Administering VMware Cloud Foundation

SDDC Manager
VMware Cloud Foundation 2.1.1

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.
You can find the most up-to-date technical documentation on the VMware Web site at:
http://www.vmware.com/support/
The VMware Web site also provides the latest product updates.
If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com
Contents

About Administering VMware Cloud Foundation 7

1 Administering Cloud Foundation Environments 9
   VMware Software Components Deployed in a Typical Cloud Foundation Environment 10
   Client Web Interfaces Used When Administering Your Cloud Foundation Environment 12

2 Getting Started with the SDDC Manager Client 13
   Log in to the SDDC Manager Client 13
   Tour of the SDDC Manager User Interface 14
   Log out of the SDDC Manager Client 19

3 On-Demand Password Rotation in Your Cloud Foundation Installation 21
   Credentials for Logging In To the SDDC Manager (vrm) Virtual Machine 22
   Look Up Account Credentials Using the Lookup-Password Command 23
   Rotate All Passwords On-Demand for the Managed Physical and Logical Entities 24
   vrm-cli Command Reference 26

4 Managing Users and Groups 31
   Active Directory and the Cloud Foundation Environment 31
      Configure an Active Directory Domain as an Identity Source for your Cloud Foundation Environment 32
      Grant Permission to Active Directory Users and Groups to Log in to the vSphere Web Client in Your Cloud Foundation Installation 34
   Add Local Users and Groups 35
   Assign Permissions to Users and Groups 37
   Add System Administrators 37
   Role-Based Access Control 38
   User Passwords in Your Cloud Foundation Environment 38
      Modify Password Policy for Users 39

5 Managing Physical Resources 41

6 Working with Management Domains and Workload Domains 43
   Creating and Provisioning Workload Domains 45
      Create a Virtual Infrastructure Workload Domain 45
      Navigate into the VI Workload Domain’s Virtual Environment 52
      Create a VDI Workload Domain 53
   Utilize Capacity on Management Domain 67
   Expanding Management and Workload Domains 68
      Expand a Management Domain 68
      Expand a VI Workload Domain 68
Expand a VDI Workload Domain 69
Delete a Workload Domain 70
Enabling vSAN Space Efficiency Features in All-Flash Installations 70
Manually Update the Credentials for the vRealize Operations for Horizon Broker Agent When Account Credentials Change for the Connection Server Administrator Account 72

7 Monitoring Capabilities in the Cloud Foundation Environment 73
Managing Workflows and Tasks 76
Managing Alerts, Events, and Audit Events 77
  Event Catalog 81
  Alert Catalog 87
  SDDC Manager Alerts Raised During Ongoing Operations 87
Using vRealize Log Insight Capabilities in Your Cloud Foundation Environment 92
  Get Started Using the vRealize Log Insight Instance 94
  Configure Syslog from the Switches to vRealize Log Insight 96
Using vRealize Operations Manager Capabilities in Your Cloud Foundation Environment 96
  Examine the Health of the Virtual Infrastructure Using vRealize Operations Manager 97

8 Settings Configuration Using the SDDC Manager Client 99
Customize Default Values Used When Creating VDI Workload Domains 99
  VDI Infrastructure Settings 100
  Additional Rack Settings Screen 102
Managing Network Settings 102
  Manage Uplink Connectivity Settings Using the SDDC Manager Client 103
About Excluding IP Address from SDDC Manager Use 104
  IP Distribution Screen 104
  Data Center Screen 105

9 Back Up Component Configurations Using the SoS Tool 107

10 Adding and Replacing Hosts 109
Add a Host to a Physical Rack 109
  Add a New Host to a Physical Rack 109
  Add a Previously Decommissioned Host to a Physical Rack 112
Replace Hosts and Hosts Components 114
  Replace Components of a Host Running in Degraded Mode 114
  Replace Dead Host or Host SAS Controller or Expander 117
  Replace SATADOM Disk on a Host 122
Install ESXi VIBs on New Host 125

11 Replacing and Restoring Switches 129
Replace a Management Switch 129
  Set Default Boot Mode on New Management Switch 130
  Image New Management Switch 130
  Restore Backup Configuration on New Management Switch 131
Replace a Cisco Top-of-Rack or Spine Switch 132
Replace an Arista Top-of-Rack or Spine Switch 135
About Administering VMware Cloud Foundation

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

Intended Audience

The Administering VMware Cloud Foundation is intended for data center system administrators who manage their organization’s Cloud Foundation environment. 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 Virtual SAN™
- 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® Operations™
- VMware vRealize® Log Insight™
- The View components from the VMware Horizon® 6 product
- VMware App Volumes™

Related Publications

The VMware Cloud Foundation Overview and Bring-Up Guide contains detailed information about a Cloud Foundation installation, its components, and the network topology of a deployed environment.
VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

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.
Cloud Foundation enables deployment of a private cloud environment based on VMware's software-defined data center (SDDC) architecture. A Cloud Foundation installation is a turnkey private cloud instance that is easily deployed in a corporate network. 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, the virtual rack. 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 environments and have licensed use of the deployed vRealize Log Insight and vRealize Operations instances, SDDC Manager configures the vRealize Log Insight and vRealize Operations instances for those environments, to provide performance management, capacity optimization, and real-time log analytics. Cloud Foundation installations 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 installation, 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 environment. An administrator of an Cloud Foundation environment performs tasks such as:

- Manage users, roles, and permissions
- Manage physical and logical resources
- Configure and provision the environments, the workload domains, that are used to provide service offerings
- Manage provisioned workload domains
- Monitor alerts and the health of the installation
- When the deployed vRealize Log Insight instance is licensed for use in your Cloud Foundation installation, use the auditing and log analytics capabilities of the vRealize Log Insight instance to troubleshoot issues and prevent problems across the physical and virtual infrastructure
- When the deployed vRealize Operations Manager instance is licensed for use in your Cloud Foundation installation, use the centralized monitoring capabilities of the vRealize Operations instance to manage performance and gain insight into the health of the environment 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 Environment,” on page 10
- “Client Web Interfaces Used When Administering Your Cloud Foundation Environment,” on page 12

**VMware Software Components Deployed in a Typical Cloud Foundation Environment**

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

Licensed for use by the base Cloud Foundation license:

- The SDDC Manager, the Hardware Management Services, and their subcomponents that provide centralized management of the Cloud Foundation software stack
- The VMware software stack that implements a software-defined data center and which are deployed by SDDC Manager are:
  - vSphere
  - Platform Services Controller, used as the identity provider
  - Virtual SAN
  - NSX for vSphere

Separately licensed software components that are deployed by SDDC Manager are:

- vCenter Server
- vRealize Operations
- vRealize Log Insight
- VMware Horizon with View that provides virtual desktop infrastructure (VDI) environments
- App Volumes

**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](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 environment after the initial bring-up process, see the *Release Notes* document for your Cloud Foundation version. If the environment has been updated after the initial bring-up process using the Life Cycle Management features, see “View Inventory Component Versions,” on page 163 for details on how to view the versions of the VMware software components that are within your environment.

**Caution** Do not manually change any of the settings that SDDC Manager sets automatically by default. 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.

Some of the default configuration settings can be customized using the SDDC Manager client. See Chapter 8, “Settings Configuration Using the SDDC Manager Client,” on page 99.

You can find the documentation for the following VMware software products and components at [www.vmware.com/support/pubs](http://www.vmware.com/support/pubs):

- vSphere
- Platform Services Controller, used as the identity provider
About the Primary Rack and the SDDC Manager Virtual IP Address

In a multirack Cloud Foundation installation, the primary rack is the one that:

- Was the rack that went through the bring-up process first, the initial one in the installation
- Has its ToR switches configured with uplink ports to carry traffic to your corporate network
- Has the environment’s three ISVM VMs and two Platform Services Controller VMs deployed on ESXi hosts in that rack

An instance of SDDC Manager is deployed on each physical rack as part of a managed cluster of services provided by the three ISVM VMs on the primary rack. Each of the SDDC Manager instances connects to those three ISVM VMs to read and write data. Even though each of those SDDC Manager instances has its own management IP address, a virtual IP (VIP) address is assigned to a network subinterface on one of the SDDC Manager instances. This VIP provides the convenience of having a single DNS name and IP address to connect to the SDDC Manager client.

Usually, the primary rack’s SDDC Manager instance is assigned the VIP address because the VIP address gets created during the bring-up process on the initial rack in an installation. However, there are situations in which you will find the VIP address is assigned to one of the other racks’ SDDC Manager instances. Whenever the vrm-tcservice service is stopped in the SDDC Manager instance having the VIP address, the VIP address is automatically reassigned to the next rack’s SDDC Manager instance. For example, if the instance that has the VIP address is rebooted, the VIP address is automatically reassigned to another SDDC Manager instance. As a result, the primary rack is not always the same rack having the SDDC Manager instance with the VIP address.

When you view the domain details for any of the management domains using the SDDC Manager client, the SDDC Manager VIP address is displayed in the domain details screens, in the table labeled VMware Cloud Foundation Management Components. For the SDDC Manager instance on a given rack, you can determine if the VIP is assigned to it by logging in to that rack’s SDDC Manager instance using the root account and issuing the `ifconfig` command:

```
rack-1-vrm-1:~ # ifconfig
```

When the VIP is assigned to that instance, the `ifconfig` commands output lists an eth0:1000 subinterface with the VIP address assigned to the subinterface’s inet addr.

For a description of SDDC Manager in a multirack setup, see the *VMware Cloud Foundation Overview and Bring-Up Guide*. 
Client Web Interfaces Used When Administering Your Cloud Foundation Environment

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

SDDC Manager does not mask the individual component management products. Along with the SDDC Manager client, for certain tasks, you might also use the following Web interfaces for administration tasks involving their associated VMware software components that are part of a VMware SDDC. All of these interfaces run in a browser, and you can launch many of them from locations in the SDDC Manager client.

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

<table>
<thead>
<tr>
<th>VMware SDDC Web Interfaces</th>
<th>Description</th>
<th>Launch Link Location in SDDC Manager Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere Web Client</td>
<td>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.</td>
<td>The General Info screen of the Domain Details page for management and workload domains has a launch link labeled vCenter.</td>
</tr>
<tr>
<td>vRealize Log Insight Web interface</td>
<td>When the vRealize Log Insight instance is licensed for use in the environment, this interface provides direct access to the logs and event data collected and aggregated in vRealize Log Insight for troubleshooting, trend analysis, and reporting.</td>
<td>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 open the vRealize Log Insight Web interface.</td>
</tr>
<tr>
<td>vRealize Operations Manager Web interface</td>
<td>When the vRealize Operations Manager instance is licensed for use in the environment, this interface provides direct access to the event and alert data collected in vRealize Operations Manager for analysis.</td>
<td>The Management Info screen of the Domain Details page for management domains has a launch link labeled vROPS.</td>
</tr>
</tbody>
</table>

If a VDI workload domain is deployed and licensed for use in your environment, you might also use the following Web interfaces for administration tasks involving the associated VMware software components in such a VDI environment:

- View Administrator Web interface
- App Volumes Manager Console

Launch links are not provided in the SDDC Manager client 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 virtual machine for the View Server or App Volumes Manager Server 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 the SDDC Manager Client

You use the SDDC Manager client to perform administration tasks on your Cloud Foundation environment. 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 client by loading it in an industry-standard Web browser. For the list of supported Web browser types and versions, see the Release Notes.

**Note** When performing out-of-band (OOB) troubleshooting of hardware using the Java-based consoles, the Firefox browser is typically used instead of the Chrome browser because of the Firefox browser's support of the Java-based console.

This chapter includes the following topics:

- “Log in to the SDDC Manager Client,” on page 13
- “Tour of the SDDC Manager User Interface,” on page 14
- “Log out of the SDDC Manager Client,” on page 19

Log in to the SDDC Manager Client

You access the SDDC Manager client using a standard Web browser.

**Prerequisites**

Verify that you have the following information:

- A user name and password for an account that is configured for accessing the SDDC Manager client. Your installation 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,” on page 38.

  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 virtual IP address (VIP). This name typically has a form like `vrm.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 initial rack in a Cloud Foundation environment, this FQDN and VIP address are created and the VIP address is assigned to a network subinterface of the SDDC Manager instance that is deployed in that initial rack.
See the VMware Cloud Foundation Overview and Bring-Up Guide for details about the IP addresses that are assigned during the bring-up process. For a description of the SDDC Manager VIP address, see “About the Primary Rack and the SDDC Manager Virtual IP Address,” on page 11.

**Procedure**

1. In a Web browser, open the login screen by navigating to `https://VIP-FQDN/vrm-ui`
   For example, point your browser to `https://vrm.sddc.example.com:8443/vrm-ui`

2. Log in using the user name and password for an account that is configured for access.

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

---

**Tour of the SDDC Manager User Interface**

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

In the client loaded in your browser, 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 | Dashboard
[Status] | Status | System status
[Lifecycle] | Lifecycle | Life cycle management
[Users] | Users | User management
[Settings] | Settings | System settings

**Dashboard**

The Dashboard page is the home page that provides the overall administrative view of your Cloud Foundation environment. The Dashboard page provides a top-level view of the physical and logical resources across all of the physical racks in the environment, 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 5, “Managing Physical Resources,” on page 41
- Chapter 6, “Working with Management Domains and Workload Domains,” on page 43

### System Status

Use this page to check on the health of the environment. You can view SDDC Manager alerts, examine historical and current information about the workflows running in the environment, 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 environment has event-driven problem detection. The software records an event for environment 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 7, “Monitoring Capabilities in the Cloud Foundation Environment,” on page 73 for the information about using alerts and events to monitor the health of your Cloud Foundation environment.

**User Management**

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

- In the Users & Groups screen, grant or revoke the ability for users and groups to use the SDDC Manager client.
- 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.


**Life Cycle Management**

Use this page to manage the patching and maintenance of the software components that are installed in the environment. 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 14, “Patching and Upgrading Cloud Foundation,” on page 149.
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 environments that you can provision in your Cloud Foundation installation. For details about setting defaults used for VDI environments, see “Customize Default Values Used When Creating VDI Workload Domains,” on page 99.
- Initiate the process for adding a new rack to the environment.
- Work with network settings, such as editing uplink connectivity settings, reviewing the IP address distribution in the environment, excluding IP addresses, entering data center network configurations, and associating those configurations with workload domains.
- Manage product license keys.

Log out of the SDDC Manager Client

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

Procedure

1. In the SDDC Manager client, 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.
On-Demand Password Rotation in Your Cloud Foundation Installation

To ensure security in your installation, you can rotate the passwords for the built-in accounts that are used by the installation’s physical and logical entities using the vrm-cli tool. Rotating these passwords periodically or when certain events occur, such as an administrator leaving your organization, reduces the likelihood of security vulnerabilities occurring.

Many of the physical and logical entities in your Cloud Foundation installation have built-in accounts. Those accounts’ passwords are managed by the SDDC Manager software’s vrm-cli tool. At the end of the bring-up process on a physical rack, you are required to rotate the account passwords by logging in to that rack’s SDDC Manager virtual machine, stopping the vrm-watchdogserver and vrm-tserver services, and running the `.vrm-cli.sh rotate-all` command. At any time, you can use the `.vrm-cli.sh lookup-password` command to get a listing of the account names and current passwords for these built-in accounts.

The types of accounts for which the passwords are rotated using the vrm-cli tool are:

- Accounts used for service consoles, for example the ESX root account
- Single sign-on account
- Default administrative user account used by virtual appliances
- Cumulus Account used by switches running Cumulus Linux, for example, the management switches
- Network-admin roles used by switches not running Cumulus Linux
- Root accounts for the LCM and LCM Backup virtual machines
- Service accounts, such as the backupuser account for the LCM Backup virtual machine
- Internal database service accounts, such as the JDBC account

To rotate IPMI passwords, you run the `.vrm-cli.sh rotate-password-ipmi` command.

The rotation process generates randomized passwords for the accounts.

**IMPORTANT** Always modify these passwords using the vrm-cli tool. Do not manually modify the passwords for the accounts that are managed by the vrm-cli tool. Manually modifying these passwords outside of the vrm-cli tool breaks the SDDC Manager software’s ability to manage the physical and logical entities.
When you rotate passwords on-demand in a steady-state installation, you must run the "./vrm-cli.sh rotate-all" command in turn on each physical rack in the installation. When the command is run on the Cloud Foundation environment’s primary rack, the passwords for entities local to that rack, such as the ESXi hosts and switches, are rotated as well as the entities that cross physical racks, such as the vRealize Operations Manager cluster nodes. After running the command on the primary rack, you run the command on the subsequent racks, which changes the passwords for entities local to that rack.

**NOTE** For a description of which rack in a Cloud Foundation installation is the primary rack, see “About the Primary Rack and the SDDC Manager Virtual IP Address,” on page 11.

You run the vrm-cli.sh rotate-all command by logging in to a rack’s SDDC Manager VM using the root account credentials. The vrm-cli.sh script is located in the /home/vrack/bin directory. For information about the SDDC Manager VM’s root account, see “Credentials for Logging In To the SDDC Manager (vrm) Virtual Machine,” on page 22.

**IMPORTANT** Before performing on-demand password rotation, ensure:

- No failed workflows exist in your installation. Use the Workflows area of the System Status page to verify there are no workflows in a failure state.
- No active workflows, such as creating or deleting workload domains, are running or are expected to run during the password rotation process. Before performing on-demand password rotation, schedule a window of time in which you expect no running workflows to occur.
- The services vrm-watchdogserver and vrm-tcserver are stopped in the SDDC Manager virtual machine in which you are running the vrm-cli tool.

This chapter includes the following topics:

- “Credentials for Logging In To the SDDC Manager (vrm) Virtual Machine,” on page 22
- “Look Up Account Credentials Using the Lookup-Password Command,” on page 23
- “Rotate All Passwords On-Demand for the Managed Physical and Logical Entities,” on page 24
- “vrm-cli Command Reference,” on page 26

**Credentials for Logging In To the SDDC Manager (vrm) Virtual Machine**

To log in to a rack’s SDDC Manager (vrm) virtual machine to perform operations using the vrm-cli tool, you log in using the root account credentials.

When the hardware for a rack is imaged, a randomized password is generated for the root account for that rack’s SDDC Manager virtual machine. That generated password is obtained at the end of the imaging process, as described in the Cloud Foundation VIA User’s Guide.

The "./vrm-cli.sh rotate-all" command does not change the password of the SDDC Manager virtual machine’s root account, and the "./vrm-cli.sh lookup-password" command does not report this password. Therefore, it is strongly recommended that you change the password for the SDDC Manager virtual machine’s root account and for the virtual machine’s vrack service account at the first opportunity to passwords that you can easily keep track of and manage in your organization.

**NOTE** When you change the passwords for the SDDC Manager virtual machine’s root and vrack accounts, they are not retrievable from your Cloud Foundation environment or from the SDDC Manager virtual machine. You must retain the passwords that you set.
Look Up Account Credentials Using the Lookup-Password Command

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 virtual machine using the root account credentials and run the vrm-cli.sh lookup-password command using the vrm-cli tool located in the /home/vrack/bin directory.

Prerequisites

You must have the root account credentials to log in to the SDDC Manager VM and run the vrm-cli.sh lookup-password command. See “Credentials for Logging In To the SDDC Manager (vrm) Virtual Machine,” on page 22.

Procedure

1. Using the root account, connect and log in, for example by SSH, to the SDDC Manager VM.
2. Change to the /home/vrack/bin directory.
3. Stop the vrm-watchdogserver and vrm-tcserver services.
   
   service vrm-watchdogserver stop
   service vrm-tcserver stop

   **Note** Even though the ./vrm-cli.sh lookup-password command can run without stopping the services, it is a best practice to stop the services before running any vrm-cli.sh command.

4. Obtain the account credentials list by typing the command:
   
   ./vrm-cli.sh lookup-password.

   The output displays the account credentials and IP addresses for the physical and logical entities on which the vrm-cli tool operates. The username and password for each account is displayed.

5. (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.

6. If you are not going to run any other vrm-cli.sh commands, restart the vrm-watchdogserver service, which also restarts the vrm-tcserver service.
   
   service vrm-watchdogserver start

   If you are going to run other vrm-cli.sh commands, leave the services stopped until you are finished running those commands and then start them.
Rotate All Passwords On-Demand for the Managed Physical and Logical Entities

On each rack in turn, you run the ./vrm-cli.sh rotate-all command in each rack's SDDC Manager virtual machine to rotate all of the passwords that are managed by SDDC Manager.

First run the ./vrm-cli.sh rotate-all command on the primary rack. After running it on the primary rack, run the ./vrm-cli.sh rotate-all command on the second rack, then on the third rack, and so on. For a description of which rack is the primary rack in the environment, see “About the Primary Rack and the SDDC Manager Virtual IP Address,” on page 11.

Note Before running any vrm-cli.sh command, it is a best practice to stop both the vrm-watchdogserver and vrm-tcserver services in the SDDC Manager VM. However, if you omit explicitly stopping these services prior to running the ./vrm-cli.sh rotate-all command, the command will attempt to stop the services automatically before it starts the rotation process. Then, at the end of the rotation process, if the command has automatically stopped the services, it will attempt to restart the vrm-watchdogserver service, which also restarts the vrm-tcserver service.

Prerequisites
Verify the following prerequisites are met:

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

- No active workflows, such as creating or deleting workload domains, are running or are expected to run during the password rotation process. Schedule a window of time when you expect to have no running workflows before performing on-demand password rotation.

- You have the root account credentials to log in to each rack's SDDC Manager VM. For details, see “Credentials for Logging In To the SDDC Manager (vrm) Virtual Machine,” on page 22.

Procedure

1. For the primary rack, using the root account, connect and log in, for example by SSH, to the rack’s SDDC Manager VM.

2. Change to the /home/vrack/VMware/vRack directory.

3. Save a copy of the /home/vrack/VMware/vRack/vrm.properties file to a secure location where you can access it later if necessary.

4. Change to the /home/vrack/bin directory.

5. Stop the vrm-watchdogserver and vrm-tcserver services.
   ```
   service vrm-watchdogserver stop
   service vrm-tcserver stop
   ```
   Note Even though the ./vrm-cli.sh lookup-password command can run without stopping the services, it is a best practice to stop both services before running any vrm-cli.sh command.

6. At the prompt, use the vrm-cli tool's lookup-password command to obtain the listing of the current account credentials so that you can compare it to the post-rotated listing.
   ```
   ./vrm-cli.sh lookup-password
   ```
   The output displays the account credentials and IP addresses for the physical and logical entities that are managed by the vrm-cli tool. The username and password for each account is displayed.
7 Save the output to a secure location.

8 Rotate this rack's passwords by typing the following command
   
   `/vrm-cli.sh rotate-all`
   
   This command changes the passwords of the physical and logical components on the rack. Because this first run is performed on the primary rack, this step also changes the passwords of entities used across the racks.

   **Note** The rotate-all command does not change the IPMI passwords.

9 To rotate the IPMI passwords, run the command `/vrm-cli.sh rotate-ipmi`

10 Obtain the listing of the updated account credentials and save a copy.

   `/vrm-cli.sh lookup-password`

11 Compare the output file you saved prior to rotation with the output file you saved now and verify that all passwords are changed.

12 Restart the vrm-watchdogserver service, which also restarts the vrm-tcserver service.

   `service vrm-watchdogserver start`

13 For the next physical rack, using the root account, connect and log in, for example by SSH, to the rack's SDDC Manager VM.

14 Stop the vrm-watchdogserver and vrm-tcserver services:

   `service vrm-watchdogserver stop`
   `service vrm-tcserver stop`

15 Change to the `/home/vrack/VMware/vRack` directory.

16 Save a copy of the `/home/vrack/VMware/vRack/vrm.properties` file to a secure location where you can access it later if necessary.

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

18 At the prompt, use the vrm-cli tool's `lookup-password` command to obtain the listing of the current account credentials.

   `/vrm-cli.sh lookup-password`

   The output displays the account credentials and IP addresses for the physical and logical entities that are managed by the vrm-cli tool. The username and password for each account is displayed.

19 Save the output to a secure location so that you can compare it to the post-rotated listing.

20 Rotate this rack's passwords by typing the following command

   `/vrm-cli.sh rotate-all`

   This command changes the passwords of the physical and logical components local to this rack.

21 To rotate the IPMI passwords, run the command `/vrm-cli.sh rotate-ipmi`

   `/vrm-cli.sh rotate-password-ipmi`

22 Obtain the listing of the updated account credentials and save a copy.

   `/vrm-cli.sh lookup-password`
23  Compare the output file you saved prior to rotation with the output file you saved now and verify that all passwords are changed.

24  Restart the vrm-watchdogserver service, which also restarts the vrm-tcservice server.

        service vrm-watchdogserver start

25  Repeat the steps to rotate the passwords for each physical rack in your installation.

vrm-cli Command Reference

The vrm-cli tool is a command-line utility to perform tasks primarily related to looking up and rotating passwords and syncing properties between racks. You can also perform some configuration tasks using this tool.

The vrm-cli tool is located in /home/vrack/bin in the SDDC Manager virtual machine’s file system. Only the root account can run the vrm-cli tool. To run a command, change to the /home/vrack/bin directory and type ./vrm-cli.sh followed by the command.

./vrm-cli.sh <command>

To list the available vrm-cli tool commands, use the following command.

./vrm-cli.sh help

**Important** You should stop the vrm-watchdogserver and vrm-tcservice server services before running these commands. Even though some of the vrm-cli tool’s commands can run without you explicitly stopping the services, it is a best practice to stop both services before running any vrm-cli.sh command. Then when you are done running the commands, restart the vrm-watchdogserver service, which will also restart the vrm-tcservice service.

rack-1-vrm-1:/home/vrack/bin # service vrm-watchdogserver stop
Stopping watchdog
rack-1-vrm-1:/home/vrack/bin # service vrm-tcservice stop
Instance is running as PID=21972, shutting down...
Instance is running PID=21972, sleeping for up to 10 seconds waiting for shutdown
Instance shut down gracefully
rack-1-vrm-1:/home/vrack/bin # ./vrm-cli.sh
all credentials for all hosts:
...
...
rack-1-vrm-1:/home/vrack/bin # service vrm-watchdogserver start
Starting watchdog
Successfully started watchdog.

Lookup Commands

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

**Table 3.1.** vrm-cli Lookup Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommands and Input</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lookup-esxi</td>
<td>None</td>
<td>Lists the IP addresses of the ESXi hosts that are visible in-band to the rack’s HMS agent, for the rack on which the command is run.</td>
</tr>
<tr>
<td>lookup-domains</td>
<td>None</td>
<td>Queries the environment’s logical inventory for the management and workload domains and lists their names.</td>
</tr>
</tbody>
</table>

26  VMware, Inc.
Table 3-1. vrm-cli Lookup Commands (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommands and Input</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lookup-history</td>
<td>store</td>
<td>Manages and retrieves the password history recorded in Zookeeper. .:/vrm-cli.sh lookup-history store records the local rack’s current password state into Zookeeper.</td>
</tr>
<tr>
<td></td>
<td>latest</td>
<td>.:/vrm-cli.sh lookup-history latest lists the account information from the most recent history recorded in Zookeeper.</td>
</tr>
<tr>
<td></td>
<td>timestamp yyyy-mm-dd hh:mm:ss</td>
<td>.:/vrm-cli.sh lookup-history timestamp yyyy-mm-dd hh:mm:ss lists the password-rotation history associated with the specified timestamp.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lookup-password</td>
<td>None</td>
<td>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 Using the Lookup-password Command,” on page 23.</td>
</tr>
<tr>
<td>lookup-password-sso</td>
<td>None</td>
<td>Lists the SSO domains, users, and passwords that are managed by the vrm-cli tool.</td>
</tr>
<tr>
<td>lookup-psc</td>
<td>None</td>
<td>Lists information about the Platform Services Controller instances that are visible in the logical inventory.</td>
</tr>
<tr>
<td>lookup-rack</td>
<td>None</td>
<td>Lists the physical racks currently visible in the inventory, by UUID and name.</td>
</tr>
<tr>
<td>lookup-vcenter</td>
<td>None</td>
<td>Lists the IP addresses of the vCenter Server instances that are visible in the inventory.</td>
</tr>
<tr>
<td>lookup-vrm</td>
<td>None</td>
<td>Lists information about the SDDC Manager virtual machines that are visible in the inventory.</td>
</tr>
</tbody>
</table>

Password Rotation, Set Up, and Generation Commands

Use these commands to rotate 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.

**Note** Because some items in your installation’s inventory are managed across all racks in the installation while other inventory items can only be managed from their controlling rack, the command’s behavior is based on whether it is run in the first rack’s SDDC Manager virtual machine or on subsequent racks. In the table, the term visible is used to indicate those inventory items that are visible to the command and to the HMS agent for the SDDC Manager in which the command is run. When run from a specific rack’s SDDC Manager virtual machine, the resources in that rack are the ones visible to the command. See Chapter 3, “On-Demand Password Rotation in Your Cloud Foundation Installation,” on page 21

Table 3-2. vrm-cli Password Rotation, Set Up, and Generation Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommands and Input</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rotate-all</td>
<td>None</td>
<td>Rotates passwords for all inventory items that are visible and safe to automatically rotate, except for the IPMI passwords. The IPMI passwords are rotated using rotate-password-ipmi.</td>
</tr>
<tr>
<td>rotate-password-esx</td>
<td>None</td>
<td>Rotates passwords for the service console accounts for all of the visible ESXi hosts.</td>
</tr>
<tr>
<td>rotate-password-ipmi</td>
<td>None</td>
<td>Rotates IPMI passwords, for all of the visible ESXi hosts.</td>
</tr>
<tr>
<td>rotate-password-isvm</td>
<td>None</td>
<td>Rotates passwords of the visible ISVM virtual appliances.</td>
</tr>
</tbody>
</table>
Table 3-2. vrm-cli Password Rotation, Set Up, and Generation Commands (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommands and Input</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rotate-password-lcm</td>
<td>None</td>
<td>Rotates passwords on resources identified as LCM.</td>
</tr>
<tr>
<td>rotate-password-lcm-backup</td>
<td>None</td>
<td>Rotates passwords on resources identified as LCM-Backup resources.</td>
</tr>
<tr>
<td>rotate-password-li-api</td>
<td>None</td>
<td>Rotates the vRealize Log Insight API password.</td>
</tr>
<tr>
<td>rotate-password-li-ssh</td>
<td>None</td>
<td>Rotates the vRealize Log Insight virtual appliance's console user password.</td>
</tr>
<tr>
<td>rotate-password-nsx</td>
<td>None</td>
<td>Rotates the NSX Manager virtual appliances' SSH password using the NSX Manager REST API.</td>
</tr>
<tr>
<td>rotate-password-nsx-controller</td>
<td>None</td>
<td>Rotates passwords for the visible NSX controllers using the NSX Manager REST API.</td>
</tr>
<tr>
<td>rotate-password-postgres</td>
<td>None</td>
<td>Rotates the password for Postgres.</td>
</tr>
<tr>
<td>rotate-password-psc</td>
<td>None</td>
<td>Rotates passwords for the visible Platform Services Controller appliances.</td>
</tr>
<tr>
<td>rotate-password-sso</td>
<td>host user old-password new-password</td>
<td>Rotates the password for a specified SSO user on a specified Platform Services Controller appliance. If no host and user are specified, then all visible SSO users have their password credentials rotated. You can optionally supply the old password and a new password for a specific user.</td>
</tr>
<tr>
<td>rotate-password-switch</td>
<td>None</td>
<td>Rotates passwords for the visible switches.</td>
</tr>
<tr>
<td>rotate-password-tor-switch</td>
<td>None</td>
<td>Rotates passwords for the visible ToR switches.</td>
</tr>
<tr>
<td>rotate-password-vcenter</td>
<td>None</td>
<td>Rotates passwords for the visible vCenter Server appliances' console user password for the visible virtual appliances.</td>
</tr>
<tr>
<td>rotate-password-vrops-api</td>
<td>None</td>
<td>Rotates the vRealize Operations Manager API password.</td>
</tr>
<tr>
<td>rotate-password-vrops-ssh</td>
<td>None</td>
<td>Rotates the vRealize Operations Manager virtual appliance's console user password.</td>
</tr>
<tr>
<td>setup-password-esx</td>
<td>host-ip current-password</td>
<td>Used by SDDC Manager when you add or replace a server. Manual use of this command is not generally needed.</td>
</tr>
<tr>
<td>generate-password</td>
<td>length</td>
<td>Used by SDDC Manager. Manual use of this command is not generally needed. Generates a password and prints it to the command line. The generated passwords conform to the environment’s password policies.</td>
</tr>
<tr>
<td>decrypt</td>
<td>encrypted-text</td>
<td>Decrypts the input text and prints the output to the command line. Primarily used by SDDC Manager. Manual use of this command is not generally needed.</td>
</tr>
<tr>
<td>encrypt</td>
<td>plain-text</td>
<td>Encrypts the input text and prints the output to the command line.</td>
</tr>
</tbody>
</table>

**Configuration-Related Commands**

Use these commands for special configuration operations.
Table 3-3. vrm-cli Configuration-Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommands and Input</th>
<th>Description</th>
</tr>
</thead>
</table>
| configure-snmp    | full-path-to-input-json-file           | Configures use of an external SNMP management server for the ToR and spine switches for the rack in which the command is run. With this command, you can use your existing network monitoring tools to monitor the switches on a rack using SNMP. Each rack in your installation has two ToR switches. Additionally, the second rack in a multirack installation has the two spine switches for the installation. SNMP v3 provides secure communication between the switches and your SNMP management server.

The input to this command is the full absolute path to a JSON file, including the file name. In the JSON file, the required JSON input is

```json
{
  "enabled": true,  # if enabled is true, turn on SNMP on switches; if enabled is false or omitted, disable SNMP on switches
  "serverIp": "nnn.nnn.nnn.nnn",  # SNMP server IP address or hostname
  "serverPort": nnn,  # (optional) SNMP server port (default = 162)
  "users": [
    # User accounts SDDC Manager uses to connect to the SNMP server
    {
      "username": "snmpuser1",
      "authType": "SHA",  # (optional) either SHA or MD5
      "authPassword": "auth password",  # (optional) Passphrase for authentication
      "privType": "AES",  # (optional) either AES or DES
      "privPassword": "priv password"  # (optional) Passphrase for privacy
    }
  ]
}
```

Where:

- `serverIP` is your SNMP management server’s IP address or host name
- `serverPort` is that server’s SNMP port. If not specified, port 162 is used as the default.
- Specified users that are used for the connection to your SNMP management server, as configured in its management software.

To disable SNMP on the switches, set "enabled": false in the JSON, or omit the "enabled" line.

You must provide the full path to the JSON file, even if the JSON file resides in the same /home/vrack/bin directory from which you are running the `./vrm-cli.sh configure-snmp` command.
<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommands and Input</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure-syslog</td>
<td>None</td>
<td>Configures syslog on the switches for the rack in which the command is run. See “Configure Syslog from the Switches to vRealize Log Insight,” on page 96.</td>
</tr>
<tr>
<td>sync-properties</td>
<td>None</td>
<td>Syncs properties between the primary rack and a new rack that you are adding to the environment. See the VMware Cloud Foundation Overview and Bring-Up Guide for details about running the command when adding a new rack. See “About the Primary Rack and the SDDC Manager Virtual IP Address,” on page 11 for the definition of the primary rack.</td>
</tr>
</tbody>
</table>

As an example, if you copy a JSON file named enablesnmp.json into the VRM VM's /home/vrack/bin directory where the vrm-cli.sh file is located, log in to the VRM VM, change directories to home/vrack/bin, then to perform the configure SNMP operation, you type: 

```
./vrm-cli.sh configure-snmp /home/vrack/bin/enablesnmp.json
```
Managing Users and Groups

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

For an overview of the User Management page, see “Tour of the SDDC Manager User Interface,” on page 14.

Authentication to the SDDC Manager client 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 installation. 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 the SDDC Manager client.

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 Environment,” on page 31
- “Add Local Users and Groups,” on page 35
- “Assign Permissions to Users and Groups,” on page 37
- “Add System Administrators,” on page 37
- “Role-Based Access Control,” on page 38
- “User Passwords in Your Cloud Foundation Environment,” on page 38

Active Directory and the Cloud Foundation Environment

To allow the users and groups in your Microsoft Active Directory domain to use their Active Directory credentials to log in to the SDDC Manager client as well as the vCenter Server instances that are deployed in your Cloud Foundation environment, you configure your Microsoft 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 environment’s initial bring-up process, you enter your root domain, domain name server (DNS) subdomain, and Platform Services Controller 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 administrator@vsphere.local account that is generated by the bring-up process, 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 client by assigning roles provided by the SDDC Manager role-based access control capabilities. See “Assign Permissions to Users and Groups,” on page 37 and “Role-Based Access Control,” on page 38.
- 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 Installation,” on page 34.

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

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 client and access the environment, as well as grant permissions to log in to the vSphere Web Client using their Active Directory credentials.

**Prerequisites**

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

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 client, 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Active Directory domain name, for example, example.com. Do not provide an IP address in this field.</td>
</tr>
</tbody>
</table>
| 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.


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 client to grant the appropriate permissions to the Active Directory domain's users and groups for accessing your environment using their Active Directory credentials. See “Assign Permissions to Users and Groups,” on page 37.

- 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 Installation**

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.

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 Environment,” on page 32.

**Procedure**

1. Open the view of the management domain's vCenter Server resources in the vSphere Web Client.
   a. In the SDDC Manager client, 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 the SDDC Manager client, 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 installation.

Prerequisites

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

1 Open the view of the management domain’s vCenter Server resources in the vSphere Web Client.
   a In the SDDC Manager client, 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a local user</td>
<td>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. The password must meet the password policy requirements for the software stack. <strong>IMPORTANT</strong> Because you cannot change the user name after you create a user, make sure the user name is typed in correctly before clicking OK.</td>
</tr>
<tr>
<td>Add a local group</td>
<td>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. <strong>IMPORTANT</strong> Because you cannot change the group name after you create a group, make sure the name is typed in correctly before clicking OK.</td>
</tr>
</tbody>
</table>

What to do next

When you add a user, that user initially has no privileges to perform management operations in your installation. 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 installation. Then use the User Management page in the SDDC Manager client to assign a role to that group.
Use the User Management page to authorize the local user for performing operations in your installation by assigning an appropriate role to that user. See “Assign Permissions to Users and Groups,” on page 37.

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 the SDDC Manager client.

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 client. See “Active Directory and the Cloud Foundation Environment,” on page 31, “Configure an Active Directory Domain as an Identity Source for your Cloud Foundation Environment,” on page 32, and “Add Local Users and Groups,” on page 35.

Procedure

1. In the SDDC Manager client, 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 client. 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 installation 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 the SDDC Manager client.
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 client. See “Active Directory and the Cloud Foundation Environment,” on page 31, “Configure an Active Directory Domain as an Identity Source for your Cloud Foundation Environment,” on page 32, and “Add Local Users and Groups,” on page 35.

Procedure

1. In the SDDC Manager client, 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 the SDDC Manager client and perform system administrator operations.

Role-Based Access Control

SDDC Manager uses roles and rights to determine what operations a user can perform using the SDDC Manager client. 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 client 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 Environment

The password restrictions, lockout, and expiration for a user’s password in your Cloud Foundation environment 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 the SDDC Manager client and various other SDDC components’ Web interfaces that you use to perform administrative tasks in your SDDC, such as the vSphere Web Client and the vRealize Operations Manager Web interfaces.

Local Users

The passwords for users of the installation’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 installation is governed by the vCenter Single Sign-On password policy. The vCenter Single Sign-On password 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 installation’s bring-up process. If you have configured your installation 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.

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

**Note** Password policies apply only to user accounts, not to system accounts in the domain.

**Prerequisites**

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

**Procedure**

1. Open the view of the management domain’s vCenter Server resources in the vSphere Web Client.
   a. In the SDDC Manager client, 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.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum lifetime</td>
<td>Password must be changed every 90 days</td>
</tr>
<tr>
<td>Restrict re-use</td>
<td>Users cannot reuse any previous 5 passwords</td>
</tr>
<tr>
<td>Maximum length</td>
<td>20</td>
</tr>
<tr>
<td>Minimum length</td>
<td>8</td>
</tr>
<tr>
<td>Character requirements</td>
<td>■ At least 1 special character</td>
</tr>
<tr>
<td></td>
<td>■ At least 2 alphabetic characters</td>
</tr>
<tr>
<td></td>
<td>■ At least 1 uppercase character</td>
</tr>
<tr>
<td></td>
<td>■ At least 1 lowercase character</td>
</tr>
<tr>
<td></td>
<td>■ At least 1 numeric character</td>
</tr>
<tr>
<td></td>
<td>■ Identical adjacent characters: 3</td>
</tr>
</tbody>
</table>

3 Click Edit.

4 Edit the password policy parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Password policy description.</td>
</tr>
<tr>
<td>Maximum lifetime</td>
<td>Maximum number of days that a password can exist before the user must change it.</td>
</tr>
<tr>
<td>Restrict reuse</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum length</td>
<td>Maximum number of characters that are allowed in the password.</td>
</tr>
<tr>
<td>Minimum length</td>
<td>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.</td>
</tr>
<tr>
<td>Character requirements</td>
<td>Minimum number of different character types that are required in the password. You can specify the number of each type of character:</td>
</tr>
<tr>
<td></td>
<td>■ Special characters, such as &amp; # %</td>
</tr>
<tr>
<td></td>
<td>■ Alphabetic characters, such as A b c D</td>
</tr>
<tr>
<td></td>
<td>■ Uppercase characters, such as A B C</td>
</tr>
<tr>
<td></td>
<td>■ Lowercase characters, such as a b c</td>
</tr>
<tr>
<td></td>
<td>■ Numeric characters, such as 1 2 3</td>
</tr>
<tr>
<td></td>
<td>The minimum number of alphabetic characters must be no less than the combined uppercase and lowercase requirements.</td>
</tr>
<tr>
<td>Identical adjacent characters</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 installation.

The Dashboard page displays high-level information about your installation'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 installation. 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,” on page 42
- “ESXi Host Details and Operations,” on page 42

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.

<table>
<thead>
<tr>
<th>Status Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑</td>
<td>The resource has no SDDC Manager alerts reported of warning, error, or critical severity.</td>
</tr>
<tr>
<td>🔴</td>
<td>The resource has SDDC Manager alerts reported with warning severity.</td>
</tr>
<tr>
<td>🔴</td>
<td>The resource has SDDC Manager alerts reported with error severity.</td>
</tr>
<tr>
<td>🔴</td>
<td>The resource has SDDC Manager alerts reported with critical severity.</td>
</tr>
<tr>
<td>🔴</td>
<td>The resource's health state cannot be determined, for example the resource is powered off.</td>
</tr>
</tbody>
</table>

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,” on page 87
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 spine switch. By clicking a switch's name, you can drill down to see that switch's detailed information.

**Note**  Spine switches are available in an installation that has two or more racks. Spine switches are installed when a second rack is added to the first rack in an installation.

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.
Working with Management Domains and Workload Domains

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

By default, the management and workload domains include these VMware capabilities:

**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 in the vSphere Documentation Center located at http://pubs.vmware.com/vsphere-60/index.jsp.

**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, DRS automatically allocates additional resources by redistributing virtual machines among the physical servers in the resource pool. For more information about DRS, see the vSphere Resource Management documentation in the vSphere Documentation Center located at http://pubs.vmware.com/vsphere-60/index.jsp.

**VMware Virtual SAN™**

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 Virtual SAN, see the VMware Virtual SAN documentation in the vSphere Documentation Center located at http://pubs.vmware.com/vsphere-60/index.jsp.
By default, each physical rack has a management domain to manage the hosts in that rack. The management domain is automatically provisioned on each physical rack using some of the rack’s ESXi hosts when the rack is configured by the bring-up process. The bring-up process chooses the appropriate number of hosts required to accommodate redundancy capabilities and VMware SDDC best practices. When the bring-up process deploys a management domain, it automatically provisions and configures the management domain with the Cloud Foundation software stack. For more information about the management domain, see the VMware Cloud Foundation Overview and Bring-Up Guide.

The two pre-packaged environments you can deploy are named Virtual Infrastructure (VI) and Virtual Desktop Infrastructure (VDI). To deploy one of these pre-packaged 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

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 Virtual SAN 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 installation. 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.

This chapter includes the following topics:

- “Creating and Provisioning Workload Domains,” on page 45
- “Utilize Capacity on Management Domain,” on page 67
- “Expanding Management and Workload Domains,” on page 68
- “Delete a Workload Domain,” on page 70
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).

Create a Virtual Infrastructure Workload Domain

You create a Virtual Infrastructure (VI) workload domain using the SDDC Manager client. 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

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 installation’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, Virtual SAN, 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 the Networking Information for the Virtual Infrastructure Workload Domain,” on page 49.

Procedure

1. **Start the Wizard to Create a VI Workload Domain** on page 46
   You start the Configure VI wizard from the Dashboard page of the SDDC Manager client.

2. **Specify General Information about the VI Workload Domain** on page 47
   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 the Performance and Availability Levels for the Virtual Infrastructure Workload Domain** on page 47
   At the Workload step of the creation wizard, you specify the levels of performance, availability, and hardware capacities you want provisioned for this VI workload domain.

4. **Specify the Networking Information for the Virtual Infrastructure Workload Domain** on page 49
   Specify the networking information for the VI workload domain.

5. **Review the Details and Start the Creation Workflow** on page 51
   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 52 section of “Review the Details and Start the Creation Workflow,” on page 51.

**Start the Wizard to Create a VI Workload Domain**

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

**Prerequisites**

Verify that you have met the prerequisites described in “Create a Virtual Infrastructure Workload Domain,” on page 45.

**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 the Performance and Availability Levels for the Virtual Infrastructure Workload Domain

At the Workload step of the creation wizard, you specify the levels of performance, availability, and hardware capacities you want provisioned for this VI workload domain.

Based on your selections, SDDC Manager will determine:

- The 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
Procedure

1. Specify the performance level.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>With this choice, the following Virtual SAN parameters are used:</td>
</tr>
<tr>
<td></td>
<td>- Number of disk stripes per object: 1</td>
</tr>
<tr>
<td></td>
<td>- Flash read cache reservation: 0%</td>
</tr>
<tr>
<td></td>
<td>- Force provisioning (in spite of non-compliance): False</td>
</tr>
<tr>
<td></td>
<td>- Object space reservation: 40%</td>
</tr>
<tr>
<td>Balanced</td>
<td>With this choice, the following Virtual SAN parameters are used:</td>
</tr>
<tr>
<td></td>
<td>- Number of disk stripes per object: 1</td>
</tr>
<tr>
<td></td>
<td>- Flash read cache reservation: 0%</td>
</tr>
<tr>
<td></td>
<td>- Force provisioning (in spite of non-compliance): False</td>
</tr>
<tr>
<td></td>
<td>- Object space reservation: 70%</td>
</tr>
<tr>
<td>High</td>
<td>With this choice, the following Virtual SAN parameters are used:</td>
</tr>
<tr>
<td></td>
<td>- Number of disk stripes per object: 4</td>
</tr>
<tr>
<td></td>
<td>- Flash read cache reservation: 0%</td>
</tr>
<tr>
<td></td>
<td>- Force provisioning (in spite of non-compliance): False</td>
</tr>
<tr>
<td></td>
<td>- Object space reservation: 100%</td>
</tr>
</tbody>
</table>

2. 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>With this choice, the following Virtual SAN parameters are used:</td>
</tr>
<tr>
<td></td>
<td>- Number of failures to tolerate: zero (0).</td>
</tr>
<tr>
<td></td>
<td>Because Virtual SAN requires a minimum of three hosts by default, three hosts are assigned to the virtual infrastructure.</td>
</tr>
<tr>
<td>Normal</td>
<td>With this choice, the following Virtual SAN parameters are used:</td>
</tr>
<tr>
<td></td>
<td>- Number of failures to tolerate: one (1).</td>
</tr>
<tr>
<td></td>
<td>Because Virtual SAN requires a minimum of three hosts by default, three hosts are assigned to the virtual infrastructure.</td>
</tr>
<tr>
<td>High</td>
<td>With this choice, the following Virtual SAN parameters are used:</td>
</tr>
<tr>
<td></td>
<td>- Number of failures to tolerate: two (2).</td>
</tr>
<tr>
<td></td>
<td>Because Virtual SAN requires a minimum of five hosts by default for this setting, five hosts are assigned to the virtual infrastructure.</td>
</tr>
</tbody>
</table>

3. Type capacities for the CPU, memory, and storage for the resource pool that will be created and assigned to this virtual environment.

4. Proceed to the next step by clicking Next.
Specify the Networking Information for the Virtual Infrastructure 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 installation's bring-up process. During deployment of the VI workload domain's infrastructure, the workflow also configures the networks used by the vMotion, Virtual SAN, 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 installation's bring-up process for that subnet. See “About Excluding IP Address from SDDC Manager Use,” on page 104.

### Table 6-1. VI Workload Domain Network Configurations

<table>
<thead>
<tr>
<th>Network Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>By default, the workload domain's management network configuration uses the management network that was configured during the bring-up process.</td>
</tr>
<tr>
<td>vMotion</td>
<td>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.</td>
</tr>
<tr>
<td>Virtual SAN</td>
<td>When you select to use the defaults, the workload domain's Virtual SAN configuration uses a portion of the Virtual SAN network configuration that was configured during the bring-up process and allocates a VLAN ID from its pool. If you choose to use this default, but the software detects inadequate IP address space in the existing Virtual SAN network, you must specify a new configuration at that step in the wizard.</td>
</tr>
<tr>
<td>VXLAN</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Data Center connection| Used for access from outside this Cloud Foundation installation to the workloads that you run in the workload domain. At this wizard step, you can:  
  - Select the network configuration that was configured during the bring-up process.  
  - Select a new network configuration that was configured in advance using the Data Center Connections settings screen.  
  - Enter a new configuration. A VLAN ID is required.  
  **IMPORTANT** Do not select a data center connection that is already associated with a VDI workload domain or unexpected results might occur. |

### Prerequisites

Verify that you have met the networking prerequisites as described in “Create a Virtual Infrastructure Workload Domain,” on page 45.

**IMPORTANT** If you enter custom network configurations for the vMotion, Virtual SAN, 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, Virtual SAN, 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 8**.

   - 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 installation'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,” on page 104.

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 installation's bring-up process, make sure the **USE DEFAULTS** check box is checked and proceed to the Virtual SAN 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 Virtual SAN network configuration. A minimum subnet mask of /22 is recommended.

   **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 Virtual SAN network configuration.
6 For the Virtual SAN network configuration, choose one of these options.

- To use the same Virtual SAN network configuration that was specified during your installation's bring-up process, check the USE DEFAULTS check box and proceed to the VXLAN network configuration.
- To specify a custom Virtual SAN network for this workload domain, clear the USE DEFAULTS check box if it is selected, type the Virtual SAN network settings, and then proceed to the VXLAN network configuration. A minimum subnet mask of /22 is recommended.

**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 installation's bring-up process. See “About Excluding IP Address from SDDC Manager Use,” on page 104.

7 For the VXLAN network configuration, choose one of these options.

- To use the same VXLAN network configuration that was specified during your installation’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 and then proceed to the Data Center network configuration. A minimum subnet mask of /22 is recommended.

8 (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 Centers screen.
- 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.

9 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.
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,” on page 52.

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.

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 http://pubs.vmware.com/vsphere-60/topic/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://www.vmware.com/support/pubs/nsx_pubs.html.
Create a VDI Workload Domain

You create a VDI workload domain using the SDDC Manager client. When you create a VDI workload domain, the SDDC Manager deploys the components from the VMware Horizon 6 product that are necessary for the VDI infrastructure to deliver network-based virtual desktops, based on your specifications.

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 VDI 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,” on page 45. 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.

- 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,” on page 56.
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,” on page 56.

In the VDI workload domain creation wizard, you are prompted to enter networking information for a data center network or you can select preconfigured 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 installation and the environment external to the installation. 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 installation. Your Data Center Network administrator must also ensure that this Cloud Foundation installation’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 installation’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 client. 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,” on page 105.

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 installation 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 Horizon 6 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 Horizon 6 version 6.2 documentation at http://pubs.vmware.com/horizon-62-view/topic/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** on page 56
   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** on page 60
   You start the Configure VDI wizard from the Dashboard page of the SDDC Manager client.

3. **Specify the General Configuration Information for the VDI Workload Domain** on page 60
   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 the Active Directory Information Required for a VDI Environment** on page 61
   In the General Configuration: Active Directory step of the creation 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** on page 63
   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.

6. **Specify the Networking Information for the VDI Workload Domain** on page 63
   In this step, you must specify the data center network that will be used for the actual desktop pools to which end users connect.
7 Specify the Windows Images for the VDI Environment on page 64

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.

8 Review the Details and Start the Creation Workflow on page 65

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.

9 Post-Deployment Tasks After Your VDI Workload Domain is Created on page 66

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,” on page 66, 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 Horizon 6 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 Horizon 6 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 View, as documented in the Optimization Guide for Desktops and Servers in View in VMware Horizon 6 and VMware Horizon Air Desktops and VMware Horizon Air Apps 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.

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 Fling that you can download. The Optimization Guide for Desktops and Servers in View in VMware Horizon 6 and VMware Horizon Air Desktops and VMware Horizon Air Apps 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 6.0 hosts. For information about virtual machine hardware versions that can run on ESXi 6.0 hosts, see the Virtual Machine Hardware Versions topic in the vSphere 6.0 Documentation Center at http://pubs.vmware.com/vsphere-60/topic/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 environment, 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 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.


**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, follow the steps documented in the Horizon 6 product documentation's Creating Virtual Machines for Remote Desktop Deployment topic located at http://pubs.vmware.com/horizon-62-view/topic/com.vmware.horizon-view.desktops.doc/GUID-B5020738-8649-4308-A8B0-70AF80527DF6.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:


- **Reviewers Guide for View in Horizon 6** white paper
- **Optimization Guide for Desktops and Servers in View in VMware Horizon 6 and VMware Horizon Air Desktops and VMware Horizon Air Apps** 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 client.

**Prerequisites**

Verify that you have met the prerequisites described in “Create a VDI Workload Domain,” on page 53.

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserve resources</td>
<td>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.</td>
</tr>
<tr>
<td>Deploy Desktops</td>
<td>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.</td>
</tr>
</tbody>
</table>

3 Select the persistence type for the desktop pools, linked clone or full clone.

As defined in the official VMware Technical Publications Glossary at https://www.vmware.com/pdf/master_glossary.pdf:

- A clone is a duplicate of a virtual machine.
- A linked clone is a copy of the original virtual machine, the parent. The copy must have access to the parent virtual machine’s virtual disks. The linked clone stores changes to the virtual disks in a separate set of files.
- A full clone is a complete copy of the original virtual machine, including all associated virtual disks.

4 Select the type of desktop access that you want the VDI environment to support.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Network</td>
<td>This choice provides access to the virtual desktops from within the customer’s network only.</td>
</tr>
<tr>
<td>Connect from Anywhere</td>
<td>This choice provides access to the virtual desktops from both within the customer’s network and from the Internet.</td>
</tr>
</tbody>
</table>

5 Proceed to the next step by clicking Next.

**Specify the Active Directory Information Required for a VDI Environment**

In the General Configuration: Active Directory step of the creation 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 VDI Workload Domain,” on page 53 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 one as part of the VDI environment.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| External | When you select this choice, you must provide the following information:  
- 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 the Virtual Desktop Location field, the organizational unit (OU) to use for the virtual desktops. This OU must already exist in your Active Directory.  
- In the View Servers Location field, the Organizational Unit (OU) in your Active Directory which the Horizon 6 environment will use for its View servers, View Connection and View Composer servers. This OU must already exist in your Active Directory.  
- In the Read-Write Account field, 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 the Horizon View Service Account field, the account credentials, 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 Horizon 6 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 Horizon 6 environment.  
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.  
When you use the External 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. |
| Internal  | When you select this choice, the workflow creates an Active Directory server internally in the VDI environment and configures it with the necessary domain name, IP address, and OU information appropriate for the VDI workload domain.  
Type the IP address of your corporate or enterprise DNS server that this internal Active Directory domain can use to resolve your domain information.  
Type a password for the domain administrator account that will be created for the domain. |

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.

Prerequisites

If you plan to use App Volumes in this VDI environment, verify that you have met the related prerequisites described in “Create a VDI Workload Domain,” on page 53.

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.
2. On the Virtual Desktops - Size step, type the number of virtual desktops that this workload domain will handle.
3. Type the amounts of CPU, RAM, and storage to configure for each desktop.
4. Proceed to the next step by clicking Next.

Specify the 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 VDI Workload Domain,” on page 53. 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 VDI Workload Domain,” on page 53.

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,” on page 56.

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 VDI Workload Domain,” on page 53 and “Prepare the OVA for the Virtual Desktops,” on page 56.

### 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 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,” on page 66.
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 6-2. Post-Deployment Tasks**

<table>
<thead>
<tr>
<th>Creation Wizard Settings</th>
<th>Post-Deployment Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Launch the View Administrator Web interface using the connection information located in the workload domain’s details page. Use the <strong>View Details</strong> button on the Dashboard page to navigate to the workload domain's details page.</td>
</tr>
<tr>
<td>All</td>
<td>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,” on page 94.</td>
</tr>
<tr>
<td>Active Directory Internal option</td>
<td>You must log in to the created Active Directory using the Active Directory administrator account and add members to the AppVolumesAdmins group. 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.</td>
</tr>
<tr>
<td>Implement App Volumes</td>
<td>You must log in to the created Active Directory using the Active Directory administrator account and add members to the AppVolumesAdmins group. 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.</td>
</tr>
</tbody>
</table>
Table 6-2. Post-Deployment Tasks (Continued)

<table>
<thead>
<tr>
<th>Creation Wizard Settings</th>
<th>Post-Deployment Tasks</th>
</tr>
</thead>
</table>
| ■ Active Directory Internal option
■ Full clones             | 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. 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. |

■ Implement App Volumes option
■ Active Directory External option
■ Your Active Directory domain is configured to provide secure LDAP connections (LDAPS) | 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.  
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. |

Utilize Capacity on Management Domain

Cloud Foundation configures the first four hosts on each physical rack as the management domain. You need at least three additional hosts in order to create a workload domain. If you do not have enough hosts to create a workload domain, you can utilize part of the capacity on the management domain by creating a workload VM and adding it to the management domain. In order to isolate the Cloud Foundation management VMs and the workload VMs, it is recommended that you create a resource pool for the workload VMs.

Procedure

1 Login to the vSphere Web Client.
2 Create a resource pool of the hosts in the management domain.  
   See Create a Resource Pool in vSphere Resource Management.
3 Create a workload VM.  
   See Create a New Virtual Machine in vSphere Resource Management.
   **NOTE** Do not move any of the Cloud Foundation management VMs into the resource pool.
4 Move the workload VM to the resource pool.  
   See Add a Virtual Machine to a Resource Pool in vSphere Resource Management.
   **NOTE** Do not move any of the Cloud Foundation management VMs to the newly created resource pool.
Expanding 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.

Expand a Management Domain

To increase the physical resources that are associated with a management domain, you can expand that management domain.

Each physical rack in your Cloud Foundation installation has a management domain. When a management domain is expanded, the expansion process uses hosts that reside in the same physical rack in which that management domain resides.

You expand a management domain from its details page.

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. At the Resources step, specify the resources to add to the management domain.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Expand Method - By Capacity</strong></td>
<td>Type the amount of CPU, memory, and storage capacity to add to the management domain.</td>
</tr>
</tbody>
</table>

4. Proceed to the next step by clicking **Next**.
5. 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 expansion process will add to the management domain to accommodate the requested capacity and the physical rack details for those hosts.

   **Note**  
   When expanding a management domain, the expansion process considers hosts only from the same physical rack in which that management domain resides.

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.

Expand a VI Workload Domain

To increase the physical resources that are associated with a Virtual Infrastructure workload domain, you can expand the workload domain.

You expand a workload domain from its details page.

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 At the Resources step, specify the resources to add to the workload domain.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand Method - By Capacity</td>
<td>Type the amount of CPU, memory, and storage capacity to add to the workload domain.</td>
</tr>
</tbody>
</table>

4 Proceed to the next step by clicking Next.

5 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.

### Expand a VDI Workload Domain

To add more virtual desktops to a VDI workload domain, you expand the workload domain.

You expand a workload domain from its details page.

**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 expansion wizard opens.

3 On the General Configuration: Topology step, click Next.

   This step displays the current settings for this workload domain. The settings are read-only because they cannot be changed using the expansion wizard.

4 On the General Configuration: Active Directory step, type the administrative account’s password and then click Next.

5 At the Virtual Desktops: Management step, click Next.

   This step displays the current settings for this workload domain. The settings are read-only because they cannot be changed using the expansion wizard.

6 At the Virtual Desktops: Size step, 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 At the Review step, 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.
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 environment.

**CAUTION** Deleting a workload domain is a destructive and irreversible operation. All VMs within the workload domain are deleted and the underlying Virtual SAN 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 and drill-down to the details about the workflow.

### Enabling vSAN Space Efficiency Features in All-Flash Installations

Your Cloud Foundation installation 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 http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.virtualsan.doc/GUID-0D43429F-E2E7-4647-8ECA-8F606E9E910F.html. Specific topics about these features include:

- Using Deduplication and Compression topic:
- Deduplication and Compression Design Considerations topic:
- Using RAID 5 or RAID 6 Erasure Coding topic:
  http://pubs.vmware.com/vsphere-60/topic/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 Virtual SAN environments having four or more fault domains. You can configure RAID 5 or RAID 6 on all-flash Virtual SAN environments having six or more fault domains.
- RAID 5 or RAID 6 Design Considerations:
- The Edit Virtual SAN Settings topic includes the detailed steps for enabling deduplication and compression:

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 Virtual SAN settings using the Manage tab and the general settings for Virtual SAN. Set the **Add disks to storage** to **Manual** to access the deduplication and compression setting.

   When you save your edits in the Virtual SAN settings to enable deduplication and compression, Virtual SAN will automatically upgrade the on-disk format, causing a rolling reformat of every disk group in the Virtual SAN 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 Virtual SAN 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 Virtual SAN 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.
Manually Update the Credentials for the vRealize Operations for Horizon Broker Agent When Account Credentials Change for the Connection Server Administrator Account

Whenever you update the account credentials for the Administrator account used for the VDI environment’s View Connection Server hosts, you must manually update the pairing of credentials between the Connection Server instances with the Horizon broker agents used by the vRealize Operations Manager instance in your environment.

When you create a VDI workload domain, the workflow configures the VDI environment to use the features of vRealize Operations® for Horizon® to collect performance data from the VDI environment. If licensed for use in your environment, that data is provided in the vRealize Operations Manager instance in the environment. One of the configured elements is the vRealize Operations for Horizon broker agent. This broker agent is a Windows service that runs on the View Connection Server hosts, collecting inventory information about the VDI environment and sending that information to vRealize Operations Manager.

When the workflow installs the broker agent, credentials are paired between the broker agent and the account credentials set up for the Horizon Administrator account when the workflow creates the Windows Server VMs and installs the Connection Servers into those VMs. When you change the account’s password, you must update those credentials in the broker agent settings.

For in-depth information about the connection between vRealize Operations Manager and VDI environments, see the vRealize Operations for Horizon product documentation at http://pubs.vmware.com/v4h62/index.jsp.

Prerequisites

Verify that you have the Administrator account credentials to log in to the VDI environment's Connection Server virtual machines. If this VDI environment was created using an internal Active Directory domain, the account uses the password that was specified in the Domain Admin Password fields. If this VDI environment was created using an external Active Directory domain, the account uses the password that was entered for the System Administrator field in the VDI workload domain creation wizard. See “Specify the Active Directory Information Required for a VDI Environment,” on page 61.

Verify you have the IP addresses for all of the Connection Server machines used by this VDI workload domain.

Procedure

1. Using the IP address for the first Connection Server machine, remote desktop into its Windows environment and log in using the Administrator account credentials.
2. From the Windows Start menu, select VMware > vRealize Operations Horizon Broker Agent Settings.
3. In the Horizon with View section of the dialog box, type the new password for the account and click Validate Credentials.
4. Click Apply to save your changes.
5. Repeat the steps for each of the VDI environment’s Connection Server machines.
The Cloud Foundation environment 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.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Monitoring Area</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are the systems online?</td>
<td>Operations and incident monitoring</td>
<td>Alerts raised to notify about issues that might require human intervention.</td>
</tr>
<tr>
<td>Why did a storage drive fail?</td>
<td>Troubleshooting</td>
<td>Hardware-centric views spanning inventory, configuration, usage, and event history to provide for diagnosis and resolution.</td>
</tr>
<tr>
<td>Is the infrastructure meeting tenant service level agreements (SLAs)?</td>
<td>Performance management</td>
<td>Analysis of system and device-level metrics to identify causes and resolutions.</td>
</tr>
<tr>
<td>At what future time will the systems get overloaded?</td>
<td>Infrastructure capacity planning</td>
<td>Trend analysis of detailed system and device-level metrics, with summarized periodic reporting</td>
</tr>
<tr>
<td>What person performed which action and when?</td>
<td>Compliance monitoring and auditing</td>
<td>Event history of secured user action, with periodic reporting. Workflow task history of actions performed in the system.</td>
</tr>
</tbody>
</table>

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 the SDDC Manager client
- 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 Environment,” on page 92.

**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.

**vRealize Operations Manager instance deployed by Cloud Foundation**

Use of the vRealize Operations Manager instance deployed by Cloud Foundation is licensed separately. When this deployed vRealize Operations Manager instance is licensed for use in your environment, the management and workload domains’ vCenter Server instances send their event and metric data into the vRealize Operations Manager instance using the vCenter Adapter for vRealize Operations Manager. If you have licensed use of this vRealize Operations Manager instance, you can use the vRealize Operations Manager features to analyze this data based on history for the various virtual resources. See “Using vRealize Operations Manager Capabilities in Your Cloud Foundation Environment,” on page 96.

**Note** The vRealize Operations Manager environment that SDDC Manager deploys is sized for monitoring the contents of your Cloud Foundation installation only. The default sizing accommodates the metrics and events expected to be sent by the Cloud Foundation environment’s vCenter Server instances and Horizon software components. This sizing might not accommodate the numbers of metrics and events for monitoring additional applications or VMs that reside outside of the Cloud Foundation environment. Therefore, configuring the vRealize Operations Manager environment that is deployed by SDDC Manager to monitor 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,” on page 76
- “Managing Alerts, Events, and Audit Events,” on page 77
- “Using vRealize Log Insight Capabilities in Your Cloud Foundation Environment,” on page 92
- “Using vRealize Operations Manager Capabilities in Your Cloud Foundation Environment,” on page 96
Managing Workflows and Tasks

From the System Status page of the SDDC Manager client, 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.

<table>
<thead>
<tr>
<th>Workflows</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>167</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NEW TASKS</th>
<th>40</th>
</tr>
</thead>
<tbody>
<tr>
<td>RUNNING TASKS</td>
<td>0</td>
</tr>
<tr>
<td>FAILED TASKS</td>
<td>1</td>
</tr>
<tr>
<td>RESUMING TASKS</td>
<td>0</td>
</tr>
<tr>
<td>SUCCESSFUL TASKS</td>
<td>126</td>
</tr>
</tbody>
</table>

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 he available underlying details, if any, about that task.
Managing Alerts, Events, and Audit Events

From the System Status page of the SDDC Manager client, you can work with the alerts, events, and audit events that have been reported by your Cloud Foundation environment.

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.

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.

After you have addressed the issue that is causing the alerts, you can clear the alerts:

- Clear an individual alert by expanding it in the list, clicking the CLEAR ALERT button within the expanded alert, and saving the change.
Clear multiple alerts at once by first clicking **Edit** to put the page into editing mode and then selecting the check boxes next to the alerts that you want to clear, clicking **CLEAR SELECTED** at the top of the listing, and then saving the change.

For a list of the alerts and their descriptions, see “**SDDC Manager Alerts Raised During Ongoing Operations**,” on page 87.

**Examining Events**

Clicking **View Details** for the total events list displays a screen in which you can examine the events that have occurred in the environment.

This screen includes events that have been raised by SDDC Manager within a system-default time period of fourteen days. Events that are older than fourteen days are not reported on this screen. To see the reports for events older than fourteen days, use the vRealize Log Insight instance, if your system is licensed for usage of vRealize Log Insight.

The count at the top of the screen reports the number of events raised within the system-default fourteen-day time period by SDDC Manager that have not yet been forwarded to the vRealize Log Insight instance. Because this count does not include events that have already been forwarded to the vRealize Log Insight instance, this count might be less than the number of events in the event listing below it, which includes both forwarded and not-yet-forwarded events.

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.
From the System Events page, you can:

- Click **Analysis** to launch the vRealize Log Insight Web interface and use the vRealize Log Insight capabilities to 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 Environment,” on page 92.

- 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,” on page 81.

### 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.
From the Audit Events page, you can:

- Click **Analysis** to launch the vRealize Log Insight Web interface and use the vRealize Log Insight capabilities to 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 Environment,” on page 92.

### 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.
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.

### Table 7.1. Hardware Operational Events Raised in a Cloud Foundation Environment

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Severity</th>
<th>Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMC_AUTHENTICATION_FAILURE</td>
<td>WARNING</td>
<td>The software is unable to authenticate to the server's out-of-band (OOB) management port.</td>
</tr>
<tr>
<td>BMC_MANAGEMENT_FAILURE</td>
<td>WARNING</td>
<td>The software failed to perform a management operation using the server's OOB management port.</td>
</tr>
<tr>
<td>BMC_NOT_REACHABLE</td>
<td>WARNING</td>
<td>The software is unable to communicate with the server's OOB management port.</td>
</tr>
<tr>
<td>CPU_CAT_ERROR</td>
<td>ERROR</td>
<td>A CPU has shut down due to the processor's catastrophic error (CATERR) signal.</td>
</tr>
<tr>
<td>CPU_INITIALIZATION_ERROR</td>
<td>ERROR</td>
<td>The software detected that a CPU startup initialization error has occurred.</td>
</tr>
<tr>
<td>CPU_MACHINE_CHECK_ERROR</td>
<td>ERROR</td>
<td>Server CPU has failed due to CPU Machine Check Error.</td>
</tr>
<tr>
<td>CPU_POST_FAILURE</td>
<td>ERROR</td>
<td>Server CPU has shut down due to POST failure.</td>
</tr>
<tr>
<td>CPU_TEMPERATURE_ABOVE_UPPER_THRESHOLD</td>
<td>WARNING</td>
<td>CPU temperature has reached its maximum safe operating temperature.</td>
</tr>
<tr>
<td>CPU_TEMPERATURE_BELOW_LOWER_THRESHOLD</td>
<td>WARNING</td>
<td>CPU temperature has reached its minimum safe operating temperature.</td>
</tr>
<tr>
<td>CPU_THERMAL_TRIP</td>
<td>ERROR</td>
<td>Server CPU has shut down due to thermal error.</td>
</tr>
<tr>
<td>DIMM_ECC_ERROR</td>
<td>ERROR</td>
<td>The software detected an uncorrectable Error Correction Code (ECC) error for a server's memory.</td>
</tr>
<tr>
<td>DIMM_TEMPERATURE_ABOVE_UPPER_THRESHOLD</td>
<td>WARNING</td>
<td>Memory temperature has reached its maximum safe operating temperature.</td>
</tr>
<tr>
<td>DIMM_THERMAL_TRIP</td>
<td>ERROR</td>
<td>Memory has shut down due to thermal error.</td>
</tr>
<tr>
<td>HDD_DOWN</td>
<td>ERROR</td>
<td>Operational status is down for an HDD storage drive.</td>
</tr>
<tr>
<td>HDD_EXCESSIVE_WRITE_ERRORS</td>
<td>WARNING</td>
<td>Excessive write errors reported for an HDD storage drive.</td>
</tr>
<tr>
<td>Event Name</td>
<td>Severity</td>
<td>Short Description</td>
</tr>
</tbody>
</table>
|------------------------------------------------|----------|Adam
| 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. |
| 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.                                       |
| PCH_TEMPERATURE_ABOVE_THRESHOLD                | WARNING  | Platform controller hub [PCH] temperature has reached its maximum safe operating temperature. |
| SERVER_DOWN                                    | ERROR    | Server is in the powered-down state.                                            |
| SERVER_PCIE_ERROR                              | ERROR    | A server's system has PCIe errors.                                              |
| SERVER_POST_ERROR                              | ERROR    | A server's system has POST failures.                                             |
| SERVER_UP                                      | INFO     | Server is in the powered-up state.                                              |
| SPINE_SWITCH_DOWN                              | ERROR    | Operational status is down for a physical rack's spine switch.                  |
| SPINE_SWITCH_PORT_DOWN                         | WARNING  | Operational status is down for a switch port: in a physical rack's spine switch. |
| SPINE_SWITCH_PORT_UP                           | INFO     | Operational status is up for a switch port: in a physical rack's spine switch.   |
| SPINE_SWITCH_UP                                | INFO     | Operational status is up for a physical rack's spine 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. |
Table 7.1. Hardware Operational Events Raised in a Cloud Foundation Environment (Continued)

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Severity</th>
<th>Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSD_UP</td>
<td>INFO</td>
<td>Operational status is up for an SSD storage device.</td>
</tr>
<tr>
<td>SSD_WEAROUT_ABOVE_THRESHOLD</td>
<td>WARNING</td>
<td>Wear-out state of an SSD storage drive is above its</td>
</tr>
<tr>
<td></td>
<td></td>
<td>defined threshold.</td>
</tr>
<tr>
<td>STORAGE_CONTROLLER_DOWN</td>
<td>ERROR</td>
<td>Operational status is down for a storage adapter.</td>
</tr>
<tr>
<td>STORAGE_CONTROLLER_UP</td>
<td>INFO</td>
<td>Operational status is up for a storage adapter.</td>
</tr>
<tr>
<td>TOR_SWITCH_DOWN</td>
<td>ERROR</td>
<td>Operational status is down for a physical rack’s ToR</td>
</tr>
<tr>
<td>TOR_SWITCH_PORT_DOWN</td>
<td>WARNING</td>
<td>Operational status is down for a switch port in a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>physical rack’s ToR switch.</td>
</tr>
<tr>
<td>TOR_SWITCH_UP</td>
<td>INFO</td>
<td>Operational status is up for a physical rack’s ToR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>switch.</td>
</tr>
<tr>
<td>TOR_SWITCH_PORT_UP</td>
<td>INFO</td>
<td>Operational status is up for a switch port in a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>physical rack’s ToR switch.</td>
</tr>
</tbody>
</table>

**Audit Events**

In a Cloud Foundation environment, 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 7.2. Audit Events Raised in a Cloud Foundation Environment

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Severity</th>
<th>Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN_ADD_FAILED</td>
<td>WARNING</td>
<td>Creation and deployment of a workload domain failed.</td>
</tr>
<tr>
<td>DOMAIN_ADD_SUCCEEDED</td>
<td>INFO</td>
<td>Creation and deployment of a workload domain succeed.</td>
</tr>
<tr>
<td>DOMAIN_RETRY_ADD</td>
<td>INFO</td>
<td>User has initiated the restart workflow action on a workload-domain-related workflow.</td>
</tr>
<tr>
<td>DOMAIN_STATUS_UPDATE</td>
<td>INFO</td>
<td>A workload-domain-related workflow has changed status.</td>
</tr>
<tr>
<td>DOMAIN_TASK_ADDED</td>
<td>INFO</td>
<td>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.</td>
</tr>
<tr>
<td>DOMAIN_TASK_FAILED</td>
<td>WARNING</td>
<td>A subtask within a workload-domain-related workflow has failed.</td>
</tr>
<tr>
<td>DOMAIN_TASK_STATUS_UPDATE</td>
<td>INFO</td>
<td>A subtask within a workload-domain-related workflow has changed status.</td>
</tr>
<tr>
<td>DOMAIN_TASK_SUCCEEDED</td>
<td>INFO</td>
<td>A subtask within a workload-domain-related workflow has completed successfully.</td>
</tr>
<tr>
<td>DOMAIN_VDI_ADD</td>
<td>INFO</td>
<td>User has initiated the operation to create a VDI workload domain in the environment.</td>
</tr>
<tr>
<td>DOMAIN_VIRTUAL_INFRASTRUCTURE_ADD</td>
<td>INFO</td>
<td>User has initiated the operation to create a Virtual Infrastructure workload domain in the environment.</td>
</tr>
<tr>
<td>PERMISSION_GRANT_FAILED</td>
<td>WARNING</td>
<td>User has initiated the action to assign a role granting permissions to a user failed.</td>
</tr>
<tr>
<td>PERMISSION_GRANT_SUCCEEDED</td>
<td>INFO</td>
<td>The user-initiated action to assign a role granting permissions to a user has succeed.</td>
</tr>
</tbody>
</table>
Table 7-2. Audit Events Raised in a Cloud Foundation Environment (Continued)

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Severity</th>
<th>Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERMISSION_REVOKE_FAILED</td>
<td>WARNING</td>
<td>The user-initiated action to remove a role from a user and revoke</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the user's permissions granted by that role has failed.</td>
</tr>
<tr>
<td>PERMISSION_REVOKE_SUCCEEDED</td>
<td>INFO</td>
<td>The user-initiated action to remove a role from a user and revoke</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the user's permissions granted by that role has succeeded.</td>
</tr>
<tr>
<td>PERMISSION_UPDATE_FAILED</td>
<td>WARNING</td>
<td>The user-initiated action the action to change a user's existing role has failed.</td>
</tr>
<tr>
<td>PERMISSION_UPDATE_SUCCEEDED</td>
<td>INFO</td>
<td>The user-initiated action to change a user's existing role to another role has</td>
</tr>
<tr>
<td></td>
<td></td>
<td>completed successfully.</td>
</tr>
<tr>
<td>ROLE_ADD_FAILED</td>
<td>WARNING</td>
<td>The user-initiated action to create a new role in the environment has failed.</td>
</tr>
<tr>
<td>ROLE_ADD_SUCCEEDED</td>
<td>INFO</td>
<td>The user-initiated action to create a new role in the environment has completed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>successfully.</td>
</tr>
<tr>
<td>ROLE_DELETE_FAILED</td>
<td>WARNING</td>
<td>The user-initiated action to delete a role has failed.</td>
</tr>
<tr>
<td>ROLE_DELETE_SUCCEEDED</td>
<td>WARNING</td>
<td>The user-initiated action to delete a role has completed successfully.</td>
</tr>
<tr>
<td>ROLE_NAME_CHANGE_FAILED</td>
<td>WARNING</td>
<td>The user-initiated action to change a role name has failed.</td>
</tr>
<tr>
<td>ROLE_NAME_CHANGE_SUCCEEDED</td>
<td>INFO</td>
<td>The user-initiated action to change a role's name has completed successfully.</td>
</tr>
<tr>
<td>ROLE_PRIVILEGE_UPDATE_FAILED</td>
<td>WARNING</td>
<td>The user-initiated action to change the privileges associated with a role has</td>
</tr>
<tr>
<td></td>
<td></td>
<td>failed.</td>
</tr>
<tr>
<td>ROLE_PRIVILEGE_UPDATE_SUCCEEDED</td>
<td>INFO</td>
<td>The user-initiated action to change the privileges associated with a role has</td>
</tr>
<tr>
<td></td>
<td></td>
<td>completed successfully.</td>
</tr>
<tr>
<td>SERVER_POWER_CYCLE_FAILED</td>
<td>WARNING</td>
<td>The user-initiated action to power cycle a server has failed.</td>
</tr>
<tr>
<td>SERVER_POWER_CYCLE_SUCCEEDED</td>
<td>WARNING</td>
<td>The user-initiated action to power cycle a server has completed successfully.</td>
</tr>
<tr>
<td>SERVER_POWER_OFF_FAILED</td>
<td>WARNING</td>
<td>The user-initiated action to power off a server has failed.</td>
</tr>
<tr>
<td>SERVER_POWER_OFF_SUCCEEDED</td>
<td>WARNING</td>
<td>The user-initiated action to power off a server has completed successfully.</td>
</tr>
<tr>
<td>SERVER_POWER_ON_FAILED</td>
<td>WARNING</td>
<td>The user-initiated action to power on a server has failed.</td>
</tr>
<tr>
<td>SERVER_POWER_ON_SUCCEEDED</td>
<td>INFO</td>
<td>The user-initiated action to power on a server has completed successfully.</td>
</tr>
<tr>
<td>USER_LOG_IN_FAILED</td>
<td>WARNING</td>
<td>Log in to SDDC Manager failed for the user.</td>
</tr>
<tr>
<td>USER_LOG_IN_SUCCEEDED</td>
<td>INFO</td>
<td>Log in to SDDC Manager succeeded for the user.</td>
</tr>
<tr>
<td>USER_LOG_OUT_FAILED</td>
<td>WARNING</td>
<td>Log out from SDDC Manager failed for the user.</td>
</tr>
<tr>
<td>USER_LOG_OUT_SUCCEEDED</td>
<td>INFO</td>
<td>Log out from SDDC Manager succeeded for the user.</td>
</tr>
</tbody>
</table>

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 environment. 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 environment, see Chapter 14, “Patching and Upgrading Cloud Foundation,” on page 149.
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Severity</th>
<th>Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUNDLE_DOWNLOAD_FAILURE</td>
<td>ERROR</td>
<td>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.</td>
</tr>
<tr>
<td>BUNDLE_DOWNLOAD_FILESIZE_MISMATCH</td>
<td>ERROR</td>
<td>The downloaded bundle's file size is greater than the file size specified in the bundle manifest.</td>
</tr>
<tr>
<td>BUNDLE_DOWNLOAD_INVALID_TAR_MANIFEST</td>
<td>ERROR</td>
<td>An error occurred while parsing the manifest file inside the downloaded bundle retrieved from the remote download source.</td>
</tr>
<tr>
<td>BUNDLE_DOWNLOAD_SCHEDULED</td>
<td>INFO</td>
<td>A bundle download is scheduled. The scheduled time is provided in the event description.</td>
</tr>
<tr>
<td>BUNDLE_DOWNLOAD_STARTED</td>
<td>INFO</td>
<td>Downloading the bundle from the bundles' remote source location has started.</td>
</tr>
<tr>
<td>BUNDLE_DOWNLOAD_SUCCEEDED</td>
<td>INFO</td>
<td>The software successfully downloaded the bundle from the bundle's remote source location.</td>
</tr>
<tr>
<td>BUNDLE_DOWNLOAD_TIMEOUT</td>
<td>ERROR</td>
<td>The bundle download process timed out while downloading the bundle from the remote source location.</td>
</tr>
<tr>
<td>BUNDLE_MANIFEST_DOWNLOAD_SUCCEEDED</td>
<td>INFO</td>
<td>The software successfully downloaded the bundle's manifest from the remote source location.</td>
</tr>
<tr>
<td>BUNDLE_MANIFEST_DOWNLOAD_FAILURE</td>
<td>ERROR</td>
<td>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.</td>
</tr>
<tr>
<td>BUNDLE_MANIFEST_INVALID</td>
<td>ERROR</td>
<td>The software has determined that the bundle manifest which was retrieved from the remote source location and written to the local repository is invalid.</td>
</tr>
<tr>
<td>BUNDLE_MANIFEST_SIGNATURE_INVALID</td>
<td>ERROR</td>
<td>The signature for the bundle manifest is invalid.</td>
</tr>
<tr>
<td>BUNDLE_MANIFEST_SIGNATURE_NOT_FOUND</td>
<td>ERROR</td>
<td>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.</td>
</tr>
<tr>
<td>BUNDLE_REPO_FILE_NOT_FOUND</td>
<td>WARNING</td>
<td>The software cannot locate the specified bundle at the expected location within the bundle repository.</td>
</tr>
<tr>
<td>BUNDLE_REPO_WRITE_FAILURE</td>
<td>ERROR</td>
<td>Problems with the bundle repository are preventing bundle downloads from completing successfully.</td>
</tr>
<tr>
<td>PARTIAL_BUNDLE_DOWNLOAD</td>
<td>ERROR</td>
<td>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.</td>
</tr>
<tr>
<td>UPGRADE_ABORTED</td>
<td>WARNING</td>
<td>The software has automatically cancelled a scheduled upgrade because a workflow is taking place, such as a workload domain creation or deletion workflow.</td>
</tr>
<tr>
<td>UPGRADE_CANCELLED</td>
<td>INFO</td>
<td>User has cancelled the upgrade.</td>
</tr>
<tr>
<td>UPGRADE_COMPLETION</td>
<td>WARNING</td>
<td>The life cycle management upgrade completed. The upgraded component and the completion status is provided in the event description.</td>
</tr>
<tr>
<td>UPGRADE_FAILED</td>
<td>WARNING</td>
<td>Upgrade operation has failed.</td>
</tr>
<tr>
<td>UPGRADE_NOT_NEEDED</td>
<td>INFO</td>
<td>The software has determined all of the environment's components have up-to-date versions and upgrading them is not needed.</td>
</tr>
<tr>
<td>UPGRADE_SCHEDULED</td>
<td>INFO</td>
<td>A bundle upgrade is scheduled. The scheduled time is provided in the event description.</td>
</tr>
<tr>
<td>Event Name</td>
<td>Severity</td>
<td>Short Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UPGRADE_STARTED</td>
<td>INFO</td>
<td>Upgrade operation has started.</td>
</tr>
<tr>
<td>UPGRADE_SUCCEEDED</td>
<td>INFO</td>
<td>Upgrade operation has succeeded.</td>
</tr>
<tr>
<td>UPGRADE_TIMEDOUT</td>
<td>WARNING</td>
<td>Upgrade operation has timed out.</td>
</tr>
<tr>
<td>VMWARE_DEPOT_CONNECT_FAILURE</td>
<td>WARNING</td>
<td>The software failed to connect to the remote source location from which the upgrade bundles are downloaded.</td>
</tr>
<tr>
<td>VMWARE_DEPOT_INDEX_FILE_NOT_FOUND</td>
<td>ERROR</td>
<td>The software failed to download a manifest file at the remote source location.</td>
</tr>
<tr>
<td>VMWARE_DEPOT_INSUFFICIENT_PERMISSION</td>
<td>ERROR</td>
<td>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.</td>
</tr>
<tr>
<td>VMWARE_DEPOT_INDEX_INVALID</td>
<td>ERROR</td>
<td>The retrieved bundle index is invalid.</td>
</tr>
<tr>
<td>VMWARE_DEPOT_MANIFEST_FILE_NOT_FOUND</td>
<td>ERROR</td>
<td>The software cannot locate a manifest file at the remote source location.</td>
</tr>
<tr>
<td>VMWARE_DEPOT_MISSING_BUNDLE</td>
<td>ERROR</td>
<td>The software cannot locate a bundle available for downloading from the remote source location.</td>
</tr>
<tr>
<td>VMWARE_DEPOT_UNKNOWN_HOST</td>
<td>ERROR</td>
<td>The software cannot resolve the VMware Depot host of the configured remote source location for downloading upgrade bundles.</td>
</tr>
</tbody>
</table>

## 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,” on page 87.

## 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 environment 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 installation in the last 24 hours is captured.

Inventory validation alerts are raised when mismatches are found between the obtained actual inventory and the expected inventory. The expected inventory is defined by the installation's manifest.

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 client.

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,” on page 81 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.

You can use the Alerts Catalog page in the SDDC Manager client 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,” on page 87.

### Table 7-4. SDDC Manager Alerts

<table>
<thead>
<tr>
<th>Alert Name</th>
<th>Short Description</th>
<th>Severity</th>
<th>Detected By</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMC_AUTHENTICATION_FAILURE_ALERT</td>
<td>The system is unable to authenticate to the server’s OOB management port. This alert is initiated by the BMC_AUTHENTICATION_FAILURE event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>BMC_MANAGEMENT_FAILURE_ALERT</td>
<td>The system failed to perform a management operation using the server’s OOB management port. This alert is initiated by the BMC_MANAGEMENT_FAILURE event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>BMC_NOT_REACHABLE_ALERT</td>
<td>The system is unable to communicate with the server’s OOB management port. This alert is initiated by the BMC_NOT_REACHABLE event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>COORDINATION_SERVICE_DOWN_ALERT</td>
<td>The system cannot establish a connection to the virtual machines that provide the required coordination service. This service is provided by the ISVM virtual machines that run in the N0 ESXi host in the environment’s primary rack. The bring-up process requires connection to the coordination service.</td>
<td>CRITICAL</td>
<td>Event 30-minute poll, 24-hour poll</td>
</tr>
<tr>
<td>CPU_CAT_FAILURE_ALERT</td>
<td>A CPU has shut down due to the processor’s catastrophic error (CATERR) signal. This alert is initiated by the CPU_CAT_ERROR event.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td>CPU_EXTRA_ALERT</td>
<td>The polling found an additional CPU that does not match what is expected according to the manifest.</td>
<td>WARNING</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>CPU_INITIALIZATION_ERROR_ALERT</td>
<td>The system detected that a CPU startup initialization error has occurred. This alert is initiated by the CPU_INITIALIZATION_ERROR event.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td>CPU_INVALID_ALERT</td>
<td>The polling detected a type of CPU in the server that does not match what is expected according to the manifest.</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>Alert Name</td>
<td>Short Description</td>
<td>Severity</td>
<td>Detected By</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>CPU_MACHINE_CHECK_ERROR_ALERT</td>
<td>A server CPU has failed due to CPU Machine Check Error. This alert is initiated by the CPU_MACHINE_CHECK_ERROR event.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td>CPU_POST_FAILURE_ALERT</td>
<td>A server CPU has shut down due to POST failure. This alert is initiated by the CPU_POST_FAILURE event.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td>CPU_TEMPERATURE_ABOVE_UPPER_THRESHOLD_ALERT</td>
<td>A CPU temperature has reached its maximum safe operating temperature. This alert is initiated by the CPU_TEMPERATURE_ABOVE_UPPER_THRESHOLD event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>CPU_TEMPERATURE BELOW_LOWER_THRESHOLD_ALERT</td>
<td>A CPU temperature has reached its minimum safe operating temperature. This alert is initiated by the CPU_TEMPERATURE BELOW_LOWER_THRESHOLD event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>CPU_THERMAL_TRIP_ERROR_ALERT</td>
<td>A server CPU has shut down due to thermal error. This alert is initiated by the CPU_THERMAL_TRIP_ERROR event.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td>CPU_UNDETECTED_ALERT</td>
<td>The polling did not detect a CPU that matches what is expected according to the manifest.</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>DIMM_ECC_MEMORY_ERROR_ALERT</td>
<td>The system detected an uncorrectable Error Correction Code (ECC) error for a server’s memory. This alert is initiated by the DIMM_ECC_MEMORY_ERROR event.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td>DIMM_TEMPERATURE_ABOVE_THRESHOLD_ALERT</td>
<td>Memory temperature has reached its maximum safe operating temperature. This alert is initiated by the DIMM_TEMPERATURE_ABOVE_THRESHOLD event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>DIMM_THERMAL_TRIP_ALERT</td>
<td>Memory has shut down due to thermal error. This alert is initiated by the DIMM_THERMAL_TRIP event.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td>HDD_DOWN_ALERT</td>
<td>Operational status is down for an HDD. This alert is initiated by the HDD_DOWN event.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td>HDD_EXCESSIVE_READ_ERRORS_ALERT</td>
<td>Excessive read errors reported for an HDD. This alert is initiated by the HDD_EXCESSIVE_READ_ERRORS event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>HDD_EXCESSIVE_WRITE_ERRORS_ALERT</td>
<td>Excessive write errors reported for an HDD. This alert is initiated by the HDD_EXCESSIVE_WRITE_ERRORS event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>HDD_EXTRA_ALERT</td>
<td>The polling found an additional HDD that does not match what is expected according to the manifest.</td>
<td>WARNING</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>HDD_INVALID_ALERT</td>
<td>The polling detected a type of HDD that does not match what is expected according to the manifest.</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>HDD_TEMPERATURE_ABOVE_THRESHOLD_ALERT</td>
<td>HDD temperature has reached its maximum safe operating temperature. This alert is initiated by the HDD_TEMPERATURE_ABOVE_THRESHOLD event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>HDD_UNDETECTED_ALERT</td>
<td>The polling did not detect an HDD that matches what is expected according to the manifest.</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>HDD_WEAROUT_ABOVE_THRESHOLD_ALERT</td>
<td>Wear-out state of an HDD is above its defined threshold. This alert is initiated by the HDD_WEAROUT_ABOVE_THRESHOLD event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>HMS_AGENT_DOWN_ALERT</td>
<td>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.</td>
<td>CRITICAL</td>
<td>30-minute poll, 24-hour poll, Event</td>
</tr>
<tr>
<td>Alert Name</td>
<td>Short Description</td>
<td>Severity</td>
<td>Detected By</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>HMS_DOWN_ALERT</td>
<td>The SDDC Manager cannot communicate with the HMS aggregator.</td>
<td>CRITICAL</td>
<td>30-minute poll</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>24-hour poll</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Event</td>
</tr>
<tr>
<td>HOST_AGENT_NOT_ALIVE_ALERT</td>
<td>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.</td>
<td>CRITICAL</td>
<td>30-minute poll</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>24-hour poll</td>
</tr>
<tr>
<td>LICENCE_PRESENT_CHECK_FAILED_ALERT</td>
<td>The check for the license for a particular bundle failed.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>MANAGEMENT_SWITCH_DOWN_ALERT</td>
<td>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.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>30-minute poll</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>24-hour poll</td>
</tr>
<tr>
<td>MANAGEMENT_SWITCH_EXTRA_ALERT</td>
<td>The polling found an additional management switch that does not match what is expected according to the manifest.</td>
<td>WARNING</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>MANAGEMENT_SWITCH_INVALID_ALERT</td>
<td>The polling detected a type of management switch that does not match what is expected according to the manifest.</td>
<td>CRITICAL</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>MANAGEMENT_SWITCH_PORT_DOWN_ALERT</td>
<td>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.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>MEMORY_EXTRA_ALERT</td>
<td>The polling found additional memory that does not match what is expected according to the manifest.</td>
<td>WARNING</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>MEMORY_INVALID_ALERT</td>
<td>The polling detected a type of memory that does not match what is expected according to the manifest.</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>MEMORY_UNDETECTED_ALERT</td>
<td>The polling did not detect memory that matches what is expected according to the manifest.</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>NIC_EXTRA_ALERT</td>
<td>The polling found an additional NIC that does not match what is expected according to the manifest.</td>
<td>WARNING</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>NIC_INVALID_ALERT</td>
<td>The polling detected a type of NIC that does not match what is expected according to the manifest.</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>NIC_PORT_DOWN_ALERT</td>
<td>Operational status is down for a NIC port in a rack’s server. This alert is initiated by the NIC_PORT_DOWN event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>NIC_UNDETECTED_ALERT</td>
<td>The polling did not detect a NIC that matches what is expected according to the manifest.</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>PCH_TEMPERATURE_ABOVE_THRESHOLD_ALERT</td>
<td>Platform controller hub [PCH] temperature has reached its maximum safe operating temperature. This alert is initiated by the PCH_TEMPERATURE_ABOVE_THRESHOLD event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>POSTGRES_DOWN_ALERT</td>
<td>The system cannot connect to an internal database.</td>
<td>CRITICAL</td>
<td>Event</td>
</tr>
<tr>
<td>SERVER_DOWN_ALERT</td>
<td>Server is in the powered-down state. This alert is initiated by the SERVER_DOWN event.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>30-minute poll</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>24-hour poll</td>
</tr>
<tr>
<td>SERVER_EXTRA_ALERT</td>
<td>The polling detected an additional server that does not match what is expected according to the manifest.</td>
<td>WARNING</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>Alert Name</td>
<td>Short Description</td>
<td>Severity</td>
<td>Detected By</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------------</td>
</tr>
<tr>
<td>SERVER_INVALID_ALERT</td>
<td>The polling detected a type of server that does not match what is expected according to the manifest.</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>SERVER_PCIE_ERROR_ALERT</td>
<td>A server’s system has PCIe errors. This alert is initiated by the SERVER_PCIE_ERROR event.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td>SERVER_POST_ERROR_ALERT</td>
<td>A server has POST failures.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td>SERVER_UNDETECTED_ALERT</td>
<td>The polling did not detect a server that matches what is expected according to the manifest.</td>
<td>ERROR</td>
<td>30-minute poll</td>
</tr>
<tr>
<td>SPINE_SWITCH_DOWN_ALERT</td>
<td>Operational status is down for a physical rack’s spine switch. This alert is initiated by the periodic polling and by the SPINE_SWITCH_DOWN event.</td>
<td>ERRORS</td>
<td>Event</td>
</tr>
<tr>
<td>SPINE_SWITCH_EXTRA_ALERT</td>
<td>The polling detected an additional spine switch that does not match what is expected according to the manifest.</td>
<td>WARNING</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>SPINE_SWITCH_INVALID_ALERT</td>
<td>The polling detected a type of spine switch that does not match what is expected according to the manifest.</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>SPINE_SWITCH_PORT_DOWN_ALERT</td>
<td>Operational status is down for a switch port in a physical rack’s spine switch. This alert is initiated by the SPINE_SWITCH_PORT_DOWN event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>SSD_DOWN_ALERT</td>
<td>Operational status is down for an SSD. This alert is initiated by the SSD_DOWN event.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td>SSD_EXCESSIVE_READ_ERRORS_ALERT</td>
<td>Excessive read errors reported for an SSD. This alert is initiated by the SSD_EXCESSIVE_READ_ERRORS event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>SSD_EXCESSIVE_WRITE_ERRORS_ALERT</td>
<td>Excessive write errors reported for an SSD. This alert is initiated by the SSD_EXCESSIVE_WRITE_ERRORS event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>SSD_EXTRA_ALERT</td>
<td>The polling found an additional SSD that does not match what is expected according to the manifest.</td>
<td>WARNING</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>SSD_INVALID_ALERT</td>
<td>The polling detected a type of SSD that does not match what is expected according to the manifest.</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>SSD_TEMPERATURE_ABOVE_THRESHOLD_ALERT</td>
<td>SSD temperature has reached its maximum safe operating temperature. This alert is initiated by the SSD_TEMPERATURE_ABOVE_THRESHOLD event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>SSD_UNDETECTED_ALERT</td>
<td>The polling did not detect an SSD that matches what is expected according to the manifest.</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>SSD_WEAROUT_ABOVE_THRESHOLD_ALERT</td>
<td>Wear-out state of an SSD is above its defined threshold. This alert is initiated by the SSD_WEAROUT_ABOVE_THRESHOLD event.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>STORAGE_CONTROLLER_DOWN_ALERT</td>
<td>Operational status is down for a storage adapter. This alert is initiated by the STORAGE_CONTROLLER_DOWN event.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td>STORAGE_CONTROLLER_EXTRA_ALERT</td>
<td>The polling detected an additional storage adapter that does not match what is expected according to the manifest.</td>
<td>WARNING</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>STORAGE_CONTROLLER_INVALID_ALERT</td>
<td>The polling detected a type of storage adapter that does not match what is expected according to the manifest.</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>STORAGE_CONTROLLER_UNDETECTED_ALERT</td>
<td>The polling did not detect a storage adapter that matches what is expected according to the manifest.</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
</tbody>
</table>
Using vRealize Log Insight Capabilities in Your Cloud Foundation Environment

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 installation 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 client, see “Get Started Using the vRealize Log Insight Instance,” on page 94.

**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.

---

Table 7-4. SDDC Manager Alerts (Continued)

<table>
<thead>
<tr>
<th>Alert Name</th>
<th>Short Description</th>
<th>Severity</th>
<th>Detected By</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOR_SWITCH_DOWN_ALERT</td>
<td>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.</td>
<td>ERROR</td>
<td>Event 30-minute poll, 24-hour poll</td>
</tr>
<tr>
<td>TOR_SWITCH_EXTRA_ALERT</td>
<td>The polling found an additional ToR switch that does not match what is expected according to the manifest.</td>
<td>WARNING</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>TOR_SWITCH_INVALID_ALERT</td>
<td>The polling detected a type of ToR switch that does not match what is expected according to the manifest.</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td>TOR_SWITCH_PORT_DOWN_ALERT</td>
<td>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.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td>VMWARE_CLOUD_FOUNDATION_BUNDLE_INCOMPLETE_ALERT</td>
<td>The ISO file is missing items, according to its manifest.</td>
<td>CRITICAL</td>
<td>Event</td>
</tr>
<tr>
<td>VMWARE_CLOUD_FOUNDATION_BUNDLE_INVALID_ALERT</td>
<td>Checksum validation for the ISO file failed.</td>
<td>CRITICAL</td>
<td>Event</td>
</tr>
<tr>
<td>VMWARE_CLOUD_FOUNDATION_BUNDLE_MISSING.Alert</td>
<td>A required ISO file or its expected checksum file or manifest file is missing.</td>
<td>CRITICAL</td>
<td>Event</td>
</tr>
</tbody>
</table>
**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,” on page 93. 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.

<table>
<thead>
<tr>
<th>Content Pack</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Foundation</td>
<td>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.</td>
</tr>
<tr>
<td>General</td>
<td>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</td>
</tr>
<tr>
<td>vSphere</td>
<td>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.</td>
</tr>
<tr>
<td>NSX for vSphere</td>
<td>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.</td>
</tr>
<tr>
<td>Horizon View</td>
<td>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.</td>
</tr>
<tr>
<td>Virtual SAN</td>
<td>This content pack provides various dashboards and filters to give you insight into the logs that are sent by the management and workload domains’ Virtual SAN features.</td>
</tr>
</tbody>
</table>

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 installation. 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 installation, 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 installation.

During the bring-up process of your installation, 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 Environment,” on page 92. 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 client, you can open the vRealize Log Insight Web interface using the following methods. During a logged-in session of the SDDC Manager client, 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 `vrm-cli.sh lookup-password` in the VM’s `/home/vrack/bin` directory. See “Credentials for Logging In To the SDDC Manager (vrm) Virtual Machine,” on page 22 and “Look Up Account Credentials Using the Lookup-Password Command,” on page 23.

**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, log in to the SDDC Manager VM and use the `vrm-cli.sh rotate-password-li-api` command.

**Procedure**

1. Open the vRealize Log Insight Web interface.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the Audit Events page, click the Analysis button.</td>
<td>The vRealize Log Insight display is filtered to show the collected audit events only.</td>
</tr>
<tr>
<td>From the Events page, click the Analysis button.</td>
<td>The vRealize Log Insight displays all collected events.</td>
</tr>
<tr>
<td>From a management domain’s details, click the launch link listed in the Management Info area.</td>
<td>The vRealize Log Insight displays all collected events.</td>
</tr>
</tbody>
</table>

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 3, “On-Demand Password Rotation in Your Cloud Foundation Installation,” on page 21.

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](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 environment, 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 remotely to the SDDC Manager virtual machines on each rack. The root account credentials are managed by your organization. See “Credentials for Logging In To the SDDC Manager (vrm) Virtual Machine,” on page 22.

**Procedure**

1. On the primary rack, using the root account, connect and log in, for example by 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**

- Repeat the steps for each rack in your installation.
- 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,” on page 94.

**Using vRealize Operations Manager Capabilities in Your Cloud Foundation Environment**

The vRealize Operations Manager instance that is deployed by SDDC Manager is licensed separately. When the vRealize Operations Manager instance is licensed for use in your Cloud Foundation environment, you can use its capabilities to work with the Cloud Foundation data that is sent to it and obtain a picture of the health of the virtual infrastructure for the management and workload domains.

The capabilities of vRealize Operations Manager help you to proactively identify and solve emerging issues with predictive analysis and smart alerts, ensuring optimal performance monitoring and availability of the virtual infrastructure it monitors. Data from the management and workload domains can propagate to the vRealize Operations Manager instance and you get a unified view of the event data and metrics for the virtual infrastructure. The vCenter Adapter for vRealize Operations Manager is installed and configured in vRealize Operations Manager. Additionally, when you create a VDI workload domain, the Horizon View
Adapter for vRealize Operations Manager is installed and configured also. Over time, you can use the vRealize Operations Manager Web interface to analyze event data for the management and workload domains' virtual infrastructure over time, providing the ability for performance management and infrastructure capacity planning.

**Note** The vRealize Operations Manager environment that SDDC Manager deploys is sized for monitoring the contents of your Cloud Foundation installation only. The default sizing accommodates the metrics and events expected to be sent by the Cloud Foundation environment’s vCenter Server instances and Horizon software components. This sizing might not accommodate the numbers of metrics and events for monitoring additional applications or VMs that reside outside of the Cloud Foundation environment. Therefore, configuring the vRealize Operations Manager environment that is deployed by SDDC Manager to monitor additional applications or VMs that reside outside of your Cloud Foundation environment is not supported in this release.

**vRealize Operations Manager Multiple-Node Cluster**

In a single-rack Cloud Foundation environment, the vRealize Operations Manager cluster is deployed as a cluster with a single node, the master node. When an additional rack is added to the environment, the vRealize Operations Manager cluster is scaled out by adding a data node on that rack, making the vRealize Operations Manager environment a multiple-node cluster. In a multiple-node cluster, the nodes act together as a single vRealize Operations Manager cluster.

Accessing the vRealize Operations Manager administrative Web interface on any node allows access to the data from all of the nodes. Adapters for the objects residing in the physical rack are created on the vRealize Operations Manager node that is on that rack, to provide for balanced operation.

**Examine the Health of the Virtual Infrastructure Using vRealize Operations Manager**

Use of the vRealize Operations Manager instance is licensed separately. When the vRealize Operations Manager instance is licensed for use in your Cloud Foundation environment, you can obtain a picture of how the virtual infrastructure for the management and workload domains is running and the health of that virtual infrastructure by using the vRealize Operations Manager Web interface to examine the event data that is sent from the management and workload domains.

In the SDDC Manager client, you can launch the vRealize Operations Manager Web interface using the following methods. When logged in to the SDDC Manager client, you must authenticate to vRealize Operations Manager the first time you open the vRealize Operations Manager 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 Operations Manager Web interface.

**Procedure**

1. Open the vRealize Operations Manager Web interface by clicking the **vROPS** launch link located in the domain details for the management domains.
   
   The vRealize Operations Manager login screen appears.

2. For the authentication source, select the **All vCenter Servers** choice.

3. Log in using your SDDC Manager administrator account credentials.

   Those account credentials are the ones for the superuser name and password entered during the bring-up process in the Create Superuser screen.

   The vRealize Operations Manager web interface displays its Solutions view. The Solution Details area indicates that vRealize Operations Manager is collecting data from your environment’s management and workload domains.

4. Click **Home**.
The vRealize Operations Manager Web interface appears and you can examine the collected data and examine the alerts and health indicators.

**What to do next**

For detailed information and procedures for using the features of vRealize Operations Manager, see the vRealize Operations Manager Documentation Center located at http://pubs.vmware.com/vrealizeoperationsmanager-6/index.jsp.
Use the Settings area of the SDDC Manager client 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,” on page 99
- “Additional Rack Settings Screen,” on page 102
- “Managing Network Settings,” on page 102

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 client, 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,” on page 100.
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,” on page 99.

<table>
<thead>
<tr>
<th>Type</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal AD Name</td>
<td>horizon.local</td>
<td>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.</td>
</tr>
<tr>
<td>AD VM Name prefix</td>
<td>ad-</td>
<td>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).</td>
</tr>
<tr>
<td>Domain Net BIOS Name</td>
<td>HORIZON</td>
<td>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.</td>
</tr>
<tr>
<td>Domain Controller Name</td>
<td>DC1</td>
<td>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).</td>
</tr>
<tr>
<td>Virtual Desktops OU</td>
<td>CN=Computers,DC=horizon,DC=local</td>
<td>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.</td>
</tr>
<tr>
<td>View Servers OU</td>
<td>OU=View,DC=horizon,DC=local</td>
<td>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.</td>
</tr>
<tr>
<td>Number of Server Processors</td>
<td>4 of 8</td>
<td>The number of processors a single VDI server must have in the deployed VDI workload domain.</td>
</tr>
<tr>
<td>Type</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Memory per Server</td>
<td>10 GB of 32 GB</td>
<td>The amount of memory a single VDI server must have in the deployed VDI workload domain.</td>
</tr>
<tr>
<td>Servers System Drive</td>
<td>80 GB of 400 GB</td>
<td>The size of the system drive that a single VDI server must have in the deployed VDI workload domain.</td>
</tr>
<tr>
<td>Connection Server Naming Convention</td>
<td>con-</td>
<td>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).</td>
</tr>
<tr>
<td>Composer Server Naming Convention</td>
<td>com-</td>
<td>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).</td>
</tr>
<tr>
<td>Security Server Naming Convention</td>
<td>sec-</td>
<td>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).</td>
</tr>
<tr>
<td>Virtual Desktops Naming Convention</td>
<td>vm-</td>
<td>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).</td>
</tr>
<tr>
<td>Max Desktops per Connection Server</td>
<td>2000</td>
<td>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.</td>
</tr>
<tr>
<td>Max Desktops per Security Server</td>
<td>500</td>
<td>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.</td>
</tr>
<tr>
<td>Type</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Max Desktops per vCenter Server</td>
<td>2000</td>
<td>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.</td>
</tr>
<tr>
<td>Max Virtual CPUs per Core</td>
<td>4</td>
<td>Specifies the maximum number of virtual processors (vCPUs) that a physical core on the ESXi hosts should handle.</td>
</tr>
<tr>
<td>Desktop System Drive Size [GB]</td>
<td>60</td>
<td>Specifies the size (in GB) of the data drive that is configured as a D: drive for each virtual desktop.</td>
</tr>
<tr>
<td>Desktop System Snapshot Size</td>
<td>5</td>
<td>Specifies the size (in GB) of the data drive that is configured as a snapshot for each virtual desktop.</td>
</tr>
<tr>
<td>Desktops accessed via the Internet [%]</td>
<td>10</td>
<td>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.</td>
</tr>
<tr>
<td>Desktop Pool Name Prefix</td>
<td>pl-</td>
<td>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).</td>
</tr>
</tbody>
</table>

### 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 spine switches to connect it to the installation’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 the SDDC Manager Client

After the Cloud Foundation bring-up process, you can use the Uplink screen in the SDDC Manager client 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 user interface. 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.

**Prerequisites**

If you plan to change the uplink settings, connect to port 48 on the management switch and log in to the SDDC Manager client 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 the 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 client, navigate to **Settings > NETWORK SETTINGS > UPLINK**.
2. Review the current uplink settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uplink Type</td>
<td>This field indicates whether the current ToR uplink uses L2 or L3 settings. Read-only.</td>
</tr>
<tr>
<td>Uplink LAG Enabled</td>
<td>Specify whether to enable link aggregation (LAG), YES or NO.</td>
</tr>
</tbody>
</table>
| Uplink Ports          | Specify the ToR switch ports that are cabled as the uplink to your corporate network. Ports must be in the ranges:  
  - 43 to 46, for uplink speeds less than 40Gbps  
  - 51 to 54, for a 40Gbps 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 addresses 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,” on page 104.

- **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 addresses 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 installation. 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 installation, 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 installation. 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.

**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 installation, a data center connection specifies the network that carries traffic between the installation and the networking environment external to the installation, such as your corporate network. During the Cloud Foundation bring-up process, a data center connection was specified. During ongoing operations, a data center connection can be specified when creating a workload domain and using this screen.

**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, 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.
- 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.
Back Up Component Configurations Using the SoS Tool

Use the SoS tool to create backup files of various components’ configurations in your Cloud Foundation environment. This Python tool resides in each SDDC Manager virtual machine in your environment.

The SoS tool makes backup files of these components’ configurations:

- ESXi hosts
- Switches (management, ToR, spine)
- The three infrastructure (ISVM) virtual machines’ Zookeeper server instances and Cassandra distributed database
- SDDC Manager instances (the virtual machines in each rack with names starting with vr)
- The SDDC Manager instances’ HMS software components

The backup files are written by default to the /var/tmp directory in the filesystems of your environment’s SDDC Manager instances:

- When you run the ./sos --backup command in the SDDC Manager instance that is currently assigned the SDDC Manager VIP, the SoS tool makes an API call to all of the SDDC Manager instances on your environment’s other racks to initiate the backup process for the component configurations on those racks. Each rack’s backup configuration files are written to the /var/tmp directory in the filesystem of each rack’s SDDC Manager instance. You then log in to each SDDC Manager instance and change directories to the /var/tmp directory to find the output files for that rack.

- When you run the ./sos --backup command in an SDDC Manager instance that is not currently assigned the VIP, the tool creates the backup files only for that rack’s components. The output files are written to the /var/tmp directory in that SDDC Manager instance’s filesystem.

After the output file are created, you can copy the files to another location to have them available for future replacement and restoration situations.

For a description of the SDDC Manager VIP and how to determine which instance it is currently assigned to, see “About the Primary Rack and the SDDC Manager Virtual IP Address,” on page 11.

Prerequisites

When running the backup command to create the backup files for all racks in the installation in a single command run, you must have the root account credentials for the SDDC Manager instance that currently has the SDDC Manager VIP. When you want to get these backup files created for all racks in a single command run, you can run the tool in that SDDC Manager instance, logging in using the root account credentials for that VM. In the managment domain on each rack, the SDDC Manager instance is the one whose virtual machine name starts with vr. See “Credentials for Logging In To the SDDC Manager (vr) Virtual Machine,” on page 22.
Procedure

1. Using the root account, connect and log in, for example by SSH, to the SDDC Manager instance in which you want to run the backup command.

2. Change to the /opt/vmware/evosddc-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-vrm-1:/opt/vmware/evosddc-support # ./sos --backup
   Welcome to SoS(Supportability and Serviceability) utility!
   Backup: /var/tmp/backup-2016-11-08-15-01-48-3650
   Progress : 0%
   ```

   The tool collects the configurations from the components and writes the output to the /var/tmp directory in the SDDC Manager instance in which the SoS tool was invoked. Inside that directory, the tool writes the output into a directory whose name reflects the timestamp when the SoS tool initiated the process. If the tool was invoked in the SDDC Manager instance that has the SDDC Manager VIP, the tool also writes backup configurations into the other SDDC Manager instances' /var/tmp directories.

   **Note** Each rack's backup files are written into the subdirectory named rack-1 in the /var/tmp/backup-timestamp directory that is created in that rack's SDDC Manager instance.

   ```
   /var/tmp
   backup-timestamp
   sos.log
   rack-1
     esx
       configBundle-hostname.domain.tgz  #One per host
     switch
       ToR-or-spine-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
   zk  #This directory appears for the rack where the ISVM VMs are deployed
     isvm-ip-address  #Three directories in the zk directory, each named using the IP address of an ISVM VM, such as 192.168.100.43
       cassandra-db-backup.tgz
       zk-db-backup.tgz
   vrm.properties
   hms_ib_inventory.json
   vrm.properties
   vrm.properties.vRack
   vrm-security.keystore
   hms.tar.gz
   vrm-timestamp.tgz
   ```

   **What to do next**

   Copy the backup files to a location where you can conveniently retrieve them for future configuration restoration situations.
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** on page 109
  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** on page 114
  The replacement procedure depends on the component being replaced and the condition of the component.

- **Install ESXi VIBs on New Host** on page 125
  Follow this procedure to install ESXi VIBs on a host.

**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** on page 109
  You can add capacity to your Cloud Foundation installation 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.

- **Add a Previously Decommissioned Host to a Physical Rack** on page 112
  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.

**Add a New Host to a Physical Rack**

You can add capacity to your Cloud Foundation installation 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 should be identical to the other hosts in the rack - from the same vendor, of the same model number, and have the same firmware version. It should be physically at your site before you begin this procedure.
Ensure that the following has been completed on the decommissioned host before adding it to a physical rack.

1. Password on the host is EvoSddc!2016, the default password for all ESXi hosts.
2. Secure Shell (SSH) is enabled.
3. Firewall on SSH host is enabled and connections are restricted to the 192.168.100.0/22 subnet.
4. DNS IP is set to 192.168.1.254.
5. Has an IP address from the range 192.168.100.50 - 192.168.100.73.
6. Appropriate VIB is installed based on the controller.

Procedure

1. Do one of the following.
   - Install ESXi VIBs on the new host, See “Install ESXi VIBs on New Host,” on page 125.
2. Mount the new host in an empty slot on the rack and connect it to the management and ToR switches according to the wiremap. See Chapter 16, “Rack Wiring,” on page 183.
3. Power on the new host.
   
The management switch learns the host MAC via the DHCP request it receives from the new host. HMS learns that a new host is connected and updates its internal inventory.
4. In a command line window, SSH to the SDDC Manager VM on the rack where you are adding the host.
5. Open the /home/vrack/VMware/vRack/server-commission.properties file and specify values for:
   - `hms.host.bmc.username`
     For example, `hms.host.bmc.username=root`
   - `hms.host.bmc.password`
     For example, `hms.host.bmc.password=calvin`

   Do not use quotes when specifying the above values.

   **Note** Verify that you have typed the user name and password correctly.

6. Type the following CLI command to run the Server Commission Tool:
   ```bash
   sudo /home/vrack/bin/server-commission.sh
   ```
   You need administrator credentials to run this command, and can commission one server at a time. During host commissioning, the system recognizes the new host and adds it to the inventory and the capacity pool.

   The command window displays the task progress.

   In loadConfig, loading configuration from '/home/vrack/VMware/vRack/server-commission.properties'.
   In loadConfig, loading configuration from '/home/vrack/VMware/vRack/vrm.properties'.
   In getNewHosts, discovering new hosts.
   In commissionServer, discovered new host. BMC - [ IP: 192.168.0.51, MAC: 64:00:6a:c4:02:16 ].
   In getNewHostInbandIpAddress, '192.168.100.51' is new host Inband IP address.
   In addHostKeyToKnownHosts, SSH key for the host '192.168.100.51' added to known hosts file '/home/vrack/.ssh/known_hosts'.
   In enableCdp, Cisco Discovery Protocol is set in 'both' mode for vSwitch: 'vSwitch0'
   In applylicense, license is applied.
   In addHostToHmsInventory, new host's hostId is 'N6'.

   Administering VMware Cloud Foundation

   110  VMware, Inc.
In addHostToHmsInventory, saved HMS inventory after adding new host to inventory.
In refreshHmsInventory, HMS inventory refreshed successfully.
In addHostToPRMInventory, adding host 'N6' to PRM inventory.
In addHostToPrmInventory, PRM inventory updated successfully.
In addHostToPRMInventory, added host 'N6' to PRM inventory.
In commissionHost, commissioning host 'N6' initiated successfully.
In getHostCommissioningStatus, host commissioning succeeded.
In commissionServer, server commissioned successfully.
In updatePRMInventoryForServer, successfully updated PRM Inventory.
In commissionServer, PRM Inventory updated after server commissioned.
In commissionServer, VRM Health service restarted.
Server Commissioning SUCCEEDED.

Note the hostId displayed in the output. In the above example, the hostId is N6.

Server commissioning is complete when the command window displays the following:
Server Commissioning SUCCEEDED

7 Configure NTP on the newly commissioned server to synchronize the time on this server with the rest of the physical rack. See this Knowledge Base article.

8 Retrieve the IP address of the commissioned host using the hostId noted earlier.
   a On the SDDC Manager Dashboard, click View Details for Physical Resources.
   b Click the rack on which the host was commissioned.
   c Click the host corresponding to the hostId you noted down in step 6.
   d Note down the inband IP address (NETWORK TWO address on the screen).

9 Change the password on the host to the common password for ESXi hosts.
   The common password is the password that was set on all ESXi hosts when you rotated passwords on the rack after bring-up.
   a Log in to the SDDC Manager VM on the rack on which you added the new host.
   b Navigate to the /home/vrack/bin directory.
   c Stop the vrm-watchdogserver and vrm-tcserver services.
      service vrm-watchdogserver stop
      service vrm-tcserver stop
   d Type the following command:
      ./vrm-cli.sh setup-password-esx hostIP Address EvoSddc\!2016
      where hostIP Address is the IP address you noted down in step 7d.
   e Restart the vrm-watchdogserver service, which also restarts the vrm-tcserver service.
      Service vrm-watchdogserver start

10 For All-flash servers, mark each flash device on the server to be used for the capacity layer as a capacity disk using the following command.
    esxcli vsan storage tag add -d diskID -t capacityFlash

    **NOTE** Make sure that you reserve two flash devices for caching and performance.

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.

1. The decommissioned host has been re-imaged or ESXi VIBs have been installed on it. Depending on what you want to do, see Image Individual Server in VIA User’s Guide or “Install ESXi VIBs on New Host,” on page 125. If you are installing ESXi VIBs manually on a host that was not cleaned up during decommissioning, you must clean the host before installing ESXi.

2. Password on the host is EvoSddc!2016, the default password for all ESXi hosts.

3. Has an IP address from the range 192.168.100.50 - 192.168.100.73.

4. Secure Shell (SSH) is enabled.

5. Firewall on SSH host is enabled and connections are restricted to the 192.168.100.0/22 subnet.

6. DNS IP is set to 192.168.1.254.

Procedure

1. Mount the host in an empty slot on the rack and connect it to the management and ToR switches according to the wiremap. See Chapter 16, “Rack Wiring,” on page 183.

2. Power on the host.

   The management switch learns the host MAC via the DHCP request it receives from the new host. HMS learns that a new host is connected and updates its internal inventory.

3. Retrieve the IP address of the SDDC Manager VM.

   a. Log in to the vCenter Web Client.

   b. Click the SDDC Manager VM (displayed as vrm-UUID).

   c. The IP address is displayed on the right panel.

4. In a command line window, SSH to the SDDC Manager VM on the rack where you are adding the host.
5 Open the /home/vrack/VMware/vRack/server-commission.properties file and specify values for:

- **hms.host.bmc.username**
  
  For example, `hms.host.bmc.username=root`

- **hms.host.bmc.password**
  
  For example, `hms.host.bmc.password=calvin`

Do not use quotes when specifying the above values.

**NOTE** Verify that you have typed the user name and password correctly.

6 Type the following CLI command to run the Server Commission Tool:

```
sudo /home/vrack/bin/server-commission.sh
```

You need administrator credentials to run this command, and can commission one server at a time. During host commissioning, the system recognizes the new host and adds it to the inventory and the capacity pool.

The command window displays the task progress.

In `loadConfig`, loading configuration from '/home/vrack/VMware/vRack/server-commission.properties'.
In `loadConfig`, loading configuration from '/home/vrack/VMware/vRack/vrm.properties'.
In `getNewHosts`, discovering new hosts.
In `commissionServer`, discovered new host. BMC – [ IP: 192.168.0.51, MAC: 64:00:6a:c4:02:16 ].
In `getNewHostInbandIpAddress`, '192.168.100.51' is new host Inband IP address.
In `addHostKeyToKnownHosts`, SSH key for the host '192.168.100.51' added to known hosts file '/home/vrack/.ssh/known_hosts'.
In `enableCdp`, Cisco Discovery Protocol is set in 'both' mode for vSwitch: 'vSwitch0'
In `applyLicense`, license is applied.
In `addHostToHmsInventory`, new host's hostId is 'N6'.
In `refreshHmsInventory`, HMS inventory refreshed successfully.
In `addHostToPRMInventory`, adding host 'N6' to PRM inventory.
In `addHostToPrmInventory`, PRM inventory updated successfully.
In `commissionHost`, commissioning host 'N6' initiated successfully.
In `getHostCommissioningStatus`, host commissioning succeeded.
In `commissionServer`, server commissioned successfully.
In `updatePRMInventoryForServer`, successfully updated PRM Inventory.
In `commissionServer`, PRM Inventory updated after server commissioned.
In `commissionServer`, VRM Health service restarted.
Server Commissioning SUCCEEDED.

Note the `hostId` displayed in the output. In the above example, the `hostId` is N6.

Sever commissioning is complete when the command window displays the following:

Server Commissioning SUCCEEDED

7 Configure NTP on the newly commissioned server to synchronize the time on this server with the rest of the physical rack. See this [Knowledge Base article](#).

8 Retrieve the IP address of the commissioned host using the `hostId` noted earlier.

   a On the SDDC Manager Dashboard, click **Physical Resources**.

   b Click the rack on which the host was commissioned.
c Click the host corresponding to the hostId you noted down in step 6.

d Note down the inband IP address (**NETWORK TWO** address on the screen).

9 Change the password on the host to the common password for ESXi hosts.

The common password is the password that was set on all ESXi hosts when you rotated passwords on the rack after bring-up.

a Log in to the SDDC Manager VM on the rack on which you added the new host.

b Navigate to the `/home/vrack/bin` directory.

c Stop the vrm-watchdogserver and vrm-tcserver services.

```
service vrm-watchdogserver stop
service vrm-tcserver stop
```

d Type the following command:

```
./vrm-cli.sh setup-password-esx hostIP Address EvoSddc\!2016
```

where `hostIP Address` is the IP address you noted down in step 7d.

e Restart the vrm-watchdogserver service, which also restarts the vrm-tcserver service.

```
service vrm-watchdogserver start
```

The new 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** on page 114
- **Replace Dead Host or Host SAS Controller or Expander** on page 117
  
  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** on page 122
  
  This section describes the replacement procedure for a failed SATADOM disk on a host.

---

**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).

8 Pull the host out of the physical rack. Note the ports on the management and ToR switches it was connected to.

9 Service the appropriate part.

10 Put the host back in the physical rack and connect it to the management and ToR switches.

11 Power on the host.

12 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 Dead Host or SAS Controller or Expander when Host Belongs to a Workload Domain** on page 117
  
  If you need to replace a SAS controller or a SAS expander, or 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 Dead Host or SAS Controller or Expander when the Host does not Belong to a Workload Domain** on page 120

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

If you need to replace a SAS controller or a SAS expander, or 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. On the Dashboard page, click **VIEW DETAILS** for **Workload Domain** and click the affected domain.
2. Click the physical rack that contains the affected host.
3. Scroll down to the **Hosts** section.
4 In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).

![Image of SDDC Manager interface]

The Host Details page displays the details for this host.

![Image of Host Details page]

**General Info**
- **CPU:** 55176 GHz
- **MEMORY:** 384 GB
- **NETWORK ONE:** 
  - IP Address: 10.15.0.25
- **NETWORK TWO:** 
  - IP Address: 10.254.96.11

**Management Info**
- **MANAGEMENT IP ADDRESS:** 10.2.198.0.52
- **DISK UTILIZATION:** 0
- **WORKLOAD DOMAIN:** MANAGEMENT-D14-RACK2
- **RACK:** D14-RACK2
- **VCENTER SERVER:** VCENTER
- **ESX CLUSTER:** VRAK-C352XG2-01

**Storage**
- **STORAGE:** 11,658 TB
- **HDD STORAGE:** 8,747 TB
- **SSD STORAGE:** 2,917 TB
- **POWERED:** ON
5 Note the OOB IP address (management IP address).

6 Click Decommission.

![Decommission Host dialog box](image)

Deecommissioning a host can be very disruptive. If this host is part of a cluster, then please expand the cluster prior to decommissioning this host. Do you want to proceed?

- Force decommission

It is recommended that the workload domain includes a minimum of 4 nodes. If there are only 4 hosts in the workload, you should expand the domain before decommissioning a host in that domain. If you still want to proceed, click **Force decommission**.

During the host decommissioning task, the faulty host is removed from the corresponding workload domain and the environment’s available capacity is updated to reflect the reduced capacity. Data from the host is not transferred to other hosts in the workload domain, and will not be recovered after decommissioning. The host is not cleaned up after being decommissioned.

7 To watch the progress of the decommission task, click **STATUS** in the left navigation pane.

8 After the host is decommissioned, the user names and passwords are set as specified in the table below.

<table>
<thead>
<tr>
<th><strong>ESXi Credentials</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User name</strong></td>
<td>root</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>D3c0mm1ss10n3d!</td>
</tr>
</tbody>
</table>

**Note** If the decommissioned host did not belong to a workload, the password is not changed to D3c0mm1ss10n3d!. It remains the same as the password you noted down in step 1.

<table>
<thead>
<tr>
<th><strong>IPMI/BMC Credentials</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User name</strong></td>
<td>Depends on host type and vendor. This is usually root or admin.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>D3c0mm1ss10n3d!</td>
</tr>
</tbody>
</table>

9 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).

10 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,” on page 112. For adding a new host, see “Add a New Host to a Physical Rack,” on page 109.
Replace Dead Host or SAS Controller or Expander when the Host 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 SDDC Manager VM on the rack.
   b. Navigate to /home/vrack/bin.
   c. Type the following command:
      ```bash
      ./vrm-cli.sh lookup-password
      ```
   d. Note the ESXi and IPMI passwords of the host that is to be decommissioned.
2. On the Dashboard page, click VIEW DETAILS for Physical Resources and click the affected rack.
3. Scroll down to the Hosts section.
4. In the HOST column, click the host name that shows a critical status (for example, N0).
   The Host Details page displays the details for this host.

5. Note the OOB IP address (management IP address).
6 Click Decommission.

![Decommission Host](image)

6 Click Decommission Host.

Decommissioning a host can be very disruptive. If this host is part of a cluster, then please expand the cluster prior to decommissioning this host. Do you want to proceed?

- Force decommission

7 Click Force decommission.

The sever decommission task is scheduled. During this task, the host is removed from the hosts list and the environment’s available capacity is updated to reflect the reduced capacity.

8 To watch the progress of the decommission task, click STATUS in the left navigation pane.

The host is not put into maintenance mode. It is in a clean state, similar to the state it was in after imaging as it has not been used for any workload.

9 After the host is decommissioned, the user names and passwords are set as specified in the table below.

<table>
<thead>
<tr>
<th>ESXi Credentials</th>
<th>IPMI/BMC Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User name</strong></td>
<td><strong>User name</strong></td>
</tr>
<tr>
<td>root</td>
<td>Depends on host type and vendor. This is usually root or admin.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td><strong>Password</strong></td>
</tr>
<tr>
<td>Password is the same as you noted down in step 1.</td>
<td>D3c0mm1ss19n3d!</td>
</tr>
</tbody>
</table>

10 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).

11 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. See “Add a Previously Decommissioned Host to a Physical Rack,” on page 112. For adding a new host, see “Add a New Host to a Physical Rack,” on page 109.
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. On the Dashboard page, click **VIEW DETAILS** for **Workload Domain** and click the affected domain.
2. Click the physical rack that contains the affected server.
3. Scroll down to the **Hosts** section.
4 In the **HOST** column, click the host name that shows a critical status (for example, N1 in the example below).

![Image of VMware SDDC Manager](image)

The Host Details page displays the details for this host.

![Image of Host Details](image)

5 Note the IP addresses displayed in the **NETWORK TWO** and **MANAGEMENT IP ADDRESS** fields.
6 Click **Decommission**.

![Decommission Host dialog box]

Decommissioning a host can be very disruptive. If this host is part of a cluster, then please expand the cluster prior to decommissioning this host. Do you want to proceed?

- [ ] Force 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.

During the host decommissioning task, the host with the faulty SATADOM 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.

7 Monitor the progress of the decommissioning task.
   a On the SDDC Manager Dashboard, click **STATUS** in the left navigation pane.
   b In the Workflow Tasks section, click **View Details**.
   c Look for the **VI Resource Pool - Decommission of hosts** task.
   d After about 10 minutes, refresh this page and wait till the task status changes to **Successful**.

8 Power off the server.

9 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).

10 Replace the faulty SATADOM on the server and power on the server.

11 Install ESXi on the host. See “Install ESXi VIBs on New Host,” on page 125.
   - Select the SATADOM for installation.
   - Set the root password on the host to *EvoSddc!2016*.

12 Reboot the host.

13 Log in to the server with the following credentials.
   - **User name:** root
   - **Password:** *EvoSddc!2016*
14 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
     ```

15 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

16 If you were unable to remove the vSAN naa, power cycle the host and re-try step 15.

**What to do next**

Add the host back to the rack. See “Add a Previously Decommissioned Host to a Physical Rack,” on page 112.

**Install ESXi VIBs on New Host**

Follow this procedure to install ESXi VIBs on a host.

**Procedure**

1 Identify the ESXi version and build in your Cloud Foundation installation.
   a Log in to the vSphere Web Client.
   b On the left navigation panel, click an operational ESXi host.
   
   The ESXi version and build are displayed on the top in the right panel.

2 Retrieve the IP address of the SDDC Manager VM.
   a Log in to the vCenter Web Client.
   b Click the SDDC Manager VM (displayed as **vrm-UUID**).
c The IP address is displayed on the right panel.

3 In a command line window, SSH to the SDDC Manager VM on the rack where you are adding the host.

4 Navigate to `/mnt/cdrom/vcfBundle-2.1.0-4726423/vmware/esxi_image` and copy the ESXi image on a USB drive.

5 Install the ESXi image on the new host.
   

6 Set the password on the host to EvoSddc!2016.

   This is the default password of all ESXi hosts.

7 Assign an IP address to the host from the following range: 192.168.100.50 - 192.168.100.73

   where the subnet is 255.255.252.0 and gateway is 192.168.100.1.

8 Enable the Secure Shell (SSH) for the new host:
   
   a Open the vSphere Web Client.
   b Right-click Host in the VMware Host Client.
   c Click SSH Enable.

9 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
   ```

10 Set the DNS IP on the host to 192.168.1.254.
11 Depending on the controller on your new host, copy the appropriate VIB to the new host. The VIBs are located in the SDDC Manager VM.

<table>
<thead>
<tr>
<th>Controller</th>
<th>VIB Location and Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERC H730</td>
<td>/mnt/cdrom/VCF_bundle/servers/dell/vibs/lsi-mr3-6.903.85.00-10EM.600.0.0.2768847.x86_64.vib</td>
</tr>
<tr>
<td>LSI 3008</td>
<td>/mnt/cdrom/VCF_bundle/servers/quanta/vibs/d51b/lsi-msgpt3-10.00.00.00-10EM.600.0.0.2159203</td>
</tr>
<tr>
<td>LSI 2308</td>
<td>/mnt/cdrom/VCF_bundle/servers/quanta/vibs/d51b/scsi-mpt2sos-18.00.00.00.1vmw-10EM.550.0.0.1331820.x86_64.vib</td>
</tr>
<tr>
<td>HP Smart Array P840</td>
<td>/mnt/cdrom/VCF_bundle/servers/hp/vibs/scsi-hpsa_6.0.0.116-10EM.600.0.0.2494585.vib</td>
</tr>
</tbody>
</table>

12 Run the following command to install the VIB on the host.

```
esxcli software vib install --force -v pathToVIB
```
Replacing and Restoring Switches

If necessary, you can replace your Cloud Foundation installation’s network switches. Each rack in the installation has one management switch and two top-of-rack (ToR) switches. The whole installation also has two spine 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 spine switches must be from the same vendor, such as all Cisco switches or all Arista switches. Mixing and matching of switches is not supported.

This chapter includes the following topics:

- “Replace a Management Switch,” on page 129
- “Replace a Cisco Top-of-Rack or Spine Switch,” on page 132
- “Replace an Arista Top-of-Rack or Spine Switch,” on page 135

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,” on page 77. 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 mult-step process. You must perform the tasks in the order in which they are documented.

**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 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 2.5.x version of Cumulus Linux OS 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. **Set Default Boot Mode on New Management Switch**
   The default boot mode for the new management switch must be set to ONIE.

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

2. **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.
   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. Imaging fails at collect BMC-IP information task. This is expected behavior.
   8. Disconnect the switch from the laptop or management host.
Restore Backup Configuration on New Management Switch

The SoS tool takes periodic backups of the Cloud Foundation racks in your environment. After you insert the imaged management switch in the physical rack, you can restore the backup configuration on the switch.

Prerequisites

Retrieve the following files.

- Backup file of the failed management switch’s configuration. This file is named cumulus-192.168.100.1.tgz.
- The hms.tar.gz backup file of the rack on which the management switch is to be replaced.

For the location of these files within the SoS tool’s output, see Chapter 9, “Back Up Component Configurations Using the SoS Tool,” on page 107.

Procedure

1. Disconnect the management switch you are replacing and remove it from the rack.
2. Install the replacement management switch into the rack and wire it according to the same wiring connections the previous one had.
   
3. Use PuTTY to log into the management switch IP address 192.168.100.1 with username cumulus and password CumulusLinux!.
4. Add the following line to the end of the /etc/dhcp/dhcpd.config file:
   ping-check false;
   If this line already exists in the file, leave it as is.
5. Use WinSCP to copy the hms.tar.gz and cumulus-192.168.100.1.tgz files to the /home/cumulus directory of the new management switch.
6. Use PuTTY to log into the management switch IP 192.168.100.1 with username cumulus and password CumulusLinux!.
7. Type the following command.
   
   sudo su
8. Restore the backup configuration to the new switch.
   
   a. Change to the root directory.
      
      cd /
   b. Unpack the contents of the hms.tar.gz file.
      
      tar zxvf /home/cumulus/hms.tar.gz
   c. Unpack the contents of the cumulus-192.168.100.1.tgz file.
      
      tar zxvf /home/cumulus/cumulus-192.168.100.1.tgz
9. Change the password of the new management switch to the current password for your Cloud Foundation environment’s management switches, as obtained from the ./vrm-cli.sh lookup-password command.
10. Reboot the new management switch.
11 The Physical Resources > Rack Details page on the Dashboard displays a message Error loading rack details. Follow these steps to resolve this error.

a Collect the following information.

Table 11-1.

<table>
<thead>
<tr>
<th>Information Required</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDDC Manager (VRM) VM IP address</td>
<td>Log in to vSphere Web Client and note down the 192.168.x.x address for the SDDC Manager (VRM) VM</td>
</tr>
<tr>
<td>PSC IP address</td>
<td>Log in to vSphere Web Client and note down the PSC1 VM IP address</td>
</tr>
</tbody>
</table>

b Using the root account, SSH to the SDDC Manager (VRM) VM IP address 192.168.x.x.

c Run the following script with Python 2.7.

```
#/opt/vmware/bin/python2.7 /opt/vmware/evosddc-support/fru-mgmtsw.py
```

Wait for the script to complete.

12 Reboot the management switch and the SDDC Manager (VRM) VM.

### Replace a Cisco Top-of-Rack or Spine Switch

When you replace a Cisco top-of-rack (ToR) or spine 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 spine 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 spine 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 spine 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 that backups have been taken of the component configurations. If the backups have not been taken, take the backups as described in Chapter 9, “Back Up Component Configurations Using the SoS Tool,” on page 107.
- Verify you have the following items:
  - The backup file of the to-be-replaced Cisco ToR or switch’s configuration. In the set of backups taken by the SoS tool for the rack, this file is named ToR-or-spine-switch-IP-address-cisco-running-config.gz where ToR-or-spine-switch-IP-address is the switch’s IP address, such as 192.168.0.20-cisco-running-config.gz for a ToR switch with IP address of 192.168.0.20. For the location of this file within the SoS tool’s output, see Chapter 9, “Back Up Component Configurations Using the SoS Tool,” on page 107.
  - The credentials for the management switch of the rack which has the ToR or spine 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 Using the Lookup-Password Command,” on page 23.
  - 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 the Cloud Foundation VIA User’s Guide for the switch wiremaps.

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

   `scp ToR-or-spine-switch-IP-address-cisco-running-config.gz cumulus@192.168.100.1:/var/tmp`

   As an example, when replacing the Cisco ToR switch with IP address 192.168.0.20, you copy the backup configuration file named 192.168.0.20-cisco-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.

   Refer to the diagram or photo you took of the previous switch before removing it or to the wiring diagrams in the Cloud Foundation VIA User’s Guide.

4. Boot the newly installed switch.

5. Exit out of the POAP (PowerOn Auto Provisioning) mode by following the instructions in the switch console screen.

6. 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.

7. Using the original switch’s IP address, configure that same IP address with subnet mask /24 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 spine 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
8 Verify the newly installed switch can reach the management switch (at IP 192.168.100.1) by using the `ping` command.

```
switch(config)# ping 192.168.100.1 vrf management
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
...
```

9 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 Step 1.

As an example, when replacing the Cisco ToR switch that has the backup configuration file named `192.168.0.20-cisco-running-config.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/192.168.0.20-cisco-running-config.gz
Enter hostname for the scp server: 192.168.100.1
Enter username: cumulus
cumulus@192.168.100.1's password: 
192.168.0.20-cisco-running-config.gz 100% 1891 1.9KB/s 00:00
Copy complete, now saving to disk (please wait)...
```

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

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

11 Decompress the copied backup configuration file.

Using the example from the previous step:

```
switch(config)# gunzip bootflash:///192.168.0.20-cisco-running-config.gz
```

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

12 Install the backup configuration into the new switch's startup configuration:

Using the example from the previous step:

```
switch(config)# copy 192.168.0.20-cisco-running-config startup-configuration
```

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

Using the example from the previous step:

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

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

**Note**  Restoring the configuration to the new switch also restores the admin password.

**What to do next**

Verify the new switch is operating correctly by seeing if all hosts and virtual machines are reachable from both ToR switches or both spine switches, depending on which type you replaced.
Replace an Arista Top-of-Rack or Spine Switch

When you replace an Arista top-of-rack (ToR) or spine 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 spine 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 spine 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 spine 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 that backups have been taken of the component configurations. If the backups have not been taken, take the backups as described in Chapter 9, “Back Up Component Configurations Using the SoS Tool,” on page 107.
- Verify you have the following items:
  - The backup file of the to-be-replaced Arista ToR or switch's configuration. In the set of backups taken by the SoS tool for the rack, this file is named ToR-or-spine-switch-IP-address-arista-running-config.gz where ToR-or-spine-switch-IP-address is the switch's IP address, such as 192.168.0.20-arista-running-config.gz for a ToR switch with IP address of 192.168.0.20. For the location of this file within the SoS tool's output, see Chapter 9, “Back Up Component Configurations Using the SoS Tool,” on page 107.
  - The credentials for the management switch of the rack which has the ToR or spine 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 Using the Lookup-Password Command,” on page 23.
  - 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 the Cloud Foundation VIA User’s Guide for the switch wiremaps.
  - 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 ToR-or-spine-switch-IP-address-arista-running-config.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.

   Refer to the diagram or photo you took of the previous switch before removing it or to the wiring diagrams in the Cloud Foundation VIA User’s Guide.
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 with subnet mask /24 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 spine 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 `192.168.0.20-arista-running-config.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:cumulus@192.168.100.1/var/tmp/192.168.0.20-arista-running-config.gz flash:/ 192.168.0.20-arista-running-config.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 192.168.0.20-arista-running-config.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: 192.168.0.20-arista-running-config startup-config

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

AristaSwitch# copy startup-config running-config

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

**What to do next**

Verify the new switch is operating correctly by seeing if all hosts and virtual machines are reachable from both ToR switches or both spine switches, depending on which type you replaced.
The SDDC Manager client’s Licensing screen provides a way to manage your Cloud Foundation licenses. The Licensing screen is available from the Settings page in the SDDC Manager client.

This chapter includes the following topics:

- “Cloud Foundation Licensing Model,” on page 139
- “Manage License Keys for the Software in Your Cloud Foundation Environment,” on page 140

**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 Virtual SAN
- VMware NSX for vSphere

The following VMware software deployed by SDDC Manager is licensed separately:

- VMware vCenter Server
- VMware vRealize Log Insight
- VMware vRealize Operations
- Content packs for Log Insight
- Management packs for vRealize Operations
- VMware Horizon 6
- VMware App Volumes

**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 installation are licensed using the base Cloud Foundation license.
Manage License Keys for the Software in Your Cloud Foundation Environment

Use the Licensing screen of the SDDC Manager client to work with the Cloud Foundation license keys.

In the Licensing screen, you can:

- Review the license keys that are currently assigned in your installation.
- Enter license keys.
- Edit the descriptions of the assigned license keys. The descriptions are displayed in the Licensing screen.
- Remove license keys.

Procedure

◆ Manage the license keys using the action menus in the screen.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a license key by clicking Actions &gt; Add License Key.</td>
<td>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.</td>
</tr>
<tr>
<td>Edit the description of an already entered license key by clicking the Edit choice in the action menu next to that license key.</td>
<td>In the Add License window, edit the description and save your changes.</td>
</tr>
<tr>
<td>Remove a license key from use by clicking the Delete choice in the action menu next to that license key.</td>
<td>Confirm the action to remove the license key from use by this environment.</td>
</tr>
</tbody>
</table>
Power Off a Dual-Rack Cloud Foundation Environment and Power It Back On

You might have situations in which you want to power off the environment and power it back on. In such situations, you must use a specific sequence to power off the virtual machines, ESXi hosts, and switches and subsequently power them on.

You power off the VMs in the secondary racks management domain first, in a prescribed sequence, and then power off the rack’s ESXi hosts. You then power off the VMs in the primary rack’s management domain, in a prescribed sequence, and ESXi hosts in the primary rack. Then the ToR switches, followed by the spine switches. You power down the management switches last.

When powering the environment back on, you power on the switches in the primary rack first, followed by the primary rack’s ESXi hosts and VMs, and then power on the switches in the secondary rack, followed by its ESXi hosts and VMs.

Prerequisites

Ensure you have the root account credentials to log in to the ESXi hosts and to the switches’ operating systems for those hardware components in your environment. For the steps to look up the credentials, see “Look Up Account Credentials Using the Lookup-Password Command,” on page 23.

Ensure you have the FQDNs for the ESXi hosts in each rack. Each ESXi host has an FQDN that starts with the rack identifier, followed by the subdomain and root DNS domain used by the environment, such as rack-1-n0.subdomain.root-domain, rack-1-n1.subdomain.root-domain, rack-2-n0.subdomain.root-domain, and so on:

- rack-1-n0.subdomain.root-domain is the ESXi host N0 in the primary rack
- rack-1-n1.subdomain.root-domain is the ESXi host N1 in the primary rack
- rack-2-n0.subdomain.root-domain is the ESXi host N0 in the secondary rack
- rack-2-n1.subdomain.root-domain is the ESXi host N1 in the secondary rack

Ensure you know which ESXi hosts are the ones used by each rack’s management domain. You can see the hosts that are used by a management domain by navigating to its domain details page in the SDDC Manager client. Write down the FQDNs of the hosts used by the primary rack’s management domain and the FQDNs used by the second rack’s management domain. You will use this information to locate the management domain’s VMs in the powering-on procedures.

Procedure

1. **Power Off the Second Rack’s VMs and Hosts** on page 142

   You power off the second rack first. You first power off the rack’s management domain’s virtual machines in a specific sequence, and then the rack’s ESXi hosts.
2 Power Off the Primary Rack’s VMs and Hosts on page 143
   After powering off the secondary rack, you power down the primary rack’s management domain's virtual machines in a specific sequence, and then the rack’s ESXi hosts.

3 Power Down Switches on page 145
   After powering down the primary rack, you power down all of the switches in a prescribed sequence.

4 Power On the Primary Rack’s Hosts and VMs on page 145
   You power on all of the switches in the dual-rack installation first. Then you power on the primary rack starting with its ESXi hosts, followed by its management domain’s virtual machines in a specific sequence.

5 Power On the Secondary Rack’s Hosts and VMs on page 146
   After powering on the primary rack’s management domain, you power on the second rack starting with its ESXi hosts, followed by its management domain’s virtual machines in a specific sequence.

What to do next
   After both rack’s management domain’s VMs are up and running, you can power on the VMs for the VI and VDI workload domains in the environment.

Power Off the Second Rack’s VMs and Hosts
   You power off the second rack first. You first power off the rack’s management domain’s virtual machines in a specific sequence, and then the rack’s ESXi hosts.

Prerequisites
   Verify you have met the prerequisites described in Chapter 13, “Power Off a Dual-Rack Cloud Foundation Environment and Power It Back On,” on page 141.

Procedure
   1 Launch the vSphere Web Client to the vCenter Server instance for the second rack’s management domain.
      a In the SDDC Manager client, open the domain details for the second rack’s management domain.
      b Click the launch link for the vCenter Server instance that is displayed in the domain details window for that management domain.
         A new browser tab opens and displays the vSphere Web Client.
   2 In the vSphere Web Client, locate the VMs for the second rack’s management domain.
      a Navigate to the Hosts and Clusters view.
      b In the left hand navigation for the Hosts and Clusters view, expand the cluster that has the name beginning with rack-2-vc-1 until you see that cluster’s VMs.
   3 Power off these VMs in that cluster whose name begins with rack-2-vc-1 in the following sequence, making sure that each VM’s console is completely shut down before powering off the next VM.

   ![NOTE](For each VM, verify that it is the one in the second rack’s management domain by looking at its Summary tab in the vSphere Web Client and verifying that its DNS name begins with rack-2-.)

   - The three NSX controllers
   - The vRealize Operations Manager instance
   - The NSX Manager instance
   - The SDDC Manager instance for the second rack’s management domain
4 In the vSphere Web Client, use the vCenter Server instance’s Summary tab to determine which ESXi host that VM is running on.
This vCenter Server instance has the DNS name beginning with rack-2-vc-1.

5 Use the vSphere Web Client to locate the IP address for that ESXi host.

6 Using the ESXi host’s IP address in the URL for the VMware Host Client, open the login screen for the VMware Host Client.
The URL to open the VMware Host Client to that ESXi host has the form https://esxi-host-ip/ui/.

7 Log in to the VMware Host Client using the ESXi host’s root account credentials.

8 In the VMware Host Client, navigate to see the vCenter Server instance whose name begins with rack-2-vc-1.

9 Power off that vCenter Server instance.

10 Log out of the VMware Host Client.

11 Open the VMware Host Client to the second rack’s N0 ESXi host, using that host’s FQDN in the browser: https://rack-2-N0.subdomain.root-domain/ui/, where subdomain and root-domain are the ones for your Cloud Foundation environment.

12 Log in to the VMware Host Client using the host’s root account credentials.

13 In the VMware Host Client, power off that ESXi host by right-clicking Host and clicking Shut down.

14 In sequence, repeat steps Step 11 through Step 13 to shut down the remaining ESXi hosts in the second rack: N1, N2, N3, and so on.

**Power Off the Primary Rack’s VMs and Hosts**

After powering off the secondary rack, you power down the primary rack’s management domain’s virtual machines in a specific sequence, and then the rack’s ESXi hosts.

**Prerequisites**

Verify you have met the prerequisites described in Chapter 13, “Power Off a Dual-Rack Cloud Foundation Environment and Power It Back On,” on page 141.

**Procedure**

1 Launch the vSphere Web Client to the vCenter Server instance for the primary rack’s management domain.
   a In the SDDC Manager client, open the domain details for the primary rack’s management domain.
   b Click the launch link (launch) for the vCenter Server instance that is displayed in the domain details window for that management domain.
      A new browser tab opens and displays the vSphere Web Client.

2 In the vSphere Web Client, locate the VMs for the primary rack’s management domain.
   a Navigate to the Hosts and Clusters view.
   b In the left hand navigation for the Hosts and Clusters view, expand the cluster that has the name beginning with rack-1-vc-1 until you see that cluster’s VMs.
3 Power off these VMs in that cluster whose name begins with rack-1-vc-1 in the following sequence, making sure that each VM's console is completely shut down before powering off the next VM.

**NOTE** For most of these VMs, you can verify that it is the one in the primary rack's management domain by looking at its Summary tab in the vSphere Web Client and verifying that its DNS name begins with rack-1-.

- The VM whose name contains LCM_Backup_Repository
- The three NSX controllers
- The vRealize Operations Manager instance
- The vRealize Log Insight instance
- The NSX Manager instance
- The VM whose name contains LCM_Repository
- The SDDC Manager instance for the primary rack's management domain
- The three ISVM VMs, the ones whose names contain ISVM-1, ISVM-2, ISVM-3.

4 In the vSphere Web Client, use the virtual machines' Summary tabs to determine on which ESXi hosts the vCenter Server VM and the two Platform Services Controller VMs are running.

- The vCenter Server instance has the DNS name beginning with rack-1-vc-1.
- The Platform Services Controller instances have DNS names beginning with rack-1-psc-1 and rack-1-psc-2.

5 Use the vSphere Web Client to locate the IP address for those ESXi hosts.

6 To power off the vCenter Server instance, use the vSphere Host Client to log in to the ESXi host on which the instance is running and power it down.

   a Use IP address of the host on which the vCenter Server instance is running in the browser URL for the VMware Host Client.

   The URL has the form https://esxi-host-ip/.

   b Log in to the VMware Host Client using the ESXi host's root account credentials.

   c In the VMware Host Client, navigate to see the vCenter Server instance whose name begins with rack-2-vc-1.

   d Power off that vCenter Server instance.

   e If any of the two Platform Service Controller instances is also on this ESXi host, power off that instance.

   f Log out of the VMware Host Client.

7 To power off the Platform Service Controller instances, repeat step Step 6 and its substeps to log in to the hosts on which those instances are running and power the VMs off.

8 Open the VMware Host Client to the primary rack's N0 ESXi host, using that host's FQDN in the browser: https://rack-1-N0.subdomain.root-domain/ui/, where subdomain and root-domain are the ones for your Cloud Foundation environment.

9 Log in to the VMware Host Client using the host's root account credentials.

10 In the VMware Host Client, power off that ESXi host by right-clicking Host and clicking Shut down.

11 In sequence, repeat steps Step 8 through Step 10 to shut down the remaining ESXi hosts in the primary rack: N1, N2, N3, and so on.
Power Down Switches

After powering down the primary rack, you power down all of the switches in a prescribed sequence.

Procedure

1. Power down the ToR switches in each rack.
2. Power down the spine switches in the second rack.
   Only the second rack in a Cloud Foundation installation has the two spine switches.
3. Power down the management switches in each rack.

Power On the Primary Rack's Hosts and VMs

You power on all of the switches in the dual-rack installation first. Then you power on the primary rack starting with its ESXi hosts, followed by its management domain's virtual machines in a specific sequence.

Prerequisites

Verify you have met the prerequisites described in Chapter 13, “Power Off a Dual-Rack Cloud Foundation Environment and Power It Back On,” on page 141.

Procedure

1. Power on all of the switches in both racks using the following sequence.
   a. Power on the spine switches.
   b. Power on the ToR switches in both racks.
   c. Power on the management switches in both racks.
2. Power on all of the primary rack's ESXi hosts in the order of N0, N1, N2, and so on.
3. Log in to each of the management domain's four ESXi hosts using the VMware Host Client and the account credentials for the hosts.

You log in to an ESXi host using the VMware Host Client by pointing a browser to the URL of the form https://host-FQDN/ui/ or https://host-IP-address/ui/, where host-FQDN is the FQDN for the host and host-IP-address is the host's IP address.

4. For each VM in the following sequence, use the Power on action in the VMware Host Client to power on the VM.

   **Note** For most of these VMs, you can verify that it is the one in the primary rack's management domain by looking at its Summary tab in the vSphere Web Client and verifying that its DNS name begins with rack-1-.

   - The two Platform Services Controller instances whose DNS names start with rack-1-psc-1 and rack-1-psc-2.
   - The vCenter Server instance whose DNS name starts with rack-1-vc-1.
   - The SDDC Manager instance whose DNS name starts with rack-1-vrm-1.
   - The VM whose name contains ISVM-1
   - The VM whose name contains ISVM-2
   - The VM whose name contains ISVM-3
   - The VM whose name contains LCM_Repository
The NSX Manager instance whose DNS name starts with rack-1-nsxmanager-1.

The vRealize Log Insight instance whose DNS name starts with rack-1-li-1.

The vRealize Operations Manager instance whose DNS name starts with rack-1-vrops-1.

The NSX Controller instance whose DNS name starts with rack-1-nsxctlr-1

The NSX Controller instance whose DNS name starts with rack-1-nsxctlr-2

The NSX Controller instance whose DNS name starts with rack-1-nsxctlr-3

The VM whose name contains LCM_Backup_Repository

**Note**: After the VMs for the primary rack’s management domain are up, but before the second rack is powered on, the web interfaces to the vCenter Server instance, vRealize Log Insight instance, vRealize Operations Manager instance are partially accessible. They will be fully accessible after you power on the second rack.

**Power On the Secondary Rack’s Hosts and VMs**

After powering on the primary rack’s management domain, you power on the second rack starting with its ESXi hosts, followed by its management domain’s virtual machines in a specific sequence.

**Prerequisites**

Verify you have met the prerequisites described in Chapter 13, “Power Off a Dual-Rack Cloud Foundation Environment and Power It Back On,” on page 141.

**Procedure**

1. Power on all of the second rack’s ESXi hosts in the order of N0, N1, N2, and so on.

2. Log in to each of the management domain’s four ESXi hosts using the VMware Host Client and the account credentials for the hosts.

   You log in to an ESXi host using the VMware Host Client by pointing a browser to the URL of the form https://host-FQDN/ui/ or https://host-IP-address/ui/, where host-FQDN is the FQDN for the host and host-IP-address is the host’s IP address.

3. For each VM in the following sequence, use the **Power on** action in the VMware Host Client to power on the VM.

   **Note**: For each VM, you can verify that it is the one in the second rack’s management domain by looking at its Summary tab in the vSphere Web Client and verifying that its DNS name begins with rack-2-.

   - The SDDC Manager instance whose DNS name starts with rack-2-vrm-1.
   - The vCenter Server instance whose DNS name starts with rack-2-vc-1.
   - The vRealize Operations Manager instance whose DNS name starts with rack-2-vrops-1.
   - The NSX Manager instance whose DNS name starts with rack-2-nsxmanager-1.
   - The NSX Controller instance whose DNS name starts with rack-2-nsxctlr-1
   - The NSX Controller instance whose DNS name starts with rack-2-nsxctlr-2
   - The NSX Controller instance whose DNS name starts with rack-2-nsxctlr-3
What to do next

After both racks are powered on, power on the virtual machines used for the VI and VDI workload domains. You can see all of those virtual machines by using the vSphere Web Client to log in to the primary rack's management domain's vCenter Server instance.
Lifecycle Management (LCM) enables you to perform automated updates on Cloud Foundation components (SDDC Manager, HMS, and LCM) as well as VMware components (vCenter Server, ESXi, and NSX).

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.

This section describes generic patching and upgrading. For information on upgrading to Cloud Foundation 2.1 or 2.1.1, see Chapter 15, “Upgrade Cloud Foundation to 2.1 or 2.1.1,” on page 167.

This chapter includes the following topics:

- “Before you Upgrade VMware Software,” on page 149
- “Save VMware Account Credentials,” on page 151
- “Use a Proxy Server to Download Upgrade Bundles,” on page 152
- “Download Update Bundle,” on page 153
- “Select Targets and Schedule Update,” on page 156
- “View Inventory Component Versions,” on page 163
- “Display Backup Locations,” on page 165

**Before you Upgrade VMware Software**

Ensure that the prerequisites in each section are met before you begin a VMware software upgrade.

**Domain Operations**

Verify that no other domain operations are running. See “Managing Workflows and Tasks,” on page 76.

**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.

3 Back up the ESXi configuration.
   a Using the root account, SSH in to the SDDC Manager VM.
   b Type the following command:
   
   ./sos --backup

   The backup is stored in the /var/tmp directory.

**NSX Prerequisites**

1 Back up the NSX configuration. See “Back up NSX Data,” on page 150.

2 If you are upgrading a workload domain, 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**.

**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/vrmcli.sh --lookup-password

3 Note down the values for the following.

   - IP address for EVO-Rack_LCM_Backup_Repository-<uuid> VM that resides in the management domain vCenter
   - 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP/Hostname</td>
<td>IP address that you noted in step 3.</td>
</tr>
<tr>
<td>Transfer Protocol</td>
<td>SFTP</td>
</tr>
<tr>
<td>Port</td>
<td>22</td>
</tr>
<tr>
<td>Username</td>
<td>Username that you noted in step 3.</td>
</tr>
<tr>
<td>Password</td>
<td>Password that you noted in step 3.</td>
</tr>
<tr>
<td>Backup Directory</td>
<td>/backup</td>
</tr>
</tbody>
</table>
### Setting | Value
--- | ---
Filename Prefix | nsx_type_domain-number
For example, type nsx_mgmt_dmn01 when taking a backup of the NSX management domain. Type nsx_vdi_dmn01 when taking a VDI domain backup.
Passphrase | nsxmgr_backup

**Save VMware Account Credentials**

You must sign in to your VMware account so that LCM can access update bundles from the VMware depot.

If you do not have external connectivity on the rack, see “Use a Proxy Server to Download Upgrade Bundles,” on page 152.

**Procedure**

1. In the SDDC Manager web interface, click **LIFECYCLE** on the left navigation pane.

   The Lifecycle Management page appears with a message saying that the VMware depot user has not been set.
2. Click **my vmware** on the top right corner.

   The sign in page appears.

3. Type your VMware account user name and password.

4. Click **SIGN IN**.

   The top right corner of the window displays a green check mark.

**What to do next**

To change account credentials, click **my vmware** on the top right corner and type in the appropriate credentials.

**Use a Proxy Server to Download Upgrade Bundles**

If you do not have external connectivity on a rack, you can use a proxy server to download the LCM update bundles.

**Procedure**

1. Using the root account, SSH to the rack's SDDC Manager VM.

2. Open the `/home/vrack/lcm/lcm-app/conf/application-prod.properties` file.

3. 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
   ```

4. Restart the LCM server by typing the following command:

   ```
   service lcm-init restart
   ```

5. Wait for 5 minutes and then proceed to the next step.
Download Update Bundle

When an update bundle is available, a notification is displayed on the SDDC Manager dashboard. You can view the available updates and determine the update bundle that you want to download. The downloaded bundle is then available in the bundle repository.

Prerequisites
Sync the laptop where you are running the SDDC Manager client with the SDDC Manager NTP server.

Procedure

1. Do one of the following:
   - Click the bundle notification on the SDDC Manager dashboard.
   - In the SDDC Manager web interface, click LIFECYCLE on the left navigation pane.

   The number of available updates is displayed next to the title of the REPOSITORY tab. The window is refreshed every 3 minutes to display the latest bundles on the SFTP server.

2. Click the Cloud Foundation drop-down to see the available updates for Cloud Foundation components and the VMware Software Update drop-down to see vCenter Server and ESXi updates.
Since this tab mirrors the depot, all bundles may be displayed here independent of the version in your environment. However, the Download link will be enabled only for the bundles appropriate to your environment.

To view the metadata details for an update bundle, click MORE next to the release date of the bundle. The bundle severity levels are described in the table below.

<table>
<thead>
<tr>
<th>Severity Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>A problem which may severely impact your production systems (including the loss of production data). Such impacts could be system down or HA not functioning. A workaround is not in place.</td>
</tr>
<tr>
<td>Important</td>
<td>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.</td>
</tr>
<tr>
<td>Moderate</td>
<td>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.</td>
</tr>
<tr>
<td>Low</td>
<td>A problem is considered 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.</td>
</tr>
</tbody>
</table>

You can filter bundles by status.

3 Do one of the following:

- Click **DOWNLOAD** to download the bundle right away.
- Click **next to DOWNLOAD to schedule the download. Select the date and time and then click **SCHEDULE**.
On the Review Download page, review the download schedule for the bundle. If the scheduled download has a dependency on other bundles, those downloads are automatically scheduled for download before the bundle you selected to download. For example, if there are update bundles available that have a release date prior to the one you are downloading, those bundles are force downloaded along with the bundle you selected.

The Review Download page also displays the total bundle size (bundle you selected to download as well as dependent bundles that need to be force downloaded).

Click **DOWNLOAD**.

The status bar next to the bundle name shows the progress update. For bundles scheduled to be downloaded at a later time, the time remaining for the download to begin is displayed.

When the bundle is downloaded, the term **DOWNLOADED** is displayed next to the bundle.
If the download fails, possible errors may be recoverable or unrecoverable. For a recoverable error, you can resolve the problem and then click RETRY DOWNLOAD. For example, the OOB agent for HMS may be down while you are downloading an SDDC Manager software update. After you restart the OOB agent, you can click RETRY DOWNLOAD.

For an unrecoverable error, you can view failure details by clicking VIEW DETAILS.

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.

![VMware Cloud Foundation Update](image)

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.
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.
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 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.
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.
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.
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 ![icon] to the right of the component name and then click GET BACKUP LOCATION.
   The backup file name and location is displayed.
Upgrade Cloud Foundation to 2.1 or 2.1.1

Table 15-1. Upgrade Matrix

<table>
<thead>
<tr>
<th>Current Version</th>
<th>Target Version</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>2.1</td>
<td>&quot;Upgrade Cloud Foundation to 2.1,&quot; on page 168</td>
</tr>
<tr>
<td>2.0</td>
<td>2.1.1</td>
<td>1 &quot;Upgrade Cloud Foundation to 2.1,&quot; on page 168</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 &quot;Upgrade Cloud Foundation 2.1 to 2.1.1,&quot; on page 176</td>
</tr>
<tr>
<td>2.1</td>
<td>2.11</td>
<td>&quot;Upgrade Cloud Foundation 2.1 to 2.1.1,&quot; on page 176</td>
</tr>
</tbody>
</table>

Prerequisites

- Ensure that vendor supported firmware and BIOS versions conform to the VMware software versions. Refer to vendor documentation.
- Before starting the upgrade, take a snapshot of all Cloud Foundation VMs - SDDC Manager VM (VRM), ISVMs, LCM VM, and LCM-Backup-Repository VM.
- During the upgrade process, Lifecycle Management takes the following backups:
  - PSC VM snapshot
  - vCenter VM snapshot
  - ESXi configuration backup.
    - Backup directory on LCM-Backup-Repository VM is /backup/1cm/ESX. Backup for each ESXi host is stored in its guid (stored in VCF database). Each backup is in a date sub folder. An example ESXi backup file name is /backup/1cm/ESX/f32b407e-8fdb-4999-ab80-2082003586fb/02/02/2017/backup/firmwareConfig865759412960483871.tgz.
  - NSX configuration backup. Backup directory on LCM-Backup-Repository VM is /backup. File names have the prefix evo–nsx–domain_id_date. An example NSX backup file name is /backup/evo–nsx–888bcb7f–30d0–3aee–9291–b7777052a1ac–01_00_00_Tue07Feb2017.
    - To access the backup directory, login to the LCM-Backup-Repository VM as root. See “Look Up Account Credentials Using the Lookup-Password Command,” on page 23.
- For best practise information, refer to the documentation for individual VMware products.

This chapter includes the following topics:

- "Upgrade Cloud Foundation to 2.1," on page 168
- "Upgrade Cloud Foundation 2.1 to 2.1.1," on page 176
Upgrade Cloud Foundation to 2.1

In a multi-rack scenario, the Cloud Foundation version must be the same on all racks. Therefore, if you are planning to add a new rack to your setup, you must first upgrade rack 1 to the latest version before adding the new rack to your environment.

Upgrading Cloud Foundation is a multi-step process. You must follow each step in the order in which it is documented.

1 Upgrade Cloud Foundation Software on Management Domain on page 168
   You begin by upgrading the VMware Cloud Foundation software on the management domain.

2 Upgrade ISVMs on Rack 1 on page 173
   Upgrade the ISVMs on rack 1.

3 Upgrade Third Party Software on page 175
   The third party upgrade script is part of the Cloud Foundation bundle and is located in the SDDC Manager VM.

4 Upgrade VMware Software on Management Domain on page 175
   Applying the VMware software bundle upgrades the VMware software that is part of Cloud Foundation software.

5 Upgrade VMware Software on VDI and VI Domains on page 175
   Upgrade VMware software on the other domains in your environment. It is recommended that you upgrade one domain at a time.

Upgrade Cloud Foundation Software on Management Domain

You begin by upgrading the VMware Cloud Foundation software on the management domain.

Prerequisites

1 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.

2 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 Save VMware account credentials. See “Save VMware Account Credentials,” on page 151.

2 Follow steps in https://kb.vmware.com/kb/2148568.

3 Download all available update bundles. See “Download Update Bundle,” on page 153.

4 On the Lifecycle Management page, click the UPDATES tab.
   The number of available updates is displayed next to the title of the UPDATE tab.

5 Click the drop-down next to Available Updates.

6 Click the UPDATE button next to the VMware Cloud Foundation update.
   On the TARGET page, the management domain is selected by default.

7 Click NEXT.
8 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.

![Select Update Schedule](image)

**NOTE** Do not reboot the physical racks, any devices on the rack, or the SDDC Manager VM while the upgrade is in progress.

9 Click NEXT.

10 On the Review Update page, review the update bundle, targets, and schedule.
11 Click **SCHEDULE UPDATE**.
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.

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.
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.
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.

Update the cacerts file that contains the VMware Depot certificate. See https://kb.vmware.com/kb/2148926.

Upgrade ISVMs on Rack 1

Upgrade the ISVMs on rack 1.

Prerequisites

- The Infrastructure VMs Anti-Affinity rule is deleted during the ISVM upgrade. Note the rule details before upgrading the ISVMs so that you can re-create the rule after the upgrade.
  a. Login to the vCenter Server.
  b. In the left navigation pane, right-click the cluster and click Edit Setting.
  c. In the left navigation pane, click Rules.
  d. Note the details of the Infrastructure VMs Anti-Affinity rule.
- Ping the ISVMs to ensure they are accessible.
**Procedure**

1. This step is required only in a multi-rack scenario. In a single rack scenario, the ISVM upgrade scripts stop the services so you can proceed to step 2.

   Stop SDDC Manager and LCM services on each additional rack.
   a. Using the root account, SSH to the 192.168.* IP address of the SDDC Manager VM on each additional rack.
   b. Type the following commands.
      - `service vrm-watchdogserver stop`
      - `service vrm-tcserver stop`
      - `service lcm-watchdogserver stop`
      - `service lcm-init stop`

      Leave this console window open.

2. This step is required only if you skipped step 1 (in a single-rack scenario).

   Using the root account, SSH to the 192.168.* IP address for the SDDC Manager VM on rack 1.

3. Type the following.
   - `ls /home/vrack/lcm/upgrade`
   - Note the upgrade ID displayed.

4. Navigate to the following directory. `upgrade_id` is the upgrade ID you noted in step 3.
   - `/home/vrack/lcm/upgrade/vrm/upgrade_id/vrm-upgrade-rtp3-vcfr0/isvm/scripts/`

5. Run the following command to update the `isvm-upgrade.conf` file.
   - `python isvm_upgrade_autoconf.py > isvm-upgrade.conf`

6. Run the following command to upgrade the ISVMs.
   - `./isvm-upgrade.sh vm-upgrade isvm-upgrade.conf ../ova/EVO-RACK-ISVM-Appliance-Version.ova 2>&1 | tee update.log`

   After the ISVM upgrade is complete, the following message is displayed in the console window.

   *** Done upgrading ISVMs ***

   If the ISVM cluster is functioning correctly, you can delete backup ISVMs. Their names end with `-isvm-upgrade-backup`.

   If you see an error, rollback the ISVM.

   Contact VMware Support and fix the error before proceeding with the upgrade. Your current environment will be functional even though the upgrade has not been completed.

7. Click Control + C to exit the command window.

8. For a multi-rack scenario, go back to the console window you had left open in step 1 and restart the SDDC Manager and LCM services.
   - `service vrm-watchdogserver start`
   - `service vrm-tcserver start`
   - `service lcm-watchdogserver start`
   - `service lcm-init start`

9. Re-create the Infrastructure VMs Anti-Affinity rule.
Upgrade Third Party Software

The third party upgrade script is part of the Cloud Foundation bundle and is located in the SDDC Manager VM.

Procedure
1. Using the root account, SSH to the 192.168.* IP address of the SDDC Manager VM on rack 1.
2. Navigate to the following directory:
   
   /home/vrack/lcm/upgrade/vrm/

   /vrm-upgrade-rtp3-vcfr0/ova_packages/

3. Run the 3rd party upgrade script:

   ./ova_packages_upgrade.sh ALL

4. In a multi-rack scenario, follow steps 1 and 2 on each additional rack and then run the following command:

   ./ova_packages_upgrade.sh VRM

Upgrade VMware Software on Management Domain

Applying the VMware software bundle upgrades the VMware software that is part of Cloud Foundation software.

Prerequisites

The VMware software bundle must be available in the local repository.

Procedure
1. Apply the workaround described in VMware Cloud Foundation 2.1.1 update bundle fails to download.
2. On the Lifecycle Management page on the SDDC Manager Dashboard, click the UPDATES tab.
3. Click the drop-down next to Available Updates.
4. Click the UPDATE button next to the VMware Software update.

   On the TARGET page, the management domain is selected by default.

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.
9. Click SCHEDULE UPDATE.

Upgrade VMware Software on VDI and VI Domains

Upgrade VMware software on the other domains in your environment. It is recommended that you upgrade one domain at a time.

Prerequisites

The VMware software bundle must be available in the local repository.
**Procedure**

1. 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.

2. On the Lifecycle Management page, click the UPDATES tab.

3. Click the drop-down next to Available Updates.

4. Click the UPDATE button next to the VMware Software update.
   
   On the TARGET page, the management domain is selected by default.

5. On the TARGET page, select the appropriate VDI and VI domains.

6. Click NEXT.

7. 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.

8. Click NEXT.

9. On the Review Update page, review the update bundle, targets, and schedule.

10. Click SCHEDULE UPDATE.

11. Enable the anti-affinity rule that separates NSX controllers across hosts.

**Upgrade Cloud Foundation 2.1 to 2.1.1**

You can upgrade to Cloud Foundation 2.1.1 only if you are at Cloud Foundation 2.1. If your environment includes a Cloud Foundation version prior to 2.1, you must first upgrade to 2.1 and then upgrade to 2.1.1.

**Procedure**

1. Save VMware account credentials. See “Save VMware Account Credentials,” on page 151.

2. Follow the steps in https://kb.vmware.com/kb/2148653.


4. On the Lifecycle Management page, click the UPDATES tab.
   
   The number of available updates is displayed next to the title of the UPDATE tab.

5. Click the drop-down next to Available Updates.

6. Click the UPDATE button next to the VMware Cloud Foundation update.
   
   On the TARGET page, the management domain is selected by default.

7. Click NEXT.

8. 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.
Do not reboot the physical racks, any devices on the rack, or the SDDC Manager VM while the upgrade is in progress.

9. Click NEXT.

10. On the Review Update page, review the update bundle, targets, and schedule.
11 Click SCHEDULE UPDATE.
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.

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.
Third party software is upgraded as part of Cloud Foundation software upgrade.

12 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.
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.
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.
Wiring for Rack with Dell Management Switch

Figure 16-1. Wiremap for rack 1 with Cisco ToR Switches and Dell Management Switch
Figure 16-2. Wiremap for rack 2 with Cisco ToR Switches and Dell Management Switch

Jump VM

Private Managed Switch

Spine 2

Spine 1

ToR 2

ToR 1

Management switch

16 switch serial console switch. For Connections, see port connectivity table

Management port

Management port

Management port

Management port

Corporate network

Corporate network

Corporate network

Management port
Wiring for Rack with Quanta Management Switch

Figure 16-3. Wiremap for rack 1 with Cisco ToR Switches and Quanta Management Switch

- Jump VM
- Private Managed Switch
- 16 switch serial console switch. For Connections, see port connectivity table

ToR 2
- Spine 2 on Rack 2
- Node 1
- Node 13
- 49
- Corporate network
- Management port

ToR 1
- Spine 1 on Rack 2
- Node 1
- Node 13
- 49
- Corporate network
- Management port

Management switch
- Node 1
- 11
- 23
- 35
- 41
- 49
- Management port

Node 2
- Node 2
- Node 12
- Node 24
- 26
- 40
- 48
- Corporate network
- Management port
Figure 16-4. Wiremap for rack 2 with Cisco ToR Switches and Quanta Management Switch

Jump VM

Private Managed Switch

16 switch serial console switch. For Connections, see port connectivity table

Management port

Spine 2

Management port

Spine 1

Management port

ToR 2

Management port

ToR 1

Management port

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

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Connects To</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Management switch console port</td>
</tr>
<tr>
<td>2</td>
<td>ToR 1 console port</td>
</tr>
<tr>
<td>3</td>
<td>ToR 2 console port</td>
</tr>
</tbody>
</table>
## Spine 2 (Rack 2 only)

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Speed</th>
<th>Connects To</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>40 Gbps</td>
<td>Rack 2 ToR 1 port 50</td>
</tr>
<tr>
<td>2</td>
<td>40 Gbps</td>
<td>Rack 2 ToR 2 port 50</td>
</tr>
<tr>
<td>3</td>
<td>40 Gbps</td>
<td>Rack 1 ToR 1 port 50</td>
</tr>
<tr>
<td>4</td>
<td>40 Gbps</td>
<td>Rack 1 ToR 2 port 50</td>
</tr>
<tr>
<td>5</td>
<td>40 Gbps</td>
<td>Rack 3 ToR 1 port 50</td>
</tr>
<tr>
<td>6</td>
<td>40 Gbps</td>
<td>Rack 3 ToR 2 port 50</td>
</tr>
<tr>
<td>7</td>
<td>40 Gbps</td>
<td>Rack 4 ToR 1 port 50</td>
</tr>
<tr>
<td>8</td>
<td>40 Gbps</td>
<td>Rack 4 ToR 2 port 50</td>
</tr>
<tr>
<td>9</td>
<td>40 Gbps</td>
<td>Rack 5 ToR 1 port 50</td>
</tr>
<tr>
<td>10</td>
<td>40 Gbps</td>
<td>Rack 5 ToR 1 port 50</td>
</tr>
<tr>
<td>11</td>
<td>40 Gbps</td>
<td>Rack 6 ToR 1 port 50</td>
</tr>
<tr>
<td>12</td>
<td>40 Gbps</td>
<td>Rack 6 ToR 1 port 50</td>
</tr>
<tr>
<td>13</td>
<td>40 Gbps</td>
<td>Rack 7 ToR 1 port 50</td>
</tr>
<tr>
<td>14</td>
<td>40 Gbps</td>
<td>Rack 7 ToR 1 port 50</td>
</tr>
<tr>
<td>15</td>
<td>40 Gbps</td>
<td>Rack 8 ToR 1 port 50</td>
</tr>
<tr>
<td>16</td>
<td>40 Gbps</td>
<td>Rack 8 ToR 1 port 50</td>
</tr>
</tbody>
</table>

## Spine 1 (Rack 2 only)

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Speed</th>
<th>Connects To</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>40 Gbps</td>
<td>Rack 2 ToR 1 port 49</td>
</tr>
<tr>
<td>2</td>
<td>40 Gbps</td>
<td>Rack 2 ToR 2 port 49</td>
</tr>
<tr>
<td>3</td>
<td>40 Gbps</td>
<td>Rack 1 ToR 1 port 49</td>
</tr>
<tr>
<td>4</td>
<td>40 Gbps</td>
<td>Rack 1 ToR 2 port 49</td>
</tr>
<tr>
<td>5</td>
<td>40 Gbps</td>
<td>Rack 3 ToR 1 port 49</td>
</tr>
<tr>
<td>6</td>
<td>40 Gbps</td>
<td>Rack 3 ToR 2 port 49</td>
</tr>
<tr>
<td>7</td>
<td>40 Gbps</td>
<td>Rack 4 ToR 1 port 49</td>
</tr>
<tr>
<td>8</td>
<td>40 Gbps</td>
<td>Rack 4 ToR 2 port 49</td>
</tr>
<tr>
<td>9</td>
<td>40 Gbps</td>
<td>Rack 5 ToR 1 port 49</td>
</tr>
</tbody>
</table>
### ToR 2 (e.g. Cisco 9372PX)

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Speed</th>
<th>Connects To</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 32</td>
<td>10 Gbps</td>
<td>node 1 - node 32 where port 1 connects to node 1, port 2 connects to node 2, and so on</td>
</tr>
<tr>
<td>33 - 38</td>
<td>NA</td>
<td>Not connected</td>
</tr>
<tr>
<td>39 - 42</td>
<td>10 Gbps</td>
<td>ToR 1 ports 39 - 42</td>
</tr>
<tr>
<td>43 - 47</td>
<td>10 Gbps</td>
<td>Corporate network as required (see note below table)</td>
</tr>
<tr>
<td>48</td>
<td>1 Gbps</td>
<td>Management switch port 50</td>
</tr>
<tr>
<td>49</td>
<td>40 Gbps</td>
<td>Spine 1 port 2</td>
</tr>
<tr>
<td>50</td>
<td>40 Gbps</td>
<td>Spine 2 port 2</td>
</tr>
<tr>
<td>51 - 52</td>
<td>NA</td>
<td>Corporate network as required (see note below table)</td>
</tr>
<tr>
<td>Management</td>
<td>1 Gbps</td>
<td>Management switch port 42</td>
</tr>
</tbody>
</table>

**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)

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Speed</th>
<th>Connects To</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 32</td>
<td>10 Gbps</td>
<td>Node 1 - node 32 where port 1 connects to node 1, port 2 connects to node 2, and so on</td>
</tr>
<tr>
<td>33 - 38</td>
<td>NA</td>
<td>Not connected</td>
</tr>
<tr>
<td>39 - 42</td>
<td>10 Gbps</td>
<td>ToR 2 ports 39 - 42</td>
</tr>
<tr>
<td>43 - 47</td>
<td>10 Gbps</td>
<td>Corporate network as required (see note below table)</td>
</tr>
<tr>
<td>48</td>
<td>1 Gbps</td>
<td>Management switch port 49</td>
</tr>
<tr>
<td>49</td>
<td>40 Gbps</td>
<td>Spine 1 port 1</td>
</tr>
<tr>
<td>50</td>
<td>40 Gbps</td>
<td>Spine 2 port 1</td>
</tr>
<tr>
<td>51 - 52</td>
<td>NA</td>
<td>Corporate network as required (see note below table)</td>
</tr>
<tr>
<td>Management</td>
<td>1 Gbps</td>
<td>Management switch port 41</td>
</tr>
</tbody>
</table>

**Note** Depending on the switches in your environment, connect two 40 Gbps ports or multiple 10 Gbps ports to your corporate network.
## Management Switch

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Speed</th>
<th>Connects To</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 32</td>
<td>1 Gbps</td>
<td>Node 1 - Node 32 where port 1 connects to node 1, port 2 connects to node 2, and so on</td>
</tr>
<tr>
<td>33 - 40</td>
<td>NA</td>
<td>Not connected</td>
</tr>
<tr>
<td>41</td>
<td>1 Gbps</td>
<td>ToR 1 management port</td>
</tr>
<tr>
<td>42</td>
<td>1 Gbps</td>
<td>ToR 2 management port</td>
</tr>
<tr>
<td>43</td>
<td>1 Gbps</td>
<td>Spine 1 management port</td>
</tr>
<tr>
<td>44</td>
<td>1 Gbps</td>
<td>Spine 2 management port</td>
</tr>
<tr>
<td>45-47</td>
<td>NA</td>
<td>Not connected</td>
</tr>
<tr>
<td>48</td>
<td>1 Gbps</td>
<td>Private managed switch</td>
</tr>
<tr>
<td>49</td>
<td>10 Gbps</td>
<td>ToR 1 port 48</td>
</tr>
<tr>
<td>50</td>
<td>10 Gbps</td>
<td>ToR 2 port 48</td>
</tr>
<tr>
<td>51-52</td>
<td>NA</td>
<td>Not connected</td>
</tr>
<tr>
<td>Management port</td>
<td>1 Gbps</td>
<td>Private managed switch</td>
</tr>
</tbody>
</table>

**Note** PDU ports are not reflected in the table above.
You can troubleshoot issues that you might experience after you install and deploy your Cloud Foundation environment.

This chapter includes the following topics:

- “Collect Logs for Your Cloud Foundation Environment,” on page 191
- “Unable to Browse to the Software Stack Web Interfaces Using their Fully Qualified Domain Names,” on page 205
- “Decommission Workflow Stops Responding at Task Named Enter Hosts Maintenance Mode,” on page 206
- “VDI Workload Creation Fails at the Import DHCP Relay Agents Task,” on page 207
- “Update Fails While Exiting Maintenance Mode,” on page 208

**Collect Logs for Your Cloud Foundation Environment**

Use the SoS tool to collect the logs for various software components in the environment. This Python tool resides in each SDDC Manager virtual machine in your Cloud Foundation environment.

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.

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. For a description of the SoS tool’s options, see “Supportability and Serviceability (SoS) Tool and Options,” on page 194.

**Prerequisites**

You must have the root account credentials for the SDDC Manager instances in your Cloud Foundation environment. In each management domain, the SDDC Manager instance is the one whose virtual machine name starts with vrm. See “Credentials for Logging In To the SDDC Manager (vrm) Virtual Machine,” on page 22.
When you run the tool from one rack and are collecting all logs for all racks, you must also provide the root account password for the other racks when prompted by the tool. If you want to collect logs only from a specific rack, you can run the tool using the \(--\text{rack} \ rackname\) option to have the tool collect the logs only from that rack. See “Supportability and Serviceability (SoS) Tool and Options,” on page 194 for a description of that option.

**NOTE** Running the tool in the SDDC Manager instance that is assigned the VIP address is the best practice. You log in to that SDDC Manager instance using the root account credentials.

For a description of the VIP address and how to determine which SDDC Manager instance the VIP address is currently assigned to, see “About the Primary Rack and the SDDC Manager Virtual IP Address,” on page 11.

**Procedure**

1. Using the root account, connect and log in, for example by SSH, to one of the SDDC Manager instances.

   In a multirack environment, you can use any of the SDDC Manager instances in your installation’s racks, although running the tool on the instance that has the VIP address is preferred. When you run the SoS tool from the SDDC Manager instance on one rack, the tool prompts for the root credentials for the instances on the other racks, collects log information from all of the racks, and writes the output to the filesystem of the instance where the command was initiated.

2. Change to the \(\text{/opt/vmware/evosddc-support}\) directory.

3. Depending on whether you have VDI workload domains in your environment, type the appropriate command to collect the logs and save to a named directory in the filesystem:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No VDI workload domains in the environment</td>
<td>Type command (./\text{sos} \ --\text{log-dir} \ named-output-dir)</td>
</tr>
<tr>
<td></td>
<td>Where (\text{named-output-dir}) is the name of the directory to which you want to save the output files.</td>
</tr>
<tr>
<td>VDI workload domains in the environment</td>
<td>Type command (./\text{sos} \ --\text{vdi-pass} \ \text{admin-password-for-VDI-environment-server-components} \ --\text{log-dir} \ named-output-dir)</td>
</tr>
<tr>
<td></td>
<td>Where (\text{admin-password-for-VDI-environment-server-components}) is the administrative account's password used by the server components in the VDI environment and (\text{named-output-dir}) is the name of the directory to which you want to save the output files</td>
</tr>
</tbody>
</table>

**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 \(--\text{no-clean-old-logs}\) option.

If you do not specify the \(--\text{log-dir}\) option, the tool writes the output to the \(\text{/var/tmp}\) directory in the SDDC Manager VM where the command is run.

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-vrm-1:/opt/vmware/evosddc-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
Progress : 0%, Initiated log collection
```
If this is a multi rack installation, you are prompted to enter the password for the SDDC Manager VM on each rack:

```
rack-1-vrm-1:/opt/vmware/evosddc-support # ./sos --log-dir /home/sos-logs
```

Welcome to SoS (Supportability and Serviceability) utility!
Please enter password for VRM (192.168.100.130):

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 the output files to the rack-1 subdirectory level, for an installation consisting of one physical rack with six ESXi hosts, configured with a DNS subdomain of subdomain.example.com, and having one VDI workload domain. The SoS tool command was run on 1 November 2016. The command included the option --log-dir /home/sos-logs to have the SoS tool write the output to the /home/sos-logs directory in the VRM VM's filesystem.

**Note** This example shows the results only down to the level of the rack-1 subdirectory. For details on the files the SoS tool creates in the output directories when collecting logs, see “Component Log Files Collected By the SoS Tool,” on page 199.

```
/home/sos-logs
sos-2016-11-01-21-22-46-17555
sos.log
rack-1
  esx
    hms
      N0_hms_logs_2016-11-01_09-25-22.zip #Directories with files, one per ESXi host
      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
      N4_hms_logs_2016-11-01_09-25-23.zip
      N5_hms_logs_2016-11-01_09-25-29.zip
  loginsight
    loginsight-agent-rack-1-vc-1.subdomain.example.com-2016-11-01--21.31.26.zip #Directories with files, one per vCenter Server instance
      nsx
      psc
      switch
      vc
      vdi
      vm.properties
      vrops
      1,2,3-full-0.zip #Directory with files
      zk
      hms.tar.gz
      vm-datetimestamp.tgz
```

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. For details about the output files and directories the SoS tool typically creates, see “Component Log Files Collected By the SoS Tool,” on page 199.

**What to do next**
Change to the output directory to examine the collected log files.
Supportability and Serviceability (SoS) Tool and Options

The SoS tool is a command-line Python tool used primarily to perform log collection and take configuration backups from all of the components in your Cloud Foundation environment.

The SoS tool is installed in /opt/vmware/evosddc-support in the SDDC Manager instance's file system. Only the root account can run the SoS tool. To run a command, change to the /opt/vmware/evosddc-support directory and type ./sos followed by the options required for your desired operation.

**Note** When using the tool to collect logs, initiating the command in the SDDC Manager instance that has the VIP address assigned to it is preferred.

When using the tool to take configuration backups:

- Initiating the command in the SDDC Manager instance is assigned the VIP address saves backup configurations for all of the racks in the installation.
- Initiating the command in an SDDC Manager instance that is not assigned the VIP address saves backup configurations only for the rack in which that instance is deployed.

For a description of the VIP address and how to determine to which SDDC Manager instance has it, see “About the Primary Rack and the SDDC Manager Virtual IP Address,” on page 11.

./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

Log files for the vRealize Log Insight agent in vCenter Server are collected when vCenter Server log files are collected.

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

SoS Options for Information About the SoS Tool

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

**Table 17-1. SoS Information Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help</td>
<td>Provides a summary of the available SoS tool options</td>
</tr>
<tr>
<td>-h</td>
<td>Provides the SoS tool's version number.</td>
</tr>
</tbody>
</table>

SoS Tool Options Used When Retrieving Support Log Files

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.
When you have a VDI workload domain in the environment and you want the SoS tool to collect logs from the VDI-specific server components, you must include the \(--vdi-pass \ vdi-password\) option. The SoS tool uses the specified \(vdi-password\) to log in as the Administrator user to the VDI environment’s server VMs and retrieve their support bundles, such as the View Composer instances, View Connection Server instances, security server instances, App Volumes instances, and AD Domain Server VM.

For steps to collect all logs, see “Collect Logs for Your Cloud Foundation Environment,” on page 191.

**Table 17-2. SoS Tool Log File Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(--log-dir)</td>
<td>Use this option to specify an output directory to which the SoS tool will write the log files, such as (/home/sos-logs).</td>
</tr>
<tr>
<td>(logdirectory)</td>
<td>If this option is not specified, the tool writes the output files to (/var/tmp) in the VM’s filesystem in which the command was run.</td>
</tr>
<tr>
<td></td>
<td>For a description of the output directory structure, see “Component Log Files Collected By the SoS Tool,” on page 199.</td>
</tr>
<tr>
<td>(--no-clean-old-logs)</td>
<td>Use this option to prevent the tool from removing any output from a previous collection run. By default, the SoS tool.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>(--vdi-pass)</td>
<td>You must specify this option if you want the logs collected from any VDI workload domains’ server VMs in the environment. For (vdi-password), specify the password used for the account for logging in to View Administrator, the VDI environment’s Web interface.</td>
</tr>
<tr>
<td>(vdi-password)</td>
<td></td>
</tr>
<tr>
<td>(--esx-logs)</td>
<td>Use this option to collect logs from the ESXi hosts only.</td>
</tr>
<tr>
<td>(--vc-logs)</td>
<td>Use this option to collect logs from the vCenter Server instances only. The logs from the vRealize Log Insight agents corresponding to the vCenter Server instances are also collected when this option is used.</td>
</tr>
<tr>
<td>(--switch-logs)</td>
<td>Use this option to collect logs from the switches only. Logs from all switches are collected: management, ToR, and, if a multirack installation, spine switches.</td>
</tr>
<tr>
<td>(--vrm-logs)</td>
<td>Use this option to collect logs from the SDDC Manager instances only.</td>
</tr>
<tr>
<td>(--zk-logs)</td>
<td>Use this option to collect 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 VMware Cloud Foundation Overview and Bring-Up Guide.</td>
</tr>
<tr>
<td>(--cassandra-logs)</td>
<td>Use this option to collect 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.</td>
</tr>
<tr>
<td>(--via-logs)</td>
<td>When the VIA virtual machine is reachable from the SDDC Manager instance where you are issuing the SoS tool command to collect the logs, you can use this option to collect logs only from the VIA virtual machine.</td>
</tr>
<tr>
<td>(--psc-logs)</td>
<td>Use this option to collect logs from the Platform Services Controller instances only.</td>
</tr>
<tr>
<td>(--nsx-logs)</td>
<td>Use this option to collect logs from the NSX Managerand NSX Controller instances only.</td>
</tr>
<tr>
<td>(--li-logs)</td>
<td>When there are vRealize Log Insight instances in your installation, use this option to collect logs from those instances only.</td>
</tr>
<tr>
<td>(--vrops-logs)</td>
<td>When there are vRealize Operations Manager instances in your installation, use this option to collect logs from those instances only.</td>
</tr>
<tr>
<td>(--hms-logs)</td>
<td>Use this option to collect logs from the HMS software component only.</td>
</tr>
<tr>
<td>(--rack)</td>
<td>In a multirack environment, use this option to collect logs from a specific rack. Without this option, the SoS tool collects logs from all of the racks in the environment.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>--vrm-ip VRM-VM-IP-address</td>
<td>In a multirack environment, use this option to collect logs from an SDDC Manager instance different from the one in which you are running the SoS tool. You run the SoS tool in a specific SDDC Manager instance, usually the one in the primary rack. When you want to run the tool in one SDDC Manager instance but collect the logs from another instance, you use this option to specify that other instance's IP address. Without this option, the SoS tool collects logs from all of the SDDC Manager instances in the environment.</td>
</tr>
<tr>
<td>--vrm-pwd VRM-VM-root-password</td>
<td>In a multirack environment, when running the SoS tool in one SDDC Manager instance to collect logs from another instance, use this option to specify the password for that other instance's root account. When running the SoS tool in one SDDC Manager instance to collect logs from another instance using the --vrm-ip VRMIP option, the SoS tool authenticates into that other SDDC Manager instance using the root account to initiate log collection in that instance. The SoS tool requires the password of that other instance's root account to log in to that instance.</td>
</tr>
<tr>
<td>--dump-only-vrm-java-threads</td>
<td>Use this option to only collect the Java thread information from the SDDC Manager instances.</td>
</tr>
<tr>
<td>--debug-mode</td>
<td>Use this option to run the log collection process in debug mode.</td>
</tr>
</tbody>
</table>

### SoS Tool Options Used for Backing Up Component Configurations

Use this option to create backup files of the configurations for various components. For the steps to run the tool using this option, see Chapter 9, “Back Up Component Configurations Using the SoS Tool,” on page 107.

When the environment has more than one rack and the command is initiated in the SDDC Manager instance that currently has the VIP address, the tool also initiates the backup command on the other racks. Each rack’s output is written into its own SDDC Manager instance’s filesystem. If you initiate the command in the SDDC Manager instance that does not have the VIP, the backup command is initiated only for that rack. For a description of how to determine which SDDC Manager instance has the VIP, see “About the Primary Rack and the SDDC Manager Virtual IP Address,” on page 11.

By default, the tool writes the backup files for a rack into the /var/tmp directory in the filesystem of that rack’s SDDC Manager instance. For example, the backup files for the one rack are written into its SDDC Manager instance’s /var/tmp directory, the backup files for the second rack are written into its SDDC Manager instance’s /var/tmp directory, and so on. When you log in to the first rack’s SDDC Manager instance, change directories to the /var/tmp directory, and list the directory contents, you see the collected set of backups that the tool has written for that rack, for example:

```
rack-1-vrm-1:/var/tmp # ls -l
```

```
-rw-r--r-- 1 root root 4096 Nov 23 00:48 backup-2016-11-23-00-46-01-20678
```

```
-rw-r--r-- 1 root root 4096 Nov 23 03:48 backup-2016-11-23-03-48-15-6185
```

```
```

```
-rw-r--r-- 1 root root 4096 Nov 25 12:24 backup-2016-11-25-12-22-54-17865
```

```
```

```
-rw-r--r-- 1 root root 4096 Nov 28 18:37 backup-2016-11-28-18-35-33-12228
```

```
```

```
-rw-r--r-- 1 root root 4096 Nov 29 13:12 backup-2016-11-29-13-10-56-8848
```
Then when you log in to the second rack’s SDDC Manager instance, change directories to the /var/tmp directory, and list the directory contents, you see the collected set of backups that the tool has written for that second rack, for example:

```
rack-2-vrm-1:/var/tmp # ls -l
drwxr-xr-x 3 root root 4096 Nov 24 11:38 backup-2016-11-24-11-38-08-32210
drwxr-xr-x 3 root root 4096 Nov 25 12:25 backup-2016-11-25-12-24-22-17923
drwxr-xr-x 3 root root 4096 Nov 25 20:46 backup-2016-11-25-20-45-20-28378
```

Table 17-3. SoS Tool Backup Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--backup</td>
<td>Use this option to take a backup of the configurations of these components:</td>
</tr>
<tr>
<td></td>
<td>- ESXi hosts</td>
</tr>
<tr>
<td></td>
<td>- Switches (management, ToR, spine)</td>
</tr>
<tr>
<td></td>
<td>- The three infrastructure (ISVM) virtual machines’ Zookeeper server instances and Cassandra datastore</td>
</tr>
<tr>
<td></td>
<td>- SDDC Manager instances (the virtual machines, one per rack, that have vrm in their names)</td>
</tr>
<tr>
<td></td>
<td>- The SDDC Manager instances’ HMS software components</td>
</tr>
</tbody>
</table>

The output is written to the /var/tmp directory in each SDDC Manager instance’s filesystem, following this directory structure:

```
backup-datatimestamp
sos.log
rack-1
  configBundle-hostname.domain.tgz #One per host
  switch
    ToR-or-spine-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
  zk
    isvm-ip-address #Three directories in the zk directory, each named using the IP address of an ISVM VM, such as 192.168.100.43
      cassandra-db-backup.tgz
      zk-db-backup.tgz
      vrm.properties
      hms_ib_inventory.json
      vrm.properties
      vrm.properties.vRack
      vrm-security.keystore
      hms.tar.gz #HMS component’s configuration data
      vrm-datatimestamp.tgz #Postgres database configuration data
```
Table 17-4. SoS Tool Options that Directly Alter the SDDC Manager Configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--change-ntp NTP-IP-address</td>
<td>This option updates the SDDC Manager configuration to replace the existing NTP server IP address with a new one. During the bring-up process on the first rack in a Cloud Foundation installation, an NTP server IP address is entered in the bring-up wizard and is saved to the distributed database. This SoS tool option updates that stored NTP server IP address.</td>
</tr>
<tr>
<td>--change-uplink-db uplink-port-1, uplink-port-2, ...</td>
<td>This option changes the uplink port information that is stored in the distributed database. This option is deprecated in this release. To update the uplink ports, use the Uplink screen in the SDDC Manager client. See “Manage Uplink Connectivity Settings Using the SDDC Manager Client,” on page 103.</td>
</tr>
<tr>
<td>--remove-esx-host-in-db ESXi-host-ip</td>
<td>After decommissioning an ESXi host, this option updates the distributed database to remove the information for the ESXi host specified in the option, either by IP address or hostname. This option is deprecated in this release. To decommission an ESXi host from the environment, use the steps as documented in “Replace Dead Host or SAS Controller or Expander when Host Belongs to a Workload Domain,” on page 117 to decommission the ESXi host.</td>
</tr>
</tbody>
</table>

SoS Tool Options for Audit Data Collection and Diff Generation

These SoS commands are used for collecting audit data and to generate diff between collected audit data. Audit data consist 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.

**NOTE** Audit tool options will work only after successful completion of second boot on the rack.

Table 17-5. SoS Tool Options for Audit Data Collection and Diff Generation

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--audit</td>
<td>This option collects audit information from all the components of Cloud Foundation. By default, audit data is saved in the /var/tmp/audit-compliance/audit directory as a JSON file. The log file is saved under /var/tmp/audit-compliance/logs.</td>
</tr>
<tr>
<td>--audit-diff</td>
<td>This option generates a diff between two audit data JSON files. This options picks the latest and the penultimate audit data JSON files from the /var/tmp/audit-compliance/audit directory and generates the diff. By default, the diff is stored as a JSON file in the /var/tmp/audit-compliance/diff directory.</td>
</tr>
<tr>
<td>--audit-output-dir &lt;path-to-audit-parent-directory&gt;</td>
<td>Use this option to save audit data JSON and diff JSON files to a directory other than the default /var/tmp/audit-compliance parent directory. <strong>NOTE</strong> This option can be used with the --audit and --audit-diff options. This option creates the following directory structure: <em>path-to-audit-parent-directory/audit-compliance</em> <em>path-to-audit-parent-directory/audit-compliance/audit</em> <em>path-to-audit-parent-directory/audit-compliance/diff</em> Audit data JSON files are saved in the <em>path-to-audit-parent-directory/audit-compliance/audit</em> directory. Audit diff JSON files are saved in the <em>path-to-audit-parent-directory/audit-compliance/diff</em> directory.</td>
</tr>
</tbody>
</table>
Table 17-5. SoS Tool Options for Audit Data Collection and Diff Generation (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--audit-files <code>&lt;full-path-to-audit-json-file-1&gt;</code> <code>&lt;full-path-to-audit-json-file-2&gt;</code></td>
<td>Use this option to generate a diff file between the two specific audit data JSON files.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This option must be with the --audit-diff option.</td>
</tr>
<tr>
<td></td>
<td>By allowing the user to specify the audit files to be diffed, this option bypasses the</td>
</tr>
<tr>
<td></td>
<td>default behavior of the --audit-diff option, described above.</td>
</tr>
<tr>
<td>--no-audit</td>
<td>Use this option to prevent audit data collection during SoS log collection.</td>
</tr>
<tr>
<td></td>
<td>By default, audit data collection runs when SoS log collection runs. This option prevents</td>
</tr>
<tr>
<td></td>
<td>this default behavior.</td>
</tr>
</tbody>
</table>

Component Log Files Collected By the SoS Tool

The SoS tool collects log files for various software components in your Cloud Foundation environment. For components that have their own utilities for gathering logs, the SoS tool invokes those utilities, and then collects the resulting log files from those components.

Components Covered by the SoS Tool

The SoS tool collects logs from these components within your Cloud Foundation installation:

- Management, ToR, and spine 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
- vRealize Operations Manager 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

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:

```
/home/sos-logs
  sos-timestamp
    sos.log
    rack-1
      esx
      hms
      hms_logs_timestamp.zip #Directory with files. One per ESXi host
    loginsight
      loginsight-agent-vcenterFQDN-timestamp.zip #Directory with files. One per vCenter Server instance
    nsx
    psc
```
In each rack-specific directory, the esx directory contains the following diagnostic files collected for each ESXi host in the rack:

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>esx-IP-address.tgz</td>
<td>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>.</td>
</tr>
<tr>
<td>vsan-health-IP-address.txt</td>
<td>Virtual SAN cluster health information from running the standard command <code>python /usr/lib/vmware/vsan/bin/vsan-health-status.pyc</code> on the ESXi host. An example file is <code>vsan-health-192.168.100.101.txt</code>.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>hms_log_archiver.sh</td>
</tr>
<tr>
<td>N0_hms_logs_2016-11-01-09-25-22.zip</td>
</tr>
<tr>
<td>N1_hms_logs_2016-11-01-09-25-35.zip</td>
</tr>
</tbody>
</table>
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 \( N_n \) refers to the file for the \( n \)th ESXi host.

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( N_n )_hms_ib_timestamp.log</td>
<td>HMS in-band (IB) log</td>
</tr>
<tr>
<td>( N_n )_hms_oob_timestamp.zip</td>
<td>HMS out-of-band (OOB) log files ( hms.log ) and ( hms.log.1 )</td>
</tr>
<tr>
<td>( N_n )_hms_events_log_timestamp.log</td>
<td>HMS events log file</td>
</tr>
<tr>
<td>( N_n )_ServerInfo_timestamp.log</td>
<td>HMS server info log file</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>li.tgz</td>
<td>Compressed TAR file consisting of the vRealize Log Insight instance’s /var/log directory.</td>
</tr>
<tr>
<td>loginsight-support-timestamp.tar.gz</td>
<td>Standard vRealize Log Insight compressed support bundle, created by the loginsight-support command.</td>
</tr>
<tr>
<td>repo.tar.gz</td>
<td>Compressed TAR file consisting of a mass export of the instance’s repository buckets. created by running the /opt/vmware/bin/loginsight-dump-repo.sh in the vRealize Log Insight instance.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config/liagent.ini</td>
<td>Configuration file containing the preconfigured default settings for the agent.</td>
</tr>
<tr>
<td>config/liagent-effective.ini</td>
<td>The agent’s effective configuration. This effective configuration is the liagent.ini dynamically joined with settings from the vRealize Log Insight server-side settings to form this liagent-effective.ini file.</td>
</tr>
<tr>
<td>log/liagent_timestamp_*.log</td>
<td>Detailed log files.</td>
</tr>
<tr>
<td>var/log/messages</td>
<td>If the agent is configured to collect messages from the vCenter Server instance’s /var/log directory, this file is the collected messages log.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware-NSX-Manager-tech-support-nsxmanagerIPaddr.tar.gz</td>
<td>Standard NSX Manager compressed support bundle, generated using the NSX for vSphere API POST <a href="https://nsxmanagerIPaddr/api/1.0/appliance-management/techsupportlogs/NSX">https://nsxmanagerIPaddr/api/1.0/appliance-management/techsupportlogs/NSX</a>, where nsxmanagerIPaddr is the IP address of the NSX Manager instance. An example is VMware-NSX-Manager-tech-support-10.0.0.8.tar.gz.</td>
</tr>
<tr>
<td>VMware-NSX-Controller-tech-support-nsxmanagerIPaddr-controllerId.tgz</td>
<td>Standard NSX Controller compressed support bundle, generated using the NSX for vSphere API to query the NSX Controller technical support logs: GET <a href="https://nsxmanagerIPaddr/api/2.0/vdn/controller/controllerId/techsupportlogs">https://nsxmanagerIPaddr/api/2.0/vdn/controller/controllerId/techsupportlogs</a>, where nsxmanagerIPaddr is the IP address of the NSX Manager instance and controllerId 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</td>
</tr>
</tbody>
</table>

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 “About the Primary Rack and the SDDC Manager Virtual IP Address,” on page 11.

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vm-support-pscIPaddr.tar.gz</td>
<td>Standard Platform Services Controller support bundle downloaded from the Platform Services Controller instance with IP address pscIPaddr.</td>
</tr>
</tbody>
</table>

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 spine switches. The SoS tool writes the logs for the spine 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.
cl_support_Management1_timestamp.tar.xz | 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 /usr/cumulus/bin/cl-support support command.

IPaddr-switchmaker-techsupport.gz | Standard support bundle collected from a ToR or spine switch at IP address IPaddr and for switch maker switchmaker. The SoS tool collects the switch's support bundle using the appropriate command for the particular switch, such as show tech-support. The ToR switches typically have IP addresses 192.168.0.20 and 192.168.0.21. The spine 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.

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

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 Horizon 6 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 Horizon 6 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.

vrm.properties Directory Contents

In each rack-specific directory, the vrm.properties directory contains the following configuration files from the SDDC Manager instance deployed in the rack:

corrHostname:vdm-sdct-timestamp-server.zip | View Connection support bundle downloaded from the View Connection instances having hostname corrserverHostname, such as corr-1-1, corr-1-2, and so on. The support bundle is obtained from the instance using the standard C:\Program Files\VMware View\Server\DCT\support.bat command for the View Connection Server.

appvolsHostname-logs.zip | App Volumes log files obtained from the App Volumes Manager instance having hostname appvolsHostname, such as appvolumes-1-1, appvolumes-1-2, and so on.
**File** Description

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hms_ib_inventory.json</td>
<td>SDDC Manager rack hardware inventory file, created during imaging of the rack. The SoS tool obtains this file from the SDDC Manager instance's /home/vrack/VMware/vRack directory.</td>
</tr>
<tr>
<td>vrm-security.keystore</td>
<td>SDDC Manager keystore file, from the SDDC Manager instance's /home/vrack/VMware/vRack directory.</td>
</tr>
<tr>
<td>vrm.properties</td>
<td>Properties file from the SDDC Manager client (webapp).</td>
</tr>
<tr>
<td>vrm.properties.vRack</td>
<td>Copy of the SDDC Manager vrm.properties file in the SDDC Manager instance's /home/vrack/VMware/vRack directory.</td>
</tr>
</tbody>
</table>

**vrops Directory Contents**

In each rack-specific directory, the vrm directory contains diagnostic information files collected from the vRealize Operations Manager instance deployed on that rack, if any.

To collect the vRealize Operations Manager support bundle, the SoS tool runs the Python generateSupportBundle.py script in the vRealize Operations Manager instance using the default filter – f=1,2,3. As described in VMware KB article 2074601, with this default filter option, all logs, configuration files, and support dumps are collected, while cluster information is not included.

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,2,3-full-0.zip</td>
<td>Even though this directory’s name end in .zip, it is a directory of files resulting from generating the standard vRealize Operations Manager support bundle from the vRealize Operations Manager instance. To generate the vRealize Operations Manager support bundle, the SoS tool runs the Python generateSupportBundle.py script in the vRealize Operations Manager instance using the default filter – f=1,2,3. As described in VMware KB article 2074601, with this default filter option, all logs, configuration files, and support dumps are collected, while cluster information is not included.</td>
</tr>
<tr>
<td>log</td>
<td>Log file of the vRealize Operations Manager support bundle generation process.</td>
</tr>
<tr>
<td>summary-0</td>
<td>Summary of the success or failure of each of the filter options (1, 2, 3) used in the support bundle generation process.</td>
</tr>
<tr>
<td>vrops_logs.tar</td>
<td>Archive of the log files obtained from the vRealize Operations Manager instance’s filesystem in /usr/lib/vmware-vcops/user/log/<em>, /var/log/vmware/</em>, /var/log/vcops_logs/<em>, and /var/log/casa_logs/</em>.</td>
</tr>
</tbody>
</table>

**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.

**Note** In a Cloud Foundation environment, the three ISVM instances are deployed in the primary rack only. As a result, this zk directory only appears in the primary rack’s log output. For the description of the primary rack, see “About the Primary Rack and the SDDC Manager Virtual IP Address,” on page 11.

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.
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 client 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 domains. 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 virtual machine’s VIP 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 client, 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 client, 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 environment'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 virtual machine 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 (the VRM VM), and try to ping the data center network.
  
  - If the VRM 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 VRM 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.
Index

A
about this information 7
Active Directory, when creating a VDI workload domain 61
Active Directory users and groups, granting vSphere Web Client access 34
add server 109
adding physical racks 102
Alert Catalog 87
alerts, ongoing operations 87
alerts based on system-detected problems 77
audit collection
diffing audit files 194
SoS tool 194

B
backing up configuration files, SoS tool 194
backups using the SoS tool 107
browser support for the SDDC Manager client 13

C
client
logging in 13
logging out 19
SDDC Manager 13
client interfaces 12
clients, administrative web interfaces 12
Cloud Foundation, VMware software components 10
compression 70
configuring settings 99
Connection Server administrator account 72
corporate network, connections to 105
creating a VDI workload domain, troubleshooting 207
creating VDI workload domains 53

D
Dashboard page 14
data center connections, working with 105
decommissioning hosts, troubleshooting 206
deduplication 70
deleting workload domains 70
desktop OVA requirements 56
domains, management and workload 43

E
Event Catalog 81
event-driven problem detection 77
excluding IP addresses, about 104
expand, management domain 68
expand a management domain 68
expanding management and workload domains 68
expanding workload domain 68, 69
external networks, networking to 105

G
glossary 7
groups
adding locally 35
assigning permissions for operations 37

I
identity sources, verifying 32
image individual device, management switch 130
intended audience 7
interfaces, administrative Web clients 12
introduction to administering an Cloud Foundation installation 9
IP addresses, excluding 104
IP addresses exclusions 104
IP Distribution screen 104

J
joining an Active Directory domain 32

L
license keys, entering 140
licenses, managing 139
licensing model 139
life cycle management, setting depot user 151
lifecycle management
backup location 165
download update 153
inventory version 163
proxy server 152
schedule update 156
Lifecycle Management page 14
list view of resources 41
log collection, SoS tool 194
log files 199
logging in 13
logging out 19
logs, collecting 191
look up built-in account credentials 23

M
management domain about 43
utilize capacity 67
management switch replacing 129
syslog 96
managing users and groups 31
map view of resources 41
monitoring your environment 73

N
names, VI workload domains 47
network settings, managing 102
networking
to external networks 105
to your corporate network 105

O
operations, assigning permissions to perform 37

P
password policy 39
passwords, rotating 21
permissions, assigning to users and groups 37
physical resources, views of 41
physical rack, port connectivity 187
physical resources, managing 41
power on an environment that was shut down 141
powering down primary rack 143
second rack 142
switches 145
powering on primary rack 145
second rack 146
primary rack 10
problem detection 77

R
RAID 5 erasure coding 70
RAID 6 erasure coding 70
RBAC 38
remove host that belongs to workload domain 117
host that does not belong to workload domain 120
replacing, management switches 129
replacing Arista ToR and spine switches 135
replacing Cisco ToR and spine switches 132
rights 38
role-based access control (RBAC) 38
roles, about 38
root account credentials for the VRM virtual machine 22
rotating passwords 21
rotating all passwords 24

S
SDDC Manager client 13
SDDC Manager, virtual IP 10
SDDC Manager user interface, tour of 14
security, password rotation 21
server, add 109
servers, adding or replacing 109
setting default values, for VDI workload domains 99
setting up environment, rack wiring 183
settings, uplink connectivity 103
settings configuration 99
Settings page 14
shutdown an environment 141
software components 10
SoS tool
log files 199
making backups with 107
Supportability and Serviceability (SoS) tool 194
Supportability and Serviceability tool, making backups with 107
switches replacing 129
restoring 129
syslog 96
syslog, switches 96
system health, examining 97
system status, workflows and tasks 76
system administrator account 37
System Status page 14

T
tasks, working with 76
ToR and spine switch replacement
Arista 135
Cisco 132
troubleshooting
logging in to Web interfaces 205
update fails exiting maintenance mode 208
VDI workload domains 207

U
update
download 153
inventory versions 163
schedule 156
upgrade
2.1 to 2.1.1 176
Cloud Foundation software on management domain 168
ISVMs 173
third party software 175
to 2.1 168
VMware software on management domain 175
VMware software on VI and VDI domains 175
uplink connectivity settings, configuring 103
User Management page 14
user interface, SDDC Manager 13
users
adding locally 35
assigning permissions for operations 37
using vRealize Log Insight 94

V
vCenter Server Single Sign-On, Active Directory 31
VDI infrastructure settings 100
VDI offering 45
VDI workload domains
creating 53
creation wizard 60
desktop OVA requirements 56
post-deployment tasks 66
setting default values 99
VDI workload domain creation
Active Directory 61
General Topology step 60
networking information 63
parent desktop template 64
Review step 65
Virtual Desktops step 63
Windows Server ISO 64
VI offering 45
VI workload domain
accessing the infrastructure using the vSphere Web Client 52
naming 47
network configurations 49
selecting performance and availability settings 47
start creation wizard 46
start deployment 51
VI workload domains, about creating 45
views of physical resources 41
VIP address, SDDC Manager 10
Virtual Infrastructure 45
Virtual Desktops step, VDI workload domain creation 63
virtual IP of the SDDC Manager 10
VMware depot user, setting 151
vRealize Log Insight 92
vRealize Operations Manager, examining system health with 97
vrm-cli utility 26

W
workflows, working with 76
workload domains
about 43
deleting 70
expanding 68, 69
VDI 53
Virtual Infrastructure 45