VMware Cloud Foundation on Dell EMC VxRail Admin Guide

VMware Cloud Foundation 4.0

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

https://docs.vmware.com/

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

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 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, virtual infrastructure (VI), and virtual desktop infrastructure (VDI)
- VMware virtualization technologies, such as VMware ESXi™, the hypervisor
- Software-defined networking using VMware NSX®
- 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™

Related Publications

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

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

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

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.

Imaging of the Management Nodes

3

Image the 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 information on how to image the VxRail nodes, contact Dell EMC Support.

VxRail First Run for the Management Cluster

4

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.

Change the Network Binding Type for the Management Network Port Group

5

Dell EMC VxRail configures the management network port with static binding which is the default setting. But as per the VMware Validated Design guidelines, you need to change the binding type to ephemeral for the management network port.

To change the binding type for the management network port:

Prerequisites

1 Log in to vCenter Server Appliance through vSphere Web client (Flash version).

2 Navigate to **Networking->Distributed Switch**.

3 Right click the **Management Network Port** group and click **Edit Settings**.

4 Verify if the network binding type is static binding and note down the VLAN ID.

Procedure

1 In vCenter Server Appliance, click **Networking**.

2 Select **Distributed Switch** > **Distributed Port Group**.

Right-click **New Distributed Port Group**, update **Name** as **TempGroup** and keep the configuration same as the management network port group.

3 Change **VLAN type** from **None** to **VLAN**.

4 Update **VLAN ID** to that of the management network port group.

5 Click **Next** and review the configurations.

6 Click **Finish**.

A new port group, **TempGroup**, is created and is shown in the port group list of the distributed switch.

7 Click **Hosts and Clusters**.

8 Select the first host of the cluster and click **Configure**.

9 Click **Virtual Switches > Distributed Switch**.

10 Click the **Migrate physical to virtual network adapters to this distributed switch** option.

11 In the **Migrate Networking** pop up screen, select only **Manage VMkernel adapters**.

Click **Next**.

12 Select the VMkernel network adapter associated with the management network.

13 Click **Assign port group**.

14 Select **TempGroupAssign destination port group** pop up screen and click **OK**.

Click **Next**.

15 Confirm **Overall impact** status as **No impact**. Click **Finish**.

16 Repeat steps 8 to 15 for all the other hosts of the cluster.

17 Click **Networking**.

18 Right-click **Management Network** and click **Edit Settings**.

In the **Edit Settings** screen, change **Port binding** from **Static binding** to **Ephemeral - no binding**.

19 Select **VLAN** and make sure **VLAN type** is **VLAN ID** is the same.

20 Click **Hosts and Clusters**.

Select the first host of the cluster and click **Configure**.

21 Select **Virtual Switches > Distributed Switch**.

22 Click the **Migrate physical to virtual network adapters to this distributed switch** option.

23 In the **Migrate Networking** pop up screen, select only **Manage VMkernel adapters**.

Click **Next**.

24 Select the VMkernel network adapter associated with the management network.

25 Click **Assign port group**.

26 Select the **Management Network in Assign destination port group** pop up screen and click **OK**. Click Next.

27 Confirm **Overall impact status** as **No impact**. Click **Finish**.

28 Repeat steps 21 to 27 for all the other hosts of the cluster.

29 Click **Networking**.

30 Select **Distributed Switch > TempGroup**.

31 Right-click **TempGroup** and click **Delete**.

32 Click **Yes** in **Delete Distributed Port Group** pop up UI screen.

Externalize vCenter Server

6

By default, VMware vCenter server is deployed within the VxRail cluster during the first run process. It must be externalized so that you can manage and lifecycle through SDDC Manager.

To convert the embedded VxRail VMware vCenter server to a customer-managed VMware vCenter server, contact Dell EMC Support.

Starting with Cloud Foundation 4.0.1, externalization of VMware vCenter server is automated during the bring-up process. For more information on the Cloud Foundation bring-up process, see Chapter 8 Initiate the Cloud Foundation Bring-Up Process.

Deploy VMware Cloud Builder Appliance

7

The VMware Cloud Builder appliance is a VM which also includes a service called the VMware Imaging Appliance service which can be utilized for installing the base ESXi operating system on your physical servers. After you image the servers, you use the Cloud Builder appliance to deploy and configure the management domain and transfer inventory and control to SDDC Manager. During the deployment process, the Cloud Builder appliance validates network information you provide in the deployment parameter workbook such as DNS, network (VLANS, IPs, MTUs), and credentials.

You must deploy the VMware Cloud Builder appliance on a suitable platform. This can be on a laptop running VMware Workstation or VMware Fusion, or on an ESXi host. The VMware Cloud Builder appliance must have network access to all hosts on the management network.

The procedure here describes deploying the VMware Cloud Builder appliance on an ESXi host. Other deployment methods have different procedures.

Prerequisites

The Cloud Builder appliance requires the following resources.

Component	Requirement
CPU	4 vCPUs
Memory	4 GB
Storage	150 GB

To automate the deployment, 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 on the Windows machine.
2. Log in to the vSphere Host Client.
3. In the navigator, select **Host**.
4. Click **Create/Register VM**.
5. On the Select creation type dialog box, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.

6 Enter a name for the VM.

7 Select **Click to select files or drag/drop**. Select the VMware Cloud Builder appliance OVA from your local file system and click **Open**.

8 Click **Next**.

9 On the Select Storage page, select the storage for the VMware Cloud Builder appliance.

10 On the License agreements dialog box, click **I agree** and then click **Next**.

11 On the Select networks dialog box, select the port group associated with the VLAN ID used by the ESXi hosts where Cloud Foundation will be deployed and then click **Next**.

12 On the Additional settings dialog box, expand **Application** and enter the following information for the VMware Cloud Builder appliance:

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.

Setting	Details
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.

13 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.

14 After the VMware Cloud Builder appliance is deployed, SSH in to the VM with the admin credentials provided in step 12.

15 Ensure that you can ping the ESXi hosts.

16 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.

Initiate the Cloud Foundation Bring-Up Process

8

The 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 Cloud Foundation software components are automatically deployed, configured, and licensed using the information provided. For Cloud Foundation 4.0.1, externalization of VMware vCenter server is automated.

Starting with Cloud Foundation 4.0.1, Cloud Foundation supports isolating system traffic (management, vSAN, and vMotion) from overlay traffic (Host, Edge, and Uplinks) across multiple physical NICs (pNICs) using two vSphere Distributed Switches. You can use the deployment parameter workbook to create up to two vSphere Distributed Switches (vDS) using up to six pNICs. For Cloud Foundation 4.0, you cannot use the deployment parameter sheet for bring-up of hosts with more than one vDS.

This chapter includes the following topics:

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 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 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 Cloud Builder appliance 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.

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.
- IP ranges, subnet mask, and a reliable L3 (default) gateway for each VLAN.
- 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.
- VLANs for management, vMotion, vSAN, NSX-T Host Overlay (Host TEP), NSX-T Edge Overlay (Edge TEP), and NSX uplink networks are created and tagged to all host ports. Each VLAN is 802.1q tagged. NSX-T Host Overlay (Host TEP) VLAN and NSX-T Edge Overlay (Host TEP) VLAN are routed to each other.
- DHCP with an appropriate scope size (one IP per physical NIC per host) is configured for the NSX Host Overlay (Host TEP) VLAN.

- 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.

Servers must be racked and cabled. ESXi version as mentioned in the *VMware Cloud Foundation Release Notes* must be installed on each host.

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

Physical Hardware and ESXi Hosts

- Physical hardware health status is "healthy" without any errors.
- The ESXi version on each host matches the build listed in the Cloud Foundation Bill of Materials (BOM). See the *VMware Cloud Foundation Release Notes* for the BOM.
- All hosts are configured and in synchronization with a central time server (NTP). NTP service policy set to `Start and stop with host`.
- Each ESXi host is running a non-expired license. The bring-up process will configure the permanent license.

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.

The required license keys are:

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

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 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 8-1. Password Complexity

Password	Complexity
VxRail Manager root account	This is the password for the VxRail Manager root account.
VxRail Manager mystic account	This is the password for the VxRail Manager mystic account.
ESXi Host root account	This is the password which you configured on the hosts during ESXi installation.
Default Single-Sign on domain administrator user	SSO
vCenter Server virtual appliance root account	Standard
NSX-T virtual appliance root account	NSX-T
NSX-T user interface and default CLI admin account	NSX-T
NSX-T audit CLI account	NSX-T
SDDC Manager	
SDDC Manager appliance root account	SSO
SDDC Manager super user	SSO
SDDC Manager REST API user	SSO

Table 8-2. Password Requirements based on Complexity

Password Type	Requirements Based on Complexity
Standard	1 Length 8-12 characters 2 Must include: ■ mix of upper-case and lower-case letters ■ a number ■ a special character such as @ ! # $ % ^ or ? 3 Cannot include: * { } [ ] ( ) / \ ' " ` ~ , ; : . < >
SSO (accounts in SSO vsphere.local)	1 Length 8-20 characters 2 Must include: ■ mix of upper-case and lower-case letters ■ a number ■ a special character
NSX-T	1 At least 12 characters 2 Must include: ■ mix of upper-case and lower-case letters ■ a number ■ a special character ■ at least five different characters

Hosts and Networks Tab

In this tab, enter details of your existing networking infrastructure. This information is configured on the appropriate 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 8-3. 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. **Note** Enter 0 if you have imaged the servers with VIA. VLAN 0 means that the management network is untagged.	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 VXLAN network. The VLAN ID can be between 0 and 4094.	N/A	N/A	N/A	Enter the MTU for the VXLAN network. The MTU can be between 1500 and 9000.
Enter VLAN ID for the NSX-T host overlay network. The VLAN ID can be between 0 and 4094.	N/A	N/A	N/A	Enter the MTU for the NSX-T host overlay network. The MTU can be between 1500 and 9000.
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 8-3. 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 1500 and 9000.

Management Domain ESXi Hosts

Enter the IP addresses of the ESXi hosts for the management domain. In a standard deployment, only four hosts are required in the management domain. 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 might be required to provide the capacity needed. In this section, only enter values for the number of hosts desired in the management domain.

Table 8-4. Input Required

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

Virtual Networking (Cloud Foundation 4.0.1 only)

In Cloud Foundation 4.0.1, you can use five vSphere Distributed Switch profiles to perform bring-up of hosts with two or four 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.

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). **Note** The primary vDS is created during the VxRail first run process. Ensure that the details provided here match with the vDS created.
Primary vSphere Distributed Switch - pNICs	Select the physical NICs to be assigned 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). You can modify the portgroup names of the management domain networks to make it clear which vDS each network uses. **Note** If you are not creating a secondary vDS, enter **`n/a`**.
Secondary vSphere Distributed Switch - pNICs	Select the unused physical NICs to be assigned 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 Cloud Foundation SDDC. External NTP sources are also utilized to synchronize the time between the software components.

Table 8-5. 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 8-6. DNS Zone

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

Table 8-7. CEIP

Parameter	Value
Enable Customer Experience Improvement Program (“CEIP”)	Select an option to turn CEIP on or off 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 8-8. 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 8-9. 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.

In the Virtual Networking - ESXi Hosts section below, the default settings are appropriate for hosts with two physical NICs (pNICs). To perform bring-up with hosts with more than two pNICs with Cloud Foundation 4.0, use the VMware Cloud Foundation API. To perform bring-up with hosts with more than two pNICs with Cloud Foundation 4.0.1, see Hosts and Networks Tab.

Table 8-10. Virtual Networking - ESXi Hosts (Cloud Foundation 4.0 only)

Parameter	Value
vmnic Allocated to vSS - Management	Select the physical NIC to assign to the management vSS.
Physical NIC to Assign to vDS - Management	Select the physical NIC to assign to the management vDS.
vSphere Distributed Switch Name	Enter a name for the management vSphere distributed switch.
vSphere Distributed Switch MTU Size	Enter the MTU size. Default value is 9000.

For Cloud Foundation 4.0, specify the names for vSphere resource pools. For Cloud Foundation 4.0.1, 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 8-11. 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 8-12. vSphere Datastore

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

Table 8-13. First Region Configuration Details

Parameter	Value
Join Existing Single-Sign-On Domain	■ Select No if you are deploying the first Cloud Foundation instance. ■ Select Yes if you are deploying the second Cloud Foundation instance. Then complete the remaining values in this section.
vCenter Server IP Address	Enter the IP address of the vCenter Server of the first instance.
vCenter Server SSO Username	Enter the user name for the vCenter Server of the first instance.
vCenter Server SSO Password	Enter the password for the vCenter Server of the first instance.

Deploy Parameters Tab: NSX-T Data Center

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

Table 8-14. 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, 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. Disconnect AVNs if you want to deploy vRealize Suite components to VLAN-backed networks.

Use the deployment parameter sheet to provide the information to create two AVNs; Region A and xRegion.

AVN	vRealize Component
Region A	vRealize Log Insight
Region A	vRealize Automation Proxy Agents
xRegion	vRealize Operations Manager
xRegion	vRealize Automation
xRegion	vRealize Suite Lifecycle Manager

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 8-15. 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 8-16. 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.

Table 8-16. North-South Routing Edge Node 1 (continued)

Parameter	Value
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 8-17. 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 8-18. 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.

Table 8-18. Top of Rack Switches for BGP Peering (continued)

Parameter	Value
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 8-19. 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 8-1. NSX-T Data Center Deployment Parameters

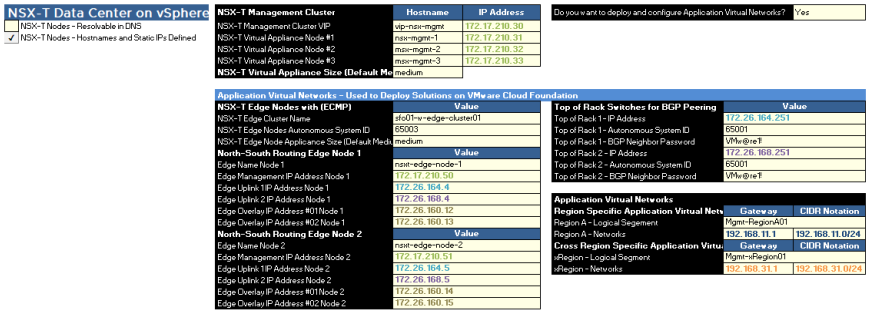
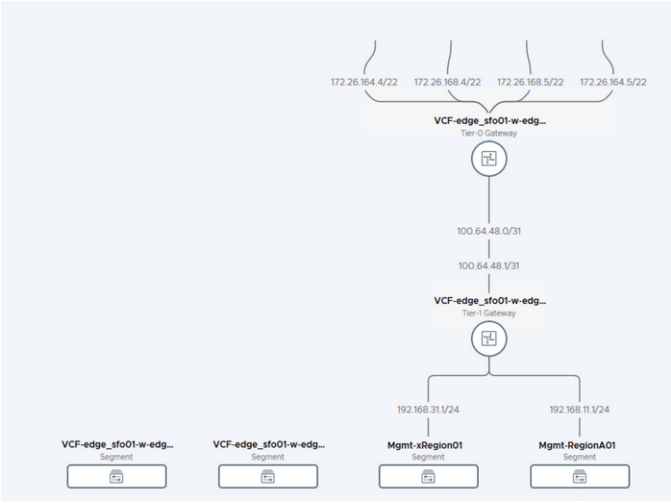


Figure 8-2. Post-Deployment Network Topology Viewed in NSX Manager



Deploy Parameters Tab: SDDC Manager

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

Table 8-20. 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 Cloud Builder appliance.
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.
Network Pool Name	Enter the network pool name for the management domain network pool.
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 Complete Deployment

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 "Troubleshooting Cloud Foundation Deployment" in the *VMware Cloud Foundation Deployment Guide* 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.

Manage Certificates

9

You can change the certificates of all VxRail Manager instances as well as the certificates for all Cloud Foundation components through SDDC Manager. See Managing Certificates for Cloud Foundation Components in *VMware Cloud Foundation Operations and Administration Guide*.

Managing Users and Groups

10

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 on Dell EMC system. See Managing Users and Groups in *VMware Cloud Foundation Operations and Administration Guide*.

Manage Passwords

11

You specify the passwords for your 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 for Managed Entities

As a security measure, you can rotate passwords for the logical and physical entities 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 entities.

- VxRail Manager
- ESXi
- vCenter Server

  By default, the vCenter Server root password expires after 90 days.
- PSC SSO
- NSX-T Edge
- NSX Manager
- vRealize Suite Lifecycle Manager

- SDDC Manager **backup** user

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 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, choose **Administration > Security > Password Management > Locally Managed**.

   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 the icon next to **User Name** and enter **admin** to display only domains with that user name value.
2. Select the component type for which you want to rotate passwords from the **Component** drop-down menu. For example, **ESXI**.
3. Select one or more components 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. Click on the task name to view sub-tasks. As each of these tasks are 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 domain account. Unlike password rotation, which generates a randomized password, you provide the new password.

You can modify only one password at a time.

Prerequisites

- Verify that there are no currently failed workflows in your 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. See Managing Users and Groups in the *VMware Cloud Foundation Operations and Administration Guide*.

Procedure

1. From the navigation pane, choose **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 update and click **Update** at the top of the page.

   Note If you select more than one domain, the **Update** button is unavailable (dimmed).

   The Update Password dialog box appears. This dialog box also displays the entity name, credential type, and user name, in case you need to confirm you have selected the correct domain.

3. Enter and confirm the new password.

   If the passwords, do not match, the dialog 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. Click on the task name to view sub-tasks.

   If the Tasks panel shows the task as having failed, click **Retry**.

Results

Password update 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 log in to the SDDC Manager VM using the root account credentials.

Prerequisites

Only a user with the ADMIN role can perform this task.

Procedure

1 SSH in to the SDDC Manager VM using the **vcf** user account.

2 (Optional) Change to the `/usr/bin` directory.

> **Note** Although the password management CLI commands are located in `/usr/bin`, you can run them from any directory.

3 Obtain the account credentials list by typing the command:

```
lookup_passwords
```

You will be required to enter the user name and the password for a user with the ADMIN role.

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 components 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.

About VI Workload Domains

12

In the VI Configuration wizard, you specify the storage, 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 additional 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 additional isolation as needed.
- Connects the specified ESXi servers to this vCenter Server instance and groups them into a cluster. Each host is configured with the port groups applicable for the workload domain.
- Configures networking on each host.
- 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 bringup with application virtual networks (AVNs), 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. Add one or more Edge clusters to a workload domain to provide north-south routing and network services.
- NSX Managers deployed as part of a VI workload domain are configured to periodically get backed up to an SFTP server. 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" in the *VMware Cloud Foundation Operations and Administration Guide*. 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 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, while creating a new workload domain, you cannot add a cluster to any other workload domain.

This chapter includes the following topics:

Prerequisites for a VI Workload Domain

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

- 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.
- A minimum of three hosts must be available for the cluster to be created during the VxRail first run.
- Decide on a name for your VI workload domain. Each VI workload domain must have a unique name. It is good practice to include region and site information in the name because resource object names (such as host and vCenter names) are generated based on the VI workload domain name. The name can be three to 20 characters long and can contain any combination of the following:
  - Lowercase alphabetic characters
  - Uppercase alphabetic characters
  - Numbers

  Note Spaces are not allowed in any of the names you specify when creating a VI workload domain.
- Decide on the following passwords - refer to the appropriate table for the Cloud Foundation version in your environment.
  - vCenter root password
  - NSX-T Manager admin password
- Update the management domain before you deploy `WLD`. To check the management domain Bill of Materials (BOM), see *VMware Cloud Foundation on Dell EMC VxRail Release Notes*. If the management domain BOM does not match, connect to the LCM depot, download, and apply the upgrade patches.

- Table 12-1. Passwords for Cloud Foundation

Account	Password Requirements
vCenter root	1 Length 8-20 characters 2 Must include: ■ mix of upper-case and lower-case letters ■ a number ■ a special character
NSX-T Manager admin	1 Minimum length 12 characters 2 Must include: ■ at least one lowercase and one uppercase letter ■ a number ■ a special character ■ exclude_char such as { } [ ] ( ) / \ ' " ` ~ , ; : . < > ■ at least five different characters 3 Must not include: ■ a dictionary word ■ a palindrome ■ more than four monotonic character sequences

- Gather the information that you need for the workload domain creation workflow.

  Table 12-2. 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

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

Start the VI Configuration Wizard

Procedure

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

Specify Name

Provide a name for the VxRail VI workload domain and organization.

Procedure

1 Type a name for the 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.

2 Type a name for the organization that requested or will use the virtual infrastructure, such as **`Finance`**. The name must contain between 3 and 20 characters.

3 Click **Next**.

Specify Compute Details

Specify the compute (vCenter) details for this workload domain.

Procedure

1 On the Compute page of the wizard, enter the vCenter IP address and DNS name.

Note Before updating the IP address in the wizard, ensure that you have reserved the IP addresses in the DNS.

2 Type the vCenter subnet mask and default gateway.

3 Type and re-type the vCenter Root password.

4 Click **Next**.

Review the Details

At the review step of the wizard, review the information about the workload domain and start the creation workflow. You can also print the information or download a printable version to print later.

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

Procedure

1 Scroll down the page to review the information.

2 Click **Finish** to begin the creation process.

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

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

Results

The status will be activating until we add the primary cluster in to domain. When the VxRail VI workload domain is created, it is added to the workload domains table along with the already listed management domain.

The OEM license is assigned by default to the workload domains.

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 The **Add VxRail Cluster to Workload Domain** page appears.

5 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**.

6 The **Hosts** page displays a list of the discovered hosts for that cluster. Update the SSH password for the discovered hosts for that cluster. Click the icon next to the name of the host to get more information about it. Click **Next**.

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

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. Skip to step e.

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

   d 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

   e Click **Next**.

Deploy NSX-T Edge Cluster on VxRail

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

See Deploying NSX-T Edge Clusters in the *VMware Cloud Foundation Operations and Administration Guide*.

Expand a Workload Domain 13

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.

This chapter includes the following topics:

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 The **Add VxRail Cluster to Workload Domain** page appears.

5 On the **VxRail Manager** page, the VxRail cluster in the vCenter is discovered. Click **Next**.

6 The **Hosts** page displays a list of the discovered hosts for that cluster. Update the SSH password for the discovered hosts for that cluster. Click the icon next to the name of the host to get more information about it. Click **Next**.

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

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. Skip to step e.

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

   d 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

   e Click **Next**.

9 Select the pNICs to use for the NSX-T Virtual Distributed Switch (N-VDS).

   You can select the pNICS based on the same network speed and the available status. Heterogeneous selection on the pNIC pair is not permitted. All the available pNICs are displayed in the list. Select any two of them from the list and click **Next**.

   Note If there are fewer than two pNICS available, an error message is shown and **Next** is unavailable (dimmed).

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

11 Review the details. Click **Finish**. The process of adding the VxRail cluster 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 **Add VxRail hosts** option in the vCenter plug in of VxRail.

   a Go to the vCenter for VxRail.

   b Click on that particular cluster. You can view the configuration.

   c Under the **Configure** tab, the Add VxRail Hosts page shows the list of the discovered hosts.

   d Click **Add** to trigger the addition of hosts to that particular cluster.

   e Provide the user credentials. Click **Next**.

   f Review the Host IP address details. Click **Next**.

   g Provide the ESXi credentials. Click **Next**.

   h (Optional Step) If required, you can select the **Maintenance mode**. Click **Next**.

   i Click **Validate**.

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.

Procedure

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

   The **Workload Domains** page displays information for all workload domains.

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

   The detail page for the selected workload domain appears.

3 Click the **Clusters** tab.

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

5 The details page for that particular cluster appears.

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

   The **Add Host To VxRail Cluster** wizard appears.

7 You can see the list of the discovered hosts. Click **Add**.

8 Under the **tasks** tab in the **cluster details** page, you can see the status of the add host task. Wait until the action is complete before performing additional workload domain tasks.

Cluster Spanning for VMware Cloud Foundation on VxRail

From Release 3.9 onwards, VMware Cloud Foundation on VxRail allows you to expand a cluster with the hosts residing in multiple L2 network domains (different VLANs and subnets).

For information on expanding a cluster that needs cluster spanning, follow the steps in the VxRail documentation. For information on adding hosts, see Add the VxRail Hosts to the Cluster in VMware Cloud Foundation.

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 for NSX-T VTEPS.
- 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. When prompted, select a workload domain to which you want to import the cluster.
5. Select a cluster from the list of clusters that are ready to be imported.
6. Enter passwords for the discovered hosts.
   - Enter a single password for all the discovered hosts.
   - Enter passwords individually for each discovered host depending upon the password setup for the hosts.

7 Create a vDS.
   a Select the command for the creation of a new vDS.
   b Enter the name of the vDS.
   c Enter a comma-separated list of at least two physical NICs.
8 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)
9 When prompted, enter the following credentials:
   a VxRail Manager root password
   b VxRail Manager admin user name and password
10 Select the license keys for NSX-T Data Center and VMware vSAN.
11 When prompted, allow the validation process to start.

Results

If the validation is successful, the workflow to add the VxRail cluster to SDDC Manager is triggered. The progress of the cluster workflow is displayed in the SDDC Manager task panel. If the validation fails, resolve the problems and repeat the process again to add a cluster with a new NSX-T cluster and vDS.

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 the host configuration has a minimum of two active and unused vmnics.
- Configure a DHCP server for NSX-T VTEPS.
- Download the `.zip` file from https://code.vmware.com/samples?id=7390. 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. 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. When prompted, select a workload domain to which you want to import the cluster.
5. Select a cluster from the list of clusters that are ready to be imported.
6. Enter passwords for the discovered hosts.
   - Enter a single password for all the discovered hosts.
   - Enter passwords individually for each discovered host depending upon the password setup for the hosts.
7. Create a vDS.
   a. Select the command for the creation of a new vDS.
   b. Enter the name of the vDS.
   c. Enter a comma-separated list of at least two physical NICs.
8. 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.
9. When prompted, enter the following credentials:
   a. VxRail Manager root password
   b. VxRail Manager admin user name and password
10. Select the license keys for NSX-T data center and VMware vSAN.
11. When prompted, allow the validation process to start.

Results

If the validation is successful, the workflow to add the VxRail cluster to SDDC Manager is triggered. The progress of the cluster workflow is displayed in the SDDC Manager task panel. If the validation fails, resolve the problems and repeat the process again to add a cluster with a new NSX-T cluster and vDS.

Reduce a Workload Domain

14

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

The two tasks involved in removing a host are:

- Remove the host from the VMware Cloud Foundation domain.
- Remove the host from the vCenter plug-in of VxRail.

This chapter includes the following topics:

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 the SDDC Manager Dashboard.

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.

Procedure

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

   The Workload Domains page displays information for all workload domains.
2. In the workload domains table, click the name of the workload domain that you want to modify.

   The detail page for the selected workload domain appears.
3. Click the **Clusters** tab.
4. Click the name of the cluster from which you want to remove a host.
5. Click the **Hosts** tab.
6. Select the host to remove and click **Remove Selected Hosts**.

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.

Remove Host using the vCenter for VxRail

Once you remove the VxRail host in VMware Cloud Foundation domain, it is moved to the Maintenance mode in the vCenter for VxRail.

Perform the following tasks in the vCenter for VxRail:

Procedure

1 Right click the particular cluster and select **VxRail** -> **Remove VxRail Host**.

2 Provide the credentials. Click **Apply** to remove the host.

Delete a VxRail Cluster

You can delete a VxRail cluster from a workload domain.

You cannot delete the last cluster in a workload domain. Delete the workload domain.

You cannot delete the cluster that you specified when creating the workload domain. This is considered the primary cluster and the only way to delete it is to delete all of clusters in the workload domain and then delete the workload domain.

Prerequisites

Migrate or backup the VMs and data on the data store associated with the cluster to another location.

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.

Delete a Workload Domain

15

When you delete a workload domain, the clusters within that workload domain are deleted. Note that a workload domain that includes an Edge cluster deployed 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

- Back up the data on the workload domain.
- Migrate the VMs that you want to keep to another workload domain.
- Shut down all VMs other than the VxRail Manager VM.

Procedure

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

   The Workload Domains page displays information for all workload domains.

2. Hover your mouse in the workload domain row that where you want to delete.

   When you select the workload domain, three vertical dots appear next to the name.

3. Click the dots and choose **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.

4. Click **Delete Domain** to proceed.

   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.

Working with Workload Management

16

With Workload Management, you can deploy and operate the compute, networking, and storage infrastructure for vSphere with Kubernetes. vSphere with Kubernetes transforms vSphere to a platform for running Kubernetes workloads natively on the hypervisor layer. When enabled on a vSphere cluster, vSphere with Kubernetes provides the capability to run Kubernetes workloads directly on ESXi hosts and to create upstream Kubernetes clusters within dedicated resource pools.

See Working with Workload Management in the *VMware Cloud Foundation Operations and Administration Guide*.

Managing Multiple Cloud Foundation Instances

17

With VMware Cloud Foundation on Dell VMC VxRail, you can manage multiple Cloud Foundation instances from a single console.

For information on using this feature, see Managing Multiple Cloud Foundation Instances in the *VMware Cloud Foundation Operations and Administration Guide*.

Deploy vRealize Suite Lifecycle Manager

18

You must deploy vRealize Suite Lifecycle Manager before deploying a vRealize Suite product. See Deploy vRealize Suite Lifecycle Manager in Cloud Foundation in the *VMware Cloud Foundation Operations and Administration Guide*.

Stretching Clusters

19

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.

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.

Table 19-1. 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
NSX-T Edge Overlay	✓	✓	2713 (Stretched)	172.27.13.0/24	✓	9000
vSphere vMotion	X	✓	1622	172.16.22.0/24	✓	9000

Table 19-1. 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
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 19-2. Workload Domain VLAN and IP Subnet Requirements

Function	Availability Zone 1	Availability Zone 2	VLAN ID	IP Range	HA Layer 3 Gateway
Management (AZ1)	✓	X	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	✓
Management (AZ2)	X	✓	2731	172.27.31.0/24	✓
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 19-3. 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 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.
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, trafficflows 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.

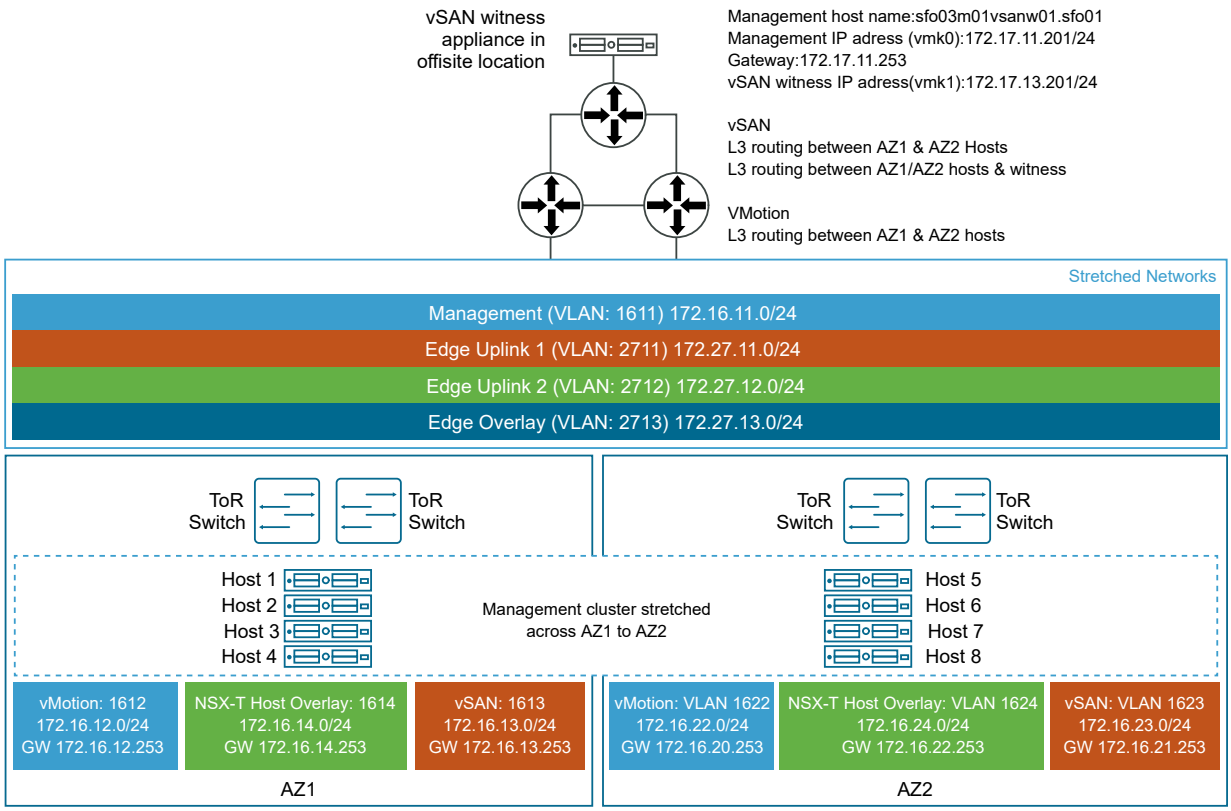
This example use case has two availability zones in two buildings in an office campus - AZ1 and AZ2. Each availability zone has its own power supply and network. The management domain is on AZ1 and contains the default cluster, SDDC-Cluster1. This cluster contains four ESXi hosts.

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 Cloud Foundation inventory yet.

We will stretch the default cluster `SDDC-Cluster1` in the management domain from AZ1 to AZ2.

Figure 19-1. Stretch Cluster Example



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

Prerequisites

- You must have deployed and configured a vSAN witness host. See Deploy and Configure 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 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.

Procedure

1. Using an SSH File Transfer tool, copy `initiate_stretch_cluster_vxrail.py` to the `/home/vcf/` directory on the SDDC Manager VM.
2. Using SSH, log in to the SDDC Manager VM 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
- ESXi host IP addresses and passwords
- 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 preferred site overlay VLAN

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 On the SDDC Manager Dashboard, 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 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.

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.
- ESXi host IP addresses, passwords, and fault domain information.
- vSAN gateway IP for the preferred (primary) and non-preferred (secondary) site.
- vSAN CIDR for the preferred (primary) and non-preferred (secondary) site.

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.

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.

Lifecycle Management 20

Lifecycle Management (LCM) enables you to perform automated updates on 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.

For more information on VMware Cloud Foundation Lifecycle Management, see Patching and Upgrading Cloud Foundation. For information on upgrading VMware Cloud Foundation, see *VMware Cloud Foundation Upgrade Guide.*.

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 Update Bundles

Download the update bundles for your environment.

Online Bundle Download

You must log in to My VMware account before downloading a bundle.

You must be logged in to My VMware account to download update bundles.

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

2 Enter the My VMware credentials as well as the Dell EMC credentials. Click **Authenticate**. You have to log into both My VMware and Dell EMC to update all the VMware Cloud Foundation and the VxRail components.

3 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 **Repository > Bundles**.
- 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.

4 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.
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.

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

Use a Proxy Server to Download Upgrade Bundles

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 VM 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.

Support for the Manual Download of Bundles for VMware Cloud Foundation

LCM polls the VMware depot to access the update bundles. If you do not have internet connectivity in your Cloud Foundation system, you can use the Bundle Transfer utility to manually the bundles from the depot on your local computer and then upload them to SDDC Manager. The utility identifies applicable bundles based on the current software versions in your environment based on a marker file generated on the SDDC Manager VM.

Prerequisites

A Windows or Linux computer with Java 8 or later and internet connectivity for downloading the bundles.

Procedure

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

2 Navigate to the `/opt/vmware/vcf/lcm/lcm-tools/bin` directory.

3 Generate a marker file by running the following command.

```
./lcm-bundle-transfer-util --generateMarker
```

The marker file (`markerFile`) is a JSON file that contains information on the current software versions running on SDDC Manager. It also contains the bundles IDs for bundles that were downloaded before this file was generated. The `markerFile.md5` contains the checksum for the `markerFile`.

The output contains the directory where the marker file is generated.

4 Copy the `/opt/vmware/vcf/lcm/lcm-tools/bin` directory, and the `markerFile` and `markerFile.md5` files from the location displayed in the output of step 3 to a computer with internet access.

The `/opt/vmware/vcf/lcm/lcm-tools/bin` directory includes the bundle transfer utility required for the next step.

5 For the VxRail SKU, when you download the NSX or vCenter bundles, provide the additional argument of `withCompatibilitySets` which will let you download the compatibility sets along with the bundles. On the computer with internet access, run the following command.

```
./lcm-bundle-transfer-util -download "withCompatibilitySets"
             -outputDirectory ${absolute-path-output-dir}
             -depotUser ${depotUser}
             -markerFile ${absolute-path-markerFile}
             -markerMd5File ${absolute-path-markerFile.md5}
```

where

absolute-path-output-dir	Path to the directory where the bundle files are to 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	User name for myVMware depot. You are prompted to enter the depot user password. If there are any special characters in the password, specify the password within single quotes.
markerFile	Absolute path to the marker file, as generated in the above step. If you do not specify the path to the marker file, all update bundles on the depot are downloaded.
markerMd5File	Absolute path to the marker MD5 checksum file, as generated in the above step.

The utility generates a delta file (`deltaFileDownloaded`) in the download directory based on the software versions in the marker file and the update bundles available on the depot. The applicable bundles identified in the delta file are downloaded. Download progress for each bundle is displayed.

6 When you download the VxRail bundles, provide the additional argument `downloadPartnerBundle`.

```
./lcm-bundle-transfer-util -download "downloadPartnerBundle"
             -outputDirectory ${absolute-path-output-dir}
             -depotUser ${vmwaredepotUser}
    -depotUserPassword ${vmwareDepotPassword}
    -pdu ${emcdepotuser}:${emcdepotpassword}
             -markerFile ${absolute-path-markerFile}
             -markerMd5File ${absolute-path-markerFile.md5}
```

7 Copy the downloaded `softwareCompatibilitySets.json` to `/nfs/vmware/vcf/nfs-mount/bundle/depot/local/softwareCompatibilitySets.json`.

8 Copy the update bundle directory from the external computer to the SDDC Manager VM.

For example:

```
scp -pr /Work/UpdateBundle vcf@SDDC_IP:/home/vcf/vCF372to38Bundle"
```

9 In the SDDC Manager VM, change the ownership and permissions of the uploaded bundle.

```
chown vcf_lcm:vcf -R /opt/vmware/vcf/vCF372to38Bundle
chmod -R 0777 /opt/vmware/vcf/vCF372to38Bundle
```

10 In the SDDC Manager VM, upload the bundle files to the internal LCM repository.

```
cd /opt/vmware/vcf/lcm/lcm-tools/bin
./lcm-bundle-transfer-util -upload "withCompatibilitySets" -bundleDirectory
${absolute-path-output-dir}
```

where *absolute-path-output-dir* is the directory where the bundle files have been be uploaded, or `/opt/vmware/vcf/vCF372to38Bundle` as shown in the previous step.

The utility uploads the bundles specified in the `deltaFileDownloaded` file. The console displays upload status for each bundle.

11 For the VxRail bundles, perform the following:

a Copy the partner bundle to `/nfs/vmware/vcf/nfs-mount/bundle/depot/local/bundles`.

b Copy `partnerBundleMetadata.json` to `/nfs/vmware/vcf/nfs-mount/bundle/depot/local/partnerBundleMetadata.json`.

c Copy `softwareCompatibilitySets.json` to `/nfs/vmware/vcf/nfs-mount/bundle/depot/local/softwareCompatibilitySets.json`

d In the SDDC Manager VM, upload the bundle files to the internal LCM repository.

```
cd /opt/vmware/vcf/lcm/lcm-tools/bin
./lcm-bundle-transfer-util -upload "uploadPartnerBundle" -bundleDirectory
${absolute-path-output-dir}
```

Update your Environment

The SDDC Manager is the first component to be upgraded on the management domain.

Components must be updated in the following order:

1 Cloud Foundation services

2 NSX-T

3 vCenter Server

4 VxRail

5 ESXi

If you have multiple clusters in the management domain or in a workload domain, you can upgrade VxRail at a cluster level.

Procedure

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

2 Click a domain and then click the **Updates/Patches** tab.

3 Click **Precheck** to validate that the appliance 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.

4 Do either of the following:

a Click **Update Now**.

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

To view the update status, click **Update History** > **Actions** >**View Update Status**. After the bundle is downloaded, the **Schedule Update** button is displayed. Click **View Details** to see the version changes for each component that the bundle will apply.

5 After the update is completed successfully, log out of the SDDC Manager Dashboard and log back in.

Update History

The **Update History** page displays all updates applied to a workload domain.

Procedure

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

2 Click the name of a workload domain and then click the **Updates History** tab.

All updates applied to this workload domain are displayed. If an update bundle was applied more than once, click **View Past Attempts** to see more information.

Upgrade VxRail by Cluster

If you have multiple clusters in the management domain or in a workload domain, you can upgrade VxRail at a cluster level.

Prerequisites

- Ensure that the domain for which you want to perform cluster-level upgrade does not have any hosts or clusters in an error state. Resolve the error state or remove the hosts and clusters with errors before proceeding.
- Download the ESXi update bundle.

Procedure

1 Navigate to the Updates/Patches tab of the appropriate domain.

2 Run the upgrade precheck.

If the clusters in your workload domain have different hardware, you can run a precheck at the cluster level using the `precheck` API. For information on this API, select **Developer Center** in the left panel on the SDDC Manager Dashboard and then search for `precheck` in the Overview tab.

3 The Available Updates section displays the bundle that you downloaded before starting the upgrade.

4 Click **View Details**,

The Resource Changes section displays the VxRail cluster in the workload domain that needs to be upgraded.

5 Click **Exit Details**.

6 Click **Update Now** or **Schedule Update** and select the date and time for the bundle to be applied.

7 Select **Enable Cluster-level selection** if you want to upgrade VxRail by cluster and then select the clusters that you want to upgrade.

8 Click **Next**.

9 If you had clicked Schedule Update, select the start date and time for the upgrade and then click **Next**.

10 On the Review page, click **Finish**.

The Cloud Foundation Update Status window displays 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.

Updating Cloud Foundation DNS and NTP Servers

21

If you need to make changes to the DNS or NTP server information that you provided during Cloud Foundation bring-up, you can use the VMware Cloud Foundation API to update the servers.

When you initially deploy Cloud Foundation, you complete the deployments parameter sheet 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.

See Updating Cloud Foundation DNS and NTP Servers in the *VMware Cloud Foundation Operations and Administration Guide*.

Note Updates apply to all Cloud Foundation components, excluding VxRail Manager.

Configuring Customer Experience Improvement Program

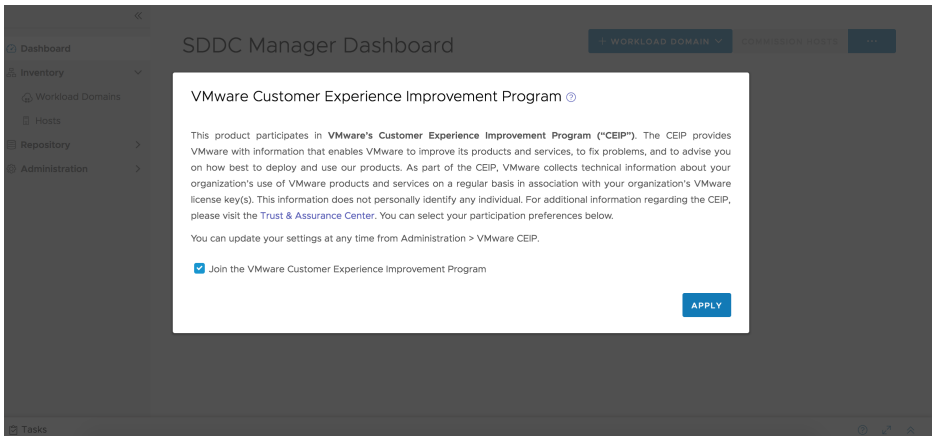
22

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.