VMware Cloud Foundation on Dell EMC VxRail 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

Contents

About VMware Cloud Foundation on Dell EMC VxRail

1

The VMware Cloud Foundation on Dell EMC VxRail Administration Guide provides information on managing the integration of VMware Cloud Foundation and Dell EMC VxRail. As this product is an integration of VMware Cloud Foundation and Dell EMC VxRail, the expected results are obtained only when the configuration is done from both the products. This guide covers all the information regarding the VMware Cloud Foundation workflow. For the instructions on configuration to be done on Dell EMC VxRail, this guide provides links to the Dell EMC VxRail documentation.

Intended Audience

The *VMware VMware Cloud Foundation on Dell EMC VxRail Administration Guide* is intended for the system administrators of the VxRail environments who want to adopt VMware Cloud Foundation. The information in this document is written for experienced data center system administrators who are familiar with:

- Concepts of virtualization, software-defined data centers, and virtual infrastructure (VI).
- 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 software products, software components, and their features:

- Dell EMC VxRail Manager
- VMware vSphere®
- VMware vCenter Server® and VMware vCenter Server® Appliance™
- VMware vRealize® Log Insight™
- VMware vSphere® with VMware Tanzu™

Related Publications

The *Planning and Preparation Workbook* provides detailed information about the software, tools, and external services that are required to deploy VMware Cloud Foundation on Dell EMC VxRail.

Administering VMware Cloud Foundation on Dell EMC VxRail

2

VMware Cloud Foundation on Dell VMC VxRail enables VMware Cloud Foundation SDDC Manager on top of the Dell EMC VxRail platform.

An administrator of a VMware Cloud Foundation on Dell EMC VxRail system performs tasks such as:

- Manage certificates.
- 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 software components.

Prepare a VxRail Environment for Cloud Builder Appliance Deployment

3

Before you can deploy the VMware Cloud Builder Appliance on the VxRail cluster, you must complete the following tasks.

Procedure

1 Imaging the VxRail Management Nodes

Image the VxRail management nodes by using Dell EMC RASR (Rapid Appliance Self Recovery) process. Ensure that you update the RASR image in each server node SD card before you start the imaging process.

2 VxRail First Run for the Management Cluster

Imaging the VxRail Management Nodes

Image the VxRail management nodes by using Dell EMC RASR (Rapid Appliance Self Recovery) process. Ensure that you update the RASR image in each server node SD card before you start the imaging process.

For detailed information about how to image the VxRail management nodes, contact Dell EMC Support.

VxRail First Run for the Management Cluster

The VxRail first run for the management cluster consists of the following tasks:

- The discovery of the VxRail Nodes occurs. All the nodes that were imaged are detected.
- Upload the JSON configuration file. Trigger the validation.
- All the configuration inputs are validated.

The following components are deployed and enabled:

- vCenter
- VSAN
- VxRail Manager

Click **Manage VxRail** to log in to the VMware vCenter server.

For information on VxRail First Run, contact Dell EMC Support.

Deploy VMware Cloud Builder Appliance

4

The VMware Cloud Builder appliance is a VM that you use to deploy and configure the management domain and transfer inventory and control to SDDC Manager. During the deployment process, the VMware Cloud Builder validates network information you provide in the deployment parameter workbook such as DNS, network (VLANS, IPs, MTUs), and credentials.

This procedure describes deploying the VMware Cloud Builder appliance to the cluster that was created during the VxRail first run.

Prerequisites

The VMware Cloud Builder requires the following resources.

Component	Requirement
CPU	4 vCPUs
Memory	4 GB
Storage	150 GB

The VMware Cloud Builder appliance must be on the same management network as the hosts to be used. It must also be able to access all required external services, such as DNS and NTP.

Procedure

1. Download the VMware Cloud Builder appliance OVA.
2. Log in to vCenter Server using the vSphere Client.
3. In the navigator, select the cluster that was created during the VxRail first run.
4. Click **Actions > Deploy OVF Template**.
5. Select **Local file** and click **Upload Files**.
6. Browse to the VMware Cloud Builder appliance OVA, select it, and click **Open**.
7. Click **Next**.
8. Enter a name for the virtual machine, select a target location, and click **Next**.
9. Select the cluster you created during the VxRail first run and click **Next**.
10. Review the details and click **Next**.
11. Accept the license agreement and click **Next**.

12 On the Select Storage page, select the storage for the VMware Cloud Builder appliance and click **Next**.

13 On the Select networks dialog box, select the management network and click **Next**.

14 On the Customize template page, enter the following information for the VMware Cloud Builder appliance and click **Next**:

Setting	Details
Admin Username	The admin user name cannot be one of the following pre-defined user names: ■ root ■ bin ■ daemon ■ messagebus ■ systemd-bus-proxy ■ systemd-journal-gateway ■ systemd-journal-remote ■ systemd-journal-upload ■ systemd-network ■ systemd-resolve ■ systemd-timesync ■ nobody ■ sshd ■ named ■ rpc ■ tftp ■ ntp ■ smmsp ■ cassandra
Admin Password/Admin Password confirm	The admin password must be a minimum of 8 characters and include at least one uppercase, one lowercase, one digit, and one special character.
Root password/Root password confirm	The root password must be a minimum of 8 characters and include at least one uppercase, one lowercase, one digit, and one special character.
Hostname	Enter the hostname for the VMware Cloud Builder appliance.
Network 1 IP Address	Enter the IP address for the VMware Cloud Builder appliance.
Network 1 Subnet Mask	For example, `255.255.255.0`.
Default Gateway	Enter the default gateway for the VMware Cloud Builder appliance.
DNS Servers	IP address of the primary and secondary DNS servers (comma separated). Do not specify more than two servers.
DNS Domain Name	For example, `vsphere.local`.
DNS Domain Search Paths	Comma separated. For example `vsphere.local, sf.vsphere.local`.
NTP Servers	Comma separated.

15 Review the deployment details and click **Finish**.

Note Make sure your passwords meet the requirements specified above before clicking **Finish** or your deployment will not succeed.

16 After the VMware Cloud Builder appliance is deployed, SSH in to the VM with the admin credentials provided in step 14.

17 Ensure that you can ping the ESXi hosts.

18 Verify that the VMware Cloud Builder appliance has access to the required external services, such as DNS and NTP by performing forward and reverse DNS lookups for each host and the specified NTP servers.

Deploy the Management Domain Using VMware Cloud Builder

5

The VMware Cloud Foundation deployment process is referred to as bring-up. You specify deployment information specific to your environment such as networks, hosts, license keys, and other information in the deployment parameter workbook and upload the file to the VMware Cloud Builder appliance to initiate bring-up. During bring-up, the management domain is created on the ESXi hosts specified in the workbook. The VMware Cloud Foundation software components are automatically deployed, configured, and licensed using the information provided.

The following procedures describe how to perform bring-up of the management domain using the deployment parameter workbook. You can also perform bring-up using a custom JSON specification. See the VMware Cloud Foundation API Reference Guide for more information.

Externalizing the vCenter Server that gets created during the VxRail first run is automated as part of the bring-up process.

Download and Complete the Deployment Parameter Workbook

The deployment parameter workbook provides a mechanism to specify infrastructure information specific to your environment. This includes information about your networks, hosts, license keys, and other information. The workbook is downloaded from the VMware Cloud Builder appliance and the completed workbook is uploaded back to the VM. The deployment parameter workbook can be reused to deploy multiple Cloud Foundation instances of the same version.

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`.
2. Enter the admin credentials you provided when you deployed the VMware Cloud Builder appliance and then click **Log In**.
3. Read the End-User License Agreement and accept it. Click **Next**.
4. Select **VMware Cloud Foundation on VxRail** on the Supported Platform page and click **Next**.

5 Review the prerequisites checklist and ensure the requirements are met before proceeding. If there are any gaps, ensure they are fixed before proceeding to avoid issues during the bring-up process.

   Select the check box at the bottom of the page to acknowledge that your environment meets the listed requirements. You can download or print the prerequisite list as well.

6 Click **Next**.

7 In the Download Deployment Parameter Workbook section, click **Download**.

8 Complete the workbook. See About the Deployment Parameter Workbook.

About the Deployment Parameter Workbook

The deployment parameter workbook contains tabs categorizing the information required for deploying VMware Cloud Foundation. The information provided is used to create the management domain.

The fields in yellow contain sample values that you should replace with the information for your environment. If a cell turns red, the required information is missing, or validation has failed.

Prerequisites Checklist Tab

This tab is a summary of infrastructure configuration requirements that need to be satisfied before deploying Cloud Foundation.

The VMware Cloud Builder runs a platform audit before starting deployment to check if the requirements listed on this tab are met. If the audit fails, you cannot proceed with the deployment.

For detailed planning guidance, see the *Planning and Preparation Workbook*.

VxRail

- The VxRail first run is completed and vCenter Server and VxRail Manager VMs are deployed.
- The vCenter Server version matches the build listed in the Cloud Foundation Bill of Materials (BOM). See the *VMware Cloud Foundation Release Notes* for the BOM.

Physical Network

- Top of Rack switches are configured. Each host and NIC in the management domain must have the same network configuration. No Ethernet link aggregation technology (LAG/VPC/LACP) is being used.
- Jumbo Frames (MTU 9000) are recommended on all VLANs. At a minimum, an MTU of 1600 is required on the NSX-T Host Overlay (Host TEP) and NSX-T Edge Overlay (Edge TEP) VLANs end-to-end through your environment.
- If using DHCP for NSX-T Host Overlay TEPs: DHCP with an appropriate scope size (one IP per physical NIC per host) is configured for the NSX Host Overlay (Host TEP) VLAN.

- If using a static IP pool for NSX-T Host Overlay TEPs: Make sure you have enough IP addresses available for the number of hosts that will use the static IP Pool. Each host requires an IP address for each physical NIC (pNIC) that is used for the vSphere Distributed Switch that handles host overlay traffic. For example, a host with four pNICs that uses two pNICs for host overlay traffic requires two IP addresses in the static IP pool.
- To use Application Virtual Networks (AVNs) for vRealize Suite components you also need:
  - Top of Rack (ToR) switches configured with the Border Gateway Protocol (BGP), including Autonomous System (AS) numbers and BGP neighbor passwords, and interfaces to connect with NSX-T Edge nodes.
  - Two VLANs configured and presented to all ESXi hosts to support the uplink configuration between the (ToR) switches and NSX-T Edge nodes for outbound communication.

Physical Hardware and ESXi Hosts

- vSAN cluster with a minimum of four hosts. vSphere Distributed Switch is configured on the cluster. Management, vSAN, and vMotion networks are created. Management network binding type is Ephemeral.
- Identical hardware (CPU, Memory, NICs, SSD/HDD, and so on) within the management cluster is highly recommended. Refer to vSAN documentation for minimum configuration.
- The ESXi version matches the build listed in the Cloud Foundation Bill of Materials (BOM). See the *VMware Cloud Foundation Release Notes* for the BOM.

DNS Configuration

Host names for the following components must be resolvable for forward, reverse, short name, and long name resolution.

- ESXi hosts
- vCenter Server
- NSX-T Management cluster
- SDDC Manager
- VxRail Manager
- NSX Edge VMs (if AVN is enabled)

Management Workloads Tab

This tab provides an overview of the components deployed by the VMware Cloud Builder appliance. The sizes and versions are not editable and are provided for reference only.

Input required:

- In column L, update the red fields with your license keys. Ensure the license key matches the product and version listed in each row. The license key audit during bring-up validates both the format of the key entered and the validity of the key.

During the bring-up process, you can provide the following license keys:

- ESXi
- vSAN
- vCenter Server
- NSX-T Data Center
- SDDC Manager

Note The ESXi license key is the only mandatory key that must be provided. If the other license keys are left blank, then VMware Cloud Builder applies a temporary OEM license for vSAN, vCenter Server, and NSX-T Data Center.

If you do not enter license keys for these products, you will not be able to create or expand VI workload domains.

Users and Groups Tab

This tab details the accounts and initial passwords for the VMware Cloud Foundation components. You must provide input for each yellow box. A red cell may indicate that validations on the password length has failed.

Input Required

Update the Default Password field for each user (including the automation user in the last row). Passwords can be different per user or common across multiple users. The tables below provide details on password requirements.

Table 5-1. Password Complexity

Password	Requirements
VxRail Manager root account	Standard
VxRail Manager mystic account	Standard. The mystic account password must be different than the VXRail Manager root account password.
ESXi Host root account	This is the password which you configured on the hosts during ESXi installation.
Default Single-Sign on domain administrator user	1 Length 8-20 characters 2 Must include: ■ mix of upper-case and lower-case letters ■ a number ■ a special character, such as @ ! # $ % ^ or ? 3 Must not include * { } [ ] ( ) / \ ' " ` ~ , ; : . < >

Table 5-1. Password Complexity (continued)

Password	Requirements
vCenter Server virtual appliance root account	1 Length 8-20 characters 2 Must include: ■ mix of upper-case and lower-case letters ■ a number ■ a special character, such as @ ! # $ % ^ or ? 3 Must not include: * { } [ ] ( ) / \ ' " ` ~ , ; : . < >
NSX-T virtual appliance root account	1 Length 12-127 characters 2 Must include: ■ mix of uppercase and lowercase letters ■ a number ■ a special character, such as @ ! # $ % ^ or ? ■ at least five different characters 3 Must not include: * { } [ ] ( ) / \ ' " ` ~ , ; : . < >
NSX-T user interface and default CLI admin account	1 Length 12-127 characters 2 Must include: ■ mix of uppercase and lowercase letters ■ a number ■ a special character, such as @ ! # $ % ^ or ? ■ at least five different characters 3 Must not include: * { } [ ] ( ) / \ ' " ` ~ , ; : . < >
NSX-T audit CLI account	1 Legnth 12-127 characters 2 Must include: ■ mix of uppercase and lowercase letters ■ a number ■ a special character, such as @ ! # $ % ^ or ? ■ at least five different characters 3 Must not include: * { } [ ] ( ) / \ ' " ` ~ , ; : . < >
SDDC Manager	
SDDC Manager appliance root account	1 Length 8-20 characters 2 Must include: ■ mix of uppercase and lowercase letters ■ a number ■ a special character, such as @ ! # $ % ^ or ? 3 Must not include: * { } [ ] ( ) / \ ' " ` ~ , ; : . < >
SDDC Manager super user	1 Length 8-20 characters 2 Must include: ■ mix of uppercase and lowercase letters ■ a number ■ a special character, such as @ ! # $ % ^ or ? 3 Must not include: * { } [ ] ( ) / \ ' " ` ~ , ; : . < >

Table 5-1. Password Complexity (continued)

Password	Requirements
Local user	1 Length 12-20 characters 2 Must include: ■ mix of uppercase and lowercase letters ■ a number ■ a special character, such as @ ! # $ % ^ or ? 3 Must not include: * { } [ ] ( ) / \ ' " ` ~ , ; : . < >
SDDC Manager REST API user	1 Length 8-20 characters 2 Must include: ■ mix of uppercase and lowercase letters ■ a number ■ a special character, such as @ ! # $ % ^ or ? 3 Must not include: * { } [ ] ( ) / \ ' " ` ~ , ; : . < >

Hosts and Networks tab

In this tab, specify details of your existing networking infrastructure. This information is configured on the appropriate VMware Cloud Foundation components.

Management Domain Networks

This section covers the VLANs, gateways, MTU, and expected IP ranges and subnet mask for each network you have configured on the Top of Rack switches in your environment.

Table 5-2. Input Required

VLAN	Portgroup Name	CIDR Notation	Gateway	MTU
Enter VLAN ID for the management network. The VLAN ID can be between 0 and 4094.	Use default data.	Enter the CIDR notation for the management network.	Enter gateway IP for the management network.	Enter the MTU for the management network. The MTU can be between 1500 and 9000.
Enter VLAN ID for the vMotion network. The VLAN ID can be between 0 and 4094.	Use default data.	N/A	N/A	N/A
Enter VLAN ID for the vSAN network. The VLAN ID can be between 0 and 4094.	Use default data.	N/A	N/A	N/A
Enter VLAN ID for the first uplink. The VLAN ID can be between 0 and 4094.	Enter a portgroup name for the first uplink.	Enter the CIDR notation for the first uplink.	Enter gateway IP for the first uplink.	Enter the MTU for the first uplink. The MTU can be between 1500 and 9000.

Table 5-2. Input Required (continued)

VLAN	Portgroup Name	CIDR Notation	Gateway	MTU
Enter VLAN ID for the second uplink. The VLAN ID can be between 0 and 4094.	Enter a portgroup name for the second uplink.	Enter the CIDR notation for the second uplink.	Enter gateway IP for the second uplink.	Enter the MTU for the second uplink. The MTU can be between 1500 and 9000.
Enter VLAN ID for the NSX-T Edge overlay network. The VLAN ID can be between 0 and 4094.	N/A	Enter the CIDR notation for the NSX-T Edge overlay network.	Enter the gateway IP for the NSX-T Edge overlay network.	Enter the MTU for the NSX-T Edge overlay network. The MTU can be between 1600 and 9000.

NSX-T Host Overlay Network

By default, VMware Cloud Foundation uses DHCP for the management domain Host Overlay Network TEPs. For this option, 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.

Caution For L3 aware or stretch clusters, DHCP is required for Host Overlay Network TEP IP assignment.

For the management domain and VI workload domains with uniform L2 clusters, you can choose to use static IP addresses instead. 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..

Caution If you use static IP addresses for the management domain Host Overlay Network TEPs, you cannot stretch clusters in the management domain or any VI workload domains.

Table 5-3. DHCP Settings

Parameter	Value
VLAN ID	Enter a VLAN ID for the NSX-T host overlay network. The VLAN ID can be between 0 and 4094.
Configure NSX-T Host Overlay Using a Static IP Pool	Select **No** to use DHCP.

Table 5-4. Static IP Pool Settings

Parameter	Value
VLAN ID	Enter a VLAN ID for the NSX-T host overlay network. The VLAN ID can be between 0 and 4094.
Configure NSX-T Host Overlay Using a Static IP Pool	Select **Yes** to use a static IP pool.
Pool Description	Enter a description for the static IP pool.
Pool Name	Enter a name for the static IP pool.
CIDR Notation	Enter CIDR notation for the NSX-T Host Overlay network.
Gateway	Enter the gateway IP address for the NSX-T Host Overlay network.
NSX-T Host Overlay Start IP	Enter the first IP address to include in the static IP pool.
NSX-T Host Overlay End IP	Enter the last IP address to include in the static IP pool.

Management Domain ESXi Hosts

Specify the IP addresses of the ESXi hosts for the management domain. In a standard deployment, only four hosts are required in the management domain. VMware Cloud Foundation can also be deployed with a consolidated architecture. In a consolidated deployment, all workloads are deployed in the management domain instead of to separate workload domains. As such, additional hosts may be required to provide the capacity needed. In this section, only enter values for the number of hosts desired in the management domain.

Table 5-5. Input Required

Host Name	IP Address
sfo01m01esx01	Enter IP address of first ESXi host where VMware Cloud Foundation is to be deployed.
sfo01m01esx02	Enter IP address of second ESXi host
sfo01m01esx03	Enter IP address of third ESXi host
sfo01m01esx04	Enter IP address of fourth ESXi host

Security Thumbprints

If you want bring-up to validate the SSH fingerprints of the ESXi hosts and the SSH fingerprint and SSL thumbprint of the vCenter Server and VxRail Manager to reduce the chance of Man In The Middle (MiTM) attack, select **Yes** in the **Validate Thumbprints** field.

If you set **Validate Thumbprints** to **Yes**, follow the steps below.

1 Connect to the VMware Cloud Builder appliance using an SSH client such as Putty.

2 Enter the admin credentials you provided when you deployed the VMware Cloud Builder appliance.

3 Retrieve the SSH fingerprint by entering the following command replacing *hostname* with the FQDN of the first ESXi host:

```
ssh-keygen -lf <(ssh-keyscan hostname 2>/dev/null)
```

4 Repeat for the remaining ESXi hosts, vCenter Server, and VxRail Manager and then enter the information in the deployment parameter workbook.

5 Retrieve the SSL thumbprint by entering the following command replacing *hostname* with the FQDN of your vCenter Server:

```
openssl s_client -connect hostname:443 < /dev/null 2> /dev/null | openssl x509 -sha256
-fingerprint -noout -in /dev/stdin
```

6 Repeat to retrieve the SSL thumbprint for the VxRail Manager and then enter the information in the deployment parameter workbook.

Virtual Networking

The deployment parameter workbook provides five vSphere Distributed Switch profiles that allow you to perform bring-up of hosts with two, four, or six pNICs and create up to two vSphere Distributed Switches for isolating the VMkernel traffic. The information that you are required to provide depends on the profile that you select.

Note You can use the VMware Cloud Foundation on Dell EMC VxRail API to perform bring-up with other combinations of vSphere Distributed Switches and pNICs that are not available using the vSphere Distributed Switch profiles.

Note For hosts using 4x25GBe NICs, only Profile 2 and Profile 3 are supported.

vSphere Distributed Switch Profile	Description
Profile 1	■ One vSphere Distributed Switch (vDS) created by VxRail Manager ■ Two physical NICs (pNICs) ■ System traffic for Management, vMotion, and vSAN networks using specified pNICs. For example: vmnic0 and vmnic1 ■ Overlay traffic for Host Overlay, Edge Overlay, and Uplink networks using specified pNICs. For example: vmnic0 and vmnic1
Profile 2	■ One vSphere Distributed Switch (vDS) created by VxRail Manager ■ Four physical NICs (pNICs) ■ System traffic for Management uses two pNICs. For example: vmnic0 and vmnic1. System traffic for vMotion and vSAN networks uses two different pNICs. For example: vmnic2 and vmnic3 ■ Overlay traffic for Host Overlay, Edge Overlay, and Uplink networks uses the same pNICs as the Management traffic. For example: vmnic0 and vmnic1
Profile 3	■ Two vSphere Distributed Switches (vDS). Primary vDS is created during VxRail first run and secondary vDS is created during VCF bring-up. ■ Four physical NICs (pNICs) ■ Primary vDS: System traffic for Management, vSAN, and vMotion networks uses two pNICs. For example: vmnic0 and vmnic1 ■ Secondary vDS: Overlay traffic for Host Overlay, Edge Overlay, and Uplink networks uses two different pNICs. For example: vmnic2 and vmnic3

vSphere Distributed Switch Profile	Description
Profile 4	■ Two vSphere Distributed Switches (vDS). Primary vDS is created during VxRail first run and secondary vDS is created during VCF bring-up. ■ Six physical NICs (pNICs) ■ Primary vDS: System traffic for Management uses two pNICs. For example: vmnic0 and vmnic1. System traffic for vMotion and vSAN networks uses two pNICs. For example: vmnic2 and vmnic3 ■ Secondary vDS: Overlay traffic for Host Overlay, Edge Overlay, and Uplink networks uses two pNICs. For example: vmnic4 and vmnic5
Profile 5	■ Two vSphere Distributed Switches (vDS). Primary vDS is created during VxRail first run and secondary vDS is created during VCF bring-up. ■ Six physical NICs (pNICs) ■ Primary vDS: System traffic for Management, vSAN, and vMotion networks uses two pNICs. For example: vmnic0 and vmnic1 ■ Secondary vDS: Overlay traffic for Host Overlay, Edge Overlay, and Uplink networks uses four pNICs. For example: vmnic2, vmnic3, vmnic4, and vmnic5

After you select a vSphere Distributed Switch Profile, enter the required information for that profile.

Primary vSphere Distributed Switch - Name	Enter a name for the primary vSphere Distributed Switch (vDS).
Primary vSphere Distributed Switch - pNICs	Select the physical NICs to assign to the primary vDS.
Primary vSphere Distributed Switch - MTU Size	Enter the MTU size for the primary vDS. Default value is 9000.
Secondary vSphere Distributed Switch - Name	Enter a name for the secondary vSphere Distributed Switch (vDS). **Note** If you are not creating a secondary vDS, enter **`n/a`**.
Secondary vSphere Distributed Switch - pNICs	Select the physical NICs to assign to the secondary vDS.
Secondary vSphere Distributed Switch - MTU Size	Enter the MTU size for the secondary vDS. Default value is 9000.

Deploy Parameters Tab: Existing Infrastructure Details

Your existing DNS infrastructure is used to provide forward and reverse name resolution for all hosts and VMs in the VMware Cloud Foundation SDDC. External NTP sources are also utilized to synchronize the time between the software components.

Table 5-6. Infrastructure

Parameter	Value
DNS Server #1	Enter IP address of first DNS server.
DNS Server #2	Enter IP address of second DNS server. If you have only one DNS server, enter n/a in this cell.
NTP Server #1	Enter IP address or FQDN of first NTP server.
NTP Server #2	Enter IP address or FQDN of second NTP server. If you have only one NTP server, enter n/a in this cell.

Table 5-7. DNS Zone

Parameter	Value
DNS Zone Name	Enter root domain name for your SDDC management components.

Table 5-8. Customer Experience Improvement Program

Parameter	Value
Enable Customer Experience Improvement Program (“CEIP”)	Select an option to turn on or off CEIP across vSphere, NSX-T, and vSAN during bring-up.

Deploy Parameters Tab: vSphere Infrastructure

Specify details for the vSphere infrastructure.

This section of the deployment parameter workbook contains sample host names, but you can update them with names that meet your naming standards. This host name is one part of the FQDN - the second part of the FQDN is the root or child DNS zone name provided above.

The specified host names and IP addresses must be resolvable using the DNS servers provided earlier, both forward (hostname to IP) and reverse (IP to hostname), otherwise the bring-up process will fail.

Table 5-9. Management Cluster

Parameter	Host Name	IP Address
vCenter Server	Enter a host name for the vCenter Server.	Enter the IP address for the vCenter Server that is part of the management VLAN. This is the same VLAN and IP address space where the ESXi management VMKernels reside.

Table 5-10. vCenter Datacenter and Cluster

Parameter	Value
Datacenter Name	Enter a name for the management datacenter.
Cluster Name	Enter a name for the management cluster.

Note Enhanced vMotion Compatibility (EVC) is automatically enabled on the VxRail management cluster.

Select the architecture model you plan to use. If you choose **Consolidated**, specify the names for the vSphere resource pools. You do not need to specify resource pool names if you are using the standard architecture model. See *Introducing VMware Cloud Foundation* for more information about these architecture models.

Table 5-11. vSphere Resource Pools

Parameter	Value
Resource Pool SDDC Management	Specify the vSphere resource pool name for management VMs.
Resource Pool SDDC Edge	Specify the vSphere resource pool name for NSX-T VMs.
Resource Pool User Edge	Specify the vSphere resource pool name for user deployed NSX-T VMs in a consolidated architecture.
Resource Pool User VM	Specify the vSphere resource pool name for user deployed workload VMs in a consolidated architecture.

Table 5-12. vSphere Datastore

Parameter	Value
vSAN Datastore Name	Enter vSAN datastore name for your management components.

Deploy Parameters Tab: NSX-T Data Center

Enter IP addresses and host names for NSX-T installation.

Table 5-13. NSX-T Management Cluster

Parameter	Value
NSX-T Management Cluster VIP	Enter the host name and IP address for the NSX Manager VIP. The host name can match your naming standards but must be registered in DNS with both forward and reverse resolution matching the specified IP. The IP address must be part of the management VLAN. This is the same VLAN and IP address space where the vCenter and ESXi management VMKernels reside.
NSX-T Virtual Appliance Node #1	Enter the host name and IP address for the first node in the NSX Manager cluster.
NSX-T Virtual Appliance Node #2	Enter the host name and IP address for the second node in the NSX Manager cluster.
NSX-T Virtual Appliance Node #3	Enter the host name and IP address for the third node in the NSX Manager cluster.
NSX-T Virtual Appliance Size	Select the size for the NSX Manager virtual appliances. The default is medium.

Application Virtual Networking

Application virtual networks (AVNs) are virtual networks, backed by overlay segments using the encapsulation protocol of NSX-T, that use a single IP network address space to span across data centers. By default, VMware Cloud Foundation deploys and configures AVNs during bring-up. If you do not want to deploy and configure AVNs, select **No** from the drop-down menu. Deselect AVNs if you want to deploy vRealize Suite components to VLAN-backed networks.

A two-node NSX-T Edge cluster routes traffic between the AVNs and the public network. Routing to the management network and external networks is dynamic and based on the Border Gateway Protocol (BGP).

Table 5-14. NSX-T Edge Nodes with ECMP

Parameter	Value
NSX-T Edge Cluster Name	Enter a name for the Edge cluster.
NSX-T Edge Nodes Autonomous System ID	Enter the AS ID of the Edge nodes to peer with ToR switches.
NSX-T Edge Node Appliance Size	The default size is medium.

Table 5-15. North-South Routing Edge Node 1

Parameter	Value
Edge Name Node 1	Enter a name for the first Edge node. The Edge node name must match the short hostname reserved for the VM. Combined with the DNS Zone Name this should match the FQDN reserved for the VM in the DNS server.
Edge Management IP Address Node 1	Enter a management IP address for the first node. The IP address must be part of the management VLAN.
Edge Uplink 1 IP Address Node 1	Enter the first uplink IP address to use for Node 1. This is the IP address connected to the first ToR switch. The IP address must be part of the NSX-T Edge Uplink 1 VLAN.
Edge Uplink 2 IP Address Node 1	Enter the second uplink IP address to use for Node 1. This is the IP address connected to the second ToR switch. The IP address must be part of the NSX-T Edge Uplink 2 VLAN.
Edge Overlay IP Address #01 Node 1	Enter the first Edge overlay IP address to use for Node 1. The IP address must be part of the NSX-T Edge Overlay VLAN.
Edge Overlay IP Address #02 Node 1	Enter the second Edge overlay IP address to use for Node 1. The IP address must be part of the NSX-T Edge Overlay VLAN.

Table 5-16. North-South Routing Edge Node 2

Parameter	Value
Edge Name Node 2	Enter a name for the second Edge node. The Edge node name must match the short hostname reserved for the VM. Combined with the DNS Zone Name this should match the FQDN reserved for the VM in the DNS server.
Edge Management IP Address Node 2	Enter a management IP address for the second node. The IP address must be part of the management VLAN.
Edge Uplink 1 IP Address Node 2	Enter the first uplink IP address to use Node 2. This is the IP address connected to the first ToR switch. The IP address must be part of the NSX-T Edge Uplink 1 VLAN.
Edge Uplink 2 IP Address Node 2	Enter the second uplink IP address to use for Node 2. This is the IP address connected to the second ToR switch. The IP address must be part of the NSX-T Edge Uplink 2 VLAN.
Edge Overlay IP Address #01 Node 2	Enter the first Edge overlay IP address to use for Node 2. The IP address must be part of the NSX-T Edge Overlay VLAN.
Edge Overlay IP Address #02 Node 2	Enter the first Edge overlay IP address to use for Node 2. The IP address must be part of the NSX-T Edge Overlay VLAN.

Prepare your top of rack (ToR) switches by configuring Border Gateway Protocol (BGP) on the switches, defining the Autonomous System (AS) number, BGP password, Router ID, and creating interfaces to connect with Edge nodes.

Table 5-17. Top of Rack Switches for BGP Peering

Parameter	Value
Top of Rack 1 - IP Address	Enter the IP address of the first ToR switch.
Top of Rack 1 - Autonomous System ID	Enter the AS ID for the first switch.
Top of Rack 1 - BGP Neighbor Password	Enter the BGP neighbor password for the first switch.
Top of Rack 2 - IP Address	Enter the IP address of the second ToR switch.
Top of Rack 2 - Autonomous System ID	Enter the AS ID for the second switch. This should match the AS ID for the first switch.
Top of Rack 2 - BGP Neighbor Password	Enter the BGP neighbor password for the second switch.

Prepare your top of rack (ToR) switches to announce the subnets configured on the logical segments over BGP to make the segments routable in the data center.

Table 5-18. Application Virtual Networks

Parameter	Value
Region A - Logical Segment	Enter a name to use for the Region A logical segment.
Region A - Networks	Enter the gateway IP and CIDR notation to use for the Region A network.
xRegion - Logical Segment	Enter a name to use for the xRegion logical segment.
xRegion - Networks	Enter the gateway IP and CIDR notation to use for the xRegion network.

The following example shows how the NSX-T Data Center parameters (with AVNs) that you specify in the deployment parameter workbook map to the network topology in NSX Manager.

Figure 5-1. NSX-T Data Center Deployment Parameters

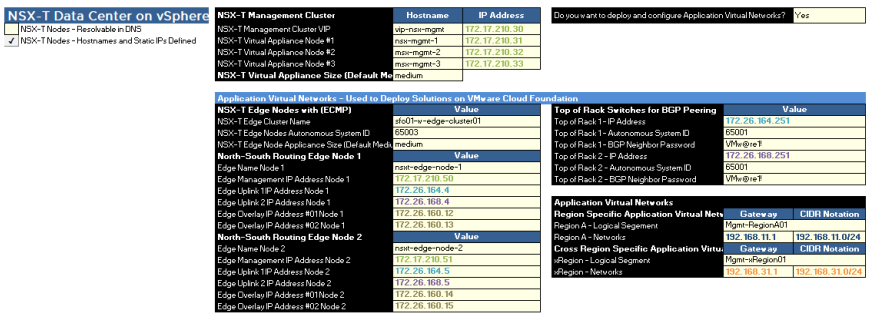
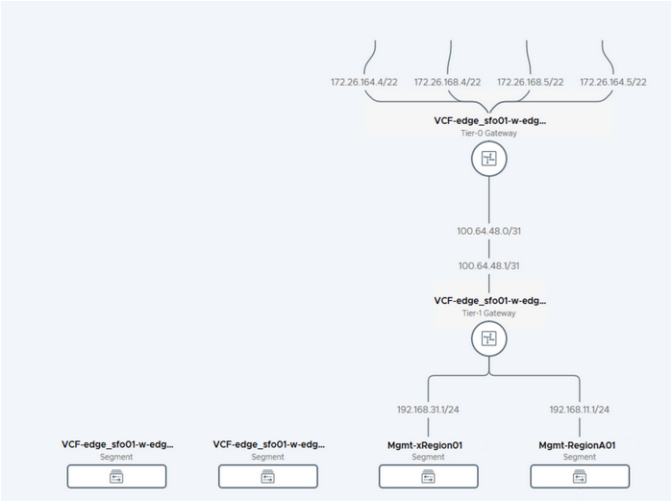


Figure 5-2. Post-Deployment Network Topology Viewed in NSX Manager



Deploy Parameters Tab: SDDC Manager

Enter the host name, IP address, and subnet mask of the SDDC Manager VM.

Table 5-19. SDDC Manager

Parameter	Value
SDDC Manager Host name	Enter a host name for the SDDC Manager VM. The specified host name must be registered with your DNS server for both forward and reverse resolution, and it must be resolvable from the VMware Cloud Builder.
SDDC Manager IP Address	Enter an IP address for the SDDC Manager VM. The IP address must be registered with your DNS server for both forward and reverse resolution, and must be part of the management VLAN.
Cloud Foundation Management Domain Name	Enter a name for the management domain. This name will appear in **Inventory > Workload Domains** in the SDDC Manager UI.

Upload the Deployment Parameter Workbook and Deploy the Management Domain

You upload the completed deployment parameter workbook to complete bring-up.

Procedure

1. In the Download Deployment Parameter Workbook section, click **Next**.
2. In the Complete Deployment Parameter Workbook section, click **Next**.
3. In the Upload File section, click **Select File**. Select the completed deployment parameter workbook and click **Open**.

4 After the file is uploaded, click **Next** to begin validation of the uploaded file. You can download or print the validation list.

   To access the bring-up log file, SSH to the VMware Cloud Builder appliance as root and open the `/opt/vmware/bringup/logs/vcf-bringup-debug.log` file.

   If there is an error during the validation and the Next button is grayed out, you can either make corrections to the environment or edit the JSON file and upload it again. Then click **Re-Try** to perform the validation again.

   If any warnings are displayed and you want to proceed, click **Acknowledge** and then click **Next**.

5 Click **Deploy SDDC**.

   During the bring-up process, the following tasks are completed.

   - vCenter Server, vSAN, and NSX-T components are deployed.
   - The management domain is created, which contains the management components - SDDC Manager, vCenter Server, and NSX-T components.

   The status of the bring-up tasks is displayed in the UI.

   After bring-up is completed, a green bar is displayed indicating that bring-up was successful. A link to the SDDC Manager UI is also displayed.

   If there are errors during bring-up, see Chapter 6 Troubleshooting VMware Cloud Foundation Deployment for guidance on how to proceed.

6 Click **Download** to download a detailed deployment report. This report includes information on assigned IP addresses and networks that were configured in your environment.

7 After bring-up is completed, click **Finish**.

8 In the SDDC Deployment Completed dialog box, click **Launch SDDC Manager**.

9 Verify the following:

   - View management domain details.
   - Log in to vCenter Server and verify the management cluster, vSAN cluster, and deployed VMs.

10 Power off the VMware Cloud Builder appliance.

   The VMware Cloud Builder appliance includes the VMware Imaging Appliance service, which you can use to install ESXi on additional servers after bring-up is complete. You can delete the VMware Cloud Builder appliance to reclaim its resources or keep it available for future server imaging.

   Caution Do not modify or delete any vDS or port groups, or modify the default configuration.

Upgrade VMware vCenter Server Appliance for VMware Cloud Foundation 4.2.1

If you are deploying VMware Cloud Foundation 4.2.1, you must upgrade the VMware vCenter Server Appliance to the version that is supported with VMware Cloud Foundation 4.2.1.

During the VxRail first run, VxRail Manager 7.0.131 deploys vCenter Server 7.0 Update 1c (build 17327517). However, the VMware Cloud Foundation 4.2.1 BOM requires vCenter Server 7.0.1.00301 (build 17956102). Until you upgrade vCenter Server, you will not be able to deploy a VI workload domain.

Procedure

- Download and apply the upgrade bundle for vCenter Server. See Download VMware Cloud Foundation on Dell EMC VxRail Bundles.

Troubleshooting VMware Cloud Foundation Deployment

6

You can run the Supportability and Serviceability (SoS) Utility and review bring-up log files to troubleshoot deployment issues.

This chapter includes the following topics:

Using the SoS Utility on VMware Cloud Builder

You can run the Supportability and Serviceability (SoS) Utility on the VMware Cloud Builder appliance to generate a support bundle, which you can use to help debug a failed bring-up of VMware Cloud Foundation.

Note After a successful bring-up, you should only run the SoS Utility on the SDDC Manager appliance. See Supportability and Serviceability (SoS) Tool in the *VMware Cloud Foundation Operations and Administration Guide*.

The SoS Utility is not a debug tool, but it does provide health check operations that can facilitate debugging a failed deployment.

To run the SoS Utility in VMware Cloud Builder, SSH in to the VMware Cloud Builder appliance using the **admin** administrative account, then 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.

```
./sos --option-1 --option-2 ... --option-n
```

SoS Utility Help Options

Use these options to see information about the SoS tool itself.

Option	Description
`--help` `-h`	Provides a summary of the available SoS tool options
`--version` `-v`	Provides the SoS tool's version number.

SoS Utility Generic Options

These are generic options for the SoS Utility.

Option	Description
`--configure-sftp`	Configures SFTP for logs.
`--debug-mode`	Runs the SoS tool in debug mode.
`--force`	Allows SoS operations from theVMware Cloud Builder appliance after bring-up. **Note** In most cases, you should not use this option. Once bring-up is complete, you can run the SoS Utility directly from the SDDC Manager appliance.
`--history`	Displays the last twenty SoS operations performed.
`--log-dir` *`LOGDIR`*	Specifies the directory to store the logs.
`--log-folder` *`LOGFOLDER`*	Specifies the name of the log directory.
`--setup-json` *`SETUP_JSON`*	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 `setup.json` file and pass the file as input to SoS. A sample JSON file is available on the VMware Cloud Builder in the `/opt/vmware/sddc-support/` directory.
`--skip-known-host-check`	Skips the specified check for SSL thumbprint for host in the known host.
`--zip`	Creates a zipped tar file for the output.

SoS Utility Log File Options

Option	Description
`--api-logs`	Collects output from APIs.
`--cloud-builder-logs`	Collects Cloud Builder logs.
`--esx-logs`	Collects logs from the ESXi hosts only. Logs are collected from each ESXi host available in the deployment.

Option	Description
`--no-clean-old-logs`	Use this option to prevent the tool from removing any output from a previous collection run. By default, before writing the output to the directory, the tool deletes the prior run's output files that might be present. If you want to retain the older output files, specify this option.
`--no-health-check`	Skips the health check executed as part of log collection.
`--nsx-logs`	Collects logs from the NSX Manager instances only.
`--rvc-logs`	Collects logs from the Ruby vSphere Console (RVC) only. RVC is an interface for ESXi and vCenter. **Note** If the Bash shell is not enabled in vCenter, RVC log collection will be skipped . **Note** RVC logs are not collected by default with ./sos log collection.
`--sddc-manager-logs`	Collects logs from the SDDC Manager only.
`--test`	Collects test logs by verifying the files.
`--vc-logs`	Collects logs from the vCenter Server instances only. Logs are collected from each vCenter server available in the deployment.
`--vm-screenshots`	Collects screen shots from all VMs.

SoS Utility JSON Generator Options

The JSON generator options within the SoS Utility provide a method to execute the creation of the JSON file from a completed deployment parameter workbook. To run the JSON generator, you must provide, as a minimum, a path to the deployment parameter workbook and the design type using the following syntax:

```
./sos --jsongenerator --jsongenerator-input JSONGENERATORINPUT --jsongenerator
JSONGENERATORDESIGN
```

Option	Description
`--jsongenerator`	Invokes the JSON generator utility.
`--jsongenerator-input` *`JSONGENERATORINPUT`*	Specify the path to the input file to be used by the JSON generator utility. For example: `/tmp/vcf-ems-deployment-parameter.xlsx`.
`--jsongenerator-design` *`JSONGENERATORDESIGN`*	Use **`vcf-public-vxrail`** for VMware Cloud Foundation on Dell EMC VxRail.
`--jsongenerator-supress`	Supress confirmation to force cleanup directory. (optional)
`--jsongenerator-logs` *`JSONGENERATORLOGS`*	Set the directory to be used for logs. (optional)

SoS Utility Platform Audit Options

The Platform Audit options provide a method to execute validation tasks from the command line and offer the flexibility to validate individual tasks, or all tasks at once. Validating individual tasks helps accelerate the troubleshooting process, since you can validate that task repeatedly until it succeeds.

To run a platform audit, you must provide, as a minimum, a path to the JSON input file:

```
./sos --platformaudit --platformaudit-input FILE
```

Note The platform audit capabilities of the SoS Utility have been deprecated and will be removed in the next release of VMware Cloud Foundation. All functionality has been ported over to the new bring-up validation service. When you initiate validation through the VMware Cloud Builder administration interface, the bring-up validation service performs the validation tasks. All logging is directed to the `vcf-bringup.log` and `vcf-debug-bringup.log` files. You can use the SoS Utility platform audit options in this release, but this method may not contain enhancements to validation tasks that are available through the bring-up validation service.

Option	Description
`--platformaudit`	Invokes the platform audit operation.
`--platformaudit-dependency`	Executes audit tests with dependencies.
`--platformaudit-input FILE`	Specify the path to the JSON input file to be used by the platform audit utility.
`--platformaudit-stop`	Stops all running platform audit processes.
`--platformaudit-modules MODULE1,MODULE2,MODULE3`	Specify the specific audit tests to run. If specifying multiple tests, separate the modules with commas.
`--platformaudit-output OUTPUT`	Saves the output to the specified file.
`--platformaudit-reason`	Outputs reasons for failed or skipped tests.
`--platformaudit-tree`	Displays a list of available audit tests.

SoS Utility Health Check Options

The SoS Utility can be used to perform health checks on various components or services, including connectivity, compute, and storage.

Note The health check options are primarily designed to run on the SDDC Manager appliance. Running them on the VMware Cloud Builder appliance requires the `--force` parameter, which instructs the SoS Utility to identify the SDDC Manager appliance deployed by VMware Cloud Builder during the bring-up process, and then execute the health check remotely. For example:

```
./sos --health-check --force
```

Option	Description
`--certificate-health`	Verifies that the component certificates are valid (within the expiry date).
`--connectivity-health`	Performs a connectivity health check to inspect whether the different components of the system such as the ESXi hosts, vCenter Servers, NSX Manager VMs, and SDDC Manager VM can be pinged.
`--compute-health`	Performs a compute health check.
`--general-health`	Verifies ESXi entries across all sources, checks the Postgres DB operational status for hosts, checks ESXi for error dumps, and gets NSX Manager and cluster status.
`--get-host-ips`	Returns server information.
`--health-check`	Performs all available health checks.
`--ntp-health`	Verifies whether the time on the components is synchronized with the NTP server in the VMware Cloud Builder appliance.
`--services-health`	Performs a services health check to confirm whether services are running
`--run-vsan-checks`	Runs proactive vSAN tests to verify the ability to create VMs within the vSAN disks.

Sample Output

The following text is a sample output from an `--ntp-health` operation.

```
root@cloud-builder [ /opt/vmware/sddc-support ]# ./sos --ntp-health --skip-known-host --force
Welcome to Supportability and Serviceability(SoS) utility!

User passed --force flag, Running SOS from Cloud Builder VM, although Bringup is completed
and SDDC Manager is available. Please expe           ct failures with SoS operations.
Health Check : /var/log/vmware/vcf/sddc-support/healthcheck-2020-02-11-23-03-53-24681
Health Check log : /var/log/vmware/vcf/sddc-support/healthcheck-2020-02-11-23-03-53-24681/
sos.log
SDDC Manager : sddc-manager.vrack.vsphere.local
NTP : GREEN
+-----+----------------------------------------+------------+-------+
| SL# |                  Area                  |   Title    | State |
+-----+----------------------------------------+------------+-------+
|  1  |    ESXi : esxi-1.vrack.vsphere.local    |  ESX Time  | GREEN |
|  2  |    ESXi : esxi-2.vrack.vsphere.local    |  ESX Time  | GREEN |
|  3  |    ESXi : esxi-3.vrack.vsphere.local    |  ESX Time  | GREEN |
|  4  |    ESXi : esxi-4.vrack.vsphere.local    |  ESX Time  | GREEN |
|  5  | vCenter : vcenter-1.vrack.vsphere.local | NTP Status | GREEN |
+-----+----------------------------------------+------------+-------+

Legend:

 GREEN - No attention required, health status is NORMAL
 YELLOW - May require attention, health status is WARNING
 RED - Requires immediate attention, health status is CRITICAL
```

```
Health Check completed successfully for : [NTP-CHECK]
```

The following text is sample output from a `--vm-screenshots` log collection operation.

```
root@cloud-builder [ /opt/vmware/sddc-support ]# ./sos --vm-screenshots
     --skip-known-host --force
Welcome to Supportability and Serviceability(SoS) utility!

User passed --force flag, Running SOS from Cloud Builder VM, although Bringup is completed
and SDDC Manager is available. Please expect failures with SoS operations.
Logs : /var/log/vmware/vcf/sddc-support/sos-2018-08-24-10-50-20-8013
Log file : /var/log/vmware/vcf/sddc-support/sos-2018-08-24-10-50-20-8013/sos.log
Log Collection completed successfully for : [VMS_SCREENSHOT]
```

VMware Cloud Builder Log Files

VMware Cloud Builder has a number of components which are used during the bring-up process and each component generates a log file which can be used for the purpose of troubleshooting.

The components and their purpose are:

- JsonGenerator: Used to convert the deployment parameter workbook into the required configuration file (JSON) that is used by the Bringup Validation Service and Bringup Service.
- Bringup Service: Used to perform the validation of the configuration file (JSON), the ESXi hosts and infrastructure where VMware Cloud Foundation will be deployed, and to perform the deployment and configuration of the management domain components and the first cluster.
- Supportability and Serviceability (SoS) Utility: A command line utility for troubleshooting deployment issues.

The following table describes the log file locations:

Component	Log Name	Location
JsonGenerator	`jsongenerator-`*`timestamp`*	`/var/log/vmware/vcf/sddc-support/`
Bringup Service	`vcf-bringup.log`	`/var/log/vmware/vcf/bringup/`
	`vcf-bringup-debug.log`	`/var/log/vmware/vcf/bringup/`
	`rest-api-debug.log`	`/var/log/vmware/vcf/bringup/`
SoS Utility	`sos.log`	`/var/log/vmware/vcf/sddc-support/sos-`*`timestamp`*`/`

Getting Started with SDDC Manager

7

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 SDDC Manager UI

You access SDDC Manager through SDDC Manager UI 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 SDDC Manager UI 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	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. You can control the widgets that are displayed and how they are arranged on the dashboard. ■ To rearrange widgets, click the heading of the widget and drag it to the desired position. ■ To hide a widget, hover the mouse anywhere over the widget to reveal the **X** in the upper-right corner, and click the **X**. ■ To add a widget, click the three dots in the upper right corner of the page and select **Add New Widgets**. This displays all hidden widgets. Select a widget and click **Add**.
Solutions	Solutions include the following section: ■ Kubernetes - Workload Management enables you to start a Workload Management deployment and view Workload Management cluster details.

Category	Functional Areas
Inventory	Inventory includes the following sections: ■ **Workload Domains** takes you to the Workload Domains page, which displays and provides access to all workload domains. 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. ■ **Hosts** takes you to the Hosts page, which displays and provides access to current hosts and controls for managing hosts. 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.
Lifecycle Management	Lifecycle Management includes the following sections: **Bundle Management** displays the available install, update, and upgrade bundles for your environment, and your bundle download history. **Note** To access bundles, you must be logged in to your My VMware account through the **Administration > Repository Settings** page.

Category	Functional Areas
Administration	Administration includes the following sections: ■ **Licensing** enables you to manage VMware product licenses. You can also add licenses for the component products in your VMware Cloud Foundation deployment. ■ **Users** enables you to manage VMware Cloud Foundation users and groups, including adding users and groups and assigning roles. ■ **Repository Settings** enables you to log in to your My VMware and Dell EMC accounts. ■ **vRealize Suite** enables you to deploy vRealize Suite Lifecycle Manager. ■ **Security** enables you to integrate with your Microsoft Certificate Authority Server and perform password management actions, such as rotation, updates and remediation. ■ **Backup** 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. ■ **VMware CEIP** to join or leave the VMware Customer Experience Improvement Program.
Developer Center	The VMware Cloud Foundation Developer Center includes the following sections: ■ **Overview**: API reference documentation. Includes information and steps for all the Public APIs supported by VMware Cloud Foundation. ■ **API Explorer**: Lists the APIs and allows you to invoke them directly on your VMware Cloud Foundation system. ■ **Code Samples**: Sample code to manage a VMware Cloud Foundation instance.

Log out of SDDC Manager UI

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

Procedure

1 In SDDC Manager UI, 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

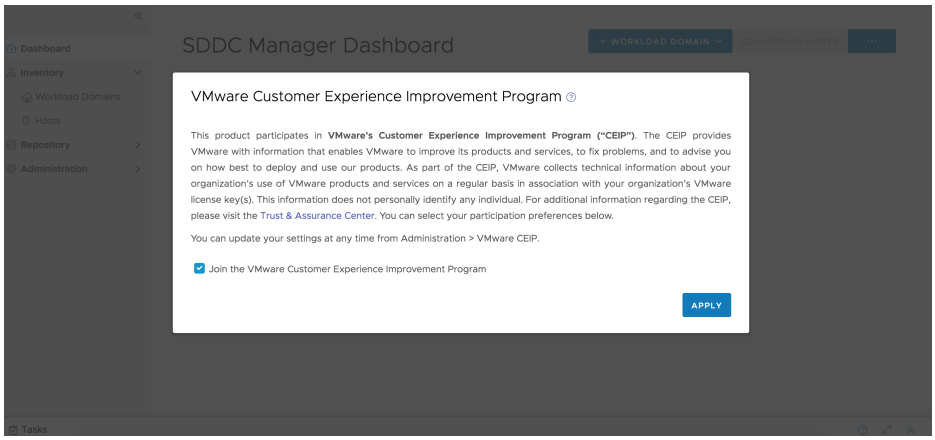
8

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

9

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
- VxRail Manager
- vRealize Suite Lifecycle Manager

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.

This chapter includes the following topics:

View Certificate Information

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

Procedure

1 In SDDC Manager UI, 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 **`Microsoft`**.
CA Server URL	Specify the URL for the CA address server. This address must begin with **`https://`** and end with **`certsrv`**, for example **`https://www.mymicrosoftca.com/certsrv`**
Username	Provide a valid user name to enable access to the address server.
Password	Provide a valid password to enable access to the address server.
Template Name	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	Specify the FQDN of OpenSSL CA.
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 SDDC Manager UI.

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 SDDC Manager UI, 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
Algorithm	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.
Key Size	Select the key size (2048 bit, 3072 bit, or 4096 bit) from the drop-down menu.
Email	Optionally, enter a contact email address.
Organizational Unit	Use this field to differentiate between divisions within your organization with which this certificate is associated.
Organization	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.
Locality	Type the city or locality where your company is legally registered.
State or Province Name	Type the full name (do not abbreviate) of the state, province, region, or territory where your company is legally registered.
Country	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 appliance 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 SDDC Manager UI and have it manually signed by a third-party CA. You can then use the controls in SDDC Manager UI 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 `.csr` file, whose name must exactly match the resource as it appears in the Resource Hostname column in the **Workload Domains > Security** tab.

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

  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`.

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

Procedure

1 In SDDC Manager UI, 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
Algorithm	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.
Key Size	Select the key size (2048 bit, 3072 bit, or 4096 bit) from the drop-down menu.
Email	Optionally, enter a contact email address.
Organizational Unit	Use this field to differentiate between divisions within your organization with which this certificate is associated.
Organization	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.
Locality	Type the city or locality where your company is legally registered.
State or Province Name	Type the full name (do not abbreviate) of the state, province, region, or territory where your company is legally registered.
Country	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 SDDC Manager UI, 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 appliance 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 appliance.

Procedure

1 Using SSH, log in to the SDDC Manager appliance 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

10

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

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

Working with Workload Domains 11

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.

vSphere Distributed Switch (vDS) for Backup or VM Traffic

When you deploy VMware Cloud Foundation on Dell EMC VxRail, you can create one or two vSphere Distributed Switches. With one vDS, all system traffic (management, vSAN, and vMotion) and overlay traffic (host, Edge, and uplinks) is carried on the same vDS. With two vDSes, system traffic is carried on one vDS and overlay traffic is carried on the other vDS.

VMware Cloud Foundation supports the manual creation of an additional vDS, using the vSphere Client, for backup or VM traffic. You can create this vDS either before or after you import the VxRail cluster into SDDC Manager. Hosts in the cluster must have two or four free pNICs and must be cabled to the ToR switches.

This additional vDS cannot be used for system or overlay traffic and is not managed by VMware Cloud Foundation. If you add new hosts to the system, you must manually add them to the vDS.

This chapter includes the following topics:

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 name, compute, and networking details for the VI workload domain. 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.

- Configures networking on each host.
- 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.
- 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.

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 available for the workload domain.

- 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 14 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
  - 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 11-1. 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.
- You must have valid license keys for the following products:
  - NSX-T Data Center
  - vSAN
  - 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 10 License Management.

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 upto 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.

Note After enabling HCI Mesh by mounting remote vSAN datastores, you can migrate VMs from the local datastore to a remote datastore. Since each cluster has its own VxRail Manager VM, you should not migrate VxRail Manager VMs to a remote datastore.

Create a VxRail VI Workload Domain

Use the VxRail VI Configuration wizard to create a workload domain.

Procedure

1 On the **SDDC Manager** Dashboard, click **+ Workload Domain** and then select **VI-VxRail Virtual Infrastructure Setup**.

2 Type a name for the VxRail VI workload domain, such as **`sfo01`**.

   The name must contain between 3 and 20 characters. It is a good practice to include location information in the name as resource object names (such as host and vCenter names) are generated on the basis of the VI workload domain name.

3 Type a name for the organization that requested or will use the virtual infrastructure, such as **`Finance`** and click **Next**.

   The name must contain between 3 and 20 characters.

4 On the Compute page of the wizard, enter the vCenter Server DNS name.

5 Type the vCenter Server subnet mask and default gateway.

6 Type and re-type the vCenter Server root password and click **Next**.

7 Review the details and click **Next**.

8 On the **Validation** page, wait until all of the inputs have been successfully validated and then click **Finish**.

   If validation is unsuccessful, you cannot proceed. Use the **Back** button to modify your settings and try again.

What to do next

Add the primary VxRail cluster to the workload domain. The status of the VI workload domain creation task will be `Activating` until you do so. See Add the Primary VxRail Cluster.

Add the Primary VxRail Cluster

The primary cluster is created during the VI domain creation.

Before adding the VxRail cluster, you need to perform the imaging of the workload domain nodes. Once you complete the imaging, perform the VxRail first run of the workload domain nodes using the external vCenter Server.

- Create a local user in vCenter server as this is an external server deployed by VMware Cloud Foundation. This is required for the VxRail first run.
  a Log in to the workload domain vCenter Server Appliance through vSphere Web Client.
  b Select **Menu > Administration > Single Sign On**.
  c Click **Users and Groups**.
  d Click **Users**.
  e Select **Domain vSphere.local**.
  f Click **Add User**.
  g In the **Add User** pop-up window, enter the values for the mandatory fields.
  h Enter **Username** as `vxadmin` and **Password.** Confirm the **Password**.

i Click **Add**.

j Wait for the task to complete.

- Image the workload domain nodes. For information on imaging the nodes, contact Dell EMC Support.
- Do a VxRail first run of the workload domain nodes using the external vCenter Server. For information on the VxRail first run, contact Dell EMC Support.
- Once the validation is complete, trigger the build VxRail operation.
- The cluster is created in VxRail.

To add a cluster with a new NSX-T cluster and vDS for an overlay traffic isolation, see Add a Cluster with a New NSX-T Cluster and vDS. To add a cluster with a shared NSX-T cluster and new vDS for an overlay traffic isolation, see Add a Cluster with a Shared NSX-T Cluster and New vDS. To add the primary VxRail cluster to a workload domain through the UI, perform the following tasks:

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, hover your mouse over workload domain in the activating state. The primary cluster needs to be added to the activating domain. This means that the domain is not created and it is waiting for the addition of primary cluster.

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

3 Click these three dots. Click **Add VxRail Cluster**.

4 On the **Discovered Clusters** page, a single VxRail cluster or multiple VxRail clusters in the vCenter are discovered. If there are multiple clusters, select a cluster. Click **Next**.

5 The **Discovered Hosts** page displays a list of the discovered hosts for that cluster. Enter the SSH password for the discovered hosts and click **Next**.

6 On the **VxRail Manager** page, enter the Admin and Root usernames and passwords.

7 On the **Thumbprint Verification** page, click  to confirm the SSH thumbprints for VxRail Manager and the ESXi hosts.

8 The **Networking** page displays all the networking details for the cluster.

a 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.

b 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. Click **Next**.

c If you are creating a new NSX Manager cluster, enter the VLAN ID for the NSX-T host overlay (host TEP) network.

d Select the IP allocation method.

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. 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.
Static IP Pool	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. To create a new static IP Pool provide the following information: ■ Pool Name ■ Description ■ CIDR ■ IP Range. ■ Gateway IP 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. **Note** You cannot stretch a cluster that uses static IP addresses for the NSX-T Host Overlay Network TEPs.

e Provide the NSX Manager cluster details:

- NSX Manager Virtual IP (VIP) address and FQDN
- IP addresses and FQDNs for three NSX Managers (nodes)
- NSX Manager Admin password

f Click **Next**.

9 Enter the license keys for NSX-T Data Center and VMware vSAN. Click **Next**.

10 Review the details and click **Next**.

11 On the **Validation** page, wait until all of the inputs have been successfully validated.

If validation is unsuccessful, you cannot proceed. Use the **Back** button to modify your settings and try again.

12 Click **Finish**.

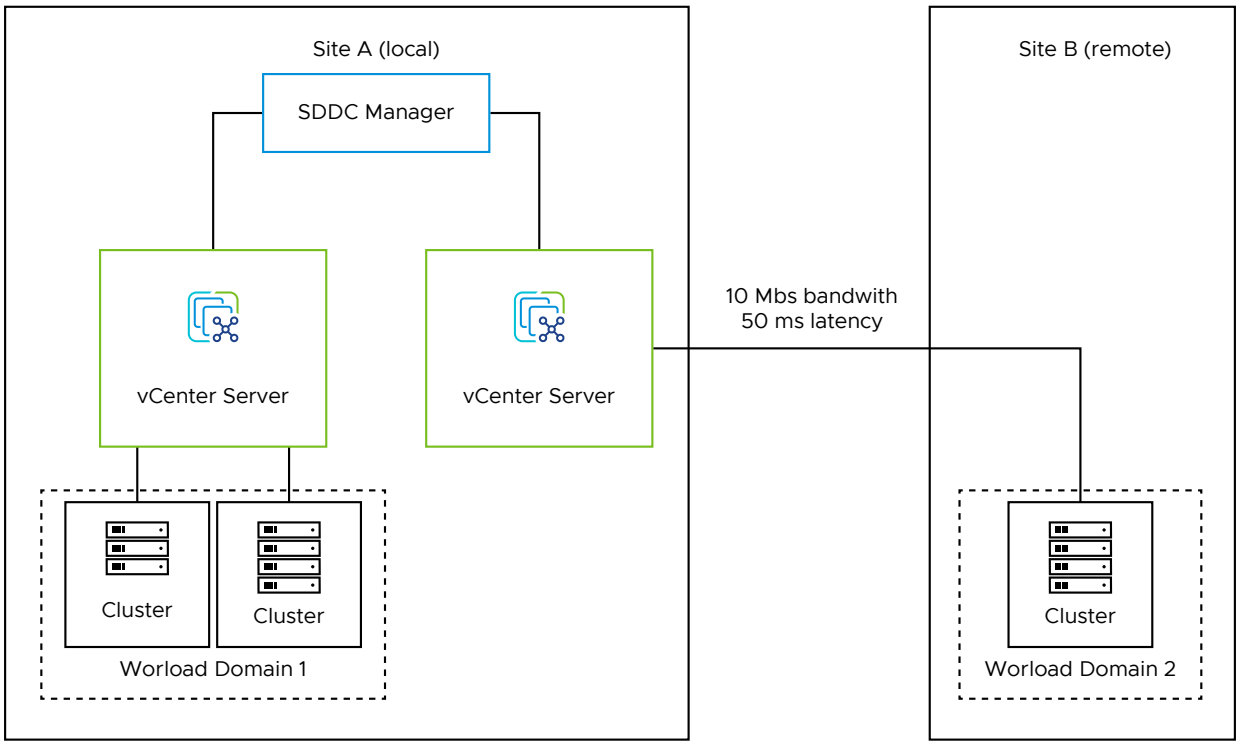
The add VxRail cluster task is triggered.

Deploying a VI Workload Domain with a Remote Cluster

With VMware 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 SDDC Manager UI.

VMware 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.
- VMware Cloud Foundation Remote Clusters supports a minimum of 3 and maximum of 4 hosts.
- Dedicated WAN connectivity is required between central site and VMware Cloud Foundation Remote Clusters site.

- Primary and secondary active WAN links are recommended for connectivity from the central site to the VMware 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 VMware 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 VMware Cloud Foundation Remote Clusters site.
- The network at the VMware 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 VMware Cloud Foundation Remote Clusters site

For information on enabling Workload Management (vSphere with Tanzu) on a cluster deployed at a remote site, see Chapter 12 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 and 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 **Default** or, if your environment requires specific Bidirectional Forwarding Detection (BFD) configuration, select **Custom**.
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 **Workload Management** to create an Edge cluster that complies with the requirements for running Workload Management. See Chapter 12 Working with Workload Management . If you select this option, you cannot modify the Edge form factor or Tier-0 service high availability settings. Select **Custom** if you want to modify those settings.
Edge Form Factor	The default setting is **Large**. ■ 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. ■ Medium: 8 GB memory, 4 vCPU, 200 GB disk space. The NSX Edge Medium appliance size is suitable for production environments with load balancing. ■ Large: 32 GB memory, 8 vCPU, 200 GB disk space. The NSX Edge Large appliance size is suitable for production environments with load balancing.. ■ 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. Workload management requires **Large**.
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 **Active-Active**. Some services are only supported in **Active-Standby**: NAT, load balancing, stateful firewall, and VPN. If you select **Active-Standby**, use exactly two Edge nodes in the Edge cluster.
Tier-0 Routing Type	Select **Static** or **EBGP** to determine the route distribution mechanism for the tier-0 gateway. If you select **Static**, you must manually configure the required static routes in NSX Manager. If you select **EBGP**, 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.
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.

Setting	Description
Edge TEP VLAN	Enter the Edge TEP VLAN ID.
Cluster	Select a vSphere cluster to host the Edge node.
Cluster Type	Select **L2 Uniform** if all hosts in the vSphere cluster have identical management, uplink, host TEP, and Edge TEP networks. Select **L2 non-uniform and L3** if any of the hosts in the vSphere cluster have different networks. **Important** VMware Cloud Foundation does not support Edge cluster creation on**L2 non-uniform and L3** vSphere clusters.
First Uplink VLAN	Enter the VLAN ID for the first uplink. This is a link from the NSX-T Edge node to the first uplink network.
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	Enter the VLAN ID for the second uplink. This is a link from the NSX-T Edge node to the second uplink network.
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.

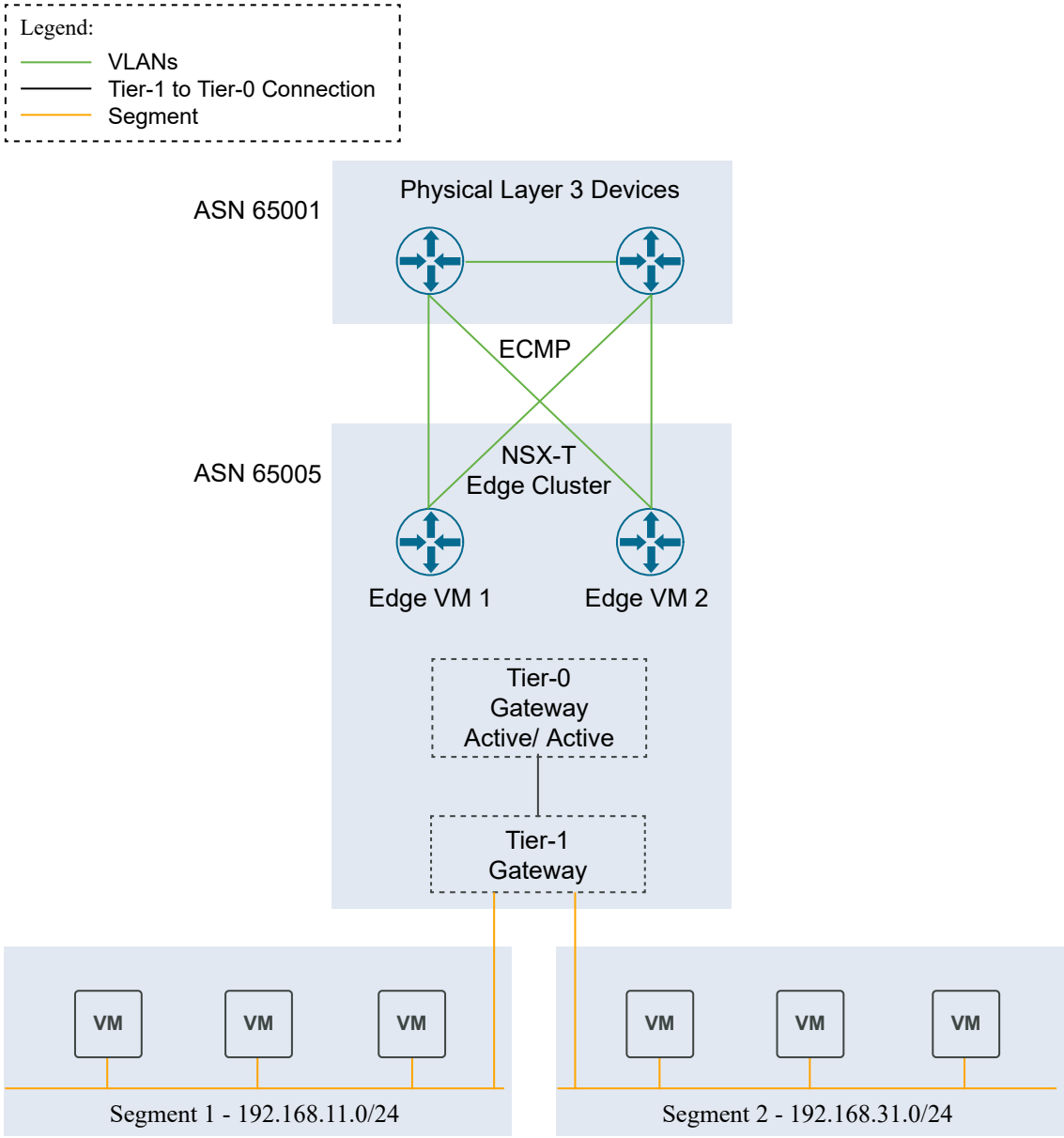
12 If validation succeeds, click **Finish** to create the NSX Edge cluster.

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 11-1. 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	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. 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.
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 Chapter 9 Certificate Management.

What to do next

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

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**.

Delete a VI Workload Domain

You can delete a VI workload domain from SDDC Manager UI.

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.

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.

Expand a Workload Domain

After you add the primary cluster, you can add more clusters to expand the workload domain.

Before adding the VxRail cluster, you need to perform the imaging of the workload domain nodes. Once you complete the imaging, perform the VxRail first run of the workload domain nodes using the vCenter Server for the workload domain.

- Create a local user in vCenter server as this is an external server deployed by VCF. This is required for the VxRail first run.
- Image the workload domain nodes. For information on imaging the nodes, refer to Dell EMC VxRail documentation.
- Do a VxRail first run of the workload domain nodes using the vCenter server for that workload domain. For information on VxRail first run, refer to the Dell EMC VxRail documentation.
- Once the validation is complete, trigger the build VxRail operation.

Add the VxRail Cluster

To add a cluster with a shared NSX-T cluster and new vDS for an overlay traffic isolation, see Add a Cluster with a Shared NSX-T Cluster and New vDS. To add the VxRail cluster to a workload domain through the UI, perform the following tasks:

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, hover your mouse in the VxRail workload domain row.

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

3 Click these three dots. Click **Add VxRail Cluster**.

4 On the **Discovered Clusters** page, the VxRail cluster in the vCenter is discovered. Click **Next**.

5 On the **Discovered Hosts** page, enter the SSH password for the discovered hosts and click **Next**.

6 On the **VxRail Manager** page, enter the Admin and Root user names and passwords.

7 On the **Thumbprint Verification** page, click  to confirm the SSH thumbprints for VxRail Manager and the ESXi hosts.

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

9 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	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. To create a new static IP Pool provide the following information: ■ Pool Name ■ Description ■ CIDR ■ IP Range. ■ Gateway IP 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. **Note** You cannot stretch a cluster that uses static IP addresses for the NSX-T Host Overlay Network.

10 Enter the license keys for NSX-T Data Center and VMware vSAN. Click **Next**.

11 Review the details and click **Next**.

12 On the **Validation** page, wait until all of the inputs have been successfully validated.

If validation is unsuccessful, you cannot proceed. Use the **Back** button to modify your settings and try again.

13 Click **Finish**.

The add VxRail cluster task is triggered.

Expand the VxRail Cluster

Once a cluster has been added to a workload domain, you can expand it further by adding hosts.

The process of expanding the VxRail cluster for a workload domain involves three steps:

1 Image the new node.

2 Discover and add new node to the cluster using the VxRail Manager plugin for vCenter Server. See the Dell EMC documentation.

3 Add the host to the VMware Cloud Foundation domain cluster. The next section provides more details about this task.

Add the VxRail Hosts to the Cluster in VMware Cloud Foundation

Once the hosts have been added to the VxRail cluster, you can add them to the cluster in VMware Cloud Foundation.

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 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 In the navigation pane, click **Inventory > Workload Domains**.

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

3 Click the **Clusters** tab.

4 Click the name of the cluster where you want to add a host.

5 Click **Actions > Add VxRail Hosts**.

6 Select the cluster expansion type.

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

Option	Description
L2 Uniform	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.
L2 non-uniform and L3	You cannot proceed if you any of the hosts you are adding to the vSphere cluster have different networks than the existing hosts in the vSphere cluster. VMware Cloud Foundation does not support adding hosts to **L2 non-uniform and L3** vSphere clusters that host an NSX-T Edge cluster.

7 On the **Discovered Hosts** page, enter the SSH password for the host and click **Add**.

8 On the **Thumbprint Verification** page, click  to confirm the SSH thumbprints for the ESXi hosts.

9 On the **Validation** page, wait until all of the inputs have been successfully validated.

If validation is unsuccessful, you cannot proceed. Use the **Back** button to modify your settings and try again.

10 Click **Finish**.

Add a Cluster with a New NSX-T Cluster and vDS

When you want to isolate overlay network traffic, you can add a cluster with a new NSX-T cluster and vDS.

Prerequisites

- Configure forward and reverse DNS settings for NSX-T and ESXi components.
- Verify that the workload domain is provisioned.
- Ensure that host configuration has a minimum of two active and unused vmnics.
- Configure a DHCP server if the Host Overlay Network TEPs will use DHCP for IP allocation.
- Download the `.zip` file from https://code.vmware.com/samples?id=7481. Copy the `.zip` file to the /home/vcf directory on the SDDC Manager VM and unzip it.

Note For a sample script, see the `README.md` file in the `/home/vcf/Multi-Dvs-Script-master/Multi-Dvs-Automator` directory.

Procedure

1 Using SSH, log in to the SDDC Manager VM with the user name `vcf` and the password you specified in the deployment parameter sheet.

2 Enter `su` to switch to the root account.

3 In the `/home/vcf/Multi-Dvs-Script-master/Multi-Dvs-Automator` directory, run the `vxrailworkloadautomator.py` script as `python3 vxrailworkloadautomator.py`.

4 Enter the SSO user name and password.

5 When prompted, select a workload domain to which you want to import the cluster.

6 Select a cluster from the list of clusters that are ready to be imported.

7 Enter passwords for the discovered hosts.

- Enter a single password for all the discovered hosts.
- Enter passwords individually for each discovered host.

8 Create a new vSphere Distributed Switch (vDS).

a Select the option to create a new vDS.

b Enter the name of the vDS.

c Enter a comma-separated list of at least two physical NICs.

9 Enter the Geneve VLAN ID.

10 Choose the option to create a new NSX-T Manager instance and provide the NSX-T Manager cluster details:

a VLAN ID for the NSX-T host overlay network

b NSX-T Manager Virtual IP (VIP) address and FQDN

c FQDNs for the NSX-T Managers (nodes)

11 Select the IP allocation method for the Host Overlay Network TEPs.

Option	Description
DHCP	With this option VMware Cloud Foundation uses DHCP for the Host Overlay Network TEPs. 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.
Static IP Pool	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. To create a new static IP Pool provide the following information: ■ Pool Name ■ Description ■ CIDR ■ IP Range. ■ Gateway IP 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. **Note** You cannot stretch a cluster that uses static IP addresses for the NSX-T Host Overlay Network TEPs.

12 Enter and confirm the VxRail Manager root password.

13 Confirm the SSH thumbprints for VxRail Manager and the ESXi hosts.

14 Select the license keys for VMware vSAN and NSX-T Data Center.

15 Press Enter to begin the validation process.

16 When validation succeeds, press Enter to import the cluster.

Add a Cluster with a Shared NSX-T Cluster and New vDS

When you want to isolate overlay network traffic, you can add a cluster with a shared NSX-T cluster and new vDS.

Prerequisites

- Configure forward and reverse DNS settings for NSX-T and ESXi components.
- Verify that the workload domain is provisioned.
- Ensure that host configuration has a minimum of two active and unused vmnics.
- Configure a DHCP server if the Host Overlay Network TEPs will use DHCP for IP allocation.
- Download the `Multi-Dvs-Script-master.zip` file from https://code.vmware.com/samples?id=7390. Copy the `Multi-Dvs-Script-master.zip` file to the /home/vcf directory on the SDDC Manager VM and unzip it.

  Note For a sample script, see the `README.md` file in the `/home/vcf/Multi-Dvs-Script-master/Multi-Dvs-Automator` directory.

Procedure

1. Using SSH, log in to the SDDC Manager VM with the user name `vcf` and the password you specified in the deployment parameter sheet.
2. To switch to the root account, run the `su` command.
3. In the `/home/vcf/Multi-Dvs-Script-master/Multi-Dvs-Automator` directory, run the `vxrailworkloadautomator.py` script as `python3 vxrailworkloadautomator.py`.
4. Enter the SSO user name and password.
5. When prompted, select a workload domain to which you want to import the cluster.
6. Select a cluster from the list of clusters that are ready to be imported.
7. Enter passwords for the discovered hosts.
   - Enter a single password for all the discovered hosts.
   - Enter passwords individually for each discovered host.
8. Create a new vSphere Distributed Switch (vDS).
   a. Select the option to create a new vDS.
   b. Enter the name of the vDS.
   c. Enter a comma-separated list of at least two physical NICs.
9. Enter the Geneve VLAN ID.

10 Provide the NSX-T Manager cluster details:

a Use an existing NSX-T instance.

b Enter VLAN ID for the NSX-T host overlay network.

c Select an existing NSX-T instance from the available list.

11 Select the IP allocation method for the Host Overlay Network TEPs.

Option	Description
DHCP	With this option VMware Cloud Foundation uses DHCP for the Host Overlay Network TEPs. 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.
Static IP Pool	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. To create a new static IP Pool provide the following information: ■ Pool Name ■ Description ■ CIDR ■ IP Range. ■ Gateway IP 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. **Note** You cannot stretch a cluster that uses static IP addresses for the NSX-T Host Overlay Network TEPs.

12 Enter and confirm the VxRail Manager root (mystic) password.

13 Confirm the SSH thumbprints for VxRail Manager and the ESXi hosts.

14 Select the license keys for VMware vSAN and NSX-T Data Center.

15 Press Enter to begin the validation process.

16 When validation succeeds, press Enter to import the cluster.

Reduce a Workload Domain

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

Remove a Host from a Cluster in a Workload Domain

You can remove a host from a cluster in a workload domain through the **Workload Domains** page in SDDC Manager UI.

When a host is removed, the vSAN members are reduced. 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

Use the vSphere Client to make sure that there are no critical alarms on the cluster from which you want to remove the host.

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(s) to remove and click **Remove Selected Hosts**.
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 and deleted from vCenter Server.

Delete a VxRail Cluster

You can delete a VxRail 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.

Prerequisites

- If vSAN remote 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 of 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 VxRail cluster or shrink the NSX Edge cluster by deleting Edge nodes hosted on the VxRail 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 VxRail 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.

Working with Workload Management

12

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 Kuberntes - 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
- 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

13

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 14 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	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. **Note** 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`.
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.

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

14

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.

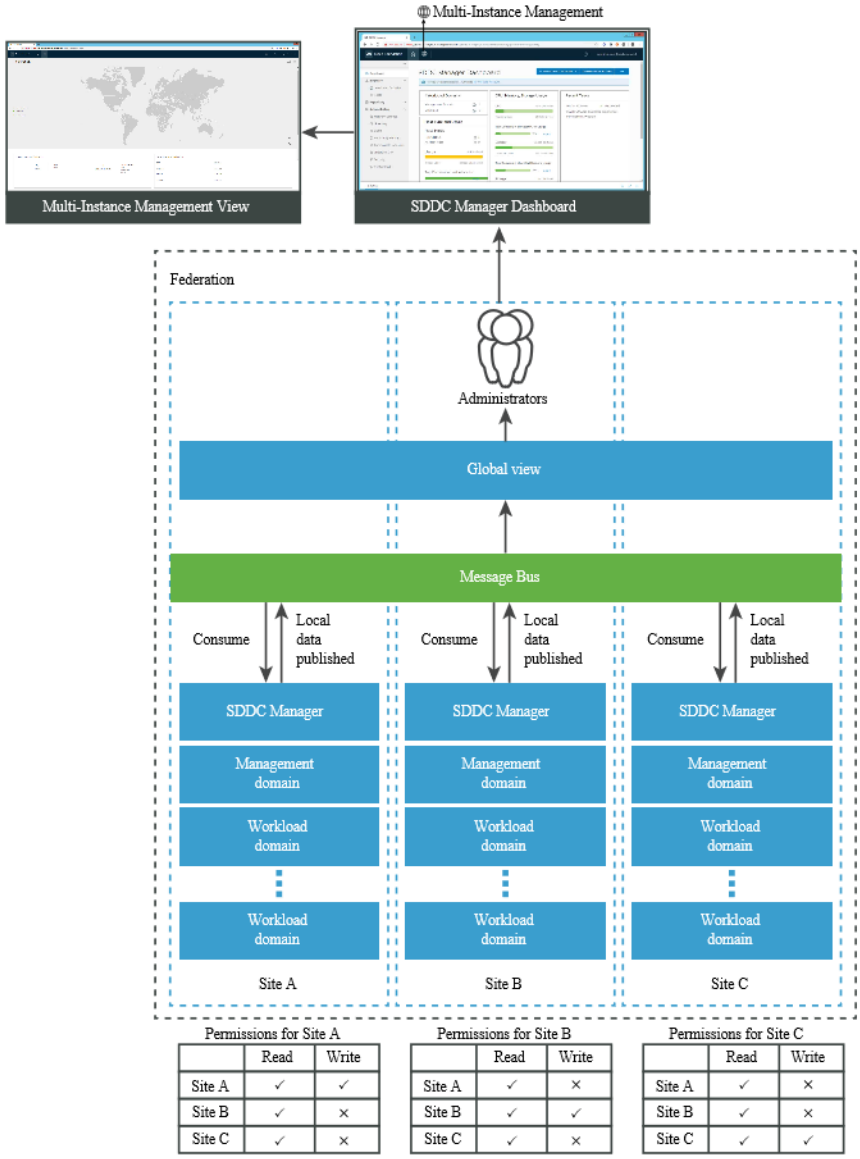
Multi-Instance Management

15

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.



Permissions for Site A

	Read	Write
Site A	✓	✓
Site B	✓	×
Site C	✓	×

Permissions for Site B

	Read	Write
Site A	✓	×
Site B	✓	✓
Site C	✓	×

Permissions for Site C

	Read	Write
Site A	✓	×
Site B	✓	×
Site C	✓	✓

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.

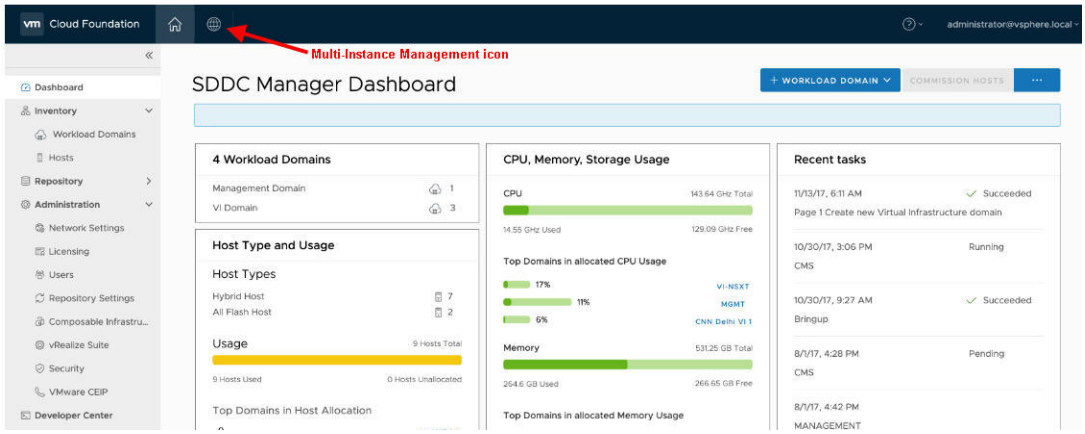
The instance who created the federation is automatically granted the controller role. If you only have two instances in the federation, there is no need to create both as controllers. Multi-Instance management works with two VMware Cloud Foundation sites; however, if one fails then the multi-instance capability is not available on the other site.

This chapter includes the following topics:

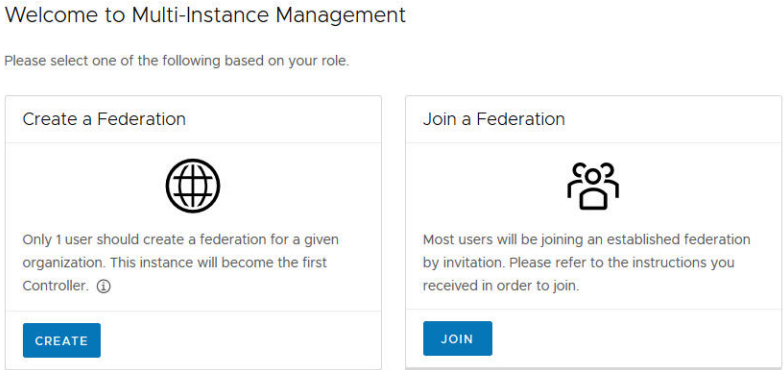
About the Multi-Instance Management Dashboard

The Multi-Instance Management Dashboard displays the inventory and capacity across the federation.

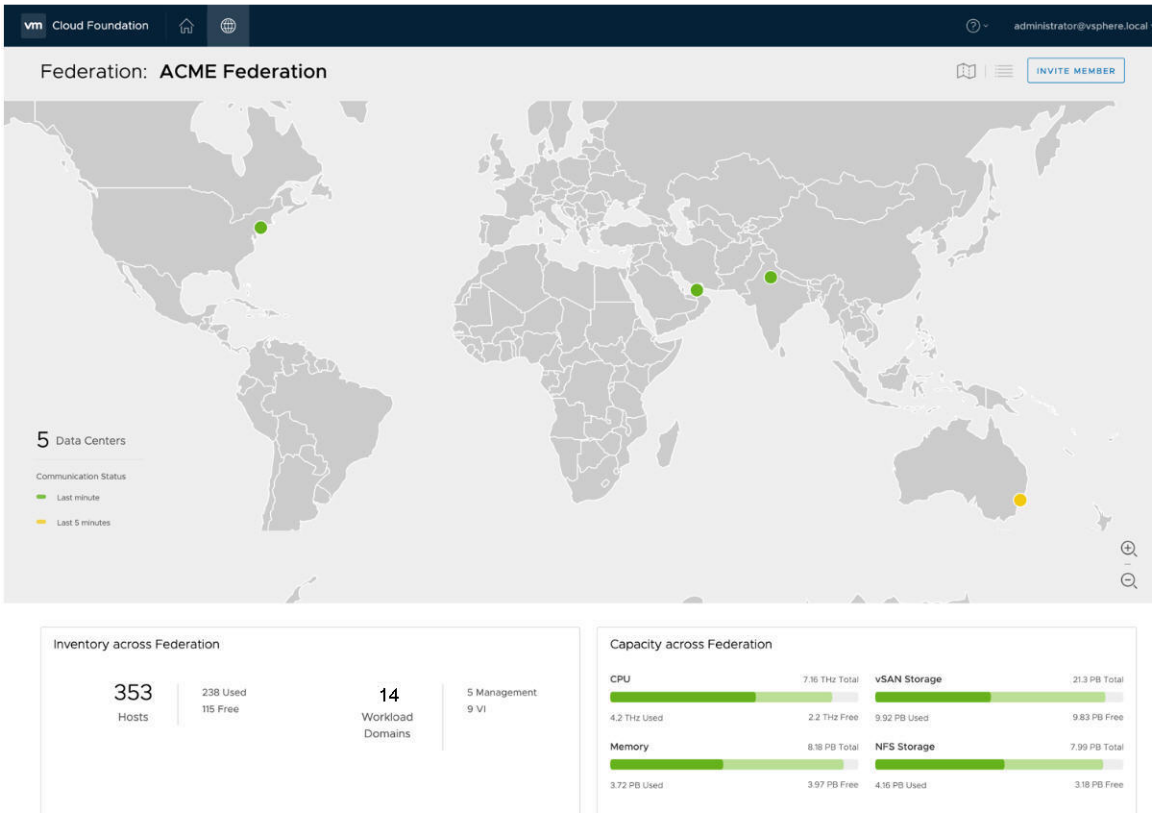
You access the Multi-Instance Management Dashboard by clicking the Multi-Instance View icon in the top left corner of the SDDC Manager Dashboard.



Before a federation is created, the dashboard displays a create and join option.



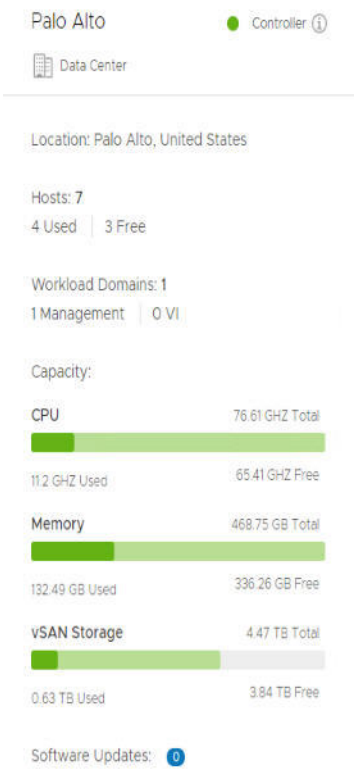
After a federation is created, the Multi-Instance Management Dashboard displays a world map showing the federation members as dots on the map.



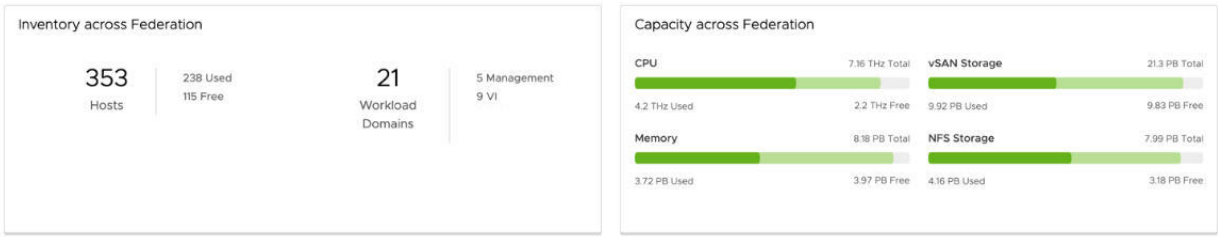
The dot color depends on the communication status between the federation members - green if they communicated within the last two minutes, yellow if they communicated within the previous five minutes, and red if they have not communicated for more than ten minutes. You can see the following information here:

- Hover over a dot to see the member name and location.

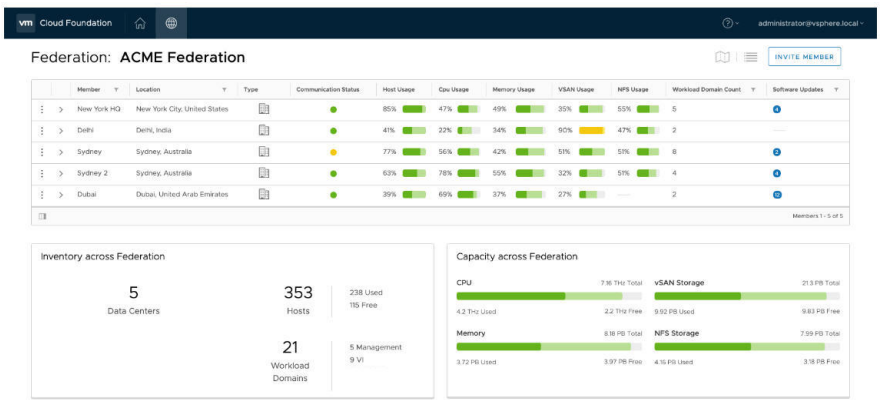
- Click the member location dot to open a panel on the right side with detailed information about the VMware Cloud Foundation instance. The panel also displays available software updates.



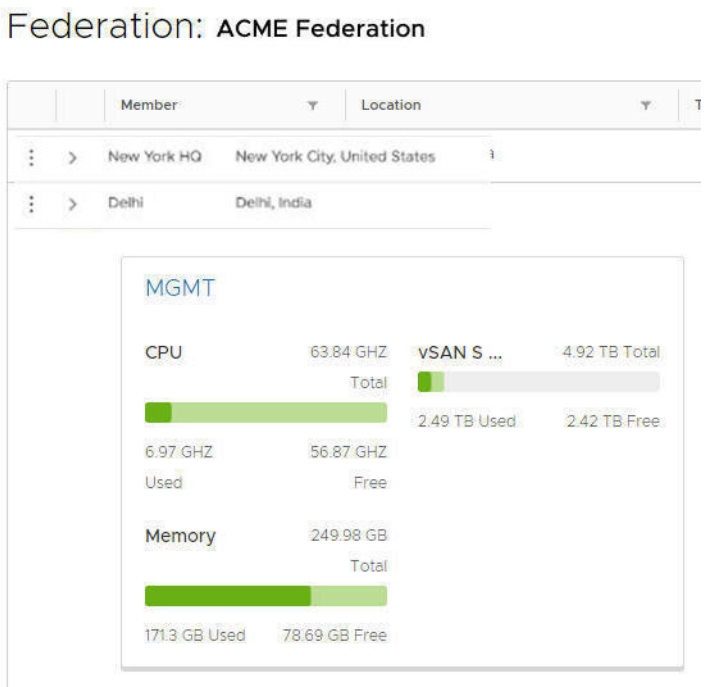
The Inventory section in the bottom half of the dashboard displays the number of hosts and workload domains along with a breakdown of the workload domain type. The capacity section displays the used and available CPU, memory, and storage across the federation.



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.



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

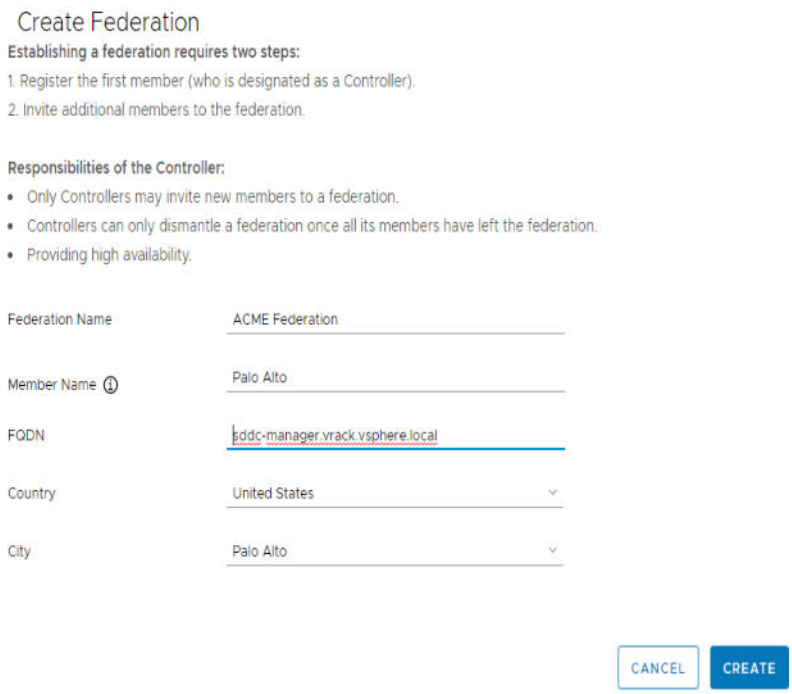
Prerequisites

- 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**.



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

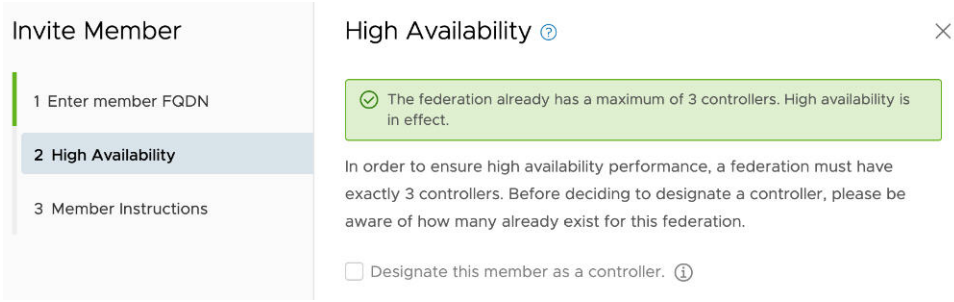
You must be a controller in the federation and have the FQDN of the member you are inviting.

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.



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.

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 SSDC 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.

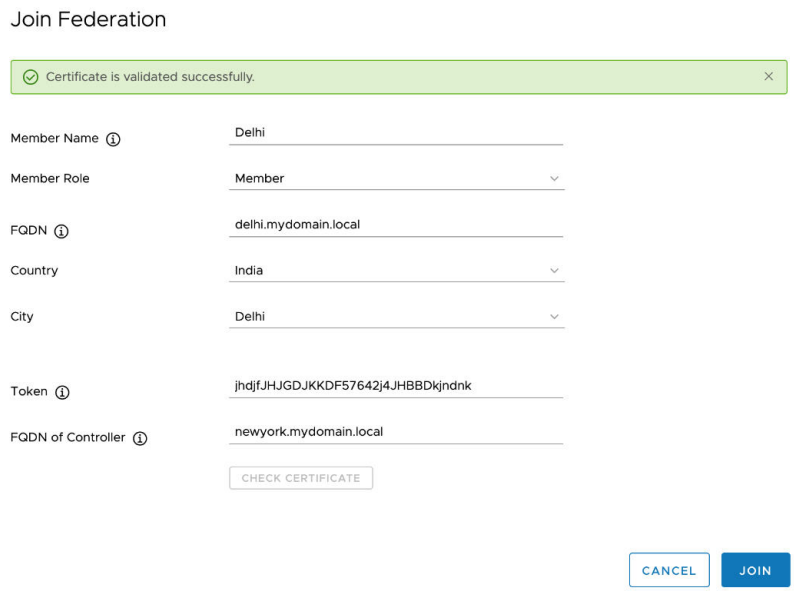
Prerequisites

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.



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 SSDC 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.

Stretching Clusters

16

You can stretch an NSX-T cluster in the management domain or in a VI workload domain 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 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 second availability zone goes down.

Note You cannot stretch a cluster in the following conditions:

- If a cluster uses static IP addresses for the NSX-T Host Overlay Network TEPs
- If remote vSAN datastores are mounted on any cluster

You may want to stretch a cluster for the following reasons.

- 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 release of Cloud Foundation does not support unstretching a cluster.

About Availability Zones and Regions

This section describes availability zones and regions 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.

VxRail 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-T Edge appliances between availability zones. The Layer 3 gateway for the management and Edge Overlay networks must be highly available across the availability zones.

Note The management network VLAN can be the same for the management domain and VI workload domains, although the table below shows an example where these VLANs are different (1611 vs 1631).

Table 16-1. 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 and AZ2)	✓	✓	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	✓	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

Table 16-1. Management 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	✓	✓	2713 (Stretched)	172.27.13.0/24	✓	9000
vSphere vMotion	X	✓	1622	172.16.22.0/24	✓	9000
vSAN	X	✓	1623	172.16.23.0/24	✓	9000
Host Overlay	X	✓	1624	172.16.24.0/24	✓	9000

Note If a VLAN is stretched between AZ1 and AZ2, then the data center needs to provide appropriate routing and failover of the gateway for that network.

Table 16-2. Workload Domain VLAN and IP Subnet Requirements

Function	Availability Zone 1	Availability Zone 2	VLAN ID	IP Range	HA Layer 3 Gateway
Management (AZ1 and AZ2)	✓	✓	1631	172.16.31.0/24	✓
vSphere vMotion	✓	X	1632	172.16.32.0/24	✓
vSAN	✓	X	1633	172.16.33.0/24	✓
Host Overlay	✓	X	1634	172.16.34.0/24	✓
vSphere vMotion	X	✓	2732	172.27.32.0/24	✓
vSAN	X	✓	2733	172.16.33.0/24	✓
Host Overlay	X	✓	1621	172.16.21.0/24	✓

Networking for Multiple Availability Zones

There are specific physical data center network requirements for a topology with multiple availability zones.

Table 16-3. Physical Network Requirements for Multiple Availability Zone

Component	Requirement
MTU	■ VLANs which are stretched between availability zones must meet the same requirements as the VLANs for intra-zone connection including MTU. ■ MTU value must be consistent end-to-end including components on the inter zone networking path. ■ 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.
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	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. **Note** You cannot stretch a cluster that uses static IP addresses for the NSX-T Host Overlay Network TEPs.
BGP routing	Each availability zone data center must have its own Autonomous System Number (ASN).
Ingress and egress traffic	■ For VLANs that are stretched between availability zones, traffic flows in and out of a single zone. Local egress is not supported. ■ For VLANs that are not stretched between availability zones, traffic flows in and out of the zone where the VLAN is located. ■ 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.
Latency	■ Maximum network latency between NSX-T Managers is 10 ms. ■ Maximum network latency between the NSX-T Manager cluster and transport nodes is 150 ms.

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 VxRail Cluster

This procedure describes how to stretch a VxRail cluster across two availability zones.

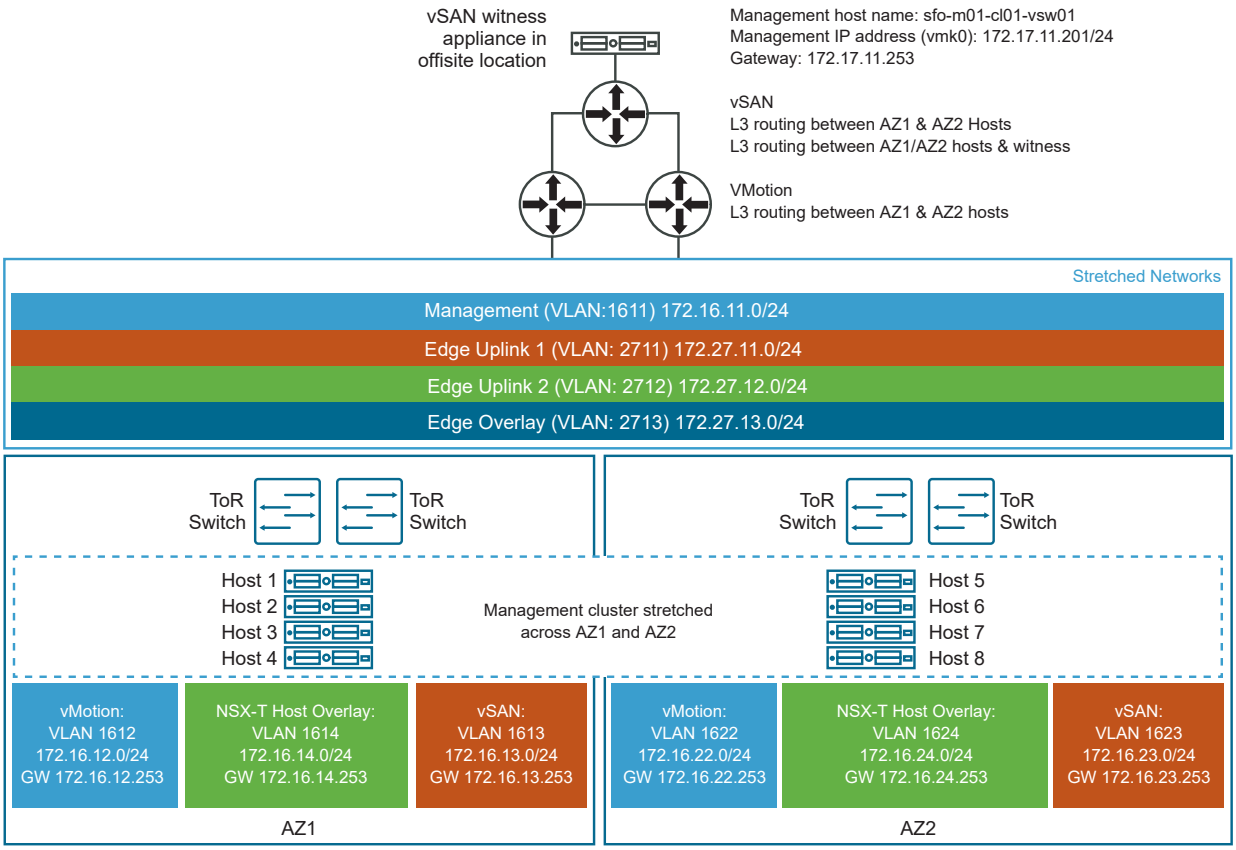
This example use case has two availability zones in two buildings in an office campus - AZ1 and AZ2. Each availability zone has its own power supply and network. The management domain is on AZ1 and contains the default cluster, SDDC-Cluster1. This cluster contains four ESXi hosts.

vSAN network	VLAN ID=1623
	MTU=9000
	Network=172.16.234.0
	netmask 255.255.255.0
	gateway 172.16.23.253
	IP range=172.16.23.11 - 172.16.234.59
vMotion network	VLAN ID=1622
	MTU=9000
	Network=172.16.22.0
	netmask 255.255.255.0
	gateway 172.16.22.253
	IP range=172.16.22.11 - 172.16.22.59

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 16-1. Stretch Cluster Example



To stretch a cluster for VMware Cloud Foundation on Dell EMC VxRail, perform the following steps:

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.
- Download initiate_stretch_cluster_vxpail.py.

Note You cannot stretch a cluster in the following conditions:

- If a cluster uses static IP addresses for the NSX-T Host Overlay Network TEPs
- If remote vSAN datastores are mounted on any cluster

Procedure

1. Using an SSH File Transfer tool, copy `initiate_stretch_cluster_vxrail.py` to the `/home/vcf/` directory on the SDDC Manager appliance.
2. Using SSH, log in to the SDDC Manager appliance with the user name `vcf` and the password you specified in the deployment parameter workbook.
3. Run the script with `-h` option for details about the script options.

```
python initiate_stretch_cluster_vxrail.py -h
```

4 Run the following command to prepare the cluster to be stretched. The command creates affinity rules for the VMs to run on the preferred site:

```
python initiate_stretch_cluster_vxrail.py --workflow prepare-stretch --sc-domain <SDDC-valid-domain-name> --sc-cluster <valid-cluster-name>
```

Replace *<SDDC-valid-domain-name>* and *<valid-cluster-name>* with the correct values for your environment. For example:

```
python initiate_stretch_cluster_vxrail.py --workflow prepare-stretch --sc-domain wdc1-workflowspec-vxrail --sc-cluster VxRail-Virtual-SAN-Cluster-8d2c9f37-e230-4238-ab35-cafd5033a59e
```

Enter the SSO user name and password when prompted to do so.

Once the workflow is triggered, track the task status in the SDDC Manager UI. If the task fails, debug and fix the issue and retry the task from the SDDC Manager UI. Do not run the script again.

5 Use the VxRail vCenter plug-in to add the additional hosts in Availability Zone 2 to the cluster by performing the VxRail Manager cluster expansion work flow.

6 Run the following command to stretch the cluster:

```
python initiate_stretch_cluster_vxrail.py --workflow stretch-vsan --sc-domain <SDDC-valid-domain-name> --sc-cluster <valid cluster name which is a part of the domain to be stretched> --sc-hosts <valid host names> --witness-host-fqdn <witness host/appliance IP or fqdn> --witness-vsan-ip <witness vsan IP address> --witness-vsan-cidr <witness-vsan-network-IP-address-with-mask>
```

Replace *<SDDC-valid-domain-name>*, *<valid cluster name which is a part of the domain to be stretched>*, *<valid host names>*, *<witness vsan IP address>*, *<witness host/appliance IP or fqdn>*, *<witness vsan IP address>*, and *<witness-vsan-network-IP-address-with-mask>* with the correct values for your environment. For example:

```
python initiate_stretch_cluster_vxrail.py --workflow stretch-vsan --sc-domain wdc1-workflowspec-vxrail --sc-cluster VxRail-Virtual-SAN-Cluster-8d2c9f37-e230-4238-ab35-cafd5033a59e --sc-hosts wdc3-005-proxy.vxrail.local --witness-host-fqdn 172.16.10.235 --witness-vsan-ip 172.16.20.235 --witness-vsan-cidr 172.16.20.0/24
```

7 When prompted, enter the following information:

- SSO user name and password
- Root user password for ESXi hosts
- vSAN gateway IP for the preferred (primary) and non-preferred (secondary) site
- vSAN CIDR for the preferred (primary) and non-preferred (secondary) site
- VLAN ID for the non-preferred site overlay VLAN
- Confirm the SSH thumbprints for the hosts

Once the workflow is triggered, the task is tracked in the SDDC Manager UI. If the task fails, debug and fix the issue and retry from SDDC Manager UI. Do not run the script again.

8 Monitor the progress of the AZ2 hosts being added to the cluster.

a In the SDDC Manager UI, click **View All Tasks**.

b Refresh the window to monitor the status.

9 Validate that stretched cluster operations are working correctly by logging in to the vSphere Web Client.

a Verify vSAN Health.

1 On the home page, click **Host and Clusters** and then select the stretched cluster.

2 Click **Monitor > vSAN > Skyline Health**.

3 Click **Retest**.

4 Fix errors, if any.

b Verify the vSAN Storage Policy.

1 On the home page, click **Policies and Profiles > VM Storage Policies > vSAN Default Storage Policies**.

2 Select the policy associated with the vCenter Server for the stretched cluster and click **Check Compliance**.

3 Click **VM Compliance** and check the **Compliance Status** column for each VM.

4 Fix errors, if any.

Configure Witness Traffic Separation for VMware Cloud Foundation on Dell EMC VxRail

Witness traffic separation allows you to use a VMkernel adapter for vSAN witness traffic that is different from the adapter for vSAN data traffic.

By default, when you stretch a cluster, the vSAN-tagged VMkernel adapter is used to carry traffic destined for the vSAN witness host. With witness traffic separation, you can use a separately tagged VMkernel adapter instead of extending the vSAN data network to the witness host. This feature allows for a more flexible network configuration by allowing for separate networks for node-to-node and node-to-witness communication.

Prerequisites

You must have a stretched cluster before you can configure it for witness traffic separation.

Procedure

1 Create Distributed Port Groups for Witness Traffic

Create a distributed port group for each availability zone on the vSphere Distributed Switch.

2 Delete Routes to the Witness Host

When you stretch a cluster, a route to the witness host is added to each ESXi host in the stretched cluster. You must delete these routes to use witness traffic separation.

3 Add VMkernel Adapters for Witness Traffic

Add VMkernel adapters for witness traffic to each availability zone's distributed port group.

4 Configure the VMkernel Adapters for Witness Traffic

Enable witness traffic for the witness traffic VMkernel adapter on each ESXi host

Create Distributed Port Groups for Witness Traffic

Create a distributed port group for each availability zone on the vSphere Distributed Switch.

Procedure

1 Log in to the vSphere Client.

2 Click **Menu > Networking**.

3 Right-click the vSphere distributed switch for the cluster and select **Distributed Port Group > New Distributed Port Group**.

4 Enter a name for the port group for the first availability zone and click **Next**.

For example, **`AZ1_WTS_PG`**.

5 Change the VLAN type to **VLAN** and enter a VLAN ID.

6 Select **Customize default policies** and click **Next**.

7 On the **Security** page, click **Next**.

8 On the **Traffic shaping** page, click **Next**.

9 On the **Teaming and failover** page, modify the failover order of the uplinks to match the existing failover order of the management traffic and click **Next**.

10 On the **Monitoring** page, click **Next**.

11 On the **Miscellaneous** page, click **Next**.

12 On the **Ready to Complete** page, review your selections and click **Finish**.

13 Repeat these steps for the second availability zone.

Delete Routes to the Witness Host

When you stretch a cluster, a route to the witness host is added to each ESXi host in the stretched cluster. You must delete these routes to use witness traffic separation.

Procedure

1 Open an SSH connection to the first ESXi host in the stretched cluster.

2 Log in as **`root`**.

3 Run the following command:

```
esxcli network ip route ipv4 list
```

The output returns something like:

```
Network      Netmask         Gateway       Interface  Source
-----------  -------------   ------------  ---------  ------
default      0.0.0.0         172.18.15.1   vmk2       MANUAL
169.254.0.0  255.255.255.0   0.0.0.0       vmk1       MANUAL
172.18.7.0   255.255.255.0   0.0.0.0       vmk3       MANUAL
172.18.13.0  255.255.255.0   0.0.0.0       vmk5       MANUAL
172.18.14.0  255.255.255.0   172.18.7.253  vmk3       MANUAL
172.18.15.0  255.255.255.0   0.0.0.0       vmk2       MANUAL
172.18.21.0  255.255.255.0   172.18.7.253  vmk3       MANUAL
```

4 Delete the route to the witness host. For example:

```
esxcfg-route -d 172.18.14.0/24 172.18.7.253
```

5 Repeat these steps for each ESXi host in the stretched cluster.

Add VMkernel Adapters for Witness Traffic

Add VMkernel adapters for witness traffic to each availability zone's distributed port group.

Procedure

1 Log in to the vSphere Client.

2 Click **Menu > Networking**.

3 Right-click the witness distributed port group for the first availability zone, for example, **`AZ1_WTS_PG`**, and select **Add VMkernel Adapters**.

4 Click **+ Attached Hosts**, select the availability zone 1 hosts from the list, and click OK.

5 Click **Next**.

6 Accept the default VMkernel port settings and click **Next**.

Note Do not select any services.

7 Select **Use static IPv4 settings** and enter the IP addresses and the subnet mask to use for the witness traffic separation network.

8 Click **Next**.

9 Review your selections and click **Finish**.

10 Repeat these steps for the witness distributed port group for the second availability zone.

Configure the VMkernel Adapters for Witness Traffic

Enable witness traffic for the witness traffic VMkernel adapter on each ESXi host

Procedure

1 Log in to the vSphere Client.

2 Click **Menu > Hosts and Clusters**.

3 For each host in the stretched cluster, click **Configure > Networking > VMkernel adapters** to determine which VMkernel adapter to use for witness traffic. For example, **vmk5**.

4 SSH to the first ESXi host in the stretched cluster.

5 Log in as root and run the following command:

```
esxcli vsan network ip add -i <vmkernel_adapter> -T=witness
```

For example:

```
esxcli vsan network ip add -i vmk5 -T=witness
```

6 Verify that the VMkernel adapter is configured for witness traffic:

```
esxcli vsan network list
```

7 Verify that the ESXi host can access the witness host:

```
vmkping -I <vmkernel_adapter> <witness_host_ip_address>
```

Replace *<vmkernel_adapter>* with the VMkernel adapter configured for witness traffic, for example **vmk5**. Replace *<witness_host_ip_address>* with the witness host IP address.

8 Repeat for each ESXi host in the stretched cluster.

Expand a Stretched VxRail Cluster

You can expand a stretched cluster by adding more VxRail nodes to the preferred and non-preferred sites.

Prerequisites

You must have a stretched cluster.

Procedure

1 Use the VxRail vCenter plug-in to add the additional hosts in availability zone 1 or availability zone 2 to the cluster by performing the VxRail Manager cluster expansion work flow.

Refer to the Dell EMC VxRail documentation for more details.

2 Log in to SDDC Manager and run the script to trigger the workflow to import the newly added hosts in the SDDC Manager inventory.

In the script, provide the root credentials for each host and specify which fault domain the host should be added to.

3 Using SSH, log in to the SDDC Manager VM with the username **vcf** and the password you specified in the deployment parameter workbook.

4 Run the following command to expand the stretched cluster:

```
python initiate_stretch_cluster_vxrail.py --workflow expand-stretch-cluster --sc-domain
<SDDC-valid-domain-name> --sc-cluster <valid cluster name which is a part of the domain
to be stretched> --sc-hosts <valid host names> --witness-host-fqdn <witness host/appliance
IP or fqdn> --witness-vsan-ip <witness vsan IP address> --witness-vsan-cidr <witness-vsan-
network-IP-address-with-mask>
```

Replace *<SDDC-valid-domain-name>*, *<valid cluster name which is a part of the domain to be stretched>*, *<valid host names>*, *<witness vsan IP address>*, *<witness host/appliance IP or fqdn>*, *<witness vsan IP address>*, and *<witness-vsan-network-IP-address-with-mask>* with the correct values for your environment.

5 When prompted, enter the following information:

- SSO user name and password
- Root user password for ESXi hosts
- Fault domain for ESXi hosts
- vSAN gateway IP for the preferred (primary) and non-preferred (secondary) site
- vSAN CIDR for the preferred (primary) and non-preferred (secondary) site
- Confirm the SSH thumbprints for the hosts

6 Once the workflow is triggered, track the task status in the SDDC Manager UI.

If the task fails, debug and fix the issue and retry from SDDC Manager UI. Do not run the script again.

What to do next

If you add hosts to a stretched cluster configured for witness traffic separation, perform the following tasks for the added hosts:

- Add VMkernel Adapters for Witness Traffic
- Delete Routes to the Witness Host
- Configure the VMkernel Adapters for Witness Traffic

Replace a Failed Host in a Stretched VxRail 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

- Check the health of the cluster.

See "Check vSAN Health" in *Administering VMware vSAN*.

Procedure

1 Remove the failed host from the cluster.

See Remove a Host from a Cluster in a Workload Domain.

2 Expand the cluster to add the new host to the cluster.

See Expand a Stretched VxRail Cluster .

Results

vSAN automatically rebuilds the stretch cluster.

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

From SDDC Manager UI, 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 SDDC Manager UI, 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

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

Note To update the DNS settings for VxRail Manager, see the Dell EMC documentation.

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 and access token and a refresh token.

```
{"accessToken":"eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiI2ZGRmZmU3MC0zZGEwLTQ5NmUtOTQzMC1hOGNkNTQ0YT
k2ZGMiLCJpYXQiOjE1ODU3ODE3ODcsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZ
i1hdXRoIiwiYXVkIjoic2RkYy1zZXJ2aWNlcyIsIm5iZiI6MTU4NTc4MTc4NywiZXhwIjoxNTg1Nzg1Mzg3LCJ1c2Vy
IjoiYWRtaW5pc3RyYXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCI
sInNjb3BlIjpbIkJBQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl
9XUklURSIsIkJBQ0tVUF9DT05GSUdfV1JJVEUiLCJPVEhFUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XU
klURSJdfQ.WCpUPRIm5A6X_406HTJF7TbTSa0g91_AQbt7OcBPblM","refreshToken":
{"id":"47c07f35-0a89-4df5-a3a3-f31265ebbb7a"}}
```

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.eyJqdGkiOiI2ZGRmZmU3MC0zZGEwLTQ5NmUtOTQzMC1hOGNkNTQ0YTk2ZGMiLCJpYXQiOj
E1ODU3ODE3ODcsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZi1hdXRoIiwiYXVkI
```

```
joic2RkYy1zZXJ2aWNlcyIsIm5iZiI6MTU4NTc4MTc4NywiZXhwIjoxNTg1Nzg1Mzg3LCJ1c2VyIjoiYWRtaW5pc3Ry
YXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsInNjb3BlIjpbIkJ
BQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl9XUklURSIsIkJBQ0
tVUF9DT05GSUdfV1JJVEUiLCJPVEhFUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XUklURSJdfQ.WCpUPR
Im5A6X_406HTJF7TbTSa0g91_AQbt7OcBPblM"
```

3 Validate the new DNS server configuration information.

```
curl -H "Authorization: Bearer
eyJhbGciOiJIUC00NGQwLTQ5MzYtYjQwMC0xMzc5NzMyMjdmOWUiLCJpYXQiOjE1ODU3ODQ5MTgsInN1YiI6ImFkbWl
uaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZi1hdXRoIiwiYXVkIjoic2RkYy1zZXJ2aWNlcyIsIm5iZi
I6MTU4NTc4NDkxOCwiZXhwIjoxNTg1Nzg4NTE4LCJ1c2VyIjoiYWRtaW5pc3RyYXRvckB2c3BoZXJlLmxvY2FsIiwib
mFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsInNjb3BlIjpbIkJBQ0tVUF9DT05GSUdfUkVBRCIsIkNS
RURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl9XUklURSIsIkJBQ0tVUF9DT05GSUdfV1JJVEUiLCJPVEh
FUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XUklURSJdfQ.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}]}'|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.

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.eyJqdGkiOiIxN2M5YThmOC00NGQwLTQ5MzYtYjQwMC0xMzc5NzMyMjdmOWUiLCJpYXQiOj
E1ODU3ODQ5MTgsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZi1hdXRoIiwiYXVkI
joic2RkYy1zZXJ2aWNlcyIsIm5iZiI6MTU4NTc4NDkxOCwiZXhwIjoxNTg1Nzg4NTE4LCJ1c2VyIjoiYWRtaW5pc3Ry
YXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsInNjb3BlIjpbIkJ
BQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl9XUklURSIsIkJBQ0
tVUF9DT05GSUdfV1JJVEUiLCJPVEhFUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XUklURSJdfQ.Ya4XsZ
ntsRHUZFRBNKGY7Js6xrGYGe8KdgJ2QbihFmg" -H 'Content-Type: application/json' -k -X GET
https://SDDC_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.eyJqdGkiOiIxN2M5YThmOC00NGQwLTQ5MzYtYjQwMC0xMzc5NzMyMjdmOWUiLCJpYXQiOj
E1ODU3ODQ5MTgsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZi1hdXRoIiwiYXVkI
joic2RkYy1zZXJ2aWNlcyIsIm5iZiI6MTU4NTc4NDkxOCwiZXhwIjoxNTg1Nzg4NTE4LCJ1c2VyIjoiYWRtaW5pc3Ry
YXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsInNjb3BlIjpbIkJ
BQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl9XUklURSIsIkJBQ0
```

```
tVUF9DT05GSUdfV1JJVEUiLCJPVEhFUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XUklURSJdfQ.Ya4XsZ
ntsRHUZFRBNKGY7Js6xrGYGe8KdgJ2QbihFmg" -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.

```
curl -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiIxN2M5YThmOC00NGQwLTQ5MzYtYjQwMC0xMzc5NzMyMjdmOWUiLCJpYXQiOj
E1ODU3ODQ5MTgsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZi1hdXRoIiwiYXVkI
joic2RkYy1zZXJ2aWNlcyIsIm5iZiI6MTU4NTc4NDkxOCwiZXhwIjoxNTg1Nzg4NTE4LCJ1c2VyIjoiYWRtaW5pc3Ry
YXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsInNjb3BlIjpbIkJ
BQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl9XUklURSIsIkJBQ0
tVUF9DT05GSUdfV1JJVEUiLCJPVEhFUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XUklURSJdfQ.Ya4XsZ
ntsRHUZFRBNKGY7Js6xrGYGe8KdgJ2QbihFmg" -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 DNS configuration was updated.

```
curl 'https://SDDC_MANAGER_IP/v1/system/dns-configuration' -k -X GET -H "Content-Type:
application/json" -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiI2ZGRmZmU3MC0zZGEwLTQ5NmUtOTQzMC1hOGNkNTQ0YTk2ZGMiLCJpYXQiOj
E1ODU3ODE3ODcsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZi1hdXRoIiwiYXVkI
joic2RkYy1zZXJ2aWNlcyIsIm5iZiI6MTU4NTc4MTc4NywiZXhwIjoxNTg1Nzg1Mzg3LCJ1c2VyIjoiYWRtaW5pc3Ry
YXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsInNjb3BlIjpbIkJ
BQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl9XUklURSIsIkJBQ0
tVUF9DT05GSUdfV1JJVEUiLCJPVEhFUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XUklURSJdfQ.WCpUPR
Im5A6X_406HTJF7TbTSa0g91_AQbt7OcBPblM"
```

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

Note To update the NTP settings for VxRail Manager, see the Dell EMC documentation.

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 and access token and a refresh token.

```
{"accessToken":"eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiI2ZGRmZmU3MC0zZGEwLTQ5NmUtOTQzMC1hOGNkNTQ0YT
k2ZGMiLCJpYXQiOjE1ODU3ODE3ODcsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZ
i1hdXRoIiwiYXVkIjoic2RkYy1zZXJ2aWNlcyIsIm5iZiI6MTU4NTc4MTc4NywiZXhwIjoxNTg1Nzg1Mzg3LCJ1c2Vy
IjoiYWRtaW5pc3RyYXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCI
sInNjb3BlIjpbIkJBQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl
9XUklURSIsIkJBQ0tVUF9DT05GSUdfV1JJVEUiLCJPVEhFUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XU
klURSJdfQ.WCpUPRIm5A6X_406HTJF7TbTSa0g91_AQbt7OcBPblM","refreshToken":
{"id":"47c07f35-0a89-4df5-a3a3-f31265ebbb7a"}}
```

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.eyJqdGkiOiI2ZGRmZmU3MC0zZGEwLTQ5NmUtOTQzMC1hOGNkNTQ0YTk2ZGMiLCJpYXQiOj
```

```
E1ODU3ODE3ODcsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZi1hdXRoIiwiYXVkI
joic2RkYy1zZXJ2aWNlcyIsIm5iZiI6MTU4NTc4MTc4NywiZXhwIjoxNTg1Nzg1Mzg3LCJ1c2VyIjoiYWRtaW5pc3Ry
YXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsInNjb3BlIjpbIkJ
BQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl9XUklURSIsIkJBQ0
tVUF9DT05GSUdfV1JJVEUiLCJPVEhFUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XUklURSJdfQ.WCpUPR
Im5A6X_406HTJF7TbTSa0g91_AQbt7OcBPblM"
```

3 Validate the new NTP server configuration information.

```
curl -H "Authorization: Bearer
eyJhbGciOiJIUC00NGQwLTQ5MzYtYjQwMC0xMzc5NzMyMjdmOWUiLCJpYXQiOjE1ODU3ODQ5MTgsInN1YiI6ImFkbWl
uaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZi1hdXRoIiwiYXVkIjoic2RkYy1zZXJ2aWNlcyIsIm5iZi
I6MTU4NTc4NDkxOCwiZXhwIjoxNTg1Nzg4NTE4LCJ1c2VyIjoiYWRtaW5pc3RyYXRvckB2c3BoZXJlLmxvY2FsIiwib
mFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsInNjb3BlIjpbIkJBQ0tVUF9DT05GSUdfUkVBRCIsIkNS
RURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl9XUklURSIsIkJBQ0tVUF9DT05GSUdfV1JJVEUiLCJPVEh
FUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XUklURSJdfQ.Ya4XsZntsRHUZFRBNKGY7Js6xrGYGe8KdgJ
2QbihFmg" -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.eyJqdGkiOiIxN2M5YThmOC00NGQwLTQ5MzYtYjQwMC0xMzc5NzMyMjdmOWUiLCJpYXQiOj
E1ODU3ODQ5MTgsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZi1hdXRoIiwiYXVkI
joic2RkYy1zZXJ2aWNlcyIsIm5iZiI6MTU4NTc4NDkxOCwiZXhwIjoxNTg1Nzg4NTE4LCJ1c2VyIjoiYWRtaW5pc3Ry
YXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsInNjb3BlIjpbIkJ
BQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl9XUklURSIsIkJBQ0
tVUF9DT05GSUdfV1JJVEUiLCJPVEhFUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XUklURSJdfQ.Ya4XsZ
ntsRHUZFRBNKGY7Js6xrGYGe8KdgJ2QbihFmg" -H 'Content-Type: application/json' -k -X GET
https://SDDC_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.eyJqdGkiOiIxN2M5YThmOC00NGQwLTQ5MzYtYjQwMC0xMzc5NzMyMjdmOWUiLCJpYXQiOj
E1ODU3ODQ5MTgsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZi1hdXRoIiwiYXVkI
joic2RkYy1zZXJ2aWNlcyIsIm5iZiI6MTU4NTc4NDkxOCwiZXhwIjoxNTg1Nzg4NTE4LCJ1c2VyIjoiYWRtaW5pc3Ry
YXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsInNjb3BlIjpbIkJ
BQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl9XUklURSIsIkJBQ0
```

```
tVUF9DT05GSUdfV1JJVEUiLCJPVEhFUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XUklURSJdfQ.Ya4XsZ
ntsRHUZFRBNKGY7Js6xrGYGe8KdgJ2QbihFmg" -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.eyJqdGkiOiIxN2M5YThmOC00NGQwLTQ5MzYtYjQwMC0xMzc5NzMyMjdmOWUiLCJpYXQiOj
E1ODU3ODQ5MTgsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZi1hdXRoIiwiYXVkI
joic2RkYy1zZXJ2aWNlcyIsIm5iZiI6MTU4NTc4NDkxOCwiZXhwIjoxNTg1Nzg4NTE4LCJ1c2VyIjoiYWRtaW5pc3Ry
YXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsInNjb3BlIjpbIkJ
BQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl9XUklURSIsIkJBQ0
tVUF9DT05GSUdfV1JJVEUiLCJPVEhFUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XUklURSJdfQ.Ya4XsZ
ntsRHUZFRBNKGY7Js6xrGYGe8KdgJ2QbihFmg" -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 'https://SDDC_MANAGER_IP/v1/system/ntp-configuration' -k -X GET -H "Content-Type:
application/json" -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiI2ZGRmZmU3MC0zZGEwLTQ5NmUtOTQzMC1hOGNkNTQ0YTk2ZGMiLCJpYXQiOj
E1ODU3ODE3ODcsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZi1hdXRoIiwiYXVkI
joic2RkYy1zZXJ2aWNlcyIsIm5iZiI6MTU4NTc4MTc4NywiZXhwIjoxNTg1Nzg1Mzg3LCJ1c2VyIjoiYWRtaW5pc3Ry
YXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsInNjb3BlIjpbIkJ
BQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl9XUklURSIsIkJBQ0
tVUF9DT05GSUdfV1JJVEUiLCJPVEhFUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XUklURSJdfQ.WCpUPR
Im5A6X_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 appliance 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
`--domain-name` *DOMAINNAME*	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 `--domain-name ALL`. **Note** If you omit the *--domain-name* flag and domain name, the SoS operation is performed only on the management domain.
`--force`	Allows SoS operations to be formed while workflows are running. **Note** It is recommended that you do not use this option.
`--history`	Displays the last 20 SoS operations performed.
`--ondemand-service`	Include this flag to execute commands on all ESXi hosts in a domain. **Warning** Contact VMware support before using this option.
`--ondemand-service` *JSON file path*	Include this flag to execute commands in the JSON format on all ESXi hosts in a domain. For example, `/opt/vmware/sddc-support/<JSON file name>`
`--setup-json` *SETUPJSON*	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 `setup.json` file and pass the file as input to SoS. A sample JSON file is available on the SDDC Manager appliance in the `/opt/vmware/sddc-support/` directory.
`--skip-known-host-check`	Skips the specified check for SSL thumbprint for host in the known host.
`--zip`	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
`--json-output-dir JSONDIR`	Outputs the results of any health check as a JSON file to the specified directory, `JSONDIR`.
`--certificate-health`	Verifies that the component certificates are valid (within the expiry date).
`--connectivity-health`	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
`--composability-infra-health`	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.
`--compute-health`	Performs a compute health check, including ESXi host licenses, disk storage, disk partitions, and health status.
`--dns-health`	Performs a forward and reverse DNS Health Check.
`--general-health`	Checks ESXi for error dumps and gets NSX Manager and cluster status.
`--get-host-ips`	Returns host names and IP addresses of ESXi hosts.
`--get-inventory-info`	Returns inventory details for the Cloud Foundation components, such as vCenter Server NSX, SDDC Manager, and ESXi hosts. Optionally, add the flag `--domain-name ALL` to return all details.
`--hardware-compatibility-report`	Validates ESXi hosts and vSAN devices and exports the compatibility report.
`--health-check`	Performs all available health checks.
`--ntp-health`	Verifies whether the time on the components is synchronized with the NTP server in the SDDC Manager appliance. It also ensures that the hardware and software time stamp of ESXi hosts are within 5 minutes of the SDDC Manager appliance.
`--password-health`	Returns the status of all current passwords, such as Last Changed Date, Expiry Date, and so on.
`--services-health`	Performs a services health check to confirm whether services within the SDDC Manager (like Lifecycle Management Server) and vCenter Server are running.
`--storage-health`	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.
`--run-vsan-checks`	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
`--disable-lockdown-esxi`	Deactivate lockdown mode on ESXi nodes in the specified domains. ■ To deactivate lockdown on ESXi nodes in a specific domain, include the flag `--domain-name DOMAINNAME`. ■ To deactivate lockdown on ESXi nodes in all domains, include the flag `--domain-name ALL`. **Note** If you do not specify domain, this command affects only the MGMT domain by default.
`--enable-lockdown-esxi`	Enables lockdown mode on ESXi nodes in the specified domains. ■ To enable lockdown on ESXi nodes in a specific domain, include the flag `--domain-name DOMAINNAME`. ■ To enable lockdown on ESXi nodes in all domains, include the flag `--domain-name ALL`. **Note** If you do not specify domain, this command affects only the MGMT domain by default.
`--disable-ssh-esxi`	Deactivate SSH on ESXi nodes in the specified domains. ■ To deactivate SSH on ESXi nodes in a specific domain, include the flag `--domain-name DOMAINNAME`. ■ To deactivate SSH on ESXi nodes in all domains, include the flag `--domain-name ALL`. **Note** If you do not specify domain, this command affects only the MGMT domain by default.
`--enable-ssh-esxi`	Enables SSH on ESXi nodes in the specified domains. ■ To enable SSH on ESXi nodes in a specific domain, include the flag `--domain-name DOMAINNAME`. ■ To enable SSH on ESXi nodes in all domains, include the flag `--domain-name ALL`. **Note** If you do not specify domain, this command affects only the MGMT domain by default.
`--refresh-ssh-keys`	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
`--api-logs`	Collects output from REST endpoints for SDDC Manager inventory and LCM.
`--esx-logs`	Collects logs from the ESXi hosts only. Logs are collected from each ESXi host available in the deployment.
`--log-dir` *`LOGDIR`*	Specifies the directory to store the logs.
`--log-folder` *`LOGFOLDER`*	Specifies the name of the log directory.
`--no-clean-old-logs`	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.
`--no-health-check`	Skips the health check executed as part of log collection.
`--nsx-logs`	Collects logs from the NSX Manager and NSX Edge instances only.
`--rvc-logs`	Collects logs from the Ruby vSphere Console (RVC) only. RVC is an interface for ESXi and vCenter. **Note** If the Bash shell is not enabled in vCenter, RVC log collection will be skipped . **Note** RVC logs are not collected by default with ./sos log collection. You must enable RVC to collect RVC logs.
`--sddc-manager-logs`	Collects logs from the SDDC Manager only. `sddc`*`<timestamp>`*`.tgz` contains logs from the SDDC Manager file system's `etc`, `tmp`, `usr`, and `var` partitions.
`--test`	Collects test logs by verifying the files.
`--vc-logs`	Collects logs from the vCenter Server instances only. Logs are collected from each vCenter server available in the deployment.
`--vm-screenshots`	Collects all VM screenshots.
`--vrealize-logs`	Collects logs from vRealize Suite Lifecycle Manager.

Procedure

1 Using SSH, log in to the SDDC Manager appliance 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 appliance

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
esx-*FQDN*.tgz	Diagnostic information from running the `vm-support` command on the ESXi host. An example file is `esx-esxi-1.vrack.vsphere.local.tgz`.
SmartInfo-*FQDN*.txt	S.M.A.R.T. status of the ESXi host's hard drive (Self-Monitoring, Analysis, and Reporting Technology). An example file is `SmartInfo-esxi-1.vrack.vsphere.local.txt`.
vsan-health-*FQDN*.txt	vSAN cluster health information from running the standard command `python /usr/lib/vmware/vsan/bin/vsan-health-status.pyc` on the ESXi host. An example file is `vsan-health-esxi-1.vrack.vsphere.local.txt`.

`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
VMware-NSX-Manager-tech-support-*nsxmanagerIPaddr*.tar.gz	Standard NSX Manager compressed support bundle, generated using the NSX API `POST https://`*`nsxmanagerIPaddr`*`/api/1.0/appliance-management/techsupportlogs/NSX`, where *nsxmanagerIPaddr* is the IP address of the NSX Manager instance. An example is VMware-NSX-Manager-tech-support-10.0.0.8.tar.gz.
VMware-NSX-Edge-tech-support-*nsxmanagerIPaddr*-*edgeId*.tgz **Note** This information is only collected if NSX Edges are deployed.	Standard NSX Edge support bundle, generated using the NSX API to query the NSX Edge support logs: `GET https://`*`nsxmanagerIPaddr`*`/api/4.0/edges/`*`edgeId`*`/techsupportlogs`, where *nsxmanagerIPaddr* is the IP address of the NSX Manager instance and *edgeID* identifies the NSX Edge instance. An example is VMware-NSX-Edge-tech-support-10.0.0.7-edge-1.log.gz.

`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
vc-*vcsaFQDN*-vm-support.tgz	Standard vCenter Server support bundle downloaded from the vCenter Server Appliance instance having a fully qualified domain name *vcsaFQDN*. The support bundle is obtained from the instance using the standard `vc-support.sh` command.

User and Group Management 20

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

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 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 20 User and Group Management.

2 Click **Developer Center > API Explorer**.

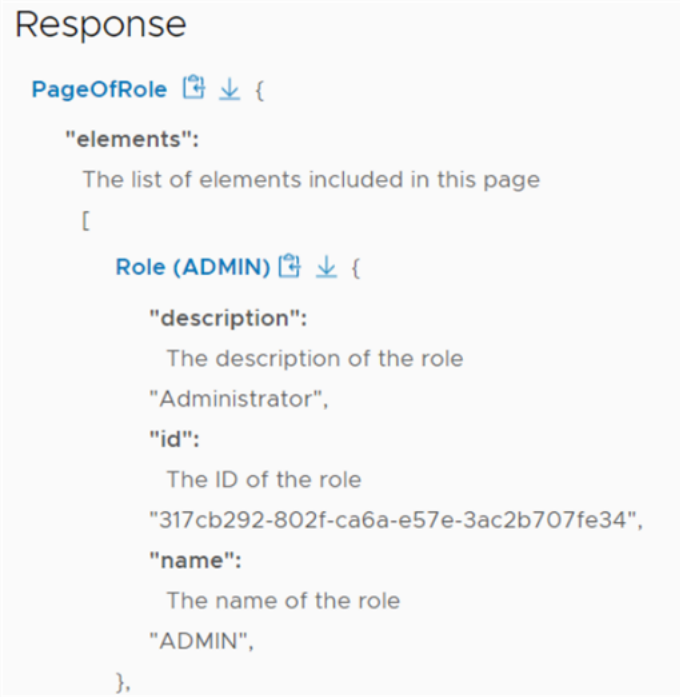
3 Get the ID for the ADMIN role.

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.



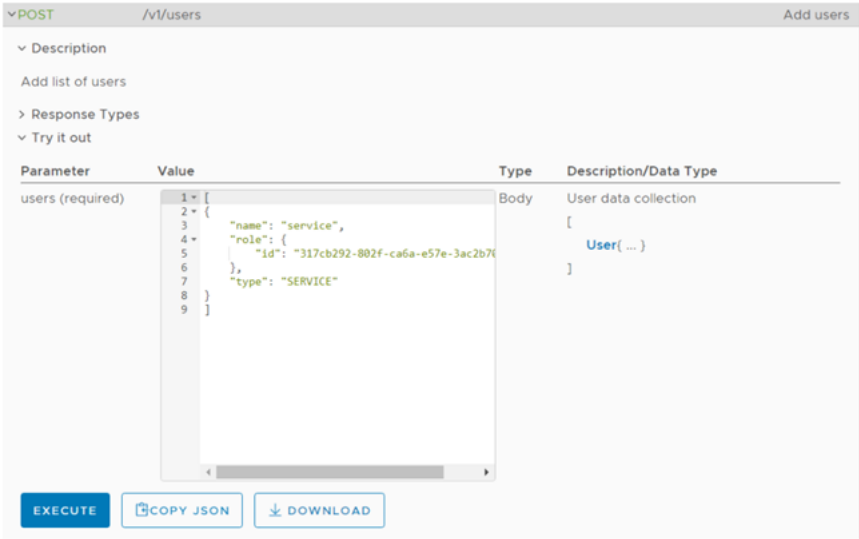
4 Create a service account with the ADMIN role and get the service account's API key.

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"
      }
  }
]
```

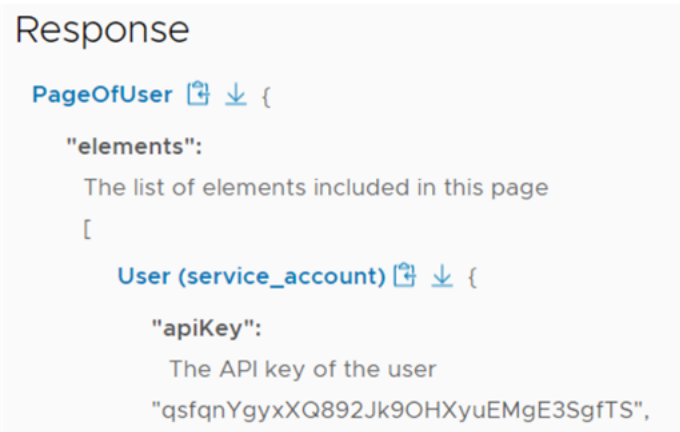
Paste the ADMIN role ID from step 3.



c Click **Execute**.

d In the Response, click `PageOfUser` and `User (service_account)`.

e Copy the API key for the service account.



5 Use the service account's API key to generate an access token.

a Expand **APIs for managing access and refresh tokens**.

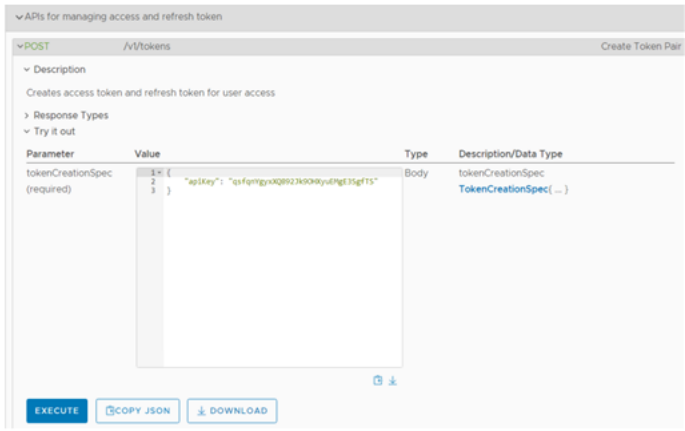
b Expand `POST /v1/tokens`.

c Click **TokenCreationSpec**.

d Replace Value with:

```
{
    "apiKey": "qsfqnYgyxXQ892Jk90HXyuEMgE3SgfTS"
}
```

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.

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 20 User and Group Management.

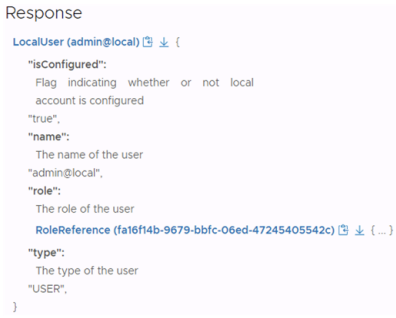
2. Click **Developer Center > API Explorer**.

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)`.

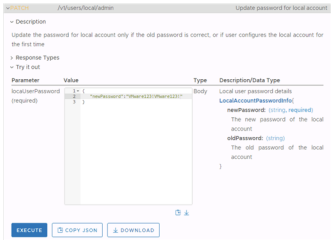


   You can also download the response by clicking the download icon to the right of `LocalUser (admin@local)`.

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.

Manage Passwords

21

You specify the passwords for your VMware Cloud Foundation system's internal accounts as part of the bring-up procedure. You can also modify the passwords for these accounts using RESTful API calls.

You can update or rotate the password for the `root` and `mystic` users of the VxRail Manager and the `root` user of ESXi hosts using the SDDC Manager. To update or rotate the passwords for other users refer to the Dell EMC VxRail documentation.

To provide the optimal security and proactively prevent any passwords from expiring, you should rotate passwords every 80 days.

This chapter includes the following topics:

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.

- VxRail Manager
- 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 20 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 20 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 appliance 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 appliance 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 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
passwd vcf	To change the super user password.
passwd root	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/commonsvcs/scripts/auth/set-basicauth-password.sh admin <password>
   ```

   For *<password>*, enter the new password for the **admin** account.

Backing Up and Restoring SDDC Manager and NSX Manager 22

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 on Dell EMC VxRail 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

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-quiesced 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 20 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 20 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 and access token and a refresh token.

```
{"accessToken":"eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiI2ZGRmZmU3MC0zZGEwLTQ5NmUtOTQzMC1hOGNkNTQ0YT
k2ZGMiLCJpYXQiOjE1ODU3ODE3ODcsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZ
i1hdXRoIiwiYXVkIjoic2RkYy1zZXJ2aWNlcyIsIm5iZiI6MTU4NTc4MTc4NywiZXhwIjoxNTg1Nzg1Mzg3LCJ1c2Vy
IjoiYWRtaW5pc3RyYXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCI
sInNjb3BlIjpbIkJBQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl
9XUklURSIsIkJBQ0tVUF9DT05GSUdfV1JJVEUiLCJPVEhFUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XU
klURSJdfQ.WCpUPRIm5A6X_406HTJF7TbTSa0g91_AQbt7OcBPblM","refreshToken":
{"id":"47c07f35-0a89-4df5-a3a3-f31265ebbb7a"}}
```

2 Set the backup schedule, for example:

```
curl 'https://SDDC_MANAGER_IP/v1/system/backup-configuration' -k -X PATCH -H 'Content-
Type: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiI2ZGRmZmU3MC0zZGEwLTQ5NmUtOTQzMC1hOGNkNTQ0YTk2ZGMiLCJpYXQiOj
E1ODU3ODE3ODcsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZi1hdXRoIiwiYXVkI
joic2RkYy1zZXJ2aWNlcyIsIm5iZiI6MTU4NTc4MTc4NywiZXhwIjoxNTg1Nzg1Mzg3LCJ1c2VyIjoiYWRtaW5pc3Ry
YXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsInNjb3BlIjpbIkJ
BQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl9XUklURSIsIkJBQ0
tVUF9DT05GSUdfV1JJVEUiLCJPVEhFUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XUklURSJdfQ.WCpUPR
Im5A6X_406HTJF7TbTSa0g91_AQbt7OcBPblM' -d '{ "backupSchedules" : [ { "resourceType" :
"SDDC_MANAGER", "frequency" : "WEEKLY", "daysOfWeek" : [ "MONDAY" ], "hourOfDay" : 12,
"minuteOfHour" : 23 } ] }'
```

Option	Description
Resource Type	Enter **SDDC_MANAGER**.
Frequency	Enter **HOURLY** or **WEEKLY**.
Days of Week	Enter the days to back up SDDC Manager. When selecting multiple days, use a comma to separate them. For example: `"daysOfWeek" : [ "SUNDAY", "THURSDAY" ]` **Note** Only available if the frequency is set to **WEEKLY**.

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.eyJqdGkiOiIxN2M5YThmOC00NGQwLTQ5MzYtYjQwMC0xMzc5NzMyMjdmOWUiLCJpYXQiOj
E1ODU3ODQ5MTgsInN1YiI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsImlzcyI6InZjZi1hdXRoIiwiYXVkI
joic2RkYy1zZXJ2aWNlcyIsIm5iZiI6MTU4NTc4NDkxOCwiZXhwIjoxNTg1Nzg4NTE4LCJ1c2VyIjoiYWRtaW5pc3Ry
YXRvckB2c3BoZXJlLmxvY2FsIiwibmFtZSI6ImFkbWluaXN0cmF0b3JAdnNwaGVyZS5sb2NhbCIsInNjb3BlIjpbIkJ
BQ0tVUF9DT05GSUdfUkVBRCIsIkNSRURFTlRJQUxfUkVBRCIsIlVTRVJfV1JJVEUiLCJPVEhFUl9XUklURSIsIkJBQ0
tVUF9DT05GSUdfV1JJVEUiLCJPVEhFUl9SRUFEIiwiVVNFUl9SRUFEIiwiQ1JFREVOVElBTF9XUklURSJdfQ.Ya4XsZ
ntsRHUZFRBNKGY7Js6xrGYGe8KdgJ2QbihFmg" -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.

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.

Lifecycle Management 23

Lifecycle Management (LCM) enables you to perform automated updates on VMware Cloud Foundation services (SDDC Manager and internal services), VMware software (NSX-T Data Center, vCenter Server, ESXi, and vRealize Suite Lifecycle manager), and Dell EMC VxRail in your environment. You can download the update bundles and apply them manually or schedule them within your maintenance window allowing for flexibility in your application.

The LCM bundles that are available are:

- VxRail Partner Bundle: You can download the Dell EMC VxRail partner bundle to update the VxRail appliance.
- Patch Update Bundle: A patch update bundle contains bits to update the appropriate Cloud Foundation software components in your management domain or VI workload domain. In most cases, a patch update bundle must be applied to the management domain before it can be applied to VI workload domains.
- Cumulative Update Bundle: With a cumulative update bundle, you can directly update the appropriate software in your workload domain to the version contained in the cumulative bundle rather than applying sequential updates to reach the target version.
- Install Bundle: If you have updated the management domain in your environment, you can download an install bundle with updated software bits for VI workload domains and vRealize Suite Lifecycle Manager.

This chapter includes the following topics:

Download VMware Cloud Foundation on Dell EMC VxRail Bundles

If SDDC Manager is configured to work with your VMware Customer Connect and Dell EMC accounts, LCM automatically polls the depots to access install and upgrade bundles. You receive a notification when a bundle is available and can then download the bundle.

If SDDC Manager does not have direct internet connectivity, you can either use a proxy server to access the depot, or download install and upgrade bundles manually using the Bundle Transfer Utility.

To download an async patch bundle, you must use the Async Patch Tool. For more information, see the Async Patch Tool documentation.

Download VMware Cloud Foundation on Dell EMC VxRail Bundles from SDDC Manager

If SDDC Manager has an internet connection, you can download bundles directly from SDDC Manager UI.

When upgrade bundles are available for your environment, a message is displayed on SDDC Manager UI. Available install bundles are displayed on the Bundle Management page.

To download an install bundle, navigate to **Repository > Bundle Management** to view the available bundles.

1 To access the bundles, you have two options:

- In the SDDC Manager Dashboard, navigate to the **Bundles** page. This page shows the available update bundles for the components.
  1 Click **Lifecycle Management > Bundle Management**.
- In the SDDC Manager Dashboard, navigate to the **Workload Domain** page.
  1 Click **Inventory > Workload Domains**.
  2 Click the name of a workload domain and then click the **Updates/Patches** tab.

    The number next to the Updates/Patches tab indicates the available updates.

    The **Available Updates** section displays all updates applicable to this workload domain.

    Also, you can view the current versions running such as the VxRail current version.

2 To view the metadata details for an update bundle, click **View Details**. The bundle severity and detailed information about each component included in the bundle is displayed. If a bundle is a cumulative bundle, this information is displayed as well. The bundle severity levels are described in the table below.

Severity Value	Description
Critical	A problem may severely impact your production systems (including the loss of production data). Such impacts could be system down or HA not functioning.
Important	A problem may affect functionality, or cause a system to function in a severely reduced capacity. The situation causes significant impact to portions of the business operations and productivity. The system is exposed to potential loss or interruption of services. A change to support hardware enablement (for example, a driver update), or a new feature for an important product capability.

Severity Value	Description
Moderate	A problem may affect partial non-critical functionality loss. This may be a minor issue with limited loss, no loss of functionality, or impact to the client's operations and issues in which there is an easy circumvention or avoidance by the end user. This includes documentation errors.
Low	A problem which has low or no impact to a product's functionality or a client's operations. There is no impact on quality, performance, or functionality of the product.

3 Click **Schedule Download**. Select the date and time for the bundle download and click **Schedule**.

Prerequisites

Automatic polling of the manifest for bundles by SDDC Manager is enabled by default. If you have previously edited the `application-prod.properties` file on the SDDC Manager appliance to download upgrade bundles in an offline mode, you must edit it again before downloading bundles from SDDC Manager. Follow the steps below:

1 Using SSH, log in to the SDDC Manager appliance as the **`vcf`** user.

2 Enter **`su`** to switch to the root user.

3 Open the `/opt/vmware/vcf/lcm/lcm-app/conf/application-prod.properties` file.

4 Set `lcm.core.enableManifestPolling=true`.

5 Restart the LCM service:

```
systemctl restart lcm
```

Procedure

1 In the SDDC dashboard, click **Administration > Repository Settings**.

2 Enter your My VMware and Dell EMC credentials and click **Authenticate**.

You have to log in to both My VMware and Dell EMC to update all the VMware Cloud Foundation and the VxRail components.

3 Enter your usernames and passwords and click **Authorize**.

4 View available bundles by navigating to **Lifecycle Management > Bundle Management** on SDDC Manager UI.

The Bundles page displays the bundles available for download. The Bundle Details section displays the bundle version and release date.

If the bundle can be applied right away, the Bundle Details column displays the workload domains to which the bundle needs to be applied and the Availability column displays **Available**. If another bundle needs to be applied before a particular bundle, the Availability column displays **Future**.

5 To view more information about the bundle, click **View Details**.

The Bundle Details section displays the bundle version, release date, and additional details about the bundle.

6 Click **Exit Details**.

7 Specify when to download the bundle.

- Click **Download Now** to start the download immediately.
- Click **Schedule Download** to set the date and time for the bundle download.

Results

The Download Status section displays the date and time at which the bundle download has been scheduled. When the download begins, the status bar displays the download progress.

Download VMware Cloud Foundation on Dell EMC VxRail Bundles with a Proxy Server

If you do not have internet access, you can use a proxy server to download the LCM bundles. LCM only supports proxy servers that do not require authentication.

Procedure

1 Using SSH, log in to the SDDC Manager appliance with the user name `vcf` and password you specified in the deployment parameter sheet.

2 Type `su` to switch to the root account.

3 Open the `/opt/vmware/vcf/lcm/lcm-app/conf/application-prod.properties` file.

4 Add the following lines to the end of the file:

```
lcm.depot.adapter.proxyEnabled=true
lcm.depot.adapter.proxyHost=proxy IP address
lcm.depot.adapter.proxyPort=proxy port
```

5 Save and close the file.

6 Restart the LCM server by typing the following command in the console window:

```
systemctl restart lcm
```

7 Wait for 5 minutes and then download the bundles.

Download Bundles for VMware Cloud Foundation on Dell EMC VxRail with the Bundle Transfer Utility

Lifecycle Management polls the VMware depot to access install and update bundles. If you do not have internet connectivity in your VMware Cloud Foundation system, you can use the Bundle Transfer Utility to manually download the bundles from the depot on your local computer and then upload them to the SDDC Manager appliance.

When you download bundles, the Bundle Transfer Utility verifies that the file size and checksum of the downloaded bundles match the expected values.

Prerequisites

- A Windows or Linux computer with internet connectivity for downloading the bundles.
- The computer must have Java 8 or later.
- A Windows or Linux computer with access to the SDDC Manager appliance for uploading the bundles.
- To upload the manifest file from a Windows computer, you must have OpenSSL installed and configured.
- Configure TCP keepalive in your SSH client to prevent socket connection timeouts when using the Bundle Transfer Utility for long-running operations.

Note The Bundle Transfer Utility is the only supported method for downloading bundles. Do not use third-party tools or other methods to download bundles.

Procedure

1 Download the Bundle Transfer Utility on a computer with internet access.
   a Log in to VMware Customer Connect and browse to the Download VMware Cloud Foundation page.
   b In the **Select Version** field, select the version to which you are upgrading.
   c Click **Drivers & Tools**.
   d Expand VMware Cloud Foundation Supplemental Tools.
   e Click **Download Now** for the Bundle Transfer Utility.
2 Extract `lcm-tools-prod.tar.gz`.
3 Navigate to `lcm-tools-prod/bin/` and confirm that you have execute permission on all folders.
4 Copy the Bundle Transfer Utility to a computer with access to the SDDC Manager appliance and then copy the Bundle Transfer Utility to the SDDC Manager appliance.
   a SSH in to the SDDC Manager appliance using the **`vcf`** user account.
   b Enter **`su`** to switch to the root user.
   c Create the `lcm-tools` directory.

```
mkdir /opt/vmware/vcf/lcm/lcm-tools
```

   d Copy the bundle transfer utility file (`lcm-tools-prod.tar.gz`) that you downloaded in step 1 to the `/opt/vmware/vcf/lcm/lcm-tools` directory.

e Extract the contents of `lcm-tools-prod.tar.gz`.

f Set the permissions for the `lcm-tools` directory.

```
cd /opt/vmware/vcf/lcm/
          chown vcf_lcm:vcf -R lcm-tools
          chmod 750 -R lcm-tools
```

5 On the computer with internet access, download the manifest file.

This is a structured metadata file that contains information about the VMware Cloud Foundation product versions included in the release Bill of Materials.

```
 ./lcm-bundle-transfer-util --download --manifestDownload --depotUser Username --
depotUserPassword Password
```

6 Copy the manifest file and `lcm-tools-prod` directory to a computer with access to the SDDC Manager appliance.

7 Upload the manifest file to the SDDC Manager appliance.

```
./lcm-bundle-transfer-util --update --sourceManifestDirectory downloaded-manifest-
directory --sddcMgrFqdn FQDN --sddcMgrUser Username
```

Use your vSphere SSO credentials for the `--sddcMgrUser` credentials in the command.

8 On the computer with internet access, run the following command:

```
./lcm-bundle-transfer-util --download "withCompatibilitySets" --outputDirectory absolute-
path-output-dir --depotUser customer_connect_email --sv current-vcf-version --p target-vcf-
version --pdu dell_emc_depot_email
```

absolute-path-output-dir	Path to the directory where the bundle files should be downloaded. This directory folder must have 777 permissions. If you do not specify the download directory, bundles are downloaded to the default directory with 777 permissions.
depotUser	VMware Customer Connect email address. You will be prompted to enter the depot user password. If there are any special characters in the password, specify the password within single quotes.
current-vcf-version	Current version of VMware Cloud Foundation. For example, **`4.3.1.1`**. If you do not specify a current version, the utility uses **`4.1.0.0`**.
target-vcf-version	Current version of VMware Cloud Foundation. For example, **`4.4.0.0`**.
dell_emc_depot_email	Dell EMC depot email address.

After you enter you VMware Customer connect and Dell EMC Depot passwords, the utility asks `Do you want to download vRealize bundles?`. Enter **`Y`** or **`N`**.

The utility displays a list of the available bundles based on the current and target versions of VMware Cloud Foundation.

9 Specify the bundles to download.

Enter one of the following options:

- **all**
- **install**
- **patch**

You can also enter a comma-separated list of bundle names to download specific bundles. For example: **bundle-38371, bundle-38378**.

Download progress for each bundle is displayed. Wait until all bundles are downloaded.

10 If you downloaded VxRail bundles:

a Copy the partner bundle to the `/nfs/vmware/vcf/nfs-mount/bundle/depot/local/bundles` directory on the SDDC Manager appliance.

b Copy `partnerBundleMetadata.json` to the `/nfs/vmware/vcf/nfs-mount/bundle/depot/local` directory on the SDDC Manager appliance.

c Copy `softwareCompatibilitySets.json` to the `/nfs/vmware/vcf/nfs-mount/bundle/depot/local` directory on the SDDC Manager appliance.

d Run following commands on the SDDC Manager appliance:

```
chown -R vcf_lcm:vcf /nfs/vmware/vcf/nfs-mount/bundle/depot/local
```

```
chmod -R 755 /nfs/vmware/vcf/nfs-mount/bundle/depot/local
```

11 If you downloaded bundles for VMware Cloud Foundation and its components, copy the entire output directory to a computer with access to the SDDC Manager appliance, and then copy it to the SDDC Manager appliance.

For example:

```
scp -pr /root/upgrade-bundles vcf@SDDC_MANAGER_IP:/nfs/vmware/vcf/nfs-mount/
```

The scp command in the example above copies the output directory (`upgrade-bundles`) to the `/nfs/vmware/vcf/nfs-mount/` directory on the SDDC Manager appliance.

12 In the SDDC Manager appliance, upload the bundle directory to the internal LCM repository.

```
./lcm-bundle-transfer-util --upload "withCompatibilitySets" --bundleDirectory
absolute-path-bundle-dir
```

where *absolute-path-bundle-dir* is the directory where the bundle files have been be uploaded, or `/nfs/vmware/vcf/nfs-mount/upgrade-bundles` as shown in the previous step.

The utility uploads the bundles and displays upload status for each bundle. Wait for all bundles to be uploaded before proceeding with an upgrade.

View VMware Cloud Foundation on Dell EMC VxRail Bundle Download History

The Download History page displays all bundles that have been downloaded.

Procedure

- In the SDDC Manager Dashboard, click **Repository > Bundle Management > Download History**.

  All downloaded bundles are displayed. Click **View Details** to see bundle metadata details.

Upgrade to VMware Cloud Foundation 4.2.1 or 4.2 on Dell EMC VxRail

The following procedures provide information about upgrading to VMware Cloud Foundation 4.2.1 on Dell EMC VxRail or VMware Cloud Foundation 4.2 on Dell EMC VxRail.

You can upgrade to VMware Cloud Foundation 4.2 from VMware Cloud Foundation 4.1.0.1 or VMware Cloud Foundation 4.1. If your environment is at a version earlier than 4.1, you must upgrade the management domain and all VI workload domains to VMware Cloud Foundation 4.1 and then upgrade to VMware Cloud Foundation 4.2.

You can upgrade to VMware Cloud Foundation 4.2.1 from VMware Cloud Foundation 4.2, 4.1.0.1, or 4.1.

Your environment may contain workload domains at different VMware Cloud Foundation releases. After upgrading to VMware Cloud Foundation 4.2, you can view the versions in your environment and the associated component versions in that release by navigating to **Lifecycle Management > Release Versions**. Note that the management domain and VI workload domains must be upgraded to the same release version. For example, suppose your environment is at VMware Cloud Foundation 4.1. If you are upgrading to VMware Cloud Foundation 4.2, the management domain and VI workload domains must be upgraded to this release.

Note You cannot upgrade to VMware Cloud Foundation 4.2 if you have Federation 3.0.x in your environment.

Upgrades are applied on a workload domain basis. The management domain contains the core infrastructure, so you must upgrade the management domain before upgrading the other VI workload domains. You must upgrade all required components to keep your system in an optimum state.

- Upgrade Prerequisites for VMware Cloud Foundation on Dell EMC VxRail

  Ensure that the following prerequisites are met before starting an upgrade.

- Upgrade the Management Domain for VMware Cloud Foundation on Dell EMC on VxRail

  You must upgrade the management domain before upgrading VI workload domains in your environment.

- Upgrade a VI Workload Domain for VMware Cloud Foundation on Dell EMC on VxRail

  Before you can upgrade a VI workload domain, you must upgrade the management domain.

Upgrade Prerequisites for VMware Cloud Foundation on Dell EMC VxRail

Ensure that the following prerequisites are met before starting an upgrade.

- Take a backup of the SDDC Manager appliance. This is required since the SDDC Manager appliance will be rebooted during the update.
- Take a snapshot of relevant VMs in your management domain.
- Do not run any domain operations while an update is in progress. Domain operations are creating a new VI domain, adding hosts to a cluster or adding a cluster to a workload domain, and removing clusters or hosts from a workload domain.
- Download the relevant bundles. See Download VMware Cloud Foundation on Dell EMC VxRail Bundles.
- If you applied an async patch to your current VMware Cloud Foundation instance you must use the Async Patch Tool to upgrade to a later version of VMware Cloud Foundation. For example, if you applied an async vCenter Server patch to a VMware Cloud Foundation 4.3.1 instance, you must use the Async Patch Tool to upgrade to VMware Cloud Foundation 4.4. See the Async Patch Tool documentation.
- Ensure that there are no failed workflows in your system and none of the VMware Cloud Foundation resources are in activating or error state. If any of these conditions are true, contact VMware Support before starting the upgrade.
- Confirm that the passwords for all VMware Cloud Foundation components are valid. An expired password can cause an upgrade to fail.
- Review the *VMware Cloud Foundation on Dell EMC Release Notes* for known issues related to upgrades.

Upgrade the Management Domain for VMware Cloud Foundation on Dell EMC on VxRail

You must upgrade the management domain before upgrading VI workload domains in your environment.

To upgrade to VMware Cloud Foundation 4.2.1 from VMware Cloud Foundation 4.2, the components in the management domain must be upgraded in the following order:

1. SDDC Manager and VMware Cloud Foundation services.
2. vCenter Server.
3. NSX-T Data Center.

To upgrade to VMware Cloud Foundation 4.2.1 from VMware Cloud Foundation 4.1.0.1 or 4.1, the components in the management domain must be upgraded in the following order:

1 SDDC Manager and VMware Cloud Foundation services.

2 vRealize Suite Lifecycle Manager and vRealize Suite products (if applicable).

3 VxRail Manager and ESXi.

4 vCenter Server.

5 NSX-T Data Center.

To upgrade to VMware Cloud Foundation 4.2, the components in the management domain must be upgraded in the following order:

1 SDDC Manager and VMware Cloud Foundation services.

2 vRealize Suite Lifecycle Manager and vRealize Suite products (if applicable).

   a vRealize Suite Lifecycle Manager

   b vRealize Log Insight

   c vRealize Operations

   d vRealize Automation

   e Workspace ONE Access

3 NSX-T Data Center.

4 vCenter Server.

5 VxRail Manager and ESXi.

The upgrade process is similar for all components. Information that is unique to a component is described in the following table.

Component	Additional Information
SDDC Manager and VMware Cloud Foundation services	The VMware Cloud Foundation software bundle to be applied depends on the current version of your environment. If you upgrading from VMware Cloud Foundation 4.2 or 4.1.0.1, you must apply the following bundles to the management domain: ■ The VMware Cloud Foundation bundle upgrades SDDC Manager, LCM, and VMware Cloud Foundation services. ■ The Configuration Drift bundle applies configuration drift on software components. If you upgrading from VMware Cloud Foundation 4.1, you apply the VMware Cloud Foundation Update bundle, which upgrades SDDC Manager, LCM, and VMware Cloud Foundation services, and also applies the configuration drift.
vRealize Log Insight	After upgrading vRealize Log Insight, upgrade the vRealize Log Insight content packs. Content packs are plugins to vRealize Log Insight that provide pre-defined knowledge about specific types of events such as log messages. You must upgrade to the latest content packs for use with vRealize Log Insight. 1 Log in to the vRealize Log Insight user interface as the admin user. 2 Click the configuration drop-down menu icon and select **Content Pack**. 3 In the **Content Pack** pane, under **Content Pack Market Place**, click **Updates**. 4 In the **Log Insight Content Pack Marketplace** pane, click **Update All** to upgrade all content packs to the latest version. After you upgrade the content packs, click each of the items under **Installed Content Packs** and verify that the version number of each content pack is the same as or newer than the version listed in the Release Notes for your version of VMware Cloud Foundation.
vRealize Operations	After the upgrade is complete, delete the vRealize Operations snapshots. 1 Log in to the management vCenter Server. 2 Select the vRealize Operations VM and click **Actions > Manage Snapshots**. 3 Delete the snapshots created during the upgrade.
vRealize Automation	After the upgrade is complete, delete the vRealize Automation snapshots. 1 Log in to the management vCenter Server. 2 Select the vRealize Automation VM and click **Actions > Manage Snapshots**. 3 Delete the snapshots created during the upgrade.

Component	Additional Information
Workspace ONE Access	If you had Workspace ONE Access in your pre-upgrade environment, you must upgrade it using vRealize Suite Lifecycle Manager. 1 On vRealize Suite Lifecycle Manager UI navigate to the **Lifecycle Operations** tab. Click **Settings > Binary Mapping**. 2 Select **Sync Binaries** to discover the upgrade image for Workspace ONE Access in SDDC Manager. 3 Click **Environments > Global Environment**. The global environment contains the Workspace ONE Access product. To upgrade the Workspace ONE Access product, see "Upgrade VMware Identity Manager" in *vRealize Suite Lifecycle Manager Installation, Upgrade, and Management*.

Component	Additional Information
NSX-T Data Center	**Important** If you are upgrading to VMware Cloud Foundation 4.2.1, you must upgrade vCenter Server before you upgrade NSX-T Data Center. Upgrading NSX-T Data Center involves the following components: ■ Upgrade Coordinator ■ Edge clusters (if deployed) ■ Host clusters ■ NSX Manager cluster Workload domains can share the same NSX Manager cluster and NSX Edge clusters. When you upgrade these components for one workload domain, they are upgraded for all workload domains that share the same NSX Manager or NSX Edge cluster. You cannot perform any operations on the workload domains while NSX-T Data Center is being upgraded. The upgrade wizard provides some flexibility when upgrading NSX-T Data Center for workload domains. By default, the process upgrades all Edge clusters in parallel, and then all host clusters in parallel. Parallel upgrades reduce the overall time required to upgrade your environment. You can also choose to upgrade Edge clusters and host clusters sequentially. If you have multiple Edge or host clusters in a workload domain, you can select which clusters to upgrade. The ability to select clusters allows for multiple upgrade windows and does not require all clusters to be available at a given time. The NSX Manager cluster is upgraded only if the **Upgrade all host clusters** setting is enabled on the NSX-T Host Clusters tab. New features introduced in the upgrade are not configurable until the NSX Manager cluster is upgraded. ■ If you have a single cluster in your environment, enable the **Upgrade all host clusters** setting. ■ If you have multiple host clusters and choose to upgrade only some of them, you must go through the NSX-T upgrade wizard again until all host clusters have been upgraded. When selecting the final set of clusters to be upgraded, you must enable the **Upgrade all host clusters** setting so that NSX Manager is upgraded. ■ If you upgraded all host clusters without enabling the **Upgrade all host clusters** setting, run through the NSX-T upgrade wizard again to upgrade NSX Manager.
ESXi	By default, the upgrade process upgrades the ESXi hosts in all clusters in a domain in parallel. If you have multiple clusters in the management domain or in a VI workload domain, you can select which clusters to upgrade. You can also choose to update the clusters in parallel or sequentially.

Component	Additional Information
	If you are using external (non-vSAN) storage, updating and patching is a manual task and falls outside of SDDC Manager lifecycle management. To ensure supportability after an ESXi upgrade, consult the vSphere HCL and your storage vendor.

Procedure

1 Navigate to the **Updates/Patches** tab of the management domain.

2 Click **Precheck** to validate that the component is ready to be updated.

Click **View Status** to see the update status for each component and the tests performed. Expand a test by clicking the arrow next to it to see further details.

If any of the tests fail, fix the issue and click **Retry Precheck**.

The precheck results are displayed below the **Precheck** button. Ensure that the precheck results are green before proceeding. A failed precheck may cause the update to fail.

3 Click **Update Now** or **Schedule Update** next to the relevant bundle.

If you selected **Schedule Update**, select the date and time for the bundle to be applied.

4 The **Update Status** window displays the components that will be upgraded and the upgrade status. Click **View Update Activity** to view the detailed tasks.

After the upgrade is completed, a green bar with a check mark is displayed.

Upgrade a VI Workload Domain for VMware Cloud Foundation on Dell EMC on VxRail

Before you can upgrade a VI workload domain, you must upgrade the management domain.

To upgrade to VMware Cloud Foundation 4.2.1 from VMware Cloud Foundation 4.2, the components in a VI workload domain must be upgraded in the following order:

1 vCenter Server.

2 NSX-T Data Center.

To upgrade to VMware Cloud Foundation 4.2.1 from VMware Cloud Foundation 4.1.0.1 or 4.1, the components in a VI workload domain must be upgraded in the following order:

1 VxRail Manager and ESXi.

2 vCenter Server.

3 NSX-T Data Center.

To upgrade to VMware Cloud Foundation 4.2, the components in a VI workload domain must be upgraded in the following order:

1 NSX-T Data Center.

2 vCenter Server.

3 VxRail Manager and ESXi.

The upgrade process is similar for all components. Information that is unique to a component is described in the following table.

Component	Additional Information
NSX-T Data Center	**Important** If you are upgrading to VMware Cloud Foundation 4.2.1, you must upgrade vCenter Server before you upgrade NSX-T Data Center. Upgrading NSX-T Data Center involves the following components: ■ Upgrade Coordinator ■ Edge clusters (if deployed) ■ Host clusters ■ NSX Manager cluster Workload domains can share the same NSX Manager cluster and NSX Edge clusters. When you upgrade these components for one workload domain, they are upgraded for all workload domains that share the same NSX Manager or NSX Edge cluster. You cannot perform any operations on the workload domains while NSX-T Data Center is being upgraded. The upgrade wizard provides some flexibility when upgrading NSX-T Data Center for workload domains. By default, the process upgrades all Edge clusters in parallel, and then all host clusters in parallel. Parallel upgrades reduce the overall time required to upgrade your environment. You can also choose to upgrade Edge clusters and host clusters sequentially. If you have multiple Edge or host clusters in a workload domain, you can select which clusters to upgrade. The ability to select clusters allows for multiple upgrade windows and does not require all clusters to be available at a given time. The NSX Manager cluster is upgraded only if the **Upgrade all host clusters** setting is enabled on the NSX-T Host Clusters tab. New features introduced in the upgrade are not configurable until the NSX Manager cluster is upgraded. ■ If you have a single cluster in your environment, enable the **Upgrade all host clusters** setting. ■ If you have multiple host clusters and choose to upgrade only some of them, you must go through the NSX-T upgrade wizard again until all host clusters have been upgraded. When selecting the final set of clusters to be upgraded, you must enable the **Upgrade all host clusters** setting so that NSX Manager is upgraded. ■ If you upgraded all host clusters without enabling the **Upgrade all host clusters** setting, run through the NSX-T upgrade wizard again to upgrade NSX Manager.
ESXi	By default, the upgrade process upgrades the ESXi hosts in all clusters in a domain in parallel. If you have multiple clusters in the management domain or in a VI workload domain, you can select which clusters to upgrade. You can also choose to update the clusters in parallel or sequentially.

Component	Additional Information
	If you are using external (non-vSAN) storage, updating and patching is a manual task and falls outside of SDDC Manager lifecycle management. To ensure supportability after an ESXi upgrade, consult the vSphere HCL and your storage vendor.

Procedure

1 Navigate to the **Updates/Patches** tab of the VI workload domain.

2 Click **Precheck** to validate that the component is ready to be updated.

Click **View Status** to see the update status for each component and the tests performed. Expand a test by clicking the arrow next to it to see further details.

If any of the tests fail, fix the issue and click **Retry Precheck**.

The precheck results are displayed below the **Precheck** button. Ensure that the precheck results are green before proceeding. A failed precheck may cause the update to fail.

3 Click **Update Now** or **Schedule Update** next to the relevant bundle.

If you selected **Schedule Update**, select the date and time for the bundle to be applied.

4 The **Update Status** window displays the components that will be upgraded and the upgrade status. Click **View Update Activity** to view the detailed tasks.

After the upgrade is completed, a green bar with a check mark is displayed.