

Administering VMware Cloud Foundation

VMware Cloud Foundation 2.3.1



vmware®

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

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

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Copyright © 2015, 2016, 2017, 2018 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

	About Administering VMware Cloud Foundation	6
1	Administering Cloud Foundation Systems	8
	VMware Software Components Deployed in a Typical Cloud Foundation System	9
	Web Interfaces Used When Administering Your Cloud Foundation System	9
2	Getting Started with SDDC Manager	11
	Log in to SDDC Manager	11
	Tour of the SDDC Manager User Interface	12
	Log out of SDDC Manager	17
3	Managing Certificates for Cloud Foundation Components	18
	Create Configuration File Package for the Certificate Generation Tool	20
	Generate Key Pairs and Certificates	22
	Build File Package for Certificate Replacement Tool	24
	Backup TrustStores	24
	Take Snapshots of Cloud Foundation Components	24
	Replace Certificates	25
	Re-trust VDI Workload Domains	25
	Verify that the System Works with the New Certificates	28
	Verify Trust for Replaced Certificates	28
	Delete Snapshots of Cloud Foundation Components	28
4	Changing the Passwords of Your Cloud Foundation System On Demand	30
	Rotate Passwords On-Demand for Managed Physical and Logical Entities	30
	Credentials for Logging in to the SDDC Manager VM	31
	Look Up Account Credentials	31
	Password Management CLI Command Reference	32
5	Backing up and Restoring a Cloud Foundation System	35
	Requirements	35
	Back Up Methods for Cloud Foundation Components	36
	Backup and Restore Considerations	37
	Backing Up and Restoring the SDDC Manager VM and SDDC Manager Utility VM	38
	Backing Up and Restoring the vCenter Server and Platform Services Controller VMs	39
	Backing Up vRealize Components	39
	Backing Up and Restoring NSX Manager	40
	Backing Up and Restoring Distributed Switches	43

- [Back Up Physical Switch Configurations](#) 43
- [Backing Up the Cloud Foundation Configuration](#) 45

6 Managing Users and Groups 51

- [Active Directory and the Cloud Foundation system](#) 51
- [Add Local Users and Groups](#) 56
- [Assign Permissions to Users and Groups](#) 57
- [Add System Administrators](#) 58
- [Role-Based Access Control](#) 59
- [User Passwords in Your Cloud Foundation System](#) 59

7 Managing Physical Resources 63

- [Host Details and Operations](#) 65
- [Adding and Replacing Hosts](#) 68
- [Switch Details and Operations](#) 88
- [Replacing and Restoring Switches](#) 88

8 Working with the Management Domain and Workload Domains 101

- [Creating and Provisioning Workload Domains](#) 103
- [Creating Workload Virtual Machines in the Management Domain](#) 132
- [Expanding the Management and Workload Domains](#) 133
- [Delete a Workload Domain](#) 136
- [Enabling vSAN Space Efficiency Features in All-Flash Systems](#) 137

9 Adding vRealize Components to Cloud Foundation 139

- [Deploy vRealize Automation in Cloud Foundation](#) 139
- [Working with vRealize Operations in Cloud Foundation](#) 148

10 Monitoring Capabilities in the Cloud Foundation System 151

- [Managing Workflows and Tasks](#) 153
- [Managing Alerts, Events, and Audit Events](#) 154
- [Using vRealize Log Insight Capabilities in Your Cloud Foundation System](#) 172

11 Settings Configuration Using SDDC Manager 178

- [Customize Default Values Used When Creating VDI Workload Domains](#) 178
- [Additional Rack Settings Screen](#) 182
- [Managing Network Settings](#) 182

12 License Management 187

- [Cloud Foundation Licensing Model](#) 187
- [Manage License Keys for the Software in Your Cloud Foundation System](#) 188
- [Enable vRealize Log Insight Logging for Workload Domains](#) 189

- 13 Supportability and Serviceability (SoS) Tool 190**
 - Calculate Configuration Changes in Your Cloud Foundation System 194
 - Collect Logs for Your Cloud Foundation System 195

- 14 Managing Shutdown and Startup of Cloud Foundation 205**
 - Shut Down a Cloud Foundation System 205
 - Start Up a Cloud Foundation System 209

- 15 Patching and Upgrading Cloud Foundation 213**
 - Prerequisites for Upgrading VMware Software 214
 - Update a Workload Domain 216
 - View Inventory Component Versions 229
 - Display Backup Locations 232
 - Upgrade Log File Locations 232
 - Upgrade Backup File Locations 233

- 16 Upgrade Cloud Foundation to 2.3.1 234**

- 17 Rack Wiring 235**
 - Rack Component Ports 239

- 18 Troubleshooting Cloud Foundation for Data Center System Administrators 243**
 - Unable to Browse to the Software Stack Web Interfaces Using their Fully Qualified Domain Names 243
 - Decommission Workflow Stops Responding at Task Named Enter Hosts Maintenance Mode 244
 - VDI Workload Creation Fails at the Import DHCP Relay Agents Task 245
 - Update Fails While Exiting Maintenance Mode 246
 - Restore ESXi Server After Update Failure 247

- 19 Cloud Foundation Glossary 249**

About Administering VMware Cloud Foundation

Administering VMware Cloud Foundation provides information about managing a VMware Cloud Foundation™ system, including managing the system's physical and virtual infrastructure, managing users, configuring and deploying service offerings, and upgrading and monitoring the system.

Intended Audience

The *Administering VMware Cloud Foundation* is intended for data center system administrators who manage their organization's Cloud Foundation system. The information in this guide 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 VMware software products, software components, and their features:

- VMware vSphere®
- VMware vCenter Server® and VMware vCenter Server® Appliance™
- VMware Platform Services Controller™
- VMware vRealize® Log Insight™
- VMware Horizon®
- VMware App Volumes™

Related Publications

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

About the Screen Shots Used in this Guide

The screen shots used in this guide typically show only that portion of the overall user interface screen that corresponds to the text at which point the screen shot appears, and not necessarily the full user interface.

Note Some screen shots are taken at a higher resolution than others, and might look grainy when the PDF is viewed at 100%. However, if you zoom to 200%, the image looks clear and readable.

Administering Cloud Foundation Systems

1

Cloud Foundation enables deployment of a private cloud based on VMware's software-defined data center (SDDC) architecture. A Cloud Foundation system is a turnkey private cloud instance that is easily deployed. In this environment, SDDC Manager enables the ability for streamlined and automated data center operations and the delivery of service offerings, such as virtual infrastructure (VI) and virtual desktop infrastructure (VDI) environments, based on a VMware SDDC architecture.

Virtual compute, storage, and networking capabilities are provided with corresponding management capabilities, and SDDC Manager makes those capabilities available as a single logical environment. This logical aggregation of the physical racks and their associated resources allows for easier management of all of the resources across the infrastructure and gives your organization the ability to rapidly provision virtual infrastructure environments and related services. When you provision VI or VDI workload domains, SDDC Manager configures the vRealize Log Insight instances for those environments, to provide real-time log analytics. Cloud Foundation systems can scale to meet the increasing demands on your data center.

See the *VMware Cloud Foundation Overview and Bring-Up Guide* for an in-depth introduction to the architecture, components, and physical topology of a Cloud Foundation system, along with detailed descriptions of the software that is deployed in the environment.

As an SDDC administrator, you use the information in the *Administering VMware Cloud Foundation* to understand how to administer and operate your installed Cloud Foundation system. An administrator of an Cloud Foundation system performs tasks such as:

- Manage users, roles, and permissions
- Manage physical and logical resources
- Configure and provision the systems, 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 Cloud Foundation software components

This chapter includes the following topics:

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

VMware Software Components Deployed in a Typical Cloud Foundation System

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

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

For the exact version numbers of the VMware products that you might see in your Cloud Foundation system after the initial bring-up process, see the *Release Notes* document for your Cloud Foundation version. If the system has been updated after the initial bring-up process using the Life Cycle Management features, see [View Inventory Component Versions](#) for details on how to view the versions of the VMware software components that are within your system.

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

You can find the documentation for the following VMware software products and components at docs.vmware.com:

- vSphere (vCenter Server, Platform Services Controller, and ESXi)
- vSAN
- NSX for vSphere
- vRealize Log Insight
- vRealize Operations
- vRealize Automation

Web Interfaces Used When Administering Your Cloud Foundation System

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

SDDC Manager does not mask the individual component management products. In addition to using the SDDC Manager Dashboard, for certain tasks, you also use the following user interfaces for administration tasks involving their associated VMware software components that are part of a VMware SDDC. All these interfaces run in a browser, and you can launch many of them from locations within the SDDC Manager Dashboard.

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

VMware SDDC Web Interfaces	Description	Launch Link Location in SDDC Manager Dashboard
vSphere Web interface	This interface provides direct management of resources managed by the vCenter Server instances, for identity management, and for management of the NSX resources that provide the software-defined networking capabilities of the SDDC. You can also manage object level storage policies for distributed software-defined storage provided by vSAN.	The General Info screen of the Domain Details page for management and workload domains has a launch link labeled vCenter .
vRealize Log Insight Web interface	When the vRealize Log Insight instance is licensed for use in the system, this interface provides direct access to the logs and event data collected and aggregated in vRealize Log Insight for troubleshooting, trend analysis, and reporting.	The Management Info screen of the Domain Details page for management domains has launch links labeled Log Insight , for the IP and virtual IP instances. The Analysis links in the Events and Audit Events listings also opens the vRealize Log Insight Web interface.

Launch links are not provided in SDDC Manager for those VDI-related interfaces. To use those interfaces, use the **vCenter** launch link on the VDI workload domain's details screen to open the vSphere Web Client and locate the appropriate virtual machine and its DNS name. A virtual machine's DNS name is typically displayed on the virtual machine's **Summary** tab in the vSphere Web Client. After locating the DNS name for the virtual machine, open a browser tab and point it to:

- <https://View-Server-VM-DNS-name/admin>, for the View Administrator Web interface, where View-Server-VM-DNS-name is the View Connection Server VM's DNS name.
- <https://App-Volumes-VM-DNS-name>, for the App Volumes Manager Console, where App-Volumes-VM-DNS-name is the App Volumes Manager VM's DNS name.

Getting Started with SDDC Manager

2

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

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

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

This chapter includes the following topics:

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

Log in to SDDC Manager

You access SDDC Manager using a supported browser.

Prerequisites

Verify that you have the following information:

- A user name and password for an account that is configured for accessing SDDC Manager. Your system uses role-based access control (RBAC) to determine what operations a user can perform, including logging in. For details about SDDC Manager and RBAC, see [Role-Based Access Control](#).

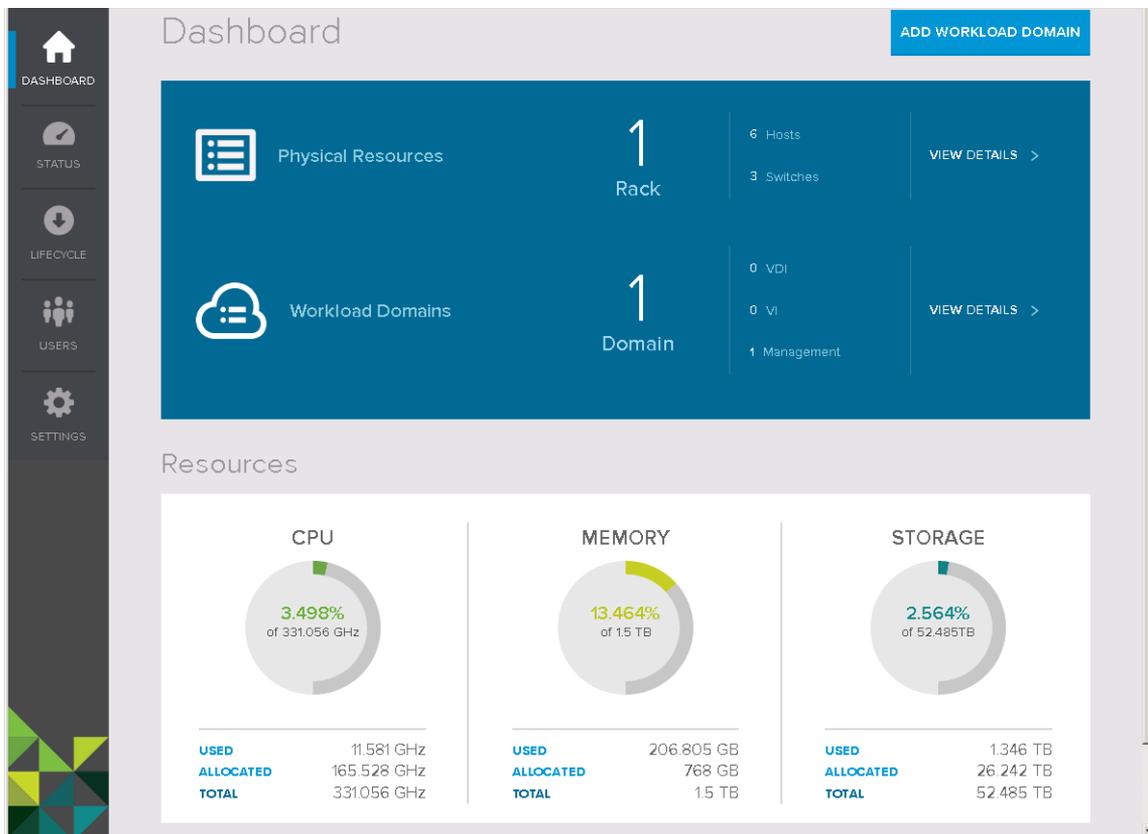
During the Cloud Foundation bring-up process, a name and password are entered to create a superuser account. If this is the first time you are logging in after running the bring-up process, you can use those superuser account credentials to log in and then authorize other users for access. The superuser account's domain is the SSO domain that was entered during the bring-up process, for example `vsphere.local`, and you log in using the form `superuser-name@domain` and the superuser password.

- The Fully Qualified Domain Name (FQDN) for the SDDC Manager IP address. This name typically has a form like `vcf.sddc.example.com`, where `sddc.example.com` is the value that was specified for the subdomain in the bring-up process wizard. During the bring-up process on the first rack in a Cloud Foundation system, this FQDN is created and an IP address is assigned. See the *VMware Cloud Foundation Overview and Bring-Up Guide* for details about the assigned IP address.

Procedure

- In a browser, open the login screen by navigating to `https://VIP-FQDN:8443/vrm-ui`
 For example, point your browser to `https://vrm.sddc.example.com:8443/vrm-ui`
- Log in using the user name and password for an account that is configured for access.

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



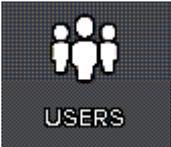
Tour of the SDDC Manager User Interface

SDDC Manager provides the user interface for your single point of control for managing and monitoring your Cloud Foundation system and for provisioning virtual environments.

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

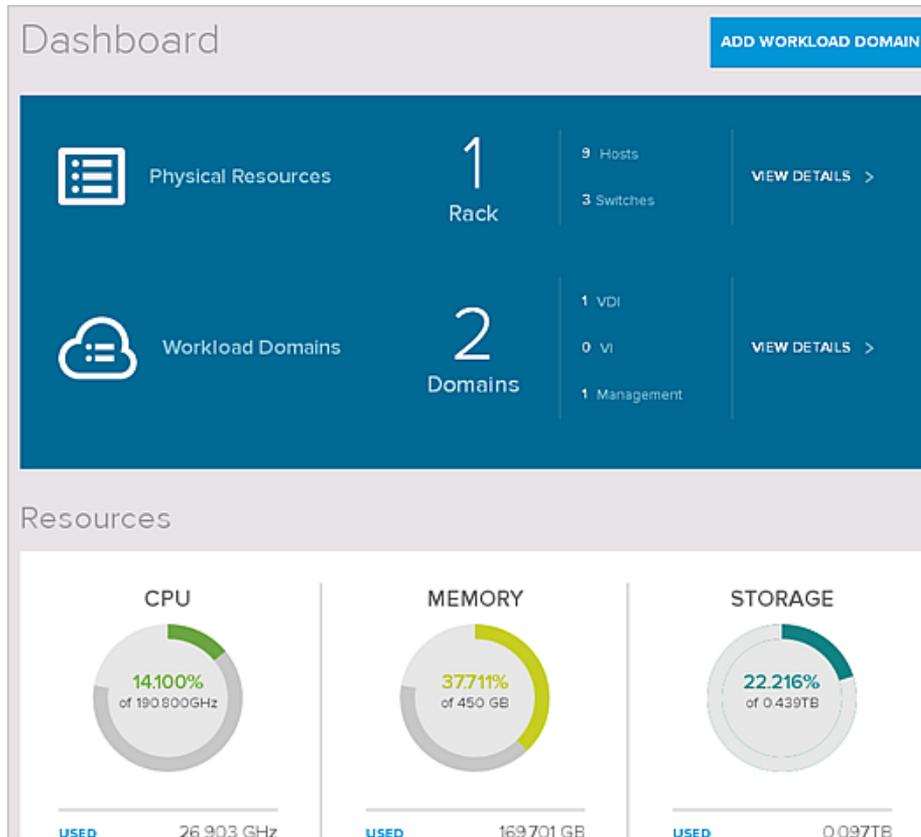
Navigation Bar

On the left side of the interface is the Navigation bar. The Navigation bar provides icons for navigating to the corresponding pages.

Navigation Bar Icon	Label	Functional Area
	Dashboard	Dashboard
	Status	System status
	Lifecycle	Life cycle management
	Users	User management
	Settings	System settings

Dashboard

The Dashboard page is the home page that provides the overall administrative view of your Cloud Foundation system. The Dashboard page provides a top-level view of the physical and logical resources across all of the physical racks in the system, including available CPU, memory, and storage capacity. From this page, you can start the process of creating a workload domain.

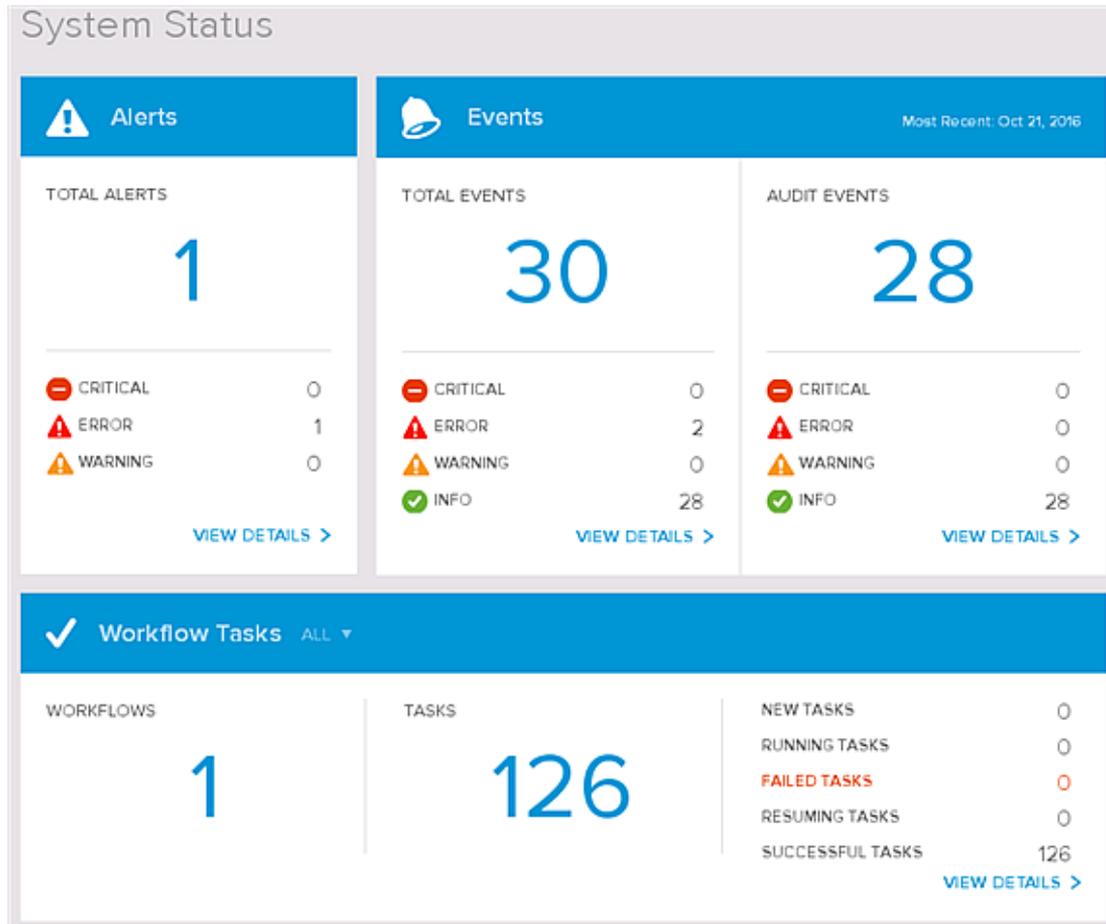


You use the links on the dashboard to drill-down and examine details about the physical resources and the virtual environments that are provisioned for the management and workload domains. For more information about each area, see:

- [Chapter 7 Managing Physical Resources](#)
- [Chapter 8 Working with the Management Domain and Workload Domains](#)

System Status

Use this page to check on the health of the system. You can view SDDC Manager alerts, examine historical and current information about the workflows running in the system, and examine the events and audit events that are raised by the SDDC Manager problem detection and monitoring components. From these event lists, you can access the Event Catalog to see descriptions of the pre-configured events that are generated through SDDC Manager. From the alerts listing, you can access the Alert Catalog to see descriptions of the SDDC Manager alerts that can be raised.



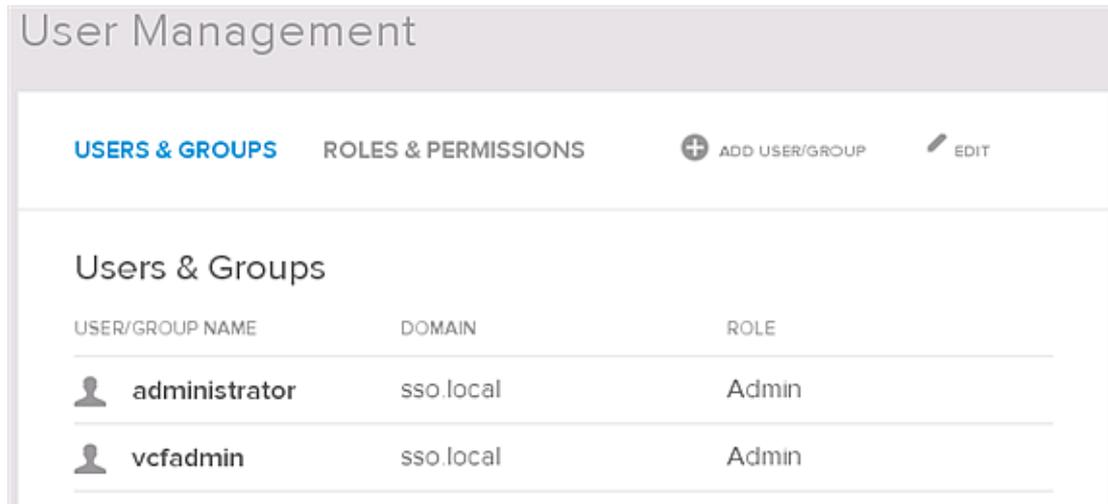
Your Cloud Foundation system has event-driven problem detection. The software records an event for system conditions that are potentially significant or interesting to you, such as a degradation, a failure, or a user-initiated configuration change. The software raises an alert when it determines a problem, based on an analysis of the event or combination of events.

See [Chapter 10 Monitoring Capabilities in the Cloud Foundation System](#) for the information about using alerts and events to monitor the health of your Cloud Foundation system.

User Management

Use this page to perform tasks related to access to the system, such as:

- In the Users & Groups screen, grant or revoke the ability for users and groups to use SDDC Manager.
- In the Roles & Permissions screen, examine the roles that provide the privileges associated with the available operations. SDDC Manager uses role-based access control (RBAC).

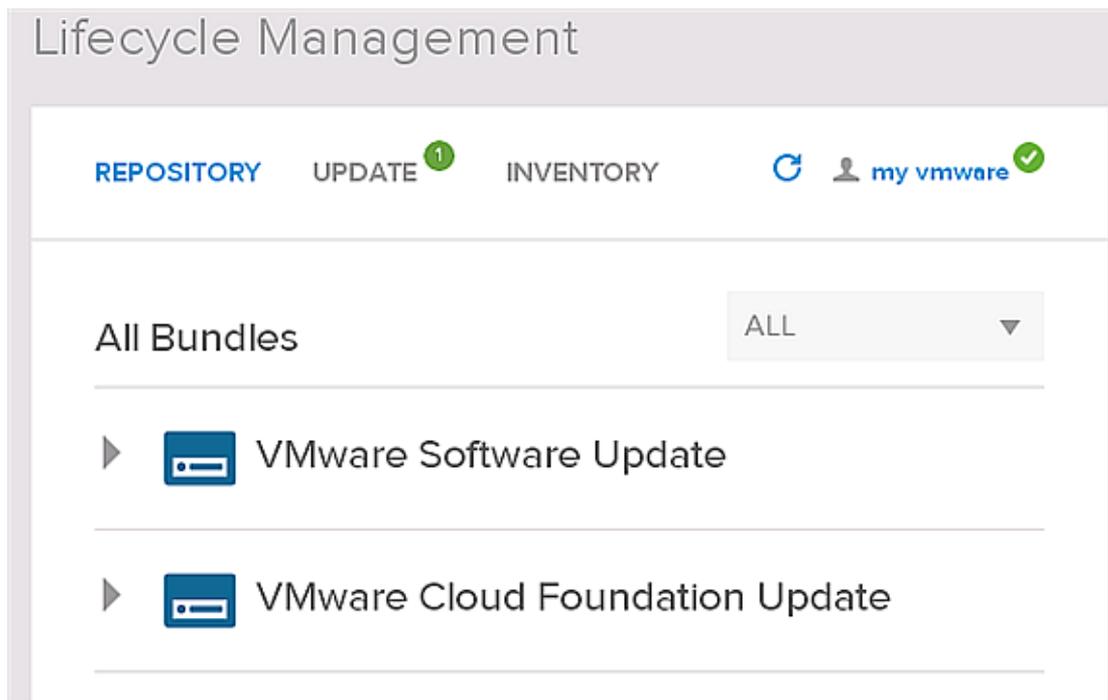


Two roles are defined by default. One is an administrator-level role that provides full administrative privileges. The other provides read-only privileges.

See [Chapter 6 Managing Users and Groups](#).

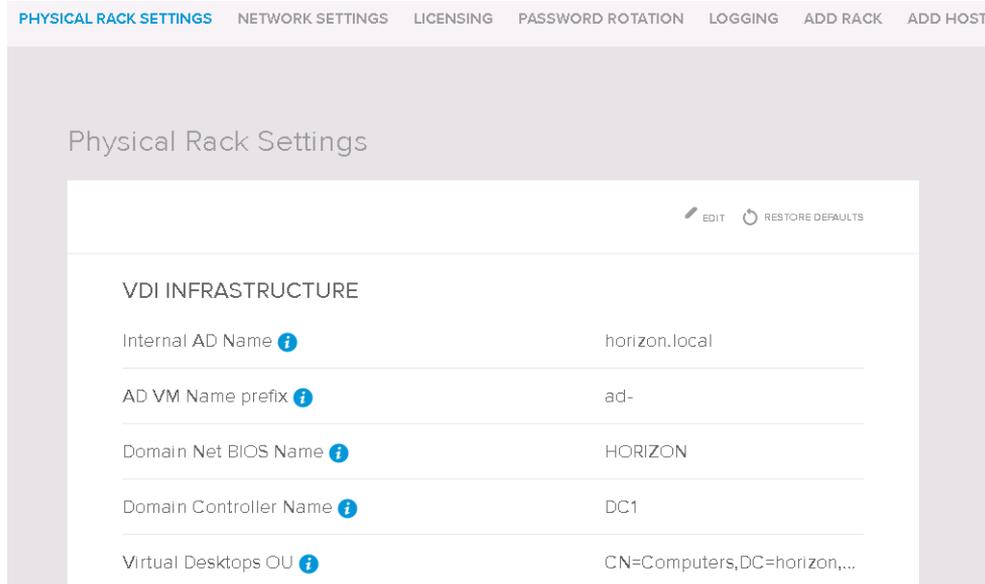
Life Cycle Management

Use this page to manage the patching and updating of the software components that are installed in the system. When the VMware depot is configured, the software notifies you when an update is available and provides the ability to download the bundles and begin the update process. For details, see [Chapter 15 Patching and Upgrading Cloud Foundation](#).



Settings

Use the page to access screens in which you perform tasks that involve customizing VDI infrastructure settings, adding a new physical rack, working with network settings, and managing license keys.



From the Settings page, you can navigate to screens in which you perform tasks such as:

- Configure default settings for the VDI systems that you can provision in your Cloud Foundation system. For details about setting defaults used for VDI systems, see [Customize Default Values Used When Creating VDI Workload Domains](#).
- Initiate the process for adding a new host or rack to the system.
- Work with network settings, such as editing uplink connectivity settings, reviewing the IP address distribution in the system, excluding IP addresses, entering data center network configurations, and associating those configurations with workload domains.
- Manage product license keys.
- Change passwords for the system components.

Log out of SDDC Manager

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

Procedure

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

Managing Certificates for Cloud Foundation Components

3

You can manage certificates for all external-facing Cloud Foundation component resources, including configuring a certificate authority, generating and downloading CSRs, and installing them. This section provides instructions for using both Microsoft and non-Microsoft certificate authorities.

You can manage the certificates for the following components.

- Platform Services Controllers
- vCenter Server
- NSX Manager
- SDDC Manager
- vRealize Automation
- vRealize Log Insight
- vRealize Operations

Note If you have errors when replacing certificates for vRealize Automation , refer to [Replace the vRealize Automation Appliance Management Site Certificate](#) in the vRealize Automation product documentation.

You replace certificates for the following reasons:

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

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

Note At the beginning of the certificate replacement workflow, the SDDC Manager Dashboard automatically takes a snapshot (`pre-replace-certificate`) of the component resources, except for the vRealize Suite components. This enables you to rollback if the certificate replacement process fails. If the process succeeds, this snapshot is automatically deleted.

Important Do not replace certificate if any update operations are in progress. Wait until updates complete before proceeding.

1 [Create Configuration File Package for the Certificate Generation Tool](#)

Create a configuration file that contains certificate information for your organization. Using this configuration file, the tool generates a file package that contains a configuration file for the VMs in each Cloud Foundation component.

2 [Generate Key Pairs and Certificates](#)

With the Certificate Generation utility, you can either create certificates signed by Microsoft Windows, or create a certificate signing request for a third-party CA.

3 [Build File Package for Certificate Replacement Tool](#)

Package the generated key pairs, CA-signed certificates, and CA chain.

4 [Backup TrustStores](#)

Backup the TrustStores for vCenter Server, Platform Services Controllers, and SDDC Manager VM.

5 [Take Snapshots of Cloud Foundation Components](#)

Take a snapshot of Cloud Foundation components.

6 [Replace Certificates](#)

Replace certificates with the signed certificates you generated.

7 [Re-trust VDI Workload Domains](#)

If you have replaced vCenter Server and PSC certificates in your Cloud Foundation system, software that has a trust relationship with vCenter Server certificates must be re-trusted using the new certificates. VI workload domains are re-trusted automatically, but you must re-trust VDI workload domains manually.

8 [Verify that the System Works with the New Certificates](#)

Access the SDDC Manager Dashboard to verify that the new certificates work.

9 [Verify Trust for Replaced Certificates](#)

If you replaced certificates for specific components, you must verify trust.

10 [Delete Snapshots of Cloud Foundation Components](#)

After certificates have been replaced successfully, delete the snapshots.

Create Configuration File Package for the Certificate Generation Tool

Create a configuration file that contains certificate information for your organization. Using this configuration file, the tool generates a file package that contains a configuration file for the VMs in each Cloud Foundation component.

You can specify the components for which you want to replace certificates in the configuration file. It is recommended that you replace all certificates immediately after you deploy Cloud Foundation. Subsequently, you can replace certificates for a subset of components, as appropriate.

Procedure

- 1 Using the root credentials, SSH in to the SDDC Manager VM.
- 2 Navigate to `/opt/vmware/cert-mgmt/bin`.
- 3 Type the following command.

```
./vcfcert-helper \
--config_file config.json \
--cert_dir cert-output \
--action build-certgen-config
```

Table 3-1. Parameter Information

Parameter	Description
<code>--config_file</code>	Name of the input configuration JSON file.
<code>--cert_dir</code>	Directory where the configuration file package is to be created.
<code>--action</code>	Action to be performed.

The file package for the Certificate Generation Tool is created in the specified directory. The tool also creates a zip file of the directory contents in the parent directory.

Example Configuration File for Certificate Replacement After Deployment

In this example file, all certificates are being replaced. The `certificateDefaults` sections contains your organizations' details.

```
{
  "replacementScope" : {
    "replaceEverything" : true
  },
  "certificateDefaults" : {
    "countryName" : "US",
    "stateOrProvinceName" : "California",
    "localityName" : "Palo Alto",
    "organizationName" : "VMWare Inc.",
  }
}
```

```

    "organizationUnitName" : "VMware IT department",
    "keySize" : 4096
  }
}

```

The maximum keySize is 4096 bits.

Example Configuration Files for Certificate Replacement on Specific Components

You can specify one or more component for certificate replacement.

The management domain contains the following VMs:

- 2 PSC VMs
- 1 vCenter Server VM
- 1 NSX Manager VM
- 3 vRealize Log Insight VMs
- 1 SDDC Manager VM
- vRealize Operations VMs if you have installed vRealize Operations
- vRealize Automation VMs if you have installed vRealize Automation

Each workload domain contains 1 vCenter Server VM and 1 NSX Manager VM.

It is recommended that you replace the certificates on a workload domain right after you create a new workload domain (both vCenter Server and NSX Manager).

From then on, you can replace certificates as appropriate - all certificates for the management domain or workload domain, or some certificates on one or more domain. The following sections have some example configuration files. vRealize Operations certificates are replaced automatically as part of the management domain components. You must replace vRealize Automation certificates manually after the initial certificate replacement after deployment.

Replace vCenter Server and NSX Manager Certificates on a Workload Domain

```

{
  "replacementScope" : {
    "replaceWorkloadDomain" : ["DomainName"],
  },
  "certificateDefaults" : {
    "countryName" : "US",
    "stateOrProvinceName" : "California",
    "localityName" : "Palo Alto",
    "organizationName" : "VMWare Inc.",
  }
}

```

```

    "organizationUnitName" : "VMware IT department",
    "keySize" : 4096
  }
}

```

You can specify more than one workload domain.

Replace vRealize Log Insight Certificates on the Management Domain

```

{
  "replacementScope" : {
    "replaceManagementDomain" : true,
    "replaceComponents" : ["LOGINSIGHT"]
  },
  "certificateDefaults" : {
    "countryName" : "US",
    "stateOrProvinceName" : "California",
    "localityName" : "Palo Alto",
    "organizationName" : "VMWare Inc.",
    "organizationUnitName" : "VMware IT department",
    "keySize" : 4096
  }
}

```

Replace NSX Manager Certificate on a Workload Domain

```

{
  "replacementScope" : {
    "replaceWorkloadDomain" : ["DomainName"],
    "replaceComponents" : ["NSX"]
  },
  "certificateDefaults" : {
    "countryName" : "US",
    "stateOrProvinceName" : "California",
    "localityName" : "Palo Alto",
    "organizationName" : "VMWare Inc.",
    "organizationUnitName" : "VMware IT department",
    "keySize" : 4096
  }
}

```

You can specify more than one workload domain.

Generate Key Pairs and Certificates

With the Certificate Generation utility, you can either create certificates signed by Microsoft Windows, or create a certificate signing request for a third-party CA.

Note There is a known security risk when copying key pairs and certificates to the `/root/certs` directory because it is not FIPS compliant.

Prerequisites

- You must have a Windows host with PowerShell installed on it.
- For a Microsoft Windows signed certificate, the Windows host must be in the same domain as the Windows CA.
- The account that you use to log in must have administrative privileges.

Although non-administrator users can download and launch the tool, all operations fail if you do not have the proper permissions.

- You must have created a Microsoft CA template. See Microsoft Certificate Authority Template in *VMware Validated Design for Software-Designed Data Center*.
- You must have downloaded and installed OpenSSL for Windows.

You can obtain the binary file from <http://gnuwin32.sourceforge.net/packages/openssl.htm>. It can be extracted anywhere in the Windows path.

Procedure

- 1 Copy the file package zip file from the SDDC Manager VM to the Windows host.

- 2 Extract the contents of the zip file on the Windows host.

The CertGenVVD-*.ps1 file is included in the extracted files.

- 3 Navigate to the directory where you extracted the contents of the zip file.

- 4 Run one of the following commands.

- To create a Microsoft Windows signed certificate, run the following command:

```
CertGenVVD-3.0.ps1 -MSCASigned -attrib 'CertificateTemplate:VMware' -inter
```

Parameter	Description
-MSCASigned	Certificate is to be signed by inter-mediate authority.
-attrib 'CertificateTemplate:VMware'	The Microsoft CA template.

- To create a certificate signing request for a third-party CA, run the following command.

```
.\CertGenVVD-3.0.1.ps1 -CSR
```

- 5 Type a password for the key file.

A folder named SignedByMSCACerts is created.

- 6 Zip the contents of the SignedByMSCACerts folder.

- 7 Copy the SignedByMSCACerts zipped folder to the SDDC Manager VM in the /opt/vmware/cert-mgmt/bin directory.

Note The zip folder contains highly sensitive private key files and must be sent over trusted paths.

- 8 Navigate to the /opt/vmware/cert-mgmt/bin directory and unzip the SignedByMSCACerts folder.

Build File Package for Certificate Replacement Tool

Package the generated key pairs, CA-signed certificates, and CA chain.

Prerequisites

If the key files are password protected, you must have the password. All password-protected key files must have the same password.

Procedure

- ◆ In the `/opt/vmware/cert-mgmt/bin` directory of the SDDC Manager VM, type the following command.

```
./vcfcerthelper \
--config_file config.json \
--cert_dir SignedByMSCACerts \
--password 'psswd' \
--action build-certrepl-config
--enable_ssl_passthrough
```

Parameter	Description
<code>--config_file</code>	Configuration file you built for the Certificate Generation tool.
<code>--cert_dir</code>	Directory where the CA signed certificates are stored.
<code>--password</code>	Key password.
<code>--action</code>	Action to be performed.
<code>--enable_ssl_passthrough</code>	Changes vRealize load balancer to SSL passthrough mode.

The file package is created in the same directory that contains the CA signed certificates.

Backup TrustStores

Backup the TrustStores for vCenter Server, Platform Services Controllers, and SDDC Manager VM.

Procedure

- ◆ In the `/opt/vmware/cert-mgmt/bin` directory of the SDDC Manager VM, type the following command.

```
./vcfcerthelper --action list-ca --cert_dir truststore-backup-day-1
```

Take Snapshots of Cloud Foundation Components

Take a snapshot of Cloud Foundation components.

Procedure

- ◆ In the `/opt/vmware/cert-mgmt/bin` directory of the SDDC Manager VM, type the following command.

```
./vcfcerthelper.py \
--config_file config.json \
--action create-snapshot
```

Parameter	Description
<code>--config_file</code>	Configuration file you built for the Certificate Generation tool.
<code>--action</code>	Action to be performed.

Replace Certificates

Replace certificates with the signed certificates you generated.

Procedure

- ◆ In the `/opt/vmware/cert-mgmt/bin` directory of the SDDC Manager VM, type the following command.

```
/usr/java/jre-vmware/bin/java \
-Djsse.enableSNIExtension=false \
-jar /opt/vmware/cert-mgmt/lib/certreplace-0.0.1-SNAPSHOT.jar \
-config SignedByMSCACerts/config-vcf.json
```

Re-trust VDI Workload Domains

If you have replaced vCenter Server and PSC certificates in your Cloud Foundation system, software that has a trust relationship with vCenter Server certificates must be re-trusted using the new certificates. VI workload domains are re-trusted automatically, but you must re-trust VDI workload domains manually.

Procedure**1 Prepare Certificate Chain**

Retrieve the certificate chain file created by the Certificate Generation Tool (`root64.cer`). If the certificate chain has more than certificate, split the chain into multiple files such that each file has a single certificate.

2 Transfer Certificate Chain Files to Windows Connection Servers

You now import the certificate chain files to each Windows connection server.

3 Verify Trust

Verify trust with the new vCenter Server certificate.

Prepare Certificate Chain

Retrieve the certificate chain file created by the Certificate Generation Tool (`root64.cer`). If the certificate chain has more than certificate, split the chain into multiple files such that each file has a single certificate.

If the `root64.cer` file is not available, obtain the certificate chain from vCenter Server by following steps 1 and 2 below. Ignore these steps if you have this file.

Procedure

- 1 SSH in to the SDDC Manager VM.
- 2 Type the following command.

```
echo | openssl s_client -connect \  
vCenterHostName.local:443 \  
-showcerts -no_ign_eof > root64.cer
```

The `root64.cer` file contains the certificates between the BEGIN and END lines.

- 3 Save the `root64.cer` file in VI.

```
:set ff=dos  
:wq
```

The file is saved as a DOS formatted file.

- 4 Ignore the first section in the file. This is the server certificate, which is not part of the certificate chain. Save each subsequent section in a separate file. Note that the last certificate in the file is the root CA certificate while the other certificates are subordinate CA certificates.

Transfer Certificate Chain Files to Windows Connection Servers

You now import the certificate chain files to each Windows connection server.

Procedure

- 1 Open MMC on the Windows connection server.
- 2 Make the necessary selections to set certificate addition to the local computer.
 - a Click **File > Add/Remove snap-in**.
 - b Click **Certificates** and then click **Add**.
 - c Click **Computer Account** and then click **Next**.
 - d Click **Local Computer**.
 - e Click **Finish** and then click **OK**.

- 3 Import the root certificate.
 - a In the navigation panel, click **Certificates > Trusted Root Certification Authorities > Certificates**.
 - b Right-click **Certificates** and select **All Tasks > Import**.
 - c Select the root CA certificate.
 - d Select **Place all certs in Trusted Root Certification Authorities** .
 - e Click **Finish**.
- 4 Import all subordinate certificates.
 - a In the navigation panel, click **Certificates > Intermediate Certification Authorities > Certificates**.
 - b Right-click **Certificates** and select **All Tasks > Import**.
 - c Select a subordinate certificate.
 - d Select **Place all certs in Intermediate Certification Authorities** .
 - e Click **Finish**.
 - f Repeat steps a - e for each subordinate certificate.
- 5 Reboot the connection server.
- 6 Repeat steps 1 - 6 for each connection server.

Verify Trust

Verify trust with the new vCenter Server certificate.

Procedure

- 1 Open the vSphere Web Client.
- 2 Locate the IP address of a connection server.
- 3 Open a web browser session to the connection server admin web app. For example, **https://10.212.0.55/admin**.
- 4 In the inventory navigation pane, click Dashboard.
- 5 Expand the list of vCenter Servers.

All vCenter Servers should have a green icon.

- 6 If a vCenter Server has a red icon, follow the steps below.
 - a Click **Verify**.
The vCenter Server should get verified.
 - b If a dialog box opens, click **Accept**.
Wait for a minute.
 - c Refresh the Dashboard.
The vCenter should now have a green icon.

Verify that the System Works with the New Certificates

Access the SDDC Manager Dashboard to verify that the new certificates work.

Procedure

- 1 In a web browser, login to the SDDC Manager Dashboard to verify that it displays correctly:
`https://IP-FQDN:8443/vrm-ui`
- 2 Launch vCenter Server to verify that it displays correctly.
- 3 If **vRealize Operations** is deployed, login to **vRealize Operations** and verify that all adapters are collecting data. Some adapters may display an error until the next collection cycle.

Verify Trust for Replaced Certificates

If you replaced certificates for specific components, you must verify trust.

Procedure

- 1 SSH in to the SDDC Manager VM.
- 2 Navigate to the `/opt/vmware/cert-mgmt/bin` directory.
- 3 Type the following command.

```
vcfcerthelper --action verify-trust --cert_dir dir
```

Parameter	Description
<code>verify-trust</code>	Command to verify trust.
<code>--cert_dir dir</code>	Saves the results of the <code>verify-trust</code> command to the specified directory.

Delete Snapshots of Cloud Foundation Components

After certificates have been replaced successfully, delete the snapshots.

Prerequisites

Delete the Cloud Foundation snapshots after certificates have been successfully replaced.

Procedure

- ◆ In the `/opt/vmware/cert-mgmt/bin/vcfcert-helper` directory of the SDDC Manager VM, type the following command.

```
./vcfcert-helper \  
--config_file config.json \  
--action remove-snapshot
```

Table 3-2. Parameter Information

Parameter	Description
<code>--config_file</code>	Name of the configuration file.
<code>--action</code>	Action to be performed.

Changing the Passwords of Your Cloud Foundation System On Demand

4

For security reasons, you can change passwords for the built-in accounts that are used by your Cloud Foundation system. Changing these passwords periodically or when certain events occur, such as an administrator leaving your organization, reduces the likelihood of security vulnerabilities occurring.

You had specified passwords for the Cloud Foundation system built-in accounts in the deployment parameters sheet before bring-up. You can modify the passwords for these accounts using RESTful API calls.

Note The NSX cluster controller password is hardcoded in the system. It is strongly recommended that you look it up and update it. See [GUID-AD195D27-5298-4FDC-A27C-5A4F3185F6FB#GUID-AD195D27-5298-4FDC-A27C-5A4F3185F6FB](#) and [GUID-6A8AEEB1-4920-4512-B039-372F75C374F3#GUID-6A8AEEB1-4920-4512-B039-372F75C374F3](#).

This chapter includes the following topics:

- [Rotate Passwords On-Demand for Managed Physical and Logical Entities](#)
- [Credentials for Logging in to the SDDC Manager VM](#)
- [Look Up Account Credentials](#)
- [Password Management CLI Command Reference](#)

Rotate Passwords On-Demand for Managed Physical and Logical Entities

You can rotate passwords for the logical and physical entities on all racks in your system.

Password rotation does not change the password of the SDDC Manager VM's root account, and the lookup command does not report this password.

Prerequisites

Verify the following prerequisites are met:

- No failed workflows exist in the system. Use the Workflows area of the System Status page to verify the system has no workflows in a failure state.

- No active workflows are running or are scheduled to run during the brief time period that the password rotation process is running. Schedule a window of time when you expect to have no running workflows before performing on-demand password rotation.

Procedure

1 On the SDDC Manager Dashboard, click **Settings**.

2 Click **Password Rotation**.

The Password Rotation page displays the results of the last password rotation iteration.

3 Click the **Rotate Password** button at the bottom center of the page.

The tasks section displays the complete list of tasks to be performed. As each of these tasks are run, the status is updated. If a task fails, take the necessary corrective action and click **Retry**.

If there is no corrective action that you can take, skip the failed task and resume the workflow by running the `resume-password-workflows --skip-failed-task` CLI command. For more information, see [Password Management CLI Command Reference](#).

Password rotation is complete when all tasks are completed successfully.

Credentials for Logging in to the SDDC Manager VM

You need to login to the root account of the SDDC Manager VM to run password management CLI commands.

When the hardware for a rack is imaged, a random password is generated for the root account of the SDDC Manager VM. That generated password is obtained at the end of the imaging process. After the bring-up process was completed on the first rack, you should have changed this password as described in the *VMware Cloud Foundation Overview and Bring-Up Guide*. You must retain this password.

Password rotation does not change the password of the SDDC Manager VM's root account, and the lookup command does not report this password.

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

You must have the root account credentials to log in to the SDDC Manager VM. See [Credentials for Logging in to the SDDC Manager VM](#).

Procedure

1 SSH in to the SDDC Manager VM using the root credentials.

2 Change to the `/home/vrack/bin` directory.

- 3 Obtain the account credentials list by typing the command:

```
lookup-passwords
```

To display the output in JSON format, use the command:

```
lookup-passwords -j
```

The output displays the account credentials and IP addresses for the physical and logical entities on all racks in your environment. The username and password for each account is displayed.

- 4 (Optional) Save the command output to a secure location so that you can access it later and use it to log in to the components as needed.

Password Management CLI Command Reference

Password management CLI commands are located in `/home/vrack/bin` in the SDDC Manager virtual machine's file system. Only the root account can run these commands. To run a command, change to the `/home/vrack/bin` directory and type the command.

To get help on a specific command, use the following option.

```
command --help
```

For example, to get help on the lookup command, use the following command.

```
lookup-passwords --help
```

Lookup Commands

Use these commands to look up information about entities managed by SDDC Manager.

Table 4-1. Lookup Commands

Command	Options	Description
lookup-history	latest timestamp <code>yyyy-mm-dd.hh:mm:ss</code> -json	Manages and retrieves the password history recorded in Zookeeper. lookup-history latest lists the account information from the most recent history recorded in Zookeeper. lookup-history timestamp <code>yyyy-mm-dd.hh:mm:ss</code> lists the password-rotation history associated with the specified timestamp.
lookup-passwords	None	Retrieves and lists the account credentials for the built-in accounts that are managed and rotated by SDDC Manager. See also Look Up Account Credentials .

Password Change, Set Up, and Generation Commands

Use these commands to change passwords to software-generated randomized passwords for the accounts that are managed by SDDC Manager, set up ESXi host passwords, and generate passwords that adhere to the SDDC Manager password policies.

Table 4-2. Password Change, Set Up, and Generation Commands

Command	Options	Description
<code>rotate-passwords</code>	None	Rotates passwords for all inventory items that are visible and safe to automatically rotate.
<code>decrypt</code>	encrypted-text	Decrypts the input text and prints the output to the command line. Used by SDDC Manager. Manual use of this command is not needed.
<code>encrypt</code>	plain-text	Encrypts the input text and prints the output to the command line. Used by SDDC Manager. Manual use of this command is not needed.
<code>setup-esx-password</code>	None	Creates a password workflow for setting an ESXi host password using the old password provided. Used by the host commissioning procedure. Manual use of this command is not needed.

Password Workflow Commands

Use these commands for password workflows. Commands are listed alphabetically.

Table 4-3. Password Workflow Commands

Command	Options	Description
<code>create-password-workflow</code>	None	Creates specific password workflows. Used by SDDC Manager. Manual use of this command is not needed. To rotate passwords, use the <code>rotate-passwords</code> or <code>setup-esx-password</code> command.
<code>delete-password-workflows</code>	<code>latest</code>	Deletes a workflow. In general, it is a workflow that has failed and cannot otherwise be corrected so that it can resume and run to completion. The identifier of the workflow can be obtained by one of the following: <ul style="list-style-type: none"> ■ For a failed workflow, use the following command. <code>get-password-workflow latest</code> ■ For an older, successful workflow, use the following command. <code>list-password-workflows</code>

Table 4-3. Password Workflow Commands (Continued)

Command	Options	Description
get-password	--ip xxx.xxx.xxx.xxx username login	Retrieves a password for a device. get-password --ip xxx.xxx.xxx.xxx retrieves the password for the device with the specified IP address.
get-password-workflow	latest	Retrieves specific password workflow instance by using its identifier. For example, the following commands displays the latest (or current) workflow. get-password-workflow latest
get-sso	-p -u	Retrieves either the SSO username or password. This command works even when SDDC Manager is not running. get-sso -p retrieves the SSO password. get-sso -u retrieves the SSO username.
list-password-workflows	None	Lists all of the password workflows in the system. You can view a few summary attributes about each workflow, including its identifier and status, as well as an error message when applicable.
resume-password-workflows	--skip-failed-task	Resumes a failed workflow. You may run this command after you take corrective action based on a failed task during password rotation. resume-password-workflows --skip-failed-task skips a failed task and resumes the workflow. After a success message is displayed, run the monitor-password-workflow to see the workflow progress.
monitor-password-workflow	None	Monitors the latest (or current) workflow, which is an asynchronous job running in the SDDC Manager. It polls the status of the workflow and reports percentage completed until the workflow finishes, at which time it reports its status.
vrm-rest	None	Private command containing implementation details of the CLI commands. Manual use of this command is not needed.

Backing up and Restoring a Cloud Foundation System

5

You can back up all the management components of your Cloud Foundation system. In the event of data corruption or loss, you can restore the domain VMs from the backup copies.

It is recommended that you schedule regular backups for all management domain VMs, and all Cloud Foundation components.

Note This chapter does not include backup and restore of workload domain VMs.

It is also recommended that you back up the management domain VMs prior to and after: upgrading Cloud Foundation; creating, deleting, or modifying the domain; and rotating the passwords. For scheduled backups, please refer to each component product section for individual component backup and restore procedures.

This chapter includes the following topics:

- [Requirements](#)
- [Back Up Methods for Cloud Foundation Components](#)
- [Backup and Restore Considerations](#)
- [Backing Up and Restoring the SDDC Manager VM and SDDC Manager Utility VM](#)
- [Backing Up and Restoring the vCenter Server and Platform Services Controller VMs](#)
- [Backing Up vRealize Components](#)
- [Backing Up and Restoring NSX Manager](#)
- [Backing Up and Restoring Distributed Switches](#)
- [Back Up Physical Switch Configurations](#)
- [Backing Up the Cloud Foundation Configuration](#)

Requirements

You must configure external storage for the domain backups.

- Verify that an external (secondary) IP-based storage is connected to the management domain.

- Verify that you have an image-level backup appliance that is integrated with VMware vSphere Storage APIs - Data Protection, and is compatible with the vSphere version used by the management domain available and installed on the management domain.
- Verify that the backup appliance is also hosted on the external, IP-based storage.
- Verify that an SFTP server is available to store file-based backup data.

Back Up Methods for Cloud Foundation Components

The following table describes the components that you can back up, and the methods for backup and restore.

Category	Component	Backup Method	Restore Method
Management	SDDC Manager VM	Image level	Image level
	SDDC Manager Utility VM	Image level	Image level
	vCenter Server VMs (including all logical switches)	Image level/file level	Image level/file level
	Platform Services Controller VMs	Image level/file level	Image level/file level
	vRealize Log Insight	Image level	Image level
	NSX Manager VMs	Files backed up by SDDC Manager	File level
Hardware	Management switch	File level	File level
	Top of rack switches	File level	File level

Category	Component	Backup Method	Restore Method
	Inter-rack switches	File level	File level
Configuration Components	<ul style="list-style-type: none"> ■ Credentials Authorization information that enable Cloud Foundation components to connect with each other. ■ Host inventory Complete information about each ESXi host in the system. ■ Cloud Foundation bundle release number 	File level	File level

Note Physical switch configurations are also backed up as part of the Cloud Foundation configuration backup. See [Backing Up the Cloud Foundation Configuration](#).

Note There will be multiple instances of vCenter Server and NSX Manager in the management cluster. One instance for the management domain and other instances for the workload domains. The NSX Manager backup includes NSX Controllers, DLR Control-VM and NSX Edge VMs, as well as DFW rules and logical switches.

Note If your chosen backup appliance supports emergency restore, you can use the image-level backup method for the vCenter and Platform Services Controller (PSC) VMs. If not, you can use the file-based method for these components.

Note Additional backup features are also available using the SoS tool. See [Chapter 13 Supportability and Serviceability \(SoS\) Tool](#).

Backup and Restore Considerations

When configuring backup and restore, consider your recovery strategy, including the backup solution being used, where it is implemented, and how the different Cloud Foundation components are backed up and restored.

Note A restore operation may result in state inconsistencies. It is recommended that you contact VMware Support before restoring a management component to get assistance with identifying and correcting any state inconsistencies that may develop.

Recovery Strategy

It is recommended that you schedule regular backups for all management VMs.

Before you can restore any management VMs, the following components must be operational:

- The management vCenter Server
- The Platform Services Controller VMs
- The SDDC Manager VM
- The SDDC Manager Utility VM

Therefore, if any of these components were impacted, restore them first before restoring any management VMs. For example, the management vCenter Server must be restored first because it manages all the other management VMs.

Using Dell EMC Avamar Virtual Edition (AVE)

You can use any backup tool that meets the [Requirements](#).

The Dell EMC Avamar Virtual Edition (AVE) appliance meets the requirements for image-level backup and restore operations, and integrates well with Cloud Foundation. For product information, see <https://www.emc.com/data-protection/avamar.htm>.

Note For deployment and configuration of Dell EMC Avamar on the management domain of Cloud Foundation, see the VMware Knowledge Base article: <https://kb.vmware.com/kb/2149872>.

It is recommended that the Avamar appliance is hosted on an IP-based storage connected to the management domain.

Backing Up and Restoring the SDDC Manager VM and SDDC Manager Utility VM

It is recommended that you schedule regular backups of SDDC Manager VM and the SDDC Manager Utility VM and perform restore in case of a corrupt appliance instance.

SDDC Manager VM image backup supports application-consistent quiescing. The SDDC Manager VM contains pre-freeze and post-thaw scripts for quiescing and un-quiescing the SDDC applications or services. These scripts are automatically called when the backup tool invokes the backup operation, and in turn the quiesced snapshot operation, on the SDDC Manager VM.

Note A quiesced snapshot operation invoked by a backup job succeeds when both the pre-freeze and post-thaw scripts return successfully. This method ensures that the backup is application consistent.

- For instructions on image-level backup and restore using a third-party appliance that meets the [Requirements](#), see the vendor instructions.
- For instructions on using Dell EMC Avamar Virtual Edition (AVE), see the Knowledge Base article [Back Up and Restore of VMs Deployed on a vSAN Datastore Using DELL EMC Avamar](#).
 - *Creating a VMware policy*
 - *Starting ad-hoc image backup*

- *Starting image restore*

The SDDC Manager VM has a Cloud Foundation ISO bundle mounted to it. This ISO is present in the management domain vSAN datastore and is required for domain creation by SDDC Manager. If your chosen backup appliance can take backups of the ISO bundle, include it in your backup program.

Note The ISO bundle is required to restore the SDDC Manager. Because the ISO bundle is not updated frequently, only occasional backups are necessary. If your backup tool can include the ISO bundle in the backup process, you can use this backup copy if you need to restore the ISO bundle. If your backup process does not include the ISO bundle, you can obtain the same version ISO bundle from the Cloud Foundation image repository.

Backing Up and Restoring the vCenter Server and Platform Services Controller VMs

Cloud Foundation supports both file-level and image-level backup and restore methods for the vCenter Server Appliance.

If your chosen backup tool supports restoring the vCenter Server and Platform Services Controller (PSC) VMs directly to ESXi independently of vCenter Server, it is recommended you use the image-level backup method for these VMs instead of the file-level backup and restore method.

- For instructions on file-level backup and restore for the vCenter Server VMs, see [File-Based Backup and Restore of vCenter Server Appliance](#) in the vSphere product documentation.

Note If you use the file-level approach, it is recommended that you configure the process to copy the backup files to a FTP server outside of your Cloud Foundation deployment.

- For instructions on image-level backup and restore using a third-party appliance that meets the [Requirements](#), see the vendor instructions.
- For instructions on using Dell EMC Avamar Virtual Edition (AVE), see the Knowledge Base article [Back Up and Restore of VMs Deployed on a vSAN Datastore Using DELL EMC Avamar](#).
 - *Creating a VMware policy*
 - *Starting ad-hoc image backup*
 - *Starting image restore*

Backing Up vRealize Components

There is no specific Cloud Foundation functionality for backing the vRealize components (vRealize Log Insight vRealize Automation, and vRealize Operations). However, you can use the procedures documented in the vRealize documentation, as shown in the following sections.

For more comprehensive documentation, see [vRealize Suite 2017 Backup and Restore](#).

Backing Up and Restoring NSX Manager

Proper backup of all NSX components is crucial to restore the system to its working state in the event of a failure.

The NSX Manager backup contains all of the NSX configuration, including controllers, logical switching and routing entities, security, firewall rules, and everything else that you configure within the NSX Manager interface or API.

Depending on whether the NSX Manager is for management domain or workload domain, the scheduled backup is auto-configured during bring-up or workload domain deployment. The backup data is saved in the SDDC Manager Utility VM, which is in turn backed up using your chosen backup appliance.

Important Because the NSX Manager backup is auto-configured, do not modify the backup configuration settings in the NSX Manager interface, or the NSX Manager backup will not be included in the Cloud Foundation process.

Additionally, you can trigger NSX Manager backups on demand directly in the NSX Manager appliance interface.

Triggering a NSX Manager Back Up On Demand

This topic describes how to manually trigger a NSX Manager backup from the NSX Manager interface.

This task is optional because the NSX Manager backup process is automated and scheduled.

Procedure

- 1 Log in to the NSX Manager Virtual Appliance.
- 2 Under Appliance Management, click **Backups & Restore**.
- 3 For an on-demand backup, click **Backup**.

A new file is added under **Backup History**.

Restore an NSX Manager Backup

You can restore a backup only on a freshly deployed NSX Manager appliance.

Before restoring NSX Manager data, it is recommended that you reinstall the NSX Manager appliance. Running the restore operation on an existing NSX Manager appliance is not officially supported. This assumes that the existing NSX Manager has failed, and therefore a new NSX Manager appliance should be deployed.

Procedure

- 1 Review the existing NSX Manager settings in the latest Cloud Foundation configuration backup.
See [Backing Up the Cloud Foundation Configuration](#).

- 2 Deploy a new NSX Manager appliance.

Important The new NSX Manager appliance must be the same version as the backed up appliance.

- 3 Log in to the new NSX Manager appliance.
- 4 Under Appliance Management, click **Backups & Restore**.
- 5 In FTP Server Settings, click **Change** to add the settings from the latest Cloud Foundation configuration backup.

The Host IP Address, User Name, Password, Backup Directory, Filename Prefix, and Pass Phrase fields in the Backup Location screen must identify the location of the backup to be restored.

- 6 In the **Backup History** section, select the required backup folder to restore.
- 7 Click **Restore**.
- 8 Click **OK** to confirm.

Restore NSX Edges

All NSX Edge configurations (logical routers and edge services gateways) are backed up as part of NSX Manager data backup.

Taking individual NSX Edge backups is not supported.

If you have an intact NSX Manager configuration, you can recreate an inaccessible or failed Edge appliance VM by redeploying the NSX Edge (click **Redeploy NSX Edge** () in the vSphere Web Client). See "Redeploy NSX Edge" in the *NSX Administration Guide*.

Caution After restoring an NSX Manager backup, you might need to take additional action to ensure correct operation of NSX Edge appliances.

- Edge appliances created after last backup are not removed during restore. You must delete the VM manually.
- Edge appliances deleted after the last backup are not restored unless redeployed.
- If both the configured and current locations of an NSX Edge appliance saved in the backup no longer exist when the backup is restored, operations such as redeploy, migrate, enable or disable HA will fail. You must edit the appliance configuration and provide valid location information. Use `PUT /api/4.0/edges/{edgeId}/appliances` to edit the appliance location configuration (*resourcePoolId*, *datastoreId*, *hostId* and *vmFolderId* as necessary). See "Working With NSX Edge Appliance Configuration" in the *NSX API Guide*.

If any of the following changes have occurred since the last NSX Manager backup, the restored NSX Manager configuration and the configuration present on the NSX Edge appliance will differ. You must **Force Sync** the NSX Edge to revert these changes on the appliance and ensure correct operation of the NSX Edge. See "Force Sync NSX Edge with NSX Manager" in the *NSX Administration Guide*.

- Changes made via Distributed Firewall for preRules for NSX Edge firewall.
- Changes in grouping objects membership.

If any of the following changes have occurred since the last NSX Manager backup, the restored NSX Manager configuration and the configuration present on the NSX Edge appliance will differ. You must **Redeploy** the NSX Edge to revert these changes on the appliance and ensure correct operation of the NSX Edge. See "Redeploy NSX Edge" in the *NSX Administration Guide*.

- Changes in Edge appliance settings:
 - HA enabled or disabled
 - appliance moved from deployed to undeployed state
 - appliance moved from undeployed to deployed state
 - resource reservation settings have been changed
- Changes in Edge appliance vNic settings:
 - add, remove, or disconnect vNic
 - port groups
 - trunk ports
 - fence parameters
 - shaping policy

Backing Up and Restoring Distributed Switches

You can export vSphere Distributed Switch and distributed port group configurations to a backup file. The file preserves valid network configurations, enabling transfer of these configurations to other Cloud Foundation systems. You can use the backup file to create multiple copies of the distributed switch configuration on an existing deployment, or to overwrite existing configurations settings.

Use the functionality in the vSphere Web Client tool to create backup files of the distributed switch and distributed port group configurations in your Cloud Foundation system.

For detailed procedures, see Knowledge Base article 2034602 [Exporting/importing/restoring Distributed Switch Configs Using vSphere Web Client](#).

Back Up Physical Switch Configurations

Use the SoS tool to create backup files of the ESXi and physical switch configurations in your Cloud Foundation system. This Python tool resides in the SDDC Manager VM in your system.

To run the SoS tool, SSH in to the SDDC Manager VM using the root account, navigate to the `/opt/vmware/sddc-support` directory and type `./sos` followed by the options required for your desired operation.

```
./sos --option-1 --option-2 --option-3 ... --option-n
```

To list the available command options, use the `--help` long option or the `-h` short option.

```
./sos --help
./sos -h
```

Note You can specify some options in the conventional GNU/POSIX syntax, using `--` for the long option and `-` for the short option.

For more information about the SoS tool, see [Chapter 13 Supportability and Serviceability \(SoS\) Tool](#).

Prerequisites

When running the backup command to create the backup files for all racks in the system in a single command run, you must have the root account credentials for the SDDC Manager VM. When you retrieve these backup files, you can run the tool in the same SDDC Manager VM, logging in using the root account credentials for that VM. See [Credentials for Logging in to the SDDC Manager VM](#).

Procedure

- 1 Using SSH, log in as root to the SDDC Manager VM.
- 2 Change to the `/opt/vmware/sddc-support` directory.

- 3 Type the command to collect the configurations and save the backup files to the `/var/tmp` directory.

```
./sos --backup
```

The tool displays Welcome to SoS(Supportability and Serviceability) utility!, and messages about the tool's progress, for example:

```
rack-1-vm-1:/opt/vmware/sddc-support # ./sos --backup
Welcome to SoS(Supportability and Serviceability) utility!
Backup: /var/tmp/backup-2016-11-08-15-01-48-3650
Log file: /var/tmp/backup-2016-11-08-15-01-48-3650/sos.log
Progress : 0%
```

- 4 (Optional) Use the following command options to run or schedule the backup.

Command	Description
<code>--switch-backup</code>	Backs up the switch configuration.
<code>--esx-backup</code>	Backs up the ESXi configuration.
<code>--schedule-backup</code>	Schedules periodic backup.
<code>--frequency-hours</code>	Sets backup interval in hours.
<code>--delete-backup-schedule</code>	Deletes existing scheduled backup.
<code>--get-backup-schedule</code>	Displays current backup schedule.
<code>--get-all-backups</code>	Gets most recent backup created by scheduler.
<code>--delete-all-backup</code>	Deletes all backups created by scheduler.

The tool collects the ESXi and switch configurations and writes the output to the `/var/tmp` directory in the SDDC Manager VM. Inside that directory, the tool writes the output into a directory whose name reflects the timestamp when the SoS tool initiated the process.

```
/var/tmp backup-timestamp sos.log
rack-1 esx configBundle-hostname.domain.tgz
#One per host switch
ToR-or-inter-rack-switch-ip-address-manufacturername-running-config.gz
#File named according to the switch's IP address and manufacturer
cumulus-192.168.100.1.tgz #Management switch configuration file
```

The ESXi and switch backup files are included in the image-level backups of the SDDC Manager VM. When needed (for example in event of a failure), you can retrieve the backups from the SDDC Manager VM. If that VM itself is not accessible, for example, in case of multiple TOR switch failures, you can also retrieve the ESXi and switch backup files from one of the SDDC Manager VM backups.

What to do next

For details about working with backing up and restoring switches, see [Replacing and Restoring Switches](#).

Backing Up the Cloud Foundation Configuration

You can schedule backups or trigger manual backups of the Cloud Foundation configuration using directly in the SDDC Manager Dashboard or using CLI commands. You can also access and view the backup files,.

Each time a backup is triggered, manually or by schedule, a date- and time-stamped archived bundle containing all the backup files is copied to the dedicated backup location. An event is generated that notifies the user of the success or failure of the backup procedure. If a backup fails, the Cloud Foundation system retries after three hours.

Prerequisites

- Verify that you have a dedicated SFTP server for storing the Cloud Foundation configuration backup files. It is recommended that the SFTP server be outside the Cloud Foundation system.
- Because the backed-up information is critical, verify that your SFTP is secure and hardened.

Automatic Backups

In addition to scheduled and manual backups, SDDC Manager automatically triggers backups after any of the following operations are completed:

- Password rotation
- Creation, deletion, or expansion of a domain
- Add a host
- Add a rack
- Decommission of a host

What Information Gets Backed Up

This process backs up the following configurations from Cloud Foundation.

Type	Description
Credentials	Authorization information (such as IP addresses, system aliases, usernames and passwords) of the Cloud Foundation components (Platform Services Controller, vCenter Server, NSX, switches, and so on).
Host inventory	Information about each ESXi host in the Cloud Foundation system including IP address, host name, domain type, and so on.
Cloud Foundation bundle information	The Cloud Foundation bundle release number.

Type	Description
NSX Manager configuration settings	Information including version, IP address, and backup setting configuration of all NSX Managers in the Management Domain.
Switch configurations	Information including all the physical switch configurations.

Note Save the configuration settings; you may need this information to recover management VMs after a hardware failure or data corruption.

Note An alert gets generated if the backup parameters have not been configured by user.

Schedule Cloud Foundation Configuration Backups in SDDC Manager

You can configure scheduled backups of the Cloud Foundation configuration directly in SDDC Manager. You can also manually trigger backups. You can access and view the backup files.

Procedure

- 1 In the the SDDC Manager Dashboard, navigate to **Settings > Configuration Backup**.
The Configuration Backup page displays.
- 2 Click **Backup Settings**.
- 3 Click **Edit** at the top of page.
- 4 Configure the parameters for manual and scheduled backups of the Cloud Foundation configuration.

Parameter	Description
SFTP Server Address	Specify the IP address for the SFTP server.
Server Key Fingerprint	Confirm the server key fingerprint for the SFTP server.
Transfer Protocol	Select the transfer protocol, based on what the destination supports. The default is SFTP .
Port	Specify the port number for the SFTP server. The default is 22 .
User Name	Specify a username for authenticating access to the SFTP site.
Backup Directory	Specify the directory path where backups are stored on the SFTP site.
Encryption Pass Phrase	Specify a pass phrase for authenticating access to the SFTP site. The pass phrase must include at least one digit.

- 5 Complete the Backup Job Parameters section to schedule the backup.

Parameter	Description
Backup Frequency	Select the frequency to set how often the backup is made. You can specify DAILY or WEEKLY .
Time	Specify the hour to trigger the backup.
Retention Count	Specify the number of backups (1 – 200) to be retained in the SFTP site.

- 6 Click **Save Edits** at the top of page.

What to do next

- [View History of Cloud Foundation Configuration Backups](#)
- [Manually Trigger a Backup of the Cloud Foundation Configuration in SDDC Manager](#)

View History of Cloud Foundation Configuration Backups

The History page lists records of all the backups currently retained on the SFTP server.

Procedure

- 1 In the SDDC Manager Dashboard, navigate to **Settings > Configuration Backup**.
The Configuration Backup page displays.
- 2 Click **History**.

Manually Trigger a Backup of the Cloud Foundation Configuration in SDDC Manager

In addition to backups triggered by schedule, you can manually trigger a backup.

Prerequisites

You must have already configured the backup parameters as described in [Schedule Cloud Foundation Configuration Backups in SDDC Manager](#).

Procedure

- 1 In the SDDC Manager Dashboard, navigate to **Settings > Configuration Backup**.
The Configuration Backup page displays.
- 2 Click **History**.
- 3 Click **Backup Now** at the top of page.

The backup is triggered. When finished, the record of the backup appears in the list of backups on the same page.

CLI Commands for Backing Up Cloud Foundation Configuration

Run the following commands from the `/home/vrack/bin` directory of the SDDC Manager VM.

Command	Description
<code>backup-configure</code>	<p>Configures the settings for manual and scheduled backups of the Cloud Foundation configuration. When using this command, you are prompted to define the following parameters:</p> <ul style="list-style-type: none"> Server IP for the SFTP server. Server Key Fingerprint for the SFTP server. Port Number for the SFTP server. Default is 22. Username for authenticating access to the SFTP site. Password for authenticating access to the SFTP site. Path of backup folder specifies the directory path where backups are stored on the SFTP site. Protocol for the transfer protocol, based on what the destination supports. The default is SFTP. Backup Frequency to set how often the backup is made. You can specify DAILY or WEEKLY. Hour of Day to trigger the backup. Specify a value between 0 and 23. Minutes after the specified hour to trigger the backup. Specify a value between 0 and 59. Number of backups to retain specifies the number of backups to be retained in the SFTP site. Retention count must be in the range 1 – 200. <p>Note Backups are deleted on a first-in-first-out basis.</p> <ul style="list-style-type: none"> Passphrase for encryption to encrypt the backup file. <p>After entering the last parameter, the command should return a "status": "SUCCEEDED" message.</p>
<code>backup-history</code>	Outputs detailed status about the last thirty days of backup operations.
<code>backup-list</code>	<p>Outputs a detailed list of the current backup files on the backup location, including:</p> <ul style="list-style-type: none"> <code>backupType</code> displays, for example, if the backup was initiated manually or scheduled <code>backupFileName</code> displays the backup filename <code>backupFileSize</code> displays the size value of the backup file <code>backupFileSizeUnitType</code> indicates the unit in which the file size is measured, for example MB or GB <code>time</code> displays the time the backup file was created
<code>backup-now</code>	<p>Manually triggers an on-demand backup of the Cloud Foundation configuration settings. After completion, the command should return a status message and <code>workFlowId</code> value. For example:</p> <pre>{ "status": "IN_PROGRESS", "workFlowId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", }</pre>

Command	Description
backup-settings	<p>Outputs the current backup settings. For example:</p> <pre>{ "username": "backupuser", "directoryPath": "backuppah", "protocol": "SFTP", "backupSchedule": { "hourOfDay": 10, "minuteOfDay": 10, "scheduleType": "DAILY" }, "lastModifiedDate": "21-Jul-2017 08:52:08", "retentionCount": 2, "server": "10.0.0.5", "serverPort": 22, "createdDate": "14-Jul-2017 12:00:00" }</pre>
backup-settings-delete	<p>Deletes the current backup settings.</p> <p>After confirming the request, the command should return a "status": "SUCCEEDED" message.</p>

Access and View Cloud Foundation Configuration Backup File Contents

You can view the contents of the Cloud Foundation configuration backup file by downloading the file from the dedicated SFTP server to a local directory, then decompressing and decrypting the contents.

Prerequisites

- Verify that you have updated your local JRE with the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.

Because the backup file uses 256-bit AES encryption, you must have the JCE policy files installed in your local JRE installation to decrypt them. You can download the JCE policy files from <http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html>.

After you download them, add the JCE policy files to your local JRE security folder (JDK_HOME/jre/lib/security). This requires overwriting the existing files in the security folder.

- Verify that you have downloaded and added the Bouncy Castle `bcprov-jdk15on-*.jar` file into your `JDK_HOME/jre/lib/ext` directory.

If this JAR file is not available, you will receive a WARNING message when you try to run the `decrypt-util.jar` utility.

Procedure

- Copy the backup file (`SDDCManager-Config_timestamp.tar.gz`) from its location on the SFTP server to a local directory.
- Decompress the `SDDCManager-Config_timestamp.tar.gz` file.

The decompressed `tar` file contains the `decrypt-util.jar` utility, four encrypted JSON files, and a switch directory containing backups of all switches in the rack.

- `credentials-timestamp.json`

- host-info-timestamp.json
- vcf-bundle-version-timestamp.json
- nsx-manager-config.json
- switch directory

3 Run the `decrypt-util.jar` utility to decrypt the encrypted files.

```
[Local Directory]\SDDCManager-Config_timestamp.tar\SDDCManager-Config_timestamp> \  
java -jar decrypt-util.jar
```

The CLI displays the contents of the tar file and prompts you to proceed. For example:

```
The following encrypted files are available in the current directory  
1 - credentials-timestamp.json  
2 - host-info-timestamp.json  
3 - vcf-bundle-version-timestamp.json
```

4 Enter Y to proceed.

5 When prompted, enter the password that was specified when the backup was configured.

```
Enter Pass Phrase ( must match the one entered during backup configuration ):
```

The files are decrypted and copied to a new subdirectory with the same name as the original tar file, for example `SDDCManager-Config_timestamp`.

A decrypted file with extension (`.txt`) is generated for each of the encrypted JSON files (`.json`) in the same folder. The contents of the decrypted files are written in JSON format and it is recommended you view them using a JSON editor.

Managing Users and Groups

You can manage users and groups using the User Management page of the SDDC Manager Dashboard. SDDC Manager provides role-based access control.

For an overview of the User Management page, see [Tour of the SDDC Manager User Interface](#).

Authentication to the SDDC Manager Dashboard uses the VMware vCenter[®] Single Sign-On authentication service that is installed with the Platform Services Controller feature during the bring-up process for your Cloud Foundation system. This authentication service constructs an internal security domain based on the values entered during the bring-up process, and the SDDC Manager is registered in that domain. The service can authenticate users from a set of users and groups that you manually configure in the environment or it can connect to trusted external directory services such as Microsoft Active Directory. Using roles, authenticated users are given permissions to operate within SDDC Manager, according to the assignments you specify using SDDC Manager.

SDDC Manager uses roles, and their associated rights, to determine which users and groups can perform which operations. System administrators can assign roles to users and groups.

This chapter includes the following topics:

- [Active Directory and the Cloud Foundation system](#)
- [Add Local Users and Groups](#)
- [Assign Permissions to Users and Groups](#)
- [Add System Administrators](#)
- [Role-Based Access Control](#)
- [User Passwords in Your Cloud Foundation System](#)

Active Directory and the Cloud Foundation system

To allow the users and groups in your Microsoft Active Directory domain to use their credentials to log in to the SDDC Manager Dashboard as well as the vCenter Server instances that are deployed in your Cloud Foundation system, you configure your Active Directory domain as an identity source for the authentication services.

The Platform Services Controller component provides the single sign-on capability for the vCenter Server Single Sign-On authentication service. During the system's bring-up process, you enter your root domain, domain name server (DNS) subdomain, and single sign-on domain information in the configuration wizard. When you intend to use your Active Directory domain as identity sources for logging into SDDC Manager and to the vCenter Server instances, you typically enter **vsphere.local** in the configuration wizard as the Platform Services Controller single sign-on domain. Once the software stack is deployed, you can log in using the superuser account created during bring-up, and then configure your Active Directory domain as an identity source.

After you configure your Active Directory domain as an identity source, the users and groups in the joined Active Directory domain become available to grant permissions to users and groups for logging in to the Web interfaces using their Active Directory credentials:

- You grant permissions for logging in to the SDDC Manager Dashboard by assigning roles provided by the SDDC Manager role-based access control capabilities. See [Assign Permissions to Users and Groups](#) and [Role-Based Access Control](#).
- You can grant permissions for logging in to the vSphere Web Client and to access all of the software components that are integrated with vSphere in Cloud Foundation by assigning roles using the Global Permissions feature in the vSphere Web Client. See [Grant Permission to Active Directory Users and Groups to Log in to the vSphere Web Client in Your Cloud Foundation System](#).

Configure an Active Directory Domain as an Identity Source for your Cloud Foundation System

Use the vSphere Web Client to log in to the management domain's vCenter Server Appliance and configure your Active Directory domain as an identity source used by the authentication service. When your Active Directory domain is configured as an identity source, you can grant permissions to those users and groups to log in to the SDDC Manager Dashboard and access the system, as well as grant permissions to log in to the vSphere Web Client using their Active Directory credentials.

Prerequisites

If you have two instances of Cloud Foundation deployed in your organization, configure Active Directory as an LDAP identity source in both instances

Verify that you are logged in to the SDDC Manager Dashboard as an administrator. You can launch the vSphere Web Client from SDDC Manager.

Verify that you have the information for joining the management domain's Platform Services Controller component to your Active Directory domain:

- The Active Directory domain name, such as example.com.
- A user name in User Principal Name (UPN) format, such as User1@example.com, of a user that has a minimum of read access in the Active Directory domain.

If your Active Directory is Windows 2008 and you will be using the Administrator account here, ensure that the Administrator account properties has the domain selected for the user logon name on the **Account** tab in the account's properties.

- Password of that user.

Procedure

1 Open the view of the management domain's vCenter Server resources in the vSphere Web Client.

- a In the SDDC Manager Dashboard, navigate from the Dashboard page to view the management domain details.

You drill down into the management domain details from the Workload Domains area on the dashboard.

- b On the General Info page of the management domain's Domain Details screen, locate the **vCenter** launch link used to open the view of the domain's vCenter Server resources in the vSphere Web Client.

One way to navigate to the management domain's General Info page from the Workload Domains page is to click **List View** and click the active link that is the name of the management domain.

- c Launch the vSphere Web Client by clicking the **vCenter** launch link.

The vSphere Web Client appears in a new browser tab, authenticated and accessing the management domain's vCenter Server resources.

2 In the vSphere Web Client, navigate to **Administration > Deployment > System Configuration > Nodes**.

3 Select the node for the psc-1 node.

4 On the **Manage** tab, navigate to **Settings > Advanced > Active Directory**.

5 Click **Join**.

6 Type your Active Directory details.

Option	Description
Domain	Active Directory domain name, for example, example.com. Do not provide an IP address in this field.
Organizational unit	Optional. The canonical name of the organizational unit, for example, mydomain.com/MyOrganizationalUnit/mycomputer. Important Use this field only if you are familiar with LDAP.
User name	User name in User Principal Name (UPN) format, for example, jchin@mydomain.com. This user must have a minimum of read access. Important Down-level login name format, for example, DOMAIN\UserName, is unsupported. Ensure the Active Directory account's properties has the @domain format specified for the login name.
Password	Password of the user.

7 Click **OK** to join the psc-1 Platform Services Controller to the Active Directory domain.

The operation silently succeeds and you can see that the **Join** button turned to **Leave**.

- 8 Right-click the node you edited and select **Reboot** to restart the psc-1 Platform Services Controller so that the changes are applied.

Important If you do not restart the appliance, you might encounter problems in the vSphere Web Client.

- 9 Select the node for the psc-2 node.
- 10 Repeat the steps to join the psc-2 node to the Active Directory domain.
- 11 Navigate to **Administration > Single Sign-On > Configuration**.
- 12 On the **Identity Sources** tab, click the **Add Identity Source** icon.
- 13 Select **Active Directory (Integrated Windows Authentication)**, enter the identity source settings of the joined Active Directory domain

For example, type the joined Active Directory name in the **Domain name** field and select **Use machine account**.
- 14 Click **OK**.

On the **Identity Sources** tab, you can see the joined Active Directory domain.

What to do next

- Use the SDDC Manager Dashboard to grant the appropriate permissions to the Active Directory domain's users and groups for accessing your system using their Active Directory credentials. See [Assign Permissions to Users and Groups](#).
- Use the vSphere Web Client to grant the appropriate permissions to the users and groups from the joined Active Directory domain to use their Active Directory credentials to log in to the vSphere Web Client. Otherwise, those users and groups are not able to log in to the vSphere Web Client and the products that integrate with it using their Active Directory credentials. For information about managing permissions and user management in vCenter Server, see *vSphere 6.0 Security Guide* located at <https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html>.

Grant Permission to Active Directory Users and Groups to Log in to the vSphere Web Client in Your Cloud Foundation System

To allow your Active Directory users and groups to log in to the vSphere Web Client using their Active Directory credentials and access the vCenter Server objects and the objects from the vSphere products that integrate with the vSphere Web Client, you can use the Global Permissions area in the vSphere Web Client to grant them the appropriate permissions. This would give the users and groups access to all current and future workload domains. Do not use this feature if you want to provide the users or groups limited access to a single workload domain.

The ability to log in to the vSphere Web Client, access inventory objects, and perform operations on those objects is granted by the rights associated with the role that is assigned to the user or group.

Prerequisites

Add the Active Directory as an identity source by following the steps in [Configure an Active Directory Domain as an Identity Source for your Cloud Foundation System](#).

Procedure

- 1 Open the view of the management domain's vCenter Server resources in the vSphere Web Client.
 - a In the SDDC Manager Dashboard, navigate from the Dashboard page to view the management domain details.

You drill down into the management domain details from the Workload Domains area on the dashboard.
 - b On the General Info page of the management domain's Domain Details screen, locate the **vCenter** launch link used to open the view of the domain's vCenter Server resources in the vSphere Web Client.

One way to navigate to the management domain's General Info page from the Workload Domains page is to click **List View** and click the active link that is the name of the management domain.
 - c Launch the vSphere Web Client by clicking the **vCenter** launch link.

The vSphere Web Client appears in a new browser tab, authenticated and accessing the management domain's vCenter Server resources.
- 2 Navigate to **Administration > Access Control > Global Permissions > Manage**.
- 3 On the **Manage** tab, add a user or group to the list by clicking the add (+) icon.
- 4 In the Global Permission Root - Add Permission window, select the users and groups to which you want to grant permissions.
 - a At the bottom of the Users and Groups column, click **Add**.

The Select Users/Groups window appears.
 - b Select your Active Directory domain in the **Domain** drop-down list.
 - c Use the selection list and the **Add** button to add the names of users and groups to the **Users** and **Groups** fields.
 - d Click **OK** to complete adding the selected users and groups to the Users and Groups column in the Global Permission Root - Add Permission window.
- 5 Assign a role to users and groups.
 - a Select the users and groups in the Users and Groups column.
 - b In the Assigned Role column, select the role that you want to assign to the selected users and groups.
 - c Select the **Propagate to children** checkbox.
- 6 When you have assigned the desired roles to the users and groups, click **OK**.

The users and groups are listed on the **Manage** tab and show their assigned roles.

For more information about managing permissions and user management in vCenter Server, see the *vSphere 6.0 Security Guide* located at <https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html>.

Add Local Users and Groups

Use the vSphere Web Client to add local users and groups. These users and groups are internal to the vCenter Single Sign-On authentication service in the Cloud Foundation software stack.

The Platform Services Controller component provides the single sign-on capability in the software stack, including SDDC Manager. Before you can authorize users and groups to perform operations using SDDC Manager, you must include them into the set of users and groups authorized by the Platform Services Controller component by either adding your Active Directory domain as an identity source or adding them as users and groups to the internal identity source. The internal identity source is the internal single sign-on domain. When added to the internal single sign-on domain, these users and groups are local to your Cloud Foundation system.

Prerequisites

Verify that you are logged in to the SDDC Manager Dashboard as an administrator. You access the user interface to add local users and groups by launching the vSphere Web Client from the SDDC Manager Dashboard.

Procedure

1 Open the view of the management domain's vCenter Server resources in the vSphere Web Client.

- a In the SDDC Manager Dashboard, navigate from the Dashboard page to view the management domain details.

You drill down into the management domain details from the Workload Domains area on the dashboard.

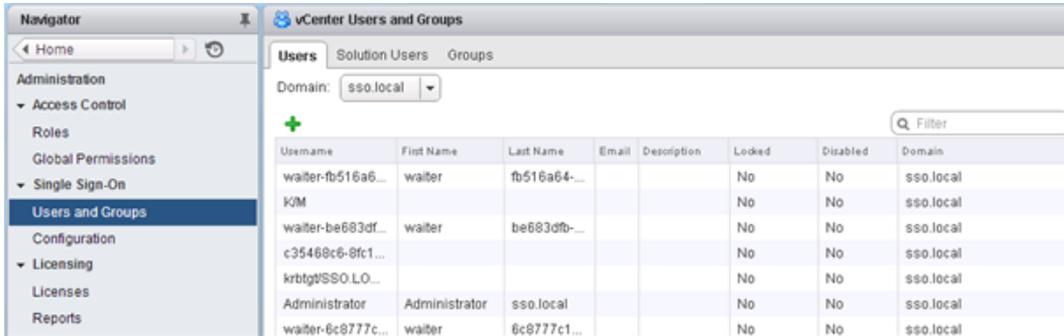
- b On the General Info page of the management domain's Domain Details screen, locate the **vCenter** launch link used to open the view of the domain's vCenter Server resources in the vSphere Web Client.

One way to navigate to the management domain's General Info page from the Workload Domains page is to click **List View** and click the active link that is the name of the management domain.

- c Launch the vSphere Web Client by clicking the **vCenter** launch link.

The vSphere Web Client appears in a new browser tab, authenticated and accessing the management domain's vCenter Server resources.

2 Navigate to **Administration > Single Sign-On > Users and Groups**.



3 Perform one of the following actions.

Option	Description
Add a local user	<p>On the Users tab, select your rack's local single sign-on domain and click Add. Type in the user's information, such as the user name and password, and click OK.</p> <p>The password must meet the password policy requirements for the software stack.</p> <p>Important Because you cannot change the user name after you create a user, make sure the user name is typed in correctly before clicking OK.</p>
Add a local group	<p>On the Groups tab, select your rack's local single sign-on domain and click Add. Type in a name for the group and optionally a description, and click OK.</p> <p>Important Because you cannot change the group name after you create a group, make sure the name is typed in correctly before clicking OK.</p>

What to do next

When you add a user, that user initially has no privileges to perform management operations in your system. Perform one of the following next steps.

- Add the local user to a group using the Platform Services Controller Web interface. When users are added to a group, you can assign permissions to the group so that all of the users in the group receive the same permissions for performing operations in your system. Then use the User Management page in the SDDC Manager Dashboard to assign a role to that group.
- Use the User Management page to authorize the local user for performing operations in your system by assigning an appropriate role to that user. See [Assign Permissions to Users and Groups](#).

Assign Permissions to Users and Groups

SDDC Manager uses roles, and their associated rights, to determine which users and groups can perform which operations using SDDC Manager.

System administrators assign roles to users and groups using the Permissions area of the User Management page. The ability to perform operations is granted by the rights associated with the role that is assigned to the user or group.

Prerequisites

Verify the user or group is present and enabled for access in the management domain's identity sources. Only such users and groups can be assigned permissions to access the SDDC Manager Dashboard. See [Active Directory and the Cloud Foundation system](#), [Configure an Active Directory Domain as an Identity Source for your Cloud Foundation System](#), and [Add Local Users and Groups](#).

Procedure

1 In the SDDC Manager Dashboard, navigate to **User Management > Users & Groups**.

2 Click **Add User/Group**.

The window displays fields to select users and groups that are known to SDDC Manager.

3 Select **User** or **Group** according to which type you are assigning permissions.

4 Select the domain that the user or group belongs to.

5 Use the filter field to display a list of users or groups.

- To display users or groups that match a set of characters, type those characters in the filter field and press Enter on your keyboard.
- To display all users or all groups, set your cursor in the filter field and press Enter on your keyboard.

A list of matching users or groups appears, according to your selections.

6 For each user or group, assign a role to the user or group.

Each role grants set of associated rights. The rights determine what operations can be performed using the SDDC Manager Dashboard. When you assign a role to a user or group, that user or group is granted that role's associated rights.

7 Click **Save** to save the changes.

The users and groups to which you assigned a role now have permissions to perform the operations governed by their assigned roles.

Add System Administrators

You can add system administrators for your Cloud Foundation system by giving user accounts the Admin role in SDDC Manager.

Giving a user account the Admin role gives that user the privileges to perform all of the operations that are performed using SDDC Manager.

Prerequisites

Verify the user is present and enabled for access in the management domain's identity sources. Only such users and groups can be assigned permissions to log in to the SDDC Manager Dashboard. See [Active Directory and the Cloud Foundation system](#), [Configure an Active Directory Domain as an Identity Source for your Cloud Foundation System](#), and [Add Local Users and Groups](#).

Procedure

- 1 In the SDDC Manager Dashboard, navigate to **User Management > Users & Groups**.
- 2 Assign the Admin role to the user.
 - If the user name is listed on the Users & Groups page, because the user is already assigned a role, edit the Users & Groups page to change the user's role to the Admin role. Enable the page for editing by clicking the edit icon, change the user's role to the Admin role, and save the changes.
 - If the user name is not listed on the Users & Groups page, because the user is not yet assigned a role, click Add User/Group to locate the user, assign the role, and save the changes.

Note The Admin role has the description Super Admin.

The user can now log in to SDDC Manager and perform system administrator operations. Once added, a user cannot be deleted.

Role-Based Access Control

SDDC Manager uses roles and rights to determine what operations a user can perform using SDDC Manager. SDDC Manager includes a number of predefined roles with specific rights.

System administrators must assign a role to each user or group before that user or group can log in to the SDDC Manager Dashboard and access operations.

Two predefined roles are provided by default: an administrator-level role and a read-only role. The administrator-level role grants all rights to perform SDDC Manager operations. The read-only role grants read-only rights.

An auditor can use the predefined read-only role to view security and non-security configurations and logs.

The predefined roles cannot be modified.

To view the rights granted by one of the predefined roles, navigate to **User Management > Roles & Permissions** and select the role name that is displayed.

User Passwords in Your Cloud Foundation System

The password restrictions, lockout, and expiration for a user's password in your Cloud Foundation system depend on the user's domain, on who the user is, and the policy settings.

The vCenter Single Sign-On authentication service manages authentication for all users who log in to SDDC Manager and various other SDDC components' Web interfaces that you use to perform administrative tasks in your SDDC, for example as the vSphere Web Client.

Local Users

The passwords for users of the system's single sign-on (SSO) domain's internal identity source that is created during the software stack's bring-up process must follow the restrictions set by the vCenter Single Sign-On password policy and lockout policy. In the vSphere Web Client, use the **Policies** tab of Configuration page to view the current settings. These passwords expire 90 days by default, though system administrators can change the expiration as part of the password policy.

Users Provided by Other Identity Sources

For users that are provided to the SSO domain by identity sources such as your joined Active Directory domain, the password restrictions, lockout, and expiration are determined by the domain to which the user can authenticate. In the vSphere Web Client, use the **Identity Sources** tab of the Configuration page to view the current identity sources. When users log in as a user in one of these domains, they include the domain name in the log in name, such as *user@domain*. The domain's password parameters apply in this situation.

Modify Password Policy for Users

For users in the single sign-on (SSO) domain's internal identity source, the password policy for accessing various Web interfaces that you use to perform SDDC tasks in your Cloud Foundation system is governed by the vCenter Single Sign-On password policy. This policy is a set of rules and restrictions on the format and expiration of vCenter Single Sign-On user passwords.

The vCenter Single Sign-On password policy applies only to users in the single sign-on (SSO) domain that was created during your system's bring-up process. If you have configured your system to use another identity provider, the password policy of that identity provider applies instead. The name of the SSO domain was specified in the bring-up wizard. See *VMware Cloud Foundation Overview and Bring-Up Guide* for details about the fields in the bring-up wizard.

Note By default, vCenter Single Sign-On passwords expire after 90 days. You can reset an expired password if you know the old password.

Prerequisites

Verify that you are logged in to SDDC Manager as an administrator. You access the internal identity source by launching the vSphere Web Client from the SDDC Manager Dashboard.

Procedure

- 1 Open the view of the management domain's vCenter Server resources in the vSphere Web Client.
 - a In the SDDC Manager Dashboard, navigate from the Dashboard page to view the management domain details.

You drill down into the management domain details from the Workload Domains area on the dashboard.

- b On the General Info page of the management domain's Domain Details screen, locate the **vCenter** launch link used to open the view of the domain's vCenter Server resources in the vSphere Web Client.

One way to navigate to the management domain's General Info page from the Workload Domains page is to click **List View** and click the active link that is the name of the management domain.

- c Launch the vSphere Web Client by clicking the **vCenter** launch link.

The vSphere Web Client appears in a new browser tab, authenticated and accessing the management domain's vCenter Server resources.

- 2 Navigate to **Administration > Single Sign-On > Configuration > Policies > Password Policies**.

The Password Policies tab displays the current settings. After the bring-up process, the default password policy parameters are:

Option	Description
Maximum lifetime	Password must be changed every 90 days
Restrict re-use	Users cannot reuse any previous 5 passwords
Maximum length	20
Minimum length	8
Character requirements	<ul style="list-style-type: none"> ■ At least 1 special character ■ At least 2 alphabetic characters ■ At least 1 uppercase character ■ At least 1 lowercase character ■ At least 1 numeric character ■ Identical adjacent characters: 3

- 3 Click **Edit**.
- 4 Edit the password policy parameters.

Option	Description
Description	Password policy description.
Maximum lifetime	Maximum number of days that a password can exist before the user must change it.
Restrict reuse	Number of the user's previous passwords that cannot be selected. For example, if a user cannot reuse any of the last six passwords, type 6.
Maximum length	Maximum number of characters that are allowed in the password.

Option	Description
Minimum length	Minimum number of characters required in the password. The minimum length must be no less than the combined minimum of alphabetic, numeric, and special character requirements.
Character requirements	Minimum number of different character types that are required in the password. You can specify the number of each type of character: <ul style="list-style-type: none">■ Special characters, such as & # %■ Alphabetic characters, such as A b c D■ Uppercase characters, such as A B C■ Lowercase characters, such as a b c■ Numeric characters, such as 1 2 3 The minimum number of alphabetic characters must be no less than the combined uppercase and lowercase requirements.
Identical adjacent characters	Maximum number of identical adjacent characters that are allowed in the password. The number must be greater than 0. For example, if you enter 1, the following password is not allowed: p@\$\$word.

5 Click **OK**.

Managing Physical Resources

From the Dashboard page of the SDDC Manager, you can work with the physical resources in your Cloud Foundation system.

The Dashboard page displays high-level information about your system's physical resources, such as the number of physical racks.

From the Dashboard page, you drill-down to the level of the hosts and switches by using the **View Details** button.

The List view displays the list of physical racks that are in your system. To see detailed information about the physical switches and hosts for a particular rack in the list, click the rack's name. For an alternative view of the physical rack information, you can use the Map view.

The details page for a specific rack lists the switches and hosts in that rack. In the rack's details page, you can click the name of a switch or host to view its details or to perform operations on it.

- [Switch Details and Operations](#)
- [ESXi Host Details and Operations](#)

SDDC Manager monitors the hardware health of the switches and hosts and reports each one's health status using these icons. On the rack's details page, the icons in the Status column indicate the hardware health state of each resource, each switch and host. The hardware health state of the resource is calculated based on the current set of alerts that SDDC Manager has raised for that hardware resource and the severities of those alerts, including any alerts on the hardware Field Replaceable Units (FRUs) contained within that resource.

Status Icon	Description
	The resource has no SDDC Manager alerts reported of warning, error, or critical severity.
	The resource has SDDC Manager alerts reported with warning severity.
	The resource has SDDC Manager alerts reported with error severity.
	The resource has SDDC Manager alerts reported with critical severity.
	The resource's health state cannot be determined, for example the resource is powered off.

To see the list of current alerts sorted by severity on a particular resource, open the resource's details page by clicking on its name and then clicking on **View Alerts** in its details page.

For information about the hardware-related alerts raised by SDDC Manager and information about the built-in monitoring capabilities, see:

- [SDDC Manager Alerts Raised During Ongoing Operations](#)
- [Chapter 10 Monitoring Capabilities in the Cloud Foundation System](#)

ESXi Host Details and Operations

Access an ESXi host's detailed information and the available operations you can perform on it by clicking its name.

The types of host information you can see in a host's details include:

- Host CPU, memory, storage
- Whether the host is powered on or off
- Management IP address of the host
- Network information
- Which management or workload domain the host is assigned to, if currently part of one
- Which rack the host is in
- Which vCenter Server instance is managing that host, if the host is currently part of a management or workload domain
- Hardware health status

The hardware health status reflects the severities of the SDDC Manager alerts currently raised on the ESXi host's underlying server and its hardware components. To examine the sorted-by-severity alert list, click **View Alerts**.

The available operations you can perform on a host are represented by the icons in the upper right corner and you can invoke an operation by clicking its icon.

Switch Details and Operations

In the Rack Details screen for a physical rack, you can see the role for each switch in that rack, whether the switch is a management, ToR, or inter-rack switch. By clicking a switch's name, you can drill down to see that switch's detailed information.

Note Inter-rack switches are available in an system that has two or more racks. Inter-rack switches are installed when a second rack is added to the first rack in an system.

The types of switch information you can see in a switch's details are:

- Management information, such as the switch's management IP address

- Firmware information
- Network information
- Hardware health status

The hardware health status reflects the severities of the SDDC Manager alerts currently raised on the switch and its components. To examine the sorted-by-severity alert list, click **View Alerts**.

This chapter includes the following topics:

- [Host Details and Operations](#)
- [Adding and Replacing Hosts](#)
- [Switch Details and Operations](#)
- [Replacing and Restoring Switches](#)

Host Details and Operations

Access an ESXi host's detailed information and the available operations you can perform on it by clicking its name.

The types of host information you can see in a host's details include:

- Host CPU, memory, storage
- Whether the host is powered on or off
- Management IP address of the host
- Network information
- Which management or workload domain the host is assigned to, if currently part of one
- Which rack the host is in
- Which vCenter Server instance is managing that host, if the host is currently part of a management or workload domain
- Hardware health status

The hardware health status reflects the severities of the SDDC Manager alerts currently raised on the ESXi host's underlying server and its hardware components. To examine the sorted-by-severity alert list, click **View Alerts**.

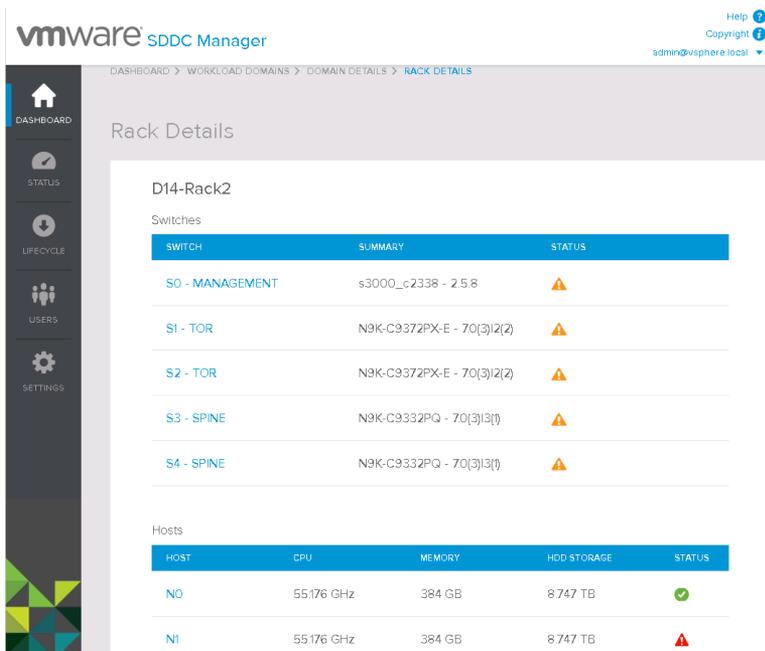
The available operations you can perform on a host are represented by the icons in the upper right corner and you can invoke an operation by clicking its icon.

Decommission an Unassigned Host

Use this procedure to decommission a host that does not belong to a workload domain.

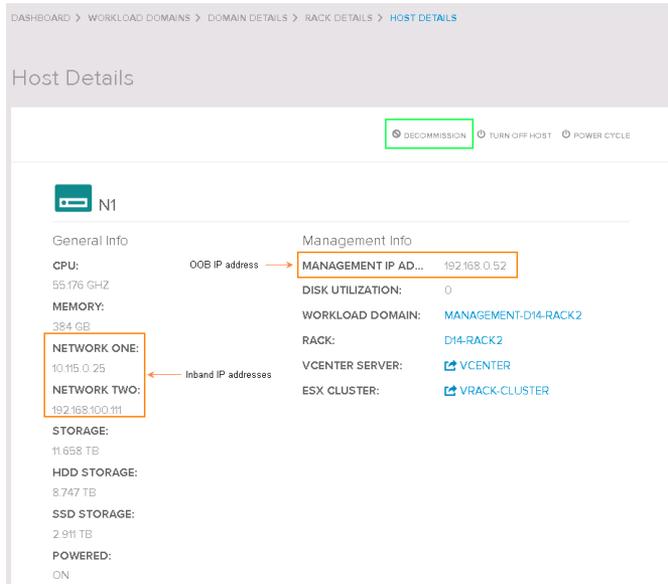
Procedure

- 1 If the host with the faulty component does not belong to a workload domain, retrieve the password of the host.
 - a In a command line window, SSH to the VM on the rack.
 - b Navigate to `/home/vrack/bin`.
 - c Type the following command:
`Lookup-password`
 - d Note the ESXi and IPMI passwords of the host that is to be decommissioned.
- 2 Decommission the dead host.
 - a If you are decommissioning a qualified vSAN Ready Node (i.e. if you did not purchase a fully integrated system from a partner), note the BMC password for the host by navigating to the `/home/vrack/bin/directory` in the SDDC Manager VM and running the `Lookup-password` command.
 - b On the Dashboard page, click **VIEW DETAILS** for **Workload Domain** and click the affected domain.
 - c In the **PHYSICAL RACKS** column, click the physical rack that contains the affected server.
 - d Scroll down to the **Hosts** section.
 - e In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).

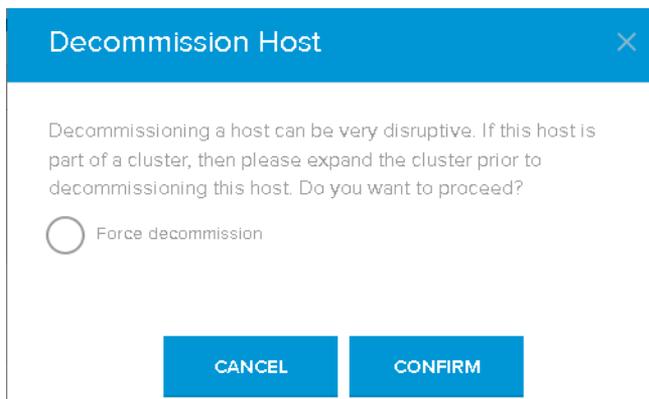


- f In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).

The Host Details page displays the details for this host.



- g In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).
- h Note the IP addresses displayed in the **NETWORK TWO** and **MANAGEMENT IP ADDRESS** fields.
- i Click **Decommission**.



If this host belongs to a workload domain, the domain must include at least 4 hosts. If the domain has fewer than 4 hosts, you must expand the domain before decommissioning the host. If the domain contains only 4 hosts and one of them is dead, click **Force decommission** to decommission the host.

- j Click **CONFIRM**.

During the host decommissioning task, the host is removed from the workload domain to which it was allocated and the environment's available capacity is updated to reflect the reduced capacity. The ports that were being used by the server are marked unused and the network configuration is updated.

- k Monitor the progress of the decommissioning task.

- 1 On the SDDC Manager Dashboard, click **STATUS** in the left navigation pane.

- 2 In the Workflow Tasks section, click **View Details**.

- 3 Look for the **VI Resource Pool - Decommission of hosts** task.

- 4 After about 10 minutes, refresh this page and wait till the task status changes to **Successful**.

- l For qualified vSAN Ready Nodes, change the password on the host to the common password for ESXi hosts. Log in to the BMC console using the password noted in step a and change the OOB password to D3c0mm1ss10n3d!.

This step is automated for hosts in an integrated system.

- 3 Turn on the chassis-identification LED on the host.

- a In a web browser, navigate to the OOB IP address that you noted earlier.

- b Login with your BMC user name and password.

- c Following the documentation from your vendor, turn on the chassis-identification LED.

The chassis-identification LED on the host starts to beacon (flashing on and off).

- 4 Power off the decommissioned host and remove it from the physical rack. Note the ports on the management and ToR switches it was connected to.

What to do next

Replace the failed component on the host as appropriate and add it back to the rack.

Adding and Replacing Hosts

You can add capacity to your Cloud Foundation stack by adding a new host or a previously decommissioned host. The inserted host behaves just as the existing hosts in the rack.

The procedure to replace a faulty host or a host with faulty components depends on whether the host is operational (reachable by vCenter Web Client) and the component that needs to be replaced.

- [Add a Host to a Physical Rack](#)

When you add a host to a physical rack, it is added to the capacity pool. You can then add it to the appropriate management or workload domain.

- [Replace Hosts and Hosts Components](#)

The replacement procedure depends on the component being replaced and the condition of the component.

Add a Host to a Physical Rack

When you add a host to a physical rack, it is added to the capacity pool. You can then add it to the appropriate management or workload domain.

Add a New Host to a Physical Rack

You can add capacity to your Cloud Foundation system depending on the power availability in the rack. You can then expand a workload domain to include the additional capacity. When you have a set of 3 hosts, you can create a new dedicated workload domain.

Prerequisites

The new host must be physically present at your site before you begin this procedure.

Note If the host was previously decommissioned, the ESXi password on the host would have been set to D3c0mm1ss10n3d!.

Procedure

- 1 Image the new host and download the inventory file. See *Image Individual Server* in *VIA User's Guide*.
- 2 Mount the new host in an empty slot on the rack and connect it to the management and ToR switches according to the wire map. See [Chapter 17 Rack Wiring](#).
- 3 Power on the new host.
- 4 On the SDDC Manager Dashboard, click **SETTINGS > Physical Rack Settings**.
- 5 Click the **Add Host** tab.
- 6 Select the rack to which you want to add the host.
- 7 Upload the manifest (inventory) file that you downloaded after the host was imaged.

After the host is discovered, the **Continue** button is enabled.

- 8 Click **Continue**.

The bring-up process is started on the host. If you move to another UI window, you must click **Continue** for the bring-up process to start. As each task is completed, a green arrow is displayed next to the task.

After bring-up is completed, a completion message is displayed.

- 9 Navigate to **Dashboard > Physical Resources > Physical Resources > Rack Details** and confirm that the newly added host is displayed here.

If the host is not visible on the SDDC Manager Dashboard, restart the SDDC Manager health service by running the following API call on the SDDC Manager VM:

```
curl -X PUT -d 'restart' http://localhost:8080/vrm-ui/api/1.0/health
```

The new host is now available for addition to workload domains.

Add a Previously Decommissioned Host to a Physical Rack

When you decommission a server, it is cleaned up as part of the workflow. However, a dead host or host with a failed SATADOM is not cleaned up during decommissioning.

Prerequisites

Ensure that the following has been completed on the decommissioned host before adding it to a physical rack.

- Verify that the decommissioned host has been re-imaged. See *Image Individual Server* in the *VIA User's Guide*.
- Verify that the manifest for the re-imaged host has been downloaded and is available. See *View Inventory* in the *VIA User's Guide*.
- Verify that the decommissioned host has a password on the host is EvoSddc!2016. This is the default password for all ESXi hosts.
- Verify that the decommissioned host has an IP address from the range 192.168.100.50 - 192.168.100.73.
- Verify that Secure Shell (SSH) is enabled.
- Verify that the firewall on the SSH host is enabled and connections are restricted to the 192.168.100.0/22 subnet.
- Verify that the DNS IP is set to 192.168.1.254.

The above prerequisites ensure that the decommissioned host has been recommissioned.

Procedure

- 1 Mount the recommissioned host in an empty slot on the rack and connect it to the management and ToR switches according to the wire map.

See [Chapter 17 Rack Wiring](#).

- 2 Start up the recommissioned host.
- 3 On the the SDDC Manager Dashboard, go to **SETTINGS > Physical Rack Settings**.
- 4 Click **Add Host**.
- 5 Select the rack to which you want to add the host.
- 6 Upload the manifest file that you downloaded after the host was imaged.
After the host is discovered, the **Continue** button is enabled.
- 7 Click **Continue**.

The bring-up process starts on the host. If you move to another UI window, you must click **Continue** for the bring-up process to start. As each task is completed, a green arrow appears next to the task.

After bring-up is completed, a completion message is displayed.

- 8 Navigate to **Dashboard > Physical Resources > Physical Resources > Rack Details** and confirm that the newly added host is displayed here.

If the host is not visible on the SDDC Manager Dashboard, restart the SDDC Manager health service:

- a Using SSH, log in as root to the SDDC Manager VM.
- b Run the following API call.

```
curl -X PUT -d 'restart' http://localhost:8080/vrm-ui/api/1.0/health
```

The recommissioned host is now available for addition to workload domains.

Replace Hosts and Hosts Components

The replacement procedure depends on the component being replaced and the condition of the component.

- [Replace Components of a Host Running in Degraded Mode](#)

- [Replace Dead Host or Host SAS Controller or Expander](#)

When the faulty host is not operational or when you need to replace the SAS controller or expander on a host, you must decommission the host before you remove it from the physical rack. The procedure you follow depends on whether the dead host belongs to a workload domain or is part of the capacity pool.

- [Replace SATADOM Disk on a Host](#)

This section describes the replacement procedure for a failed SATADOM disk on a host.

- [Move Disks from a Dead Host to a New Host](#)

If a host is dead, but the disks are still working (SATADOM, capacity, and cache drives), you can move the disks to a new host.

- [Replace Capacity Drive \(SSD or HDD\) or Cache Drive \(SSD\) in a Host](#)

You can replace the capacity drive in a host when you see an `Operation status is down for storage device` alert. The alert description says `SSD_DOWN_ALERT` or `HDD_DOWN_ALERT`.

Replace Components of a Host Running in Degraded Mode

Follow this procedure to replace the components of a server running in degraded mode. This procedure applies to the following components:

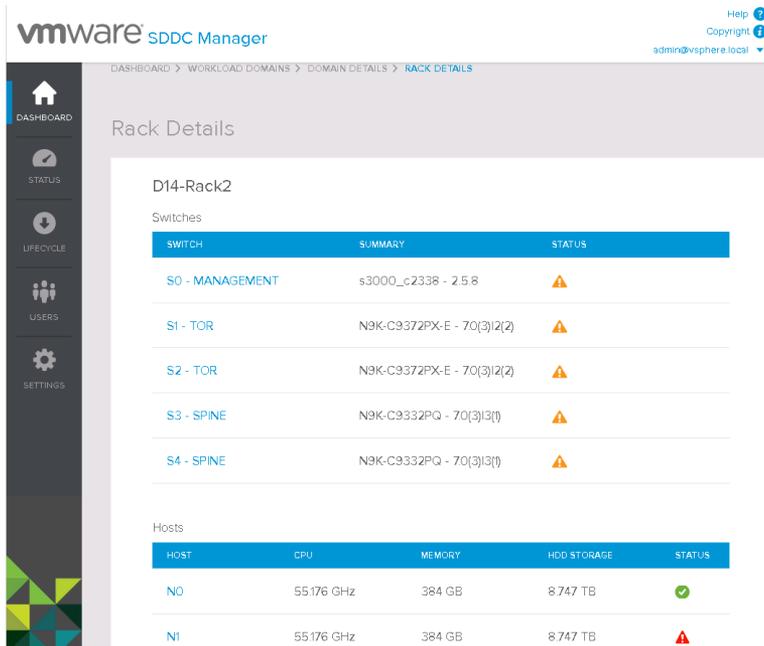
- CPU
- memory
- NIC
- power supply
- iDRAC

Prerequisites

- Host is operational and is reachable by vCenter Web Client.
- Management, vSAN, and vMotion networks must be available on the host
- The HDD and SSD disks on the host are in a good state.

Procedure

- 1 Log in to vSphere Web Client.
- 2 Right-click the affected host and click **Enter Maintenance Mode**.
- 3 If the host belongs to a domain, click **Full Data Migration**.
- 4 On the Dashboard page, click **VIEW DETAILS** for **Workload Domain** and click the affected domain.
- 5 Click the physical rack that contains the affected server.
- 6 Scroll down to the **Hosts** section.
- 7 In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).



The Host Details page displays the details for this host.

- 8 Click **TURN OFF HOST**.
- 9 Pull the host out of the physical rack. Note the ports on the management and ToR switches it was connected to.
- 10 Service the appropriate part.
- 11 Put the host back in the physical rack and connect it to the management and ToR switches.
- 12 Power on the host.

13 In vSphere Web Client, right-click the host and click **Exit Maintenance Mode**.

Replace Dead Host or Host SAS Controller or Expander

When the faulty host is not operational or when you need to replace the SAS controller or expander on a host, you must decommission the host before you remove it from the physical rack. The procedure you follow depends on whether the dead host belongs to a workload domain or is part of the capacity pool.

- [Replace a Dead Host that Belongs to a Workload Domain](#)

If you need to replace a dead host, you must remove the host from the physical rack. You can then add a new host or replace the failed component on the host and add it back.

- [Replace SAS Controller or Expander when Host Belongs to a Workload Domain](#)

If you need to replace a SAS controller or a SAS expander, you can do so without removing the host from the physical rack.

- [Replace Dead Host or SAS Controller or Expander when the Host does not Belong to a Workload Domain](#)

If you need to replace a SAS controller or a SAS expander that does not belong to workload domain, you must decommission the host and remove it from the physical rack.

Replace a Dead Host that Belongs to a Workload Domain

If you need to replace a dead host, you must remove the host from the physical rack. You can then add a new host or replace the failed component on the host and add it back.

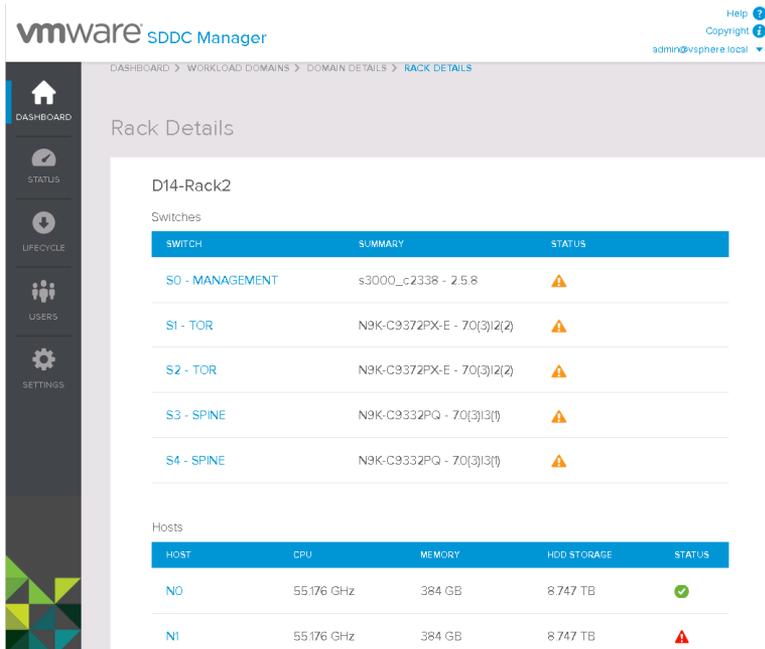
Prerequisites

Ensure that there are at least 4 hosts in the management or workload domain to which the faulty host belongs. If there are less than 4 hosts, add a host to the domain from the capacity pool if possible.

Procedure

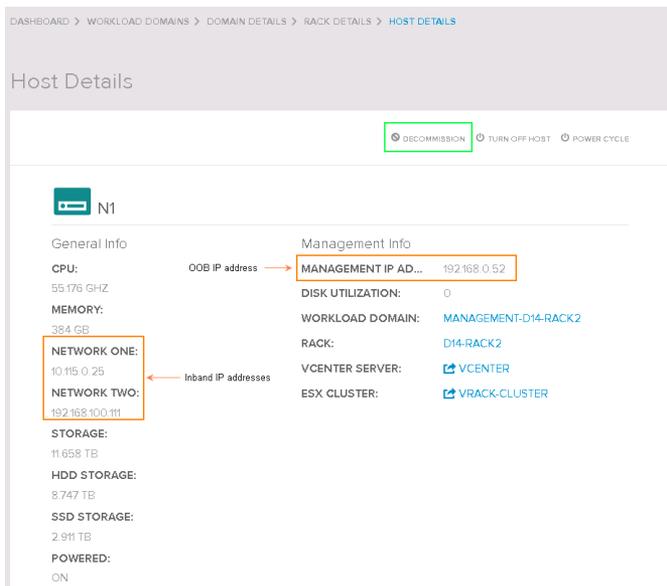
- 1 Decommission the host.
 - a If you are decommissioning a qualified vSAN Ready Node (i.e. if you did not purchase a fully integrated system from a partner), note the BMC password for the host by navigating to the `/home/vrack/bin/directory` in the SDDC Manager VM and running the `lookup-password` command.
 - b On the Dashboard page, click **VIEW DETAILS** for **Workload Domain** and click the affected domain.
 - c In the **PHYSICAL RACKS** column, click the physical rack that contains the affected server.
 - d Scroll down to the **Hosts** section.

- e In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).



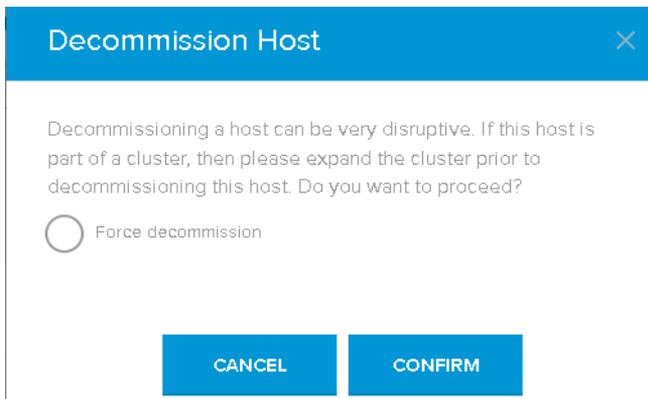
- f In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).

The Host Details page displays the details for this host.



- g In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).
- h Note the IP addresses displayed in the **NETWORK TWO** and **MANAGEMENT IP ADDRESS** fields.

- i Click **Decommission**.



If this host belongs to a workload domain, the domain must include at least 4 hosts. If the domain has fewer than 4 hosts, you must expand the domain before decommissioning the host. If the domain contains only 4 hosts and one of them is dead, click **Force decommission** to decommission the host.

- j Click **CONFIRM**.

During the host decommissioning task, the host is removed from the workload domain to which it was allocated and the environment's available capacity is updated to reflect the reduced capacity. The ports that were being used by the server are marked unused and the network configuration is updated.

- k Monitor the progress of the decommissioning task.

- 1 On the SDDC Manager Dashboard, click **STATUS** in the left navigation pane.
- 2 In the Workflow Tasks section, click **View Details**.
- 3 Look for the **VI Resource Pool - Decommission of hosts** task.
- 4 After about 10 minutes, refresh this page and wait till the task status changes to **Successful**.

- l For qualified vSAN Ready Nodes, change the password on the host to the common password for ESXi hosts. Log in to the BMC console using the password noted in step a and change the OOB password to D3c0mm1ss10n3d!.

This step is automated for hosts in an integrated system.

- 2 Turn on the chassis-identification LED on the host.

- a In a web browser, navigate to the OOB IP address that you noted down in step 6.
- b Login with your BMC user name and password.
- c Following the documentation from your vendor, turn on the chassis-identification LED.

The chassis-identification LED on the host starts to beacon (flashing on and off).

- 3 Power off the host and remove it from the physical rack. Note the ports on the management and ToR switches it was connected to.

What to do next

Replace the failed component on the host as appropriate and add it back to the rack. See [Add a Previously Decommissioned Host to a Physical Rack](#). For adding a new host, see [Add a New Host to a Physical Rack](#).

Replace SAS Controller or Expander when Host Belongs to a Workload Domain

If you need to replace a SAS controller or a SAS expander, you can do so without removing the host from the physical rack.

Prerequisites

Ensure that there are at least 4 hosts in the management or workload domain to which the faulty host belongs. If there are less than 4 hosts, add a host to the domain from the capacity pool if possible.

Procedure

- 1 Place the affected host in maintenance mode.
- 2 Add or update the driver for the new controller.
- 3 Shut down the host.
- 4 Replace the controller.

See [SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility](#) in the vSphere product documentation.

- 5 Restart the host.
- 6 Verify that the driver is properly loaded and used by the controller. All disks are seen, all disk groups are healthy.
For example, all disks are visible and all disk groups have a status of Healthy.
- 7 Take the host of maintenance mode.

Replace Dead Host or SAS Controller or Expander when the Host does not Belong to a Workload Domain

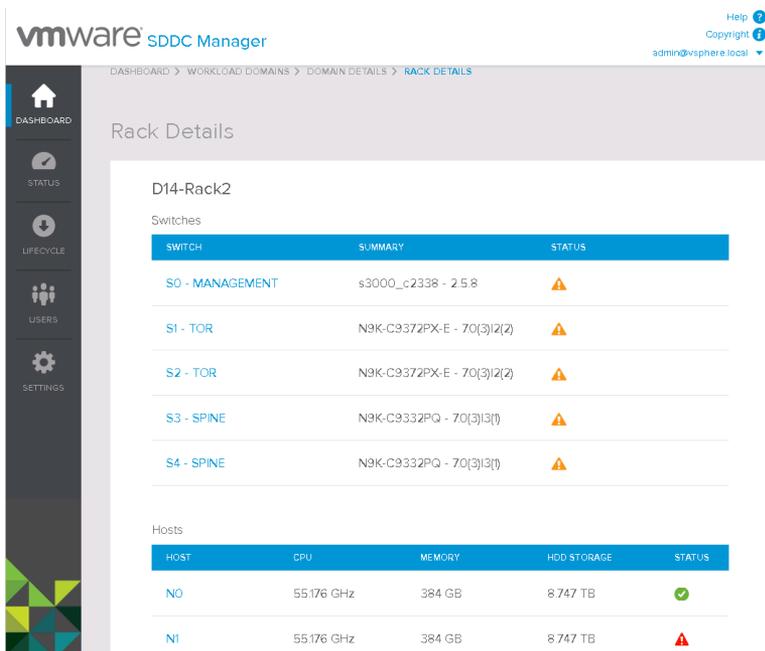
If you need to replace a SAS controller or a SAS expander that does not belong to workload domain, you must decommission the host and remove it from the physical rack.

Procedure

- 1 If the host with the faulty component does not belong to a workload domain, retrieve the password of the host.
 - a In a command line window, SSH to the VM on the rack.
 - b Navigate to `/home/vrack/bin`.
 - c Type the following command:
`lookup-password`
 - d Note the ESXi and IPMI passwords of the host that is to be decommissioned.

2 Decommission the dead host.

- a If you are decommissioning a qualified host (i.e. if you did not purchase a fully integrated system from a partner), note the BMC password for the host by navigating to the /home/vrack/bin/directory in the SDDC Manager VM and running the `Lookup-password` command.
- b On the Dashboard page, click **VIEW DETAILS** for **Workload Domain** and click the affected domain.
- c In the **PHYSICAL RACKS** column, click the physical rack that contains the affected server.
- d Scroll down to the **Hosts** section.
- e In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).

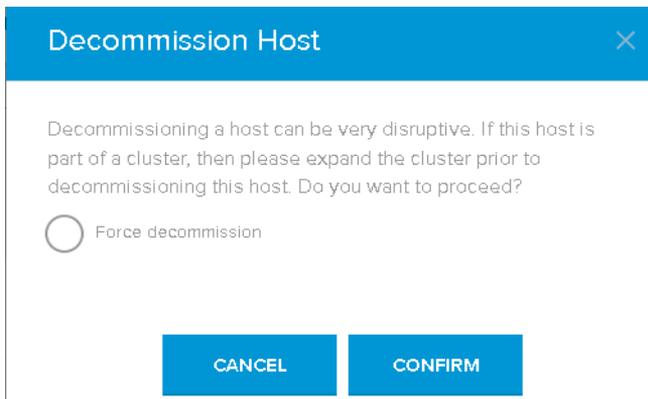


- f In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).

The Host Details page displays the details for this host.

- g In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).
- h Note the IP addresses displayed in the **NETWORK TWO** and **MANAGEMENT IP ADDRESS** fields.

- i Click **Decommission**.



- j Click **CONFIRM**.

- k Monitor the progress of the decommissioning task.

- 1 On the SDDC Manager Dashboard, click **STATUS** in the left navigation pane.
- 2 In the Workflow Tasks section, click **View Details**.
- 3 Look for the **VI Resource Pool - Decommission of hosts** task.
- 4 After about 10 minutes, refresh this page and wait till the task status changes to **Successful**.

- l For qualified servers, change the password on the host to the common password for ESXi hosts. Log in to the BMC console using the password noted in step a and change the OOB password to D3c0mm1ss10n3d!.

This step is automated for hosts in an integrated system.

- 3 Turn on the chassis-identification LED on the host.
 - a In a web browser, navigate to the OOB IP address that you noted earlier.
 - b Login with your BMC user name and password.
 - c Following the documentation from your vendor, turn on the chassis-identification LED.

The chassis-identification LED on the host starts to beacon (flashing on and off).

- 4 Power off the decommissioned host and remove it from the physical rack. Note the ports on the management and ToR switches it was connected to.

What to do next

Replace the failed component on the host as appropriate and add it back to the rack. For adding a new host, see [Add a New Host to a Physical Rack](#).

Replace SATADOM Disk on a Host

This section describes the replacement procedure for a failed SATADOM disk on a host.

Prerequisites

Ensure that there are at least 4 hosts in the management or workload domain to which the faulty host belongs. If there are less than 4 hosts, add a host to the domain from the capacity pool, if possible.

Procedure

- 1 Decommission the affected host.
 - a If you are decommissioning a qualified vSAN Ready Node (i.e. if you did not purchase a fully integrated system from a partner), note the BMC password for the host by navigating to the `/home/vrack/bin/directory` in the SDDC Manager VM and running the `lookup-password` command.
 - b On the Dashboard page, click **VIEW DETAILS** for **Workload Domain** and click the affected domain.
 - c In the **PHYSICAL RACKS** column, click the physical rack that contains the affected server.
 - d Scroll down to the **Hosts** section.
 - e In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).

The screenshot shows the VMware SDDC Manager interface. The breadcrumb trail is: DASHBOARD > WORKLOAD DOMAINS > DOMAIN DETAILS > RACK DETAILS. The page title is "Rack Details" for "D14-Rack2".

Switches

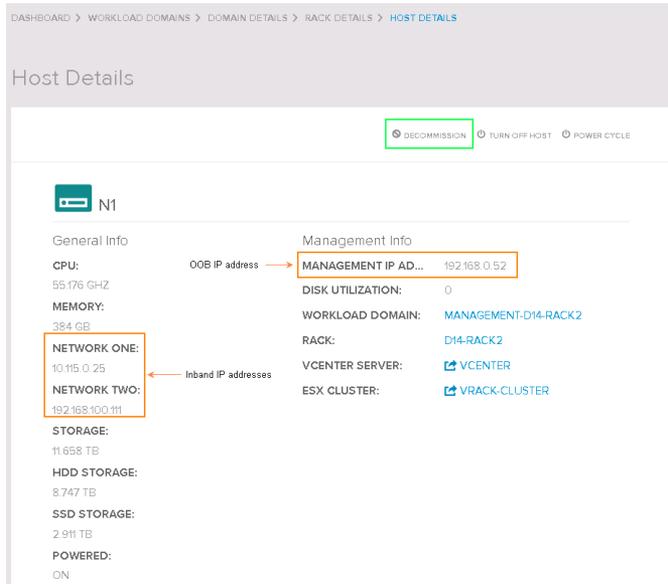
SWITCH	SUMMARY	STATUS
S0 - MANAGEMENT	s3000_c2338 - 2.5.8	⚠️
S1 - TOR	N9K-C9372PX-E - 70(3)12(2)	⚠️
S2 - TOR	N9K-C9372PX-E - 70(3)12(2)	⚠️
S3 - SPINE	N9K-C9332PQ - 70(3)13(1)	⚠️
S4 - SPINE	N9K-C9332PQ - 70(3)13(1)	⚠️

Hosts

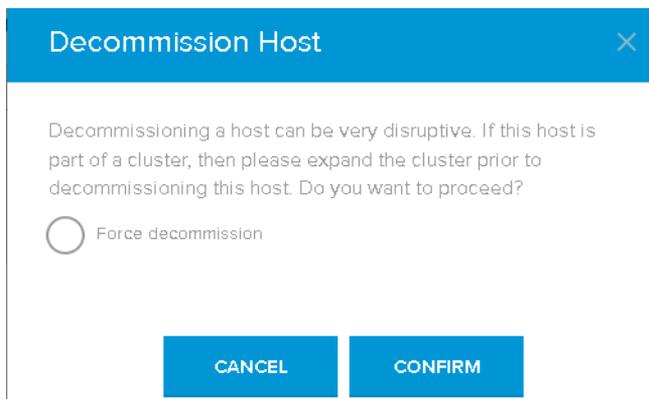
HOST	CPU	MEMORY	HDD STORAGE	STATUS
N0	55.176 GHz	384 GB	8.747 TB	✅
N1	55.176 GHz	384 GB	8.747 TB	⚠️

- f In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).

The Host Details page displays the details for this host.



- g In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).
- h Note the IP addresses displayed in the **NETWORK TWO** and **MANAGEMENT IP ADDRESS** fields.
- i Click **Decommission**.



If this host belongs to a workload domain, the domain must include at least 4 hosts. If the domain has fewer than 4 hosts, you must expand the domain before decommissioning the host. If the domain contains only 4 hosts and one of them is dead, click **Force decommission** to decommission the host.

- j Click **CONFIRM**.

During the host decommissioning task, the host is removed from the workload domain to which it was allocated and the environment's available capacity is updated to reflect the reduced capacity. The ports that were being used by the server are marked unused and the network configuration is updated.

- k Monitor the progress of the decommissioning task.

- 1 On the SDDC Manager Dashboard, click **STATUS** in the left navigation pane.

- 2 In the Workflow Tasks section, click **View Details**.

- 3 Look for the **VI Resource Pool - Decommission of hosts** task.

- 4 After about 10 minutes, refresh this page and wait till the task status changes to **Successful**.

- l For qualified vSAN Ready Nodes, change the password on the host to the common password for ESXi hosts. Log in to the BMC console using the password noted in step a and change the OOB password to D3c0mm1ss10n3d!.

This step is automated for hosts in an integrated system.

- 2 Power off the server.

- 3 Turn on the chassis-identification LED on the host.

- a In a web browser, navigate to the Management IP address that you noted down in step 5.

- b Login with your BMC user name and password.

- c Following the documentation from your vendor, turn on the chassis-identification LED.

The chassis-identification LED on the host starts to beacon (flashing on and off).

- 4 Replace the faulty SATADOM on the server and power on the server.

- 5 Reimage the server. See Image Individual Server in *VIA User's Guide*.

- 6 Reboot the host.

- 7 Log in to the server with the following credentials.

User name: root

Password: EvoSddc!2016

- 8 Perform the following steps on the host.

- a Assign a static IPv4 address between the range 192.168.100.50 - 192.168.100.73, subnet 255.255.252.0, and gateway 192.168.100.1.

- b Set the DNS IP to 192.168.1.254.

- c Enable SSH.
- d Enable firewall on SSH host and restrict connections to the 192.168.100.0/22 subnet by running the following commands:

```
esxcli network firewall ruleset set --ruleset-id=sshServer --allowed-all
false
```

```
esxcli network firewall ruleset allowedip add --ip-address=192.168.100.0/22
--ruleset-id=sshServer
```

- 9 SSH to the host and clean the vSAN partitions by running the following commands.

```
#esxcli vsan storage automode set --enabled=false
```

```
#esxcli vsan storage list|grep "Is SSD: true" -C5| grep "Display Name" |awk
'{{print $3}}'
```

Note the SSD naa.

```
#esxcli vsan storage remove -s SSD naa
```

Run this command for each diskgroup.

```
#esxcli vsan cluster leave
```

- 10 If you were unable to remove the vSAN naa, power cycle the host and re-try step 9.

What to do next

Add the host back to the rack.

Move Disks from a Dead Host to a New Host

If a host is dead, but the disks are still working (SATADOM, capacity, and cache drives), you can move the disks to a new host.

Prerequisites

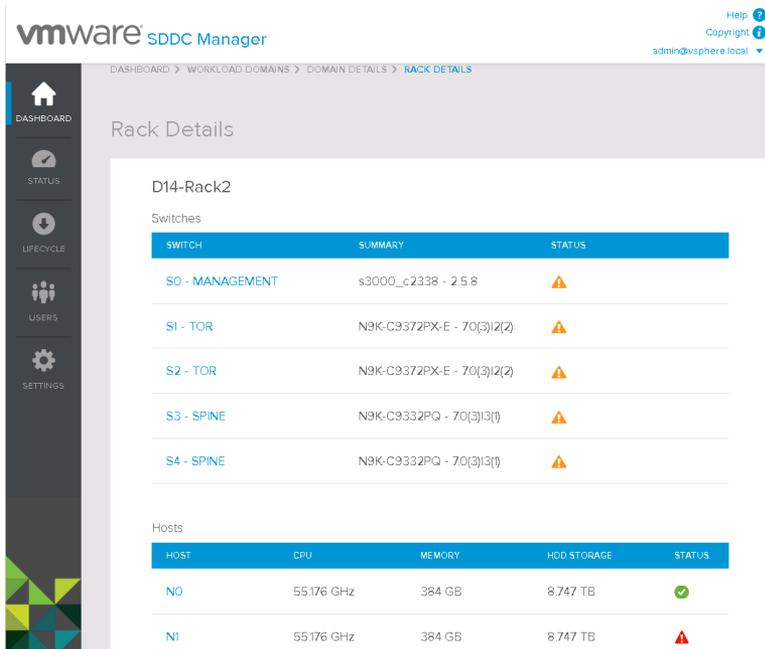
The new host should have the necessary firmware and BIOS settings.

Procedure

- 1 Note down name and IP details of the dead host.
 - a On the Dashboard page, click **VIEW DETAILS** for Physical Resources and click the affected rack.
 - b Scroll down to the Hosts section.
 - c In the **HOST** column, click the host name that shows a critical status.
The Host Details page displays the details for this host.
 - d Note down the host name, and Management IP, Network One, and Network Two IP addresses.

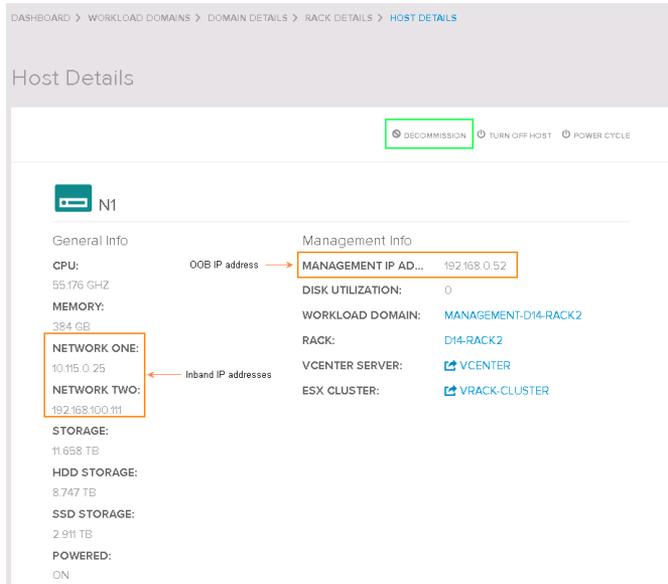
2 Decommission the dead host.

- a If you are decommissioning a qualified vSAN Ready Node (i.e. if you did not purchase a fully integrated system from a partner), note the BMC password for the host by navigating to the /home/vrack/bin/directory in the SDDC Manager VM and running the `Lookup-password` command.
- b On the Dashboard page, click **VIEW DETAILS** for **Workload Domain** and click the affected domain.
- c In the **PHYSICAL RACKS** column, click the physical rack that contains the affected server.
- d Scroll down to the **Hosts** section.
- e In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).

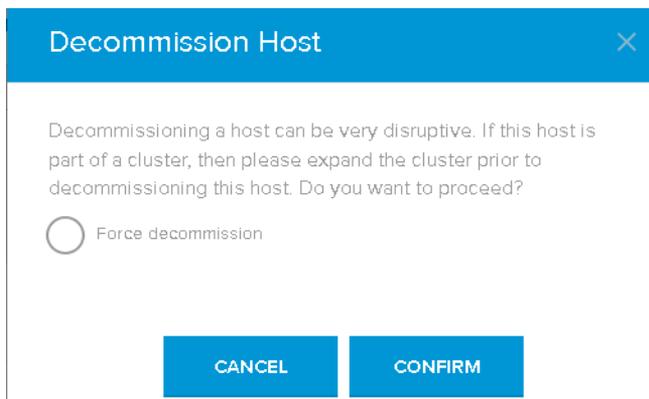


- f In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).

The Host Details page displays the details for this host.



- g In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).
- h Note the IP addresses displayed in the **NETWORK TWO** and **MANAGEMENT IP ADDRESS** fields.
- i Click **Decommission**.



If this host belongs to a workload domain, the domain must include at least 4 hosts. If the domain has fewer than 4 hosts, you must expand the domain before decommissioning the host. If the domain contains only 4 hosts and one of them is dead, click **Force decommission** to decommission the host.

- j Click **CONFIRM**.

During the host decommissioning task, the host is removed from the workload domain to which it was allocated and the environment's available capacity is updated to reflect the reduced capacity. The ports that were being used by the server are marked unused and the network configuration is updated.

- k Monitor the progress of the decommissioning task.

- 1 On the SDDC Manager Dashboard, click **STATUS** in the left navigation pane.

- 2 In the Workflow Tasks section, click **View Details**.

- 3 Look for the **VI Resource Pool - Decommission of hosts** task.

- 4 After about 10 minutes, refresh this page and wait till the task status changes to **Successful**.

- l For qualified vSAN Ready Nodes, change the password on the host to the common password for ESXi hosts. Log in to the BMC console using the password noted in step a and change the OOB password to D3c0mm1ss10n3d!.

This step is automated for hosts in an integrated system.

- 3 SSH to the management switch (IP address 192.168.100.1) and take backup of dhcpd.leases file with the following command.

```
cp /var/lib/dhcp/dhcpd.leases /var/lib/dhcp/dhcpd.leases.bk
```

- 4 SSH to the SDDC Manager VM and take a backup of hms_ib_inventory.json and prm-manifest.json files with the following commands:

```
cp /home/vrack/VMware/vRack/hms_ib_inventory.json /home/vrack/VMware/vRack/hms_ib_inventory.json.bk
```

```
cp /home/vrack/VMware/vRack/prm-manifest.json /home/vrack/VMware/vRack/prm-manifest.json.bkp
```

- 5 Power off the dead host and note the ports on the management and ToR switches it is connected to. Remove all physical connections from it and remove it from the rack.

Note In vSphere Web Client, the dead host will not be responsive . Do not remove the dead host from the inventory. After the disks are moved to the new host, the new host will automatically reconnect.

- 6 Remove the SATADOM, SSDs, and HDDs from the dead host and install them in the new host in the appropriate order and slots.
- 7 Mount the new host in the rack and connect it to the same ports of the management and ToR switches as the dead host. Refer to your notes from step 4.
- 8 Power on the new host.
- 9 Retrieve the password of the root account. See [Look Up Account Credentials](#).

- 10 Login to the vCenter Web Client with the root account and confirm that the new host is connected to the vCenter Server. If it is not connected, right-click on the disconnected host, click **Connection**, and then click **Connect**.
- 11 If the dead host belonged to a workload domain, ensure that re-synching is in progress.
 - a In vCenter Web Client, click the cluster name.
 - b Click **Monitor > vSAN > Resyncing Components**.
 - c Check for any reported issues.
- 12 On the SDDC Manager Dashboard, confirm that the replacement host has the same host name, Management, and Network IP addresses as the dead host that you removed from the rack. Refer to your notes in step 1.
- 13 If the Management IP address of the new server is different from the one assigned to the dead host, update the IP address by following the steps below.
 - a Note the OOB Mac address of the new host. For details, refer to the vendor documentation.
 - b SSH to the management switch (IP address 192.168.100.1) and type the following command.


```
cp /var/lib/dhcp/dhcpd.leases
```

Look for the OOB MAC (Management IP) address for the new host from step 13a. Note the IP address 192.168.0.x next to lease.
 - c SSH to the SDDC Manager VM and type


```
vi /home/vrack/VMware/vRack/hms_ib_inventory.json.
```
 - d Search for the 192.168.100.x (Network Two) IP address noted in step 13b.
 - e Press the Insert key and update the managementIP record with this new IP address.
 - f On the SDDC Manager Dashboard, confirm that the Management IP address of the new host has been updated.
- 14 SSH to the management switch and reboot it by typing the command `sudo reboot`.
- 15 SSH to the SDDC Manager VM and reboot it by typing the command `sudo reboot`.
- 16 Check vSAN status, and health and disk groups to ensure that they are healthy and operational.
 - a In vCenter Web Client, click the vRack-Cluster, and select **Manage > Settings > Disk Management**.
 - b Click the host that you added in and check the State and vSAN columns.
- 17 Perform vSAN proactive tests to confirm that the vSAN disks are healthy. In the vcenter server click on the cluster name, go to Monitor, vSAN, Proactive Tests. Click on each of the tests and press the green play button. Once the tests complete, logout of the system.
 - a In vCenter Web Client, click the cluster and select **Monitor > vSAN > Proactive Tests**.
 - b Click each test and press the green Play button.
 - c After the tests are complete, log out of vCenter Web Client.

Replace Capacity Drive (SSD or HDD) or Cache Drive (SSD) in a Host

You can replace the capacity drive in a host when you see an `Operation status is down for storage device` alert. The alert description says `SSD_DOWN_ALERT` or `HDD_DOWN_ALERT`.

Procedure

- 1 Expand the alert and note the rack number, host name, and disk type displayed in the `Description` field.
- 2 On the SDDC Manager Dashboard, click **View Details** in the **Physical Resources** section.
- 3 Click the affected rack and then click the host name.

The Host Details page displays host details.

- 4 If the host does not belong to a workload domain (the **Workload Domain** field is blank), pull the disk out of the host and replace it with a new disk. For details, refer to the vendor documentation.
- 5 If the host is part of a workload domain (the **Workload Domain** field displays the domain name), follow the steps below.

- a Note the **ESX Cluster** name.
- b In **vCenter Server**, click the **vCenter** link.
- c Navigate to the **ESX Cluster** name you had noted earlier.
- d In the **Manage** tab, select **vSAN > General**.
- e In the **vSAN is Turned On** field, click **Edit**.
- f In **Add disks to Storage**, select **Manual** and click **OK**.
- g Select the host with the failed disk, click the **Manage** tab and select **Disk Management** in the vSAN section.
- h Select the disk group with the failed capacity drive.
- i Select the failed capacity drive and click **Remove selected disk(s) from disk group**.
- j Wait for the disk to be deleted and then remove the disk from the host.

Note For a cache drive, the corresponding disk group is also deleted.

- k Add the new disk to the host and wait for vCenter Server to detect it.
If vCenter Server is unable to detect the drive, confirm that the disk is seated properly in the slot and perform a device re-scan.
- l Select the host with the newly replaced disk, click the **Manage** tab and select **Disk management** in the vSAN section.
- m For a cache drive, re-create the disk group.
 - 1 In vCenter, select the host with the replaced cache drive.

- 2 In the **Manage** tab, select **vSAN > Disk Management** and select the host that had the drive replaced.
 - 3 Click **Create a new disk group**.
 - 4 Select a flash device under cache tier and select 4 HDD/SSD devices under Capacity tier.
 - 5 Click **OK**.
 - 6 Wait for the task to complete and then verify that the new disk group was created for the host.
- n In the **vSAN is Turned On** field, click **Edit**.
 - o In **Add disks to Storage**, select **Automatic** and click **OK**.
 - p Log out of all open systems.
- 6 If the host you just replaced contains all flash storage, mark the disk as capacity.
 - a SSH to the ESXi host and run the `esxcli storage core device list` command. Locate the diskID of the newly added SSD.
 - b Run the `esxcli vsan storage tag add -d diskID -t capacityFlash` command.
 - c SSH to the SDDC Manager VM and copy the `/opt/vmware/scripts/capacityflash.py` script to the host on which you replaced the SSD.
 - d Run the `capacityflash.py` script on the host.

The drive on the host is successfully replaced.

Switch Details and Operations

In the Rack Details screen for a physical rack, you can see the role for each switch in that rack, whether the switch is a management, ToR, or inter-rack switch. By clicking a switch's name, you can drill down to see that switch's detailed information.

The types of switch information you can see in a switch's details are:

- Management information, such as the switch's management IP address
- Firmware information
- Network information
- Hardware health status

The hardware health status reflects the severities of the SDDC Manager alerts currently raised on the switch and its components. To examine the sorted-by-severity alert list, click **View Alerts**.

Replacing and Restoring Switches

If necessary, you can replace your Cloud Foundation system's network switches. Each rack in the system has one management switch and two top-of-rack (ToR) switches. The whole system also has two inter-rack switches.

You can also restore a switch to a configuration backup previously created.

Note The replacement switches must be from the supported list in the [VMware Cloud Foundation Compatibility Guide](#). Your ToR and inter-rack switches must be from the same vendor, such as all Cisco switches or all Arista switches. Mixing and matching of switches is not supported.

Replace a Management Switch

The HMS component does a periodic ping on your Cloud Foundation system to check the health of the management switch and reports failures. When a management switch failure occurs, the system raises a `MANAGEMENT_SWITCH_DOWN` critical alert.

For information on viewing alerts, see [Managing Alerts, Events, and Audit Events](#). When you replace the management switch in a rack, you must replace it with a switch that has the same identical specifications as the one you are replacing. The replacement management switch must be from the same manufacturer and be the same model as the one it is replacing.

Replacing the management switch is a multi-step process. You must perform the tasks in the order in which they are documented.

Prerequisites

- Verify your Cloud Foundation system is operational. You can do this by verifying that the workload domains you have in the system are running.
- Verify you have a replacement switch from the same manufacturer and of the same model as the management switch you are replacing.
- Verify the replacement switch has the Cumulus Linux OS version that is supported for this Cloud Foundation release. For the Cumulus Linux OS version that is supported in this release, see the *Release Notes*.

Procedure

1 [Retrieve Backup File for Failed Switch](#)

The SoS tool takes periodic backups of the Cloud Foundation racks in your environment. You must retrieve the backup file for the failed switch from the SoS backup.

2 [Set Default Boot Mode on New Management Switch](#)

The default boot mode for the new management switch must be set to ONIE.

3 [Image New Management Switch](#)

Imaging the new management switch with VIA installs the necessary software on the switch.

4 [Restore Backup Configuration on New Management Switch](#)

After you insert the imaged management switch in the physical rack, you can restore the backup configuration on the switch.

Retrieve Backup File for Failed Switch

The SoS tool takes periodic backups of the Cloud Foundation racks in your environment. You must retrieve the backup file for the failed switch from the SoS backup.

Procedure

1 SSH in to the SDDC Manager VM with your root account.

2 Navigate to the `/var/tmp/scheduled-backup-latestDate/switch` directory.

This directory contains zip files with names in the format `switchID-switchIP-datetime`. For example, the file for a Quanta management switch may be named `R1S0-192.168.3.254-quanta-2017-11-28-11-33-47`.

3 Identify the latest zip file for the switch.

If a backup file for the management switch does not exist, generate a backup file. See [Back Up Physical Switch Configurations](#).

Set Default Boot Mode on New Management Switch

The default boot mode for the new management switch must be set to ONIE.

Procedure

1 Power on the management switch.

Check to see if the default boot mode is ONIE. If autoboot starts, press the Esc key to display the Boot screen and select ONIE.

2 If the switch comes up in BMP mode, install ONIE on the switch. Refer to the vendor documentation.

Image New Management Switch

Imaging the new management switch with VIA installs the necessary software on the switch.

Prerequisites

- Management switch must be connected to the laptop or management host where VIA is installed.
 - If VIA is installed on a laptop, the NIC port on the laptop must be connected to port 48 of the management switch.
 - If VIA is installed on a management host, the management host must be connected to a private managed switch that is connected to port 48 of the management switch.
- Identify the Cloud Foundation version in your environment and ensure that the appropriate bundle and md5sum file is uploaded on VIA.

Note Do not connect the management switch to any host before or during imaging.

Procedure

- 1 In the VIA user interface, click **Imaging**.
Ensure that you are in the **Details** tab.
- 2 (Optional) Type a name and description for the imaging run.
- 3 In **Deployment Type**, select **Cloud Foundation Individual Deployment**.
- 4 In **Device Type**, select **MGMT_SWITCH**.
- 5 Select the vendor and model number of the switch. The IP address is displayed.
- 6 Click **Start Imaging**.
- 7 Disconnect the switch from the laptop or management host.

Restore Backup Configuration on New Management Switch

After you insert the imaged management switch in the physical rack, you can restore the backup configuration on the switch.

Procedure

- 1 Retrieve the IP address, switch ID, and the password of the management switch to be replaced and note it down.
 - a SSH to the SDDC Manager VM.
 - b Run the following command.

```
#!/home/vrack/bin/lookup-password
```

Here is a sample output.

```
MANAGEMENT: quanta lb9
  identifiers: 192.168.3.254, R1S0
  workload: hardware
  username: cumulus
  password: EvoSddc!2016
  type: SSH
```

In this example, the switch IP address is 192.168.3.254, ID is R1S0 and the password is EvoSddc!2016.

- 2 Unplug the management switch you are replacing.
Several critical alerts on the management switch may be generated.
- 3 Note down the current connections to TOR and inter-rack switches.
- 4 Remove the management switch from the rack.
- 5 Log in to the management switch console with username cumulus and password EvoSddc!2016 .
- 6 Use WinSCP to copy the backup file for the failed management switch from the SDDC Manager VM to the /home/cumulus directory of the new management switch.

7 Restore the backup configuration to the new switch.

a Change to the root directory.

```
cd /
```

b Unpack the contents of the `cumulus-R1S0-mgmt-switch-ip.timestamp.tgz` file.

```
sudo tar zxvf /home/cumulus/cumulus-R1S0-mgmt-switch-ip.timestamp.tgz
```

8 Install the replacement management switch into the rack and wire it according to the wiring connections of the previous switch. Refer to your notes from step 3.

9 Log in to the management console of the new switch with username `cumulus` and password `EvoSddc!2016`.

10 For user `cumulus`, change the password of the new management switch from `EvoSddc!2016` to the current password for your Cloud Foundation system's management switches, as obtained from the `lookup-password` command.

11 If you use VLAN IDs in the range 3000-3999 in any of your networks, and the `cumulus` version is on your new management switch is 3.3 or later, exclude this range from the reserved VLANs.

a Open the `/etc/cumulus/switchd.conf` file.

b Un-comment the following line:

```
#resv_vlan_range = 3000-3999
```

c Edit the reserved VLAN range to exclude the VLANs you use.

```
For example, resv_vlan_range = 3998-3999
```

d Restart the switch and networking services.

```
systemctl restart switchd.service
```

```
service networking restart
```

12 SSH to the SDDC Manager VM and type the following command to remove the existing ssh key from the `known_hosts` file.

```
su vrack
```

```
ssh-keygen -R 192.168.3.254
```

13 Generate an SSH key with RSA by typing the following command.

```
#ssh -oHostKeyAlgorithms='ssh-rsa' cumulus@192.168.3.254
```

Type the `cumulus` user password when prompted. Type `exit` to log out of the management switch and return to the SDDC Manager VM.

14 Rotate the SSH key by typing the following API call in the console window.

```
#curl -H "Content-Type: application/json" -X PUT --data
'{"keyGenAlgorithm":"RSA", "keyLength":2048}' http://localhost:8080/hms-
local/api/1.0/hms/napi/switches/switch-id/sshkeys/rotate
```

15 Update the new SSH key in the `/home/vrack/.ssh/known_hosts` file.

- a Open the `.ssh/known_hosts` file with a text editor.
- b Locate the entry that begins with `192.168.3.254`.
- c Replace the SSH key value after `ssh-rsa` with the value returned in Step 13.
- d Save and close the file.

16 Verify that the switch is accessible by typing the following API call.

```
#curl -X GET http://localhost:8080/hms-local/api/1.0/hms/switches/switch-id
```

The output is similar to the sample output below.

```
{
  "fruId": "1862331373",
  "componentIdentifier": {
    "description": null,
    "manufacturer": "quanta",
    "product": "lb9",
    "partNumber": "1LB9BZZ0STR",
    "manufacturingDate": "2014/12/23",
    "serialNumber": "QTFCA65100034",
    "location": null,
    "rackId": "93dfd957-b561-489c-ae63-103cf79c19ed",
    "switchId": "R1S0",
    "switchPorts": [
      "eth0", "swp1", "swp2", "swp3", "swp4", "swp5", "swp6", "swp7", "swp8", "swp9", "swp10", "swp11", "swp12", "swp13", "swp14", "swp15", "swp16", "swp17", "swp18", "swp19", "swp20", "swp21", "swp22", "swp23", "swp24", "swp25", "swp26", "swp27", "swp28", "swp29", "swp30", "swp31", "swp32", "swp33", "swp34", "swp35", "swp36", "swp37", "swp38", "swp39", "swp40", "swp41", "swp42", "swp43", "swp44", "swp45", "swp46", "swp47", "swp48", "swp49", "swp50", "swp51", "swp52"],
      "ipAddress": "192.168.3.254",
      "managementPort": null,
      "managementMacAddress": "2c:60:0c:45:89:b6",
      "operational_status": "true",
      "osName": "Cumulus Linux",
      "osVersion": "2.5.8",
      "firmwareName": "ONIE",
      "firmwareVersion": "2014.05.01-b23b0ab",
      "adminStatus": null,
      "role": "MANAGEMENT",
      "validationStatus": null,
      "powered": true,
      "discoverable": true
    ]
  }
}
```

22. Log in to the SDDC Manager UI.

17 On the SDDC Manager, clear all alerts for the management switch.

- a Navigate to the Status page and click **View Details** link in the Alerts pane.
- b Click **Edit**.
- c Select any alerts related to the management switch.
- d Click **Clear Selected Alerts**.

18 On the SDDC Manager Dashboard, click **View Details** next to Physical Resources.

Click the rack and then click on the management switch. Verify that the switch is healthy and the configuration is accurate. If the management switch is shown as being powered off, wait for 15-20 minutes and then refresh the Dashboard.

What to do next

If the Cumulus Linux OS version of the new management switch is different from the OS version on the original management switch, update the OS version in the SDDC Manager VM database.

1 Login to the management switch and check the current version of the cumulus OS

```
#cumulus@Management1$ cat /etc/os-release | grep VERSION_ID | cut -d "=" -f2
```

2 Using your root account, SSH in to the SDDC Manager VM.

3 Type the following commands.

```
su - postgres
Psql -d vrm
vrm=# update switch set os_version='cumulus_version_on_new_switch' where
id=id_of_management_switch;
vrm=# update manifest_switch set sw_version=<cumulus version on replacement switch>where
id=id_of_management_switch;
```

Replace a Cisco Top-of-Rack or Inter-rack Switch

When you replace a Cisco top-of-rack (ToR) or inter-rack switch in a rack, you must replace it with a Cisco switch that has the same identical specifications as the one you are replacing. The replacement ToR or inter-rack switch must be the same model and have the same version of the Cisco switch operating system as the one it is replacing.

For a list of the Cisco switch models that are supported for use as a ToR or inter-rack switch in this release, see [VMware Cloud Foundation Compatibility Guide](#).

The goal of this procedure is to restore the previously taken backup configuration of the working state of the system on to the replacement ToR or inter-rack switch.

Prerequisites

- Verify your Cloud Foundation environment is operational. You can do this by verifying that the workload domains you have in the environment are running.
- Verify you have the following items:
 - The backup file of the to-be-replaced Cisco ToR or switch's configuration. See [Retrieve Backup File for Failed Switch](#).
 - The credentials for the management switch of the rack which has the ToR or inter-rack switch you are replacing. Steps in the replacement procedure require copying files to and from the management switch. For steps on how to look up this password, see [Look Up Account Credentials](#).
 - A replacement Cisco switch of the same model as the Cisco switch you are replacing.
 - A diagram or photo of the to-be-replaced switch's wiring, so that you can refer to it after you have disconnected the switch. See [Chapter 17 Rack Wiring](#).
- Verify the replacement switch has the same version of the Cisco OS installed on it that is supported for use in this Cloud Foundation release. For the Cisco OS version that is supported in this release, see the *Release Notes*.

Procedure

- 1 Retrieve the IP address, switch ID, and the password of the switch to be replaced and note it down.

- a SSH to the SDDC Manager VM.
- b Run the following command.

```
#/home/vrack/bin/lookup-password
```

- 2 Copy the to-be-replaced switch's backup configuration file to the rack's management switch's /var/tmp directory.

```
scp backupFile.gz cumulus@192.168.100.1:/var/tmp
```

- 3 Disconnect the switch you are replacing and remove it from the rack.
- 4 Install the replacement switch into the rack and wire it according to the same wiring connections the previous one had.

See [Chapter 17 Rack Wiring](#).

- 5 Boot the newly installed switch.
- 6 Exit out of the POAP (Power On Auto Provisioning) mode by following the instructions in the switch console screen.
- 7 Following the prompts in the switch console screen, set a password for the "admin" user.

Important Make a note of the password you set. This step is required for all Cisco Nexus switches. Even though the admin password will be updated when the backup configuration is applied to this switch in a later step, you want to ensure you have a working password as you perform the steps prior to applying the backup configuration.

- 8 Using the original switch's IP address, configure that same IP address with the same subnet mask on the new switch on the interface named mgmt 0 and configure VRF (virtual routing and forwarding) to the mgmt 0 port.

As an example, when replacing a ToR switch that has IP address 192.168.0.20, the example configuration is:

```
switch# configure Terminal
switch(config)# interface mgmt 0
switch(config-if)# ip address 192.168.0.20/24
switch(config-if)# vrf member management
switch(config-if)# no shut
switch(config-if)# end
```

When replacing a inter-rack switch that has IP address 192.168.0.31, the example configuration is:

```
switch# configure Terminal
switch(config)# interface mgmt 0
switch(config-if)# ip address 192.168.0.31/24
switch(config-if)# vrf member management
switch(config-if)# no shut
switch(config-if)# end
```

- 9 Verify the newly installed switch can reach the management switch (at IP 192.168.3.254) by using the ping command.

```
switch(config)# ping 192.168.3.254 vrf management
PING 192.168.3.254 (192.168.3.254): 56 data bytes
64 bytes from 192.168.3.254: icmp seq=0 ttl=63 time=1.574 ms
...
```

- 10 Copy the previous switch's backup configuration file to the newly installed switch from the location on the rack's management switch where you copied it in step 2.

As an example, when replacing the Cisco ToR switch that has the backup configuration file named *backupFile.gz* that was copied to the */var/tmp* location on the rack's management switch at IP address 192.168.100.1:

```
switch(config)# copy scp: bootflash: vrf management
Enter source filename: /var/tmp/backupFile.gz
Enter hostname for the scp server: 192.168.100.1
Enter username: cumulus
cumulus@192.168.100.1's password:
backupFile.gz 100% 1891 1.9KB/s 00:00
Copy complete, now saving to disk (please wait)...
```

- 11 Use the `dir bootflash:` command to verify the backup configuration file was copied to the flash.

```
switch(config)# dir bootflash:
```

- 12 Decompress the copied backup configuration file.

Using the example from the previous step:

```
switch(config)# gunzip bootflash:///backupFile.gz
```

As a result of this step, the backup file is saved in bootflash: without the *.gz* extension.

- 13 Install the backup configuration into the new switch's startup configuration:

Using the example from the previous step:

```
switch(config)# copy backupFile startup-config
```

- 14 Copy the switch's startup configuration to its running configuration.

Using the example from the previous step:

```
switch(config)# copy startup-config running-config
```

- 15 Update the password to the password on the original switch that you noted in step 1.

```
switch(config)# username admin password passwd
```

- 16 SSH to the SDDC Manager VM.

- 17 Navigate to `/opt/vmware/sddc-support/fru-scripts/fru_switch_2.3.py`.

- 18 Run the following script to generate a self signed certificate and configure the replaced switch with this certificate.

```
python fru_switch_2.3.py
```

- 19 Run the following API calls to ensure that a 200 OK response is received.

```
# curl -X GET http://localhost:8448/api/1.0/hms/switches/switchId
# curl -X GET http://localhost:8080/hms-local/api/1.0/hms/switches/switchId
```

The replacement switch is in place and has the backup configuration from the switch it replaced.

Replace an Arista Top-of-Rack or Inter-rack Switch

When you replace an Arista top-of-rack (ToR) or inter-rack switch in a rack, you must replace it with a Arista switch that has the same identical specifications as the one you are replacing. The replacement ToR or inter-rack switch must be the same model and have the same version of the Arista switch operating system as the one it is replacing.

For a list of the Arista switch models that are supported for use as a ToR or inter-rack switch in this release, see [VMware Cloud Foundation Compatibility Guide](#).

The goal of this procedure is to restore the previously taken backup configuration of the working state of the system on to the replacement ToR or inter-rack switch.

Prerequisites

- Verify your Cloud Foundation environment is operational. You can do this by verifying that the workload domains you have in the environment are running.
- Verify you have the following items:
 - The backup file of the to-be-replaced Arista ToR or switch's configuration. See [Retrieve Backup File for Failed Switch](#).

- The credentials for the management switch of the rack which has the ToR or inter-rack switch you are replacing. Steps in the replacement procedure require copying files to and from the management switch. For steps on how to look up this password, see [Look Up Account Credentials](#).
- A replacement Arista switch of the same model as the Arista switch you are replacing.
- A diagram or photo of the to-be-replaced switch's wiring, so that you can refer to it after you have disconnected the switch. See [Chapter 17 Rack Wiring](#).
- Verify the replacement switch has the same version of the Arista OS installed on it that is supported for use in this Cloud Foundation release. For the Arista OS version that is supported in this release, see the *Release Notes*.

Procedure

- 1 Copy the to-be-replaced switch's backup configuration file to its rack's management switch's `/var/tmp` directory.

```
scp backupFile.gz cumulus@192.168.100.1:/var/tmp
```

As an example, when replacing the Arista ToR switch with IP address 192.168.0.20, you copy the backup configuration file named `192.168.0.20-arista-running-config.gz` to the management switch in that ToR switch's rack.

- 2 Disconnect the switch you are replacing and remove it from the rack.
- 3 Install the replacement switch into the rack and wire it according to the same wiring connections the previous one had.
- 4 Boot the newly installed switch and cancel the Zero Touch Provisioning (ZTP) mode.

```
AristaSwitch# zerotouch cancel
```

- 5 Log in to the replacement switch, using the default credentials that came with your replacement switch.
- 6 Using the original switch's IP address, configure that same IP address on the new switch on the interface named `management1`.

As an example, when replacing a ToR switch that has IP address 192.168.0.20, you configure the `management1` interface as:

```
interface management1
 ip address 192.168.0.20/24
```

When replacing a inter-rack switch that has IP address 192.168.0.31, you configure the `management1` interface as:

```
interface management1
 ip address 192.168.0.31/24
```

- 7 Verify the newly installed switch can reach the management switch (at IP 192.168.100.1) by using the ping command.

```
AristaSwitch# ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1): 56 data bytes
64 bytes from 192.168.100.1: icmp seq=0 ttl=63 time=1.574 ms
...
```

- 8 Copy the previous switch's backup configuration file to the newly installed switch from the location on the rack's management switch where you copied it in [Step 1](#).

As an example, when replacing the Arista ToR switch that has the backup configuration file named *backupFile.gz* that was copied to the `/var/tmp` location on the rack's management switch at IP address 192.168.100.1:

```
AristaSwitch#copy scp:backupFile.gz flash:/ backupFile.gz
cumulus@192.168.100.1's password: *****
192.168.0.20-arista-running-config.gz      100% 1761 1.7KB/s 00:00
Copy completed successfully.
AristaSwitch#
```

- 9 Use the `dir flash` command to verify the backup configuration file was copied to the flash.

```
AristaSwitch#dir flash:
```

- 10 Go into bash and decompress the copied backup configuration file .

Using the example from the previous step:

```
AristaSwitch# bash
Arista Networks EOS shell
[admin@ AristaSwitch ~]$ cd /mnt/flash
[admin@ AristaSwitch flash]$ gunzip backupFile.gz
```

As a result of this step, the extension `.gz` is removed from the file.

- 11 Exit out of bash.

```
[admin@ AristaSwitch flash]$ exit
AristaSwitch#
```

- 12 Copy the backup configuration file that resulted from the decompression to the switch's startup configuration.

Using the example from the previous step:

```
AristaSwitch# copy flash: backupFile
```

- 13 Copy the switch's startup configuration to its running configuration.

```
AristaSwitch# copy startup-config running-config
```

- 14 SSH to the SDDC Manager VM.

- 15 Navigate to `/opt/vmware/sddc-support/fru-scripts/fru_switch_2.3.py`.
- 16 Run the following API calls to ensure that a 200 OK response is received.

```
# curl -X GET http://localhost:8448/api/1.0/hms/switches/switchId
# curl -X GET http://localhost:8080/hms-local/api/1.0/hms/switches/switchId
```

The replacement switch is in place and has the backup configuration from the switch it replaced.

Working with the Management Domain and Workload Domains

8

Your Cloud Foundation system's management domain and deployed workload domains are logical units that carve up the compute, network, and storage resources of the entire system. The logical units are groups of ESXi hosts managed by vCenter Server instances with specific characteristics for redundancy and VMware SDDC best practices.

The management domain and workload domains include these VMware capabilities by default:

VMware vSphere® High Availability (HA)

In a VMware virtual environment, this feature supports distributed availability services for a group of ESXi hosts, to provide rapid recovery from outages and cost-effective high availability for applications running in virtual machines. When DRS is configured and one of the hosts in the group becomes unavailable, all virtual machines on that host are immediately restarted on another host in the group. For more information about vSphere HA, see the *vSphere Availability* documentation at <https://docs.vmware.com/en/VMware-vSphere/>.

VMware vSphere® Distributed Resource Scheduler™ (DRS)

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

VMware vSAN®

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

By default, the Cloud Foundation system has a management domain dedicated to infrastructure and management tasks. The management domain is automatically provisioned when you perform bring-up on a rack and includes the hosts you selected during bring-up. The Cloud Foundation software stack is deployed on the management domain. When you add racks to your system, the management domain automatically covers the additional racks. If you run out of resources, you can expand the management domain by selecting eligible hosts on any rack in your system.

If you have deployed Cloud Foundation on seven or more hosts, the deployment is based on the standard architecture. On this architecture model, you can deploy two pre-packaged environments named Virtual Infrastructure (VI) and Virtual Desktop Infrastructure (VDI). To deploy one of these environments, you use a workflow to carve a pool of capacity out of the available capacity, and the SDDC Manager provisions the environment, called the workload domain, using that carved-out pool of capacity. The software automatically determines the required amount of capacity to carve out based on your input for:

- Resources (CPU, memory, and storage)
- Performance
- Availability

If you have deployed Cloud Foundation six or fewer hosts, the deployment is based on the consolidated architecture. Since you do not have enough hosts to create a workload domain, you can utilize part of the capacity on the management domain by creating workload VMs and adding them to the management domain.

The SDDC Manager software provides this policy-driven approach to capacity deployment. Based on the levels you specify, the necessary hardware resources are reserved out of the available physical infrastructure. Then using those reserved hardware resources, the workflow deploys the appropriate software stack, applies storage policies, and automatically provisions and configures the virtual environment with the software required for the VMware SDDC stack and the elements required for the selected workload type. The workflow automatically:

- Deploys the vSphere environment and configures it for vSAN and enables vSphere HA and DRS, if required by your selected availability policy
- Configures the virtual networks, including the appropriate NSX for vSphere elements, as appropriate for the specified workload domain configuration
- Integrates the workload domain's resources with the appropriate pieces in the Cloud Foundation software stack

The result is a workload-ready SDDC environment.

Each Cloud Foundation instance is one SSO domain to which all vCenter Servers are joined. The maximum number of supported workload domains and vCenter Servers per Cloud Foundation instance depends on the vSphere version in the management cluster. For more information, see the *Configuration Maximums vSphere* document.

Note All of the instances for the VDI environment's servers — the vCenter Server, View Connection Server, View Composer, and so on — are created within a management domain.

The Dashboard page displays high-level information about the management and workload domains that are deployed in your system. From the Dashboard page, you can drill-down to details on each management and workload domain by using the **View Details** button.

Note You cannot create a workload domain or make any changes to a workload domain while an update is in progress.

Note If you intend to migrate VMs between vCenter instances on potentially different hardware, you should enable EVC on the affected clusters to avoid issues. See [Enable EVC on an Existing Cluster](#) in the vSphere product documentation.

This chapter includes the following topics:

- [Creating and Provisioning Workload Domains](#)
- [Creating Workload Virtual Machines in the Management Domain](#)
- [Expanding the Management and Workload Domains](#)
- [Delete a Workload Domain](#)
- [Enabling vSAN Space Efficiency Features in All-Flash Systems](#)

Creating and Provisioning Workload Domains

The flexibility of the software-defined data center provided by Cloud Foundation gives you the ability to offer virtual infrastructure to your consumers with minimal overhead. You can deploy pre-packaged environments on which you can base service offerings.

The two pre-packaged environments you can deploy are named Virtual Infrastructure (VI) and Virtual Desktop Infrastructure (VDI). These can span across racks in your Cloud Foundation system.

Create a Virtual Infrastructure Workload Domain

You create a Virtual Infrastructure (VI) workload domain using the SDDC Manager Dashboard. When you create a VI workload domain, SDDC Manager reserves the necessary pool of capacity from the available resources and deploys the VMware software stack appropriate for that VI environment.

When the creation workflow deploys the VI workload domain, it deploys one or more vCenter Server Appliance instances, associates the ESXi hosts with those instances, and performs the appropriate configuration of the hosts and virtual networks.

SDDC Manager uses the information you provide in each step of the VI workload domain creation wizard to determine the virtual environment to provision. After providing the requested information in a particular step, proceed to the next step by clicking **Next**.

Prerequisites

Using the root account, SSH in to the SDDC Manager VM and run the `./sos --health-check` command to ensure that the system is running correctly. Fix any issues that are discovered and clear the corresponding alerts.

Decide on a name for your VI workload domain. The name can be three to twenty characters long and can contain any combination of the following:

- Lowercase alphabetic characters
- Uppercase alphabetic characters
- Numbers
- Hyphens
- Underscores

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

Verify that you have the networking information to use for the workload domain's access to your corporate network. In the wizard, this network is called the Data Center connection. This network is used for access to the workloads that you run in the VI workload domain. You can use either the network configuration that was configured during your rack's bring-up process or enter a new configuration at that step in the wizard. A VLAN ID is required.

If you are planning not to use the existing default configurations for this workload domain's vMotion, vSAN, and VXLAN network connections, verify that you have the networking information you want to use for those network configurations.

Note As you progress through the wizard, if you select to use the defaults for one of these networks, but the software detects that the IP address space in the existing network configuration is inadequate to fulfill the needs of the workload domain's infrastructure, you must specify a new configuration for that network at that step in the wizard.

See also the description of the networks in [Specify Networking Information for the VI Workload Domain](#).

Procedure

1 [Start the Wizard to Create a VI Workload Domain](#)

You start the Configure VI wizard from the Dashboard page of the SDDC Manager Dashboard.

2 [Specify General Information about the VI Workload Domain](#)

In the General step of the creation wizard, you provide a name for the VI workload domain and optionally the name of the requesting organization.

3 [Select Hosts to Build the VI Domain](#)

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

4 [Select the Availability Level for the VI Workload Domain](#)

At the Storage step of the creation wizard, specify the availability you want provisioned for the VI workload domain.

5 [Specify Networking Information for the VI Workload Domain](#)

Specify the networking information for the VI workload domain.

6 Review the Details and Start the Creation Workflow

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

What to do next

For a description of actions you should perform after starting the creation workflow, see the [page 111](#) section of [Review the Details and Start the Creation Workflow](#).

Start the Wizard to Create a VI Workload Domain

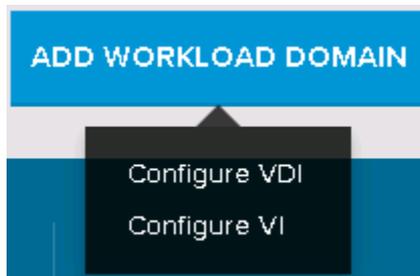
You start the Configure VI wizard from the Dashboard page of the SDDC Manager Dashboard.

Prerequisites

Verify that you have met the prerequisites described in [Create a Virtual Infrastructure Workload Domain](#).

Procedure

- 1 Start the wizard by selecting **ADD WORKLOAD DOMAIN > Configure VI**.



The wizard starts and the VI Configuration window appears. The top of the window shows the progress of the wizard as you complete each step.

- 2 Proceed to the next step by clicking **Next**.

Specify General Information about the VI Workload Domain

In the General step of the creation wizard, you provide a name for the VI workload domain and optionally the name of the requesting organization.

Spaces are not allowed in these names. The names can be three to twenty characters long and can contain any combination of the following:

- Lowercase alphabetic characters
- Uppercase alphabetic characters
- Numbers
- Hyphens
- Underscores

Procedure

- 1 Type a name for this VI workload domain, such as **Analytics**.
- 2 (Optional) Type a name for the organization that requested or will use the virtual infrastructure, such as **Finance**.
- 3 Proceed to the next step by clicking **Next**.

Select Hosts to Build the VI Domain

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

- For a VI workload domain, you can only select hosts that have the same storage type. When you select the first host, hosts that have a storage type different from the selected host are grayed out.
- When selecting hosts, select only healthy hosts. To check a host's health, log into it and run use the SoS health check command:

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

For more information, see [Chapter 13 Supportability and Serviceability \(SoS\) Tool](#).

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

Procedure

- 1 Select hosts for building the VI workload domain.

When you select hosts with sufficient storage to form a VI cluster, the Next button is enabled.

- 2 Click **Next**.

Select the Availability Level for the VI Workload Domain

At the Storage step of the creation wizard, specify the availability you want provisioned for the VI workload domain.

Based on your selections, SDDC Manager will determine:

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

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

Procedure

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

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

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

- 2 Click **Next**.

Specify Networking Information for the VI Workload Domain

Specify the networking information for the VI workload domain.

For the workload domain's management network, the creation workflow uses the management network that was configured during your system's bring-up process. During deployment of the VI workload domain's infrastructure, the workflow also configures the networks used by the vMotion, vSAN, and VXLAN capabilities in the workload domain. You can choose to use the default configurations or specify new ones in the Network step of the wizard. For each subnet, you can also specify excluded IP addresses to prevent the workflow from assigning those IP addresses to the workload domain's resources.

Important If you specify IP addresses for exclusion for a subnet in these wizard screens, they override any IP exclusions that were entered originally during your system's bring-up process for that subnet. See [About Excluding IP Address from SDDC Manager Use](#).

Table 8-1. VI Workload Domain Network Configurations

Network Configuration	Description
Management network	By default, the workload domain's management network configuration uses the management network that was configured during the bring-up process.
vMotion network	When you select to use the defaults, the workload domain's vMotion configuration uses the vMotion network that was configured during the bring-up process. If you choose to use this default, but the software detects inadequate IP address space in the existing vMotion network, you must specify a new configuration at that step in the wizard.
vSAN network	When you select to use the defaults, a VLAN ID between 3000 - 4000 is assigned to the VI workload domain. If you choose to use this default, but the software detects inadequate IP address space in the existing vSAN network, you must specify a new configuration at that step in the wizard.
VXLAN network	When you select to use the defaults, the workload domain's VXLAN configuration uses the VXLAN network that was configured during the bring-up process. If you choose to use this default, but the software detects inadequate IP address space in the existing VXLAN network, you must specify a new configuration at that step in the wizard.
Data center network	Used for access from outside this Cloud Foundation system to the workloads that you run in the workload domain. At this wizard step, you can: <ul style="list-style-type: none"> ■ Select the network configuration that was configured during the bring-up process. ■ Select a network configuration that was configured in advance using the Data Center Connections settings screen. ■ Enter a new configuration. A VLAN ID is required. <p>Important Do not select a data center connection that is already associated with a VDI workload domain or unexpected results might occur.</p>

Prerequisites

Verify that you have met the networking prerequisites as described in [Create a Virtual Infrastructure Workload Domain](#).

Important If you enter custom network configurations for the vMotion, vSAN, and VXLAN networks instead of using the default configurations, do not duplicate any of the VLAN ID, subnet (network ID), or gateway addresses that you already entered during creation of other workload domains. For example, if you previously created a VI workload domain and used value 50.0.0.0 for its vMotion network subnet field, do not re-use that value.

Procedure

- 1 Choose whether to use already-configured vMotion, vSAN, and VXLAN networks for this VI workload domain.

- Select the **USE ALL DEFAULT NETWORKS** check box. After selecting the **USE ALL DEFAULT NETWORKS** check box, click **Next** to proceed to the next wizard step for specifying the Data Center connection.

Note When you select the **USE ALL DEFAULT NETWORKS** check box, you need to configure the Data Center connection only.

Continue with Step 9 below.

- Leave the **USE ALL DEFAULT NETWORKS** check box unselected and click **Next** to proceed.
- 2 (Optional) For the management network configuration, if you want to prevent the workflow from assigning some of the subnet's IP addresses to the workload domain's resources, type those addresses or ranges.

Other than the IP address exclusion fields, the other fields on this screen are read-only. The displayed management network settings are the ones that were specified during your system's bring-up process. Because the workload domains use the same management network, you cannot change these settings when configuring a workload domain.

Caution If you specify IP addresses for exclusion in this screen, they override any IP exclusions that were entered originally during the bring-up process. See [About Excluding IP Address from SDDC Manager Use](#).

- 3 Click **Next** to proceed to the vMotion network configuration.
- 4 For the vMotion network configuration, choose one of these options.

- To use the same vMotion network configuration that was specified during your system's bring-up process, make sure the **USE DEFAULTS** check box is checked and proceed to the vSAN network configuration.
- To specify a custom vMotion network for this workload domain, clear the **USE DEFAULTS** check box, type the network settings, and then proceed to the vSAN network configuration.

Note If you choose to use the defaults, but the software detects inadequate IP address space in the existing network, you must specify a new configuration.

- 5 Click **Next** to proceed to the vSAN network configuration.

6 For the vSAN network configuration, choose one of these options.

- To use the same vSAN network configuration that was specified during your system's bring-up process, check the **USE DEFAULTS** check box and proceed to the VXLAN network configuration.
- To specify a custom vSAN network for this workload domain, clear the **USE DEFAULTS** check box if it is selected, type the vSAN network settings, and then proceed to the VXLAN network configuration.

Note If you choose to use the defaults, but the software detects inadequate IP address space in the existing network, you must specify a new configuration.

Caution If you specify IP addresses for exclusion in this screen, they override any IP exclusions that were entered originally during your system's bring-up process. See [About Excluding IP Address from SDDC Manager Use](#).

7 For the VXLAN network configuration, choose one of these options.

- To use the same VXLAN network configuration that was specified during your system's bring-up process, check the **USE DEFAULTS** check box and proceed to the Data Center connection configuration.
- To specify a custom VXLAN network for this workload domain, type the VXLAN network settings. Use the following guidelines to determine the best configuration for your workload domain.

Number of hosts	Subnet mask setting
30	/27
62	/26
126	/25

Note If you specified a large IP subnet mask (for example, /22) for VXLAN during the bring-up phase of installation, the following recommendations apply when configuring the VXLAN network for your VI workload domain.

- Cloud Foundation uses the NSX Unicast Replication mode by default, which may result in ESXi host overhead when a high number of ESXi hosts belong to a single subnet.
- VXLAN ESXi host overhead also depends on the amount of multi-destination broadcast, unknown unicast, and multicast (BUM) traffic.
- To avoid high ESXi host overhead, it is recommended that you use a dedicated IP subnet/VLAN for VXLAN for each VI/VDI workload domain.

For more information about the NSX Unicast Replication mode, see [Understanding Replication Modes](#) in the NSX product documentation.

8 Proceed to the Data Center network configuration.

9 (Optional) For the Data Center connection, choose one of these options.

- Select one of the configurations that is already in place. During ongoing operations, Data Center configurations are established using the **Settings > Network Settings > Data Center** screen.
- Select **Public** to use the data center network provided during bring-up.
- Use the drop-down **Custom Configuration** choice to create a new configuration to be used for this workload domain. A VLAN ID is required.

Explicitly specifying a data center connection at this step is optional. If you do not specify a data center connection, the workflow uses the one associated with the management domain by default.

Important Do not select a data center connection that is already associated with a VDI workload domain or unexpected results might occur.

10 Proceed to the next step by clicking **Next**.

Review the Details and Start the Creation Workflow

At the Review step of the wizard, you review the information about the to-be-created 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.

The hosts that will be added to the workload domain are listed along with the names of the physical racks in which those hosts are located. Unless you chose **High** availability, the hosts can be located in different physical racks.

This page also displays the IP addresses of the vCenter Server instances that will be deployed to manage the resources assigned to the virtual environment.

Procedure

- 1 Scroll down the page to review the information.
- 2 (Optional) Print the information or download a printable version to print later.
- 3 Click **Finish** to begin the creation process.

The VI Workload Triggered window appears, letting you know that the workflow is starting the tasks that create and deploy the VI workload domain.

What to do next

To confirm the progress of the provisioning workflow's tasks, navigate to the System Status page and drill-down to the details about the workflow. When the VI workload domain is created, the Dashboard page refreshes to indicate the new domain exists. From the Dashboard page, you can click **View Details** to navigate to see the details of the new VI workload domain. From that details page, you can launch the vSphere Web Client to see the configured virtual environment and begin working within it. See [Navigate into the VI Workload Domain's Virtual Environment](#).

Navigate into the VI Workload Domain's Virtual Environment

Navigate to a VI workload domain's virtual environment using the launch link from the workload domain's details page. When you click the launch link, the vSphere Web Client opens to a view of the virtual environment associated with that workload domain and you can use the standard capabilities of the vSphere Web Client to work within the environment.

When a VI workload domain is created, SDDC Manager deploys and configures the required VMware SDDC infrastructure within your environment. Within that SDDC infrastructure, you can perform the typical workload-related tasks that you would typically do in a virtual environment built on a vSphere software stack.

Note All of the capabilities of a VMware SDDC are available to you in the VI workload domain's environment, such as creating, provisioning, and deploying virtual machines, configuring the software-defined networking features, and so on.

Procedure

- 1 From the SDDC Manager dashboard, navigate to the VI workload domain's details page.
- 2 In the domain details page, locate the **vCenter** launch link and click it to launch the vSphere Web Client.

The vSphere Web Client opens to the VI workload domain's environment.

What to do next

Begin provisioning the VI workload domain's SDDC environment for your organization's needs. In the vSphere Web Client, you can perform all of the tasks that you typically perform in a VMware SDDC environment.

- For detailed information about VM management and administration in a vCenter Server environment using the related capabilities of the vSphere Web Client, see the vSphere Virtual Machine Administration topics in the vSphere 6.0 Documentation Center at https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-55238059-912E-411F-A0E9-A7A536972A91.html.
- For detailed information about configuring the NSX for vSphere software-defined networking features, see the NSX for vSphere documentation at <https://docs.vmware.com/en/VMware-NSX-for-vSphere/index.html>.

Create a Virtual Desktop Infrastructure Workload Domain

You create a Virtual Desktop Infrastructure (VDI) workload domain using the SDDC Manager Dashboard. When you create a VDI workload domain, the SDDC Manager deploys the components from the VMware Horizon product that are necessary for the VDI infrastructure to deliver network-based virtual desktops, based on your specifications. You can also create and save VDI workload domain configurations.

When you create and deploy a VDI workload domain, SDDC Manager reserves the necessary hardware capacity and deploys the VMware software stack appropriate to provision the necessary components for a VDI environment. The creation workflow is a two-step process:

- 1 SDDC Manager first runs the VI workload domain creation workflow, to create a virtual infrastructure (VI) environment. For a description of VI workload domains and the VMware SDDC software that makes up a virtual infrastructure environment, see [Create a Virtual Infrastructure Workload Domain](#). The VI workload domain is sized based on the parameters you enter in the VDI workload domain creation wizard, such as the number of virtual desktops, the amount of vCPU and memory, and the persistence type for the desktops.
- 2 Then using that base VI environment, the creation workflow deploys and configures the additional VMware software needed for a VDI environment. The additional VMware software that supports the VDI environment on top of the base virtual infrastructure includes View Connection Server, View Agent, View Administrator, View Composer, and the various client applications used for accessing the virtual desktops. When you specify the App Volumes choice in the configuration wizard, the VMware App Volumes™ software is also configured in the VDI environment and the VMware App Volumes agent is installed in the deployed virtual desktops as part of the VDI environment creation process.

Prerequisites

Verify that you meet the following prerequisites before starting the process.

- Your OVA file hardware must be version 11 or later.
- You must provide the ISO image for a 64-bit Windows Server 2012 R2 Volume License (VL) Edition operating system. You will upload the ISO image in one of the wizard's steps. The creation workflow creates a virtual machine and installs this Windows Server operating system into it, and then installs View Connection Server software into the Windows Server operating system.

The Windows Server 2012 R2 VL edition that is supported for use in this release is:

- Standard
- Datacenter

Note The Essentials and Foundation editions are not supported for use in a VDI workload domain because the View software that underlies the VDI environment does not support those editions.

- You must provide a valid VL license key for that ISO image. You must test this license in advance and enter it carefully. The VDI workload domain deployment process does not check the validity of the key.

Caution If you enter a key that is not a VL key valid for use for the 64-bit Windows Server 2012 R2 Volume License (VL) Standard Edition or Datacenter Edition ISO, the VDI workload domain creation process will fail part way through and you will have to delete the partially created workload domain.

- When you are using the **Deploy Desktops** option in the wizard, instead of the **Reserve Resources** option, you must provide a Windows 7, Windows 8, or Windows 10 operating system in the form of an OVA file and the Windows installation in the OVA must be prepared with specific criteria to ensure that SDDC Manager can successfully deploy and manage the virtual desktops. Ensure your OVA file has been prepared according to the criteria and steps described in [Prepare the OVA for the Virtual Desktops](#).
- When you are selecting the **Persistence Type** option to have full clones instead of linked clones, the VDI environment creation process does not customize the virtual desktops. This behavior is by design from the View infrastructure software that underlies the VDI infrastructure. In the case of full clones, the desktops that the wizard creates are only copies of the OVA template that you upload in the wizard, and if you want customized full clones, you must implement the customization script in the Windows installation used for the OVA template and customize the virtual desktop the way you want it before generating the OVA file. See [Prepare the OVA for the Virtual Desktops](#).
- In the VDI workload domain creation wizard, you are prompted to enter networking information for a data center network or you can select pre-configured information from a drop-down list. During the VDI workload domain creation workflow, the SDDC Manager places the virtual desktops on this network and configures the network to carry traffic between this Cloud Foundation system and the environment external to the system. Prior to starting the VDI workload domain creation wizard, contact your organization's Data Center Network Administrator to determine the correct vlan ID, subnet, subnet, mask, default gateway, and DNS server information to use for this VDI environment's data center network.

Your Data Center Network administrator must ensure that the settings for the data center network provide for secure traffic and is routable outside the Cloud Foundation system. Your Data Center Network administrator must also ensure that this Cloud Foundation system's public management network is able to communicate with that secure data center network. Otherwise, the VDI workload domain creation workflow will fail. Your Cloud Foundation system's management network must be able to communicate with that secure data center network to provision and manage the VDI environment. This management network's information is specified during the Cloud Foundation bring-up process. By the time you are creating VDI workload domains, the management network is already configured.

As you proceed through the VDI workload domain creation wizard, instead of entering new data center networking information, you can select from one of the existing unused data center configurations previously entered using the SDDC Manager Dashboard. To see the existing data center network configurations and any workload domains they are already associated with, use the Settings page's Data Center screen. See [Data Center Screen](#).

To review the details of already configured networks, navigate to **Settings > Network Settings > IP Distribution** and use the **Download** button in the IP Allocations area to download a CSV file containing the details.

- Additionally, when you are selecting the **Connect from anywhere** option, the data center network must be securely routable to your company's demilitarized zone (DMZ), which will be used for creating a network in the Cloud Foundation. When you select the **Connect from anywhere** option, you are specifying that users can access their virtual desktops over the Internet using their View

clients. When the VDI environment is configured and ready for use, those View clients must be proxied through View Security servers that are placed within your company's demilitarized zone (DMZ) so that the View clients can reach the routable network in your Cloud Foundation system and the virtual desktops within.

- If you plan to use the **External** option for the Active Directory configuration, you must:
 - Have the information for your organization's Microsoft Active Directory domain and whether it requires use of secure LDAP (LDAPS). With the **External** option, your existing Active Directory infrastructure is used for the VDI infrastructure's Active Directory requirements.
 - Verify that your DHCP is installed and reachable by broadcast from the Data Center network configuration you select in the wizard. The virtual desktops must be able to reach that DHCP.
 - Have the following items set up in your Active Directory in advance:
 - An Organizational Unit (OU) in your Active Directory where the VDI infrastructure's servers will be created.
 - An Organizational Unit (OU) where the virtual desktops will be created. This OU can be the same as the OU for the VDI infrastructure's servers.
 - A user account with read-write access to those two OUs.
 - A user account that will be used to add View Composer servers in the VDI infrastructure. This View Service account is a user account that is used to authenticate when accessing View Composer servers from View Connection servers. This user account must have the permissions required by the VMware Horizon software components that provision the VDI infrastructure. The key permissions needed are Create Computer Objects, Delete Computer Objects, and Write All Properties permissions, including permissions that are assigned by default (List Contents, Read All Properties, Read Permissions, Reset Password). For more details about the account requirements on the user account for View Composer AD operations, see the related VMware Horizon version 7.2 documentation at <https://docs.vmware.com/en/VMware-Horizon-7/7.2/com.vmware.horizon-view.installation.doc/GUID-3446495C-FEC8-425C-AFF8-A6CAABA5E973.html>.
- If you plan to use the **Implement App Volumes** option and the Active Directory **External** option together, you must create a group in your Active Directory whose members will be the App Volumes administrator accounts. This group must be created in your Active Directory in advance of running the VDI workload domain creation process. You enter this group name in the wizard.
- If you plan to the **Implement App Volumes** option and the Active Directory **Internal** option together, the process creates a group named AppVolumesAdmins automatically in the auto-generated Active Directory. However no members are added. As a result, when the VDI workload domain creation process is completed, you must log in to the created Active Directory using the Active Directory administrator account and add members to the AppVolumesAdmins group. Until you add members to the AppVolumesAdmins group, no one will be able to log in to App Volumes.

Procedure

1 Prepare the OVA for the Virtual Desktops

Using the **Deploy Desktops** option in the VDI workload domain creation wizard means that the creation workflow will deploy the virtual machines that are the virtual desktops as part of creating the VDI environment. Therefore, when you plan to use the **Deploy Desktops** option, you must prepare a Windows 7, Windows 8, or Windows 10 operating system installation with specific criteria and then provide that installation in the form of an OVA file.

2 Start the Wizard to Create a VDI Workload Domain

You start the Configure VDI wizard from the Dashboard page of the SDDC Manager Dashboard.

3 Specify the General Configuration Information for the VDI Workload Domain

In the General Configuration: Topology step of the creation wizard, you provide a name for the VDI workload domain and other characteristics that determine the topology of the VDI environment.

4 Specify Active Directory and SQL for the VDI Environment

In the General Configuration: Active Directory and SQL step of the wizard, you specify details about the Microsoft Active Directory infrastructure that the VDI environment will use to authenticate the desktop users.

5 Specify Characteristics of the Virtual Desktops

In the Virtual Desktops: Management and Size steps of the creation wizard, you choose whether to configure the VDI environment to use VMware App Volumes to manage the desktops, specify the number of virtual desktops to be deployed in this environment, and specify the capacity to configure for each desktop. You can also choose to save the VDI workload domain configuration to facilitate the creation of workloads in the future.

6 Select Hosts for the VDI Domain

The Server Selection page displays hosts available for VDI workload domains. Hosts that are powered off, cannot be accessed via SSH, or have not been properly commissioned are not displayed.

7 Specify Networking Information for the VDI Workload Domain

In this step, you must specify the data center network that will be used for the actual desktop pools to which end users connect.

8 Specify the Windows Images for the VDI Environment

In the Images step of the creation wizard, you specify the Microsoft Windows Server ISO file and license key that are required for use by the VDI environment's server components. If you selected to have desktops deployed as part of the workload domain creation process, you also specify a Microsoft Windows template as an OVA to use for the parent virtual machine.

9 Review the Details and Start the Creation Workflow

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

10 Post-Deployment Tasks After Your VDI Workload Domain is Created

After the VDI workload domain creation workflow has completed, you typically launch the View Administrator Web interface to view and work with the VDI infrastructure that is configured for the workload domain. Depending on the options you selected in the creation wizard, you also must perform post-deployment tasks.

What to do next

After the workflow has completed, perform the tasks described in [Post-Deployment Tasks After Your VDI Workload Domain is Created](#), especially:

- If you selected the **Implement App Volumes** option and the Active Directory **External** option together, and your Active Directory domain controllers are configured with TLS certificates for secure LDAP connections, you should configure the deployed App Volumes Manager instance to use secure connection port 636.
- If you selected the **Implement App Volumes** option and the Active Directory **Internal** option together, you must log in to the created Active Directory using the Active Directory administrator account and add members to the AppVolumesAdmins group. The process creates a group named AppVolumesAdmins automatically in the auto-generated Active Directory, but does not add members to the group. Until you add members to the AppVolumesAdmins group, no one will be able to log in to App Volumes.
- If you selected to have full clones and the Active Directory **Internal** option together, you must manually join the created full clones to the created internal Active Directory domain.

Prepare the OVA for the Virtual Desktops

Using the **Deploy Desktops** option in the VDI workload domain creation wizard means that the creation workflow will deploy the virtual machines that are the virtual desktops as part of creating the VDI environment. Therefore, when you plan to use the **Deploy Desktops** option, you must prepare a Windows 7, Windows 8, or Windows 10 operating system installation with specific criteria and then provide that installation in the form of an OVA file.

Typically, your organization has its own approved end-user desktop image with software, configurations, and policy settings that your organization wants in its end-user desktops, such as anti-virus and VPN software, browser configurations, user settings, policies, and so on. The VDI environment creation process does not configure such organization-specific needs. However, Cloud Foundation needs the end-user desktop image to be prepared so that the VMware Horizon software and its View components that make up the VDI environment's infrastructure can use the desktop image as a template for the virtual desktops that are served by the VDI environment.

Therefore, to ensure the desktop image can meet the requirements of the VMware Horizon software, you must prepare the Windows operating system in advance and ensure it meets the specific criteria before you generate the OVA file from it. In this Cloud Foundation release, the Windows operating system can be Windows 7, Windows 8, or Windows 10. Cloud Foundation uses the uploaded Windows OVA as the

desktop template to create all of the virtual desktops that will be deployed in the workload domain. Therefore, you must create this Windows installation in advance on another machine, either a physical or virtual machine, prepare the installation to meet the detailed requirements, and then convert into the OVA format that you can upload into the VDI workload domain creation wizard.

To avoid deployment issues and have the Windows OVA successfully used as a template virtual desktop in the deployed VDI environment, it must meet specific requirements. Many of the criteria are determined by the View software that underlies the VDI environment. Some requirements might differ according to the Windows operating system, whether it is Windows 7 or Windows 8 or Windows 10. In general, the prepared Windows installation must meet the requirements of a Windows image optimized for VMware Horizon, as documented in the *VMware Windows Operating System Optimization Tool Guide: VMware Horizon 6, VMware Horizon 7, and VMware Horizon Cloud-Hosted* white paper. This white paper is available at <http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/vmware-view-optimizationguidewindows7-en-white-paper.pdf> and includes settings to optimize Windows 7 and Windows 8.x for desktops.

Note Your OVA file hardware must be version 11 or later.

Along with the white paper, you can use the VMware OS Optimization Tool (OSOT) to optimize your Windows desktop images. The OSOT takes the white paper's recommendations and automates them. The OSOT is a free VMware Flings that you can download. The *VMware Windows Operating System Optimization Tool Guide: VMware Horizon 6, VMware Horizon 7, and VMware Horizon Cloud-Hosted* white paper describes how to use the OSOT and the white paper's Appendix A lists all of the optimization settings used in the OSOT templates. The OSOT can help optimize the Windows 7, Windows 8, and Windows 10 operating systems that this release of Cloud Foundation supports using for virtual desktops. The OSOT is available at <https://labs.vmware.com/flings/vmware-os-optimization-tool>

To achieve successful results in the deployed VDI environment, at a minimum, the prepared virtual machine and its installed Windows operating system must meet the following configuration requirements:

- You must set the virtual hardware version of the template desktop virtual machine to hardware version 11. This release of Cloud Foundation has ESXi 6.5 hosts. For information about virtual machine hardware versions that can run on ESXi 6.5 hosts, see the *Virtual Machine Hardware Versions* topic in the vSphere 6.0 Documentation Center at <https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.hostclient.doc/GUID-68E5EDAE-66DE-43F8-9420-F424AFEADB1D.html>
- You must use Microsoft Key Management Service (KMS) system license activation to activate the prepared Windows installation, and activate it against the same KMS system that will be reachable by the virtual desktops that will be created during the VDI workload domain creation process. That KMS system must be the same one, so that the virtual desktops can subsequently activate against the same KMS system. That KMS system must be discoverable by broadcast in the Data Center network that you specify in the VDI workload domain creation wizard. If the prepared Windows installation was not already activated for the KMS system or that KMS system is not reachable from your Cloud Foundation system, the virtual desktops that are created based on the prepared Windows image will be unusable.

This requirement is determined by the View Composer software that is deployed in the VDI environment. As described in VMware KB article 1026556, by default the View Composer QuickPrep process uses KMS to activate Windows guest operating systems. To ensure linked-clone desktops are properly activated, you must use KMS license activation on the parent virtual machine. QuickPrep does not use other volume activation methods such as Multiple Activation Key (MAK) licensing.

- You must disable TLS 1.0. See <https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.security.doc/GUID-BAE07BBA-33D3-494C-90AD-C28DC72DC55C.html>
- You must enable the local Administrator user account in the Local Users and Groups in the Windows operating system and it must not be renamed.
- You must set the password for that Administrator user account and have it in advance of starting the VDI workload domain creation wizard so you can enter that password as you complete the wizard's steps. The VDI environment creation process uses the Administrator account to install additional agents into the Windows installation that are used by the VDI environment infrastructure, such as the App Volumes agent.
- You must install the latest VMware Tools in the template desktop virtual machine, or upgrade the already installed VMware Tools to the latest version. The latest VMware Tools must be installed prior to installing the View Agent. If the New Hardware wizard appears as you follow the Install/Upgrade VMware Tool on-screen instructions, go through the wizard and accept the defaults.

For detailed information, see the Installing and Configuring VMware Tools paper at <http://www.vmware.com/pdf/vmware-tools-installation-configuration.pdf> and the how-to video in the KB article at kb.vmware.com/kb/1018377

- You must install the View Agent, and install it only after the latest VMware Tools is installed.

Important The order of installation of VMware Tools and the View Agent is important. If you install them in the incorrect order, or if you do not know the order in which they were installed, uninstall both and reinstall in the correct order.

- Do not install the App Volumes agent. The App Volumes agent is installed by the VDI environment creation process as needed.
- You must configure the Windows installation to obtain an IP address using DHCP.
- If your desktop image is a Windows 7 installation and you intend to use App Volumes in the VDI environment, ensure that the Microsoft Security Update for Windows 7 KB3033929 is installed in that Windows 7 installation. The Microsoft KB article is located at <https://www.microsoft.com/en-us/download/details.aspx?id=46078>
- If you intend to have full clones instead of linked clones, you must implement the customization script in the Windows installation and customize the virtual desktop the way you want it before generating the OVA file. The VDI environment creation process does not customize the virtual desktops. This behavior is by design from the View infrastructure software that underlies the VDI infrastructure. In

the case of full clones, the desktops that the wizard creates are only copies of the OVA template that you upload in the wizard. Therefore, if you want customized full clones, the customization script must already exist in the Windows installation and the virtual desktop customized the way you want it for your end users before the OVA file is generated.

In addition to the minimum preparation requirements, you should also perform a full anti-virus scan of the prepared Windows installation before the final step of creating an OVA file.

For best practices recommendations beyond the minimum preparation requirements, see the *Reviewers Guide for View in Horizon 6* white paper located at <http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/view/vmware-view-evaluators-guide-white-paper.pdf>.

Procedure

- 1 Obtain the virtual machine that will be the template desktop image for the virtual desktops served by the VDI environment.

The way you obtain the parent virtual machine depends on whether your organization already has its own approved end-user desktop image that it wants for this VDI environment or if you need to create the virtual machine. If you need to create the virtual machine, see the VMware Horizon product documentation at <https://docs.vmware.com/en/VMware-Horizon-7/index.html>

- 2 Set the virtual hardware version of the desktop virtual machine to hardware version 11.
- 3 Configure the Windows operating system in the virtual machine to use KMS system license activation using the same KMS system that will be reachable by the Data Center network configuration you will use for the VDI environment.
- 4 Activate the virtual machine's Windows operating system against that KMS system.
- 5 Install the latest VMware Tools in the operating system, or upgrade the already installed VMware Tools to the latest version.

If the New Hardware wizard appears as you follow the Install/Upgrade VMware Tool on-screen instructions, go through the wizard and accept the defaults.

- 6 Enable the local Administrator user account in the Local Users and Groups in the Windows operating system.

Important Do not change the name of this account. It must remain named Administrator.

- 7 Set the password for that Administrator user account and make sure you know it for entering in the workload domain creation wizard.

You would typically use a password that meets your organization's policies for its end-user desktops.

- 8 Configure the Windows installation to obtain an IP address using DHCP.
- 9 (Optional) Depending on the software that your organization already requires installed in the operating system, increase the size of the virtual disk to ensure the View Agent can be installed.
- 10 Install the View agent in the operating system.

- 11 If you are planning to select the **Persistence Type** option in the VDI workload domain creation wizard to have full clones instead of linked clones, implement the customization script in the Windows installation.

When the option to have full clones is selected in the wizard, the VDI environment creation process does not customize the virtual desktops. This behavior is by design from the View infrastructure software that underlies the VDI infrastructure. In the case of full clones, the desktops that the wizard creates are only copies of the OVA template that you upload in the wizard, and if you want customized full clones, you must implement the customization script in the Windows installation and customize the virtual desktop the way you want it.

- 12 If your desktop image is a Windows 7 installation and you intend to specifying using App Volumes in the VDI environment, install the Microsoft Security Update for Windows 7 KB3033929 into the Windows 7b installation. The Microsoft KB article is located at <https://www.microsoft.com/en-us/download/details.aspx?id=46078>
- 13 (Optional) Make any additional configurations or install additional software, according to your organization's needs.

You might obtain additional configuration recommendations from:

- VMware Horizon product documentation <https://docs.vmware.com/en/VMware-Horizon-7/index.html>
- *Reviewers Guide for View in Horizon 6* white paper
- *VMware Windows Operating System Optimization Tool Guide: VMware Horizon 6, VMware Horizon 7, and VMware Horizon Cloud-Hosted* white paper
- Running the OSOT

- 14 Perform a full anti-virus scan of the prepared Windows installation.

Even though running an anti-virus scan is not required for the prepared desktop image to work in the VDI environment, it is strongly recommended.

- 15 Export the prepared virtual machine as an OVA.

You have an OVA that is prepared with the requirements for the template desktop virtual machine needed by the VDI environment creation process.

Start the Wizard to Create a VDI Workload Domain

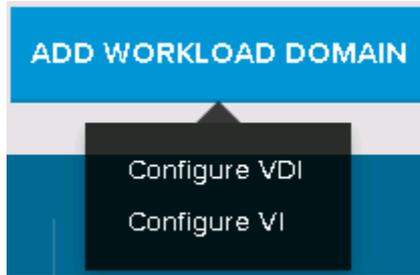
You start the Configure VDI wizard from the Dashboard page of the SDDC Manager Dashboard.

Prerequisites

Verify that you have met the prerequisites described in [Create a Virtual Desktop Infrastructure Workload Domain](#).

Procedure

- 1 Start the wizard by selecting **ADD WORKLOAD DOMAIN > Configure VDI**.



The wizard starts and the VDI Checklist window appears.

- 2 Review the information and verify that the requirements are met before proceeding.
- 3 Click **BEGIN**.

The wizard starts and the VDI window appears. The top of the window shows the progress of the wizard as you complete each step.

- 4 Proceed to the next step by clicking **Next**.

Specify the General Configuration Information for the VDI Workload Domain

In the General Configuration: Topology step of the creation wizard, you provide a name for the VDI workload domain and other characteristics that determine the topology of the VDI environment.

Spaces are not allowed in the VDI name that you enter in this wizard step. The name can be three to twenty characters long and can contain any combination of the following:

- Lowercase alphabetic characters
- Uppercase alphabetic characters
- Numbers
- Hyphens
- Underscores

Procedure

- 1 Type a name for this VDI workload domain.
- 2 Select a deployment type.

Option	Description
Reserve resources	With this choice, the workflow provisions the necessary physical and logical resources that are required for the VDI environment, according to specifications you make in the wizard. However, the View desktop pools are not created. After the VDI environment is provisioned, you must log in to the View Administrator in the workload domain's deployed environment to create and provision the desktop pools.
Deploy Desktops	With this choice, the workflow provisions the necessary physical and logical resources that are required for the VDI environment and creates and provisions the desktop pools.

3 Select the desktop type for the domain.

Option	Description
Linked	A linked clone is a copy of a virtual machine that shares virtual disks with the parent virtual machine. This conserves disk space and allows multiple virtual machines to use the same software installation. The linked clone virtual machine must have access to the parent virtual machine's virtual disks. It stores changes to the virtual disks in a snapshot dedicated to the virtual machines.
Instant	An instant clone is a virtual machine created from the memory and disk of the running parent virtual machine. It uses copy-on-write for memory and disk management. After the instant clone is created, it shares the read disks of the replica virtual machine, exactly like a linked clone.
Full	A full clone is a complete copy of the original virtual machine, including all associated virtual disks.

4 Select the assignment type for the domain.

Option	Description
Floating Desktops	In a floating desktop assignment, users receive a virtual machine randomly selected from the desktop pool when they log in. When a user logs out, the virtual machine is destroyed and a new one is added to the pool. The advantage of this assignment type is that only a small number of virtual machines need to be powered on at any given time.
Dedicated Desktops	In a dedicated desktop assignment, users receive the same virtual machine each time they log in to the desktop pool. Other users cannot access that virtual machine. In this assignment type, all desktops need to be powered on at all times.

5 Select the type of desktop access that you want the VDI environment to support.

Option	Description
Corporate Network	This choice provides access to the virtual desktops from within the customer's network only.
Connect from Anywhere	This choice provides access to the virtual desktops from both within the customer's network and from the Internet.

6 Select **Use Legacy Security Servers** if you want to use Unified Access Gateways (UAG) to route traffic to the internet.

7 Proceed to the next step by clicking **Next**.

Specify Active Directory and SQL for the VDI Environment

In the General Configuration: Active Directory and SQL step of the wizard, you specify details about the Microsoft Active Directory infrastructure that the VDI environment will use to authenticate the desktop users.

A VDI environment requires the desktop users to authenticate using an Active Directory infrastructure. You can use your organization's existing Active Directory domain or have the creation workflow create an Active Directory infrastructure as part of the provisioned VDI workload domain. If you use your organization's existing Active Directory domain, you must provide the DNS server IP address used by your Active Directory server. If you select to have the workflow create an internal Active Directory server, specify the IP address of your corporate or enterprise DNS server to use so the internal Active Directory server can resolve your enterprise domain information. All of the VDI infrastructure's components will point to the internal Active Directory server for DNS resolution.

Prerequisites

Verify that you have met the prerequisites described in [Create a Virtual Desktop Infrastructure Workload Domain](#) for the type of Active Directory infrastructure you want to use with this VDI environment.

If you are using your organization's existing Active Directory domain, verify whether your Active Directory domain requires use of secure LDAP (LDAPS). If it does, then you must select the checkbox to use LDAPS.

Procedure

- 1 Select whether to use your organization's existing Active Directory domain or to have the workflow create a new one.

Option	Description
<p>Existing</p>	<p>Select this option to have the VDI environment use your organization's existing Active Directory domain.</p> <p>Provide the following information:</p> <ul style="list-style-type: none"> ■ The System Administrator's password. This password is the one that will be set for the Administrator user in all of the VDI environment's Windows servers. ■ Domain name ■ IP address of the Active Directory domain controller ■ In Virtual Desktop Location, type the organizational unit (OU) to use for the virtual desktops. This OU must already exist in your Active Directory. ■ In Horizon Servers Location, type the Organizational Unit (OU) in your Active Directory which the VMware Horizon environment will use for its View servers, View Connection and View Composer servers. This OU must already exist in your Active Directory. ■ If your Active Directory domain requires use of LDAPS, select the Use secure connection (port 636) check box. When you select this check box, the thumbprint of the public certificate is retrieved from the IP address of the domain controller and displayed. ■ In Read-Write Account, type the account credentials, user name and password for a user account in your Active Directory that has read/write access for those OUs. This user account must already exist in your Active Directory. ■ In Horizon View Service Account, the account credentials, type the user name and password of a user account in your Active Directory that will be used to add the View Composer Service servers that are in the VMware Horizon environment. This user is used to authenticate when accessing View Composer servers from View Connection servers. This user account must already exist in your Active Directory and have the permissions required by the VMware Horizon environment. ■ In SQL Type, select Existing to have the VDI environment use your organization's existing SQL setup. Select New to have the workflow create a new dedicated SQL sever. <p>When you use the Existing option for the VDI environment's Active Directory, your DHCP is expected to be reachable by the virtual desktops using the Data Center network configuration that you specify in the wizard. When you select this choice, the workflow does not install DHCP for the desktops and SDDC Manager expects that you have DHCP installed and reachable by broadcast from the Data Center network configuration.</p>
<p>New</p>	<p>Select this option to have the workflow create a new dedicated Active Directory server internally in the VDI environment and configure it with the necessary domain name, IP address, and OU information appropriate for the VDI workload domain.</p> <p>Type the IP address of your corporate or enterprise DNS server that this internal Active Directory domain can use to resolve your domain information.</p> <p>Type a password for the domain administrator account that will be created for the domain.</p>

Option	Description
	In SQL Type , select Existing to have the VDI environment use your organization's existing SQL setup. Select New to have the workflow create a new dedicated SQL sever.

- 2 Proceed to the next step by clicking **Next**.

Specify Characteristics of the Virtual Desktops

In the Virtual Desktops: Management and Size steps of the creation wizard, you choose whether to configure the VDI environment to use VMware App Volumes to manage the desktops, specify the number of virtual desktops to be deployed in this environment, and specify the capacity to configure for each desktop. You can also choose to save the VDI workload domain configuration to facilitate the creation of workloads in the future.

Prerequisites

If you plan to use App Volumes in this VDI environment, verify that you have met the related prerequisites described in [Create a Virtual Desktop Infrastructure Workload Domain](#).

Procedure

- 1 On the Virtual Desktops - Management step, choose whether to configure the workload domain to use VMware App Volumes and then proceed to the next step.

If you select to use App Volumes and you previously selected the **New** option for Active Directory, you must also specify a group in your Active Directory whose members will have App Volumes administrator accounts. This group must already exist in your Active Directory in advance of starting the VDI workload domain creation process.

- 2 On the Virtual Desktops - Size step, type the number of virtual desktops that this workload domain will handle.

Note You can deploy a maximum of 2000 virtual desktops per workload domain.

- 3 Type the amounts of CPU, RAM, and storage to configure for each desktop.
- 4 (Optional) Save the current VDI workload domain configuration by clicking **SAVE AND CLOSE**.

This action takes you directly to the Dashboard.

- a To view and work with the saved configuration, click **View Details** in the Workload Domains table.
The saved configuration is listed under the Saved Configurations header on the Workload Domains page.
- b Click the name of the saved configuration to open the details page.

- c To create a new VDI domain workload based on the saved configuration, click **Resume Configuration**.

This action returns you to the VDI Configuration workflow with the saved configuration settings in place.

- d To delete the saved configuration, click **Delete Configuration**.

- 5 Proceed to the next step by clicking **Next**.

Select Hosts for the VDI Domain

The Server Selection page displays hosts available for VDI workload domains. Hosts that are powered off, cannot be accessed via SSH, or have not been properly commissioned are not displayed.

When selecting hosts, select only healthy hosts. To check a host's health, log into it and run use the SoS health check command:

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

For more information, see [Chapter 13 Supportability and Serviceability \(SoS\) Tool](#).

Procedure

- 1 Click **Cluster Resource Info** to see the minimum CPU, memory, and storage required to deploy the required virtual desktops.
- 2 To select hosts to be used for the VDI domain, select VC1 in the VC drop-down for the appropriate hosts.

For optimal performance, select hosts identical in terms of CPU, memory, storage, and disks. Note that unhealthy hosts, or hosts that are not properly commissioned are not displayed.

- 3 Click **Cluster Resource Info** again to ensure that the total usable resources on the selected hosts match the required resources. Note that the CPU, memory and storage in the Total Usable Resources section is not necessarily the sum of the CPU, memory, and storage on the selected hosts.

When the selected usable resources match or exceed the required resources, the **Next** button is enabled.

- 4 Click **Next**.

Specify Networking Information for the VDI Workload Domain

In this step, you must specify the data center network that will be used for the actual desktop pools to which end users connect.

If you selected the **Connect from anywhere** option in a previous wizard step, you must also provide a DMZ network configuration. The servers created for the VDI infrastructure will be installed in the environment's existing management network and the virtual desktops will be installed on the data center network.

Important Ensure that the configuration for the data center network, the DMZ network configuration, and the environment's management network meets the networking prerequisites described in [Create a Virtual Desktop Infrastructure Workload Domain](#). If not all of the networking prerequisites are met prior to completing the wizard, the creation workflow might fail.

Prerequisites

Verify that you have met the networking prerequisites as described in [Create a Virtual Desktop Infrastructure Workload Domain](#).

Procedure

- 1 On the Network Configuration: Data Center step, specify the data center network configuration to use for this VDI workload domain.
 - Select one of the existing configurations that are already in place in your installation. During ongoing operations, data center network configurations can be saved using the **Settings > Network Settings > Data Center** screen.
 - Click **Custom Configuration** and provide a network configuration to be used for this VDI environment.

If you selected to use the Active Directory domain **External** option in a previous wizard step, ensure that your external DHCP is installed and reachable by broadcast from your selected network configuration.
- 2 Proceed to the next step by clicking **Next**.
- 3 If you selected **Connect from anywhere** in a previous wizard step, you must provide a DMZ network configuration by selecting an existing configuration or by selecting **Custom Configuration** and providing a new configuration to be used for this environment.
- 4 Proceed to the next step by clicking **Next**.

Specify the Windows Images for the VDI Environment

In the Images step of the creation wizard, you specify the Microsoft Windows Server ISO file and license key that are required for use by the VDI environment's server components. If you selected to have desktops deployed as part of the workload domain creation process, you also specify a Microsoft Windows template as an OVA to use for the parent virtual machine.

The VDI infrastructure's components, such as the View Connection Server and View Composer components, must be installed on a Microsoft Windows Server operating system. You must provide a license key that is valid for that operating system.

If you have selected **Deploy Desktops** at the General - Topology step of the wizard, you provide a Windows OVA in this wizard step. This Windows OVA must be prepared in advance with specific criteria, as described in [Prepare the OVA for the Virtual Desktops](#).

If the Windows Server 2012 ISO file and Windows OVA files have already been uploaded into the software environment during a prior run of the VDI workload domain creation wizard, those existing files are displayed in the screen as selected by default.

Prerequisites

Verify that you have met the detailed prerequisites that are required on the Microsoft Windows Server operating system, on the license key, and on the Windows OVA, as described in [Create a Virtual Desktop Infrastructure Workload Domain](#) and [Prepare the OVA for the Virtual Desktops](#).

Procedure

1 Specify the Windows Server 2012 image.

See the prerequisites list earlier in this topic for details on the Microsoft Windows Server operating system that is required. You must ensure that the license key you enter in the **Windows License Key** field is valid for the specified Windows Server 2012 image.

- If an ISO file is available in the software environment for this purpose, because it was previously uploaded during a prior run of this wizard, the file's name is displayed in the field by default. You can retain that file if you have the valid license key or you can remove it and upload a different one.
- Use the **BROWSE** button to locate and upload an appropriate ISO file.

Depending on the size of the ISO file, the upload process might take some time. The displayed progress bar indicates the upload status.

2 Type the valid license key to use for that Windows Server operating system.

Important Test the license key in advance and enter it carefully. The VDI environment creation process does not check the key's validity.

- 3 If you selected **Deploy Desktops** at the General - Topology step, specify the Windows OVA to use for the parent virtual machine and its Administrator account's password.
 - a Specify the Windows OVA.
 - If an OVA file is available for this purpose, because it was previously uploaded into the environment during a prior run of this wizard, the file's name is displayed in the field by default. You can retain that file or you can remove it and upload a different one.
 - Use the **BROWSE** button to locate and upload the prepared OVA file.

Depending on the size of the OVA file, the upload process might take some time. The displayed progress bar indicates the upload status.
 - b Type the Windows Administrator password for the enabled Administrator account in the Windows installation from which the Windows OVA was built.

The Administrator user in this Windows operating system must be enabled and must not have been renamed. VMware Tools and Horizon View agent must also be installed in this Windows system. See the prerequisites list earlier in this topic for the requirements on the Windows installation that must be met.
- 4 Proceed to the next step by clicking **Next**.

Review the Details and Start the Creation Workflow

At the Review step of the wizard, you review the information about the to-be-created 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 this VDI environment.

You can use the **View Configuration Details** and **View Component Details** drop-down arrows to review information related to the VDI infrastructure that will be created and deployed, such as the number of View Connection Server appliances.

Procedure

- 1 Scroll down the page to review the information.
- 2 (Optional) Print the information or download a printable version to print later.
- 3 Click **Finish** to begin the creation process.

The VDI Workload Triggered window appears, letting you know that the workflow is starting the tasks that create and deploy the VDI workload domain.

What to do next

To confirm the progress of the provisioning workflow's tasks, navigate to the System Status page and drill-down to the details about the workflow. When the VDI workload domain is created, the Dashboard page refreshes to indicate the new domain exists. From the Dashboard page, you can use the **View Details** button to navigate to see the details of the new VDI workload domain. From that details page, you can obtain the IP address for the View Administrator Web interface and use that IP address in a browser tab to launch the View Administrator Web interface's login screen. When you log in to the View Administrator Web interface, you can see the VDI infrastructure that is configured for this workload domain.

Important After the workflow has completed, complete any applicable items described in [Post-Deployment Tasks After Your VDI Workload Domain is Created](#).

Post-Deployment Tasks After Your VDI Workload Domain is Created

After the VDI workload domain creation workflow has completed, you typically launch the View Administrator Web interface to view and work with the VDI infrastructure that is configured for the workload domain. Depending on the options you selected in the creation wizard, you also must perform post-deployment tasks.

After the workflow has completed, perform one or more of the following post-deployment tasks. You must perform some of these tasks if you chose certain options in the creation wizard.

Table 8-2. Post-Deployment Tasks

Creation Wizard Settings	Post-Deployment Tasks
All	Launch the View Administrator Web interface using the connection information located in the workload domain's details page. Use the View Details button on the Dashboard page to navigate to the workload domain's details page.
All	As described in the vRealize Log Insight documentation, the workload domain's View Administrator installation is pre-configured to send the View Administrator logs to the vRealize Log Insight instance using the HKLM\Software\Policies\VMware, Inc.\VMware VDM\Log\SyslogSendSpec registry key. The View Administrator installation is not pre-configured with a syslog server on its Event Configuration screen. You can configure the vRealize Log Insight instance that SDDC Manager deploys for syslog forwarding. You use the Event Forwarding page of the vRealize Log Insight Web interface to configure forwarding incoming events to a syslog target. For information on logging in to the vRealize Log Insight instance, see Get Started Using the vRealize Log Insight Instance .

Table 8-2. Post-Deployment Tasks (Continued)

Creation Wizard Settings	Post-Deployment Tasks
<ul style="list-style-type: none"> ■ Active Directory Internal option ■ Implement App Volumes 	<p>You must log in to the created Active Directory using the Active Directory administrator account and add members to the AppVolumesAdmins group.</p> <p>The deployment process creates a group named AppVolumesAdmins automatically in the auto-generated Active Directory, but does not add members to the group. Until you add members to the AppVolumesAdmins group, no one will be able to log in to App Volumes.</p>
<ul style="list-style-type: none"> ■ Active Directory Internal option ■ Full clones 	<p>You must manually join the created full clones to the created internal Active Directory domain. The created virtual desktops are not automatically joined to the internal Active Directory domain that was also created.</p> <p>If instead you selected to use linked clones and the Active Directory Internal option, the View software customizes the linked-clone machines when they are created, including joining them to the internal Active Directory domain.</p>
<ul style="list-style-type: none"> ■ Implement App Volumes option ■ Active Directory External option ■ Your Active Directory domain is configured to provide secure LDAP connections (LDAPS) 	<p>When your Active Directory domain controllers are configured with TLS certificates for secure LDAP connections, you should configure the deployed App Volumes Manager instance to use secure connection port 636.</p> <ol style="list-style-type: none"> 1 From the Dashboard, navigate to the domain details for the created VDI workload domain and locate the IP address of the App Volumes Manager instance. 2 Use that IP address in a new browser tab to launch the App Volumes Manager user interface. 3 In the App Volumes user interface, navigate to Configuration > Active Directory. 4 Click Edit on the Active Directory screen. 5 In the Use LDAPS field, select the Use secure connection (port 636) check box. This option ensures that communication between App Volumes and your Active Directory domain is encrypted. 6 Click Save to save the updated configuration.

Creating Workload Virtual Machines in the Management Domain

If you have six or fewer hosts in your rack, your Cloud Foundation deployment is based on the consolidated architecture. Since you do not have enough hosts to create a workload domain, you can utilize part of the capacity on the management domain by creating workload VMs and adding them to the management domain. In order to isolate the workload VMs from the Cloud Foundation management VMs, you must create these workload VMs in the **Compute-ResourcePool**, which is automatically created on the management domain during bring-up.

For more information on architecture models, see the *VMware Cloud Foundation Overview and Bring-Up Guide*.

Expanding the Management and Workload Domains

To increase the physical resources that are associated with a management domain or a workload domain, you can use the **Expand** action available on its details page. The management domain and workload domains can span across racks in your Cloud Foundation system.

Before expanding a domain, SSH in to the SDDC Manager VM and run the `./sos --health-check` to ensure that the system is running correctly. Fix any issues that are discovered and clear the corresponding alerts.

Expand a Management Domain

You can expand the management domain to increase the physical resources that are associated with it. The management domain can span across physical racks. Configure vRealize Operations to monitor the health and performance of the domain and provide alerts about resource utilization.

See [Working with vRealize Operations in Cloud Foundation](#).

Procedure

- 1 From the SDDC Manager dashboard, navigate to details page for the management domain you want to expand.

- 2 In the Domain Details page, click **EXPAND DOMAIN**.

The Expand Domain wizard opens.

- 3 On the Domain Resources page, select enough additional hosts to accommodate the expanded workload domain.

The hosts being used for this workload domain are pre-selected on this page. You must select enough additional hosts to proceed.

- 4 At the Resources step, specify the resources to add to the management domain.

Option	Description
Expand Method - By Capacity	Type the amount of CPU, memory, and storage capacity to add to the management domain.

- 5 Proceed to the next step by clicking **Next**.

- 6 At the Review step, review the displayed information.

The Review page displays the CPU, memory, and storage that will be added to the management domain based on the additional hosts you selected. The Additional Hosts sections lists the additional hosts you selected and the associated cluster details.

- 7 Click **Apply** to begin the expansion workflow.

A message indicating the status of the workflow appears at the top of the Domain Details window. To confirm the progress of the expansion workflow's tasks, navigate to the System Status page and drill-down to the details about the workflow.

What to do next

If the host you added to the domain is at a lower version than the domain, follow the steps below.

- 1 Put the newly added host in maintenance mode via vCenter Web Client.
- 2 Upgrade the domain. See [Chapter 15 Patching and Upgrading Cloud Foundation](#).

After the host is upgraded, it comes out of maintenance mode.

Expand a VI Workload Domain

You can expand a VI workload domain to increase the physical resources associated with it. The domain can span across physical racks.

Procedure

- 1 From the SDDC Manager dashboard, navigate to the workload domain's details page.
- 2 In the Domain Details page, click **EXPAND DOMAIN**.
The Expand Domain wizard opens.
- 3 On the Resources page, specify the resources to add to the workload domain.

Option	Description
Expand Method - By Capacity	Type the amount of CPU, memory, and storage capacity to add to the workload domain.

- 4 Click **Next**.
- 5 On the **Server Selection** page, select enough additional hosts to accommodate the expanded workload domain.
The hosts being used for this workload domain are pre-selected on this page. You must select enough additional hosts to proceed.
- 6 Click **Next**.
- 7 At the Review step, review the displayed information and then click **Apply** to begin the expansion workflow.
The Review page lists the hosts that the workflow will add to the workload domain to accommodate the requested capacity and the physical rack details for those hosts.

A message indicating the status of the workflow appears at the top of the Domain Details window. To confirm the progress of the expansion workflow's tasks, navigate to the System Status page and click **Tasks**.

What to do next

If the host you added to the domain is at a lower version than the domain, follow the steps below.

- 1 Put the newly added host in maintenance mode via vCenter Web Client.
- 2 Upgrade the domain. See [Chapter 15 Patching and Upgrading Cloud Foundation](#).

After the host is upgraded, it comes out of maintenance mode.

Expand a VDI Workload Domain

You expand a VDI workload domain to add more virtual desktops to it. The domain can span across physical racks.

Procedure

- 1 From the SDDC Manager dashboard, navigate to the workload domain's details page.

- 2 On the Domain Details page, click **EXPAND DOMAIN**.

The General Configuration: Topology page displays the current settings for this workload domain. The settings are read-only and they cannot be changed.

- 3 Click **Next**.

- 4 On the General Configuration: Active Directory page, type the administrative account's password and then click **Next**.

the Virtual Desktops: Management page displays the current settings for this workload domain. The settings are read-only and cannot be changed.

- 5 Click **Next**.

- 6 On the Virtual Desktops: Size page, update the number of virtual desktops to the total number that you want for this workload domain.

The displayed number of virtual desktops is the number currently configured for the workload domain. Change the number to the total number of virtual desktops you want for this workload domain. For example, if the displayed number is 100 and you want to add another 100, type 200 in the **Number of Virtual Desktops** field.

The remaining fields on this step are read-only.

- 7 Click **Next**.

- 8 On the Server Selection page, select additional hosts to accommodate the additional virtual desktops that you want to deploy.

The hosts being used for this workload domain are pre-selected on this page. You must select enough additional hosts to proceed. Click **Cluster Resource Info** to see the required resources and the resources currently selected. The **Next** button is enabled only when the selected resources match or exceed the required resources.

- 9 Click **Next**.

- 10 On the Review page, review the displayed information and then click **Apply** to begin the expansion workflow.

A message indicating the status of the workflow appears at the top of the Domain Details window. To confirm the progress of the expansion workflow's tasks, navigate to the System Status page and drill-down to the details about the workflow.

What to do next

If the host you added to the domain is at a lower version than the domain, follow the steps below.

- 1 Put the newly added host in maintenance mode via vCenter Web Client.
- 2 Upgrade the domain. See [Chapter 15 Patching and Upgrading Cloud Foundation](#).

After the host is upgraded, it comes out of maintenance mode.

Delete a Workload Domain

To free up physical resources currently associated with a workload domain that you no longer have a need for, you must delete the workload domain. After the workload domain is deleted, the physical resources are returned to the pool of available capacity in your Cloud Foundation system.

Caution Deleting a workload domain is a destructive and irreversible operation. All VMs within the workload domain are deleted and the underlying vSAN environment is destroyed. If you accidentally delete a workload domain, all of its data will be lost.

Note During the deletion process, other Domain view windows may open more slowly.

Resources in the workload domain that are shared or in common with other workload domains are not deleted in this process. For example, for VDI workload domains, if a View Composer virtual machine is shared among multiple VDI workload domains, that View Composer virtual machine is not removed by this process.

Prerequisites

- Ensure that any user data that you want retained after the workload domain deletion is backed up. You are responsible for backing up such user data.
- Ensure that any virtual machines that you deployed into the workload domain and that you want retained after the workload domain deletion are migrated. You are responsible for migrating the virtual machines that you deployed in the workload domain.

Procedure

- 1 From the SDDC Manager dashboard, navigate to the workload domain's details page.
- 2 In the Domain Details page, click **DELETE DOMAIN**.

A confirmation window appears.

3 Click **Delete**.

Note The deleted workload remains visible in the Domain Details window until the deletion process is completed.

A message indicating the status of the workflow appears at the top of the Domain Details window. To confirm the progress of the delete workflow's tasks, navigate to the System Status page and drill-down to the details about the workflow.

Enabling vSAN Space Efficiency Features in All-Flash Systems

Your Cloud Foundation system might be an all-flash storage environment. For all-flash storage, the software stack's vSAN space efficiency features enable you to reduce the amount of space for storing data in your workload domains.

As provided by the vSAN features installed in an all-flash environment, you can use these techniques to reduce the total storage capacity required to meet the needs in your workload domains:

- You can enable deduplication and compression on a workload domain's underlying vSAN environment to eliminate duplicate data and reduce the amount of space needed to store data.
- RAID 5 or RAID 6 erasure coding is a policy attribute in a workload domain's vSAN policy. Erasure coding can protect your data while using less storage space than the default RAID 1 mirroring. You set the **Failure tolerance method** in the vSAN policy to enable these features.

For detailed information about these vSAN space efficiency features, see the vSAN documentation at <https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.virtualsan.doc/GUID-0D43429F-E2E7-4647-8ECA-8F606E9E910F.html>. Specific topics about these features include:

- Using Deduplication and Compression topic: <https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.virtualsan.doc/GUID-3D2D80CC-444E-454E-9B8B-25C3F620EFE D.html>
- Deduplication and Compression Design Considerations topic: <https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.virtualsan.doc/GUID-2285B446-46BF-429C-A1E7-BEE276ED40F7.html>
- Using RAID 5 or RAID 6 Erasure Coding topic: <https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.virtualsan.doc/GUID-AD408FA8-5898-4541-9F82-FE72E6CD6227.html>. As described in that topic, RAID 5 or RAID 6 erasure coding enables vSAN to tolerate the failure of up to two capacity devices in the datastore. You can configure RAID 5 on all-flash vSAN environments having four or more fault domains. You can configure RAID 5 or RAID 6 on all-flash vSAN environments having six or more fault domains.
- RAID 5 or RAID 6 Design Considerations: <https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.virtualsan.doc/GUID-6D818555-8DE8-4F06-9498-66903FB9C775.html>

- The Edit vSAN Settings topic includes the detailed steps for enabling deduplication and compression: <https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.virtualsan.doc/GUID-FF1AE93F-817A-4894-9A38-EB474AA754F1.html>
- The Expanding vSAN Cluster Capacity and Performance topic describes how to extend vSAN disk groups: <https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.virtualsan.doc/GUID-41F8B336-D937-498E-AE87-94953A66DF00.html>

You enable these features on a workload domain's underlying environment by using the vSphere Web Client to edit the vSAN settings.

Prerequisites

Enable the deduplication and compression features on a workload domain after the workload domain creation process is successfully completed.

Procedure

- 1 Navigate to the workload domain's virtual environment in the vSphere Web Client using the **vCenter** launch link on the workload domain's details page.
- 2 Enable deduplication and compression by editing the vSAN settings using the Manage tab and the general settings for vSAN.

Set the **Add disks to storage** to **Manual** to access the deduplication and compression setting.

When you save your edits in the vSAN settings to enable deduplication and compression, vSAN will automatically upgrade the on-disk format, causing a rolling reformat of every disk group in the vSAN environment. Wait until this process is completed before making additional changes to the workload domain.

- 3 (Optional) Enable RAID 5 or RAID 6 erasure coding.
 - To use RAID 5, navigate to the vSAN storage policy and edit it to set **Failure tolerance method to RAID-5/6 (Erasure Coding) - Capacity** and **Number of failures to tolerate** to 1.
 - To use RAID 6, navigate to the vSAN storage policy and edit it to set **Failure tolerance method to RAID-5/6 (Erasure Coding) - Capacity** and **Number of failures to tolerate** to 2.

As described in the vSphere Product Documentation's [Using RAID 5 or RAID 6 Erasure Coding](#) topic, RAID 5 and RAID 6 erasure codings do not support a **Number of failures to tolerate** value of 3.

Adding vRealize Components to Cloud Foundation

9

In SDDC Manager, you can deploy vRealize Operations and vRealize Automation as Cloud Foundation components. You can also enable vRealize Log Insight directly in the SDDC Manager Dashboard.

All vRealize Suite products require separately purchased licenses.

This chapter includes the following topics:

- [Deploy vRealize Automation in Cloud Foundation](#)
- [Working with vRealize Operations in Cloud Foundation](#)

Deploy vRealize Automation in Cloud Foundation

You can deploy and manage vRealize Automation in SDDC Manager.

Prerequisites

- Verify that you have created an Active Directory (AD) account.
You must create an AD user account with permission to join Windows VMs to the domain. This account is used to install and run the management agents and IaaS components for the vRealize Automation infrastructure including proxy agents.
- Verify that both AD and SDDC Manager use a valid NTP server and are synchronized.
- Verify that you have a valid license key for vRealize Automation, which is purchased separately from Cloud Foundation.
- Verify certificate and private key.
You must have a multi-SAN certificate and private key generated by a trusted certificate authority. During generation, you must specify the short and full names of all vRealize Automation VMs and load balancer servers.
- Verify that you have created a subzone in the Active Directory DNS.
Specifically, you must configure zone forwarding from the AD's DNS to the SDDC Manager's DNS. See [Configure a Subzone for Zone Forwarding](#).
- Verify that Microsoft SQL Server is configured properly.

You must join the Microsoft SQL Server VM to the Active AD, create a new login for the AD administrative user in SQL Server, modify the firewall and port configuration, and create the SQL database.

Note For more information about the SQL Server configuration prerequisite, see [Configure Microsoft SQL Server for vRealize Automation in Cloud Foundation](#).

- Verify that you have an OVA template for the vRealize Automation Windows VM, using Windows 2012 R2.

Your Windows server image must meet the following requirement for IaaS.

- All Windows servers that host IaaS components must meet certain requirements. See [Requirements for IaaS Windows Servers](#).
- A Windows server that hosts the Web component must meet additional requirements. See [IaaS Web Server](#) in the vRealize Automation documentation.
- A Windows server that hosts the Manager Service component must meet additional requirements. See [IaaS Manager Service Host](#) in the vRealize Automation documentation.
- Ports on the IaaS Windows servers must be configured before vRealize Automation installation. See <https://docs.vmware.com/en/vRealize-Automation/7.3/com.vmware.vra.install.upgrade.doc/GUID-497EECE9-018E-428B-9ED9-AB4B6722D2AB.html> in the vRealize Automation documentation.

For details about preparing this OVA template, see [GUID-69758E3B-C486-4426-9A31-C8B6C1298D33#GUID-69758E3B-C486-4426-9A31-C8B6C1298D33](#).

Procedure

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

- 2 Click **vRealize**.

The vRealize page displays, showing all vRealize products.

- 3 Click **vRealize Automation**.

The vRealize Automation splash page displays.

- 4 Click **Deploy vRealize Automation**.

The Installation Prerequisites page displays the prerequisites you must complete before beginning the installation.

- 5 Verify the readiness of each prerequisite by checking the adjacent check box.

When each check box is checked, it turns green. When all the boxes are checked, the **BEGIN** button at the bottom of the page is activated.

Note You can select all the check boxes by clicking **Select All** in the top right corner of the page.

6 Click **BEGIN**.

The Configure vRealize Automation Environment page displays.

7 Complete the following settings to continue the installation.

All settings are required.

Setting	Description	
vRealize Automation Appliances	HA Appliance 1	Enter the short hostname as it appears in the SAN certificate.
	HA Appliance 2	Enter the short hostname as it appears in the SAN certificate.
IaaS Web VMs	IaaS Web VM 1	Enter the short hostname as it appears in the SAN certificate.
	IaaS Web VM 2	Enter the short hostname as it appears in the SAN certificate.
IaaS Manager VMs	IaaS Manager VM 1	Enter the short hostname as it appears in the SAN certificate.
	IaaS Manager VM 2	Enter the short hostname as it appears in the SAN certificate.
IaaS DEM VMs	IaaS DEM VM 1	Enter the short hostname.
	IaaS DEM VM 2	Enter the short hostname.
IaaS Agent VMs	Agent VM 1	Enter the short hostname.
	Agent VM 2	Enter the short hostname.
Certificate Details	Certificate Chain	Enter the certificate chain.
	Certificate Private Key	Enter a private key for the certificate.
	Certificate Passphrase	Enter the configured passphrase for the certificate.
vRealize Automation License	License Key	Enter your vRealize Automation license key.

Setting	Description
Default Tenant Administrator	<p>First Name Enter the administrator's first name.</p> <p>Last Name Enter the administrator's last name.</p> <p>Email Enter the administrator's email.</p> <p>Username Define a username for the tenant administrator.</p> <p>Password / Confirm Password Define and confirm a password for the tenant administrator.</p>
Load Balancers	<p>When you deploy vRealize Automation, a NSX edge with three load balancers is automatically created.</p> <p>vRealize Automation Enter the short hostname as it appears in the SAN certificate.</p> <p>iaaS Web Enter the short hostname as it appears in the SAN certificate.</p> <p>iaaS Manager Enter the short hostname as it appears in the SAN certificate.</p>

8 Click **Next**.

The Configure Windows IAAS page displays.

9 Complete the following settings to continue the installation.

All settings are required.

Setting	Description	
IAAS Template	Use Existing OVA Template	Select to use and specify an existing OVA template.
	Windows OVA Template Path	Provide the existing Windows OVA template path from vCenter Server.
	Windows License Key	Provide the license key for the Windows installation.
	Local Administrator Password	Set the password for the local Windows administrator.
Active Directory	IP Address	Provide the IP address of the DNS server (for the Active Directory) to resolve the service records for the Active Directory.
	Domain Controller Name	Provide the name of the Active Directory controller.
	Domain Name	Provide the full domain name for the Active Directory.
	Sub-domain Name	Specify the zone delegated to the SDDC Manager where all the management products reside. For example, if the domain is domain.local , the sub domain would be sub.domain.local .
	Username	Provide a username with administrative permission to join Windows VMs to the active directory.
	Password / Confirm Password	Provide and confirm a password for the administrative user.
MS SQL Server	Fully Qualified Domain Name	Provide the FQDN for the database server.
	Database Name	Specify the database name. This value is case-sensitive.
	Username	Optional. Provide the username of the database. The default value is the account used to join the vRealize VMs to Active Directory.
	Password / Confirm Password	A password is only required if a non-default value was specified for the Username.

Note See [Configure Microsoft SQL Server for vRealize Automation in Cloud Foundation](#).

10 Click **Next**.

The VLAN Configuration page displays.

11 Configure the dedicated VLAN for the vRealize components.

If you completed this VLAN configuration when deploying vRealize Operations, you can skip this step. See [Deploy vRealize Operations in Cloud Foundation](#).

Setting	Description
VLAN ID	Enter a valid vRealize Operations VLAN ID between 24 and 3967.
Subnet	Provide a valid address for the dedicated VLAN subnet.
Subnet Mask	Provide a valid address for the dedicated VLAN subnet mask.
Exclude IP Address Ranges	Optionally, specify IP ranges to be excluded from the dedicated VLAN. You can specify multiple ranges. To apply an exclusion range, click Click to Add .

Note You can also add exclusion ranges through the **Settings > Network Settings > IP Distribution > IP Exclusions** page.

12 Click **Next**.

The vRealize Automation Deployment Summary page displays.

13 Review the configuration details in the Deployment Summary.

If necessary, you can use the **BACK** button to return to preceding pages to modify your settings.

14 Click **Submit**.

If the deployment fails, this page displays a deployment status of Failed. In this case, you have the option to **Retry** or **Uninstall**.

Important If you elect to uninstall, be aware that the uninstall operation does not remove the computer accounts from AD or the DNS records of IaaS hosts. As a result, this could cause future re-installation operations to fail. It is recommended that you manually remove the computer accounts from AD and the DNS records, and delete and rebuild the SQL Server database. See [Configure Microsoft SQL Server for vRealize Automation in Cloud Foundation](#).

After vRealize Automation successfully deploys in your Cloud Foundation environment, the **SDDC Manager > Settings > vRealize > vRealize Automation** page displays an ACTIVE status. The **Connect Workloads...** link is now activated, enabling you to connect workloads to vRealize Automation.

What to do next

You must manually start the vRealize Orchestrator configuration service. See [Start the vRealize Orchestrator Configuration Service](#).

Start the vRealize Orchestrator Configuration Service

After deploying vRealize Automation in Cloud Foundation, you must manually start the vRealize Orchestrator configuration service to access the vRealize Orchestrator configuration interface.

Procedure

- 1 Start the vRealize Orchestrator Configuration service.
 - a Log in to the vRealize Automation appliance Linux console as root.
 - b Enter **service vco-configurator start** and press Enter.

- 2 Connect to the vRealize Automation URL in a Web browser.

- 3 Click **vRealize Orchestrator Control Center**.

You are redirected to `https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter`.

- 4 Log in to the vRealize Orchestrator Control Center.

The user name is configured by the vRealize Automation appliance administrator.

Configure Microsoft SQL Server for vRealize Automation in Cloud Foundation

One of the prerequisites for installing vRealize Automation in Cloud Foundation is configuring Microsoft SQL Server. Specifically, you must join the SQL Server VM to Active Directory, create a new administrative user for SQL Server access, and create the SQL database.

Prerequisites

- Microsoft SQL Server

For a complete list of supported versions, see the [vRealize Automation Support Matrix](#) (PDF).
- Active Directory
- Verify that you have the administrative permissions necessary to make configuration changes to both Active Directory and Microsoft SQL Server.

Procedure

- 1 For Microsoft SQL Server, configure a firewall exception on port 1433.
- 2 Join the Microsoft SQL Server VM to Active Directory.
 - a In the Computer Name/Domain Changes screen, select the domain and enter the domain name.
 - b Click **OK**.
 - c Specify the credentials and reboot the VM to apply the new settings.
- 3 Enable Microsoft Distributed Transaction Coordinator (MSDTC) on the Microsoft SQL Server VM.
 - a Open the Component Services manager and click **Run**.
 - b Enter **comexp.msc** in the **Open** field, and click **OK**.
 - c In the navigation tree, select **Component Services > Computers > My Computer > Distributed Transaction List > Local DTC**.

- d Right-click **Local DTC** and choose **Properties** to open the **Local DTC Properties** dialog box.
 - e Click the **Security** tab and select the following options:
 - Network DTC Access
 - Allow Remote Clients
 - Allow Inbound
 - Allow Outbound
 - f Click **OK**.
- 4 Create the vRealize Automation database login.
- a Open SQL Server Management Studio and connect to the SQL server instance.
 - b Navigate to the **Security > Logins** page, and select **New Login**.
 - c Select the **General** tab and enter the service user name (for example, **rainpole\svc-vra**) in the **Login Name** field.
 - d Select the **Server Roles** tab and select the **sysadmin** option, and click **OK**.
- 5 Create an empty database for vRealize Automation.
- a Open SQL Server Management Studio and connect to the SQL server instance.
 - b In the Object Explorer, right-click **Databases** and choose **New Database**.
 - c The New Database dialog box, select the **General** tab and enter the database name, for example, **vRA**.
 - d Set database owner to the same value as the service user name, for example **svc-vra**
 - e Select the **Options** tab and configure the following settings:
 - Set Recovery Model option to **Simple**.
 - Under **Other options**, select the **Snapshot Isolation** option.
 - Under **Other options**, select the **Read Committed Snapshot** option.
 - f Click **OK**.

Configure a Subzone for Zone Forwarding

Deploying vRealize Automation in c requires you to have zone forwarding configured in the DNS server that is responsible for the domain prepared for the vRealize Automation Windows VMs .

The DNS server should forward all requests for the Cloud Foundation sub-domain to the SDDC Manager VM IP address.

This topic briefly describes this process. Please refer to the documentation for your DNS server for specific instructions on how to forward requests for a specific sub-domain to an external DNS server.

Procedure

- 1 (Optional) Identify the sub-domain.
 - a Using SSH, log in as root to the SDDC Manager VM.
 - b Run the following grep.

```
grep "local-zone" /etc/unbound.conf
```

The output should look something like:

```
local-zone: "vcf.internal.vmware.com." static
```

Where `local-zone` indicates the sub-domain, in this example: `vcf.internal.vmware.com`.

- 2 Following the product documentation for your DNS server, configure it to forward requests for a specific sub-domain to an external DNS server.

After this configuration, you should resolve the FQDNs from `vcf.internal.vmware.com` through the DNS server.

- 3 Verify that you are able to resolve the FQDNs from the sub-domain (for example,) `vcf.internal.vmware.com` through the DNS server.

```
nslookup sddc-manager-controller.vcf.internal.vmware.com <IP_address_of_the_DNS_server>
```

You have now configured DNS forwarding that is required to deploy vRealize Automation in vRealize Automation.

Note During deployment of vRealize Automation, SDDC Manager will be configured to forward DNS requests for the unknown hosts to the IP address that you specify in the IP Address field in the Active Directory pages in the vRealize Automation wizard. In most cases, this IP address belongs to the DNS server that you have just configured.

Requirements for IaaS Windows Servers

All Windows servers that host IaaS components must meet certain requirements. Address requirements before you run the vRealize Automation Installation Wizard or the standard Windows-based installer.

- Place all IaaS Windows servers on the same domain. Do not use Workgroups.
- Each server needs the following minimum hardware.
 - 2 CPUs
 - 8 GB memory
 - 40 GB disk storage

A server that hosts the SQL database together with IaaS components might need additional hardware.

- Because of the hardware resource demand, do not deploy on VMware Workstation.
- Install Microsoft .NET Framework 3.5.
- Install Microsoft .NET Framework 4.5.2 or later.

A copy of .NET is available from any vRealize Automation appliance:

<https://vrealize-automation-appliance-fqdn:5480/installer/>

If you use Internet Explorer for the download, verify that Enhanced Security Configuration is disabled. Navigate to `res://iesetup.dll/SoftAdmin.htm` on the Windows server.

- Install Microsoft PowerShell 2.0, 3.0, or 4.0, based on your version of Windows.
Note that some vRealize Automation upgrades or migrations might require an older or newer PowerShell version, in addition to the one that you are currently running.
- If you install more than one IaaS component on the same Windows server, plan to install them to the same installation folder. Do not use different paths.
- Verify that the Secondary Log On service is running. If desired, you may stop the service after installation is complete.
- Verify that User Account Control (UAC) is disabled on the Windows server.

The UAC settings are located at **System Configuration > Tools tab > Change UAC** settings. For details, see the Microsoft server documentation.

Working with vRealize Operations in Cloud Foundation

SDDC Manager helps automate the deployment of vRealize Operations within Cloud Foundation.

This section describes the vRealize Operations deployment process, and shows you how to use vRealize Operations to monitor and collect data on workload domains.

Deploy vRealize Operations in Cloud Foundation

You can deploy and manage vRealize Operations in SDDC Manager.

Prerequisites

Verify that you have a valid license key for vRealize Operations, which is purchased separately from Cloud Foundation.

Procedure

- 1 On the SDDC Manager Dashboard, click **Settings**.
- 2 Click **vRealize**.
The vRealize page displays, showing all vRealize products.
- 3 Click **vRealize Operations**.
The vRealize Operations splash page displays.

4 Click **Deploy vRealize Operations**.

The Deployment Settings page displays.

5 Complete the following settings to continue the installation.

Setting	Description
License Key	Enter a valid vRealize Operations license key.
High Availability	Check the check box to deploy vRealize Operations with high availability configured.
Node Size	Select node size based on your specific requirements. Note If you selected the High Availability option, you must specify a node size of medium or larger.
Node Count	Specify the number of desired nodes. Note If you selected the High Availability option, you must specify at least two nodes.

Note The node size limits the number of nodes you can specify. For sizing guidelines, see the Knowledge Base article [vRealize Operations Manager 6.6 and 6.6.1 Sizing Guidelines](#).

6 Click **Submit**.

After vRealize Operations successfully deploys in your Cloud Foundation environment, the **SDDC Manager > Settings > vRealize > vRealize Operations** page displays an ACTIVE status. The **Expand Existing Installation** and **Enable Monitoring...** links are now activated, enabling you to connect workloads to vRealize Operations.

If the deployment fails, this page displays a deployment status of Failed. In this case, you have the option to **Retry** or **Uninstall**.

Configuring the vRealize Operations Adapter for VMware Horizon

As part of deploying vRealize Operations, you must configure the adapter for Horizon, including upgrading the Broker Agent.

The Desktop Agent is built into the vRealize Operations deployment in Cloud Foundation.

Procedure

1 Install and configure vRealize Operations for VMware Horizon.

For procedures, see [Installing and Configuring vRealize Operations for Horizon](#) in the vRealize Operations documentation.

2 Upgrade the Broker Agent to version 6.5.

For procedures, see [Upgrade Broker Agent](#) in the vRealize Operations documentation.

What to do next

For VMware Horizon documentation relevant to this configuration, [VMware vRealize Operations for Horizon Installation](#).

Add Nodes to vRealize Operations in Cloud Foundation

You can add nodes to expand an existing vRealize Operations in SDDC Manager.

The capacity of your vRealize Operations in SDDC Manager to accept additional nodes is restricted by its original sizing configuration. See the Knowledge Base article [vRealize Operations Manager 6.6 and 6.6.1 Sizing Guidelines](#).

Procedure

1 On the SDDC Manager Dashboard, click **Settings**.

2 Click **vRealize**.

The vRealize splash page displays, showing all vRealize products.

3 Click **vRealize Operations**.

The vRealize Operations splash page displays.

4 Click **Expand Existing Installation**.

Note If the **Expand Existing Installation** link is inactive, verify that the initial deployment succeeded and if so, the deployment has capacity for additional nodes.

The **Add Nodes...** page displays.

5 Add the desired number of nodes.

6 Click **Submit**.

Monitoring Capabilities in the Cloud Foundation System

10

The Cloud Foundation system provides built-in capabilities to help you perform effective operations monitoring, troubleshooting, performance management, infrastructure capacity planning, and compliance monitoring and auditing.

You use the built-in monitoring capabilities for these typical scenarios.

Scenario	Monitoring Area	Examples
Are the systems online?	Operations and incident monitoring	Alerts raised to notify about issues that might require human intervention.
Why did a storage drive fail?	Troubleshooting	Hardware-centric views spanning inventory, configuration, usage, and event history to provide for diagnosis and resolution.
Is the infrastructure meeting tenant service level agreements (SLAs)?	Performance management	Analysis of system and device-level metrics to identify causes and resolutions.
At what future time will the systems get overloaded?	Infrastructure capacity planning	Trend analysis of detailed system and device-level metrics, with summarized periodic reporting
What person performed which action and when?	Compliance monitoring and auditing	Event history of secured user action, with periodic reporting. Workflow task history of actions performed in the system.

The monitoring capabilities involve these features:

Events

An event is a record of a system condition that is potentially significant or interesting to you, such as a degradation, failure, or user-initiated configuration change. Multiple events might be generated for the same condition.

Audit events

In Cloud Foundation, an audit event is an event raised for a user-initiated or system-generated actions. The following lists show some examples of actions that raise audit events. These lists are not meant to be a complete list of the actions that result in audit events.

Examples of user-initiated actions that raise audit events:

- Users logging in and out of SDDC Manager

- Users performing actions involving workflows, such as creating a workload domain
- User actions involving provisioning
- Users granting or revoking a role from other users
- Account password changes, including successful and failed actions
- Users performing actions on physical resources, such as powering off a host
- Users performing the actions for life cycle management of the Cloud Foundation software

Examples of system-generated actions that raise audit events:

- Validation activity, such as during the bring-up process
- All workflows and tasks, including successful and failed actions
- All actions of Cloud Foundation that are performed to fulfill user-initiated actions, such as host configuration activities to fulfill a user-initiated action to expand a workload domain
- Network interface configuration changes

Alerts

An alert is a record of a known detected problem. Cloud Foundation has a built-in capability for detecting problems using events raised at a device level, and generating alerts that warn you about problems that would impact workload Service Level Agreements (SLAs) or which require human intervention. Multiple alerts are not generated for the same problem. Each alert generates two events, an event when the alert is raised and an event when the alert is cleared.

Workflows and tasks

A task is a unit of work performed by SDDC Manager that changes the state of a resource. A workflow is a long-running group of tasks that perform an overall goal, such as creating a workload domain.

vRealize Log Insight instanced deployed by Cloud Foundation

Use of the vRealize Log Insight instance deployed by Cloud Foundation is licensed separately. When this deployed vRealize Log Insight instance is licensed for use in your environment, events and log content for the physical resources and the VMware SDDC virtual infrastructure are sent to the vRealize Log Insight instance. As a result, when you log in to the vRealize Log Insight Web interface, you can obtain a unified view of event and syslog information to assist with troubleshooting. Data from the events and audit events raised by Cloud Foundation is also sent to

vRealize Log Insight. You can use the searching, query, and reporting features of vRealize Log Insight to create trend reports and auditing reports from the event history. See [Using vRealize Log Insight Capabilities in Your Cloud Foundation System](#).

Note The vRealize Log Insight environment that SDDC Manager deploys is sized for monitoring the hardware and software of your Cloud Foundation installation only. The default sizing accommodates the events and logs expected to be sent by the Cloud Foundation environment. This sizing might not accommodate the numbers of events and logs coming from additional applications or VMs that reside outside of your Cloud Foundation environment. Therefore, configuring the vRealize Log Insight environment that is deployed by SDDC Manager to collect events logs from additional applications or VMs that reside outside of your Cloud Foundation environment is not supported in this release.

This chapter includes the following topics:

- [Managing Workflows and Tasks](#)
- [Managing Alerts, Events, and Audit Events](#)
- [Using vRealize Log Insight Capabilities in Your Cloud Foundation System](#)

Managing Workflows and Tasks

From the System Status page of the SDDC Manager Dashboard, you can work with the SDDC Manager workflows and tasks. A task is a unit of work that changes the state of a resource. A workflow is a long-running group of tasks that perform an overall goal, such as creating a workload domain.

On the System Status page, you can see the total count of workflows and tasks at a glance, as well as a listing of tasks by state: new, running, failed, resuming, and successful. As a result, you have immediate knowledge of their progress.



On the System Status page, you can filter the displayed workflow and task counts according to the time frame within which they were reported. You can use the **View Details** link to drill-down for details on the workflows and their tasks.

Workflow Details

When you click the **View Details** link, the Workflows page displays and lists all of the workflows that have been reported by the SDDC Manager software. In this page, you can:

- Search for a workflow in the list.
- Filter the displayed workflows list by the workflow state and time frame.
- Expand a workflow to see the number of tasks it has and how many in each state: new, running, successful, or failed.
- If a workflow is in a failed state because a task has failed, you can have the software attempt to restart the workflow. On the Workflows page, the **Restart Workflow** button is available for a workflow that is in a failed state. To access the **Restart Workflow** button on the Workflows page, expand the failed workflow to where you can see its description and how many subtasks are successful and then click **Restart Workflow** next to that workflow.

Task Details

When you expand a workflow in the list on the Workflows page, the **View Sub Tasks** link is available to see detailed information about each of the tasks involved in that workflow. When you click **View Sub Tasks** for a particular workflow, a page displays that lists the tasks involved in that workflow. In the page, you can:

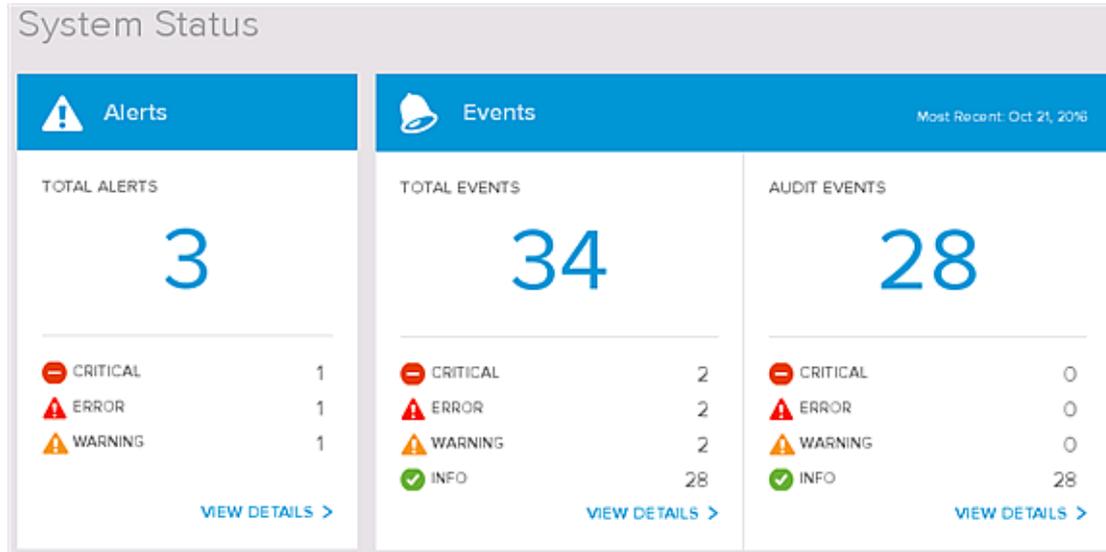
- Search for a task in the list.
- Filter the displayed workflows list by the workflow state and time frame.
- Expand a task to examine the available underlying details, if any, about that task.

Managing Alerts, Events, and Audit Events

From the System Status page of the SDDC Manager Dashboard, you can work with the alerts, events, and audit events that have been reported by your Cloud Foundation system.

On the System Status page, you can see the total count of alerts, events, and audit events at a glance, and then use the **View Details** links to drill-down for details about each type.

The vRealize Log Insight instance that SDDC Manager deploys is the final destination for all events. SDDC Manager maintains 1000 events in its local database. Once those events have been forwarded to vRealize Log Insight, the locally stored events are deleted. The locally stored events are deleted when the event count reaches a system-default upper limit of 80% of 1000, or 800 events. The oldest events are deleted first. When the upper limit of 800 is reached, events are deleted in batches of 100 events, until the current event count is reduced to less than a system-default lower limit of 60% of 1000 events, or 600 events.

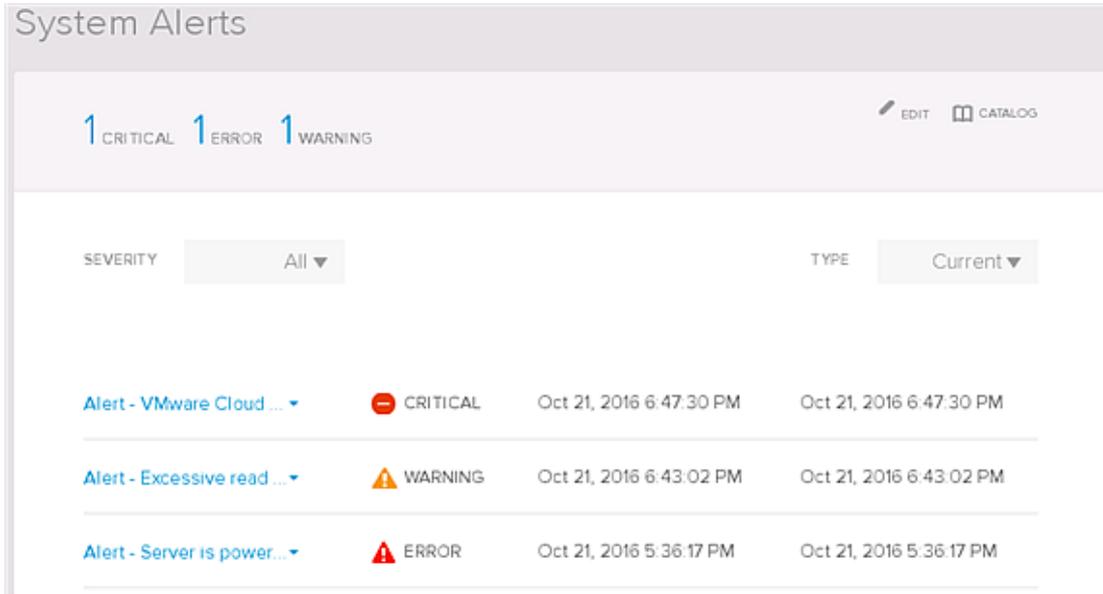


Note

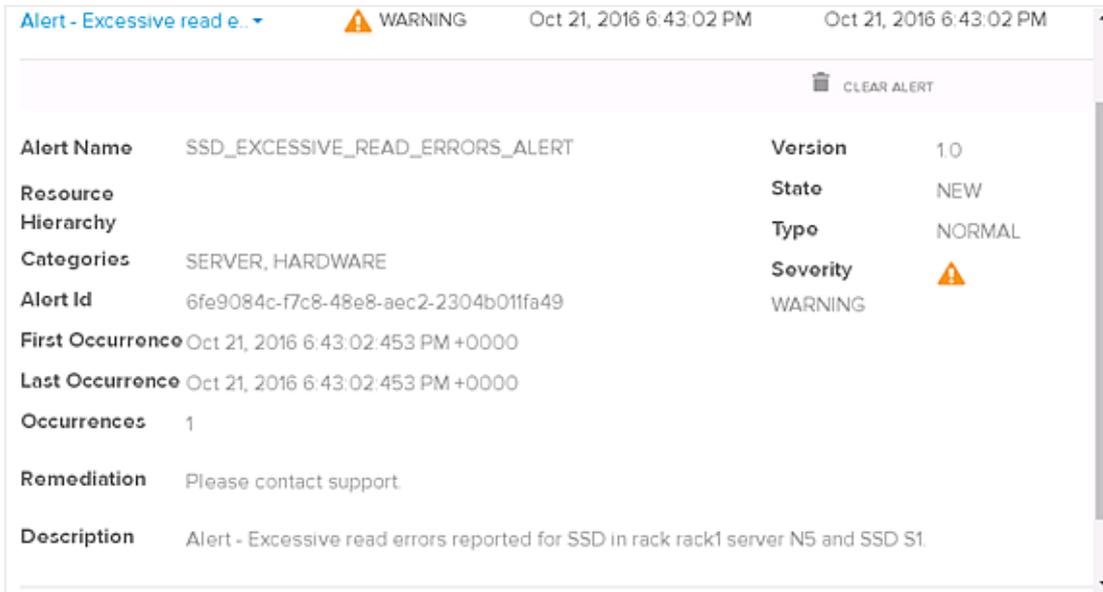
- For details about events in SDDC Manager, see [Event Catalog](#).
- For details about alerts that are raised during system operations, see [SDDC Manager Alerts Raised During Ongoing Operations](#).
- For details about alerts that are raised during Power On System Validation (POSV), see the *Alerts List* section of the *VMware Cloud Foundation Overview and Bring-Up Guide*.

Examining, Filtering, and Clearing Alerts

Clicking **View Details** for the alerts displays a page in which you can examine and clear the alerts that have been raised. Alerts are raised based on dynamic discovery of problem conditions in the hardware or virtual resources. You can expand the alerts to see details such as the time an alert was reported and its description.



You can expand an alert to see details such as the time it was reported and its description.



By default, the list shows alerts of any severity (all) that have not yet been cleared (new). To see a subset, filter the list:

- Use the **Severity** menu to filter by severity of the alert (critical, error, warning). To see all of the alerts, select **All** in the **Severity** drop-down menu.
- Use the **Type** menu to filter by type (new, cleared). When **Cleared** is selected in the **Type** menu, only the alerts that have been cleared are displayed in the list.

The event listing in the lower part of the screen includes both forwarded events and not-yet-forwarded events, in order of occurrence. Because the not-yet-forwarded events are the most recent, those events appear at the top of the list. As you scroll down, more of the events that have been forwarded to vRealize Log Insight are displayed, until all events that have occurred within the past fourteen days are loaded into the list. You can expand each event to see details such as the time an event was reported and its description.

System Events

2 CRITICAL 2 ERROR 2 WARNING 28 INFO

ANALYSIS CATALOG

SEVERITY All

Server is powered down for rack rack1, server N5. ERROR Oct 21, 2016 5:36:16 PM

Event Name	SERVER_DOWN	Version	1.0
Resource	RACK: 64ef6cd4-d5d6-4538-af19-b6ba155983fd	Agent	HMS
Hierarchy	SERVER: N5	Type	NORMAL
Categories	SERVER, HARDWARE	Severity	ERROR
Time	Oct 21, 2016 5:36:16.192 PM +0000		
Description	Server is powered down for rack rack1, server N5.		

User vcfadmin@sso.local log in to SDDC Manager ... INFO Oct 21, 2016 2:36:40 AM

From the System Events page, you can:

- Click **Analysis** to launch the vRealize Log Insight Web interface and use the vRealize Log Insight capabilities examine the log data and troubleshoot, or create trend reports and auditing reports from the event history. See [Using vRealize Log Insight Capabilities in Your Cloud Foundation System](#).
- Click **Catalog** to open the Event Catalog and view the definitions of all of the events that the software monitors and records as part of its event-driven problem detection capabilities. See [Event Catalog](#).

Examining Audit Events

Clicking **View Details** for the audit events list displays a page in which you can examine the events that have occurred from user-initiated actions. You can expand the audit events to see details such as the time an event was reported, which user initiated it, and its description.

Audit Events

0 CRITICAL 0 ERROR 0 WARNING 28 INFO ANALYSIS

SEVERITY All ▼

User vcfadmin@sso.local log in to SDDC Manager ... INFO Oct 21, 2016 2:36:40 AM

Event Name	USER_LOG_IN_SUCCEEDED	Version	1.0
Resource Hierarchy	USER: vcfadmin@sso.local	Agent	VRM
Categories	USER_ACTION, SECURITY	Type	NORMAL
Time	Oct 21, 2016 2:36:40.337 AM +0000	Severity	INFO
Description	User vcfadmin@sso.local log in to SDDC Manager succeeded.		

From the Audit Events page, you can:

- Click **Analysis** to launch the vRealize Log Insight Web interface and use the vRealize Log Insight capabilities examine the log data and troubleshoot, or create trend reports and auditing reports from the event history. See [Using vRealize Log Insight Capabilities in Your Cloud Foundation System](#).

Searching and Filtering When Viewing Details

After you click **View Details** to see one of the lists, you can use the displayed filtering features to see that subset that matches your selected criteria. The Workflows screen also has a search feature to search using text in a workflow's name.

Event Catalog

You use the Event Catalog to view the definitions of all of the events that the SDDC Manager monitors and records as part of its event-driven problem detection capabilities.

From the Events page, you open the Event Catalog by clicking **Catalog**. You can open the Events page from the SDDC Manager dashboard by navigating to the System Status page and clicking on the **View Details** button in the Events area.

Expand an event to see its definition, containing details such as its severity, description, resource hierarchy, categories, and type.

HDD_EXCESSIVE_WRITE_ERRORS ▾	
Severity	WARNING
Resource Hierarchy	RACK, SERVER, STORAGE
Categories	SERVER, HARDWARE
Type	NORMAL
Description	Storage drive for rack (RACK_NAME) server (SERVER) and HDD (STORAGE) has excessive write errors.

You can filter the displayed list by the event severity.

Hardware Operational Events

The software raises these events that are related to hardware operations. The event is raised when the software has determined the event's condition exists. When the event is raised, the event report includes identifying information about the hardware device for which the event was raised and its containing physical device, such as the server name in which the device resides and the name of the physical rack in which the server resides. As appropriate for the particular event, other relevant values are reported in the event, such as current temperature values for temperature-related events.

Note Events for CPU, memory, and BMC are not displayed because OOB IP addresses are not managed by Cloud Foundation.

Table 10-1. Hardware Operational Events Raised in a Cloud Foundation System

Event Name	Severity	Short Description
HDD_DOWN	ERROR	Operational status is down for an HDD storage drive.
HDD_EXCESSIVE_READ_ERRORS	WARNING	Excessive read errors reported for an HDD storage drive.
HDD_EXCESSIVE_WRITE_ERRORS	WARNING	Excessive write errors reported for an HDD storage drive.
HDD_TEMPERATURE_ABOVE_THRESHOLD	WARNING	HDD storage drive temperature has reached its maximum safe operating temperature.
HDD_UP	INFO	Operational status is up for an HDD storage drive.
HDD_WEAROUT_ABOVE_THRESHOLD	WARNING	Wear-out state of an HDD storage drive is above its defined threshold.
HMS_AGENT_DOWN	CRITICAL	A physical rack's Hardware Management Services agent is down.
HMS_AGENT_UP	INFO	A physical rack's Hardware Management Services agent is operational.
MANAGEMENT_SWITCH_DOWN	CRITICAL	Operational status is down for a physical rack's management switch.
MANAGEMENT_SWITCH_PORT_DOWN	WARNING	Operational status is down for a switch port in a physical rack's management switch.

Table 10-1. Hardware Operational Events Raised in a Cloud Foundation System (Continued)

Event Name	Severity	Short Description
MANAGEMENT_SWITCH_PORT_UP	INFO	Operational status is up for a switch port in a physical rack's management switch.
MANAGEMENT_SWITCH_UP	INFO	Operational status is up for a physical rack's management switch.
NIC_LINK_DOWN	WARNING	Deprecated. NIC_PORT_DOWN event is used instead.
NIC_PACKET_DROP_ABOVE_THRESHOLD	WARNING	A NIC's packet drop is above its defined threshold.
NIC_PORT_DOWN	ERROR	Operational status is down for a NIC port.
NIC_PORT_UP	INFO	Operational status is up for a NIC port.
SERVER_DOWN	CRITICAL	Server is in the powered-down state.
SERVER_UP	INFO	Server is in the powered-up state.
SPINE_SWITCH_DOWN	ERROR	Operational status is down for a physical rack's inter-rack switch.
SPINE_SWITCH_PORT_DOWN	WARNING	Operational status is down for a switch port: in a physical rack's inter-rack switch.
SPINE_SWITCH_PORT_UP	INFO	Operational status is up for a switch port: in a physical rack's inter-rack switch.
SPINE_SWITCH_UP	INFO	Operational status is up for a physical rack's inter-rack switch.
SSD_DOWN	ERROR	Operational status is down for an SSD storage device.
SSD_EXCESSIVE_READ_ERRORS	WARNING	Excessive read errors reported for an SSD storage drive.
SSD_EXCESSIVE_WRITE_ERRORS	WARNING	Excessive write errors reported for an SSD storage drive.
SSD_TEMPERATURE_ABOVE_THRESHOLD	WARNING	SSD storage drive temperature has reached its maximum safe operating temperature.
SSD_UP	INFO	Operational status is up for an SSD storage device.
SSD_WEAROUT_ABOVE_THRESHOLD	WARNING	Wear-out state of an SSD storage drive is above its defined threshold.
STORAGE_CONTROLLER_DOWN	ERROR	Operational status is down for a storage adapter.
STORAGE_CONTROLLER_UP	INFO	Operational status is up for a storage adapter.
TOR_SWITCH_DOWN	ERROR	Operational status is down for a physical rack's ToR switch.
TOR_SWITCH_PORT_DOWN	WARNING	Operational status is down for a switch port in a physical rack's ToR switch.

Table 10-1. Hardware Operational Events Raised in a Cloud Foundation System (Continued)

Event Name	Severity	Short Description
TOR_SWITCH_PORT_UP	INFO	Operational status is up for a switch port in a physical rack's ToR switch.
TOR_SWITCH_UP	INFO	Operational status is up for a physical rack's ToR switch.

Audit Events

In a Cloud Foundation system, an audit event is an event raised for a user-initiated or system-generated action. The audit event is raised when the software has determined the event's related auditable condition exists. As appropriate for the particular event, when the event is raised, the event report includes information such as the user who initiated the event, the type of operation that was performed, whether the operation succeeded or failed, and so on.

Table 10-2. Audit Events Raised in a Cloud Foundation System

Event Name	Severity	Short Description
BRINGUP_FAILED	ERROR	{OPERATION} failed due to {FAILURE_REASON}.
BRINGUP_TASK_STATE_CHANGED	INFO	Bringup with bringup id {BRINGUPID}, task id {TASKID}, task name {TASKNAME} is changed to state {TASKSTATE}."
DOMAIN_ADD_FAILED	WARNING	Creation and deployment of a workload domain failed.
DOMAIN_ADD_SUCCEEDED	INFO	Creation and deployment of a workload domain succeed.
DOMAIN_RETRY_ADD	INFO	User has initiated the restart workflow action on a workload-domain-related workflow. The domain identifier is included in the event information.
DOMAIN_STATUS_UPDATE	INFO	A workload-domain-related workflow has changed status. The domain identifier is included in the event information.
DOMAIN_TASK_ADDED	INFO	The software has added a new subtask to a workload-domain-related workflow. The software creates workflows for certain user actions and this event is raised when the software adds a new subtask to such workflows.
DOMAIN_TASK_FAILED	WARNING	A subtask within a workload-domain-related workflow has failed.
DOMAIN_TASK_STATUS_UPDATE	INFO	A subtask within a workload-domain-related workflow has changed status. The domain identifier is included in the event information.
DOMAIN_TASK_SUCCEEDED	INFO	A subtask within a workload-domain-related workflow has completed successfully.
DOMAIN_VDI_ADD	INFO	User has initiated the operation to create a VDI workload domain in the system.
DOMAIN_VIRTUAL_INFRASTRUCTURE_ADD	INFO	User has initiated the operation to create a Virtual Infrastructure workload domain in the system.

Table 10-2. Audit Events Raised in a Cloud Foundation System (Continued)

Event Name	Severity	Short Description
HOST_CANNOT_BE_USED	CRITICAL	Server {SERVER} in Rack {RACK} was not configured during {OPERATION} due to a hardware problem. For information on why the host was not configured, see the VMware Cloud Foundation Overview and Bring-Up Guide. To put this host into production, you must decommission it, fix the problem, and re-image it. Then add the host back to the inventory.
PERMISSION_GRANT_FAILED	WARNING	User has initiated the action to assign a role granting permissions to a user failed.
PERMISSION_GRANT_SUCCEEDED	INFO	The user-initiated action to assign a role granting permissions to a user has succeeded.
PERMISSION_REVOKE_FAILED	WARNING	The user-initiated action to remove a role from a user and revoke the user's permissions granted by that role has failed.
PERMISSION_REVOKE_SUCCEEDED	INFO	The user-initiated action to remove a role from a user and revoke the user's permissions granted by that role has succeeded.
PERMISSION_UPDATE_FAILED	WARNING	The user-initiated action the action to change a user's existing role to another role has failed.
PERMISSION_UPDATE_SUCCEEDED	INFO	The user-initiated action to change a user's existing role to another role has completed successfully.
ROLE_ADD_FAILED	WARNING	The user-initiated action to create a new role in the system has failed.
ROLE_ADD_SUCCEEDED	INFO	The user-initiated action to create a new role in the system has completed successfully.
ROLE_DELETE_FAILED	WARNING	The user-initiated action to delete a role has failed.
ROLE_DELETE_SUCCEEDED	WARNING	The user-initiated action to delete a role has completed successfully.
ROLE_NAME_CHANGE_FAILED	WARNING	The user-initiated action to change a role name has failed.
ROLE_NAME_CHANGE_SUCCEEDED	INFO	The user-initiated action to change a role's name has completed successfully.
ROLE_PRIVILEGE_UPDATE_FAILED	WARNING	The user-initiated action to change the privileges associated with a role has failed.
ROLE_PRIVILEGE_UPDATE_SUCCEEDED	INFO	The user-initiated action to change the privileges associated with a role has completed successfully.
SERVER_POWER_ON_FAILED	WARNING	The user-initiated action to power on a server has failed.
SERVER_POWER_ON_SUCCEEDED	INFO	The user-initiated action to power on a server has completed successfully.
UPGRADE_RECOVERED	INFO	{BUNDLETYPE} bundle upgrade failed earlier in {RESOURCETYPE} with id {RESOURCEID}, has recovered for upgrade-id {UPGRADEID}.
USER_LOG_IN_FAILED	WARNING	Log in to SDDC Manager failed for the user.
USER_LOG_IN_SUCCEEDED	INFO	Log in to SDDC Manager succeeded for the user.

Table 10-2. Audit Events Raised in a Cloud Foundation System (Continued)

Event Name	Severity	Short Description
USER_LOG_OUT_FAILED	WARNING	Log out from SDDC Manager failed for the user.
USER_LOG_OUT_SUCCEEDED	INFO	Log out from SDDC Manager succeeded for the user.
VCF_CONFIGURATION_BACKUP_FAILED	WARNING	Backup of the VMware Cloud Foundation Configuration failed in workflow {WORKFLOWID}. {MESSAGE} An on-demand backup can be triggered using the backup command line tool. The backup will be automatically retried at the next scheduled time.
VCF_CONFIGURATION_BACKUP_NOT_CONFIGURED	WARNING	There is no scheduled backup of the VMware Cloud Foundation Configuration. Please use the backup command line tool to create a backup schedule.
VCF_CONFIGURATION_BACKUP_SUCCEEDED	INFO	Backup of the VMware Cloud Foundation Configuration was successfully completed by workflow {WORKFLOWID}.

Life Cycle Management Events

The software raises these events that are related to the life cycle management operations that are available in your Cloud Foundation system. As appropriate for the particular event, when the event is raised, the event report includes information such as the type of operation that was performed, whether the operation succeeded or failed, and the condition for which the event was raised. For details about using the life cycle management features available in your system, see [Chapter 15 Patching and Upgrading Cloud Foundation](#).

Table 10-3. Life Cycle Management Events Raised in a Cloud Foundation System

Event Name	Severity	Short Description
BUNDLE_DOWNLOAD_FAILURE	ERROR	The software failed to download a bundle from the remote source location. The exact cause of the failure could not be detected by the software.
BUNDLE_DOWNLOAD_FILESIZE_MISMATCH	ERROR	The downloaded bundle's file size is greater than the file size specified in the bundle manifest.
BUNDLE_DOWNLOAD_INVALID_TAR_MANIFEST	ERROR	An error occurred while parsing the manifest file inside the downloaded bundle retrieved from the remote download source.
BUNDLE_DOWNLOAD_SCHEDULED	INFO	A bundle download is scheduled. The scheduled time is provided in the event description.
BUNDLE_DOWNLOAD_STARTED	INFO	Downloading the bundle from the bundles' remote source location has started.
BUNDLE_DOWNLOAD_SUCCEEDED	INFO	The software successfully downloaded the bundle from the bundle's remote source location.
BUNDLE_DOWNLOAD_TIMEOUT	ERROR	The bundle download process timed out while downloading the bundle from the remote source location.
BUNDLE_MANIFEST_DOWNLOAD_SUCCEEDED	INFO	The software successfully downloaded the bundle's manifest from the remote source location.

Table 10-3. Life Cycle Management Events Raised in a Cloud Foundation System (Continued)

Event Name	Severity	Short Description
BUNDLE_MANIFEST_DOWNLOAD_FAILURE	ERROR	The software failed to retrieve the bundle manifest file from the remote source location. The exact cause of the failure could not be detected by the software.
BUNDLE_MANIFEST_INVALID	ERROR	The software has determined that the bundle manifest which was retrieved from the remote source location and written to the local repository is invalid.
BUNDLE_MANIFEST_SIGNATURE_INVALID	ERROR	The signature for the bundle manifest is invalid.
BUNDLE_MANIFEST_SIGNATURE_NOT_FOUND	ERROR	The software cannot locate the bundle manifest's signature file in the expected location. The signature file is used for validating the bundle manifest file.
BUNDLE_REPO_FILE_NOT_FOUND	WARNING	The software cannot locate the specified bundle at the expected location within the bundle repository.
BUNDLE_REPO_WRITE_FAILURE	ERROR	Problems with the bundle repository are preventing bundle downloads from completing successfully.
PARTIAL_BUNDLE_DOWNLOAD	ERROR	A bundle was not fully downloaded from its remote source location. The number of bytes downloaded does not match the number of bytes stated in the bundle manifest.
UPGRADE_ABORTED	WARNING	The software has automatically cancelled a scheduled upgrade because a workflow is taking place, such as a workload domain creation or deletion workflow.
UPGRADE_CANCELLED	INFO	User has cancelled the upgrade.
UPGRADE_COMPLETION	WARNING	The life cycle management upgrade completed. The upgraded component and the completion status is provided in the event description.
UPGRADE_FAILED	WARNING	Upgrade operation has failed.
UPGRADE_NOT_NEEDED	INFO	The software has determined all of the environment's components have up-to-date versions and upgrading them is not needed.
UPGRADE_SCHEDULED	INFO	A bundle upgrade is scheduled. The scheduled time is provided in the event description.
UPGRADE_STARTED	INFO	Upgrade operation has started.
UPGRADE_SUCCEEDED	INFO	Upgrade operation has succeeded.
UPGRADE_TIMEDOUT	WARNING	Upgrade operation has timed out.
UPGRADE_VCENTER_VSAN_HCL_UPDATE_FAILURE	ERROR	Update of VSAN HCL {HCL_FILE_REPO_PATH} failed for upgrade {UPGRADEID}. Please update the VSAN HCL DB through vSphere Client. Refer to Knowledge Base article at https://kb.vmware.com/kb/2145116 .
VMWARE_DEPOT_CONNECT_FAILURE	WARNING	The software failed to connect to the remote source location from which the upgrade bundles are downloaded.

Table 10-3. Life Cycle Management Events Raised in a Cloud Foundation System (Continued)

Event Name	Severity	Short Description
VMWARE_DEPOT_INDEX_FILE_NOT_FOUND	ERROR	The software cannot locate an index file at the remote source location.
VMWARE_DEPOT_INSUFFICIENT_PERMISSION	ERROR	The software failed to download a bundle or bundle manifest from the remote source location because the user account used to connect to the remote location does not have read permission for the remote directory or file.
VMWARE_DEPOT_INDEX_INVALID	ERROR	The retrieved bundle index is invalid.
VMWARE_DEPOT_MANIFEST_FILE_NOT_FOUND	ERROR	The software cannot locate a manifest file at the remote source location.
VMWARE_DEPOT_MISSING_BUNDLE	ERROR	The software cannot locate a bundle available for downloading from the remote source location.
VMWARE_DEPOT_UNKNOWN_HOST	ERROR	The software cannot resolve the VMware Depot host of the configured remote source location for downloading upgrade bundles.

Alert Catalog

You use the Alert Catalog page to view the SDDC Manager alert definitions.

In this page, you can expand an alert to see its definition, containing details such as its severity, description, resource hierarchy, categories, and type.

You can use the keyword search to locate an alert in the catalog and you can filter the displayed list by severity.

For more information about how system alerts are raised during ongoing system operations and an alphabetical listing of the system alerts, see [SDDC Manager Alerts Raised During Ongoing Operations](#).

SDDC Manager Alerts Raised During Ongoing Operations

An alert is a stateful record for a problem. SDDC Manager raises an alert based on the detection of problem conditions in the hardware or virtual resources. Problem detection can occur during the Power On System Validation (POSV) portion of the Cloud Foundation bring-up process and during ongoing operations.

During ongoing operations, SDDC Manager raises alerts for problems detected as a result of its periodic polling of hardware status or from alert-raising events. Alerts are not generated for fleeting conditions or for problems that the system can resolve itself. Alerts are raised for issues that:

- Persist
- Require human intervention to resolve

The software periodically polls the status of the hardware resources and raises alerts when analysis of the results indicates a problem condition exists.

- Every 30 minutes, the servers and switches are polled to verify that those resources are discoverable and to obtain the power status of the servers and switches. This 30-minute polling ensures that any status change of a server or switch is captured, if it has not already been captured by generated events.
- Every 24 hours, the hardware resources are polled to determine the current hardware resources and refresh its hardware inventory information with the obtained information. This 24-hour polling ensures that any hardware change that has occurred in the system in the last 24 hours is captured.

In addition to alerts raised as a result of conditions found by the periodic polling, certain events initiate the raising of alerts at the time when those events are generated. Unless noted otherwise in the following table, the event-initiating alert's name is the event's name plus the suffix `_ALERT` added to the end of the event name. As an example, the `BMC_AUTHENTICATION_FAILURE` event raises the alert named `BMC_AUTHENTICATION_FAILURE_ALERT`. See [Event Catalog](#) for a list of the event definitions that you can view in the Event Catalog user interface.

Some of the alerts are more likely to be raised during the Power On System Validation (POSV) portion of the bring-up process. As an example, the alert named `VMWARE_CLOUD_FOUNDATION_BUNDLE_INCOMPLETE_ALERT` is raised during POSV if the system detects elements are missing from the software ISO file. For the list of alerts that are raised during POSV, see the *VMware Cloud Foundation Overview and Bring-Up Guide*.

After each polling interval, the built-in problem-detection service is called to analyze the updated status and inventory information and determine whether a persistent condition exists. If a problem that requires human intervention exists, an alert is raised. Even though multiple events can be generated for a particular outstanding problem, only one alert is created about the persistent problem. You then verify and resolve the reported problem and clear the alert using the SDDC Manager Dashboard.

You can use the Alerts Catalog page in the SDDC Manager Dashboard to view the SDDC Manager alert definitions. You open the Alert Catalog from the System Alerts page by clicking **Catalog**. For more information about using the Alerts Catalog page, see [Alert Catalog](#).

Table 10-4. SDDC Manager Alerts

Alert Name	Short Description	Severity	Detected By
<code>CONFIGURATION_BACKUP_TRIGGER_ALERT</code>	This alert is raised when domain creation, domain deletion, password rotation, domain expansion, host addition, rack addition, host decommission is done.	INFO	Event 30-minute poll 24-hour poll
<code>COORDINATION_SERVICE_DOWN_ALERT</code>	The system cannot establish a connection to the virtual machines that provide the required coordination service. The bring-up process requires connection to the coordination service.	CRITICAL	Event 30-minute poll 24-hour poll
<code>CPU_EXTRA_ALERT</code>	The polling found an additional CPU that does not match what is expected according to the manifest.	WARNING	24-hour poll

Table 10-4. SDDC Manager Alerts (Continued)

Alert Name	Short Description	Severity	Detected By
CPU_INVALID_ALERT	The polling detected a type of CPU in the server that does not match what is expected according to the manifest.	WARNING	24-hour poll
CPU_UNDETECTED_ALERT	The polling did not detect a CPU that matches what is expected according to the manifest.	ERROR	24-hour poll
HDD_DOWN_ALERT	Operational status is down for an HDD. This alert is initiated by the HDD_DOWN event.	ERROR	Event
HDD_EXCESSIVE_READ_ERRORS_ALERT	Excessive read errors reported for an HDD. This alert is initiated by the HDD_EXCESSIVE_READ_ERRORS event.	WARNING	Event
HDD_EXCESSIVE_WRITE_ERRORS_ALERT	Excessive write errors reported for an HDD. This alert is initiated by the HDD_EXCESSIVE_WRITE_ERRORS event.	WARNING	Event
HDD_EXTRA_ALERT	The polling found an additional HDD that does not match what is expected according to the manifest.	WARNING	24-hour poll
HDD_INVALID_ALERT	The polling detected a type of HDD that does not match what is expected according to the manifest.	WARNING	24-hour poll
HDD_TEMPERATURE_ABOVE_THRESHOLD_ALERT	HDD temperature has reached its maximum safe operating temperature. This alert is initiated by the HDD_TEMPERATURE_ABOVE_THRESHOLD event.	WARNING	Event
HDD_UNDETECTED_ALERT	The polling did not detect an HDD that matches what is expected according to the manifest.	WARNING	24-hour poll
HDD_WEAROUT_ABOVE_THRESHOLD_ALERT	Wear-out state of an HDD is above its defined threshold. This alert is initiated by the HDD_WEAROUT_ABOVE_THRESHOLD event.	WARNING	Event
HMS_AGENT_DOWN_ALERT	The Hardware Management Services (HMS) aggregator cannot communicate with the HMS agent on the rack's management switch through the private management network, either because the agent is down or the network is not available. This alert is initiated by the HMS_AGENT_DOWN event or by polling.	CRITICAL	30-minute poll 24-hour poll Event
HMS_DOWN_ALERT	The SDDC Manager cannot communicate with the HMS aggregator.	CRITICAL	30-minute poll 24-hour poll Event
HOST_AGENT_NOT_ALIVE_ALERT	This alert is raised when the polling detects that an ESXi host does not have its hostd process running or when the system is unable to determine if the hostd process is running. The hostd (host daemon) is an infrastructure service agent in the ESXi operating system.	CRITICAL	30-minute poll 24-hour poll

Table 10-4. SDDC Manager Alerts (Continued)

Alert Name	Short Description	Severity	Detected By
HOST_CANNOT_BE_USED_ALERT	Host {SERVER} in rack {RACK} was not configured correctly when it was added to the inventory. For information on why the host was not configured, see the VMware Cloud Foundation Overview and Bring-Up Guide.	CRITICAL	Event
HOST_DISKS_UNUSABLE_ALERT	This alert is raised if the disks in the host are not suitable for use with VSAN, either due to physical health or configuration issues. Please check physical connectivity of disks in the host to assure all are present. Also check the configuration of the disks on the ESXi host. For additional assistance, please contact support.	CRITICAL (DEBUG in logs)	30-minute poll 24-hour poll
HOST_VSAN_UNUSABLE_ALERT	This alert is raised if the vSAN status in the host is not suitable for use, either due to physical health or configuration issues. Please check physical connectivity of disks in the host to assure all are present and check the configuration of the disks on the ESXi host. For additional assistance, please contact support.	CRITICAL	30-minute poll 24-hour poll
LICENSE_PRESENT_CHECK_FAILED_ALERT	The check for the license for a particular bundle failed.	WARNING	Event
MANAGEMENT_SWITCH_DOWN_ALERT	Operational status is down for a physical rack's management switch. This alert is initiated by the periodic polling and by the MANAGEMENT_SWITCH_DOWN event.	WARNING	Event 30-minute poll 24-hour poll
MANAGEMENT_SWITCH_EXTRA_ALERT	The polling found an additional management switch that does not match what is expected according to the manifest.	WARNING	24-hour poll
MANAGEMENT_SWITCH_INVALID_ALERT	The polling detected a type of management switch that does not match what is expected according to the manifest.	CRITICAL	24-hour poll
MANAGEMENT_SWITCH_PORT_DOWN_ALERT	Operational status is down for a switch port in a physical rack's management switch. This alert is initiated by the MANAGEMENT_SWITCH_PORT_DOWN event.	WARNING	Event
MEMORY_EXTRA_ALERT	The polling found additional memory that does not match what is expected according to the manifest.	WARNING	24-hour poll
MEMORY_INVALID_ALERT	The polling detected a type of memory that does not match what is expected according to the manifest.	WARNING	24-hour poll
MEMORY_UNDETECTED_ALERT	The polling did not detect memory that matches what is expected according to the manifest.	WARNING	24-hour poll

Table 10-4. SDDC Manager Alerts (Continued)

Alert Name	Short Description	Severity	Detected By
NETWORK_DOWN_ALERT	<p>Network is down. The data connectivity among the servers transiting the switches cannot be assured.</p> <p>This alert is raised when the inter-switch connectivity of our deployment is incorrect. Connectivity loss may be due to:</p> <ul style="list-style-type: none"> ■ Switch port is physically down: no cable connected, wrong cable type, bad cable, loose connection, unsupported SFP, bad port. ■ Switch port has been administratively shut down. ■ Switch port has an error: such as bad or unsupported SFP, duplex mismatch, UDLD detects one-way link, BPDU port-guard and portfast configured simultaneously. 	CRITICAL	<p>30-minute poll</p> <p>24-hour poll</p>
NIC_EXTRA_ALERT	The polling found an additional NIC that does not match what is expected according to the manifest.	WARNING	24-hour poll
NIC_INVALID_ALERT	The polling detected a type of NIC that does not match what is expected according to the manifest.	WARNING	24-hour poll
NIC_PORT_DOWN_ALERT	Operational status is down for a NIC port in a rack's server. This alert is initiated by the NIC_PORT_DOWN event.	WARNING	Event
NIC_UNDETECTED_ALERT	The polling did not detect a NIC that matches what is expected according to the manifest.	WARNING	24-hour poll
POSTGRES_DOWN_ALERT	The system cannot connect to an internal database.	CRITICAL	Event
SDDC_MANAGER_NON_OPERATIONAL_ALERT	SDDC Manager is non-operational. A service in the SDDC Manager controller VM has failed and could not be restarted successfully.	ERROR	Event
SERVER_DOWN_ALERT	Server is in the powered-down state. This alert is initiated by the SERVER_DOWN event.	CRITICAL	<p>Event</p> <p>30-minute poll</p> <p>24-hour poll</p>
SERVER_EXTRA_ALERT	The polling detected an additional server that does not match what is expected according to the manifest.	WARNING	24-hour poll
SERVER_INVALID_ALERT	The polling detected a type of server that does not match what is expected according to the manifest.	WARNING	24-hour poll
SERVER_UNDETECTED_ALERT	The polling did not detect a server that matches what is expected according to the manifest.	ERROR	<p>30-minute poll</p> <p>24-hour poll</p>
SPINE_SWITCH_DOWN_ALERT	Operational status is down for a physical rack's inter-rack switch. This alert is initiated by the periodic polling and by the SPINE_SWITCH_DOWN event.	ERRORS	<p>Event</p> <p>30-minute poll</p> <p>24-hour poll</p>

Table 10-4. SDDC Manager Alerts (Continued)

Alert Name	Short Description	Severity	Detected By
SPINE_SWITCH_EXTRA_ALERT	The polling detected an additional inter-rack switch that does not match what is expected according to the manifest.	WARNING	24-hour poll
SPINE_SWITCH_INVALID_ALERT	The polling detected a type of inter-rack switch that does not match what is expected according to the manifest.	ERROR	24-hour poll
SPINE_SWITCH_PORT_DOWN_ALERT	Operational status is down for a switch port: in a physical rack's inter-rack switch. This alert is initiated by the SPINE_SWITCH_PORT_DOWN event.	WARNING	Event
SSD_DOWN_ALERT	Operational status is down for an SSD. This alert is initiated by the SSD_DOWN event.	ERROR	Event
SSD_EXCESSIVE_READ_ERRORS_ALERT	Excessive read errors reported for an SSD. This alert is initiated by the SSD_EXCESSIVE_READ_ERRORS event.	WARNING	Event
SSD_EXCESSIVE_WRITE_ERRORS_ALERT	Excessive write errors reported for an SSD. This alert is initiated by the SSD_EXCESSIVE_WRITE_ERRORS event.	WARNING	Event
SSD_EXTRA_ALERT	The polling found an additional SSD that does not match what is expected according to the manifest.	WARNING	24-hour poll
SSD_INVALID_ALERT	The polling detected a type of SSD that does not match what is expected according to the manifest.	WARNING	24-hour poll
SSD_TEMPERATURE_ABOVE_THRESHOLD_ALERT	SSD temperature has reached its maximum safe operating temperature. This alert is initiated by the SSD_TEMPERATURE_ABOVE_THRESHOLD event.	WARNING	Event
SSD_UNDETECTED_ALERT	The polling did not detect an SSD that matches what is expected according to the manifest.	WARNING	24-hour poll
SSD_WEAROUT_ABOVE_THRESHOLD_ALERT	Wear-out state of an SSD is above its defined threshold. This alert is initiated by the SSD_WEAROUT_ABOVE_THRESHOLD event.	WARNING	Event
STORAGE_CONTROLLER_DOWN_ALERT	Operational status is down for a storage adapter. This alert is initiated by the STORAGE_CONTROLLER_DOWN event.	ERROR	Event
STORAGE_CONTROLLER_EXTRA_ALERT	The polling detected an additional storage adapter that does not match what is expected according to the manifest. The alert message includes the PCI ID of the controller.	WARNING	24-hour poll
STORAGE_CONTROLLER_INVALID_ALERT	The polling detected a type of storage adapter that does not match what is expected according to the manifest. The alert message includes the PCI ID of the controller.	WARNING	24-hour poll
STORAGE_CONTROLLER_UNDETECTED_ALERT	The polling did not detect a storage adapter that matches what is expected according to the manifest. The alert message includes the PCI ID of the controller.	WARNING	24-hour poll

Table 10-4. SDDC Manager Alerts (Continued)

Alert Name	Short Description	Severity	Detected By
TOR_SWITCH_DOWN_ALERT	Operational status is down for a physical rack's ToR switch. This alert is initiated by the periodic polling and by the TOR_SWITCH_DOWN event.	ERROR	Event 30-minute poll 24-hour poll
TOR_SWITCH_EXTRA_ALERT	The polling found an additional ToR switch that does not match what is expected according to the manifest.	WARNING	24-hour poll
TOR_SWITCH_INVALID_ALERT	The polling detected a type of ToR switch that does not match what is expected according to the manifest.	ERROR	24-hour poll
TOR_SWITCH_PORT_DOWN_ALERT	Operational status is down for a switch port in a physical rack's ToR switch. This alert is initiated by the TOR_SWITCH_PORT_DOWN event.	WARNING	Event
VCF_CONFIGURATION_BACKUP_NOT_CONFIGURED_ALERT	There is no scheduled backup of the VMware Cloud Foundation configuration.	WARNING	Event
VMWARE_CLOUD_FOUNDATION_BUNDLE_INCOMPLETE_ALERT	The ISO file is missing items, according to its manifest.	CRITICAL	Event
VMWARE_CLOUD_FOUNDATION_BUNDLE_INVALID_ALERT	Checksum validation for the ISO file failed.	CRITICAL	Event
VMWARE_CLOUD_FOUNDATION_BUNDLE_MISSING_ALERT	A required ISO file or its expected checksum file or manifest file is missing.	CRITICAL	Event

Using vRealize Log Insight Capabilities in Your Cloud Foundation System

The vRealize Log Insight instance that is deployed by SDDC Manager is licensed separately. When the vRealize Log Insight instance is licensed for use in your Cloud Foundation environment, you can use the capabilities of vRealize Log Insight to work with the event and log data that is collected from the various hardware devices and SDDC virtual infrastructure.

vRealize Log Insight is a log aggregator that provides simplified log viewing and analysis. Events and log content for the environment's physical resources and the virtual infrastructure are collected by the vRealize Log Insight instance, which indexes them and then provides unified querying and analysis of the content for problem diagnosis and repair. As a result, logging in to the vRealize Log Insight Web interface provides a unified view of event and log information to assist with troubleshooting. Data from the events and audit events raised by SDDC Manager is also sent to the vRealize Log Insight instance, and you can use its searching, query, and reporting features to create trend reports and auditing reports from the event history.

You can configure the vRealize Log Insight instance for remote syslog forwarding to an instance of vRealize Log Insight that is external to the Cloud Foundation system or to another syslog server. You configure vRealize Log Insight to forward incoming events to a syslog target using the Event Forwarding page of the vRealize Log Insight Web interface. For the steps on configuring event forwarding in the vRealize Log Insight Web interface, see [Add vRealize Log Insight Event Forwarding Destination](#) in the vRealize Log Insight 3.3 documentation center at <http://pubs.vmware.com/log-insight-33/index.jsp>.

For the steps to log in to the vRealize Log Insight Web interface from the SDDC Manager Dashboard, see [Get Started Using the vRealize Log Insight Instance](#).

Note The vRealize Log Insight environment that SDDC Manager deploys is sized for monitoring the hardware and software of your Cloud Foundation installation only. The default sizing accommodates the events and logs expected to be sent by the Cloud Foundation environment. This sizing might not accommodate the numbers of events and logs coming from additional applications or VMs that reside outside of your Cloud Foundation environment. Therefore, configuring the vRealize Log Insight environment that is deployed by SDDC Manager to collect events logs from additional applications or VMs that reside outside of your Cloud Foundation environment is not supported in this release.

Content Packs

The vRealize Log Insight instance includes a set of content packs. Content packs are read-only plug-ins to vRealize Log Insight that provide pre-defined knowledge about specific types of events such as log messages. The purpose of a content pack is to provide knowledge about a specific set of events in a format that is easily understandable by administrators, monitoring teams, and executives. A content pack consists of information that can be saved from either the Dashboards or Interactive Analytics pages in the vRealize Log Insight Web interface. Such information typically includes:

- Queries
- Fields
- Aggregations
- Alerts
- Dashboards

The vRealize Log Insight instance includes a number of VMware content packs, including the Cloud Foundation content pack. For a detailed description of the Cloud Foundation content pack, see [SDDC Manager Content Pack](#). For descriptions of the other installed content packs, use the Content Packs choice from the upper right drop-down menu in the vRealize Log Insight Web interface and select the content pack's name in the list.

Content Pack	Overview
Cloud Foundation	This content pack includes an overview dashboard that gives overall summary views of the data sent by the Cloud Foundation, and also provides detailed views for the various levels of interest, such as rack-level, server-level, switch-level, device-level, and so on.
General	This content pack includes four dashboards, providing generic information about any events being sent to the vRealize Log Insight instance, configured vRealize Log Insight agents, and information discovered by the machine learning capabilities
vSphere	This content pack provides various dashboards and filters to give you insight into the data that is sent by the management and workload domains' vCenter Server instances.
NSX for vSphere	This content pack provides various dashboards and filters to give you insight into the data that is sent by the NSX for vSphere virtual infrastructure in the management and workload domains' vCenter Server instances.
Horizon View	This content pack provides various dashboards and filters to give you insight into the data that is sent by the VDI workload domain's virtual infrastructure. Log information from the VDI workload domain's servers is collected and consolidated.
vSAN	This content pack provides various dashboards and filters to give you insight into the logs that are sent by the management and workload domains' vSAN features.

To see the dashboards for one of the content packs in the vRealize Log Insight Web interface, select **Dashboards** and then select the specific content pack in the left hand drop-down menu.

SDDC Manager Content Pack

The SDDC Manager content pack provides graphical summary views for various SDDC Manager events that are sent to vRealize Log Insight. The content pack organizes the views into multiple tabs that display collected information about various aspects of the system. The top **Overview** tab includes high-level overview of all events such as count of events by severity, count of events by rack, critical events by server and by switch, server and network events by rack, timeline view of events, audit event summary and so on. The content pack's other tabs provide detailed information about events at the various hardware levels of the system, such as the rack-level, server-level, switch-level, component-level, and so on. As a result, this set of tabs gives you the ability to get an overall cross-system view using the **Overview** tab, and then drill-down into the hardware level you are interested in by using the other tabs.

The **Audits - Summary** tab provides views of the collected audit event data by severity, by system audit event and user audit event, and a timeline view of audit events.

Get Started Using the vRealize Log Insight Instance

Use of the vRealize Log Insight instance that is deployed by SDDC Manager is licensed separately. vRealize Log Insight delivers real-time log management for VMware environments, providing visibility of logs and easier troubleshooting across the physical and virtual infrastructure in your Cloud Foundation system.

During the bring-up process of your system, SDDC Manager deploys and configures the vRealize Log Insight virtual appliance. When you have the license to use that deployed vRealize Log Insight instance, you use the vRealize Log Insight Web interface to perform the tasks related to the collected log and events data, such as troubleshooting and trend analysis and reporting tasks.

Note The vRealize Log Insight environment that SDDC Manager deploys is sized for monitoring the hardware and software of your Cloud Foundation installation only. The default sizing accommodates the events and logs expected to be sent by the Cloud Foundation environment. This sizing might not accommodate the numbers of events and logs coming from additional applications or VMs that reside outside of your Cloud Foundation environment. Therefore, configuring the vRealize Log Insight environment that is deployed by SDDC Manager to collect events logs from additional applications or VMs that reside outside of your Cloud Foundation environment is not supported in this release.

Also as part of the bring-up process, content packs are installed and configured in the vRealize Log Insight instance. In vRealize Log Insight, a content pack provides dashboards, extracted fields, predefined queries, and alerts that are related to the content pack's specific product or set of logs. When you launch the vRealize Log Insight Web interface, the installed content packs are ready for use. For an overview of these content packs, see [Using vRealize Log Insight Capabilities in Your Cloud Foundation System](#). For detailed information on how to use the dashboards, predefined queries, and collected log data in vRealize Log Insight, see the vRealize Log Insight product documentation at <https://www.vmware.com/support/pubs/log-insight-pubs.html>.

From the SDDC Manager Dashboard, you can open the vRealize Log Insight Web interface using the following methods. During a logged-in session of the SDDC Manager Dashboard, you must authenticate to vRealize Log Insight the first time you open the vRealize Log Insight Web interface. Subsequent launches do not require re-authentication until the cache for the logged-in session expires or you log out of the vRealize Log Insight Web interface. The launch of the Web interface is context-aware. For example, if you launch using the **Analysis** button from the Audit Events page, the vRealize Log Insight display is filtered to show the audit events only. You can navigate within the Web interface to view other information collected from your environment.

If this is the first time after the initial bring-up process that the vRealize Log Insight Web interface is launched, type the system-assigned credentials into the login screen and then click **Login**. Then use the vRealize Log Insight Web interface to assign permissions to your superuser account and other user accounts. You can look up the system-assigned credentials for the vRealize Log Insight Web interface by logging in to the SDDC Manager VM and running the `/home/vrack/bin/lookup-password` command. See [Credentials for Logging in to the SDDC Manager VM](#) and [Look Up Account Credentials](#).

Note Do not change the password of the admin account from within the vRealize Log Insight Web interface, or unpredictable results can occur. To change the admin account's password without rotating all account passwords, see [Rotate Passwords On-Demand for Managed Physical and Logical Entities](#).

Procedure

- 1 Open the vRealize Log Insight Web interface.

Option	Description
From the Audit Events page, click the Analysis button.	The vRealize Log Insight display is filtered to show the collected audit events only.
From the Events page, click the Analysis button.	The vRealize Log Insight displays all collected events.
From a management domain's details, click the launch link listed in the Management Info area.	The vRealize Log Insight displays all collected events.

- 2 If the vRealize Log Insight login screen appears, log in with the appropriate credentials.
 - If this is the first time logging in to vRealize Log Insight after the initial bring-up process, use the username **admin** and the randomized password that was set when the passwords were rotated at the end of the bring-up process.
 - If you are using an account that was set up for you in vRealize Log Insight, use those credentials to log in.

When you are logging in to the vRealize Log Insight Web interface with the **admin** account after doing a password rotation, you must use the randomized password that is set for that account by the rotation procedure. For details about password rotation, see [Chapter 4 Changing the Passwords of Your Cloud Foundation System On Demand](#).

The vRealize Log Insight Web interface appears with the display filtered to show the events that meet the criteria for the launch context from SDDC Manager.

What to do next

Examine the descriptions of the content packs that are available by selecting **Content Packs** in the upper right corner menu.

Examine the data available in the content packs. To display the dashboards for an installed content pack, click **Dashboards** and use the drop-down menu at the upper left to select the content pack.

Enable login accounts for additional users. See the [Managing User Accounts in vRealize Log Insight](#) topic and its subtopics in the vRealize Log Insight product documentation available at the following locations:

- From the **Help** menu choice in the vRealize Log Insight Web interface.
- In the vRealize Log Insight product documentation online at <http://pubs.vmware.com/log-insight-33/index.jsp>.

For detailed information about how to use the content packs and other capabilities of the vRealize Log Insight Web interface, see the vRealize Log Insight product documentation also available at those two locations.

Configure Syslog from the Switches to vRealize Log Insight

A vRealize Log Insight instance is a syslog collector. When vRealize Log Insight is licensed for use in your Cloud Foundation system, you can manually configure the switches to export their log files to the vRealize Log Insight instance.

Prerequisites

Verify that you have the root account credentials to log in to the SDDC Manager VM. The root account credentials are managed by your organization. See [Credentials for Logging in to the SDDC Manager VM](#).

Procedure

- 1 SSH to the SDDC Manager VM.
- 2 Change to the `/home/vrack/bin` directory.
- 3 Configure ability to export the switches' log files to the vRealize Log Insight instance by typing the command:

```
./vrm-cli.sh configure-syslog
```

The command output displays information that the command is running and when it is finished.

What to do next

Log in to the vRealize Log Insight Web interface to verify that it is receiving the logs. For steps for logging in, see [Get Started Using the vRealize Log Insight Instance](#).

Settings Configuration Using SDDC Manager

11

Use the Settings area of SDDC Manager to review and configure settings for parameters that are used in various features of the environment.

This chapter includes the following topics:

- [Customize Default Values Used When Creating VDI Workload Domains](#)
- [Additional Rack Settings Screen](#)
- [Managing Network Settings](#)

Customize Default Values Used When Creating VDI Workload Domains

You can set default values for some of the parameters that SDDC Manager uses when creating VDI workload domains so that each time you create a VDI workload domain, the default values are used. Some of the parameters for which you can set defaults are the prefixes for the View Connection Server names, the maximum number of virtual desktops per View Connection Server, among others.

When you create a VDI workload domain, the workflow creates those VDI-specific resources for a View infrastructure that are appropriate for the selections you make in the Configure VDI wizard. Default values are used for the View infrastructure's required parameters. You can customize those default values using the VDI Settings page.

Procedure

- 1 In the SDDC Manager Dashboard, navigate to **Settings > PHYSICAL RACK SETTINGS > VDI Settings**.
- 2 Set the page to edit mode by using the edit icon.

To change a parameter's value, type over the value currently displayed in the entry field for that parameter.

For descriptions of the parameters, see [VDI Infrastructure Settings](#).
- 3 Save your changes using the save icon.

The customized default values are subsequently used when a new VDI infrastructure is provisioned using the Create VDI wizard.

To revert to the original default values, click **RESTORE DEFAULTS** and then click **CONFIRM**.

VDI Infrastructure Settings

VDI infrastructure settings are the parameters that SDDC Manager uses when creating VDI workload domains.

VDI Parameters

If you do not customize these values, when you configure a new VDI workload domain, the default values are used for the VDI parameters. To see the steps for customizing these default values, see [Customize Default Values Used When Creating VDI Workload Domains](#).

Type	Default Value	Description
Internal AD Name	horizon.local	When the choice to deploy an internal Active Directory is selected in the configuration wizard, this name is used for the Active Directory DNS name.
AD VM Name prefix	ad-	When the choice to deploy an internal Active Directory is selected in the configuration wizard, this prefix is used in the name of the VM on which the Active Directory Domain Controller is installed. The actual name of the VM is generated by adding the VDI domain's ID plus an incremental number to the end of this prefix, starting with the number one (1).
Domain Net BIOS Name	HORIZON	When the choice to deploy an internal Active Directory is selected in the configuration wizard, this parameter sets the NetBIOS name of the Active Directory that is deployed in the VDI workload domain.
Domain Controller Name	DC1	When the choice to deploy an internal Active Directory is selected in the configuration wizard, this prefix is used as the server name prefix of the Active Directory Domain Controller. The actual name of the Domain Controller is generated by adding the VDI domain's ID plus an incremental number to the end of this prefix, starting with the number one (1).

Type	Default Value	Description
Virtual Desktops OU	CN=Computers,DC=horizon,DC=local	When the choice to deploy an internal Active Directory is selected in the configuration wizard, this parameter is the LDAP location within the internal Active Directory where the virtual desktops are deployed.
View Servers OU	OU=View,DC=horizon,DC=local	When the choice to deploy an internal Active Directory is selected in the configuration wizard, this parameter is the LDAP location within the internal Active Directory where the virtual servers are deployed.
Number of Server Processors	4 of 8	The number of processors a single VDI server must have in the deployed VDI workload domain.
Memory per Server	10 GB of 32 GB	The amount of memory a single VDI server must have in the deployed VDI workload domain.
Servers System Drive	80 GB of 400 GB	The size of the system drive that a single VDI server must have in the deployed VDI workload domain.
Connection Server Naming Convention	con-	The prefix used in the Horizon View Connection server names that are deployed in the infrastructure of the VDI workload domain. The server names are generated by adding the VDI workload domain ID plus an incremental number to the end of the prefix, starting with the number one (1).
Composer Server Naming Convention	com-	The prefix used in the Horizon View Composer server names that are deployed in the infrastructure of the VDI workload domain. The server names are generated by adding the VDI workload domain ID plus an incremental number to the end of the prefix, starting with the number one (1).
Security Server Naming Convention	sec-	The prefix used in the Horizon View Security server names that are deployed in the infrastructure of the VDI workload domain. The server names are generated by adding the VDI workload domain ID plus an incremental number to the end of the prefix, starting with the number one (1).

Type	Default Value	Description
Virtual Desktops Naming Convention	vm-	The prefix used in the names of the virtual desktops that are deployed in the VDI workload domain. The virtual desktop names are generated by adding the VDI workload domain ID plus an incremental number to the end of the prefix, starting with the number one (1).
Max Desktops per Connection Server	2000	Specifies the maximum number of virtual desktops that one Horizon View Connection server in the deployed VDI workload domain should handle. If the total number of virtual desktops exceeds this number, a Replica Connection server is deployed in the VDI environment.
Max Desktops per Security Server	500	Specifies the maximum number of virtual desktops that one Horizon View Security server in the deployed VDI workload domain should handle. If the total number of virtual desktops exceeds this number, a Replica Security server is deployed in the VDI environment.
Max Desktops per vCenter Server	2000	Specifies the maximum number of virtual desktops that a single VDI workload domain can handle. By default, each VDI workload domain is managed by a single vCenter Server instance. If the total number of virtual desktops exceeds this number, an additional vCenter Server instance is deployed.
Max Virtual CPUs per Core	4	Specifies the maximum number of virtual processors (vCPUs) that a physical core on the ESXi hosts should handle.
Desktop System Drive Size [GB]	60	Specifies the size (in GB) of the data drive that is configured as a D: drive for each virtual desktop.
Desktop System Snapshot Size	5	Specifies the size (in GB) of the data drive that is configured as a snapshot for each virtual desktop.

Type	Default Value	Description
Desktops accessed via the Internet [%]	10	Specifies the percentage of the virtual desktops that are going to connect to this VDI workload domain from outside your corporate network compared to the total number of virtual desktops handled by this VDI workload domain.
Desktop Pool Name Prefix	pl-	The prefix used in the desktop pool names that are deployed in the infrastructure of the VDI workload domain. The pool names are generated by adding the VDI workload domain ID plus an incremental number to the end of the prefix, starting with the number one (1).

Additional Rack Settings Screen

Use the Additional Rack Settings screen to add physical racks to your Cloud Foundation installation.

As described in the *VMware Cloud Foundation Overview and Bring-Up Guide*, when you follow the steps to power on a new rack and use the inter-rack switches to connect it to the system's existing racks, the thumbprint of the added rack is displayed in this screen. Then you start the Add Rack wizard to verify the identity of the new rack using its thumbprint and bootstrap password.

See the Bringing-Up on Additional Racks procedure in the *VMware Cloud Foundation Overview and Bring-Up Guide* for the detailed steps.

Managing Network Settings

Use the Network Settings screen to examine and make changes to network-related settings in your Cloud Foundation installation.

Manage Uplink Connectivity Settings Using SDDC Manager

After the Cloud Foundation bring-up process, you can use the Uplink screen in the SDDC Manager to review and update the uplink connectivity settings. The uplinks are used by the top-of-rack (ToR) switches to carry traffic to your corporate network.

Note Not every feature that the ToR switches support can be configured using the SDDC Manager Dashboard. You must manually set advanced switch features during installation of the physical rack. Examples of these advanced switch features are spanning tree parameters, redundancy features using Hot Standby Router Protocol (HSRP), and so on.

The ToR uplink settings are entered during the bring-up process. The ToR uplink connectivity can be either L2 or L3 to the upstream network. After the bring-up process, you use this screen to change the settings that were previously entered.

Note You cannot use this screen to change the uplink type, from L2 to L3 or L3 to L2.

For additional information, see [Chapter 17 Rack Wiring](#) in this guide, and the following topics in the *VMware Cloud Foundation Overview and Bring-Up Guide*: [Physical Topology](#) and [Specify Datacenter Uplink Details](#).

Prerequisites

If you plan to change the uplink settings, connect to port 48 on the management switch and log in to SDDC Manager using that connection.

Important Changing the settings triggers uplink reconfiguration on the switches. Because the reconfiguration process might take a few minutes to complete, connectivity to the corporate network might be lost during the process. To avoid losing connectivity with SDDC Manager, it is strongly recommended that you are connected to port 48 on the management switch when updating the settings using this screen.

Procedure

- 1 In the SDDC Manager Dashboard, navigate to **Settings > NETWORK SETTINGS > UPLINK**.
- 2 Review the current uplink settings.

Option	Description
Uplink Type	This field indicates whether the current ToR uplink uses L2 or L3 settings. Read-only.
Uplink LAG Enabled	Specify whether to enable link aggregation (LAG), YES or NO .
Uplink Ports	Specify the ToR switch ports that are cabled as the uplink to your corporate network. Ports must be in the ranges: <ul style="list-style-type: none"> ■ 43 to 46, for uplink speeds less than 40Gbps ■ 51 to 54, for a 40Gps uplink speed ■ When LAG is not enabled, the ToR switch uplink uses one port number in the valid range. ■ When LAG is enabled, the ToR switch uplink can use up to four ports. Typically the number of switch ports in the uplink is related to the required bandwidth.
Uplink IP	For an L3 uplink, this field displays the starting IP used for the L3 uplink.
Mask IP	For an L3 uplink, this field displays the netmask used for the L3 uplink.
Next-hop IP	For an L3 uplink, this field displays the IP address used for the next hop IP.
Uplink Speed	This field displays the uplink speed in Gbps.

3 Click **Edit** to update the settings.

When you edit the settings, you click **Save Edits** to save your changes.

About Excluding IP Address from SDDC Manager Use

You can exclude IP addresses in the subnets used in your installation to prevent SDDC Manager from assigning those addresses to resources.

SDDC Manager allocates IP addresses to resources from the subnets you enter during the Cloud Foundation bring-up process or during the workload domain creation process. When those subnets include IP address that are already used in your corporate network for other purposes, or which you want to reserve for another use, you exclude those IP addresses to prevent IP conflicts.

SDDC Manager has two types of exclusions:

Global exclusions Global exclusions are persistent and are configured using the IP Exclusions area on the IP Distribution screen. See [IP Distribution Screen](#).

Local exclusions Local exclusions are valid until another local exclusion is subsequently created for that subnet's addresses. For each subnet, the most recent local exclusion overwrites the earlier one. Local exclusions are created by the bring-up process and the VI workload domain creation workflow.

For example, during the bring-up process on the first rack in a Cloud Foundation installation, specifying excluded IP addresses in the management subnet screen of the bring-up wizard prevents the software from using those excluded IP addresses as it assigns management IPs to the physical and logical resources involved in this process, such as the ESXi hosts in the rack, the management domain and the virtual appliances, and so on. The list of excluded IP addresses is saved.

Then, during creation of a VI workload domain, the software uses the same management network subnet that was used during bring-up process. When you specify excluded IP addresses for the management network subnet in the VI workload domain creation wizard, that list of excluded IP addresses replaces the excluded IP addresses that were entered during the bring-up process.

IP Distribution Screen

You use the IP Distribution screen to work with the set of excluded IP addresses and to download information about the IP addresses allocated by the SDDC Manager software's IP address management (IPAM).

IP Exclusions

This area displays the set of IP addresses and range of addresses that are currently registered in the software as excluded addresses. SDDC Manager is prevented from assigning the IP addresses in this set to resources. You usually want to exclude an IP address when it is already assigned to a service in your corporate network or which you want reserved for other uses.

SDDC Manager allocates IP addresses to internal resources from the subnets you enter during the Cloud Foundation bring-up process or during the Virtual Infrastructure workload domain creation process. When those subnets include IP address that are already used in your corporate network for other purposes, or which you want to reserve for another use, you exclude those IP addresses to prevent IP conflicts. Using this screen, you can add those IP addresses or ranges of addresses that you want to prevent from automatic assignment to resources in your Cloud Foundation system. Excluding such IP addresses helps to prevent IP conflicts.

When you make a change in this screen, you must use the **Update** button to confirm the change.

Add to the excluded set by entering the address or range that you want to exclude, clicking **+**, and clicking **Update**. Remove an item from the set by clicking its **-** and clicking **Update**.

IP Allocations

Click **Download** to download a CSV file that contains information about the IP address allocations made by IPAM, such as:

- Information about each subnet established in your system, such as the subnet address, broadcast address, and so on
- Number of IPs currently available in each subnet
- The distributed port group associated with each subnet

Data Center Screen

You use the Data Center screen to manage the relationships between workload domains and the data center network connections that are in place for your Cloud Foundation system. You can review the information for the existing connections, add new data center connections, associate and disassociate data center connections with workload domains, and remove data center connections that are no longer associated with a workload domain.

A data center network consists of a connection name, VLAN ID, IP subnet, subnet mask, and DHCP relay agent.

Data Center Connections

By default, this screen opens with the **New Connection** choice selected and the fields for defining a new data center connection displayed. Click **Cancel** if you want to review the list without creating a new data center connection.

The screen displays the list of data center connections that are already established. For a Cloud Foundation system, a data center connection specifies the network (VLAN and vSphere portgroup) that carries traffic between VMs and the networking environment external to the system, such as your corporate network. During the Cloud Foundation bring-up process, a data center connection was specified. During ongoing operations, a data center connections can be specified when creating a new workload domain. Also, additional data center connections can be specified and associated with existing workload domains.

Note Associations between data center connection and VDI workload domains must be one to one. A VDI workload domain cannot share data center connections with any other management or workload domain.

In the Data Center screen you can:

- Examine the settings of a data center connection and the workload domains that are associated with it by selecting its name. By default, the management domains that are associated with the data center connection are also displayed. The management and workload domains that are associated with the selected data center connection are highlighted.
- Add a new data center connection by clicking **Actions > ADD NEW DATACENTER NETWORK**, typing the network details (such as connection name, VLAN ID, IP subnet, subnet mask, and DHCP relay agent), and clicking **Save**.
- Associate a data center connection with a workload domain by selecting the data center connection, clicking **Actions > ASSOCIATE DOMAINS**, and clicking the workload domain's icon.

You can also click **NEW CONNECTION** and enter the network details, selecting the management or workload domain, and click **Save**.

- Disassociate the data center connection from an associated workload domain by selecting the data center connection and clicking the workload domain's icon.
- Remove a data center connection that is no longer associated with any management or workload domains by selecting it and clicking **Actions > REMOVE**. You cannot remove a data center connection if it has an associated management or workload domain.

License Management

You can manage the licenses for your Cloud Foundation system in the SDDC Manager Dashboard.

This chapter includes the following topics:

- [Cloud Foundation Licensing Model](#)
- [Manage License Keys for the Software in Your Cloud Foundation System](#)
- [Enable vRealize Log Insight Logging for Workload Domains](#)

Cloud Foundation Licensing Model

The SDDC Manager software is licensed under the Cloud Foundation license. As part of the Cloud Foundation product, SDDC Manager deploys specific VMware software products, some of which are licensed under the Cloud Foundation license and some are licensed separately.

The following VMware software deployed by SDDC Manager is licensed under the Cloud Foundation license:

- VMware vSphere
- VMware vSAN
- VMware NSX for vSphere
- VMware vRealize Log Insight for the management domain

The following VMware software deployed by SDDC Manager is licensed separately:

- VMware vCenter Server
- VMware vRealize Log Insight for VI workload domains
- Content packs for Log Insight
- VMware Horizon
- VMware App Volumes
- vRealize Operations

- vRealize Automation

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

All physical processors in your system are licensed using the base Cloud Foundation license.

Product	Product Licensing Model Within the Base License
VMware vSphere®	Per CPU
VMware vSAN™	Per CPU
VMware NSX® for vSphere®	Per CPU

Manage License Keys for the Software in Your Cloud Foundation System

Use the Licensing screen of the SDDC Manager Dashboard to work with the Cloud Foundation license keys.

In the Licensing screen, you can:

- Review the license keys that are currently assigned in your system.
- Enter license keys.
- Edit the descriptions of the assigned license keys. The descriptions are displayed in the Licensing screen.

Procedure

- 1 On the SDDC Manager Dashboard, navigate to **Settings > Licensing**.
- 2 Manage the license keys using the action menus in the screen.

Option	Description
Enter a license key by clicking Actions > Add License Key.	The Add License window opens for entering the details. Type in the license key and an optional description and click Verify . When the verification is successful, click Add .
Edit the description of an already entered license key by clicking the Edit choice in the action menu next to that license key.	In the Add License window, edit the description and save your changes.

Enable vRealize Log Insight Logging for Workload Domains

During the bring-up process on the first rack, vRealize Log Insight is deployed and configured to collect logs from the management domain components (vCenter, NSX Manager, and SDDC Manager). To enable logging on VI and VDI workload domains, you must opt-in and agree to provide your own license for vRealize Log Insight. After you opt-in, Cloud Foundation automatically connects vRealize Log Insight to the workload domains. You can then enter the license key for vRealize Log Insight.

Once logging is enabled for workload domains, you cannot disable this setting.

Procedure

1 On the SDDC Manager Dashboard, navigate to **Settings > Logging**.

2 Click **Enable Logging for Workload Domains**.

3 In the Logging for Workload Domains window, click **Enable**.

The IP addresses for the external vRealize Log Insight and Sys Log servers are displayed.

4 Click **Update**.

5 On the SDDC Manager Dashboard, click **Licensing**.

6 Click **Actions > Add License Key**.

7 In the Add License window, type in the license key and an optional description.

8 Click **Verify**.

9 When the verification is successful, click **Add**.

Cloud Foundation connects vRealize Log Insight to workload domains.

Supportability and Serviceability (SoS) Tool

13

The SoS tool is a command-line Python tool that can be used for the following.

- Run health check.
- Collect audit information.
- Delete datacenter networks.
- Synch physical inventory IP addresses.
- Display configuration changes in your environment. See [Calculate Configuration Changes in Your Cloud Foundation System](#).
- Collect logs for Cloud Foundation components. See [Collect Logs for Your Cloud Foundation System](#)
- Take ESXi and Switch backups. See [Back Up Physical Switch Configurations](#).

To run the SoS tool, SSH in to the SDDC Manager VM using the root account, navigate to the `/opt/vmware/sddc-support` directory and type `./sos` followed by the options required for your desired operation.

```
./sos --option-1 --option-2 --option-3 ... --option-n
```

To list the available command options, use the `--help` long option or the `-h` short option.

```
./sos --help  
./sos -h
```

Note You can specify some options in the conventional GNU/POSIX syntax, using `--` for the long option and `-` for the short option.

SoS Tool Help Options

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

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

SoS Tool Options

These are generic options for the SoS tool.

Option	Description
--configure-sftp	Configures SFTP for logs and backup.
--debug-mode	Runs the SoS tool in debug mode.
--backup	Domain name on which the SoS operation is to be performed.
--domain-name <i>DOMAINNAME</i>	
--history	Displays the last twenty SoS operations performed.
--remote	Tags file for backup to SFTP.
--setup-json <i>SAMPLE_JSON</i>	Custom setup-json file for log collection. SoS prepares the inventory automatically based on the environment where it is running. If you want to collect logs for a pre-defined set of components, you can create a setup.json file and pass the file as input to SoS. A sample JSON file is available on the SDDC Manager VM in the /opt/vmware/sddc-support/ directory.
--zip	Creates a zipped tar file for the output.

SoS Tool Options for Health Check

These SoS commands are used for checking the health status of various components or services, including connectivity, compute, storage, database, domains, and networks.

A green status indicates that the health is normal, yellow provides a warning that attention may be required, and red (critical) indicates that the component needs immediate attention.

Option	Description
--certificate-health	Verifies that the component certificates are valid (within the expiry date).
--connectivity-health	Performs a connectivity health check to inspect whether the different components of the system such as the ESXi hosts, Virtual Center Servers, Inventory Service VMs, Log Insight VM, NSX Manager VMs, PSC VMs, SDDC Manager VM can be pinged.
--compute-health	Performs a compute health check.
--db-health	Performs a database health check.
--general-health	Verifies ESXi entries across all sources, checks the Postgres DB operational status for hosts, checks ESXi for error dumps, and gets NSX Manager and cluster status.

Option	Description
<code>--get-host-ips</code>	Returns server information.
<code>--get-used-ips</code>	Returns IP addresses that are being used in your environment.
<code>--health-check</code>	Performs all available health checks.
<code>--json-output-dir <i>JSONDIR</i></code>	Outputs health check results JSON file to the specified directory.
<code>--network-health</code>	Verifies whether the switches in the system are reachable and connectivity exists between the management, ToR, and inter-rack switches.
<code>--network-wire-map</code>	Performs a network wire map health check.
<code>--ntp-health</code>	Verifies whether the time on the components is synchronized with the NTP server in the SDDC Manager VM. It also ensures that the hardware and software timestamp of ESXi hosts are within 5 minutes of the SDDC Manager VM.
<code>--services-health</code>	Performs a services health check to confirm whether services within the Inventory Service VM (Cassandra / Zookeeper) and within SDDC Manager (like Life Cycle Management Server, Postgres DB server, NTP Server, HMS) are running
<code>--storage-health</code>	Performs a check on the VSAN disk health of the ESXi hosts and vCenter clusters. Also runs Proactive vSAN tests to verify ability to create VMs within the vSAN disks.

SoS Tool Options for Audit Data Collection

These SoS commands are used for collecting audit data. Audit data consists of version and configuration details obtained from the various physical and logical components that constitute VMware Cloud Foundation, including racks, servers, switches, domains and VMs.

Option	Description
<code>--audit</code>	This option collects audit information from all the components of Cloud Foundation. By default, audit data is saved in the <code>/var/tmp/audit-compliance/audit</code> directory as a JSON file. The log file is saved under <code>/var/tmp/audit-compliance/logs</code> .
<code>--audit-output-dir</code>	Use this option to save audit data JSON files to a directory other than the default <code>/var/tmp/audit-compliance</code> parent directory. Note This option can be used with the <code>--audit</code> option.
<code>--no-audit</code>	Use this option to prevent audit data collection during SoS log collection. By default, audit data collection runs when SoS log collection runs. This option prevents this default behavior.

SoS Tool Options for Deleting Datacenter Networks

Use these options to delete one or more datacenter networks.

Option	Description
<code>--delete-dc-nw</code>	Deletes a datacenter network.
<code>--dc-nw-name</code>	Passes datacenter network name to be deleted.
<code>DATACENTERNWA</code>	
<code>ME</code>	
<code>-v</code>	

SoS Tool Options for Physical Inventory IP Synchron

Use this option to check physical inventory IP address issues.

Option	Description
<code>sync-physical-inventory</code>	Check and resolve physical inventory IP address issues.

SoS Tool Options for Backing Up Configurations

Use the following SoS options when creating and configuring backups with the SoS tool.

Table 13-1. Backup Command Options

Command	Description
<code>--backup</code>	Creates a backup of the system configuration.
<code>--switch-backup</code>	Backs up the switch configuration.
<code>--esx-backup</code>	Backs up the ESXi configuration.
<code>--sddc-manager-backup</code>	Backs up the SDDC Manager configuration.
<code>--cassandra-backup</code>	Backs up the Cassandra configuration.
<code>--zk-backup</code>	Backs up the Zookeeper configuration.
<code>--hms-backup</code>	Backs up the HMS configuration.
<code>--host-mgmt-backup</code>	Backs up the Management Hosts.

Table 13-2. Backup Scheduling Options

Command	Description
<code>--schedule-backup</code>	Schedules periodic backup.
<code>--frequency-hours</code>	Sets backup interval in hours.
<code>--delete-backup-schedule</code>	Deletes existing scheduled backup.
<code>--get-backup-schedule</code>	Displays current backup schedule.
<code>--get-all-backups</code>	Gets most recent backup created by scheduler.
<code>--delete-all-backup</code>	Deletes all backups created by scheduler.

This chapter includes the following topics:

- [Calculate Configuration Changes in Your Cloud Foundation System](#)
- [Collect Logs for Your Cloud Foundation System](#)

Calculate Configuration Changes in Your Cloud Foundation System

After you create a baseline configuration for your system, you can calculate the configuration changes as compared to the baseline with the Config Insight tool. The *VMware Cloud Foundation Guardrails* document lists the base configuration for a Cloud Foundation system and includes information about supported configuration changes.

Calculate Configuration Changes

- 1 SSH in to the SDDC Manager VM.
- 2 Navigate to the `/opt/vmware/sddc-support` directory.
- 3 Start the Config Insight tool.

```
./sos --configinsight-start
```
- 4 Populate the database with the baseline configuration.

```
./sos --configinsight-discovery
```
- 5 (Optional) Retrieve information about the resource for which you want to calculate the configuration change.

```
./sos --configinsight-resourceinfo
```

Example output:

```
Welcome to Supportability and Serviceability(SoS) utility!
ConfigInsight Logs : /var/tmp/configinsight-2018-02-22-20-18-59-822
Log file : /var/tmp/configinsight-2018-02-22-20-18-59-822/sos.log

Fetching all resources info from the inventory...
For resource info please refer : /var/tmp/configinsight-2018-02-22-20-18-59-822/resource-info.json
```

- 6 Calculate configuration changes.

```
./sos --configinsight-drift --resource-type
{sddc,cluster,host,vcenter,psc,nsxmanager,vsan} | (--domain-name DOMAIN_NAME)
```

The output displays configuration changes for the specified resource or domain as compared to the baseline you generated in step 4. If you do not specify the `--resource-type` or `--domain-name` option, configuration changes for resources for the entire system are calculated.

Example command and output.

```
root@sddc-manager-controller [ /opt/vmware/sddc-support ]# ./sos --configinsight-drift --domain-
name MGMT --resource-type sddc
Welcome to Supportability and Serviceability(SoS) utility!
ConfigInsight Logs : /var/tmp/configinsight-2018-02-22-20-24-33-3870
Log file : /var/tmp/configinsight-2018-02-22-20-24-33-3870/sos.log

Starting ConfigInsight Drift Operation!

Calculating drift for vCenter : vcenter-1.vrack.vsphere.local
ConfigInsight Drift task completed!
For drift results refer : /var/tmp/configinsight-2018-02-22-20-24-33-3870/drift-results.json
root@sddc-manager-controller [ /opt/vmware/sddc-support ]#
cat /var/tmp/configinsight-2018-02-22-20-24-33-3870/drift-results.json
{u'vcenter-1.vrack.vsphere.local': {'drift': None, 'reason': None, 'result': 'NO_DRIFT'}}
```

7 Stop the Config Insight tool.

```
./sos --configinsight-stop
```

Config Insight Commands

Option	Description
<code>./sos --configinsight-discovery</code>	Populates the database with baseline inventory.
<code>./sos --configinsight-drift</code>	Calculates configuration changes for the specified resource. Can be used with the following options: <ul style="list-style-type: none"> ■ <code>--resource-type {sddc,cluster,host,vcenter,psc,nxmanager,vsan}</code> option to calculate changes for the specified resource ■ <code>--domain-name</code> option to calculate changes for the specified domain.
<code>./sos --configinsight-resourceinfo</code>	Retrieves information about resources from the inventory in JSON format. Can be used with the <code>--domain-name</code> option to retrieve information for resources in the specified domain.
<code>./sos --configinsight-start</code>	Starts the Config Insight tool.
<code>./sos --configinsight-status</code>	Displays the status of the Config Insight tool.
<code>./sos --configinsight-stop</code>	Stops the Config Insight tool.

Collect Logs for Your Cloud Foundation System

Use the SoS tool to collect the logs for various software components in the system.

The SoS tool collects logs from these components within your Cloud Foundation system:

- Management, ToR, and inter-rack switches

- SDDC Manager instances (the virtual machines in each rack with names starting with vrm), including the life cycle management (LCM) logs
- HMS software component of SDDC Manager
- Infrastructure virtual machines (ISVM VMs, including the Zookeeper and Cassandra service logs)
- ESXi hosts
- vCenter Server instances
- Platform Services Controller instances
- NSX Manager and NSX Controller instances
- vRealize Log Insight instances deployed by SDDC Manager in the environment
- Virtual machines used for the VDI workload domains' infrastructure, if any VDI workload domains exist in the environment
- VIA virtual machine, if reachable on the network from the SDDC Manager instance where the SoS tool is invoked

Use these options when retrieving support logs from your environment's various components.

- To collect all logs from all components except VDI-specific components, you can run the SoS tool without specifying any component-specific options.
- To collect logs for a specific component, run the tool with the appropriate options.

Log files for the vRealize Log Insight agent in vCenter Server are collected when vCenter Server log files are collected.

After running the SoS tool, you can examine the resulting logs to troubleshoot issues, or provide to VMware Technical Support if requested. VMware Technical Support might request these logs to help resolve technical issues when you have submitted a support request. The diagnostic information collected using the SoS tool includes logs for the various VMware software components and software products deployed in your Cloud Foundation environment.

Procedure

- 1 Using the root account, SSH to the SDDC Manager VM.
- 2 Change to the `/opt/vmware/sddc-support` directory.
- 3 To collect the logs, run the SoS tool without specifying any component-specific options. To collect logs for a specific component, run the tool with the appropriate options.

Note By default, before writing the output to the directory, the tool deletes the prior run's output files that might be present. If you want to retain the older output files, specify the `--no-clean-old-logs` option.

If you do not specify the `--log-dir` option, the tool writes the output to the `/var/tmp` directory in the SDDC Manager VM.

Table 13-3. SoS Tool Log File Options

Option	Description
<code>--api-logs</code>	Collects output from APIs.
<code>--cassandra-logs</code>	Collects logs from the Apache Cassandra database only. Apache Cassandra processes run in each of the infrastructure virtual machines, the ones with ISVM in their names. These ISVM VMs run in your installation's primary rack.
<code>--dump-only-sddc-java-threads</code>	Collects only the Java thread information from the SDDC Manager.
<code>--esx-logs</code>	Collects logs from the ESXi hosts only.
<code>--hms-logs</code>	Collects logs from the HMS software component only.
<code>--hms-host-debug-logs</code>	Collects HMS host debug logs only.
<code>--li-logs</code>	Collects logs from vRealize Log Insight VMs only.
<code>--no-audit</code>	Skips the audit executed as part of log collection.
<code>--no-clean-old-logs</code>	Use this option to prevent the tool from removing any output from a previous collection run. By default, the SoS tool. By default, before writing the output to the directory, the tool deletes the prior run's output files that might be present. If you want to retain the older output files, specify this option.
<code>--no-health-check</code>	Skips the health check executed as part of log collection.
<code>--nsx-logs</code>	Collects logs from the NSX Manager and NSX Controller instances only.
<code>--psc-logs</code>	Collects logs from the Platform Services Controller instances only.
<code>--sddc-manager-logs</code>	Collects logs from the SDDC Manager only.
<code>--switch-logs</code>	Collects logs from the switches only. Logs from all switches are collected: management, ToR, and, if a multirack installation, inter-rack switches.
<code>--test</code>	Collects test logs by verifying the files.
<code>--vc-logs</code>	Collects logs from the vCenter Server instances only.
<code>--vdi-logs</code>	Collects logs from VDI domains only.
<code>--via-logs</code>	When the VIA VMs are reachable from the SDDC Manager VM, you can use this option to collect logs only from the VIA virtual machine.

Table 13-3. SoS Tool Log File Options (Continued)

Option	Description
<code>--vm-screenshots</code>	Takes screen shots of all Cloud Foundation VMs.
<code>--zk-logs</code>	Collects logs from the Zookeeper server instances only. Zookeeper server processes run in each of the infrastructure virtual machines, the ones with ISVM in their names. These ISVM VMs run in your installation's primary rack. For more details about Zookeeper in the environment, see the <i>VMware Cloud Foundation Overview and Bring-Up Guide</i> .

The tool displays `Welcome to SoS log collection utility!`, the output directory, `sos.log` file location, and messages about the tool's progress, for example:

```
rack-1-vm-1:/opt/vmware/sddc-support # ./sos --log-dir /home/sos-logs --vdi-pass VDIadminpwd
Welcome to SoS(Supportability and Serviceability) utility!
Logs: /home/sos-logs/sos-2016-10-26-19-54-48-8666
Log file: /home/sos-logs/sos-2016-10-26-19-54-48-8666/sos.log
Progress : 0%, Initiated log collection
```

The tool collects the log files from the various software components in all of the racks and writes the output to the directory named in the `--log-dir` option. Inside that directory, the tool generates output in a specific directory structure.

The following example shows a sample output.

```
root@sddc-manager-controller [ /tmp/sos ]# ./sos
Welcome to Supportability and Serviceability(SoS) utility!
Logs : /var/tmp/sos-2017-09-13-17-29-51-8575
Log file : /var/tmp/sos-2017-09-13-17-29-51-8575/sos.log
Log Collection completed successfully for : [AUDIT, VIA, SDDC-MANAGER, SDDC-CASSANDRA, NSX_MANAGER, PSC, AUDIT LOG,
ZOOKEEPER, API-LOGS, ESX, VDI, SWITCH, HMS, VMS_SCREENSHOT, VCENTER-SERVER, LOGINSIGHT, HEALTH-CHECK]
```

When the environment has more than one rack, the output includes directories for each rack, according to the naming pattern `rack-1`, `rack-2`, `rack-3`, and so on. .

What to do next

Change to the output directory to examine the collected log files.

Component Log Files Collected By the SoS Tool

The SoS tool writes the component log files into an output directory structure within the filesystem of the SDDC Manager instance in which the command is initiated, for example:

```
root@sddc-manager-controller [ /tmp/sos ]# ./sos
Welcome to Supportability and Serviceability(SoS) utility!
Logs : /var/tmp/sos-2017-09-13-17-29-51-8575
Log file : /var/tmp/sos-2017-09-13-17-29-51-8575/sos.log
Log Collection completed successfully for : [AUDIT, VIA, SDDC-MANAGER, SDDC-CASSANDRA, NSX_MANAGER, PSC, AUDIT LOG,
ZOOKEEPER, API-LOGS, ESX, VDI, SWITCH, HMS, VMS_SCREENSHOT, VCENTER-SERVER, LOGINSIGHT, HEALTH-CHECK]
```

esx Directory Contents

In each rack-specific directory, the esx directory contains the following diagnostic files collected for each ESXi host in the rack:

File	Description
<code>esx-IP-address.tgz</code>	Diagnostic information from running the <code>vm-support</code> command on the ESXi host. An example file is <code>esx-192.168.100.101.tgz</code> .
<code>SmartInfo-IP-address.txt</code>	S.M.A.R.T. status of the ESXi host's hard drive (Self-Monitoring, Analysis, and Reporting Technology). An example file is <code>SmartInfo-192.168.100.101.txt</code> .
<code>vsan-health-IP-address.txt</code>	vSAN cluster health information from running the standard command <code>python /usr/lib/vmware/vsan/bin/vsan-health-status.py</code> on the ESXi host. An example file is <code>vsan-health-192.168.100.101.txt</code> .

hms Directory Contents

In each rack-specific directory, the hms directory contains subdirectories named `N0_hms_logs_timestamp.zip`, `N1_hms_logs_timestamp.zip`, `N2_hms_logs_timestamp.zip`, and so on, one subdirectory for each ESXi host in the rack.

An example of the files and subdirectories in the hms directory is:

```
hms
  hms_log_archiver.sh
  N0_hms_logs_2016-11-01_09-25-22.zip
  N1_hms_logs_2016-11-01_09-25-35.zip
  N2_hms_logs_2016-11-01_09-25-38.zip
  N3_hms_logs_2016-11-01_09-25-29.zip
  ...
```

The `hms_log_archiver.sh` file that appears in the hms directory is the script that obtains the HMS diagnostic files for each subdirectory. Each subdirectory contains the following files, where `Nn` refers to the file for the `n`th ESXi host.

File	Description
<code>Nn_hms_ib_timestamp.log</code>	HMS in-band (IB) log
<code>Nn_hms_oob_timestamp.zip</code>	HMS out-of-band (OOB) log files <code>hms.log</code> and <code>hms.log.1</code>
<code>Nn_hms_events_log_timestamp.log</code>	HMS events log file
<code>Nn_ServerInfo_timestamp.log</code>	HMS server info log file

loginsight Directory Contents

In each rack-specific directory, the loginsight directory contains the diagnostic information files collected from the vRealize Log Insight instance deployed on that rack, if any. Not every rack in the installation will have a vRealize Log Insight instance deployed on it.

File	Description
li.tgz	Compressed TAR file consisting of the vRealize Log Insight instance's <code>/var/log</code> directory.
<code>loginsight-support-timestamp.tar.gz</code>	Standard vRealize Log Insight compressed support bundle, created by the <code>loginsight-support</code> command.
<code>repo.tar.gz</code>	Compressed TAR file consisting of a mass export of the instance's repository buckets. created by running the <code>/opt/vmware/bin/loginsight-dump-repo.sh</code> in the vRealize Log Insight instance.

loginsight-agent-vcenterFQDN-timestamp.zip Directory Contents

Even though these directories' names end in `.zip`, each one is a directory of files. In each rack-specific directory, each of these directories contains the diagnostic information files for the vRealize Log Insight Linux agent configured for each vCenter Server instance in the rack. When a vRealize Log Insight instance is deployed in the Cloud Foundation environment, each vCenter Server instance is configured with the vRealize Log Insight Linux agent to collect events from that vCenter Server instance and forward them to the vRealize Log Insight instance. Because a vCenter Server instance is deployed for the rack's management domain and for any of that rack's VI or VDI workload domains, at least one or more of these `loginsight-agent-vcenterFQDN-timestamp.zip` directories appears in each of the log output's rack-specific directories.

The vRealize Log Insight Linux agent writes its own operation log files. The files in each `loginsight-agent-vcenterFQDN-timestamp.zip` directory result from the SoS tool running the `/usr/lib/loginsight-agent/bin/loginsight-agent-support` command to generate the standard vRealize Log Insight Linux agent support bundle.

File	Description
<code>config/liagent.ini</code>	Configuration file containing the preconfigured default settings for the agent.
<code>config/liagent-effective.ini</code>	The agent's effective configuration. This effective configuration is the <code>liagent.ini</code> dynamically joined with settings from the vRealize Log Insight server-side settings to form this <code>liagent-effective.ini</code> file.
<code>log/liagent_timestamp_*.log</code>	Detailed log files.
<code>var/log/messages</code>	If the agent is configured to collect messages from the vCenter Server instance's <code>/var/log</code> directory, this file is the collected messages log.

nsx Directory Contents

In each rack-specific directory, the `nsx` directory contains the diagnostic information files collected for the NSX Manager instances and NSX Controller instances deployed in that rack.

The number of files in this directory depends on the number of NSX Manager and NSX Controller instances that are deployed in the rack. In a given rack, each management domain has one NSX Manager instance and a minimum of three NSX Controller instances, and any VI or VDI workload domains in the rack each have one NSX Manager instance and at least three NSX Controller instances.

File	Description
VMware-NSX-Manager-tech-support- <i>nsxmanagerIPAddr</i> .tar.gz	Standard NSX Manager compressed support bundle, generated using the NSX for vSphere API POST https://nsxmanagerIPAddr/api/1.0/appliance-management/techsupportlogs/NSX , where <i>nsxmanagerIPAddr</i> is the IP address of the NSX Manager instance. An example is VMware-NSX-Manager-tech-support-10.0.0.8.tar.gz.
VMware-NSX-Controller-tech-support- <i>nsxmanagerIPAddr</i> - controller- <i>controllerId</i> .tgz	Standard NSX Controller compressed support bundle, generated using the NSX for vSphere API to query the NSX Controller technical support logs: GET https://nsxmanagerIPAddr/api/2.0/vdn/controller/controllerId/techsupportlogs , where <i>nsxmanagerIPAddr</i> is the IP address of the NSX Manager instance and <i>controllerID</i> identifies the NSX Controller instance. Examples are VMware-NSX-Controller-tech-support-10.0.0.8-controller-1.tgz, VMware-NSX-Controller-tech-support-10.0.0.8-controller-2.tgz, VMware-NSX-Controller-tech-support-10.0.0.8-controller-3.tgz

psc Directory Contents

In the rack-1 directory, the psc directory contains the diagnostic information files collected for the Platform Services Controller instances deployed in that rack.

Note In a Cloud Foundation environment, the two Platform Services Controller instances are deployed in the primary rack only. As a result, this psc directory only appears in the primary rack's log output. For the description of the primary rack, see [VMware Software Components Deployed in a Typical Cloud Foundation System](#).

File	Description
vm-support- <i>pscIPAddr</i> .tar.gz	Standard Platform Services Controller support bundle downloaded from the Platform Services Controller instance with IP address <i>pscIPAddr</i> .

switch Directory Contents

In the rack-specific directory, the switch directory contains the diagnostic information files collected for that rack's switches.

Each physical rack in the installation has a management switch and two ToR switches. A multirack system additionally has two inter-rack switches. The SoS tool writes the logs for the inter-rack switches into the rack-1/switch subdirectory.

Only certain switch makers and models are supported for use in a Cloud Foundation installation. See the [VMware Cloud Foundation section](#) of the VMware Compatibility Guide for details on which switch makers and models are supported for this release.

File	Description
<code>cl_support_Management1_timestamp.tar.xz</code>	Standard support bundle collected from a management switch. In this release, the management switches run the Cumulus Linux operating system, and the SoS tool collects the switch's support bundle using the standard Cumulus <code>/usr/cumulus/bin/cl-support</code> support command.
<code>IPAddr-switchmaker-techsupport.gz</code>	Standard support bundle collected from a ToR or inter-rack switch at IP address <code>IPAddr</code> and for switch maker <code>switchmaker</code> . The SoS tool collects the switch's support bundle using the appropriate command for the particular switch, such as <code>show tech-support</code> . The ToR switches typically have IP addresses 192.168.0.20 and 192.168.0.21. The inter-rack switches typically have IP addresses 192.168.0.30 and 192.168.0.31.

vc Directory Contents

In each rack-specific directory, the `vc` directory contains the diagnostic information files collected for the vCenter Server instances deployed in that rack.

The number of files in this directory depends on the number of vCenter Server instances that are deployed in the rack. In a given rack, each management domain has one vCenter Server instance, and any VI or VDI workload domains in the rack each have one vCenter Server instance.

File	Description
<code>vc-vcsaFQDN-timestamp.tgz</code>	Standard vCenter Server support bundle downloaded from the vCenter Server Appliance instance having a fully-qualified domain name <code>vcsaFQDN</code> . The support bundle is obtained from the instance using the standard <code>vc-support.sh</code> command.

vdi Directory Contents

If the rack has a deployed VDI workload domain, the SoS tool creates a `vdi` directory in the log directory for that rack. The `vdi` directory contains the diagnostic information files collected for the VDI environment's VMware server components deployed in that rack.

The SoS tool collects the standard VMware support bundles from the VMware server components from VMware Horizon and App Volumes that are deployed as VMs for use by the VDI environment:

- View Connection Server instances, including when View Connection Server is deployed as a security server for the VDI environment. A security server is a special instance of View Connection Server as described in the [VMware Horizon product documentation](#). A security server is deployed for the VDI environment if the **Connect from anywhere** option was specified when the VDI workload domain was created.
- App Volumes Manager. The App Volumes Manager instance is deployed for the VDI environment if the **Implement App Volumes** option was specified when the VDI workload domain was created.

File	Description
<i>connHostname.vdm-sdct-timestamp-server.zip</i>	View Connection support bundle downloaded from the View Connection instances having hostname <i>connserverHostname</i> , such as con-1-1, con-1-2, and so on. The support bundle is obtained from the instance using the standard <code>C:\Program Files\VMware View\Server\DCT\support.bat</code> command for the View Connection Server.
<i>appvolsHostname-logs.zip</i>	App Volumes log files obtained from the App Volumes Manager instance having hostname <i>appvolsHostname</i> , such as appvolumes-1-1, appvolumes-1-2, and so on.

vrn.properties Directory Contents

In each rack-specific directory, the `vrn.properties` directory contains the following configuration files from the SDDC Manager instance deployed in the rack:

File	Description
<i>hms_ib_inventory.json</i>	SDDC Manager rack hardware inventory file, created during imaging of the rack. The SoS tool obtains this file from the SDDC Manager instance's <code>/home/vrack/VMware/vRack</code> directory.
<i>vrn-security.keystore</i>	SDDC Manager keystore file, from the SDDC Manager system's <code>/home/vrack/VMware/vRack</code> directory.
<i>vrn.properties</i>	Properties file from the SDDC Manager Dashboard.
<i>vrn.properties.vRack</i>	Copy of the SDDC Manager <code>vrn.properties</code> file in the SDDC Manager system's <code>/home/vrack/VMware/vRack</code> directory.

zk Directory Contents

In the `rack-1` directory, the `zk` directory contains three subdirectories, each containing the diagnostic information files collected for the SDDC Manager ISVM instances deployed in that rack.

The subdirectories in the `zk` directory are named according to the three ISVM instances' IP addresses, such as:

- 192.168.100.43
- 192.168.100.44
- 192.168.100.45

Each subdirectory contains two files.

File	Description
<i>cassandra-bundle.tgz</i>	Compressed TAR file containing the Cassandra database's logs and diagnostic information.
<i>zk-bundle.tgz</i>	Compressed TAR file containing the Zookeeper logs and diagnostic information.

hms.tar.gz Contents

Each rack-specific directory has an `hms.tar.gz` file.

File	Description
<i>hms.tar.gz</i>	Compressed file containing <code>hms.tar</code> , which contains the HMS software component's diagnostic information.

vrn- *timestamp* .tgz Contents

Each rack-specific directory has a *vrn-timestamp.tgz* file.

File	Description
<i>vrn-timestamp.tgz</i>	Compressed file containing <i>vrn-timestamp.tar</i> , which contains diagnostic information for SDDC Manager.

via- *timestamp* .tgz Contents

If the VIA virtual machine is reachable from the SDDC Manager instance where the SoS tool is invoked, the logs directory for that rack contains a *via-timestamp.tgz* file.

Under standard operating conditions, the VIA virtual machine is not reachable from the SDDC Manager instances in a Cloud Foundation installation. The VIA virtual machine is used to image a rack for use in a Cloud Foundation installation, and is reachable from that newly imaged rack's SDDC Manager instance at the end of the imaging process. You can use the SoS tool in the newly imaged rack's SDDC Manager instance to collect the VIA VM's logs at the end of the imaging process.

File	Description
<i>via-timestamp.tgz</i>	Compressed file containing <i>vrn-timestamp.tar</i> , which contains the VIA VM's diagnostic information.

Managing Shutdown and Startup of Cloud Foundation

14

You might have situations in which you want to shut down and start up the system. In such situations, you must start up and shut down the management virtual machines according to a predefined order.

The following situations require shutting down and starting up the Cloud Foundation system:

- Performing patch or upgrade operations of SDDC Manager applications.
- Performing recovery or failover operations of SDDC Manager applications.
- Performing imaging at one location and shipping the rack for deployment at another location.

This chapter includes the following topics:

- [Shut Down a Cloud Foundation System](#)
- [Start Up a Cloud Foundation System](#)

Shut Down a Cloud Foundation System

You must shut down the system components in a strict order to avoid data loss and faults in the components.

Prerequisites

- Verify that you have direct console access to the switches and ESXi hosts in the system.
- Coordinate the shutdown in advance with business stakeholders to minimize any impact.
- Verify that no VMs are running on snapshots.
- Verify that you have saved the account passwords to a location external from the Cloud Foundation system you are shutting down. See [Look Up Account Credentials](#).
- Verify that valid backups of all management VMs, tenant VMs, and switch configurations are available and saved to a location external from the Cloud Foundation system you are shutting down. See [Chapter 5 Backing up and Restoring a Cloud Foundation System](#).
- If a data protection solution is running on any of the domains, verify that it is properly shut down per vendor instructions.
- See Knowledge Base article 2142676 [Shutting down and powering on a vSAN 6.x Cluster when vCenter Server is running on top of vSAN](#) for information about verifying the state of the vSAN cluster before a shutdown.

Procedure

- 1 Before starting the shutdown procedure, note down the following information:
 - The hostname and IP address of the ESXi hosts that are members of the management domain. To see the hosts in the management domain, navigate to the Domain Details page in the SDDC Manager Dashboard.
 - The hostname and IP address of the ESXi hosts that are members of each workload domain. To see the hosts in the VI workload domains, for each domain navigate to the Domain Details page in the SDDC Manager Dashboard.
- 2 Shut down the workload VMs in each VI workload domain.
 - a On the SDDC Manager Dashboard, navigate to the workload domain.
 - b Click the launch link  for the vCenter Server instance that is displayed in the domain details window for that workload domain.
A new browser tab opens and displays the vSphere Web Client.
 - c Locate the VMs for that workload domain.
 - d Shut down these VMs.

Note Each workload domain includes a three-node NSX Controller cluster. Shut down these VMs last.

- e Perform the above steps for each VI workload domain.
- 3 Place the hosts for each workload domain in maintenance mode.
You must use the ESXCLI command, which supports setting the vSAN mode when entering maintenance mode.
 - a For each ESXi host, connect and log in to the ESXi console using SSH.
 - b Place each host into maintenance mode using the following command, with the `noAction` option included.

```
esxcli system maintenanceMode set -e true -m noAction
```

- c After a few minutes, confirm each host is in maintenance mode by repeating the command.

```
esxcli system maintenanceMode set -e true -m noAction
```

It should return the following:

```
Maintenance mode is already enabled.
```

- d Shut down all the ESXi hosts in the VI workload domain.

```
# poweroff
```

- e Repeat the above steps for each VI workload domain.

- 4 Shut down the vRealize Log Insight virtual appliances in the management domain in the following order:

Important Verify that the console of each virtual appliance and its services are fully shut down before proceeding to the next step.

- All vRealize Log Insight Worker nodes.
- The vRealize Log Insight Master node.

- 5 Shut down the vRealize Operations Manager virtual appliances in the management domain in the following order:

Important Verify that the console of each virtual appliance and its services are fully shut down before proceeding to the next step.

- All vRealize Operations Manager Remote Collector nodes.
- All vRealize Operations Manager Data nodes.
- The vRealize Operations Manager Replica node.
- The vRealize Operations Manager Master node.

- 6 Shut down the vRealize Automation virtual appliance and IaaS components in the management domain in the following order:

Important Verify that the console of each virtual appliance or VM and its services are fully shut down before proceeding to the next step.

- All vRealize Automation IaaS Distributed Execution Management (DEM) VMs.
- All vRealize Automation IaaS Proxy Agent VMs.
- All vRealize Automation IaaS Manager Server VMs.

Note Shut down the secondary IaaS Manager Server VM first; shut down the primary IaaS Manager Server VM second.

- All vRealize Automation IaaS Web Server VMs.

Note Shut down the secondary IaaS Web Server VM first; shut down the primary IaaS Web Server VM second.

- All vRealize Automation virtual appliances.
- The vRealize Automation IaaS SQL Server VM.

- 7 Shut down the infrastructure management virtual appliances in the management domain in the following sequence.
 - a Shut down the following virtual appliances using the SSH console, verifying that the console of each virtual appliance and its services are fully shut down before proceeding to the next step.
 - All NSX Edge Service Gateway virtual appliances.
 - The NSX Manager virtual appliances for the VI workload domains.
 - The NSX Manager virtual appliance for the management domain.
 - All NSX Controller cluster virtual appliances for the management domain.
 - b Shut down the remaining virtual appliances or VMs from their hosts in the ESXi Host Client on each management ESXi host.
 - The vCenter Server virtual appliance for the VI workload domains.
 - The vCenter Server virtual appliance for the management domain.
 - The Platform Services Controller virtual appliances.
 - SDDC Manager Utility VM.
 - SDDC Manager VM.
- 8 Place the management domain ESXi hosts in maintenance mode.

Important By shutting down the SDDC Manager VM and SDDC Manager Utility VM, you cease operations for the embedded DNS in the Cloud Foundation system. As a result, you must use the IP address of each ESXi host.

You must use the ESXCLI command that supports setting the vSAN mode when entering maintenance mode.

- a For each ESXi host, connect and log in to the ESXi console using SSH.
- b Put each host into maintenance mode using the following command, with the `noAction` option included.

```
# esxcli system maintenanceMode set -e true -m noAction
```

- c After a few minutes, confirm each host is in maintenance mode by repeating the command.

```
esxcli system maintenanceMode set -e true -m noAction
```

It should return the following:

```
Maintenance mode is already enabled.
```

- d Shut down all the ESXi hosts in the management domain.

```
# poweroff
```

- 9 Shut down the unassigned ESXi hosts in the Cloud Foundation system, if any.

```
# poweroff
```

- a For each unassigned ESXi host, connect and log in to the ESXi console using SSH.
b Shut down each unassigned ESXi host.

```
# poweroff
```

- 10 Shut down the switches in the following order.

Important For a management switch, log in first and then shut it down.

- a ToR switches in each rack.
b Inter-rack switches in rack 2.

Note In some deployments, inter-racks switches may be used for egress (instead of the ToR switches). By shutting down the switch, you may break that connection. It is recommended that you have physical access to the switch to remedy such a break.

- c Management switches in each rack.

Start Up a Cloud Foundation System

You must start up the system components of the system in a strict order to avoid data loss and faults in the components.

Prerequisites

- Verify that you have direct console access to the switches and ESXi hosts in the system.
- Verify that you have the host names and IP addresses of the ESXi hosts that are members of the management domain.

You can obtain this information in the Domain Details pages in the SDDC Manager Dashboard.

- Verify that you have the host names and IP addresses of the ESXi hosts that are members of each VI and VDI workload domain.

You can obtain this information in the Domain Details pages in the SDDC Manager Dashboard.

- See Knowledge Base article 2142676 [Shutting down and powering on a vSAN 6.x Cluster when vCenter Server is running on top of vSAN](#) for information about starting up hosts and exiting maintenance mode.

Procedure

- 1 Power on the switches in the following order.
 - a Inter-rack switches
 - b ToR switches
 - c Management switches
- 2 From the console of each switch, verify that the switches are online.
- 3 Power on each ESXi host in the management domain, and exit maintenance mode.
 - a Use SSH to connect and log in to the ESXi console.
 - b Use the following CLI command to exit maintenance mode.

```
# esxcli system maintenanceMode set -e false
```

- c Perform the above steps on each ESXi host until none are in maintenance mode.
- 4 Power on each ESXi host in the first VI workload domain, and exit maintenance mode.
 - a Use SSH to connect and log in to the ESXi console.
 - b Use the following CLI command to exit maintenance mode.

```
# esxcli system maintenanceMode set -e false
```

- c Perform the above steps on each ESXi host in the VI workload domain until none are in maintenance mode.
 - d Repeat the above steps for each VI workload domain.
- 5 Power on the infrastructure management VMs in the management domain.

Important You must power on the VMs using the ESXi host client on each management ESXi host.

Important You must wait until each VM is powered on and all its services started before powering on the next VM.

Power on the VMs in the following order:

- SDDC Manager Utility VM.
- Platform Services Controller virtual appliances.

- vCenter Server for the management domain.
- SDDC Manager VM.
- NSX Manager virtual appliance for the management domain.
- NSX Controller cluster virtual appliances for the management domain.
- NSX Edge Service Gateway virtual appliances.
- vCenter Server for each VI workload domain.
- NSX Manager virtual appliance for each VI workload domain.

If you also have VDI workload domains, power on the VDI workload domain vCenter Server and NSX Manager virtual appliances, then the Horizon and AppVolumes VMs.

- 6 Log in to the SDDC Manager Dashboard to verify that it displays correctly.
 - a On the SDDC Manager Dashboard, navigate to the management domain.
 - b In the domain details panel, click the launch for the vCenter Server instance.

A new browser tab opens and displays the vSphere Web Client.
- 7 Power on the vRealize Automation virtual appliance and IaaS components in the management domain.

Important You must wait until each VM or virtual appliance is powered on and all of its services started before running on the next VM.

Power on the VMs in the following order:

- The vRealize Automation IaaS SQL Server VM.
- All vRealize Automation virtual appliances.
- All vRealize Automation IaaS Web Server VMs.

Note Power on the primary IaaS Web Server VM first.

- All vRealize Automation IaaS Manager Services.

Note Power on the primary IaaS Manager Server VM first.

- All vRealize Automation IaaS proxy agents.
- All vRealize Automation IaaS Distributed Execution Management (DEM) hosts.

- 8 Power on the vRealize Operations Manager virtual appliances in the management domain.

Important You must wait until each VM or virtual appliance is powered on and all of its services running before powering on the next VM.

Power on the VMs in the following order:

- The vRealize Operations Manager master node.

- The vRealize Operations Manager master replica node.
- All vRealize Operations Manager data nodes.
- All vRealize Operations Manager remote collector nodes.

9 Power on the vRealize Log Insight virtual appliances in the management domain.

Important You must wait until each VM or virtual appliance is powered on and all of its services running before powering on the next VM.

Power on the VMs in the following order:

- The vRealize Log Insight master node.
- All vRealize Log Insight worker nodes.

10 Power on the VMs in the first VI workload domain.

Important Each workload domain includes a three-node NSX Controller cluster. Power on these VMs first.

- a On the SDDC Manager Dashboard, navigate to the management domain.
- b In the domain details panel, click the launch for the vCenter Server instance.
A new browser tab opens and displays the vSphere Web Client.
- c In the vSphere Web Client, power on the VMs in the following order:
 - The three-node NSX Controller cluster.
 - The workload domain VMs.
- d Repeat this procedure on each VI workload domain.

If you also have VDI workload domains, power on the VMs in the same order. Log in to the Horizon View Administrator to verify operations.

11 Using SSH, log in as root to the SDDC Manager VM and run the `./sos --health-check` command to verify that everything works correctly.

Patching and Upgrading Cloud Foundation

15

Lifecycle Management (LCM) enables you to perform automated updates on Cloud Foundation components (SDDC Manager, HMS, and LCM), VMware components (vCenter Server, ESXi, and NSX), and third party tools.

SDDC Manager is pre-configured to communicate with the VMware software repository. The high level update workflow is described below.

- 1 Receive notification of update availability.
- 2 Download update bundle.
- 3 Select update targets and schedule update.

Update is applied to the selected targets at the scheduled time.

Even though SDDC Manager may be available while the update is installed, it is recommended that you schedule the update at a time when it is not being heavily used.

For an unassigned host (host in the capacity pool that is not part of a workload domain), you must bring the unassigned host into a workload domain, and then update the domain as described in [Update a Workload Domain](#).

Important When you delete a workload domain, it is recommended that you [Decommission an Unassigned Host](#), image it with the current, upgrade ESXi version, and then perform the [Add a Previously Decommissioned Host to a Physical Rack](#). This ensures that when the hosts are required for new workload domain, they are ready and their ESXi versions up to date. (When a workload domain is deleted, the hosts revert to the ESXi version their rack was originally imaged with.)

This section describes generic patching and upgrading. For information on upgrading to Cloud Foundation 2.3, see [Chapter 16 Upgrade Cloud Foundation to 2.3.1](#).

This chapter includes the following topics:

- [Prerequisites for Upgrading VMware Software](#)
- [Update a Workload Domain](#)
- [View Inventory Component Versions](#)
- [Display Backup Locations](#)
- [Upgrade Log File Locations](#)

- [Upgrade Backup File Locations](#)

Prerequisites for Upgrading VMware Software

Ensure that the prerequisites in each section are met before you begin a VMware software upgrade.

Domain Operations

Verify that no domain operations are running. See [Managing Workflows and Tasks](#).

ESXi Prerequisites

- 1 Verify that all ESXi hosts are within a domain cluster in vCenter.
- 2 Verify that all ESXi hosts within the cluster are in a healthy state. If a host is not healthy, and therefore in maintenance mode, the upgrade will fail.

NSX Prerequisites

- 1 Back up the NSX configuration.
 - a Using the root account, SSH in to the SDDC Manager VM.
 - b Type the following command.


```
/home/vrack/bin/lookup-password
```
 - c Note down the values for the following.
 - IP address for SDDC Manager Utility VM that resides in the management domain vCenter
 - username
 - password
 - d Follow the procedure *Back Up NSX Manager Data* in *Upgrading NSX*. For the NSX backup files to be accessible by Cloud Foundation, you must specify the settings specified in the table below.

Setting	Value
IP/Hostname	IP address that you noted in step 3.
Transfer Protocol	SFTP
Port	22
Username	Username that you noted in step 3.
Password	Password that you noted in step 3.
Backup Directory	/backup

Setting	Value
Filename Prefix	<i>nsx_type_domain-number</i> For example, type <i>nsx_mgmt_dmn01</i> when taking a backup of the NSX management domain. Type <i>nsx_vdi_dmn01</i> when taking a VDI domain backup.
Passphrase	<i>nsxmgr_backup</i>

- 2 If you are upgrading a workload domain that contains 3 hosts, disable the anti-affinity rule that separates NSX controllers across hosts.
 - a Login to the vCenter Server of the domain.
 - b In the left navigation pane, right-click the cluster and click **Edit Setting**.
 - c In the left navigation pane, click **Rules**.
 - d Un-select the NSX-Controller Anti-Affinity rule.
 - e Click **OK**.
 - f After the upgrade is complete, enable the rule again.

Back up NSX Data

For the NSX upgrade to succeed, valid backup files must be available.

Procedure

- 1 Using the root account, SSH in to the SDDC Manager VM.
- 2 Type the following command.

```
/home/vrack/bin/lookup-password
```
- 3 Note down the values for the following.
 - IP address for SDDC Manager Utility VM
 - username
 - password
- 4 Follow the procedure *Back Up NSX Manager Data* in *Upgrading NSX*. For the NSX backup files to be accessible by Cloud Foundation, you must specify the settings specified in the table below.

Setting	Value
IP/Hostname	IP address that you noted in step 3.
Transfer Protocol	SFTP
Port	22
Username	Username that you noted in step 3.
Password	Password that you noted in step 3.
Backup Directory	/backup

Setting	Value
Filename Prefix	<i>nsx_type_domain-number</i> For example, type <code>nsx_mgmt_dmn01</code> when taking a backup of the NSX management domain. Type <code>nsx_vdi_dmn01</code> when taking a VDI domain backup.
Passphrase	<code>nsxmgr_backup</code>

Update a Workload Domain

Updating a workload domain is a multi-step process. Perform the steps in the order in which they are documented.

Important When you delete a workload domain, it is recommended that you [Decommission an Unassigned Host](#), image it with the current, upgrade ESXi version, and then perform the [Add a Previously Decommissioned Host to a Physical Rack](#). This ensures that when the hosts are required for new workload domain, they are ready and their ESXi versions up to date. (When a workload domain is deleted, the hosts revert to the ESXi version their rack was originally imaged with.)

Procedure

1 [Download LCM Bundles](#)

This section describes how to download an LCM bundle. LCM update bundles must be available on SDDC Manager before you can apply the update.

2 [Running the Upgrade Pre-Check](#)

The upgrade pre-check utility validates that your Cloud Foundation system is ready for an upgrade.

3 [Select Targets and Schedule Update](#)

You can schedule an update after it has been downloaded. You can also view updates in progress, scheduled updates, and installed updates.

Download LCM Bundles

This section describes how to download an LCM bundle. LCM update bundles must be available on SDDC Manager before you can apply the update.

Download Update Bundle from the the SDDC Manager Dashboard

When an update bundle is available, a notification is displayed on the workload domain page in the Update/Patches tab.

Procedure

- 1 Log in to your My VMware account.
 - a In the SDDC Manager Dashboard, click **Administration > Update Management** .
 - b Click **Login**.
The sign in page appears.
 - c Type your My VMware account user name and password.
 - d Click **Log In**.
The top right corner of the window displays a green check mark.



- 2 In the SDDC Manager Dashboard, click **Inventory > Workload Domains**..
- 3 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.

- 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 Do one of the following:
 - Click **Download Now**.
The bundle download status is displayed.

- Click **Schedule Download**.

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

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.

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 update 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 update bundles.

Manually Download Update Bundles

LCM polls the VMware depot to access 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 internet connectivity for downloading the bundles. If it is a Windows computer, it must have Java 8 or later.

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 `markerFile` and `markerFile.md5` files from the location displayed in the output of step 3 to a computer with internet access.
- 5 On the external computer, run the following command.

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

where

<i>absolute-path-output-dir</i>	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.
<i>sku</i>	Optional. SKU or Service Provider of the index file.
<i>depotUser</i>	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.
<i>markerFile</i>	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.
<i>markerMd5File</i>	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.

Figure 15-1. Download Directory Structure

```

downloadDir
  \_ bundles
    \_ bundle-EVORACK-2.1.2-100182.tar
    \_ bundle-VMWARE_SOFTWARE-2.1.3-100185.tar
    \_ bundle-VMWARE_SOFTWARE-2.1.4-100189.tar

  \_ manifests
    \_ bundle-EVORACK-2.1.2-100182.manifest
    \_ bundle-VMWARE_SOFTWARE-2.1.3-100185.manifest
    \_ bundle-VMWARE_SOFTWARE-2.1.4-100189.manifest
    \_ bundle-EVORACK-2.1.2-100182.manifest.sig
    \_ bundle-VMWARE_SOFTWARE-2.1.3-100185.manifest.sig
    \_ bundle-VMWARE_SOFTWARE-2.1.4-100189.manifest.sig

  \_ deltaFileDownloaded
  \_ deltaFileDownloaded.md5
  \_ index

```

- 6 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/vCF231to232Bundle"
```

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

```
chown vcf_lcm:vcf -R /opt/vmware/vcf/vCF231to232Bundle
chmod -R 0777 /opt/vmware/vcf/vCF231to232Bundle
```

- 8 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 -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/vCF231to232Bundle` as shown in the previous step.

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

Running the Upgrade Pre-Check

The upgrade pre-check utility validates that your Cloud Foundation system is ready for an upgrade.

You manually trigger the pre-check utility directly in the SDDC Manager Dashboard or by logging into the SDDC Manager VM and running a command in the CLI.

Note It is recommended that you run both checks before upgrading.

The upgrade pre-check utility validates the following components of your Cloud Foundation system:

- SDDC Manager
- Hardware Management Services (HMS)
- Lifecycle Management (LCM)
- Platform Services Controller
- vCenter Server
- ESXi
- vSAN
- Bring-Up
- All racks
- All workload domains

Run the Upgrade Pre-Check in the SDDC Manager Dashboard

In the SDDC Manager Dashboard, the upgrade pre-check utility validates each component and returns a health status indicated by green (HEALTHY), yellow (WARNING), or red (ERROR) icon. In the SDDC Manager Dashboard, the Pre-Check Status page displays a high level report on each component and its readiness. You can click the icon for any component to view the details of the status.

Procedure

- 1 In the SDDC Manager Dashboard, click **Lifecycle Management** in the left navigation bar.
- 2 Click the **Pre-Check** button to manually trigger a new pre-check operation.
- 3 At the top of the Lifecycle Management page, click **Upgrade Pre-Check** to display the Pre-Check Status page.

- 4 Next to the MGMT Management heading, click **View Status** to expand the page contents.

The Pre-Check Status page displays the system components and their current status or readiness for the upgrade process.

- 5 (Optional) To view details of any component status, click the status icon or component name.

The details panel lists out the tasks that comprise the status check. You can click each task to view another level of detail that includes description, and time of most recent status check. If the status for the task is yellow or red, the details include the impact of the error and steps for remediation.

Run the Upgrade Pre-Check in the CLI

The upgrade pre-check validates the readiness of your Cloud Foundation system through the SDDC Manager VM.

Procedure

- 1 SSH in to the SDDC Manager VM with your root account.
- 2 Type the following command.

```
/opt/vmware/evosddc-support/sos --pre-upgrade-check
```

The console window displays the status of the health check. The log file is written to the `/var/temp` directory. Wait for the health check to be completed before proceeding with the upgrade. For actions that you can take if a component fails the health check, see [Knowledge Base article 2150030](#).

Select Targets and Schedule Update

You can schedule an update after it has been downloaded. You can also view updates in progress, scheduled updates, and installed updates.

Even though SDDC Manager may be available while the update is applied, it is recommended that you schedule the update at a time when SDDC Manager is not being heavily used.

Note You cannot schedule an update while a workload is running. If an update is scheduled to start while a workload is in progress, the upgrade is cancelled.

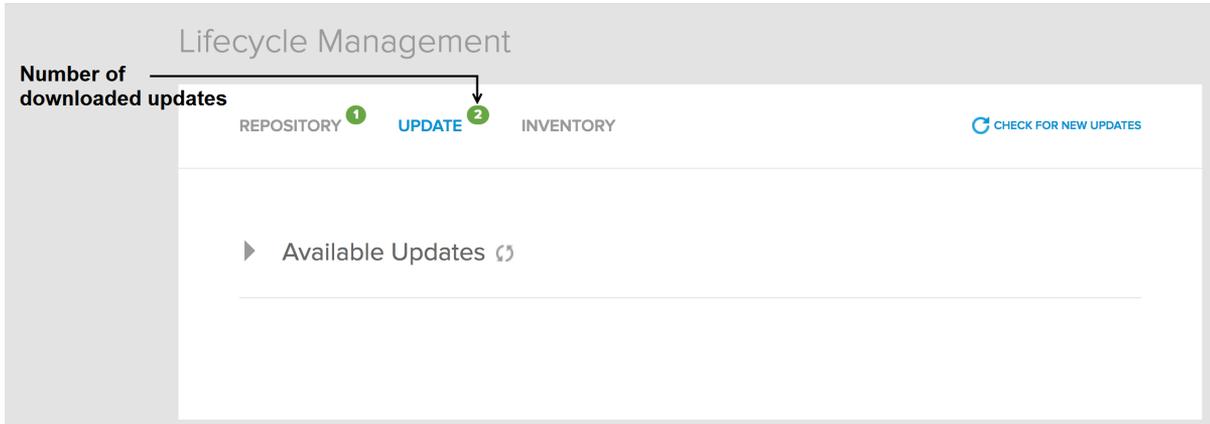
Prerequisites

- 1 You must have downloaded the appropriate bundle so that it is available in the local repository.
- 2 Ensure that the SDDC Manager and HMS are at the same version. In a dual rack scenario, the SDDC Manager and HMS versions must be the same on both racks. To confirm this, click the **LIFECYCLE** tab and then click **INVENTORY**.
- 3 Ensure that the existing version of Horizon View is compatible with the software versions in the LCM update you are applying. Refer to the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php#db. If there is a mismatch, manually upgrade the Horizon View components before applying the LCM patch. Refer to the Horizon View documentation on www.vmware.com/support/pubs.

Procedure

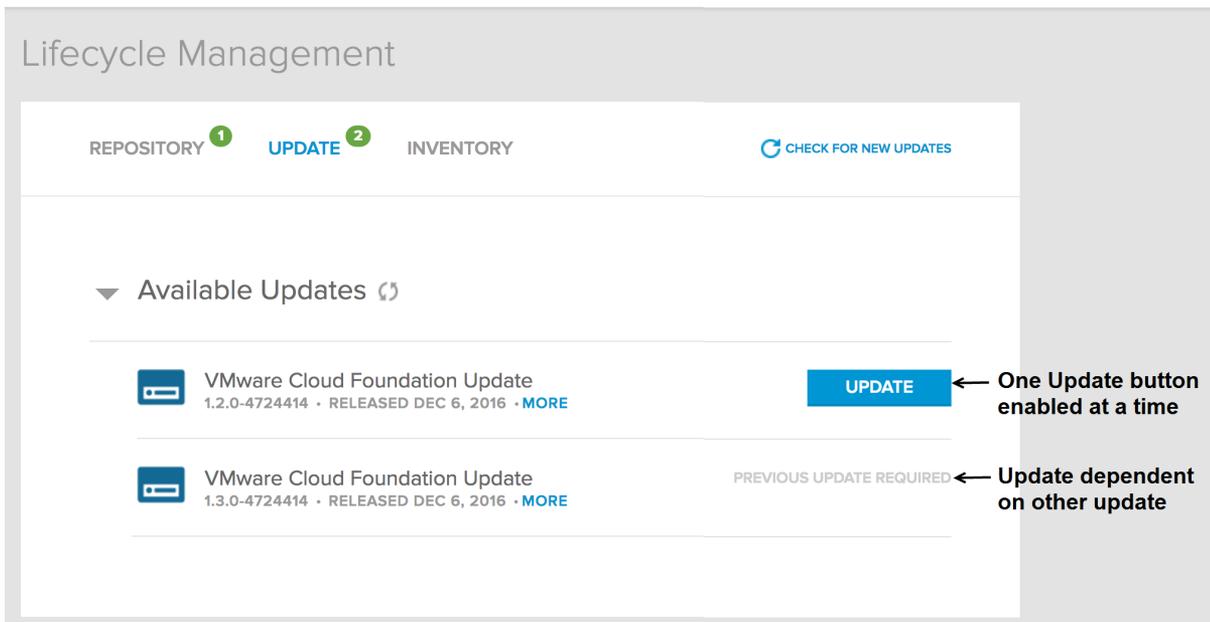
- 1 On the Lifecycle Management page, click the **UPDATES** tab.

The number of available updates is displayed next to the title of the **UPDATE** tab.



- 2 Click the drop-down next to Available Updates.

If an update is dependent on another update, it displays **PREVIOUS UPDATE REQUIRED**. Once the dependency update is installed, the **UPDATE** button becomes available. As an example, a VMware software update may be dependent on a Cloud Foundation update.



- 3 Click **UPDATE**.

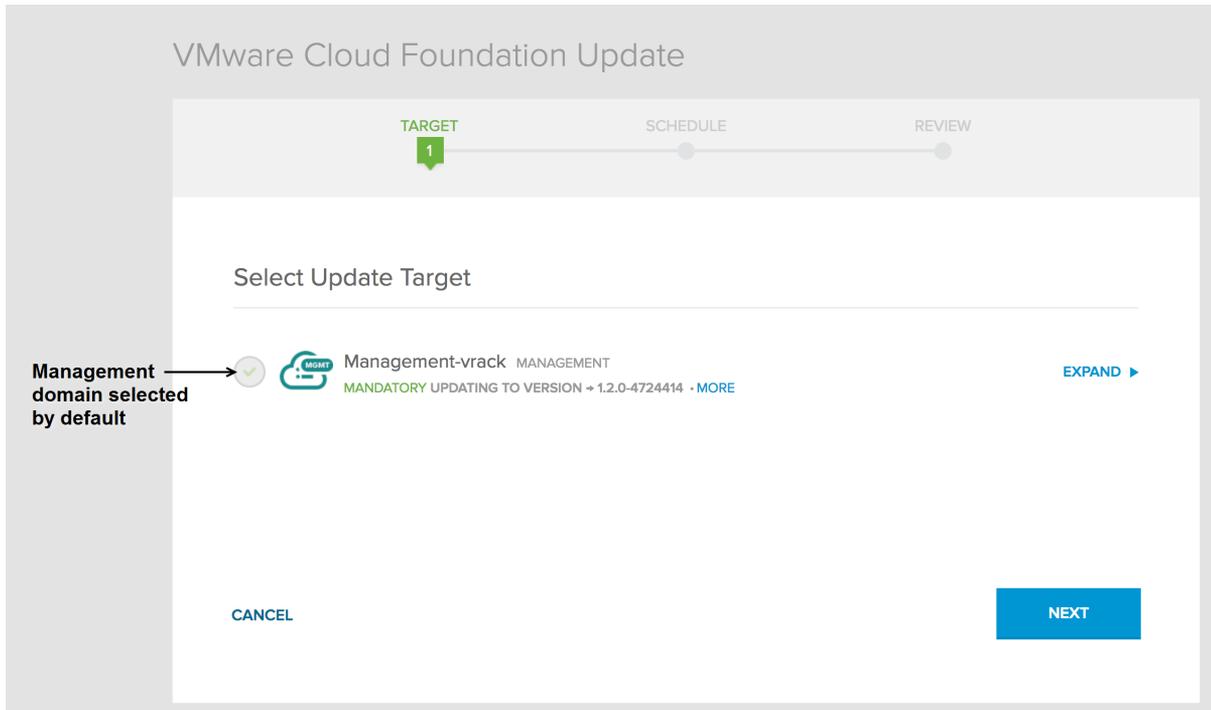
The **UPDATE** button is enabled only for one update at a time. Once you schedule a Cloud Foundation update, the UI allows you to schedule a VMware software update. However, VMware recommends that you schedule only one update at a time. Wait for the scheduled update to be installed successfully before scheduling another update.

The system validates that update pre-requisites are met before displaying the target selection.

- 4 On the **TARGET** page, select the domains where the update is to be applied.

When a new version of the software is available, it must be installed on the management domain. So the management domain is automatically selected for update and the checkbox next to it grayed out.

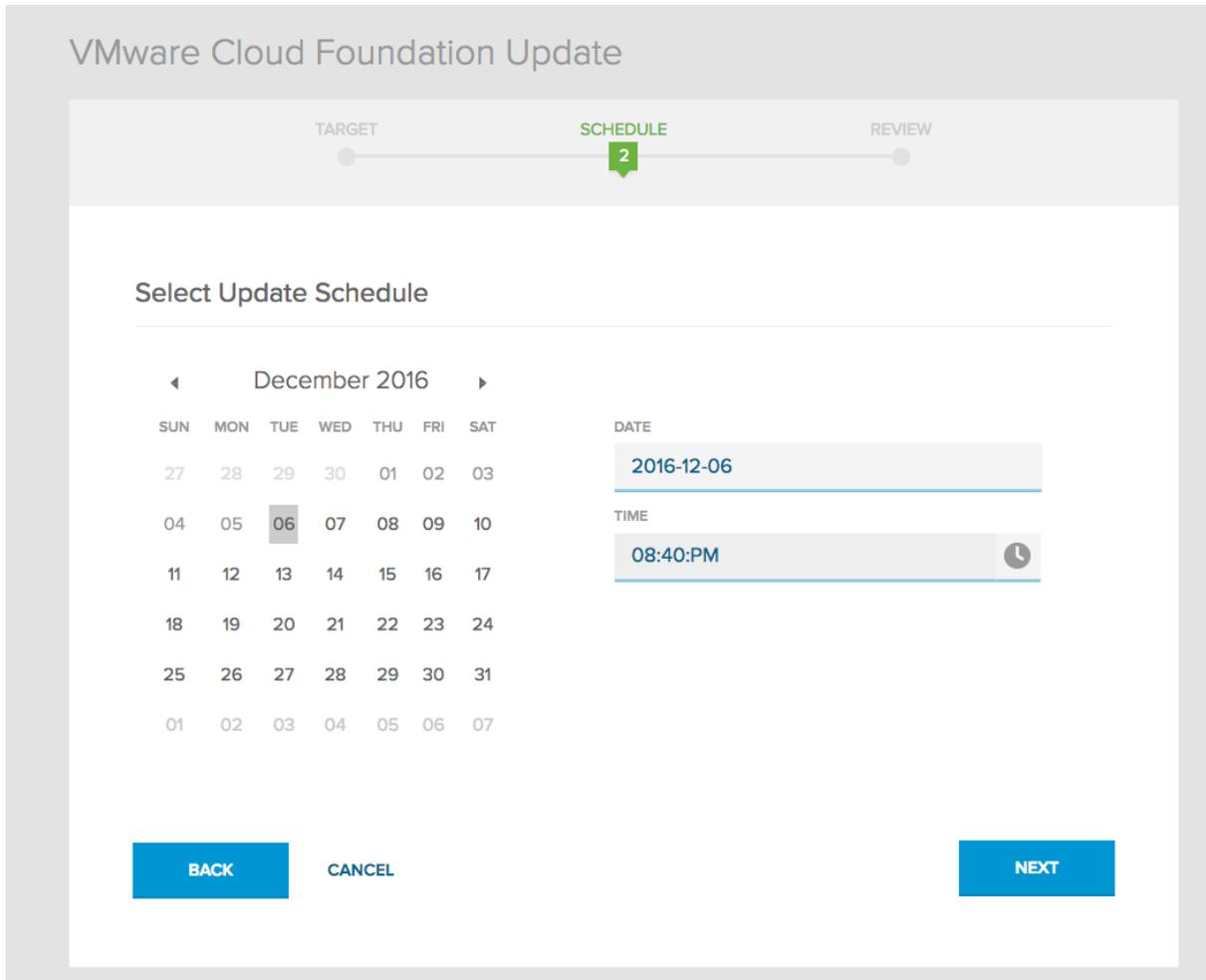
Click **EXPAND** next to the domain to see the areas of your datacenter that will be updated.



The targets on the primary rack (the rack that contains the PSCs) are updated before the targets on additional racks.

Note If you select only a subset of the domains in your datacenter to be updated, the update will be displayed in both the Available Updates section (since some domains are yet to be updated) as well the Scheduled Updates section. You cannot schedule an update on a failed domain. If the system does not let you select a domain, click the **INVENTORY** tab to check the status of the domain. Resolve the issue and then re-schedule the update.

- 5 Click **NEXT**.
- 6 On the **SCHEDULE** page, select the date and time for the update to be applied to the target domains and click **NEXT**. You can select a date within a year from the present date.



Note Do not reboot the physical racks, any devices on the rack, or the SDDC Manager VM while the upgrade is in progress.

- 7 Click **NEXT**.
- 8 On the Review Update page, review the update bundle, targets, and schedule.

VMware Cloud Foundation Update

TARGET — SCHEDULE — 3 REVIEW

Review Update

Warning : Avoid any changes to the domains being upgraded until after the upgrade is complete

BUNDLE TYPE	UPDATE SCHEDULE
VMware Cloud Foundation Update	12/06/2016 8:45PM

UPDATE TARGETS	UPDATE VERSION
Management-vrack <small>MANAGEMENT</small>	1.2.0-4724414

BACK
CANCEL
SCHEDULE UPDATE

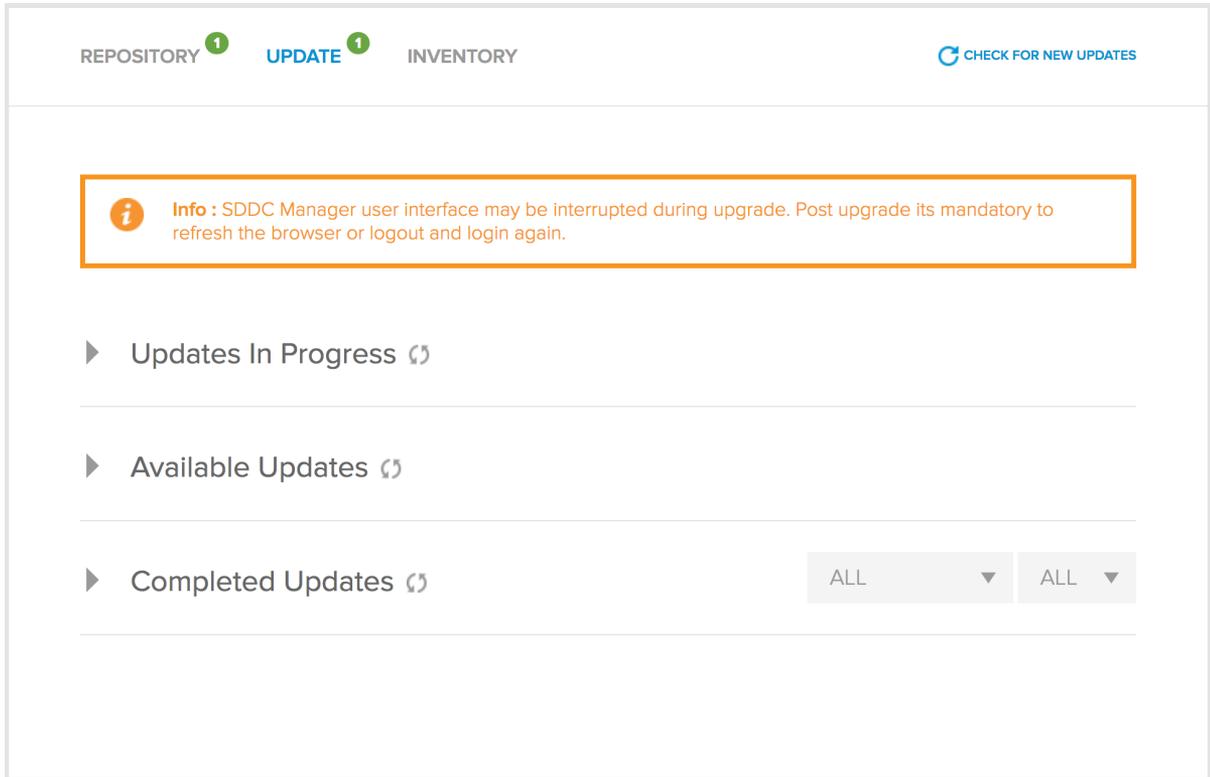
If you had selected multiple domains on the Target page, the Review Update page displays a notification that the management domain is updated first, followed by the other domains.

- 9 Click **SCHEDULE UPDATE**.

The screenshot shows the Lifecycle Management interface with the UPDATE tab selected. The top navigation bar includes REPOSITORY (with a notification icon), UPDATE (with a notification icon), and INVENTORY. A 'CHECK FOR NEW UPDATES' button is visible on the right. The main content area is divided into 'Scheduled Updates' and 'Available Updates' sections. Under 'Scheduled Updates', there is a card for 'VMware Cloud Foundation Update 1.2.0-4724414 · RELEASED DEC 6, 2016 · MORE'. A dropdown menu is open for this update, showing a scheduled time of '8:45PM 12.06.2016' and options to 'RESCHEDULE UPDATE', 'VIEW UPDATE DETAILS', and 'CANCEL UPDATE'. Filter buttons for 'ALL' are present for both sections.

The scheduled update appears in the SCHEDULED UPDATES section on the UPDATES tab and displays the time it is scheduled to be installed. Click **MORE** to see the update bundle details. When it is time for a scheduled update to be installed, the UPDATE tab is refreshed within 3 minutes of the start time. The **In Progress** section displays the update details. Click **VIEW UPDATE DETAILS** to display the Update Status. The Update Status page displays the resources within the domain being updated as well as the update progress (tasks completed and the total number of tasks). The resource being updated displays the  icon. Resources that have been updated display the  icon. If an update is scheduled to start while a workload is running, the update is cancelled so that the system is kept in a consistent state. You must re-schedule the update.

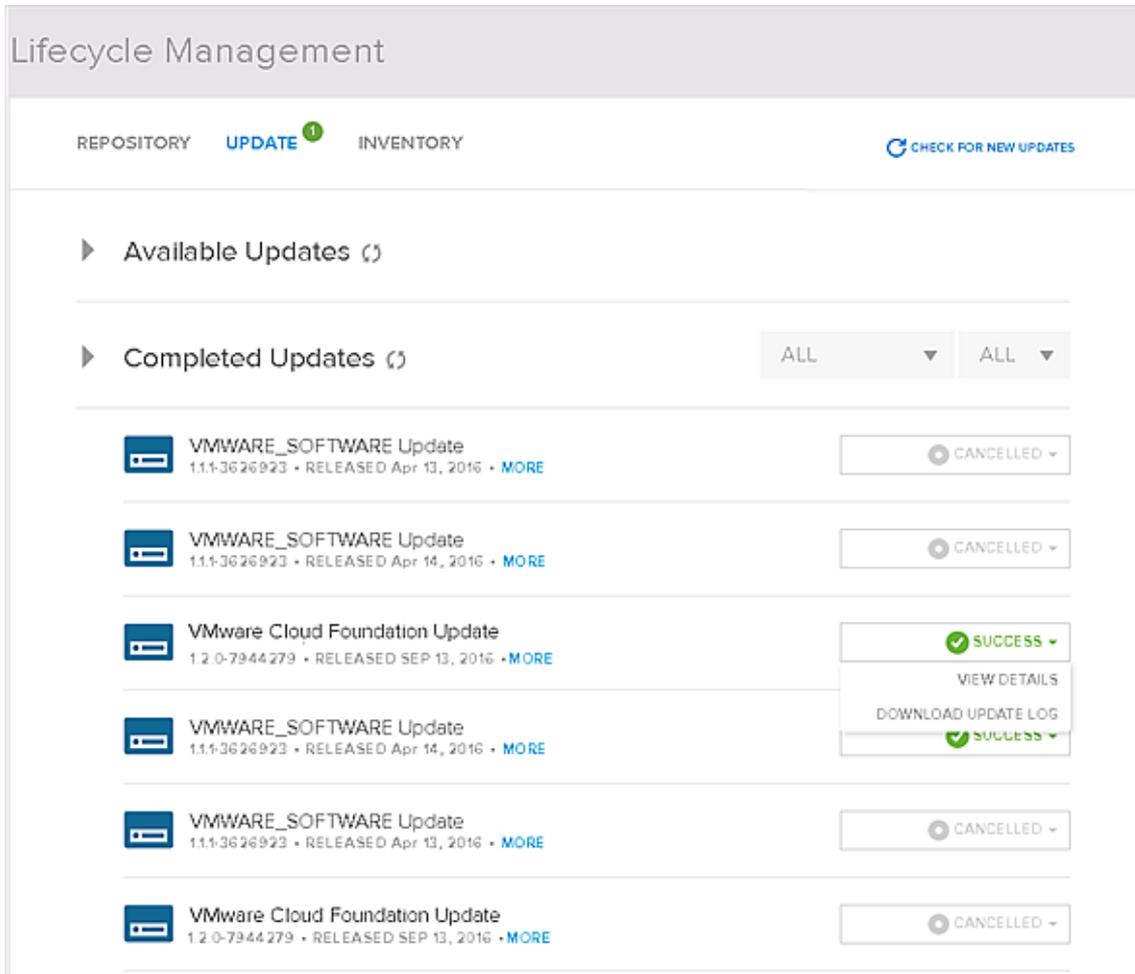
When an update is in progress, the Lifecycle Management page displays a warning message that the interface may be unresponsive and require user log out and back in after the update.



10 Click on a resource to view the update details on that resource.

Caution Do not cancel an in-progress update.

When all resources within the domain have been updated, the overall status of the domain update is displayed as COMPLETED. Click **LIFECYCLE MANAGEMENT** to go back to the UPDATE page where the completed update is displayed under COMPLETED UPDATES with the SUCCESS status.



- 11 To download the log file, click next to SUCCESS and then click **DOWNLOAD UPDATE LOG**.

If an update on a resource fails, a failure message is displayed on the Update Status page. You must resolve the issue with the resource that failed to be updated. The failed update is displayed on the UPDATE tab under Available Updates. You can re-schedule this update once the issue is resolved.

Here is an example of why an update might fail. For a VMware software update, an ESXi update is installed on the ESXi hosts in the appropriate domain sequentially. During an update, the system puts each host into maintenance mode to perform the update on that host, and then tells the host to exit maintenance mode after its update is completed. If an issue on the host prevents it from entering maintenance mode, the update fails. This might happen when a VM is not protected by HA and cannot be migrated to another host. In this case, you can manually resolve this problem by enabling HA on that VM. Then navigate back to the **UPDATE** tab and click **Available Updates**. Re-schedule the update and follow the update progress on the **Update Status** page.

View Inventory Component Versions

The Inventory Status displays the current versions of all workload domains and the domain components in your inventory.

Procedure

- 1 On the Lifecycle Management page, click the **INVENTORY** tab.

The current version and resource status for all domains in your datacenter is displayed.

Lifecycle Management

REPOSITORY ¹ UPDATE ¹ INVENTORY REFRESH STATUS

Inventory Status

 Management-rack MANAGEMENT COLLAPSE ▾

VMware Cloud Foundation Software

VRM 2.1.0-RELEASE-4724414	HMS 2.1.0-RELEASE-4712935	LCM 2.1.0-RELEASE-4712935
-------------------------------------	-------------------------------------	-------------------------------------

 **vcenter-mgmt** 4 ESXI NODES
6.0.0-3634791

rack-1-n0 6.0.0-4192238	rack-1-n1 6.0.0-4192238	rack-1-n3 6.0.0-4192238	rack-1-n2 6.0.0-4192238
-----------------------------------	-----------------------------------	-----------------------------------	-----------------------------------

 **PSC rack-1-psc-2.vrack.vmware.com**
6.0.0-3634791

 **PSC rack-1-psc-1.vrack.vmware.com**
6.0.0-3634791

 **10.0.0.10** NSX MANAGER
6.2.4-4292526

 **NSX Controller Cluster** CONTROLLER CLUSTER
6.2.47844

 Host Prep Clusters

vRack-Cluster 6.2.4.4292526

- 2 Click a component to view the upgrade history for that component.

The Upgrade History tab for that component is displayed.

Display Backup Locations

For LCM and ESXi updates, you can display the location where the configuration files for the updates are backed up.

Prerequisites

The LCM and/or ESXi update for which you want to see the backup location must have been completed.

Procedure

- 1 On the Lifecycle Management page, click the **INVENTORY** tab.
- 2 Click an LCM or ESXi resource.
The Resource Details page is displayed.
- 3 Click  to the right of the component name and then click **GET BACKUP LOCATION**.
The backup file name and location is displayed.

Upgrade Log File Locations

The log files for upgrade processes can be accessed from the following locations within the Cloud Foundation system.

To view the log files, log into the SDDC Manager VM as root (`root@sddc-manager-controller`)

Component	Log File Location	Log File Names
Bring-Up	<code>/opt/vmware/upgrades/bringup/<upgrade identifier>/backup/logs/</code>	<code>evosddc-bringup.log</code>
Lifecycle Management	<code>/home/vrack/lcm/upgrade/lcm/<upgrade identifier>/logs/</code>	<code>upgrade.log</code>
SDDC Manager	<code>/home/vrack/vrm/logs/</code>	<code>evosddc-upgrade.log</code>
System Controller Service (installation service)	<code>/opt/vmware/scs/logs/</code>	<code>scsupgradehelper.log</code> <code>post-install.log</code> <code>scsd.log</code> <code>scsdiag</code> <code>scsupgradehelper.log</code>
Supportability and Serviceability (SoS) tool	<code>/home/vrack/lcm/upgrade/lcm/<upgrade identifier>/thirdparty/sddc-support/logs/</code>	<code>sos_upgrade.log</code> <code>sos_upgrade.status</code>

Component	Log File Location	Log File Names
Java Runtime Environment (JRE)	/home/vrack/lcm/upgrade/lcm/<upgrade identifier>/thirdparty/<third-party upgrade id>/jre/logs/	jre_upgrade.log jre_upgrade.status
BaseOS	/home/vrack/lcm/upgrade/lcm/5eac6af9-f382-4ef1-9702-e2134e25eda3/thirdparty/<third-party upgrade id>/baseos-rpm-upgrades/logs/baseos_upgrade.log	baseos_upgrade.log baseos_upgrade.status

Upgrade Backup File Locations

During the upgrade process, each Cloud Foundation component are stored in the following locations within the systems.

Table 15-1.

Component	Location
Bring-Up	/opt/vmware/upgrades/bringup/<upgrade identifier>/backup
Lifecycle Management	/home/vrack/lcm/upgrade/lcm/<upgrade identifier>/backup
SDDC Manager	/home/vrack/lcm/upgrade/vrm/<upgrade identifier>/vrm-upgrade-r1/evoma

Upgrade Cloud Foundation to 2.3.1

16

Cloud Foundation 2.3.1 is a sequential upgrade.

Prerequisites

You must be at version 2.3 in order to upgrade to version 2.3.1. If you are at a version lower than 2.3, you must first upgrade to version 2.3 and then to version 2.3.1.

Procedure

- 1 Download all bundles. See [Download LCM Bundles](#).
- 2 Run pre-upgrade check. See [Run the Upgrade Pre-Check in the CLI](#).
- 3 Apply each Cloud Foundation bundle to the management domain and then to the remaining workload domains in your environment. See [Select Targets and Schedule Update](#).

Rack Wiring

17

Download VCF Wiremap from the Product Downloads page and connect the wires in your physical rack according to the wiremap. This section contains the logical views of the wiremaps.

High Level Wiring for Rack with Dell Management Switch

Figure 17-1. Wiremap for rack 1 with Cisco ToR Switches and Dell Management Switch

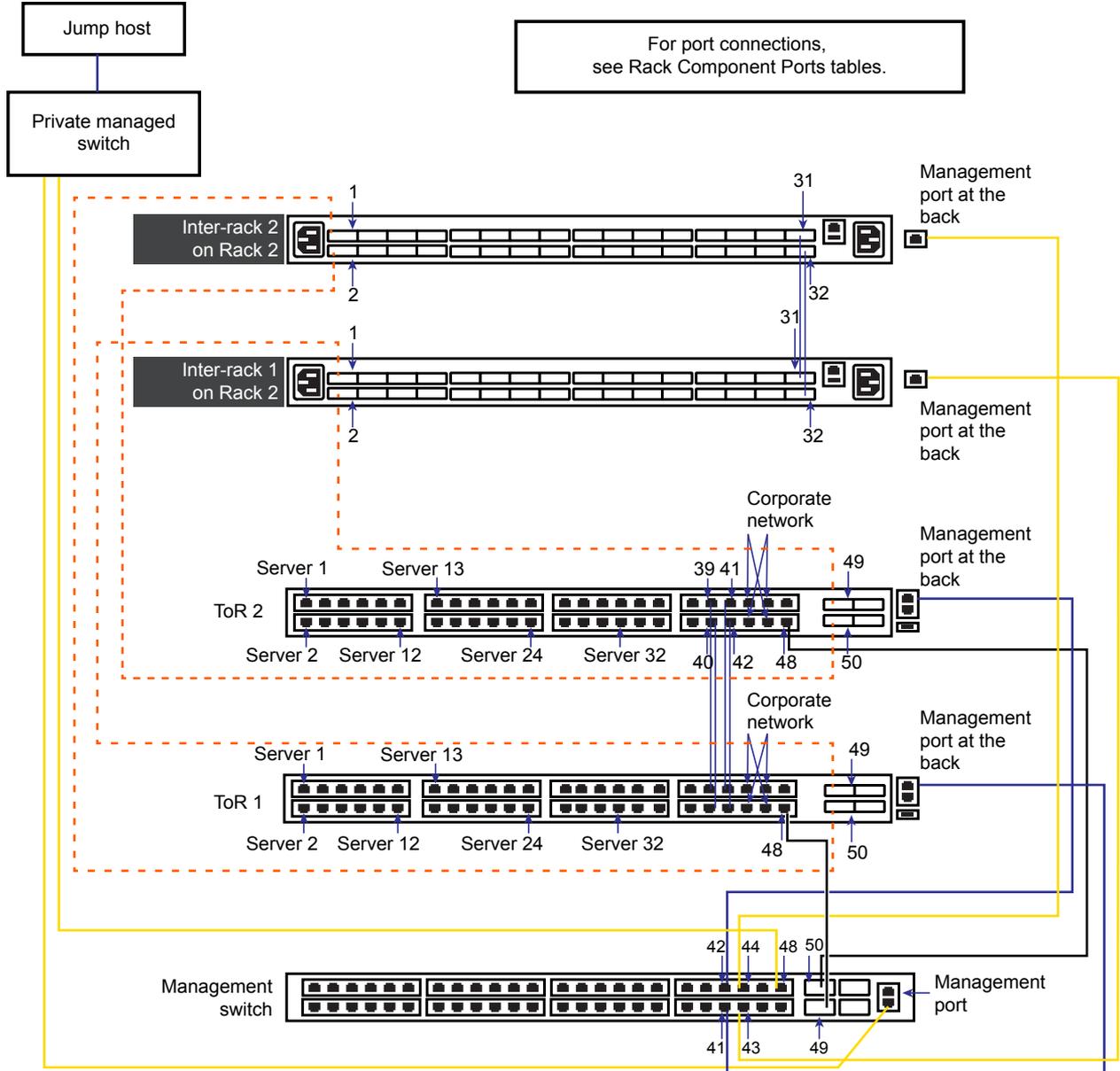
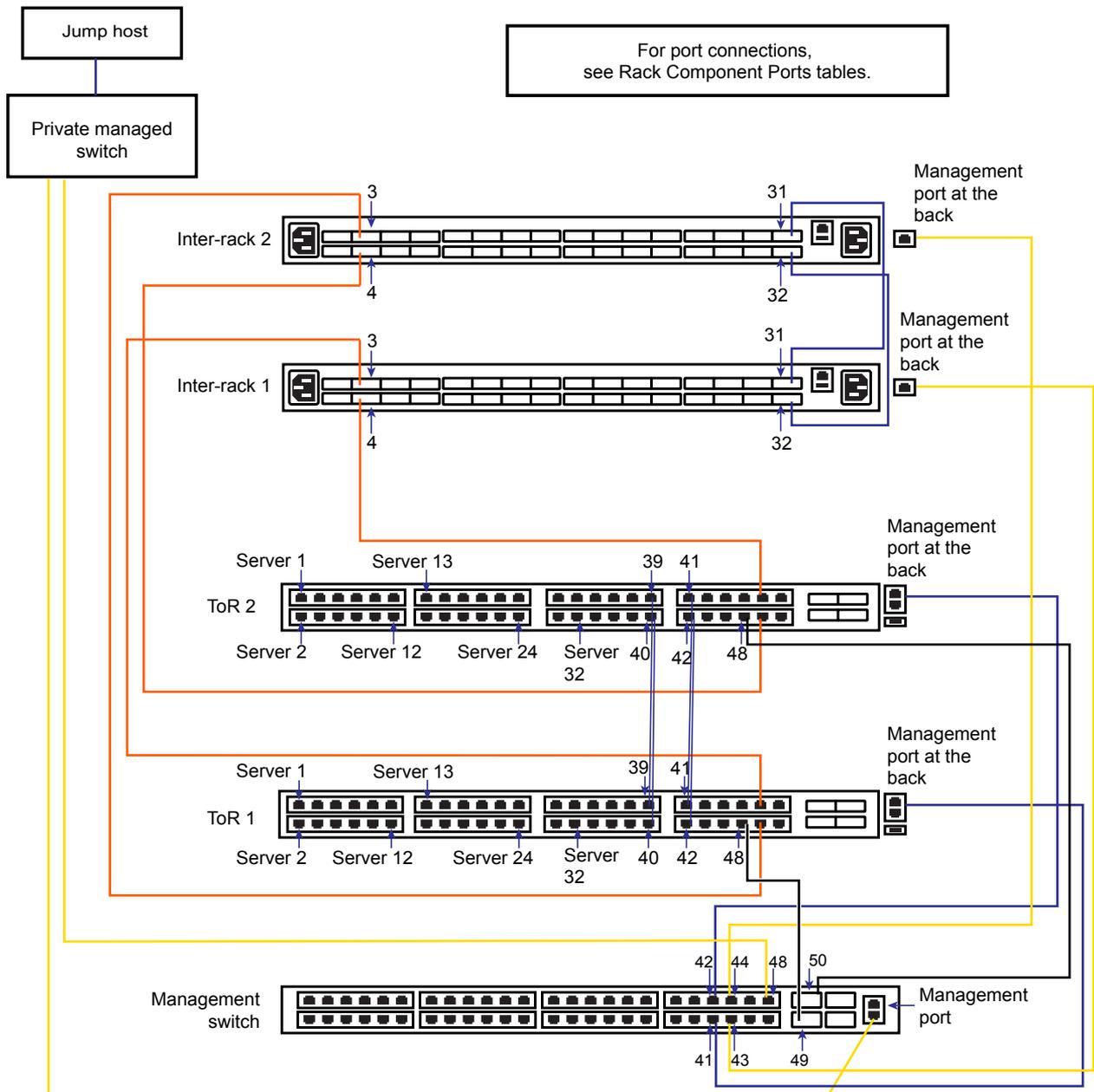


Figure 17-2. Wiremap for rack 2 with Cisco ToR Switches and Dell Management Switch



High Level Wiring for Rack with Quanta Management Switch

Figure 17-3. Wiremap for rack 1 with Cisco ToR Switches and Quanta Management Switch

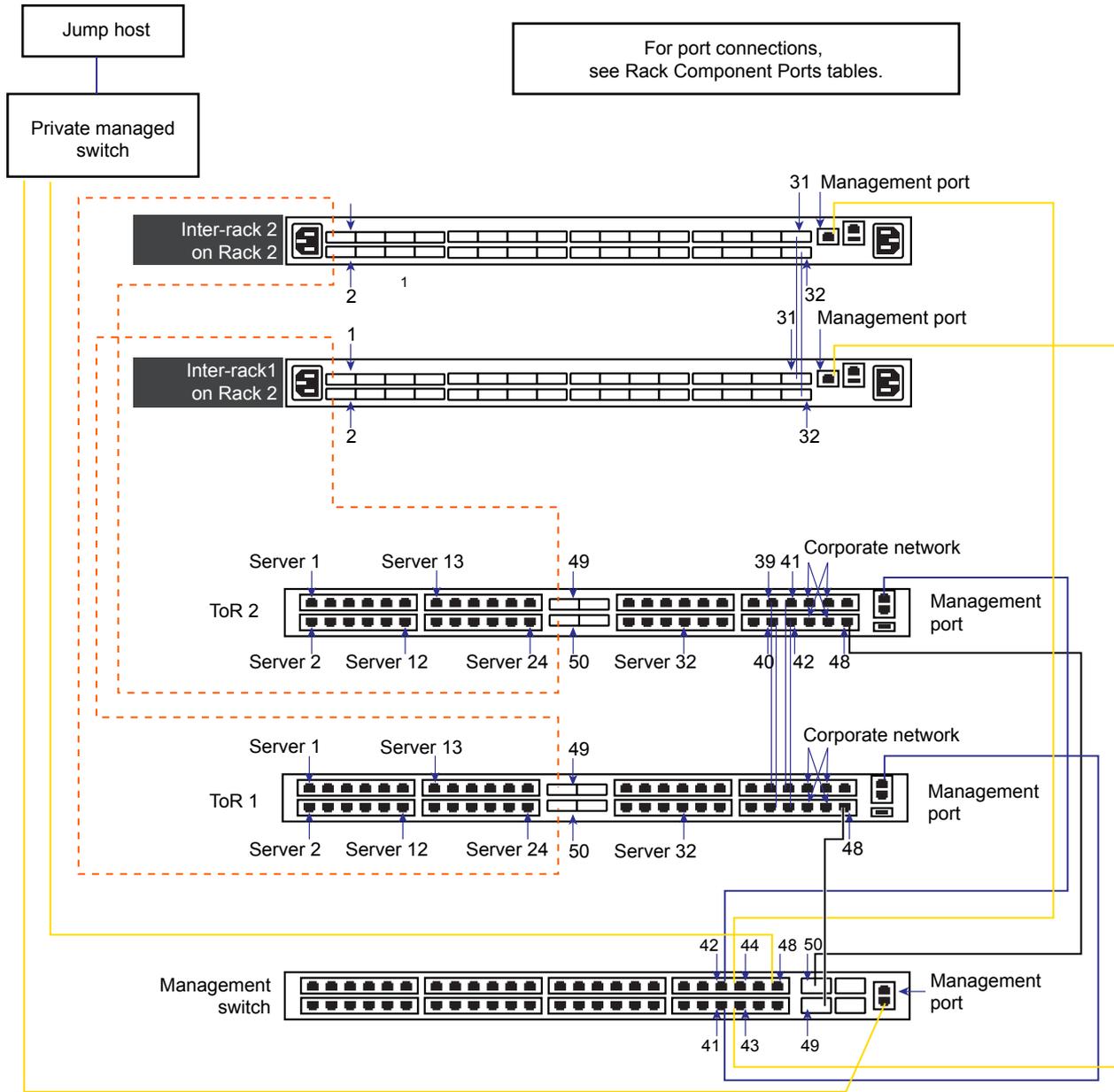
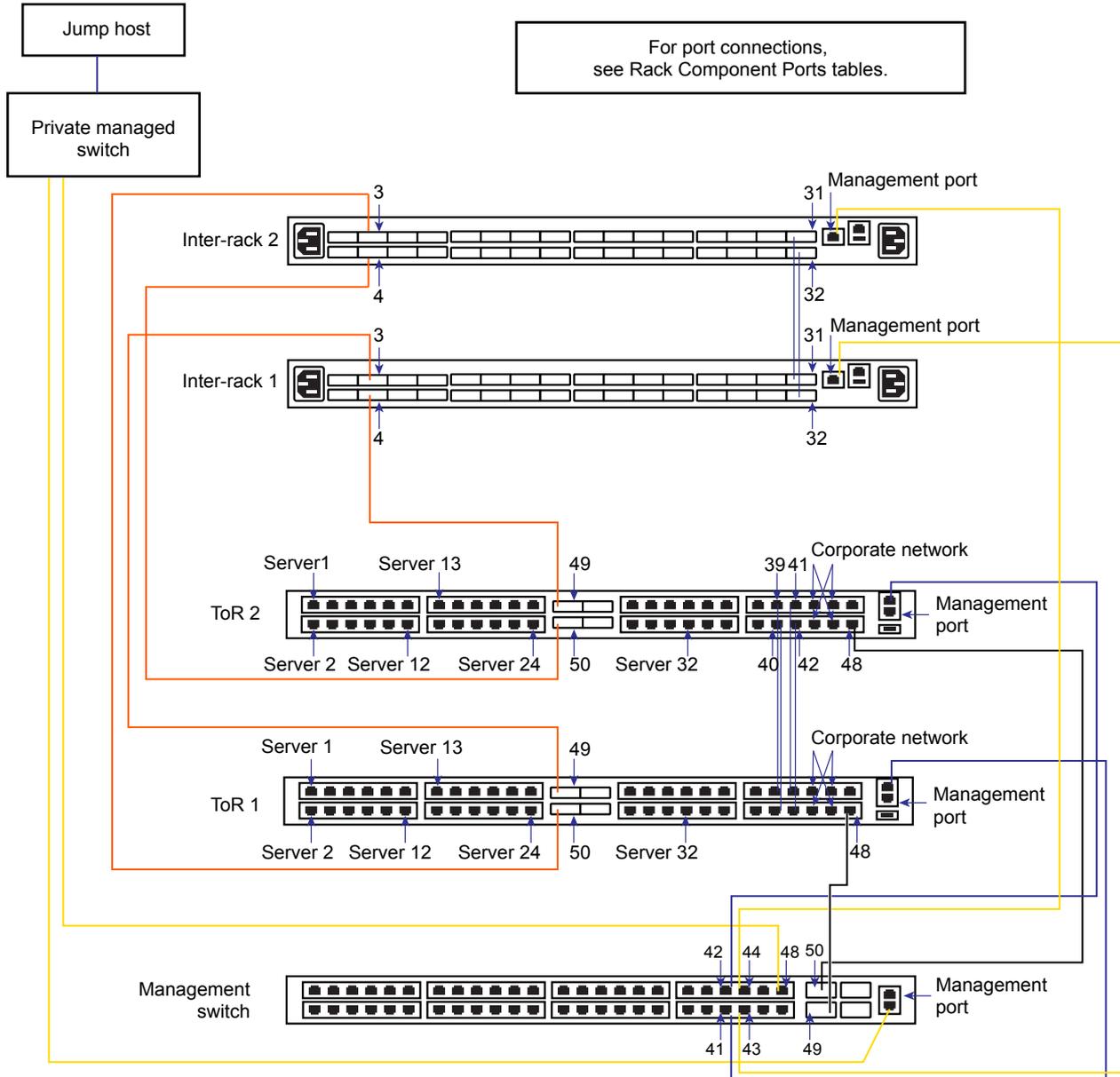


Figure 17-4. Wiremap for rack 2 with Cisco ToR Switches and Quanta Management Switch



Rack Component Ports

Refer to the tables below for port connectivity information using Cisco 9372PX as the illustrative example. Connections in your environment may vary based on the actual switches being used.

Console Serial Switch

Port Number	Connects To
1	Management switch console port
2	ToR 1 console port7

Port Number	Connects To
3	ToR 2 console port
4	Inter-rack 1 console port
5	Inter-rack 2 console port
6	PDU 1
7	PDU 2
8	PDU 3
9	PDU 4
10 - 16	Not connected

Inter-rack 2 (Rack 2 only)

Port Number	Speed	Connects To
1	40 Gbps	Rack 1 ToR 1 port 50
2	40 Gbps	Rack 1 ToR 2 port 50
3	40 Gbps	Rack 2 ToR 1 port 50
4	40 Gbps	Rack 2 ToR 2 port 50
5	40 Gbps	Rack 3 ToR 1 port 50
6	40 Gbps	Rack 3 ToR 2 port 50
7	40 Gbps	Rack 4 ToR 1 port 50
8	40 Gbps	Rack 4 ToR 2 port 50
9	40 Gbps	Rack 5 ToR 1 port 50
10	40 Gbps	Rack 5 ToR 2 port 50
11	40 Gbps	Rack 6 ToR 1 port 50
12	40 Gbps	Rack 6 ToR 2 port 50
13	40 Gbps	Rack 7 ToR 1 port 50
14	40 Gbps	Rack 7 ToR 2 port 50
15	40 Gbps	Rack 8 ToR 1 port 50
16	40 Gbps	Rack 8 ToR 2 port 50

Inter-rack 1 (Rack 2 only)

Port Number	Speed	Connects To
1	40 Gbps	Rack 1 ToR 1 port 49
2	40 Gbps	Rack 1 ToR 2 port 49
3	40 Gbps	Rack 2 ToR 1 port 49
4	40 Gbps	Rack 2 ToR 2 port 49

Port Number	Speed	Connects To
5	40 Gbps	Rack 3 ToR 1 port 49
6	40 Gbps	Rack 3 ToR 2 port 49
7	40 Gbps	Rack 4 ToR 1 port 49
8	40 Gbps	Rack 4 ToR 2 port 49
9	40 Gbps	Rack 5 ToR 1 port 49
10	40 Gbps	Rack 5 ToR 2 port 49
11	40 Gbps	Rack 6 ToR 1 port 49
12	40 Gbps	Rack 6 ToR 2 port 49
13	40 Gbps	Rack 7 ToR 1 port 49
14	40 Gbps	Rack 7 ToR 2 port 49
15	40 Gbps	Rack 8 ToR 1 port 49
16	40 Gbps	Rack 8 ToR 2 port 49

ToR 2 (e.g. Cisco 9372PX)

Port Number	Speed	Connects To
1 - 32	10 Gbps	node 1 - node 32 where port 1 connects to node 1, port 2 connects to node 2, and so on
33 - 38	NA	Not connected
39 - 42	10 Gbps	ToR 1 ports 39 - 42
43 - 46	10 Gbps	Corporate network as required (see note below table)
47	Blank	
48	1Gbps	Management switch port 50
49	40 Gbps	Inter-rack 1 port 2
50	40 Gbps	Inter-rack 2 port 2
51 - 54	40 Gbps	Corporate network as required (see note below table)
Management	1 Gbps	Management switch port 42

Note Depending on the switches in your environment, connect two 40 Gbps ports or multiple 10 Gbps ports to your corporate network.

ToR 1 (e.g. Cisco 9372PX)

Port Number	Speed	Connects To
1 - 32	10 Gbps	Node 1 - node 32 where port 1 connects to node 1, port 2 connects to node 2, and so on
33 - 38	NA	Not connected

Port Number	Speed	Connects To
39 - 42	10 Gbps	ToR 2 ports 39 - 42
43 - 46	10 Gbps	Corporate network as required (see note below table)
47	Blank	
48	1Gbps	Management switch port 49
49	40 Gbps	Inter-rack 1 port 1
50	40 Gbps	Inter-rack 2 port 1
51 - 54	40 Gbps	Corporate network as required (see note below table)
Management	1 Gbps	Management switch port 41

Note Depending on the switches in your environment, connect two 40 Gbps ports or multiple 10 Gbps ports to your corporate network.

Management Switch

Port Number	Speed	Connects To
1 - 32	1 Gbps	Ports 1 - 32 are blank. You can connect these ports to the BMC ports on servers. This is optional and is not required for imaging. See "Guidance on Server OOB Port Management" in the <i>VIA User's Guide</i> .
33 - 40	NA	Not connected
41	1Gbps	ToR 1 management port
42	1Gbps	ToR 2 management port
43	1Gbps	Inter-rack 1 management port
44	1Gbps	Inter-rack 2 management port
45-47	NA	Not connected
48	1Gbps	Private managed switch
49	10 Gbps	ToR 1 port 48
50	10 Gbps	ToR 2 port 48
51-52	NA	Not connected
Management port		Private managed switch

Note PDU ports are not reflected in the table above.

Troubleshooting Cloud Foundation for Data Center System Administrators

18

You can troubleshoot issues that you might experience after you install and deploy your Cloud Foundation environment.

This chapter includes the following topics:

- [Unable to Browse to the Software Stack Web Interfaces Using their Fully Qualified Domain Names](#)
- [Decommission Workflow Stops Responding at Task Named Enter Hosts Maintenance Mode](#)
- [VDI Workload Creation Fails at the Import DHCP Relay Agents Task](#)
- [Update Fails While Exiting Maintenance Mode](#)
- [Restore ESXi Server After Update Failure](#)

Unable to Browse to the Software Stack Web Interfaces Using their Fully Qualified Domain Names

You point your browser to the fully qualified domain name (FQDN) of one of the VMware SDDC products in the Cloud Foundation software stack, but the login screen for that software product does not appear in the browser.

Problem

In the SDDC Manager Dashboard in your browser, you can see a list of the FQDN names that are assigned to the VMware SDDC products' Web interfaces on the Management Info area of the management domain. However, when you directly type one of those names into your browser, the login screen does not appear and the browser cannot complete the request.

Cause

The FQDN names contain a portion that is the value that was entered for the subdomain when you ran the Cloud Foundation bring-up process. For example, the FQDN for a rack's vCenter Server instance might be listed as rack-1-vc-1.sddc.example.com, where sddc.example.com is the full value that appeared in the bring-up wizard screens.

The SDDC Manager runs an internal DNS server so that it can guarantee that FQDN resolution works within the installation. If a delegation record was not configured in the specified root domain to point to the SDDC Manager DNS server for the specified Cloud Foundation zone, these FQDNs cannot be resolved.

You configure the zone delegation using the standard administration tools used by your company or organization to manage the DNS server that was specified in bring-up wizard, such as Server Manager on Microsoft Windows Server operating systems.

The following steps illustrate configuring the zone delegation using Server Manager on Windows 2008 Server.

Solution

1 In Microsoft Server Manager, expand the navigation tree to see the Forward Lookup Zones and the name of the root domain.

2 Right-click the root domain and click **New Delegation** in the pop-up menu.

The New Delegation wizard appears.

3 Start the wizard by clicking **Next** and typing the subdomain portion for your installation in the **Delegated domain** field.

The **Full qualified domain name (FQDN)** field automatically fills in.

4 Verify that the automatically filled-in name matches the portion in the VMware SDDC components' FQDN names that you are attempting to use in the browser to log in to those components' Web interfaces, and then click **Next** to proceed.

5 Click **Add** to specify the VIP address of the SDDC Manager virtual machine.

The New Name Server Record window appears.

6 Type the SDDC Manager VM's IP in the **Server the fully qualified domain name** field.

7 Click **Resolve**.

After you click **Resolve**, the IP address is listed in the **IP Addresses** list box and validated as OK if your DNS server can reach the SDDC Manager virtual machine.

8 If the IP address validates, click **OK** to proceed.

If the IP address does not validate, call support to request assistance.

The IP address is listed in the **Name servers** list box.

9 Click **Next** to proceed.

The delegation record has been created and you can click **Finish** to close the wizard.

Decommission Workflow Stops Responding at Task Named Enter Hosts Maintenance Mode

During the running of the workflow to decommission an ESXi host, the workflow's progress appears stuck at the task for putting the host in maintenance mode.

Problem

When you examine the progress of the decommission workflow on the Workflows page, you see the workflow has reached the task named `Enter hosts maintenance mode`. However, the workflow does not progress beyond that task.

Cause

During the decommission workflow, the workflow invokes the standard vSphere operation to put the host in maintenance mode. When the host you are decommissioning is part of a management domain or a workload domain, DRS is in force on that management or workload domain. If the host has VMs running on it, when the decommission workflow invokes the operation to put the host in maintenance mode, DRS is automatically invoked to migrate those VMs to another host.

In some situations, DRS might fail to automatically migrate all of the VMs off of the host. For example, if migrating all of the VMs to the other hosts in the underlying group might violate a VM/Host DRS or vSphere HA failover rule, then DRS does not migrate the VMs.

If VMs remain on the host, the host cannot enter maintenance mode and the decommission workflow cannot complete that task and progress to its next task. To resolve this situation, you can manually migrate the VMs to another host in the group and then use the Restart Workflow icon to restart the decommission workflow.

Solution

- 1 Verify that DRS has failed to automatically migrate VMs off the host by opening the vSphere Web Client and examining the recent tasks.
 - a In the SDDC Manager Dashboard, navigate to that host's Host Details page.
 - b Click the vCenter Server launch link to launch the vSphere Web Client.
 - c In the vSphere Web Client, locate the `Enter maintenance mode` task in the Recent Tasks pane. Confirm the status of the `Enter maintenance mode` task indicates it is waiting for all VMs to be powered off or migrated.
- 2 Locate the VMs that remain on the host by clicking **Related Objects > Virtual Machines** for the host.
- 3 Migrate each VM to another host in the workload domain until there are no VMs running on that host.
- 4 In the SDDC Manager Dashboard, restart the decommission workflow.
 - a Navigate to **System Status > Workflows** and expand the decommission workflow to see its details.
 - b Click **RESTART WORKFLOW**.

VDI Workload Creation Fails at the Import DHCP Relay Agents Task

When routing is not set up between your Cloud Foundation system's management network and the data center network specified in the VDI workload domain creation wizard, the creation workflow fails at the Import DHCP Relay Agents task.

Problem

In the Workflows screen, you see that the creation workflow for your VDI workload domain environment has failed in the task Import DHCP Relay Agents.

Cause

When your Cloud Foundation installation's public management network cannot communicate with the VDI environment's data center network, the Import DHCP Relay Agents task will fail. During the creation workflow, SDDC Manager deploys a virtual machine used for DHCP relay on the data center network. This DHCP relay is used by the virtual desktops, which are also deployed in the data center network. However, the SDDC Manager VM resides on the management network and must be able to communicate with the DHCP Relay VM. When routing has not been set up between the management network and the data center network specified in the VDI workload domain creation wizard such that the two VMs can communicate with each other, the workflow fails at this task.

Solution

- ◆ Verify that the SDDC Manager VM can communicate with the data center network.

One way to verify is to remotely log in to the SDDC Manager VM, and try to ping the data center network.

- If the SDDC Manager VM can ping the data center network, then communication exists between the management network and the data center network, and the failed task is due to a different cause.
- If the SDDC Manager VM cannot ping the data center network, speak to your organization's networking administrator to have the necessary routing set up.

Update Fails While Exiting Maintenance Mode

vCenter Server and ESXi update on a host might fail in the task of exiting maintenance mode.

Problem

Sometimes during an ESXi and vCenter update process, a host might fail to exit maintenance mode, which results in a failed update process.

Cause

During an update, the system puts a host into maintenance mode to perform the update on that host, and then tells the host to exit maintenance mode after its update is completed. At that point in time, an issue on the host might prevent it from exiting maintenance mode.

Solution

- 1 Attempt to remove the host from maintenance mode in vSphere Web Client.
 - a In the vSphere Web Client, locate the host.
 - b Right-click the host name and select **Maintenance Mode > Exit Maintenance Mode**.
The vSphere Web Client reports any issues with the host regarding maintenance mode.
 - c Address any reported issues and remove the host from maintenance mode.
- 2 When the host has successfully existed from maintenance mode, return to the SDDC Manager interface.
- 3 Retry the update from the **Available Updates** list.

Restore ESXi Server After Update Failure

During the update process, the ESXi update fails, returning the error code ESX_UPGRADE_FAILED.

Problem

Sometimes during an ESXi update, the process fails. In this case, you can restore the ESXi server from the configuration backup file taken before the update process. Restoring the host configuration also restores the state of the ESXi and the vSphere standard switch networking configuration.

Cause

ESXi server requires restoration following a failed ESXi update process.

Solution

- 1 Copy the backup file from the backup VM to a location that is accessible from the current ESXi host.
If necessary, you can obtain information about the backup from the failed ESXi host.
 - a Log in to the SDDC Manager and click the **LIFECYCLE** tab.
 - b Click the **UPDATE** tab and open **Completed Updates**.
 - c Locate the update and select **View Details** from the drop-down list.
 - d Expand the detailed view and locate the failed ESXi update.
 - e Click the failed ESXi host and select **Get Backup Information** from the drop-down list.
- 2 Enter maintenance mode.
- 3 Restore the backup using the PowerCLI or the ESXi Command Line.

For more information about using the PowerCLI, see the [VMware PowerCLI Documentation](#).

Note The build number of the host must match the build number of the host that created the backup file. Use the `-force` option to override this requirement.

To restore the backup using the PowerCLI.

- a Put the host into maintenance mode.

```
Set-VMHost -VMHost <ESXi_host_IP_address> -State 'Maintenance'
```

- b Restore the configuration from the backup bundle.

```
Set-VMHostFirmware -VMHost <ESXi_host_IP_address> \  
-Restore -SourcePath <backup_file_path_and_name> \  
-HostUser <username> -HostPassword <password>
```

- c Take the host out of maintenance mode.

```
Set-VMHost -VMHost <ESXi_host_IP_address> -State 'Connected'
```

To restore the backup using the ESXi Command Line.

- a Put the host into maintenance mode.

```
vim-cmd hostsvc/maintenance_mode_enter
```

- b Copy the backup configuration file on the host.

The backup file is located at /tmp/configBundle.tgz.

- c Restore the configuration from the backup bundle.

Note This command will initiate an automatic reboot of the host.

```
vim-cmd hostsvc/firmware/restore_config /tmp/configBundle.tgz
```

- d Take the host out of maintenance mode.

```
vim-cmd hostsvc/maintenance_mode_exit
```

Cloud Foundation Glossary

19

Term	Description
add rack	Configure an additional rack for a Cloud Foundation system.
additional rack	Additional racks (added after the first rack) to a Cloud Foundation system.
bring-up	Initial configuration of a newly deployed Cloud Foundation system. .
Cloud Foundation system.	Set of physical racks managed as a unit by a single SDDC Manager.
first rack	First (primary) rack in the Cloud Foundation system. The management domain is deployed on this rack.
Hardware Management System (HMS)	Manages hosts and switches in the Cloud Foundation system.
host	An imaged server.
imaging	During imaging, SDDC software is pre-configured on a physical rack.
integrated system	System that combines hardware and software. Can be purchased from select VMware partners. The partner images the rack before sending it to the customer site.
inter-rack switches	Connects individual ToR switches with each other to provide connectivity across racks. These switches are required only when you have more than one rack in your Cloud Foundation system, and are placed on the second rack.
Lifecycle Manager (LCM)	Automates patching and upgrading of the software stack.
management domain	Cluster of physical hosts (first four hosts in the physical rack) that house the management component VMs
management host	Standalone ESXi server to host the Windows jump VM used for imaging.
primary host	Host on which VIA deploys the SDDC Manager VMs during imaging, and which bootstraps the first rack during bring-up.
SDDC Manager	Software component that provisions, manages, and monitors the logical and physical resources of a Cloud Foundation system.
SDDC ManagerController VM	Contains the SDDC Managerservices and a shell from which command line tools can be run. This VM exposes the SDDC Manager UI.
SDDC Manager Utility VM	Contains the LCM depot, backup repository containing NSX Manager and host backups, and 2nd DNS instance.
server	Bare metal server in a physical rack. After imaging, it is referred to as a host.
Top of Rack (ToR) switch	Connects servers within a rack through 10Gbps links to the NICs on each server. A Cloud Foundation rack contains two ToR switches connected to each other.

Term	Description
unassigned host	Host in the capacity pool that does not belong to a workload domain.
workload domain	A policy based resource container with specific availability and performance attributes and combining vSphere, vSAN and NSX into single a consumable entity. A workload domain can be created, expanded, and deleted as part of the SDDC lifecycle operations.