Management License](#).

## View Workload Management Cluster Details

The Workload Management page displays clusters with Workload Management. The status of each cluster, number of hosts in the cluster, and associated workload domain is also displayed.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Solutions**.
- 2 In the Kubernetes - Workload Management section, click **View Details**.
- 3 Click vSphere Workload Management Clusters to see cluster details in vSphere.

## Update Workload Management License

Once you enable Workload Management on a cluster, you must assign a Tanzu edition license to the cluster before the evaluation license expires.

### Prerequisites

You must have added the vSphere with Tanzu license key to the Cloud Foundation license inventory. See [Add License Keys for the Software in Your VMware Cloud Foundation System](#).

### Procedure

- 1 On the SDDC Manager Dashboard, click **Solutions**.
- 2 Click the dots to the left of the cluster for which you want to update the license and click **Update Workload Management license**.
- 3 Select the appropriate license and click **Apply**.

After the license update processing is completed, the Workload Management page is displayed. The task panel displays the licensing task and its status.

# vRealize Suite Lifecycle Manager in Cloud Foundation

# 12

VMware Cloud Foundation deploys vRealize Suite Lifecycle Manager in VMware Cloud Foundation mode, which aligns the behavior of vRealize Suite Lifecycle Manager with the VMware Cloud Foundation architecture.

vRealize Suite Lifecycle Manager in VMware Cloud Foundation mode includes the following capabilities:

- Binary mapping optimization. When vRealize Suite Lifecycle Manager runs in VMware Cloud Foundation mode, it can poll and use the vRealize binaries directly from SDDC Manager's downloaded bundles.
- Automatic load balancer configuration. Load balancer preparation and configuration are no longer a prerequisite when you use vRealize Suite Lifecycle Manager to deploy or perform a cluster expansion on Workspace ONE Access, vRealize Operations, or vRealize Automation. Load balancer preparation and configuration take place as part of the deploy or expand operation.
- Automatic infrastructure selection in vRealize Suite Lifecycle Manager's deployment wizards. When you deploy a vRealize Suite product through vRealize Suite Lifecycle Manager, infrastructure objects such as clusters and networks are prepopulated. They are fixed and cannot be changed to ensure alignment with the VMware Cloud Foundation architecture.
- Cluster deployment for a new environment. You can deploy vRealize Log Insight, vRealize Operations, or vRealize Automation in clusters. You can deploy Workspace ONE Access either as a cluster or a single node. If you deploy Workspace ONE Access as a single node, you can expand it to a cluster later.
- Consistent Bill Of Materials (BOM). vRealize Suite Lifecycle Manager in VMware Cloud Foundation mode only displays product versions that are compatible with VMware Cloud Foundation to ensure product interoperability.
- Inventory synchronization between vRealize Suite Lifecycle Manager and SDDC Manager. vRealize Suite Lifecycle Manager can detect changes made to vRealize Suite products and update its inventory through Environment Refresh. When vRealize Suite Lifecycle Manager in VMware Cloud Foundation mode is enabled, Environment Refresh in vRealize Suite Lifecycle Manager also updates SDDC Manager's inventory to get in sync with the current state of the system.

This chapter includes the following topics:

- [Deploy vRealize Suite Lifecycle Manager in Cloud Foundation](#)
- [Connect vRealize Suite Products to Workload Domains in VMware Cloud Foundation](#)

## Deploy vRealize Suite Lifecycle Manager in Cloud Foundation

Before you can deploy vRealize Log Insight, vRealize Operations, or vRealize Automation, you must deploy vRealize Suite Lifecycle Manager.

By default, VMware Cloud Foundation uses NSX-T Data Center to create application virtual networks (AVNs) and deploys vRealize Suite Lifecycle Manager to these AVNs. If you deactivate AVNs during bring-up, you can configure VLAN-backed networks as described in [KB 80864](#).

VMware Cloud Foundation automates the deployment of the vRealize Suite components through an integration with vRealize Suite Lifecycle Manager. You can use vRealize Suite Lifecycle Manager to deploy and manage those components.

### Prerequisites

- Download the vRealize Suite Lifecycle Manager installation package from the VMware Depot to the local bundle repository. See [Chapter 13 Download an Install Bundle](#).
- Allocate an IP address for the vRealize Suite Lifecycle Manager virtual appliance and prepare forward/reverse DNS records.
- Allocate an IP address for a standalone Tier-1 load balancer for the vRealize components. The IP address must be a free IP address from the xRegion logical segment.
- Verify that there are no firewalls rules that block the required ports listed at [VMware Ports and Protocols](#).

### Procedure

- 1 On the **SDDC Manager Dashboard**, navigate to **Administration > vRealize Suite**.
- 2 Click **Deploy**.

The **vRealize Lifecycle Manager Installation Prerequisites** page displays the prerequisites that you must complete before beginning the installation.

- 3 Review the readiness of each prerequisite and verify by selecting each adjacent check box.  
When all the boxes are selected, the **Begin** button is activated.

- 4 Click **Begin**.
- 5 On the **Network Settings** page, review the settings and click **Next** to continue.

- 6 On the **Virtual Appliance Settings** page, enter the settings and click **Next** to continue.

Setting	Description
Virtual Appliance FQDN	Enter the FQDN for the vRealize Suite Lifecycle Manager virtual appliance.
NSX-T Tier 1 Gateway IP Address	Enter a free IP address from the xRegion logical segment. This address is used for deploying a new Tier 1 NSX-T gateway.
System Administrator	<p>Create and confirm a password for the vRealize Suite Lifecycle Manager system administrator account (vcfadmin@local). The password created is the credential that allows SDDC Manager to connect to the vRealize Suite Lifecycle Manager system.</p> <hr/> <p><b>Note</b> When vRealize Suite Lifecycle Manager in VMware Cloud Foundation mode is enabled, the local administrator account for vRealize Suite Lifecycle Manager is changed from admin to vcfadmin.</p>
SSH Root Account	Create and confirm a password for the vRealize Suite Lifecycle Manager virtual appliance root account.

- 7 On the **Review Summary** page, review the installation configuration settings.

- 8 Click **Finish**.

SDDC Manager validates the inputs and reports any errors or warnings.

---

**Note** If necessary, you can use the **Back** button to return to preceding pages and modify settings.

---

- 9 Address any validation issues and then click **Finish**.

The **vRealize Suite Lifecycle Manager** page displays the following message: `Deployment in progress`. If the deployment fails, this page displays a deployment status of `Failed`. In this case, you can click **Restart Task** or **Uninstall**.

- 10 (Optional) To view the details of the deployment in progress or a deployment failure, click **View Status in Tasks**.

The **Tasks** panel opens at the bottom page. You can open individual tasks to view details.

- 11 (Optional) After the successful deployment of vRealize Suite Lifecycle Manager, click the vRealize Suite Lifecycle Manager link below the page title.

The vRealize Suite Lifecycle Manager user interface opens in a new browser tab.

#### What to do next

You can now deploy vRealize Log Insight, vRealize Operations, and vRealize Automation. See [Deployment of Cloud Operations and Automation in the First Region](#).

# Connect vRealize Suite Products to Workload Domains in VMware Cloud Foundation

If you have deployed vRealize Suite components, then you can connect your vRealize Operations and vRealize Log Insight deployments to your workload domains in VMware Cloud Foundation.

When connected, vRealize Operations and vRealize Log Insight monitor and collect data on the workload domains in VMware Cloud Foundation.

---

**Note** This version of VMware Cloud Foundation does not support connecting vRealize Automation to workload domains through the SDDC Manager Dashboard. Use the vRealize Automation console instead.

For more information about vRealize Automation, see "How do I get started with vRealize Automation using the VMware Cloud Foundation Quickstart" in the *Getting Started with vRealize Automation Cloud Assembly* in the [vRealize Automation Product Documentation](#).

---

By default, the management workload domain is connected to vRealize Operations and vRealize Log Insight.

---

**Note** You can create only one connection at a time.

---

## Prerequisites

- Verify that one or more workload domains have been created.
- Verify that vRealize Operations and vRealize Log Insight are deployed and operational.
- Verify that there are no firewalls rules that block the required ports listed at [VMware Ports and Protocols](#).
- 

## Procedure

- 1 On the **SDDC Manager Dashboard**, navigate to **Administration > vRealize Suite**.
- 2 To connect your vRealize Operations deployment to workload domains:
  - a Select **vRealize Operations**.
  - b Under **Connect Workload Domains...**, click **Connect**.

The **Connect to Workload Domains** wizard opens to the **Modify Connection** page. This page lists all currently configured workload domains. You can connect vRealize Operations to each of the workload domains.

For information about configuring NSX-T in vRealize Operations, see "Add NSX-T Adapters in vRealize Operations Manager in Region A" in the *Deployment of Cloud Operations and Automation in the First Region* in the [VMware Validated Design Documentation](#).

3 To connect your vRealize Log Insight deployment to workload domains:

- a Select **vRealize Log Insight**.
- b Under **Connect Workload Domains...**, click **Connect**.

The **Connect to Workload Domains** wizard opens to the **Modify Connection** page. This page lists all currently configured workload domains. You can connect vRealize Log Insight to each of the workload domains.

4 Select **Enable** for the desired workload domains.

5 Review the connection and click **Finish**.

6 (Optional) Confirm the modified connection in vRealize Operations or vRealize Log Insight.

- a On the **vRealize Operations** or **vRealize Log Insight** page, click the product name link below the page title.

The vRealize Operations or vRealize Log Insight administrative opens the Home page.

- b For vRealize Operations, navigate to **Administration > Solutions**.

The **Solutions** page displays the status of adapters for solutions connected to vRealize Operations. When successfully connected, the status indicates *Data Receiving*.

---

**Note** You must refresh the **Solutions** page to update the status.

---



# Download an Install Bundle

# 13

Cloud Foundation includes the following install bundles.

- A VI workload domain install bundle is used to deploy later versions of the software components instead of the versions in your original Cloud Foundation installation. It includes software bits for vCenter Server and NSX-T Data Center.
- The vRealize Suite Lifecycle Manager install bundle is used for deploying vRealize Suite Lifecycle Manager.

This section describes the procedure for downloading install bundles from SDDC Manager. To download install bundles using a proxy server or in an offline mode, refer to the Download Bundles section in the *VMware Cloud Foundation Lifecycle Management*.

## Procedure

- 1 Log in to your My VMware Account.
  - a On the SDDC Manager Dashboard, click **Administration > Repository Settings**.
  - b Click **Authenticate**.
  - c Type your My VMware user name and password.
  - d Click **Authorize**.
- 2 On the SDDC Manager Dashboard, click **Lifecycle Management > Bundles** in the left navigation pane.

All available bundles are displayed. Install bundles display an Install Only Bundle label.
- 3 For the bundle you want to download, do one of the following:
  - Click **Download Now**.

The bundle download begins right away.
  - Click **Schedule Download**.

Select the date and time for the bundle download and click **Schedule**.
- 4 Navigate to **Lifecycle Management > Download History** to see the downloaded bundles.

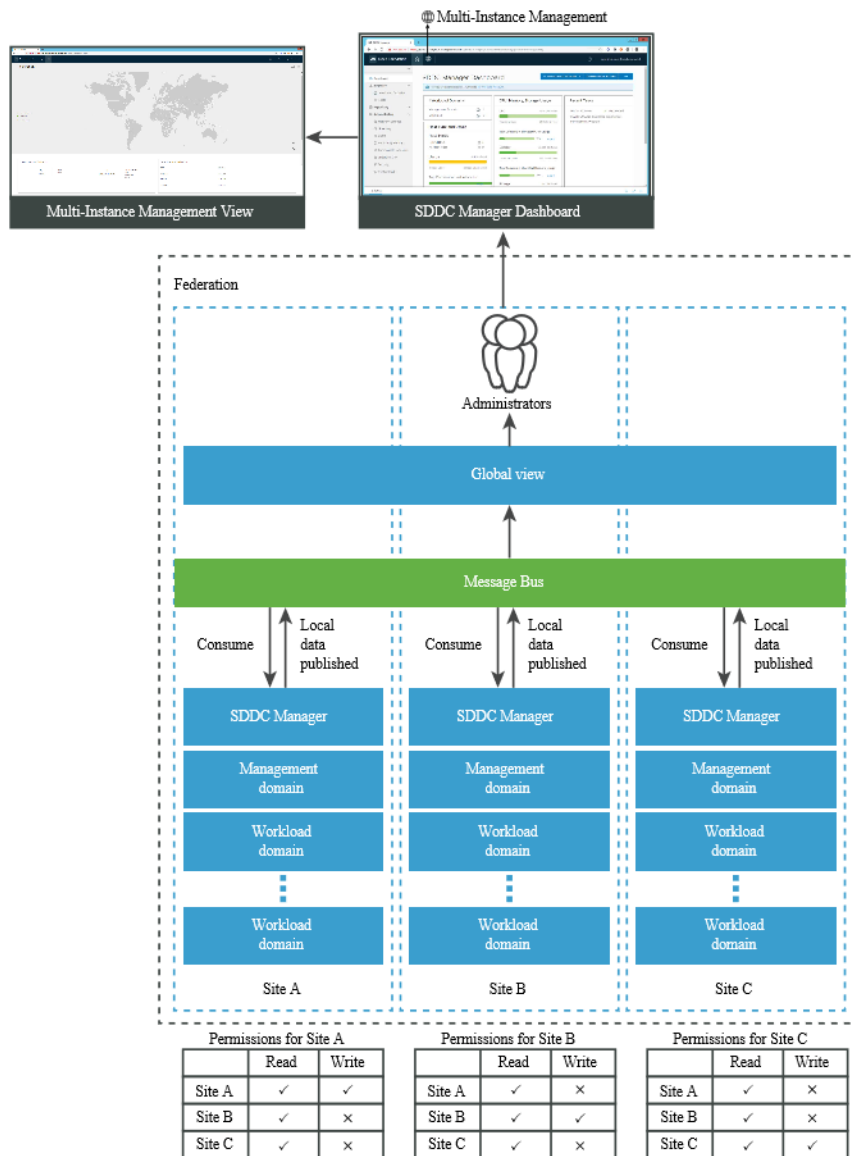
# Multi-Instance Management

# 14

With the Multi-Instance Management feature, you can monitor and manage multiple VMware Cloud Foundation instances from a single console.

Multiple Cloud Foundation instances can be managed together by grouping them into a federation, such that each member can view information about the entire federation and the individual instances within it. Federation members can view inventory across the VMware Cloud Foundation instances in the federation as well as the available and used capacity (CPU, memory, and storage). This allows you to maintain control over the different sites and ensure that they are operating with the right degree of freedom and meeting compliance regulations for your industry. It also simplifies patch management by showing the number of patches available across sites in the global view.

Federation members communicate with each other via a message bus. Each participant publishes their local data to the message bus and the remaining participants can read this data for global visibility across the federation.



An instance can see details about the federation only if it is a member of the federation, and can belong only to a single federation at a time. It is possible to create multiple federations within an organization; however, there is no global visibility between federations. For example, it might be desirable to have a dev-test federation and a production federation. In such an example, members of dev-test can see other dev-test members but they are not able to see production members.

Federation members can either be controllers or regular members. A controller member has capabilities of a regular member and runs some additional message bus components to allow multi-instance management to work.

A controller member can invite other instances to become members as controller or regular members. The controller role can be granted to a maximum of three instances within a federation. High Availability of multi-instance management functionality is only possible when there are exactly three controllers in the federation. Though the controller members can be at any three sites in the federation, it is recommended that each controller is in a different availability zone.

The instance who created the federation is automatically granted the controller role. If you only have two instances in the federation, there is no need to create both as controllers. Multi-Instance management works with two VMware Cloud Foundation sites; however, if one fails then the multi-instance capability is not available on the other site.

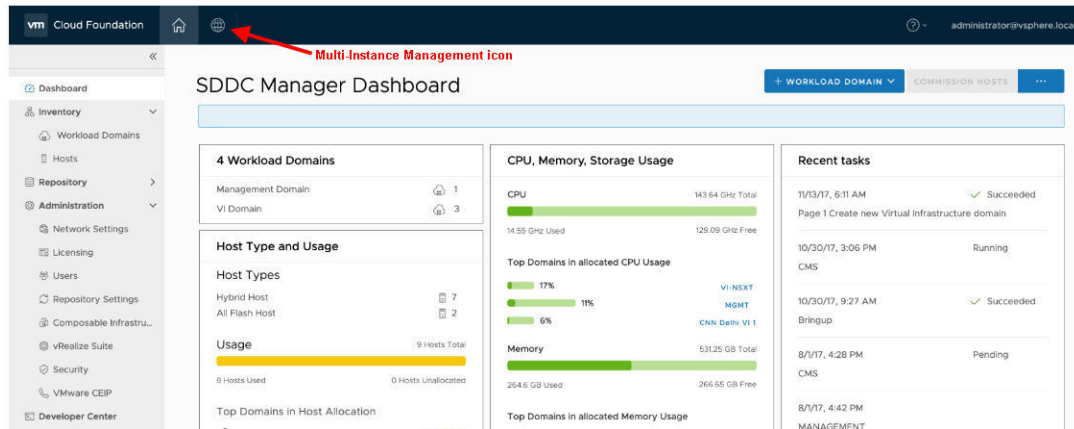
This chapter includes the following topics:

- [About the Multi-Instance Management Dashboard](#)
- [Create a Federation](#)
- [Invite a VMware Cloud Foundation Instance to Join a Federation](#)
- [Join a Federation](#)
- [Leave a Federation](#)
- [Dismantle a Federation](#)
- [Certificate Rotation](#)

## About the Multi-Instance Management Dashboard

The Multi-Instance Management Dashboard displays the inventory and capacity across the federation.

You access the Multi-Instance Management Dashboard by clicking the Multi-Instance View icon in the top left corner of the SDDC Manager Dashboard.




Before a federation is created, the dashboard displays a create and join option.

## Welcome to Multi-Instance Management

Please select one of the following based on your role.


### Create a Federation



Only 1 user should create a federation for a given organization. This instance will become the first Controller. ⓘ

[CREATE](#)

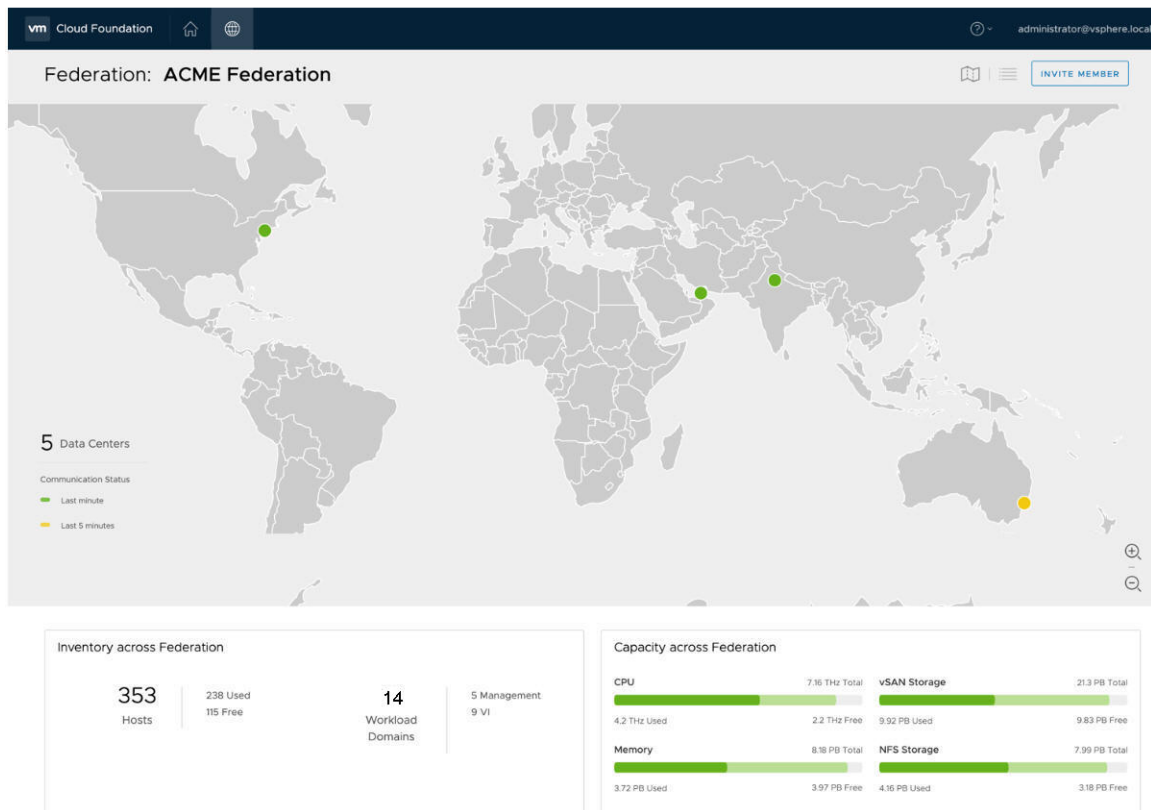
### Join a Federation



Most users will be joining an established federation by invitation. Please refer to the instructions you received in order to join.

[JOIN](#)

After a federation is created, the Multi-Instance Management Dashboard displays a world map showing the federation members as dots on the map.

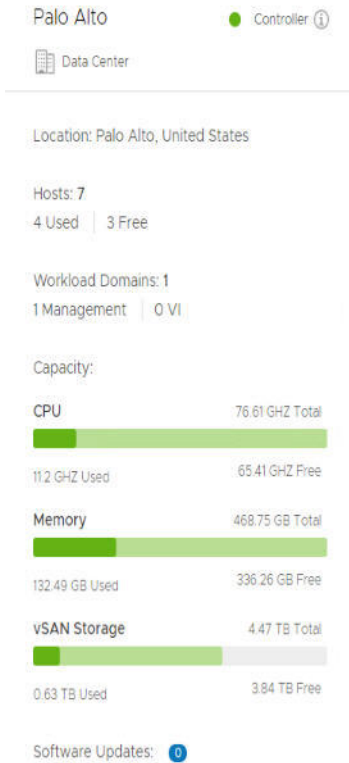


The dot color depends on the communication status between the federation members - green if they communicated within the last two minutes, yellow if they communicated within the previous five minutes, and red if they have not communicated for more than ten minutes. You can see the following information here:

- Hover over a dot to see the member name and location.



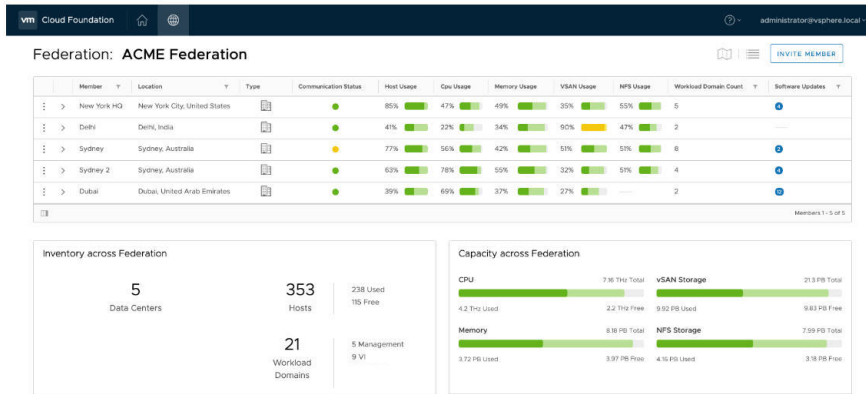
- Click the member location dot to open a panel on the right side with detailed information about the VMware Cloud Foundation instance. The panel also displays available software updates.



The Inventory section in the bottom half of the dashboard displays the number of hosts and workload domains along with a breakdown of the workload domain type. The capacity section displays the used and available CPU, memory, and storage across the federation.

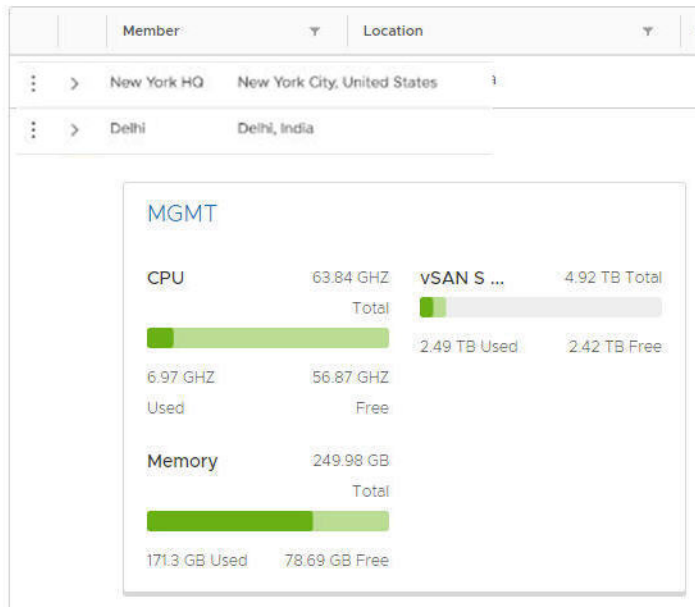


Click the Table icon at the top right of the dashboard to display member information in a grid format. Information for all federation members is displayed in a tabular format.



Clicking the arrow (➤) next to the member name displays the CPU, memory, and storage usage for that member.

## Federation: ACME Federation



Clicking MGMT takes you to the management domain of that member.

## Create a Federation

A federation is a group of VMware Cloud Foundation instances, such that each member can view information about the other VMware Cloud Foundation instances in the group. The federation creator is granted the controller role by default.


You can create multiple federations within your organization, but global visibility is available only within a federation. Members can belong to only a single federation at a time.

See [VMware Configuration Maximums](#) for information about the maximum number of SDDC Manager instances that can be managed using Multi-Instance Management

## Prerequisites

- The SDDC Manager certificate requires TLS Web server authentication and TLS Web client authentication extended key usage (EKU). If you are using Microsoft CA or a third-party CA, you must ensure that the Certificate Authority template is configured with both these EKUs.
- Retrieve the FQDN of your SDDC Manager.

## Procedure

- 1 On the SDDC Manager dashboard, click the Multi-Instance View () icon at the top of the window.
- 2 Click **Create**.

**Create Federation**

Establishing a federation requires two steps:

1. Register the first member (who is designated as a Controller).
2. Invite additional members to the federation.

**Responsibilities of the Controller:**

- Only Controllers may invite new members to a federation.
- Controllers can only dismantle a federation once all its members have left the federation.
- Providing high availability.

Federation Name	ACME Federation
Member Name ⓘ	Palo Alto
FQDN	sddc-manager.vrack.vsphere.local
Country	United States ▼
City	Palo Alto ▼

CANCEL CREATE

- 3 Enter a name for the federation.
- 4 Enter a display name for the member. You may want to base this on the location of this VMware Cloud Foundation instance.
- 5 Type the FQDN of the SDDC Manager.
- 6 Select the city and country of this VMware Cloud Foundation instance and click **Create**.

## Results

It can take a few minutes for the federation to be created. After the federation is created, the Multi Instance Management Dashboard is displayed. The federation location is marked with a green dot on the world map. You can zoom in or out of the map.



The dashboard also displays the inventory (hosts and workload domains) and capacity (CPU, memory, and storage) across the federation. These details are updated when additional members join the federation.

### What to do next

Invite a VMware Cloud Foundation instance to join the federation.

## Invite a VMware Cloud Foundation Instance to Join a Federation

You can invite VMware Cloud Foundation instances to join a federation. They can be invited as a controller or a regular member. High Availability of multi-instance management functionality is only possible when there are exactly three controllers in the federation. Though the controller members can be at any three sites in the federation, it is recommended that each controller is in a different availability zone.

### Prerequisites

You must be a controller in the federation and have the FQDN of the member you are inviting.

### Procedure

- 1 On the top right corner of the Multi-Instance Management dashboard, click **Invite Member**.
- 2 Enter the SDDC Manager FQDN of the member you are inviting and click **Check Certificate**.  
The invited member's certificate thumbprint is displayed.
- 3 Validate the thumbprint and click **Confirm fingerprint**.
- 4 Click **Next**.
- 5 Select the check box on the High Availability page if you want to designate the controller role to the member.
- 6 Click **Next**.

The Instructions page displays the URL that the invited member needs to access.

Invite Member

1 Enter member FQDN

2 High Availability

3 Member Instructions

High Availability

✓

The federation already has a maximum of 3 controllers. High availability is in effect.

In order to ensure high availability performance, a federation must have exactly 3 controllers. Before deciding to designate a controller, please be aware of how many already exist for this federation.

☐ Designate this member as a controller. ⓘ

- 7 Click **Copy Info** to copy the information displayed on this page or copy the URL manually and send it to the member through an offline method.

VMware, Inc.

121

## What to do next

The invitation and joining process is a coordinated effort between the invitee controller and joining member. An additional dot on your Multi-Instance Management Dashboard indicates that the member you invited is joining the federation. When a controller joins a federation, it can take a few minutes for the federation to stabilize.

## Join a Federation

You can join a federation as a controller or member depending on the assigned role in the invitation. An invitation is valid for ten days. You must request a new invitation after this period. If a new invitation is generated for the same site, only the latest invite is valid.

### Prerequisites

- Verify that the federation is healthy - there should be no red dots on the world map of the Multi-Instance Management Dashboard. A red dot indicates that SDDC Manager is unable to communicate with that member.
- The SDDC Manager certificate requires TLS Web server authentication and TLS Web client authentication extended key usage (EKU). If you are using Microsoft CA or a third-party CA, you must ensure that the Certificate Authority template is configured with both these EKUs.
- Retrieve the FQDN of your SDDC Manager.

## Join a Federation by Clicking an Invitation

If you join a federation by clicking the invitation you received, federation details are pre-populated in the UI.

### Prerequisites

Retrieve the invitation you received.

### Procedure

- 1 Click the URL in the invitation you received.

The Join Federation window displays the role assigned in the invitation, the FQDN of the invited member, token, and the FQDN of the controller member who invited you to join the federation.

## Join Federation

✔ Certificate is validated successfully. ✕

Member Name ⓘ	<input type="text" value="Delhi"/>
Member Role	<input style="border-bottom: 1px solid #ccc;" type="text" value="Member"/>
FQDN ⓘ	<input type="text" value="delhi.mydomain.local"/>
Country	<input style="border-bottom: 1px solid #ccc;" type="text" value="India"/>
City	<input style="border-bottom: 1px solid #ccc;" type="text" value="Delhi"/>
Token ⓘ	<input type="text" value="jhdjfJHJGDJJKDF57642j4JHBDKjndnk"/>
FQDN of Controller ⓘ	<input type="text" value="newyork.mydomain.local"/>

## 2 Click **Join**.

### Results

The join process is initiated. If you see an error, resolve the issue and then request a new invitation and follow the steps described above. After the join process is successful, your VMware Cloud Foundation instance becomes a member of the federation.

After a controller joins or leaves a federation, Kafka is restarted on all controllers in the federation. It can take several minutes for the federation to stabilize even after the dashboard is refreshed. If an operation performed on the dashboard during this time fails, re-try the operation.

## Join a Federation through the Multi-Instance Management Dashboard

You can join a federation through the Multi-Instance Management Dashboard.

### Procedure

- 1 Click **Join Federation** on the Multi-Instance Management Dashboard.
- 2 Type a display name for the site to be added.
- 3 Select the member role as indicated in the invitation you received.
- 4 Type the FQDN of your SDDC Manager.
- 5 Select the country and city for your site.
- 6 Type the token as indicated in the invitation you received.
- 7 Type the FQD of the controller who invited you.
- 8 Click **Join**.

## Results

The join process is initiated. If you see an error, resolve the issue and then request a new invitation and follow the steps described above. After the join process is successful, your VMware Cloud Foundation instance becomes a member of the federation.

After a controller joins or leaves a federation, Kafka is restarted on all controllers in the federation. It can take several minutes for the federation to stabilize even after the dashboard is refreshed. If an operation performed on the dashboard during this time fails, re-try the operation.

## Leave a Federation

Leaving a federation removes the Multi-Instance Management view from your SDDC Manager Dashboard.

If you are a controller, you can leave a federation only if there is at least one more controller in the federation. If you are the only controller member in a federation, you must dismantle a federation instead of leaving it.

### Prerequisites

Verify that the federation is healthy - there should be no red dots on the world map of the Multi-Instance Management Dashboard. A red dot indicates that SDDC Manager is unable to communicate with that member. A controller must remove the member using the leave API. See the *VMware Cloud Foundation API Reference Guide*.

### Procedure

- 1 Click the Grid icon at the top right of the Multi-Instance Management Dashboard.
- 2 In the member table, click the dot icon next to your member name and click **Leave Federation**.
- 3 Type the federation name and click **Leave**.

### What to do next

Do not perform any operation for a few minutes after leaving a federation.

## Dismantle a Federation

You can dismantle a federation if you are the last controller member in the federation. Only members with the controller role can dismantle a federation.

### Procedure

- 1 Click the Grid icon at the top right of the Multi-Instance Management Dashboard.
- 2 In the member table, click the dot icon next to your member name and click **Dismantle Federation**.
- 3 Type the federation name and click **Dismantle**.

### What to do next

After the federation is dismantled, the Create Federation screen is displayed instead of the Multi-Instance Management Dashboard.

## Certificate Rotation

When you rotate certificates for a VMware Cloud Foundation instance that is part of a Federation, the Certificate Signing Request (CSR) must match the CSR of the original certificate.

For more information on certificate rotation, see [Chapter 4 Certificate Management](#).

# Stretching Clusters

# 15

You can stretch an NSX-T cluster in the management domain, or in a VI workload domain using vLCM baselines, across two availability zones within a region. Both availability zones must contain an equal number of hosts to ensure failover in case any of the availability zones goes down.

The default management cluster must be stretched before a VI workload domain cluster can be stretched. This ensures that the NSX control plane and management VMs (vCenter, NSX, SDDC Manager) remain accessible if the stretched cluster in the primary availability zone goes down.

---

**Note** You cannot stretch a cluster in the following conditions:

- the cluster uses static IP addresses for the NSX-T Data Center Host Overlay Network TEPs
  - the cluster has a vSAN remote datastore mounted on it
  - the cluster uses vSphere Lifecycle Manager images
- 

Some use cases for stretching a cluster are described below.

- **Planned maintenance**

You can perform a planned maintenance on an availability zone without any downtime and then migrate the applications after the maintenance is completed.

- **Automated recovery**

Stretching a cluster automatically initiates VM restart and recovery, and has a low recovery time for the majority of unplanned failures.

- **Disaster avoidance**

With a stretched cluster, you can prevent service outages before an impending disaster.

This chapter includes the following topics:

- [About Availability Zones and Regions](#)
- [Stretched Cluster Requirements](#)
- [Deploy and Configure vSAN Witness Host](#)
- [Stretch a Cluster](#)
- [Expand a Stretched Cluster](#)
- [Unstretch a Cluster](#)

- [Replace a Failed Host in a Stretched Cluster](#)
- [Change the vSAN Witness Host in a Stretched Cluster](#)

## About Availability Zones and Regions

This section describes an availability zone and region as used for stretch clusters.

### Availability Zones

An availability zone is a collection of infrastructure components. Each availability zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. Each zone should have independent power, cooling, network, and security.

Additionally, these zones should be physically separate so that disasters affect only one zone. The physical distance between availability zones is short enough to offer low, single-digit latency (less than 5 ms) and large bandwidth (10 Gbps) between the zones.

Availability zones can either be two distinct data centers in a metro distance, or two safety or fire sectors (data halls) in the same large-scale data center.

### Regions

Regions are in two distinct locations - for example, region A can be in San Francisco and region B in Los Angeles (LAX). The distance between regions can be rather large. The latency between regions must be less than 150 ms.

## Stretched Cluster Requirements

In an environment with multiple availability zones, Layer 2 networks must be stretched between the availability zones by the physical infrastructure. You also must provide a Layer 3 gateway that is highly available between availability zones. The method for stretching these Layer 2 networks and providing a highly available Layer 3 gateway is vendor-specific.

### VLANs and Subnets for Multiple Available Zones

This section displays a sample configuration for an environment with multiple availability zones. The management, Uplink 01, Uplink 02, and Edge Overlay networks in each availability zone must be stretched to facilitate failover of the NSX Edge appliances between availability zones. The Layer 3 gateway for the management and Edge Overlay networks must be highly available across the availability zones.

**Table 15-1. Management Domain VLAN and IP Subnet Requirements**

Function	Availability Zone 1	Availability Zone 2	VLAN ID	IP Range	HA Layer 3 Gateway	Recommended MTU
Management (AZ1)	✓	✓	1611 (Stretched)	172.16.11.0/24	✓	1500
vSphere vMotion	✓	X	1612	172.16.12.0/24	✓	9000
vSAN	✓	X	1613	172.16.13.0/24	✓	9000
NSX-T Host Overlay	✓	X	1614	172.16.14.0/24 (DHCP)	✓	9000
NSX-T Edge Uplink01	✓	✓	2711 (Stretched)	172.27.11.0/24	X	9000
NSX-T Edge Uplink02	✓	✓	2712 (Stretched)	172.27.12.0/24	X	9000
NSX-T Edge Overlay	✓	✓	2713 (Stretched)	172.27.13.0/24	✓	9000
Management (AZ2)	X	✓	1621	172.16.21.0/24	✓	1500
vSphere vMotion	X	✓	1622	172.16.22.0/24	✓	9000
vSAN	X	✓	1623	172.16.23.0/24	✓	9000
NSX-T Host Overlay	X	✓	1624	DHCP	✓	9000

**Note** If VLAN is stretched between AZ1 and AZ2, the Layer 3 network must also be stretched between the two AZs.

**Table 15-2. Workload Domain VLAN and IP Subnet Requirements**

Function	Availability Zone 1	Availability Zone 2	VLAN ID	IP Range	HA Layer 3 Gateway	Recommended MTU
Management (AZ1)	✓	✓	1631 (Stretched)	172.16.31.0/24	✓	1500
vSphere vMotion	✓	X	1632	172.16.32.0/24	✓	9000
vSAN	✓	X	1633	172.16.33.0/24	✓	9000
NSX-T Host Overlay	✓	X	1634	172.16.34.0/24 (DHCP)	✓	9000
NSX-T Edge Uplink01	✓	✓	2731 (Stretched)	172.27.31.0/24	X	9000
NSX-T Edge Uplink02	✓	✓	2732 (Stretched)	172.27.32.0/24	X	9000



Table 15-2. Workload Domain VLAN and IP Subnet Requirements (continued)

Function	Availability Zone 1	Availability Zone 2	VLAN ID	IP Range	HA Layer 3 Gateway	Recommended MTU
NSX-T Edge Overlay	✓	✓	2733 (Stretched)	172.27.33.0/24	✓	9000
Management (AZ2)	X	✓	1641	172.16.41.0/24	✓	1500
vSphere vMotion	X	✓	1642	172.16.42.0/24	✓	9000
vSAN	X	✓	1643	172.16.43.0/24	✓	9000
NSX-T Host Overlay	X	✓	1644	172.16.44.0/24 (DHCP)	✓	9000

**Note** If VLAN is stretched between AZ1 and AZ2, the Layer 3 network must also be stretched between the two AZs.

## Networking for Multiple Availability Zones

There are specific physical data center network requirements for a topology with multiple availability zones.

Table 15-3. Physical Network Requirements for Multiple Availability Zone

Component	Requirement
MTU	<ul style="list-style-type: none"> <li>■ VLANs which are stretched between availability zones must meet the same requirements as the VLANs for intra-zone connection including MTU.</li> <li>■ MTU value must be consistent end-to-end including components on the inter zone networking path.</li> <li>■ Set MTU for all VLANs and SVIs (management, vMotion, Geneve, and Storage) to jumbo frames for consistency purposes. Geneve overlay requires an MTU of 1600 or greater.</li> </ul>
Layer 3 gateway availability	For VLANs that are stretched between available zones, configure data center provided method, for example, VRRP or HSRP, to failover the Layer 3 gateway between availability zones.
DHCP availability	<p>For VLANs that are stretched between availability zones, provide high availability for the DHCP server so that a failover operation of a single availability zone will not impact DHCP availability.</p> <p><b>Note</b> You cannot stretch a cluster that uses static IP addresses for the NSX-T Host Overlay Network TEPs.</p>
BGP routing	Each availability zone data center must have its own Autonomous System Number (ASN).

**Table 15-3. Physical Network Requirements for Multiple Availability Zone (continued)**

Component	Requirement
Ingress and egress traffic	<ul style="list-style-type: none"> <li>■ For VLANs that are stretched between availability zones, traffic flows in and out of a single zone. Local egress is not supported.</li> <li>■ For VLANs that are not stretched between availability zones, traffic flows in and out of the zone where the VLAN is located.</li> <li>■ For NSX-T virtual network segments that are stretched between regions, traffic flows in and out of a single availability zone. Local egress is not supported.</li> </ul>
Latency	<ul style="list-style-type: none"> <li>■ Maximum network latency between NSX Managers is 10 ms.</li> <li>■ Maximum network latency between the NSX Manager cluster and transport nodes is 150 ms.</li> </ul>

## Deploy and Configure vSAN Witness Host

Each vSAN stretched cluster requires a witness host deployed in a vSAN Witness zone, which must be different from the location of both availability zones. The witness appliance should be running the same version of ESXi as the ESXi hosts in the stretched cluster. The maximum RTT on the witness is 200ms.

See [Deploy and Configure the vSAN Witness Host](#) in the VMware Validated Design document. This document follows a preset object naming convention. Treat this as an example and follow your own naming convention.

## Stretch a Cluster

This procedure describes how to stretch a cluster across two availability zones. Stretch clusters are supported for the management domain and for VI workload domains using vLCM baselines.

Our example use case has two availability zones in two buildings in an office campus - AZ1 and AZ2. Each availability zone has its own power supply and network. The management domain is on AZ1 and contains the default cluster, **SDDC-Cluster1**. This cluster contains four ESXi hosts. AZ1 also contains the default bring-up pool, bringup-networkpool.

**Table 15-4.**

Availability Zone 1	
vSAN network	VLANID=1613
	MTU=9000
	Network=172.16.13.0
	netmask 255.255.255.0

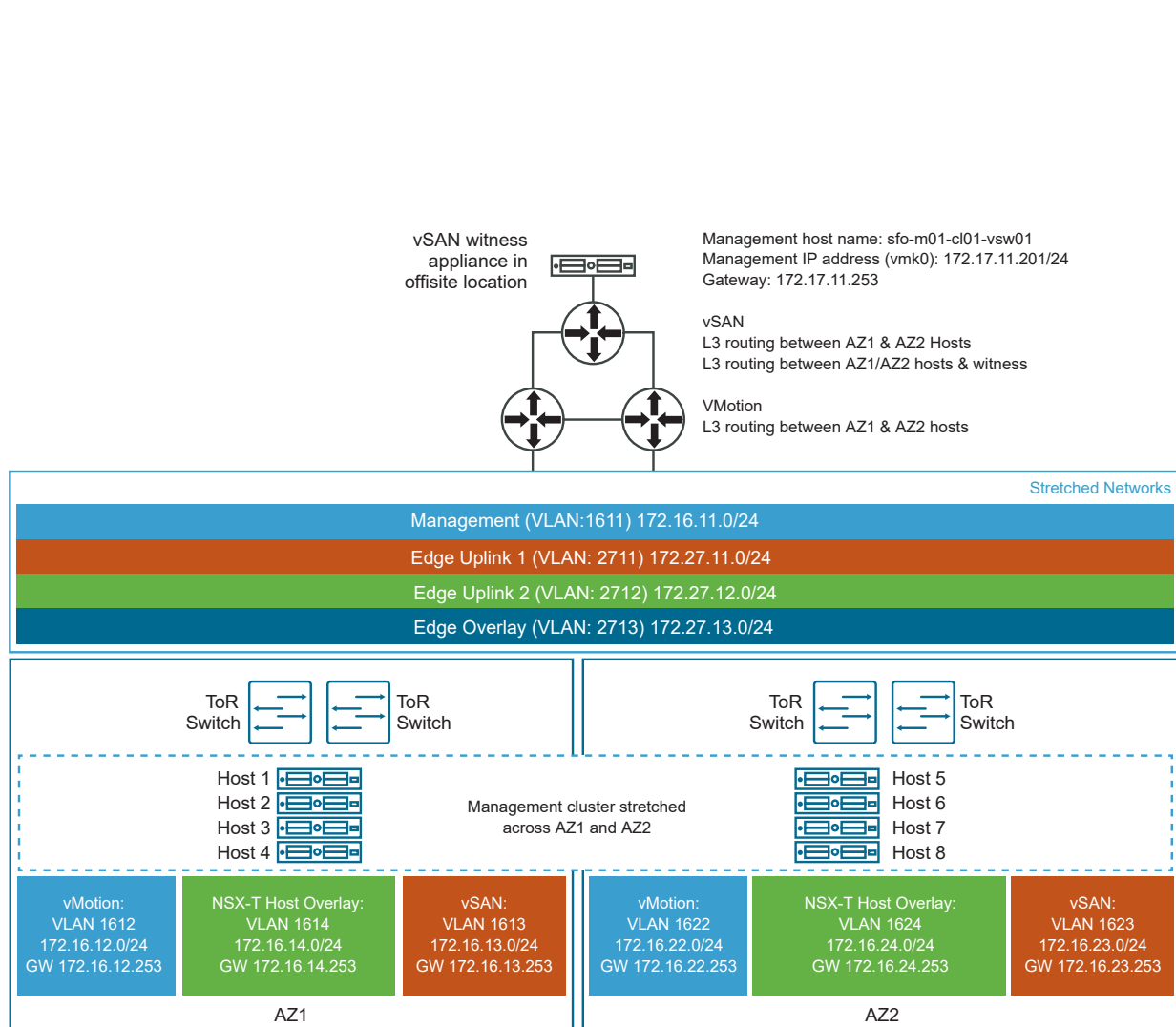
Table 15-4. (continued)

Availability Zone 1	
	gateway 172.16.13.253
vMotion network	VLANID=1612
	MTU=9000
	Network=172.16.12.0
	netmask 255.255.255.0
	gateway 172.16.12.253

There are four ESXi hosts in AZ2 that are not in the VMware Cloud Foundation inventory yet.

We will stretch the default cluster `SDDC-Cluster1` in the management domain from AZ1 to AZ2.

Figure 15-1. Stretch Cluster Example



## Prerequisites

- Verify that your environment satisfies the prerequisites for the implementation of Availability Zone 2 in the management domain. See [Prerequisites for Implementing Availability Zone 2 for the Management Domain](#).
- You must have deployed and configured a vSAN witness host. See [Deploy and Configure the vSAN Witness Host](#).
- Configure routing to the datacenter infrastructure in the second availability zone and set the infrastructure VM restart order in case of a failure. See [NSX-T Data Center Configuration for Availability Zone 2 for the Management Domain in Region A](#) in the VMware Validated Design document. This document follows a preset object naming convention. Treat this as an example and follow your own naming convention.
- All VMs on an external network must be on an overlay backed segment. If they are on a VLAN, that VLAN must be stretched as well.
- Ensure that you have enough hosts such that there is an equal number of hosts on each availability zone. This is to ensure that there are sufficient resources in case an availability zone goes down completely.
- Ensure that the required TCP and UDP ports for vSAN network are open for communication between the availability zones and between the witness host and both availability zones. See KB article [52959](#).
- If you are stretching a cluster in a VI workload domain, the default management domain cluster must have been stretched.

---

**Note** You cannot stretch a cluster that uses static IP addresses for the NSX Host Overlay Network TEP, includes a remote vSAN datastore, or uses vSphere Lifecycle Manager images.

---

## Procedure

- 1 Create a network pool, `AZ2-networkpool1`, on AZ2. See [Create a Network Pool](#).

Based on our example, here are the network details for the network pool.

**Table 15-5.**

Availability Zone 2	
vSAN network	VLANID=1623
	MTU=9000
	Network=172.16.23.0
	Netmask=255.255.255.0
	Gateway=172.16.23.253
vMotion network	VLANID=1622

Table 15-5. (continued)

Availability Zone 2	
	MTU=9000
	Network=172.16.22.0
	netmask 255.255.255.0
	gateway 172.16.22.253

- 2 Commission the four hosts in AZ2 and associate them with `AZ2-networkpool`. In our example, these are 172.16.21.105, 172.16.21.106, 172.16.21.107, 172.16.21.108.

See [Commission Hosts](#).

- 3 Get the UUIDs of the hosts in AZ2.
  - a On the SDDC Manager Dashboard, click **Developer Center > API Explorer**.
  - b Under APIs for managing hosts, click **GET /v1/hosts**.
  - c Click **Execute**.
  - d Click **Download** to download the JSON file.
  - e Open the JSON file and copy the UUIDs of the hosts in AZ2.
- 4 Get the ID of the cluster you are stretching (`SDDC-Cluster1` in our example).
  - a In the API Explorer, navigate to APIs for managing clusters and click `GET /v1/clusters`.
  - b Click **Execute**.
  - c Click **Download** to download the JSON file.
  - d Open the JSON file and copy the cluster ID for `SDDC-Cluster1`.

## 5 Validate the stretch cluster API.

### a Prepare the JSON request body.

- 1 In the API section for **Managing Clusters**, click `POST /v1/clusters/id/validations`.
- 2 Under `clusterUpdateSpec`, click `Cluster Update Data`  
`ClusterOperationSpecValidation`.
- 3 Click **Download** to download the JSON file.
- 4 Edit the downloaded JSON file so that it contains only the stretch section similar to the example below.

```
{
  "clusterUpdateSpec" : {
    "clusterStretchSpec": {
      "hostSpecs": [ {
        "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx",
        "licenseKey": "XXXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
      }, {
        "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx",
        "licenseKey": "XXXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
      }, {
        "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx",
        "licenseKey": "XXXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
      }, {
        "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx",
        "licenseKey": "XXXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
      } ],
      "secondaryAzOverlayVlanId": 1624,
      "isEdgeClusterConfiguredForMultiAZ":true,
      "witnessSpec": {
        "fqdn": "sfo03m01vsanw01.sfo.rainpole.local",
        "vsanCidr": "172.17.13.0/24",
        "vsanIp": "172.17.13.201"
      }
    }
  }
}
```

- 5 Update the values for witness FQDN, CIDR, vSAN IP address, and host IDs and license keys.

### b Run the API command.

- 1 Click `POST /v1/clusters/id/validations`.

- 2 For the `ClusterOperationSpecValidation` field, update the cluster UID (you retrieved this in step 4) and host UID ((you retrieved this in step 3).

c Click **Execute**.

Ensure that the validation is successful. If there are any errors, resolve them and run the validation again.

6 Stretch the cluster.

a Prepare the JSON request body.

- 1 Click `Patch /v1/clusters/id`.
- 2 Under `ClusterUpdateSpec`, click `Cluster Update Data`  
`ClusterUpdateSpec{ ... }`.
- 3 Click **Download** to download the JSON file.
- 4 Edit the JSON file so that it contains only the stretch section similar to the example below.

```
{
  "clusterStretchSpec": {
    "hostSpecs": [ {
      "id": "2c1744dc-6cb1-4225-9195-5cbd2b893be6",
      "licenseKey": "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
    }, {
      "id": "6b38c2ea-0429-4c04-8d2d-40a1e3559714",
      "licenseKey": "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
    }, {
      "id": "5b704db6-27f2-4c87-839d-95f6f84e2fd0",
      "licenseKey": "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
    }, {
      "id": "5333f34f-f41a-44e4-ac5d-8568485ab241",
      "licenseKey": "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
    } ],
    "secondaryAzOverlayVlanId": 1624,
    "isEdgeClusterConfiguredForMultiAZ": true,
    "witnessSpec": {
      "fqdn": "sfo03m01vsanw01.sfo.rainpole.local",
      "vsanCidr": "172.17.13.0/24",
      "vsanIp": "172.17.13.201"
    }
  }
}
```

- 5 Update the values for witness FQDN, CIDR, vSAN IP address, and host IDs and license keys.
- 6 Click **Execute**.  
The stretch cluster task is displayed in the SDDC Manager task panel.
- 7 Monitor the stretch cluster task till it is completed.



- 7 Log in to the vCenter Server to validate that the cluster has been stretched correctly.
  - a Check the vSAN health page.
    - 1 Click **Host and Clusters**.
    - 2 Select the stretched cluster (SDDC-Cluster1 in our example).
    - 3 Click **Monitor > vSAN > Health**.
    - 4 Click **Retest**.
    - 5 Fix errors, if any.
  - b Check the vSAN storage policy page.
    - 1 Click **Policies and Profiles > VM Storage Policies > vSANDefault Storage Policies**.
    - 2 Select the policy associated with the vCenter Server for the stretched cluster (SDDC-Cluster1 in our example)
    - 3 Click **Monitor > VMs and VirtualDisks**.
    - 4 Click **Refresh**.
    - 5 Click **Trigger VM storage policy compliance check**.
    - 6 Fix errors, if any.

#### What to do next

Add new VMs to the primary AZ and associate the host rule for the new VMs with the primary AZ rule.

## Expand a Stretched Cluster

You can expand a stretched cluster by adding hosts. It is recommended that you add the same number of hosts to both availability zones for symmetry and cluster balance.

#### Procedure

- 1 Commission the additional hosts to VMware Cloud Foundation.  
See [Commission Hosts](#).
- 2 Get the UUIDs of the hosts you commissioned.
  - a On the SDDC Manager Dashboard, click **Developer Center > API Explorer**.
  - b Under APIs for managing hosts, click **GET /v1/hosts**.
  - c Click **Execute**.
  - d Click **Download** to download the JSON file.
  - e Open the JSON file and copy the the UUIDs of the hosts.

- 3 Get the ID of the cluster you are expanding (SDDC-Cluster1 in our example).
  - a In the API Explorer, navigate to APIs for managing clusters and click `GET /v1/clusters`.
  - b Click **Execute**.
  - c Click **Download** to download the JSON file.
  - d Open the JSON file and copy the the cluster ID for SDDC-Cluster1.
- 4 Get the primary and secondary availability zone names from vCenter Server.
  - a Log in to vCenter Server.
  - b Navigate to **Cluster > Configure > vSAN > Fault Domains**.
  - c Note down the primary and secondary availability zone names.

## 5 Run the expand API command.

### a Prepare the JSON request body.

- 1 Click `Patch /v1/clusters/id`.
- 2 Under `ClusterUpdateSpec` field, click `Cluster Update Data`  
`ClusterUpdateSpec{ ... }`.
- 3 Click **Download** to download the JSON file.
- 4 Edit the downloaded JSON file so that it contains only the expand section similar to the example below. In the **azName** field, type the primary and secondary names you had retrieved in step 4.

```
{
  "clusterExpansionSpec": {
    "hostSpecs": [ {
      "id": "2c1744dc-6cb1-4225-9195-5cbd2b893be6",
      "licenseKey": "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX",
      "azName": "primary/secondary"
    }, {
      "id": "6b38c2ea-0429-4c04-8d2d-40a1e3559714",
      "licenseKey": "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX",
      "azName": "primary/secondary"
    }, {
      "id": "5b704db6-27f2-4c87-839d-95f6f84e2fd0",
      "licenseKey": "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX",
      "azName": "primary/secondary"
    }, {
      "id": "5333f34f-f41a-44e4-ac5d-8568485ab241",
      "licenseKey": "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX",
      "azName": "primary/secondary"
    } ]
  }
}
```

### b Run the expand cluster API.

- 1 For the `ClusterUpdateSpec` field, update the cluster ID (you retrieved this in step 3) and unstretch JSON file with the payload you prepared in step 5a.iii.
  - 2 Click **Execute**.  
The stretch cluster task is displayed in the SDDC Manager task panel.
  - 3 Monitor the task till it is completed.
- 6 If required, SSH in to each newly added host and add a static route to the vSAN network of the witness host. Also add static routes in the witness if it could not reach the vSAN network of the newly added hosts.

- 7 Update the value of **Host failure cluster tolerates** to the number of hosts in AZ1 after cluster expansion.
  - a Log in to the management vCenter Server.
  - b Select **Hosts and Clusters** and expand the stretched cluster (SDDC-Cluster1 in our example).
  - c Click the **Configure** tab.
  - d Under **Services**, click **vSphere Availability**, and then click **Edit**.
  - e On the Admission Control page of the Edit Cluster Settings dialog box, set **Host failures cluster tolerates** to the number of hosts in AZ1 and click **OK**.

## Unstretch a Cluster

This procedure describes how to unstretch a vSAN cluster.

In this procedure, we will unstretch the default cluster in the management domain (**SDDC-Cluster1**) that has been stretched from AZ1 to AZ2.

### Procedure

- 1 Get the ID of the cluster you are unstretching (SDDC-Cluster1 in our example).
  - a On the SDDC Manager Dashboard, click **Developer Center > API Explorer**.
  - b In the API Explorer, navigate to APIs for managing clusters and click `GET /v1/clusters`.
  - c Click **Execute**.
  - d Click **Download** to download the JSON file.
  - e Open the JSON file and copy the the cluster ID for SDDC-Cluster1.

## 2 Unstretch the cluster.

### a Prepare the JSON request body.

- 1 Click `Patch /v1/clusters/id`.
- 2 Under `ClusterUpdateSpec` field, click `Cluster Update Data`  
`ClusterUpdateSpec{ ... }`.
- 3 Click **Download** to download the JSON file.
- 4 Edit the downloaded JSON file so that it contains only the unstretch information similar to the example below.

```
{
  "clusterUnstretchSpec": {}
}
```

### b Run the unstretch cluster API.

- 1 For the `ClusterUpdateSpec` field, update the cluster UID (you retrieved this in step 1) and unstretch JSON file with the payload you prepared in step 2a.
- 2 Click **Execute**.

The unstretch cluster task is displayed in the SDDC Manager task panel.

- 3 Monitor the unstretch cluster task till it is completed.

All hosts from AZ2 are removed from the unstretched cluster and cluster is converted to standard vSAN cluster.

## Replace a Failed Host in a Stretched Cluster

If a host or host component in a stretched cluster fails, it is recommended that you replace the host with a new host.

### Prerequisites

- Image the replacement host with the same ESXi version as the other hosts in the cluster.
- Check the health of the cluster.

See "Check vSAN Health" in *Administering VMware vSAN*.

### Procedure

- 1 Get the ID of the host to be removed.
  - a On the SDDC Manager Dashboard, click **Developer Center > API Explorer**.
  - b Under APIs for managing hosts, click **GET /v1/hosts**.
  - c Click **Execute**.

- d Click **Download** to download the JSON file.
  - e Open the JSON file and copy the the ID of the host to be removed.
- 2 Get the ID of the cluster from where the host is to be removed.
- a In the API Explorer, navigate to APIs for managing clusters and click `GET /v1/clusters`.
  - b Click **Execute**.
  - c Click **Download** to download the JSON file.
  - d Open the JSON file and copy the the cluster ID.
- 3 Run the compact cluster API.
- a Prepare the JSON request body.
    - 1 Click `Patch /v1/clusters/id`.
    - 2 Under `ClusterUpdateSpec`, click **Cluster Update Data ClusterUpdateSpec{ ... }**.
    - 3 Click **Download** to download the JSON file.
    - 4 Edit the JSON file so that it contains only the compact section similar to the example below.

```
{
  " clusterCompactionSpec": {
    "hosts": [ {
      "id": "2c1744dc-6cb1-4225-9195-5cbd2b893be6"
    }, {
      "id": "6b38c2ea-0429-4c04-8d2d-40a1e3559714"
    }, {
      "id": "5b704db6-27f2-4c87-839d-95f6f84e2fd0"
    } ]
  }
}
```

- 5 In the `id` field, replace the values with the host IDs you retrieved in step 1.
  - 6 Click **Execute**.
- The compact cluster task is displayed in the SDDC Manager task panel.
- 7 Monitor the task till it is completed.
- 4 Decommission the host to be removed.
- See [Decommission Hosts](#).
- 5 Commission the replacement host to the same network pool as the removed host.
- See [Commission Hosts](#) .
- 6 Expand the cluster to add the commissioned host to the cluster. See [Expand a Stretched Cluster](#).

- 7 If required, SSH in to each newly added host and add a static route to the vSAN network of the witness host. Also add static routes in the witness if it could not reach the vSAN network of the newly added hosts.

### Results

vSAN automatically rebuilds the stretch cluster.

## Change the vSAN Witness Host in a Stretched Cluster

You can replace or change the vSAN witness host for a stretched cluster using the vSphere Client without affecting life cycle operations of SDDC Manager.

### Prerequisites

Verify that the vSAN witness host is not in use by another cluster, has a VMkernel configured for vSAN traffic, and has no vSAN partitions on its disks.

### Procedure

- 1 In a web browser, log in to vCenter Server at `https://vcenter_server_fqdn/ui`.
- 2 Select **Menu > Hosts and Clusters**.
- 3 In the inventory panel, expand **vCenter Server > Datacenter**.
- 4 Select the stretched cluster and click **Configure**.
- 5 Under vSAN, click **Fault Domains**.
- 6 Click the **Change** button.
- 7 Select a new host to use as the vSAN witness host and click **Next**.
- 8 Claim disks on the new witness host and click **Next**.
- 9 Review the configuration and click **Finish**.

# Composability Management

# 16

With composability, you can dynamically configure servers to meet the needs of your workloads without physically moving any hardware components. You bind disaggregated hardware components (compute, network, storage, and offload components) together to create a logical system based on the needs of your applications. These logical systems function like traditional rack mount systems.

The VMware Cloud Foundation composability feature is available for HPE Synergy and Dell MX servers and uses the Redfish translation layer to connect to the composable hardware infrastructure. Redfish Translation Layer supports data models used to get composable resources and zones restrictions from the hardware infrastructure. It is designed to be extensible and vendor agnostic. You must obtain and install the Redfish appliance from the composable hardware vendor.

It is recommended that you compose and decompose servers only through VMware Cloud Foundation, and not through the vendor software.

---

**Note** Ensure that you follow the restriction on storage sled placement on Dell MX servers. Refer to vendor documentation for more information.

---

This chapter includes the following topics:

- [Configure Translation Layer](#)
- [Compose a Server](#)
- [View Composability Information](#)
- [Add Storage](#)
- [Remove Storage](#)
- [Decompose a Server](#)

## Configure Translation Layer

Redfish translation layer is the interface between SDDC Manager and hardware vendor. You must configure this translation layer by providing the Redfish translation layer URL and credentials.



## Procedure

- 1 As a best practice, increase the queue capacity for the thread pool.

- a Open the `application.properties` file:

```
vi /etc/vmware/vcf/operationsmanager/application.properties
```

- b Update the queue capacity line as follows:

```
om.executor.queuecapacity=300
```

- c Save and close the file.

- 2 If you are using a self-signed certificate, import the Redfish certificate from the Redfish VM to SDDC Manager VM by following the steps below. If you are using a CA signed certificate, skip to step 3.

- a Using SSH, log in to the SDDC Manager VM with the following credentials:

User name: `vcf`

Password: use the password specified in the deployment parameter workbook.

- b Enter `su` to switch to the `root` user.

- c Import the Redfish certificate from the Redfish VM to SDDC Manager VM by running the following command:

```
/opt/vmware/vcf/commonsvcs/scripts/cert-fetch-import-refresh.sh --ip=redfish-FQDN --port=port --service-restart=operationsmanager
```

Replace *redfish-FQDN* with the translation layer FQDN. Replace *port* with the TLS/SSL port.

The output displays information about the certificate to import including owner, issuer, serial number, validity, certificate fingerprints (md5, sha1, or sha256), signature algorithm name, subject, public key algorithm, and version. Verify this information.

- d Answer the prompt.

Operations Manager is restarted. Wait for a few minutes and then proceed to step 4.

- 3 Restart Operations Manager:

```
systemctl restart operationsmanager
```

Wait for a few minutes before proceeding to the next step.

- 4 On the SDDC Manager Dashboard, click **Administration > Composable Infrastructure**.
- 5 Enter the URL for the Redfish translation layer.
- 6 Enter the user name and password for the Redfish translation layer.
- 7 Click **Connect**.

## Compose a Server

You can compose one or more servers by selecting the compute, network, and storage resources.

### Prerequisites

- The translation layer must have been configured.
- The composed server must meet the minimum hardware requirements. See the *Planning and Preparation Workbook*.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Administration > Composable Infrastructure**.
- 2 From the Available Resources table, select the zone where you want to compose a server. A zone corresponds to a physical boundary.
- 3 Click **Compose**.
- 4 In the Allocate Resources dialog box, select the compute for the server.
- 5 Select the storage.
- 6 Select the network interface.

The Choose number of servers section displays the number of servers you can compose based on the selected resources.

- 7 Select the number of servers you want to compose.
- 8 Click **Next**.
- 9 On the Review page, review the allocated resources to the servers.  
Click **Back** to make any changes.
- 10 Click **Compose**.

### Results

The compose server task is displayed in the Tasks table at the bottom of the Composable Infrastructure page. Click the name of the task for more information. When the server is composed, it is added to the Server Composition Summary table.

If VMware Cloud Foundation does not receive a response from Redfish due to an external error, an error message is displayed. The hardware resources in the compose request are locked and cannot be used. You must free up these resources using the vendor UI. For more information, refer to the vendor documentation.

### What to do next

- 1 Image the composed servers. See [Chapter 6 Prepare ESXi Hosts for VMware Cloud Foundation](#).
- 2 Commission the composed servers. See [Commission Hosts](#).

## View Composability Information

The Composable Infrastructure page displays information about available resources and composed servers.

### Procedure

- ◆ On the SDDC Manager Dashboard, click **Administration > Composable Infrastructure**.

The Composable Infrastructure page appears. The Redfish translation layer information is displayed on the top of the page.

The Available Resources table displays the available zones and computer, storage, and network information available in each zone.

The Server Composition Summary table displays the composed servers.

The task panel at the bottom of the page shows the tasks performed and their status.

## Add Storage

You can add storage to Dell MX composed servers.

### Prerequisites

The server you are adding storage to must be unassigned.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Administration > Composable Infrastructure**.
- 2 In the Composed Servers section, click the three dots next to the server you want to add storage to and click **Add Storage**.  
  
The Allocate Storage dialog box displays the composed server details. Hovering over the Information icon next to the Current Storage field displays the SSD and HDD details of the server.
- 3 In the Add to Current Storage section, select the storage units you want to add and click **Next**.
- 4 On the Review page, verify the storage you are adding and click **Add**.

## Remove Storage

You can remove storage units from a Dell MX composed server.

### Prerequisites

The server you are removing storage from must be unassigned.

### Procedure

- 1 On the Composable Infrastructure page, click the three dots next to the server you want to remove storage from.
- 2 Click **Remove Storage**.
- 3 For the storage type you want to remove, set the Remove from Allocated value to the appropriate value.
- 4 Click **Next**.
- 5 On the Review page, verify the storage you are removing and click **Remove**.

## Decompose a Server

You can decompose a server that has not been assigned to a VI workload domain.

### Prerequisites

The server to be decomposed must be unassigned.

### Procedure

- 1 On the SDDC Manager Dashboard, click **Administration > Composable Infrastructure**.
- 2 From the Server Composition Summary table, select the server to be decomposed.
- 3 Click **Decompose**.
- 4 In the Decompose Servers dialog box, click **Decompose**.

# Monitoring Capabilities in the VMware Cloud Foundation System

17

The VMware Cloud Foundation system provides built-in capabilities to help you perform effective operations monitoring, troubleshooting, performance management, infrastructure capacity planning, and compliance monitoring and auditing.

You use the built-in monitoring capabilities for these typical scenarios.

Scenario	Examples
Are the systems online?	A host or other component shows a failed or unhealthy status.
Why did a storage drive fail?	Hardware-centric views spanning inventory, configuration, usage, and event history to provide for diagnosis and resolution.
Is the infrastructure meeting tenant service level agreements (SLAs)?	Analysis of system and device-level metrics to identify causes and resolutions.
At what future time will the systems get overloaded?	Trend analysis of detailed system and device-level metrics, with summarized periodic reporting.
What person performed which action and when?	History of secured user actions, with periodic reporting. Workflow task history of actions performed in the system.

The monitoring capabilities involve these features:

This chapter includes the following topics:

- [Viewing Tasks and Task Details](#)

## Viewing Tasks and Task Details

From the SDDC Manager Dashboard, you can access all tasks. By default, the Dashboard displays the Recent Tasks widget, providing general information at a glance about the most recent tasks. A task is a unit of work or a series of subtasks that perform an overall goal, such as creating a workload domain.

In addition to the most recent tasks, you can view and search for all tasks by clicking **View All Tasks** at the bottom of the Recent Tasks widget. This opens the Tasks panel.

**Note** For more information about controlling the widgets that appear on the Dashboard page of the SDDC Manager Dashboard, see [Tour of the SDDC Manager User Interface](#).

## Viewing and Filtering Task Details

The Tasks panel provides a high level view all tasks, displaying the descriptive task name, task status (for example, running, succeeded, or failed), and the timestamp for the last change in task status. You can also filter and search the task information as follows:

- Search tasks by clicking the filter icon in the Task column header and entering a search string.
- Filter tasks by status by clicking the filter icon in Status column. Select by category **All**, **Failed**, **Successful**, **Running**, or **Pending**.

---

**Note** Each category also displays the number of tasks with that status.

---

- Clear all filters by clicking **Reset Filter** at the top of the Tasks panel.
- Click **Refresh** to refresh the task list.

---

**Note** You can also sort the table by the contents of the Status and Last Occurrence columns.

---

## Managing Tasks and Subtask Details

Expand a task to view details including the subtasks that comprise the task and their individual statuses.

- If a task is in a Failed state, you can also attempt to restart it by clicking **Restart Task**.

---

**Note** Not all tasks are restartable.

---

- If a task is in a Failed state, click on the icon next to the Failed status to view a detailed report on the cause.
- To view subtasks and their details, click **View Subtasks**.

---

**Note** You can filter subtasks in the same way you filter tasks.

---

---

**Note** You can also sort the table by the contents of the Status and Last Occurrence columns.

---

## Resizing the Task Panel

Use the icons on the task panel to increase or decrease the panel size, or to close or reopen it.

# Updating Cloud Foundation DNS and NTP Servers

# 18

If you need to make changes to the DNS or NTP server information that you provided during VMware Cloud Foundation bring-up, you can use the VMware Cloud Foundation API to update the servers.

When you initially deploy VMware Cloud Foundation, you complete the deployment parameter workbook to provide the system with the information required for bring-up. This includes up to two DNS servers and up to two NTP servers. You can change this server information at a later date, using the VMware Cloud Foundation API.

This chapter includes the following topics:

- [Update DNS Server Configuration](#)
- [Update NTP Server Configuration](#)

## Update DNS Server Configuration

Use this procedure to update the DNS server information that you provided during VMware Cloud Foundation bring-up.

VMware Cloud Foundation uses DNS servers to provide name resolution for various components in the system. You must provide root DNS domain information. Optionally, you can provide subdomain information. When you update the DNS server configuration, VMware Cloud Foundation updates the components in a specific order:

- SDDC Manager
- vCenter Servers
- ESXi hosts
- NSX-T Managers
- NSX-T Edge nodes
- vRealize Suite Lifecycle Manager
- vRealize Log Insight
- vRealize Operations
- vRealize Automation

If the update fails, SDDC Manager rolls back the DNS settings for the failed component. Fix the underlying issue and retry the update starting with the failed component.

**Note** There is no rollback for vRealize Suite Lifecycle Manager. Check the logs, resolve any issues, and retry the update.

Updating the DNS server configuration can take some time to complete, depending on the size of your environment. Schedule DNS updates at a time that minimizes the impact to the system users. This procedure uses the Cloud Foundation API, which is secured by token-based authentication.

### Prerequisites

- Ensure that both forward and reverse DNS resolution is functional for each component using the updated DNS server.
- The new DNS server should be reachable from the VMware Cloud Foundation components.
- All VMware Cloud Foundation components should be reachable from SDDC Manager.
- All VMware Cloud Foundation components must be in an `Active` state.

## Procedure

- 1 To obtain an access token, run the following command:

```
curl 'https://SDDC_MANAGER_IP/v1/tokens' -k -X POST -H 'Content-Type: application/json' -H 'Accept: application/json' -d '{"username" : "user name", "password" : "user password"}'
```

Replace the SDDC Manager IP address, user name, and password with the information for your environment.

The command returns an access token and a refresh token.

[illegible]

- 2 Get the current DNS server configuration information.

```
curl 'https://SDDC_MANAGER_IP/v1/system/dns-configuration' -k -X GET -H "Content-Type:  
application/json" -H "Authorization: Bearer  
eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiI2ZGRmZmUzMCM0ZzZGEwLTQ5NmUtOTQzMCIhOGNkNTQ0YTktZGMiLCJpYXQiOiJlODU3ODE3ODcsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbiCIslmlzcyl6InZjZilhdXRoIiwiaXYXVki  
joic2RkYy1zZXZlbnNlcysIm5iziI6MTU0NTc4MTC4NywiZCJxZWljoxNtq1Nzg1Mzg3LCAj1c2VyIjoyYWRtaW5pc3Ry
```



YXRvckB2c3BoZXJlLmxvY2YsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsInNjb3BlIjpbIkK  
BQ0tVUF9DT05GSUdfUkVBRClSIkNSRURFTlRJRQXfUkVBRClSIiVTRVJfVlJJVEUiLCJPVEhFUl9XUklURSIkJBQ0  
tVUF9DT05GSUdfVlJJVEUiLCJPVEhFUl9SRUFEIiwiVFNFUl9SRUFEIiwiQ1JFREVOVElBTf9XUklURSIjdfQ.WCpUPR  
Im5A6X 406HTJF7TbTsa0g9l\_AQbt7OcBPblm"

- 3 Validate the new DNS server configuration information.

```
curl -H "Authorization: Bearer eyJhbGciOiJIUUC00NGQwLTQ5MzYtYjYqWMC0xMzc5NzMyMjdmOWUiLCJpYXQiOjE0ODU3ODQ5MTgsInN1YiI6ImFkbWl  
uaXN0cmF0b3BAdnNwaGVyZS5sb2NhbcIsImVudCI6Im9ja3RkYyZm9kaWwucmVudCIsIm54IjoiIjE6MTU4NTc4NDKxOCwiZXBhbnVjoxtg1Nzg4NTE4LClc1c2VyIjoiYWRTaW5wc3RyYXRvckB2c3BoZXJlLmxvY2FsIiwib  
mFtZI2Si6ImFkbWluaXN0cmF0b3BAdnNwaGVyZS5sb2NhbcIsInNjb3BlIjpjbIkJBQ0tVUF9DT05GSUdfUkVBRCSikNS  
RURFTlRJQUxfUkVBRCSilVTRVJfvlJJVEUilCJPVEhfUL9XUKlURSIsIkJBQ0tVUF9DT05GSUdfvJJVEUilCJPVEh  
FUL9SRUFEIiwiVVNFUL9SRUFEIiwiQ1JFREVOVELBTf9XUklURSIdfQ.Ya4XszntsRHUZFRBNKGy7Js6xrGYGe8KdgJ  
2QbihFmg" -H 'Content-Type: application/json' -k -X POST https://SDDC_MANAGER_IP/v1/system/  
dns-configuration/validations -d '{"dnsServers":[{"ipAddress":"<dns-server-  
ip>","isPrimary":true}]}' | jq .pp
```

Replace `<dns-server-ip>` with the IP address of the new DNS server. Specify `true` or `false` for `isPrimary`, depending on whether or not the new DNS server is the primary DNS server.

Note the *<id>* that gets returned.

The validator verifies forward and reverse name resolution for VMware Cloud Foundation components using the new DNS server.

4 Monitor the status of the validation task.

```
curl -H "Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiIxNzMyYThmOC00NGQwLTQ5MzYtYjJqWmC0xMzc5NzMyMjdmOWUiLCJpYXQiOiE1ODU3ODQ5MTgsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbmCIslmZcyI6InZjZilhdXRoIiwiaXYXVkaioic2RkYy1zZXZlIiwibmlycysIm5iziI6MTU4NTc4NDkxOCwiZXhwIjoxtNg4NTE4LCJlc2VyIjoiYWRTaW5pc3RyYXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbmCIslmNjb3BlIjpjbIkjBQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfvlJJVEUilCJPVEhfUL9XUKlURSIslkJBQ0tVUF9DT05GSUdfVLJJVEUilCJPVEhfUL9SRUFEIiwivVNful9SRUFEIiw1JFREVOVELBTf9XUKlURSJdfQ.Ya4XSzntsRHUZFRBNKGY7Js6xrGYGe8KdgJ2QbihFmg" -H 'Content-Type: application/json' -k -X GET https://SDCC_MANAGER_IP/v1/system/dns-configuration/validations/<id>|json_pp
```

Replace *<id>* with the ID from the previous step.

If validation succeeds, you can proceed to change the DNS server configuration. If validation fails, correct any issues and try again.

**5** Change the DNS server configuration information.

```
curl -H "Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiIxNzMyYThmOC00NGQwLTQ5MzYtYjJqWmC0xMzc5NzMyMjdmdWOUiLCJpYXQiOjE1ODU3ODQ5MTgsInNlYiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbmCIslmlycyI6InZjZilhdXRoIiwiaXYXVkiOiJoic2RkYy1zZXJ2aWNlcysIm5iZiI6MTU4NTc4NDkxOCwiZXhwIjoxtNgTlNzg4NTE4LClc1c2VyIjoiyWRtaW5pc3RyYXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbmCIslbnjb3BlIjpjbIkjBQ0tVUF9DT05GSudfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfv1JJVEUiLCJPVEhfUL9XUklURSIsIkJBQ0tVUF9DT05GSudfV1JJVEUiLCJPVEhfUL9SRUFEIiwivVNfUL9SRUFEIiw1Q1JFREVOVELBTf9XUklURSJdfQ.Ya4XsZntsRHUZFRBNKGY7Js6xrGYGe8KdgJ2QbihFmg" -H 'Content-Type: application/json' -k -X PUT https://SDDC_MANAGER_IP/v1/system/dns-configuration -d '{"dnsServers":[{"ipAddress":"<dns-server-ip>", "isPrimary":true}]}' | json_pp
```

Replace *<dns-server-ip>* with the IP address of the new DNS server. Specify `true` or `false` for `isPrimary`, depending on whether or not the new DNS server is the primary DNS server.

Note the `<id>` that gets returned.

## 6 Track the status of the DNS update.

[illegible]

Replace `<id>` with the ID from the previous step. Wait for the task to complete.

7 Verify that the DNS configuration was updated.

```
curl 'https://SDDC_MANAGER_IP/v1/system/dns-configuration' -k -X GET -H "Content-Type: application/json" -H "Authorization: Bearer eyJhbGciOiJIUzI1Ni9y.eyJqdGkiOiI2ZGRmZmUzMCM0zZGEwLTQ5NmUtOTQzMCIhOGNkNTQ0YTk2ZGMiLCJpYXQiOiE1ODU3ODE3ODcsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbcIsImlzcYi6InZjZilhdXR0IiwiaXYXkiOiJC2RkYylzZXJ2aWNlcysIm5iziI6MTU0NTc4Mtc4NywiZXBwIjoibG9jaWZmZGZ3LjCjE2V2YjoiYWRTaW5pc3RyYXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbcIsInNjb3BlIjpjbKJBQ0tVUF9DT05GSUdfUkVBRCIsIkNSURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhfU19XUklURSIsIkJBQ0tVUF9DT05GSUdfV1JJVEUiLCJPVEhfU19SRUFEIiwiaWF0IjE5OTU0MDA0MCB8Im5kaWE6X406HTJF7TbTsao91AQbt70cBPblM"
```

## Update NTP Server Configuration

Use this procedure to update the NTP server information that you provided during VMware Cloud Foundation bring-up.

VMware Cloud Foundation uses NTP servers to synchronize time between the various components in the system. You must have at least one NTP server. When you update the NTP server configuration, VMware Cloud Foundation updates the components in a specific order:

- SDDC Manager
- vCenter Servers
- ESXi hosts
- NSX-T Managers
- NSX-T Edge nodes
- vRealize Suite Lifecycle Manager
- vRealize Log Insight
- vRealize Operations

- vRealize Automation

If the update fails, SDDC Manager rolls back the NTP settings for the failed component. Fix the underlying issue and retry the update starting with the failed component.

**Note** There is no rollback for the vRealize Suite Lifecycle Manager. Check the logs, resolve any issues, and retry the update.

Updating the NTP server configuration can take some time to complete, depending on the size of your environment. Schedule NTP updates at a time that minimizes the impact to the system users.

This procedure uses the Cloud Foundation API, which is secured by token-based authentication.

### Prerequisites

- Any new NTP server is reachable by all components.
- Time skew between new NTP servers is less than 5 minutes.

## Procedure

- 1 To obtain an access token, run the following command:

```
curl 'https://SDDC_MANAGER_IP/v1/tokens' -k -X POST -H 'Content-Type: application/json' -H 'Accept: application/json' -d '{"username" : "user_name", "password" : "user_password"}'
```

Replace the SDDC Manager IP address, user name, and password with the information for your environment.

The command returns an access token and a refresh token.

[illegible]

- 2 Get the current NTP server configuration information.

```
curl 'https://SDDC_MANAGER_IP/v1/system/ntp-configuration' -k -X GET -H "Content-Type: application/json" -H "Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiI2ZGRmZmU3MC0zZGEwLTQ5NmUtOTQzMCIhOGNkNTQ0YTk2ZGMiLCJpYXQiOiJlODU3ODE3ODcsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbnCI8mlzczyI6InZjZilhdXR0eIIiwYXVkiOjoic2RkYyIzXXZl2aWNlcysIm5iZiI6MTU4NTc4MTC4NywiZXhwIjoxNzg1Mzg3LCljc2VyIjoiYWYWRtaW5pc3RyYXRvcnB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbnCI8InNjb3BlIjpjbikJBQ0tVUF9DT05GSudfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVFvIjV1JJEVEUI8LClJPVEhfU19XUklURSIsIkJBQ0tVUF9DT05GSudfV1JJVEVEULClJPVEhfU19SRUFEIiwivVNlU19SRUFEIiwq1JFREVOVElBTf9XUklURSJdfQ.WCpUPRI8A6X 406HTJF7TbTSa0q91 AQt7OcBPblM"
```

- 3 Validate the new NTP server configuration information.

```
curl -H "Authorization: Bearer eyJhbGciOiJIUC00NGQwLTQ5MzYtYjQwMC0xMzc5NzMyMjdmOWUiLCJpYXQiOjE0ODU3ODQ5MTgsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbmVzcyI6InZjZilhdXRoIiwiaXYXkiOiJCkRkYyZlZXJ2aWNlcysIm5iZiI6MTU0NTc4NDkxOCwiZXBhbnVjoxtNg4NTE4LClc1c2VyIjoiYWRTaW5pc3RyYXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbmVzcyI6InNjb3B1IjpjbikJBQ0tVUF9DT05GSUdfUkVBRCSIkNSRURFTlRJQUxfUkVBRCSIlVTRVJfvlJJVEUilCJPVEhfUl9XUklURSIsIkJBQ0tVUF9DT05GSUdfvJJVEUilCJPVEhfUl9SRUFEIiwiVVNFUL9SRUFEIiwiQ1JFREVOVELBTf9XUklURSIdfQ.Ya4XsZntsRHUZFRBNKGy7Js6xrGYGe8KdgJ2QbihFmg" -H 'Content-Type: application/json' -k -X POST https://SDDC_MANAGER_IP/v1/system/ntp-configuration/validations -d '{"ntpServers":[{"ipAddress":"<ntp-server-ip>}"]}' | json_pp
```

Replace `<ntp-server-ip>` with the IP address of the new NTP server. To enter multiple NTP servers, use the following format: `{"ntpServers":[{"ipAddress":"<ntp-server-ip-1>"}, {"ipAddress":"<ntp-server-ip-2>"}]}`.

Note the *<id>* that gets returned.

The validator verifies that the VMware Cloud Foundation components can communicate with the new NTP server.

4 Monitor the status of the validation task.

```
curl -H "Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiIxNzMyYThmOC00NGQwLTQ5MzYtYjJqWmC0xMzc5NzMyMjdmOWUiLCJpYXQiOjE1ODUzODQ5MTgsInNlYiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbmCIslmZcyI6InZjZilhdXRoIiwiaXYXVkaioic2RkYyIzZXZlIiwibmlyIsIm5iZiI6MTU0NTc4NDkxOCwiZXhwIjoxtNgTlNzg4NTE4LClc1c2VyIjoieWRtaW5pc3RyYXRvckB2c3BoZXJlImxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbmCIslm5jb3BlIjpjbIkjBQ0tVUF9D0T05GSudfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfv1JJVEUiLCJPVEhfUL9XUklURSIsIkJBQ0tVUF9D0T05GSudfV1JJVEUiLCJPVEhfUL9SRUFEIiwivVNfUL9SRUFEIiw1Q1JFREVOVELBTf9XUklURSJdfQ.Ya4XsZntsRHUZFRBNKGY7Js6xrGYGe8KdgJ2QbihFmg" -H 'Content-Type: application/json' -k -X GET https://SDCC_MANAGER_IP/v1/system/ntp-configuration/validations/<id>|json pp
```

Replace *<id>* with the ID from the previous step.

If validation succeeds, you can proceed to change the NTP server configuration. If validation fails, correct any issues and try again.

**5** Change the NTP server configuration information.

```
curl -H "Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiIxNzMyYThmOC00NGQwLTQ5MzYtYjJqWmC0xMzc5NzMyMjdmOWUiLCJpYXQiOjE1ODU3ODQ5MTgsInNlYiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbmCIslmlycyI6InZjZilhdXRoIiwiaXYXVkiOiJoic2RkYy1zZXJ2aWNlcysIm5iZiI6MTU4NTc4NDkxOCwiZXhwIjoxtNg1Nzg4NTE4LClc2VyIjoyYWRTaW5pc3RyYXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbmCIslbnjb3BlIjpjbIkjBQ0tVUF9DT05GSudfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfv1JJVEUiLCJPVEhfUL9XUklURSIsIkJBQ0tVUF9DT05GSudfV1JJVEUiLCJPVEhfUL9SRUFEIiwivVNfUL9SRUFEIiw1Q1JFREVOVELBTf9XUklURSJdfQ.Ya4xsZntsRHUZFRBNKGY7Js6xrGYGe8KdgJ2QbihFmg" -H 'Content-Type: application/json' -k -X PUT https://SDDC_MANAGER_IP/v1/system/ntp-configuration -d '{"ntpServers":[{"ipAddress":"<ntp-server-ip>}]}' | json_pp
```

Replace `<ntp-server-ip>` with the IP address of the new NTP server. To enter multiple NTP servers, use the following format: `{"ntpServers":[{"ipAddress": "<ntp-server-ip-1>"}, {"ipAddress": "<ntp-server-ip-2>"}]}`.

Note the *<id>* that gets returned.

- 6 Track the status of the NTP update.

```
curl -H "Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiIxNm5YThmOC00NGQwLTQ5MzYtYjJqWMC0xMzc5NzMyMjdmOWUiLCJpYXQiOiE1ODU3ODQ5MTgsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbmCIslmVycyI6InZjZilhdXRoIiwiaXYXkKIjoic2RkYy1zZXJ2aWNlcysIm5iziI6MTU4NTc4NDkxOCwiZXhwIjoxNtg1Nzg4NTE4LCJ1c2VyIjoiYWRTaW5wc3RyYXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbmCIslmVycyI6InNjb3BlIjpjbIkjBQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhfU19XUKlURSIsIkJBQ0tVUF9DT05GSUdfV1JJVEUiLCJPVEhfU19SRUFEIiwivVNfU19SRUFEIiw1JFREVOVElBTf9XUklURSIdfQ.Ya4xsZntsRHUZFRBNKGY7Js6xrGYGe8KdgJ2QbihFmg" -H 'Content-Type: application/json' -k -X GET https://SDDC_MANAGER_IP/v1/tasks/<id>|json_pp
```

Replace `<id>` with the ID from the previous step. Wait for the task to complete.

7 Verify that the NTP configuration was updated.

```
curl -H "https://SDDC_MANAGER_IP/v1/system/ntp-configuration" -k -X GET -H "Content-Type: application/json" -H "Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiI2ZGRmZmUzMCM0zZGEwLTQ5NmUtOTQzMCIhOGNkNTQ0YTtk2ZGMiLCJpYXQiOiJlODU0ODE3ODcsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbcIsImVzcyI6InZjZilhdXRoIiwiaXVkaWoiOiJlc3R5YXRvcnB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbcIsInNjb3BlIjpjbIkjBQ0tVUF9D0T05GSudfUkVBRCIsIkNSRURFTlRJQUxkfUkVBRCIsIlVTRVJfv1JJVEUiLCJPVEhfU19XUklURSIsIkJBQ0tVUF9D0T05GSudfV1JJVEUiLCJPVEhfU19SRUFEIiwivVNfU19SRUFEIiwq1JFREVOVELBTf9XUklURSjdFQ.WCPUPRIm5A6X 406HTJF7TbTSa0g91 AQbt7OcBPblM"
```

# Supportability and Serviceability (SoS) Utility

# 19

The SoS utility is a command-line tool that you can use to run health checks, collect logs for VMware Cloud Foundation components, and so on.

To run the SoS utility, SSH in to the SDDC Manager VM using the **vcf** user account. For basic operations, enter the following command:

```
sudo /opt/vmware/sddc-support/sos --option-1 --option-2 --option-3 ... --option-n
```

To list the available command options, use the **--help** long option or the **-h** short option.

```
sudo /opt/vmware/sddc-support/sos --help
sudo /opt/vmware/sddc-support/sos -h
```

---

**Note** You can specify options in the conventional GNU/POSIX syntax, using **--** for the long option and **-** for the short option.

---

For privileged operations, enter **su** to switch to the root user, and navigate to the `/opt/vmware/sddc-support` directory and type `./sos` followed by the options required for your desired operation.

This chapter includes the following topics:

- [SoS Utility Options](#)
- [Collect Logs for Your VMware Cloud Foundation System](#)

## SoS Utility Options

This section lists the specific options you can use with the SoS utility.

### SoS Utility Help Options

Use these options to see information about the SoS utility itself. For these options, SSH in to the SDDC Manager VM using the **vcf** user account and enter the following command:

```
sudo /opt/vmware/sddc-support/sos --option-name
```

Enter the **vcf** password when prompted.

Option	Description
--help -h	Provides a summary of the available SoS utility options
--version -v	Provides the SoS utility's version number.

## SoS Utility VMware Cloud Foundation Summary Options

These options provide information about the Cloud Foundation system and tasks. For these options, SSH in to the SDDC Manager VM using the **vcf** user account and enter the following command:

```
sudo /opt/vmware/sddc-support/sos --option-name
```

Enter the **vcf** password when prompted.

Option	Description
--get-vcf-summary	Returns information about your Cloud Foundation system, including CEIP, domains and clusters, hosts, licensing, network pools, SDDC Manager, and VCF services.
--get-vcf-services-summary	Returns information about SDDC Manager uptime and when Cloud Foundation services (for example, LCM) started and stopped.
--get-vcf-tasks-summary	Returns information about Cloud Foundation tasks, including the time the task was created and the status of the task.

## SoS Utility Generic Options

These are generic options for the SoS utility. For these options, SSH in to the SDDC Manager VM using the **vcf** user account and enter the following command:

```
sudo /opt/vmware/sddc-support/sos --option-name
```

Enter the **vcf** password when prompted.

**Note** For generic options related to log collection, see [Collect Logs for Your VMware Cloud Foundation System](#).

Option	Description
--configure-sftp	Configures SFTP for logs.
--debug-mode	Runs the SoS utility in debug mode.

Option	Description
<code>--domain-name DOMAINNAME</code>	Specify the name of the workload domain name on which the SoS operation is to be performed. To run the operation on all domains, specify <code>--domain-name ALL</code> .  <b>Note</b> If you omit the <code>--domain-name</code> flag and domain name, the SoS operation is performed only on the management domain.
<code>--force</code>	Allows SoS operations to be formed while workflows are running.  <b>Note</b> It is recommended that you do not use this option.
<code>--history</code>	Displays the last 20 SoS operations performed.
<code>--ondemand-service</code>	Include this flag to execute commands on all ESXi hosts in a domain.  <b>Warning</b> Contact VMware support before using this option.
<code>--ondemand-service JSON file path</code>	Include this flag to execute commands in the JSON format on all ESXi hosts in a domain. For example, <code>/opt/vmware/sddc-support/&lt;JSON file name&gt;</code>
<code>--setup-json SETUPJSON</code>	Custom setup-json file for log collection. SoS prepares the inventory automatically based on the environment where it is running. If you want to collect logs for a pre-defined set of components, you can create a <code>setup.json</code> file and pass the file as input to SoS. A sample JSON file is available on the SDDC Manager VM in the <code>/opt/vmware/sddc-support/</code> directory.
<code>--skip-known-host-check</code>	Skips the specified check for SSL thumbprint for host in the known host.
<code>--zip</code>	Creates a zipped TAR file for the output.

## SoS Utility Options for Health Check

These SoS commands are used for checking the health status of various components or services, including connectivity, compute, storage, database, domains, and networks. For these options, SSH in to the SDDC Manager VM using the **vcf** user account and enter the following command:

```
sudo /opt/vmware/sddc-support/sos --option-name
```

Enter the **vcf** password when prompted.

A green status indicates that the health is normal, yellow provides a warning that attention might be required, and red (critical) indicates that the component needs immediate attention.

Option	Description
<code>--json-output-dir JSONDIR</code>	Outputs the results of any health check as a JSON file to the specified directory, <code>JSONDIR</code> .
<code>--certificate-health</code>	Verifies that the component certificates are valid (within the expiry date).
<code>--connectivity-health</code>	Performs a connectivity health check to inspect whether the different components of the system such as the ESXi hosts, vCenter Servers, NSX Managers, and SDDC Manager can be pinged.



Option	Description
<code>--composability-infra-health</code>	Performs an API connectivity health check of the composable infrastructure. If no composable infrastructure exists, this flag is ignored. If found, the utility checks connectivity status through the composable infrastructure API, such as Redfish.
<code>--compute-health</code>	Performs a compute health check, including ESXi host licenses, disk storage, disk partitions, and health status.
<code>--dns-health</code>	Performs a forward and reverse DNS Health Check.
<code>--general-health</code>	Checks ESXi for error dumps and gets NSX Manager and cluster status.
<code>--get-host-ips</code>	Returns host names and IP addresses of ESXi hosts.
<code>--get-inventory-info</code>	Returns inventory details for the Cloud Foundation components, such as vCenter Server NSX, SDDC Manager, and ESXi hosts. Optionally, add the flag <code>--domain-name ALL</code> to return all details.
<code>--hardware-compatibility-report</code>	Validates ESXi hosts and vSAN devices and exports the compatibility report.
<code>--health-check</code>	Performs all available health checks.
<code>--ntp-health</code>	Verifies whether the time on the components is synchronized with the NTP server in the SDDC Manager VM. It also ensures that the hardware and software time stamp of ESXi hosts are within 5 minutes of the SDDC Manager VM.
<code>--password-health</code>	Returns the status of all current passwords, such as Last Changed Date, Expiry Date, and so on.
<code>--services-health</code>	Performs a services health check to confirm whether services within the SDDC Manager (like Lifecycle Management Server) and vCenter Server are running.
<code>--storage-health</code>	Performs a check on the vSAN disk health of the ESXi hosts and vCenter clusters. Also runs proactive vSAN tests to verify the ability to create VMs within the vSAN disks.
<code>--run-vsan-checks</code>	Runs proactive vSAN tests to verify the ability to create VMs within the vSAN disks.

## SoS Utility Options for Managing ESXi Hosts

Use these options to manage ESXi hosts, including enabling SSH and locking down hosts. For these options, SSH in to the SDDC Manager VM using the **vcf** administrative user account, enter **su** to switch to the root user, navigate to the `/opt/vmware/sddc-support` directory, and type the following command:

```
./sos --option-name
```

Option	Description
<code>--disable-lockdown-esxi</code>	<p>Deactivate lockdown mode on ESXi nodes in the specified domains.</p> <ul style="list-style-type: none"> <li>■ To deactivate lockdown on ESXi nodes in a specific domain, include the flag <code>--domain-name DOMAINNAME</code>.</li> <li>■ To deactivate lockdown on ESXi nodes in all domains, include the flag <code>--domain-name ALL</code>.</li> </ul> <p><b>Note</b> If you do not specify domain, this command affects only the MGMT domain by default.</p>
<code>--enable-lockdown-esxi</code>	<p>Enables lockdown mode on ESXi nodes in the specified domains.</p> <ul style="list-style-type: none"> <li>■ To enable lockdown on ESXi nodes in a specific domain, include the flag <code>--domain-name DOMAINNAME</code>.</li> <li>■ To enable lockdown on ESXi nodes in all domains, include the flag <code>--domain-name ALL</code>.</li> </ul> <p><b>Note</b> If you do not specify domain, this command affects only the MGMT domain by default.</p>
<code>--disable-ssh-esxi</code>	<p>Deactivate SSH on ESXi nodes in the specified domains.</p> <ul style="list-style-type: none"> <li>■ To deactivate SSH on ESXi nodes in a specific domain, include the flag <code>--domain-name DOMAINNAME</code>.</li> <li>■ To deactivate SSH on ESXi nodes in all domains, include the flag <code>--domain-name ALL</code>.</li> </ul> <p><b>Note</b> If you do not specify domain, this command affects only the MGMT domain by default.</p>
<code>--enable-ssh-esxi</code>	<p>Enables SSH on ESXi nodes in the specified domains.</p> <ul style="list-style-type: none"> <li>■ To enable SSH on ESXi nodes in a specific domain, include the flag <code>--domain-name DOMAINNAME</code>.</li> <li>■ To enable SSH on ESXi nodes in all domains, include the flag <code>--domain-name ALL</code>.</li> </ul> <p><b>Note</b> If you do not specify domain, this command affects only the MGMT domain by default.</p>
<code>--refresh-ssh-keys</code>	Refreshes the SSH keys.

## Collect Logs for Your VMware Cloud Foundation System

Use the SoS utility to collect the logs for various software components in the system.

Use these options when retrieving support logs from your environment's various components.

- To collect all logs from all components, you can run the SoS utility without specifying any component-specific options.
- To collect logs for a specific component, run the utility with the appropriate options.

For example, the `--domain-name` option is important. If omitted, the SoS operation is performed only on the management domain. See [SoS Utility Options](#).

After running the SoS utility, you can examine the resulting logs to troubleshoot issues, or provide to VMware Technical Support if requested. VMware Technical Support might request these logs to help resolve technical issues when you have submitted a support request. The diagnostic information collected using the SoS utility includes logs for the various VMware software components and software products deployed in your VMware Cloud Foundation environment.

**Table 19-1. SoS Utility Log File Options**

Option	Description
<code>--api-logs</code>	Collects output from REST endpoints for SDDC Manager inventory and LCM.
<code>--esx-logs</code>	Collects logs from the ESXi hosts only. Logs are collected from each ESXi host available in the deployment.
<code>--log-dir LOGDIR</code>	Specifies the directory to store the logs.
<code>--log-folder LOGFOLDER</code>	Specifies the name of the log directory.
<code>--no-clean-old-logs</code>	Use this option to prevent the utility from removing any output from a previous collection run. By default, the SoS utility. By default, before writing the output to the directory, the utility deletes the prior run's output files that might be present. If you want to retain the older output files, specify this option.
<code>--no-health-check</code>	Skips the health check executed as part of log collection.
<code>--nsx-logs</code>	Collects logs from the NSX Manager and NSX Edge instances only.
<code>--rvc-logs</code>	Collects logs from the Ruby vSphere Console (RVC) only. RVC is an interface for ESXi and vCenter.  <b>Note</b> If the Bash shell is not enabled in vCenter, RVC log collection will be skipped .  <b>Note</b> RVC logs are not collected by default with <code>./sos</code> log collection. You must enable RVC to collect RVC logs.
<code>--sddc-manager-logs</code>	Collects logs from the SDDC Manager only. <code>sddc &lt;timestamp&gt;.tgz</code> contains logs from the SDDC Manager file system's <code>etc</code> , <code>tmp</code> , <code>usr</code> , and <code>var</code> partitions.
<code>--test</code>	Collects test logs by verifying the files.
<code>--vc-logs</code>	Collects logs from the vCenter Server instances only. Logs are collected from each vCenter server available in the deployment.
<code>--vm-screenshots</code>	Collects all VM screenshots.
<code>--vrealize-logs</code>	Collects logs from vRealize Suite Lifecycle Manager.

## Procedure

- 1 Using SSH, log in to the SDDC Manager VM with the following credentials:

Username: **vcf**

Password: use the password specified in the deployment parameter workbook.

- 2 To collect the logs, run the SoS utility without specifying any component-specific options.

```
sudo /opt/vmware/sddc-support/sos
```

Enter the **vcf** password when prompted.

To collect logs for a specific component, run the utility with the appropriate options.

```
sudo /opt/vmware/sddc-support/sos --option-name
```

---

**Note** By default, before writing the output to the directory, the utility deletes the prior run's output files that might be present. If you want to retain the older output files, specify the `--no-clean-old-logs` option.

---

If you do not specify the `--log-dir` option, the utility writes the output to the `/var/log/vmware/vcf/sddc-support` directory in the SDDC Manager VM

## Results

The utility collects the log files from the various software components in all of the racks and writes the output to the directory named in the `--log-dir` option. Inside that directory, the utility generates output in a specific directory structure.

## Example

```
vcf@sddc-manager [ ~ ]$ sudo /opt/vmware/sddc-support/sos --domain-name MGMT --skip-known-
host-check --log-dir /tmp/new
[sudo] password for vcf
Welcome to Supportability and Serviceability(SoS) utility!
Performing SoS operation for MGMT domain components
Logs : /tmp/new/sos-2019-09-03-21-04-40-11793
Log file : /tmp/new/sos-2019-09-03-21-04-40-11793/sos.log
Log Collection completed successfully for : [HEALTH-CHECK, SDDC-MANAGER, NSX_MANAGER, API-
LOGS, ESX, VMS_SCREENSHOT, VCENTER-SERVER, VCF-SUMMARY]
```

## What to do next

Change to the output directory to examine the collected log files.

## Component Log Files Collected by the SoS Utility

The SoS utility writes the component log files into an output directory structure within the file system of the SDDC Manager instance in which the command is initiated, for example:

```
vcf@sddc-manager [ ~ ]$ sudo /opt/vmware/sddc-support/sos
[sudo] password for vcf
Welcome to Supportability and Serviceability(SoS) utility!
Performing SoS operation for MGMT domain components
Logs : /var/log/vmware/vcf/sddc-support/sos-2019-09-03-20-55-41-10053
Log file : /var/log/vmware/vcf/sddc-support/sos-2019-09-03-20-55-41-10053/sos.log
NOTE : The Health check operation was invoked without --skip-known-host-check, and so will skip
```

Connectivity Health, Password Health and Certificate Health Checks because of security reasons.

Log Collection completed successfully for : [HEALTH-CHECK, SDDC-MANAGER, NSX\_MANAGER, API-LOGS, ESX, VMS\_SCREENSHOT, VCENTER-SERVER, VCF-SUMMARY]

## esx Directory Contents

In each rack-specific directory, the `esx` directory contains the following diagnostic files collected for each ESXi host in the rack:

File	Description
<code>esx-FQDN.tgz</code>	Diagnostic information from running the <code>vm-support</code> command on the ESXi host. An example file is <code>esx-esxi-1.vrack.vsphere.local.tgz</code> .
<code>SmartInfo-FQDN.txt</code>	S.M.A.R.T. status of the ESXi host's hard drive (Self-Monitoring, Analysis, and Reporting Technology). An example file is <code>SmartInfo-esxi-1.vrack.vsphere.local.txt</code> .
<code>vsan-health-FQDN.txt</code>	vSAN cluster health information from running the standard command <code>python /usr/lib/vmware/vsan/bin/vsan-health-status.py</code> on the ESXi host. An example file is <code>vsan-health-esxi-1.vrack.vsphere.local.txt</code> .

## nsx Directory Contents

In each rack-specific directory, the `nsx` directory contains the diagnostic information files collected for the NSX Managers and NSX Edge instances deployed in that rack.

The number of files in this directory depends on the number of NSX Manager and NSX Edge instances that are deployed in the rack. In a given rack, each management domain has a cluster of three NSX Managers. The first VI workload domain has an additional cluster of three NSX Managers. Subsequent VI workload domains can deploy their own NSX Manager cluster, or use the same cluster as an existing VI workload domain. NSX Edge instances are optional.

File	Description
<code>VMware-NSX-Manager-tech-support-<i>nsxmanagerIPAddr</i>.tar.gz</code>	Standard NSX Manager compressed support bundle, generated using the NSX API POST <code>https://<i>nsxmanagerIPAddr</i>/api/1.0/appliance-management/techsupportlogs/NSX</code> , where <i>nsxmanagerIPAddr</i> is the IP address of the NSX Manager instance. An example is <code>VMware-NSX-Manager-tech-support-10.0.0.8.tar.gz</code> .
<code>VMware-NSX-Edge-tech-support-<i>nsxmanagerIPAddr</i>-<i>edgeId</i>.tgz</code>	Standard NSX Edge support bundle, generated using the NSX API to query the NSX Edge support logs: GET <code>https://<i>nsxmanagerIPAddr</i>/api/4.0/edges/<i>edgeId</i>/techsupportlogs</code> , where <i>nsxmanagerIPAddr</i> is the IP address of the NSX Manager instance and <i>edgeId</i> identifies the NSX Edge instance. An example is <code>VMware-NSX-Edge-tech-support-10.0.0.7-edge-1.log.gz</code> .

**Note** This information is only collected if NSX Edges are deployed.

## vc Directory Contents

In each rack-specific directory, the `vc` directory contains the diagnostic information files collected for the vCenter Server instances deployed in that rack.

The number of files in this directory depends on the number of vCenter Server instances that are deployed in the rack. In a given rack, each management domain has one vCenter Server instance, and any VI workload domains in the rack each have one vCenter Server instance.

File	Description
<code>vc-<i>vcsaFQDN</i>-vm-support.tgz</code>	Standard vCenter Server support bundle downloaded from the vCenter Server Appliance instance having a fully qualified domain name <i>vcsaFQDN</i> . The support bundle is obtained from the instance using the standard <code>vc-support.sh</code> command.

# Replacing Host Components

# 20

This section provides procedures for repairing or replacing hosts in VMware Cloud Foundation. These procedures are provided for scenarios where there is no risk of data loss, such as repairing an unassigned host or replacing a host in a non-vSAN-based workload domain.

These procedures are not intended for scenarios where there is a risk of data loss or involving a catastrophic failure. If there is a risk of data loss or you have experienced a catastrophic failure, before taking any steps to remediate the situation, contact VMware Support to review your recovery plan. This strategy ensures that additional damage is not done while troubleshooting.

---

**Note** Before performing any maintenance, review [Avoiding Unintentional Downtime](#).

---

For covered failure scenarios, the replacement procedure depends on the component being replaced and the condition of the component.

This chapter includes the following topics:

- [Avoiding Unintentional Downtime](#)
- [Replacing Components of a Host Running in Degraded Mode](#)
- [Replace a Dead Host](#)
- [Replace Boot Disk on a Host](#)

## Avoiding Unintentional Downtime

Many outages are caused by human error. Before performing maintenance on hosts or the network and storage infrastructure on which they depend, take precautions to avoid unintentional downtime.

There are a few steps you can take to avoid unintentional downtime.

- For operations that could impact access to storage, check that you have current backups for the VMs in the cluster, and if not, take a backup before proceeding. These operations include maintenance on hosts in a vSAN cluster, datastore mount points for external storage, and storage-array LUN masks.
- For operations that may take compute capacity offline, check that there is sufficient capacity available to continue running the VMs if the host being repaired cannot be brought back online as planned.

In addition, if the maintenance involves a host in a cluster, before proceeding with the maintenance, check the vCenter Server and NSX Managers associated with the host for any alerts that indicate a problem beyond the one you are planning to fix. If there are any alerts, address them first.

## Replacing Components of a Host Running in Degraded Mode

The procedures for replacing components of hosts in degraded depend on whether the host is assigned or unassigned. An assigned host belongs to the management domain or a workload domain. An unassigned host has been commissioned, but is not assigned to a domain.

These procedures apply to the following components:

- CPU
- Memory
- BMC
- Power supply

### Prerequisites

Before proceeding, review the guidance provided in the [Avoiding Unintentional Downtime](#).

## Replace Components of an Assigned Host Running in Degraded Mode

This procedure shows you how to replace the components of an assigned host running in degraded mode.

### Prerequisites

- Verify that the host is operational and is accessible by VMware Host Client.
- Verify that the Management, vSAN, and vMotion networks are available on the host. This can be viewed through the **Inventory > Hosts** page.
- Verify that the HDD and SSD disks on the host are in a good state.
- Verify that there are no alerts reported in vCenter Server for the host's cluster, and, if the cluster is a vSAN cluster, verify there are no vSAN health alerts.

### Procedure

- 1 Log in to the vSphere Client.
- 2 Right-click the affected host and click **Maintenance Mode > Enter Maintenance Mode**.
- 3 If the host belongs to a domain, click **Full Data Migration**.
- 4 Right-click the affected host and select **Shutdown**.



- 5 Pull the host out of the physical rack.

Note the ports on the switches it was connected to.

- 6 Service the appropriate part following the OEM vendor documentation.
- 7 Put the host back in the physical rack and connect it back to the appropriate switches.
- 8 Power on the host.
- 9 In vSphere Client, right-click the host and click **Maintenance Mode > Exit Maintenance Mode**.

## Replace Components of an Unassigned Host Running in Degraded Mode

This procedure shows you how to replace the components of an unassigned host that is running in degraded mode.

### Prerequisites

- Verify that the host is operational and is accessible by VMware Host Client.
- Verify that the HDD and SSD disks on the host are in a good state.

### Procedure

- 1 Log in to vSphere Web Client.
- 2 Right-click the affected host and select **Shutdown**.
- 3 Pull the host out of the physical rack.  
Note the ports on the switches it was connected to.
- 4 Service the appropriate part following the OEM vendor documentation.
- 5 Put the host back in the physical rack and connect it back to the appropriate switches.
- 6 Power on the host.
- 7 In the SDDC Manager Dashboard, verify that the host is available in the free pool.

## Replace a Dead Host

If you need to replace a dead host, you must remove the host from the physical rack. You can then add a new host or replace the failed component on the host and add it back.

This procedure applies chiefly to the following components:

- Storage controllers
- Motherboards
- Boot disks

### Prerequisites

If the host is assigned to a workload domain, verify that there are at least four hosts in the management or workload domain to which the faulty host belongs. If there are fewer than 4 hosts, contact VMware Support for assistance. Before proceeding, review the guidance provided in [Avoiding Unintentional Downtime](#).

### Procedure

- 1 If the host is assigned to a workload domain, it must be forcibly removed.
- 2 Decommission the host.  
See [Decommission Hosts](#).
- 3 Power off the host and remove it from the physical rack.
- 4 Replace and reconfigure, as follows.
  - a Replace the failed component on the host.
  - b Perform a fresh reinstall of ESXi.
  - c Commission the host.

See [Commission Hosts](#).

## Replace Boot Disk on a Host

This section describes the replacement procedure for a failed boot disk on a host.

### Prerequisites

If the host is operational, verify that there are at least four hosts in the management or workload domain to which the faulty host belongs. If there are fewer than four hosts, add a host to the domain from the capacity pool, if possible. If the host is not operational, see [Replace a Dead Host](#).

### Procedure

- 1 If there are dual boot disks in the host setup as RAID 1 and only one of them fails:
  - See [Replacing Components of a Host Running in Degraded Mode](#) to replace the failed disk.

The RAID 1 feature will rebuild the disks as needed. For more details, refer to the OEM vendor documentation.

- 2 If there is a single boot disk in the host and it fails, see [Replace a Dead Host](#).

# User and Group Management

# 21

You can allow the users and groups in your Microsoft Active Directory (AD) domain to use their credentials to log in to the SDDC Manager Dashboard as well as the vCenter Server instances that are deployed in your Cloud Foundation system.

You provided a password for the superuser account (user name `vcf`) in the deployment parameter workbook before bring-up. After VMware Cloud Foundation is deployed, you can log in with the superuser credentials and then add vCenter Server or AD users or groups to VMware Cloud Foundation. Authentication to the SDDC Manager Dashboard uses the VMware vCenter® Single Sign-On authentication service that is installed during the bring-up process for your VMware Cloud Foundation system.

Users and groups can be assigned roles to determine what tasks they can perform from the UI and API.

In addition to user accounts, VMware Cloud Foundation includes the following accounts:

- Automation accounts for accessing VMware Cloud Foundation APIs. You can use these accounts in automation scripts.
- Local account for accessing VMware Cloud Foundation APIs when vCenter Server is down.  
For a VMware Cloud Foundation 4.1 deployment, you can specify the local account password in the deployment parameter workbook. If you upgraded to VMware Cloud Foundation 4.1, you configure the local account through VMware Cloud Foundation API.
- Service accounts are automatically created by VMware Cloud Foundation for inter-product interaction. These are for system use only.

This chapter includes the following topics:

- [Add a User or Group to VMware Cloud Foundation](#)
- [Remove a User or Group](#)
- [Create a Local Account](#)
- [Create an Automation Account](#)

## Add a User or Group to VMware Cloud Foundation

You can add users or groups so that they can log in to SDDC Manager with their AD credentials.

### Prerequisites

Only a user with the ADMIN role can perform this task.

### Procedure

- 1 Log in to the SDDC Manager Dashboard with your superuser credentials.
- 2 Click **Administration > Users**.
- 3 Click **+ User or Group**.
- 4 Select one or more users or group by clicking the check box next to the user or group.  
You can either search for a user or group by name, or filter by user type or domain.
- 5 Select a Role for each user and group.

Role	Description
ADMIN	This role has access to all the functionality of the UI and API.
OPERATOR	This role cannot access user management, password management, or backup configuration settings.
VIEWER	This role can only view the SDDC Manager. User management and password management are hidden from this role.

- 6 Scroll down to the bottom of the page and click **Add**.

## Remove a User or Group

You can remove a user or group, for example when an employee leaves the company. The removed user or group will not be able to log in to the SDDC Manager Dashboard.

### Prerequisites

Only a user with the ADMIN role can perform this task.

### Procedure

- 1 In a Web browser, log in to SDDC Manager administration interface.
- 2 Click **Administration > Users**.
- 3 Click the vertical ellipsis (three dots) next to a user or group name and click **Remove**.
- 4 Click **Delete**.

## Create a Local Account

A local account is used to access VMware Cloud Foundation APIs when the management vCenter Server is down. If you upgraded from a previous release or didn't configure the account when deploying using the API, you can set a password using VMware Cloud Foundation APIs.

## Procedure

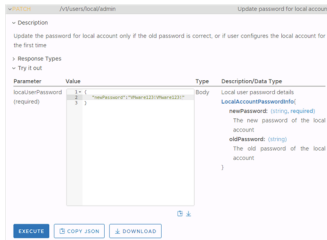
- 1 Log in to the SDDC Manager Dashboard as a user with the ADMIN role.  
For more information about roles, see [Chapter 21 User and Group Management](#).
- 2 Click **Developer Center > API Explorer**.
- 3 To verify if the local account is configured, perform the following tasks:
  - a Expand **APIs for managing Users**.
  - b Expand `GET /v1/users/local/admin` and click **EXECUTE**.
  - c In the Response, click `LocalUser (admin@local)`.

### Response

```
LocalUser (admin@local) [ ] {
  "isConfigured":
    Flag indicating whether or not local
    account is configured
    "true",
  "name":
    The name of the user
    "admin@local",
  "role":
    The role of the user
    RoleReference (fa16f14b-9679-bbfc-06ed-47245405542c) [ ] { ... }
  "type":
    The type of the user
    "USER",
}
```

You can also download the response by clicking the download icon to the right of `LocalUser (admin@local)`.

- 4 If the local account is not configured, perform the following tasks to configure the local account:
  - a Expand `PATCH /v1/users/local/admin`.
  - b Enter a password for the local account and click **EXECUTE**.



Password requirements are described below:

- Minimum length: 12
- Maximum length: 127
- At least one lowercase letter, one uppercase letter, a number, and one of the following special characters ! % @ \$ ^ # ? \*
- A character cannot be repeated more than three times consecutively
- Must not include three of the same consecutive characters

---

**Note** You must remember the password that you created because it cannot be retrieved. Local account passwords are used in password rotation.

---

## Create an Automation Account

Automation accounts are used to access VMware Cloud Foundation APIs in automation scripts.

### Procedure

- 1 Log in to the SDDC Manager Dashboard as a user with the ADMIN role.  
For more about roles, see [Chapter 21 User and Group Management](#).
- 2 Click **Developer Center > API Explorer**.
- 3 Get the ID for the ADMIN role.
  - a Expand **APIs for managing Users**.
  - b Expand `GET /v1/roles` and click **Execute**.

- c In the Response, click `PageOfRole` and `Role (ADMIN)`.
- d Copy the ID for the ADMIN role.

## Response

`PageOfRole`   {

"elements":

The list of elements included in this page

[

`Role (ADMIN)`   {

"description":

The description of the role

"Administrator",

"id":

The ID of the role

"317cb292-802f-ca6a-e57e-3ac2b707fe34",

"name":

The name of the role

"ADMIN",

},

- 4 Create a service account with the ADMIN role and get the service account's API key.
  - a Expand `POST /v1/users` and click **User**.
  - b Replace the Value with:

```
[
  {
    "name": "service_account",
    "type": "SERVICE",
    "role": {
      "id": "317cb292-802f-ca6a-e57e-3ac2b707fe34"
    }
  }
]
```

Paste the ADMIN role ID from step 3.

POST /v1/users Add users

Description  
Add list of users

Response Types

Try it out

Parameter	Value	Type	Description/Data Type
users (required)	<pre>[   {     "name": "service",     "role": {       "id": "317cb292-802f-ca6a-e57e-3ac2b707fe34"     },     "type": "SERVICE"   } ]</pre>	Body	User data collection [ User{ ... } ]

EXECUTE COPY JSON DOWNLOAD

- c Click **Execute**.
- d In the Response, click `PageOfUser` and `User (service_account)`.
- e Copy the API key for the service account.

**Response**

`PageOfUser` {

"elements":  
The list of elements included in this page  
[

`User (service_account)` {

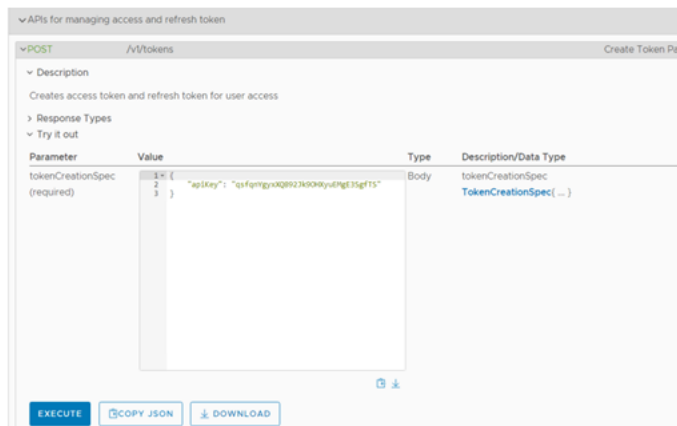
"apiKey":  
The API key of the user  
"qsfqnYgyxXQ892Jk9OHXyuEMgE3SgfTS",



- 5 Use the service account's API key to generate an access token.
  - a Expand **APIs for managing access and refresh tokens**.
  - b Expand `POST /v1/tokens`.
  - c Click **TokenCreationSpec**.
  - d Replace Value with:

```
{
  "apiKey": "qsfgnYgyxXQ892Jk90HXyuEMgE3SgfTS"
}
```

Paste the service account's API key from step 4.



- e Click **Execute**.
- f In the Response, click `TokenPair` and `RefreshToken` and save the access and refresh tokens.

#### Response

```
TokenPair {
  "accessToken":
    Bearer token that can be used to make
    public API calls
    "eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiJkMWQ1OGM5NiJmZmZlTGwODMTYjU3Yi1hODYxOTUwODY0YTQilCjYXQiOiE1ODU1ODgyNDAsInN1..."
  "refreshToken":
    Refresh token that can be used to request
    new access token
    RefreshToken (33f88c60-862e-4a38-8e8e-6479c4cd9f33) {
      "id":
        Refresh token id that can be used to
        request new access token
        "33f88c60-862e-4a38-8e8e-6479c4cd9f33",
    }
}
```

# Password Management

# 22

For security reasons, you can change passwords for the accounts that are used by your VMware Cloud Foundation system. Changing these passwords periodically or when certain events occur, such as an administrator leaving your organization, reduces the likelihood of security vulnerabilities.

You entered passwords for your VMware Cloud Foundation system as part of the bring-up procedure. You can rotate and update some of these passwords using the password management functionality in the SDDC Manager Dashboard. For example:

- Accounts used for service consoles, such as the ESXi root account.
- The single sign-on administrator account.
- The default administrative user account used by virtual appliances.
- Service accounts that are automatically generated during bring-up, host commissioning, and workload creation.

Service accounts have a limited set of privileges and are created for communication between products. Passwords for service accounts are randomly generated by SDDC Manager. You cannot manually set a password for service accounts. To update the credentials of service accounts, you can rotate the passwords.

To provide optimal security and proactively prevent any passwords from expiring, you must rotate passwords every 80 days.

---

**Note** Do not change the passwords for system accounts and the `administrator@vsphere.local` account outside SDDC Manager. This can break your VMware Cloud Foundation system.

---

You can also use the VMware Cloud Foundation API to look up and manage credentials. From the SDDC Manager Dashboard, click **Developer Center > API Explorer** and browse to the APIs for managing credentials.

This chapter includes the following topics:

- [Rotate Passwords](#)
- [Manually Update Passwords](#)
- [Remediate Passwords](#)

- [Look Up Account Credentials](#)
- [Updating SDDC Manager Passwords](#)

## Rotate Passwords

As a security measure, you can rotate passwords for the logical and physical accounts on all racks in your system. The process of password rotation generates randomized passwords for the selected accounts.

You can rotate passwords for the following accounts.

- ESXi
- vCenter Server
  - By default, the vCenter Server root password expires after 90 days.
- PSC SSO
- NSX-T Edge
- NSX-T Manager
- vRealize Suite Lifecycle Manager
- vRealize Log Insight
- vRealize Operations
- vRealize Automation
- Workspace ONE Access
- SDDC Manager **backup** user

The default password policy for rotated passwords is:

- 20 characters in length for VMware Cloud Foundation 4.2.1.
- 15 character in length for VMware Cloud Foundation 4.2.
- At least one uppercase letter, a number, and one of the following special characters: ! @ # \$ ^ \*
- No more than two of the same characters consecutively

For VMware Cloud Foundation 4.2.1, if you changed the vCenter Server password length using the vSphere Client or the ESXi password length using the VMware Host Client, rotating the password for those components from SDDC Manager generates a password that complies with the password length that you specified.

To update the SDDC Manager root, super user, and API passwords, see [Updating SDDC Manager Passwords](#).

### Prerequisites

- Verify that there are no currently failed workflows in your VMware Cloud Foundation system. To check for failed workflows, click **Dashboard** in the navigation pane and expand the **Tasks** pane at the bottom of the page.
- Verify that no active workflows are running or are scheduled to run during the brief time period that the password rotation process is running. It is recommended that you schedule password rotation for a time when you expect to have no running workflows.
- Only a user with the ADMIN role can perform this task.

### Procedure

- 1 From the navigation pane, select **Administration > Security > Password Management**.

The Password Management page displays a table with detailed information about all domains, including their account, credential type, FQDN, IP address, and user name. This table is dynamic. Each column can be sorted.

You can click the filter icon next to the table header and filter the results by a string value. For example, click the icon next to **User Name** and enter **admin** to display only domains with that user name value.

- 2 Select the account for which you want to rotate passwords from the **Component** drop-down menu. For example, **ESXI**.
- 3 Select one or more accounts and click **Rotate**.

A message appears at the top of the page showing the progress of the operation. The Tasks panel also shows detailed status for the password rotation operation. To view sub-tasks, click the task name. As each of these tasks is run, the status is updated. If the task fails, you can click **Retry**.

### Results

Password rotation is complete when all sub-tasks are completed successfully.

## Manually Update Passwords

You can manually change the password for a selected account. Unlike password rotation, which generates a randomized password, you provide the new password.

---

**Note** You can update passwords for **USER** and **SYSTEM** account types.

---

You can update only one password at a time.

Although individual VMware Cloud Foundation accounts support different password requirements, it is recommended that you set passwords following a common set of requirements across all accounts:

- Minimum length: 12

- Maximum length: 20
- At least one lowercase letter, one uppercase letter, a number, and one of the following special characters: ! @ # \$ ^ \*
- Must NOT include:
  - A dictionary word
  - A palindrome
  - More than four monotonic character sequences
  - Three of the same consecutive characters

### Prerequisites

- Verify that there are no currently failed workflows in your VMware Cloud Foundation system. To check for failed workflows, click **Dashboard** in the navigation pane and expand the **Tasks** pane at the bottom of the page.
- Verify that no active workflows are running or are scheduled to run during the manual password update.
- Only a user with the ADMIN role can perform this task. For more information about roles, see [Chapter 21 User and Group Management](#).

### Procedure

- 1 From the navigation pane, select **Administration > Security > Password Management**.

The Password Management page displays a table with detailed information about all domains, including their account, credential type, FQDN, IP address, and user name. This table is dynamic. Each column can be sorted.

You can click the filter icon next to the table header and filter the results by a string value. For example, click this icon next to **User Name** and enter **admin** to display only domains with that user name value.

- 2 Select the account whose password you want to update and click **Update** at the top of the page.

---

**Note** If you select more than one account, the **Update** button will be unavailable (dimmed).

---

The Update Password dialog box appears. This dialog box also displays the account name, account type, credential type, and user name, in case you must confirm you have selected the correct account.

- 3 Enter and confirm the new password.

If the passwords do not match, the dialog box displays a red alert.

#### 4 Click **Update**.

A message appears at the top of the page showing the progress of the operation. The Tasks panel also shows detailed status of the password update operation. To view sub-tasks, click the task name.

If the Tasks panel shows the task as having failed, click **Retry**.

#### Results

Password updation is complete when all sub-tasks are completed successfully.

## Remediate Passwords

When an error occurs, for example after a password expires, you must reset the password in the component. After you reset the password, you must remediate the password. Password remediation updates the new password in the SDDC Manager database and the dependent Cloud Foundation workflows.

To resolve any errors that might have occurred during password rotation or updation, you must use password remediation. Password remediation manually syncs the password of the component account stored in the SDDC Manager with the updated password in the component.

For **USER** and **SYSTEM** account types, you must manually enter the password set in the component. The SDDC Manager updates the stored password with the new password.

For the **SERVICE** account type, you must manually enter the password set in the component. The SDDC Manager updates the service account password with the new password. After password remediation, the password is rotated to a new password.

---

**Note** You can remediate password for only one account at a time.

---

Although the individual VMware Cloud Foundation components support different password requirements, you must set passwords following a common set of requirements across all components. For information on updating passwords manually, see [Manually Update Passwords](#).

#### Prerequisites

- Verify that there are no currently failed workflows in your VMware Cloud Foundation system. To check for failed workflows, click **Dashboard** in the navigation pane and expand the **Tasks** pane at the bottom of the page.
- Verify that no active workflows are running or are scheduled to run during the manual password remediate.
- Only a user with the ADMIN role can perform this task. For more information about roles, see [Chapter 21 User and Group Management](#).

**Procedure**

- 1 From the navigation pane, select **Administration > Security > Password Management**.

The Password Management page displays a table with detailed information about all domains, including their component, credential type, FQDN, IP address, and user name. This table is dynamic. Each column can be sorted.

You can click the filter icon next to the table header and filter the results by a string value. For example, click this icon next to **User Name** and enter **admin** to display only domains with that user name value.

- 2 Select the domain entity whose password you want to remediate, and click **Remediate** at the top of the page.

---

**Note** If you select more than one account, the **Remediate** button is unavailable (dimmed).

---

The Remediate Password dialog box appears. This dialog box also displays the entity name, account type, credential type, and user name, in case you must confirm you have selected the correct account.

- 3 Enter and confirm the new password set at the component.

If the passwords do not match, the dialog box displays a red alert.

- 4 Click **Remediate**.

A message appears at the top of the page showing the progress of the operation. The Task panel also shows detailed status of the password remediation operation. To view subtasks, you can click the task name.

If the Task panel shows the task as having failed, click **Retry**.

**Results**

Password remediation is complete when all sub-tasks are completed successfully.

## Look Up Account Credentials

To look up the account credentials for the built-in accounts that are managed and rotated by SDDC Manager, you can log in to the SDDC Manager VM using any SDDC Manager account credentials.

**Prerequisites**

Only a user with the **ADMIN** role can perform this task.

**Procedure**

- 1 SSH in to the SDDC Manager VM using the **vcf** user account.

- 2 (Optional) Change to the `/usr/bin` directory.

---

**Note** Although the password management CLI commands are located in `/usr/bin`, you can run them from any directory.

---

- 3 Obtain the account credentials list by typing the command:

```
lookup_passwords
```

You must enter the user name and password for a user with the ADMIN role.

---

**Note** Accounts with type **USER** and **SYSTEM** will be displayed.

---

- 4 (Optional) Save the command output to a secure location with encryption so that you can access it later and use it to log in to the accounts as needed.

## Updating SDDC Manager Passwords

You cannot update SDDC Manager passwords through the SDDC Manager Dashboard or by using cURL API requests. Instead, you will need to SSH into the SDDC Manager VM and make the changes there.

The process for updating SDDC Manager passwords varies, depending on which account you are updating.

- [Update SDDC Manager Root and Super User Passwords](#)

For security reasons, you can change passwords for the SDDC Manager root (**root**) and super user (**vcf**) accounts. Changing these passwords periodically or when certain events occur, such as an administrator leaving your organization, reduces the likelihood of security vulnerabilities.

- [Update SDDC Manager REST API Account Password](#)

To use the VMware Cloud Foundation API, an API client logs in using the SDDC Manager **admin** account. For security reasons, you should periodically update the password for this account.

- [Update SDDC Manager Local Account Password](#)

The SDDC Manager local account is used to access VMware Cloud Foundation APIs when the management vCenter Server is down. For security reasons, you should periodically update the password for this account.

- [Update Expired SDDC Manager root Password](#)

This section describes the procedure for updating an expired password for the SDDC Manager root (**root**) user.



## Update SDDC Manager Root and Super User Passwords

For security reasons, you can change passwords for the SDDC Manager root (**root**) and super user (**vcf**) accounts. Changing these passwords periodically or when certain events occur, such as an administrator leaving your organization, reduces the likelihood of security vulnerabilities.

The SDDC Manager **root** password expires after 365 days.

### Procedure

- 1 SSH in to the SDDC Manager VM using the **vcf** user account.
- 2 Enter **su** to switch to the root user.
- 3 Enter one of the following commands:

Option	Description
<code>passwd vcf</code>	To change the super user password.
<code>passwd root</code>	To change the root password.

- 4 Enter and retype the new password. For example:

```
root@sddc-manager [ /home/vcf ]# passwd vcf
New password:
Retype new password:
passwd: password updated successfully
```

### Results

The password is updated.

## Update SDDC Manager REST API Account Password

To use the VMware Cloud Foundation API, an API client logs in using the SDDC Manager **admin** account. For security reasons, you should periodically update the password for this account.

If you write a script that invokes the APIs, the script should either prompt the user for the password for the **admin** account or should accept the password as a command line option. As a best practice, you should not encode the password for the account in the script code itself.

Password requirements:

- Length 8-12 characters
- Must include: mix of upper-case and lower-case letters a number a special character such as @ ! # \$ % ^ or ?
- Cannot include: \* { } [ ] ( ) / \ ' " ` ~ , ; : . < >

### Procedure

- 1 SSH in to the SDDC Manager VM using the **vcf** user account.

- 2 Enter **su** to switch to the root user.
- 3 Enter the following command:

```
/opt/vmware/vcf/commonsvc/scripts/auth/set-basicauth-password.sh admin <password>
```

For *<password>*, enter the new password for the **admin** account.

## Update SDDC Manager Local Account Password

The SDDC Manager local account is used to access VMware Cloud Foundation APIs when the management vCenter Server is down. For security reasons, you should periodically update the password for this account.

Password requirements for the SDDC Manager local account:

- At least 12 characters
- No more than 127 characters
- At least one lowercase letter
- At least one uppercase letter
- At least one digit
- At least one special character, such as @ ! # \$ % ^ or ?
- A character cannot be repeated more than 3 times consecutively

### Procedure

- 1 Log in to the SDDC Manager Dashboard as a user with the ADMIN role.  
For more information about roles, see [Chapter 21 User and Group Management](#).
- 2 Click **Developer Center > API Explorer**.
- 3 Expand **APIs for managing Users**.
- 4 Expand **PATCH /v1/users/local/admin**.
- 5 In the **Description/Data Type** column, click **LocalAccountPasswordInfo{...}**.
- 6 In the **Value** box, type the new and old passwords and click **Execute**.
- 7 Click **Continue** to confirm.

A response of **Status: 204, No Content** indicates that the password was successfully updated.

## Update Expired SDDC Manager root Password

This section describes the procedure for updating an expired password for the SDDC Manager root (**root**) user.

## Prerequisites

### Procedure

- 1 Log into the vSphere Client and select the SDDC Manager VM from Mgmt-ResourcePool.
- 2 From the panel on the right side of the window, select **Summary** and click on **Launch Web Console**.
- 3 In the popup window, select web console and click **OK**. This will open the console in a new browser tab.

The console opens in a new browser window.

- 4 Click **Login**.
- 5 Type **root** as the user name and enter the current password for the root user.
- 6 When prompted for current password, enter the current password.
- 7 When prompted for a new password, enter a different password than the previous one and click **OK**.

# Backing Up and Restoring SDDC Manager and NSX Manager

# 23

Regular backups of the management VMs are important to avoid downtime and data loss in case of a system failure. If a VM does fail, you can restore it to the last backup.

You can backup and restore SDDC Manager with an image-based or a file-based solution. File-based backup is recommended for customers who are comfortable with configuring backups using APIs, and are not using composable servers.

For a file-based backup of SDDC Manager VM, the state of the VM is exported to a file that is stored in a domain different than the one where the product is running. You can configure a backup schedule for the SDDC Manager VM and enable task-based (state-change driven) backups. When task-based backups are enabled, a backup is triggered after each SDDC Manager task (such as workload domain and host operations or password rotation).

You can also define a backup retention policy to comply with your company's retention policy. For more information, see the *VMware Cloud Foundation API Reference Guide*.

By default, NSX Manager file-based backups are taken on the SFTP server that is built into SDDC Manager. It is recommended that you configure an external SFTP server as a backup location for the following reasons:

- An external SFTP server is a prerequisite for restoring SDDC Manager file-based backups.
- Using an external SFTP server provides better protection against failures because it decouples NSX backups from SDDC Manager backups.

This section of the documentation provides instructions on backing up and restoring SDDC Manager, and on configuring the built-in automation of NSX backups. For information on backing up and restoring a full-stack SDDC, see *VMware Validated Design Backup and Restore*.

This chapter includes the following topics:

- [Image-Based Backup and Restore](#)
- [File-Based Backup and Restore](#)

## Image-Based Backup and Restore

For an image-based backup of the SDDC Manager, use a solution compatible with the VMware vSphere Storage APIs - Data Protection (formerly known as VMware vStorage APIs for Data Protection or VADP).

vSphere Storage APIs - Data Protection compatible backup software connects to the vCenter servers in the management domain to perform the backup to a remote site. In the event of failure, the backup software connects to the vCenter servers in the management domain to restore the VMs. If the management domain is lost, the vCenter servers are no longer available and must be restored first. Choosing a backup software that supports Direct Restore to an ESXi host allows restoring the vCenter servers.

For an SDDC Manager backup, connect your backup with the management domain vCenter Server. Configure the product to take non-quieted backups of SDDC Manager. To reduce the backup time and storage cost, use incremental backups in addition to full ones.

## File-Based Backup and Restore

You can use a file-based backup and restore solution for SDDC Manager and NSX Manager.

In a file-based solution, the state of a product is periodically exported to a file that is stored in a different domain than the one where the product is running. If the product needs to be restored, the OVA is redeployed and a selected backup file is used to restore the state. Finally, the post-restore steps are done.

In case you have to restore the SDDC Manager VM or an NSX Manager VM, you select the backup file to restore and download the appropriate OVA file. You can deploy this OVA either through vCenter Server or through the OVF tool. You then load the state on the newly deployed VM.

Note the following limitations for file-based backup:

- This solution requires that you register an external SFTP server. See [Configure an External SFTP Server for File-Based Backups](#). If you do not use an external SFTP server, NSX Managers continue to write backups to the built-in SFTP server on the SDDC Manager VM. This process does not back up the NSX Manager backup files, which leave a gap in protection.
- For the SDDC Manager VM, you must set a backup schedule after setting up an external SFTP server. Backups are not configured automatically. See [Configure a Backup Schedule for SDDC Manager VM](#).
- Neither SDDC Manager nor NSX Manager currently manage the files they back up. It is your responsibility to delete the files that are backed up once their age exceeds your company's retention policy.
- This solution cannot be used for composable servers.

## Configure an External SFTP Server for File-Based Backups

VMware Cloud Foundation allows you to register an external SFTP server with SDDC Manager for backing up NSX Managers and the SDDC Manager VM.

It is important to deploy a reliable SFTP server and ensure it is accessible from the VMware Cloud Foundation instance. If the SFTP server is not available when the SDDC Manager VM or an NSX Manager attempts to back up its state, the backup will not be taken, and any recent changes are not backed up until the retries succeed. To ensure that this situation does not occur, it is recommended that you periodically check that backups are successfully taken, and monitoring that the backups for other products are also being successfully taken. If the SFTP server is not available at the time of deploying a workload domain or upgrading NSX, these operations fail.

When you configure an external SFTP server, SDDC Manager saves the SFTP server details, and then configures the SDDC Manager and all existing NSX Managers to use the SFTP server. When subsequent NSX Managers are deployed, SDDC Manager configures them to use this SFTP server as well.

When you configure an external SFTP server, NSX Manager backups are automatically scheduled at regular intervals. You can check and modify the backup interval in the NSX Manager UI. SDDC Manager VM backups are not scheduled automatically. Use the Cloud Foundation API to set a backup schedule for the SDDC Manager VM. See [Configure a Backup Schedule for SDDC Manager VM](#).

To configure an external SFTP server, perform the following steps:

#### Prerequisites

- The external SFTP server must support ECDSA SSH public key.
- Only a user with the ADMIN role can perform this task. See [Chapter 21 User and Group Management](#).
- You will need the SHA256 fingerprint of RSA key of the SFTP server.

#### Procedure

- 1 In the SDDC Manager dashboard, select **Administration > Backup**.
- 2 Click **Register External**.
- 3 Enter the FQDN or IP address of the backup server. Ensure that the server is available for the successful configuration.
- 4 Enter the port number at which the SFTP service is running.
- 5 Select **SFTP** as the transfer protocol.
- 6 Enter the credentials of the server.
- 7 Enter the backup directory path of the server.

Ensure that the user you specify in step 6 can access the directory path since the backups are saved to this location. It is recommended to provide different directory paths for the different VMware Cloud Foundation instances in case you are using the same SFTP server across all.

- 8 Confirm the fingerprint that is auto populated for the given FQDN or IP address and the port.

- 9 Enter the encryption passphrase which is used for both NSX Manager and SDDC Manager backups.
- 10 Click **Save**.
- 11 Click **Confirm**.
- 12 If you have to edit the backup configuration information, perform the following steps:
  - a On the SDDC Manager dashboard, select **Administration > Backup Configuration**.
  - b Click **Edit**.
  - c Update the configuration information.  
 If there is any change in the FQDN/IP address or the backup directory path, if you save the configuration, the existing backups are not copied to the new location. Copy them manually.
  - d Enter the backup server password and the passphrase.  
 If you change the passphrase it only applies to future backups. You need to use the old passphrase while restoring previous backups.
  - e Click **Save**.
  - f Click **Confirm**.

## Configure a Backup Schedule for SDDC Manager VM

Use the Cloud Foundation API to configure a backup schedule for the SDDC Manager VM. You can also enable task-based (state-change driven) backups. When task-based backups are enabled, a backup is triggered after each SDDC Manager task (such as workload domain and host operations or password rotation). You can also define a backup retention policy to comply with your company's retention policy.

This procedure uses the Cloud Foundation API, which is secured by token-based authentication. Follow the best practices below:

- Schedule backups when no other workflows are running.
- Take periodic backups on a daily to weekly frequency.
- If a workflow does not complete successfully and the environment is in this state when the scheduled backup is taken, resolve the failure as soon possible and take an unscheduled backup. Restoring your environment from a backup that includes unresolved failures is more difficult than restoring from a clean backup.

A workflow is resolved when the environment is not in an intermediate state. Some workflows can only be resolved by fixing the failure conditions and retrying the operation. Other workflows can also be resolved by invoking the corresponding delete operation. For example, if adding a host to a workload domain fails, either fix the condition that caused the workflow to fail, or run the workflow that removes the host from the cluster. Contact VMware Support if you are unable to resolve a workflow.

### Prerequisites

- You must have configured an external SFTP server for file-based backups. See [Configure an External SFTP Server for File-Based Backups](#).
- Only a user with the ADMIN role can perform this task. See [Chapter 21 User and Group Management](#).

## Procedure

- 1 To obtain an access token, run the following command:

```
curl 'https://SDDC_MANAGER_IP/v1/tokens' -k -X POST -H 'Content-Type: application/json' -H 'Accept: application/json' -d '{"username" : "user_name", "password" : "user_password"}'
```

Replace the SDDC Manager IP address, user name, and password with the information for your environment.

The command returns an access token and a refresh token.

```
{ "accessToken": "eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiI2ZGRmZmUzMCM0czZGEwLTQ5NmUtOTQzMCIhOGNkNTQ0YT  
k2ZGMiLCJpYXQiOjE0ODU3ODE3ODcsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbcCIsmImlzcyl6InZlZj  
ilhdXR0eSIiwiyXVkbWluaiIjoic2RkYyZlZXJ2aWNlcysIm5iziI6MTU0NTc4MTC4NywiZXBhbmVjaXN0TglNzg1Mzg3LClc2Vy  
IjoyiWRtaW5pc3RyYXRvckB2c3BoZSJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbcCI  
sInNjb3BlIjpjbIkJBQ0tVUF9DT05GSUdfUkVBRCIsIkNsRURFTlRJQUxufUkVBRCIsIlVTRVJfvlJJVEUiLCJPVEhFUL  
9XUklURSIsIkJBQ0tVUF9DT05GSUdfVlJJVEUiLCJPVEhFUL9SRUFEIiwivVNful9SRUFEIiwiaWF0IjE1JFREVOVELBTf9XU  
klURSjdFQ.WCpUPRI5A6X_406HTJF7TbTSa0g91_AQbt7OcBPblM","refreshToken":  
{"id":"47c07f35-0a89-4df5-a3a3-f31265ebbb7a"}}}
```

- 2** Set the backup schedule, for example:

[illegible]

Option	Description
Resource Type	Enter <b>SDDC_MANAGER</b> .
Frequency	Enter <b>HOURLY</b> or <b>WEEKLY</b> .
Days of Week	<p>Enter the days to back up SDDC Manager. When selecting multiple days, use a comma to separate them. For example: "daysOfWeek" : [ "SUNDAY", "THURSDAY" ]</p> <p><b>Note</b> Only available if the frequency is set to <b>WEEKLY</b>.</p>



Option	Description
Hour of Day	Enter the hour of day (0-23) to perform the backup.
Minute of Hour	Enter the minute of the hour (0-59) to perform the backup.

Note the `<id>` that gets returned.

### 3 Track the status of the backup schedule configuration.

```
curl -H "Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiIxNm5YThmOC00NGQwLTQ5MzYtYjYjQWMC0xMzc5NzMyMjdmOWUiLCJpYXQiOiJlODUzODQ5MTgsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbmCI9ImZlcyI6InZjZilhdXRoIiwiaXVkaWoiOiJ0c2RkYy1zZXJ2aWNLcyIsIm5iZiI6MTU4NTc4NDkxOCwiZXhwIjoxNTg1Nzg4NTE4LCJ1c2VyIjoiYWRtaW5pc3RyYXRvcjB2c3BoZXJlImxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbmCI9InNjb3BlIjpbIkJBQ0tVUF9DT05GSUdfUkVBRCl9IkNSRURFTlRJRQ0xUkVBRCl9IlVTRVJfV1JJVEUiLCJpVEhFb2N1YXUkLURSI9IkJBQ0tVUF9DT05GSUdfV1JJVEUiLCJpVEhFb2N1YXUkLURSI9SRUFEIiwiaXVnF19SRUFEIiwiaWF0Ij01JFREV0VElBTf9XUkLURSI9JdfQ.Ya4XsZntsRHUZFBNKGY7Js6xrGYGe8KdgJ2QbiHfmg" -H 'Content-Type: application/json' -k -X GET https://SDCC_MANAGER_IP/v1/tasks/<id>|json_pp
```

Replace `<id>` with the ID from the previous step.

4 Repeat the previous step until the task status is `SUCCESSFUL`.

For information on task-based backups and retention policy, see the *VMware Cloud Foundation API Guide*.

## Restore SDDC Manager

See the Backup and Restore Section of the *VMware Cloud Foundation API Reference Guide* for the manual procedure to restore SDDC Manager from file-based backups using the Cloud Foundation APIs.

# VMware Cloud Foundation Glossary

24

Term	Description
availability zone	Collection of infrastructure components. Each availability zone is isolated from other availability zones to prevent the propagation of failure or outage across the data center.
Application virtual networks (AVNs)	Virtual networks backed by overlay segments using the encapsulation protocol of NSX-T. Virtual Networks use a single IP network address space, to span across data centers.
bring-up	Initial configuration of a newly deployed VMware Cloud Foundation system. During the bring-up process, the management domain is created and the VMware Cloud Foundation software stack is deployed on the management domain.
cluster image	Precise description of the software, components, vendor add-ons, and firmware to run on a host. With this new functionality, you set up a single image and apply it to all hosts in a cluster, thus ensuring cluster-wide host image homogeneity.
commission host	Adding a host to VMware Cloud Foundation inventory. The host remains in the free pool until it is assigned to a workload domain.
composability	Ability to dynamically configure servers to meet the needs of your workloads without physically moving any hardware components. You bind disaggregated hardware components (compute, network, storage, and offload components) together to create a logical system based on the needs of your applications.
dirty host	A host that has been removed from a cluster in a workload domain. A dirty host cannot be assigned to another workload domain until it is decommissioned, reimaged, and commissioned again.
decommission host	Remove an unassigned host from the VMware Cloud Foundation inventory. SDDC Manager does not manage decommissioned hosts.
Edge cluster	A logical grouping of NSX-T Data Center Edge nodes. These nodes run on a vSphere cluster, and provide north-south routing and network services for the management and VI workload domains.
free pool	Hosts in the VMware Cloud Foundation inventory that are not assigned to a workload domain
host	An imaged server.
inventory	Logical and physical entities managed by VMware Cloud Foundation.
Kubernetes - Workload Management	With Kubernetes - Workload Management, you can deploy and operate the compute, networking, and storage infrastructure for vSphere with Tanzu workloads. A vSphere with Tanzu workload is an application with containers running inside vSphere pods, regular VMs, or Tanzu Kubernetes clusters.

Term	Description
Lifecycle Manager (LCM)	Automates patching and upgrading of the software stack.
management domain	Cluster of physical hosts that contains the management component VMs
network pool	Automatically assigns static IP addresses to vSAN and vMotion vmkernel ports so that you don't need to enter IP addresses manually when creating a VI workload domain or adding a host or cluster to a workload domain.
patch update bundle	Contains bits to update the appropriate Cloud Foundation software components in your management or VI workload domain.
region	Regions are geographically separate locations, that can provide disaster recovery between data centers. Latency between them must be 150 ms or lower. A region can consist of one or more VMware Cloud Foundation instances.
SDDC Manager	Software component that provisions, manages, and monitors the logical and physical resources of a VMware Cloud Foundation system.
SDDC Manager VM	Virtual machine (VM) that contains the SDDC Manager services and a shell from which command line tools can be run. This VM exposes the SDDC Manager UI.
server	Bare metal server in a physical rack. After imaging, it is referred to as a host.
unassigned host	Host in the free pool that does not belong to a workload domain.
vSphere Lifecycle Manager (vLCM)	A vCenter service, which is now integrated with Cloud Foundation, that enables centralized and simplified lifecycle management of ESXi hosts.
workload domain	A policy based resource container with specific availability and performance attributes that combines vSphere, storage (vSAN, NFS, or VMFS on FC) and networking (NSX-T) into a single consumable entity. A workload domain can be created, expanded, and deleted as part of the SDDC lifecycle operations. It can contain cluster(s) of physical hosts with a corresponding vCenter to manage them. The vCenter for a workload domain physically lives in the management domain.