Administering VMware EVO SDDC

VMware EVO SDDC 1.2

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
About Administering VMware EVO SDDC  5

1 Overview of EVO SDDC System Administration  7
   VMware Software Components in an EVO SDDC System  8
   Client Web Interfaces Used When Administering an EVO SDDC System  9

2 Getting Started with the EVO SDDC Manager Web Interface  11
   Log in to the EVO SDDC Manager Web Interface  11
   Tour of the EVO SDDC Manager Web Interface  12
   Log out of the EVO SDDC Manager Web Interface  17

3 On-Demand Password Rotation in Your EVO SDDC System  19
   Credentials for Logging In To the EVO SDDC Manager (vrm) Virtual Machine  20
   Look Up Account Credentials Using the Lookup-Password Command  20
   Rotate All Passwords On-Demand for the Managed Physical and Logical Entities  21
   vrm-cli Command Reference  23

4 Managing Users and Groups  29
   Active Directory and Your EVO SDDC System  29
   Add Local Users and Groups  33
   Assign Permissions to Users and Groups  35
   Add a System Administrator  35
   Role-Based Access Control  36
   User Passwords in Your EVO SDDC System Environment  36

5 Managing Physical Resources  39

6 Working with Management Domains and Workload Domains  41
   Creating and Provisioning Workload Domains  42
   Expanding Management and Workload Domains  65
   Delete a Workload Domain  67
   Enabling Virtual SAN Space Efficiency Features in All-Flash Systems  68
   Manually Update the Credentials for the vRealize Operations for Horizon Broker Agent When Account Credentials Change for the Connection Server Administrator Account  69

7 Monitoring Your EVO SDDC System  71
   Managing Workflows and Tasks  73
   Managing Alerts, Events, and Audit Events  74
   Using the vRealize Log Insight Capabilities in Your System  89
   Using the vRealize Operations Manager Capabilities of Your System  93
About Administering VMware EVO SDDC

Administering VMware EVO SDDC provides information about managing a system powered by VMware EVO™ SDDC™ software, including managing the system's physical and virtual infrastructure, managing users, configuring and deploying service offerings, and upgrading and monitoring the system.

Intended Audience

The Administering VMware EVO SDDC is intended for data center system administrators who manage their organization's EVO SDDC suite of software. 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®
- 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 EVO SDDC Overview and Bring-Up Guide contains detailed information about the EVO SDDC solution, its components, and the network topology of an installed and deployed EVO SDDC system.
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.
Overview of EVO SDDC System Administration

EVO SDDC enables deployment of a private cloud system based on VMware’s software-defined data center (SDDC) architecture. A system powered by EVO SDDC is a turnkey private cloud instance that is easily deployed in a corporate network and 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.

An EVO SDDC system provides integrated physical and virtual compute, storage and networking capabilities with corresponding management capabilities, and makes those capabilities available as a single logical system, 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, the system automatically configures vRealize Log Insight and vRealize Operations for those environments, to provide performance management, capacity optimization, and real-time log analytics. An EVO SDDC system can scale to meet the increasing demands on your data center.

See the EVO SDDC Overview and Bring-Up Guide for an in-depth introduction to the architecture, components, and physical topology of a system powered by EVO SDDC, along with detailed descriptions of the software that comes prepackaged as part of the system.

As an SDDC administrator, you use the information in the Administering VMware EVO SDDC to understand how to administer and operate the system. An administrator of the system 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 system
- Use the auditing and log analytics capabilities of the integrated vRealize Log Insight software to troubleshoot issues and prevent problems across the physical and virtual infrastructure
- Use the centralized monitoring capabilities of the integrated vRealize Operations software to manage performance and gain insight into the health of the system across the physical and virtual infrastructure
- Perform life cycle management on the EVO SDDC software components

This chapter includes the following topics:

- “VMware Software Components in an EVO SDDC System,” on page 8
- “Client Web Interfaces Used When Administering an EVO SDDC System,” on page 9
VMware Software Components in an EVO SDDC System

A deployed EVO SDDC system includes the following VMware software as standard components.

- The EVO SDDC software components that provide centralized management of the integrated system, such as the EVO SDDC Manager, the Hardware Management Services, and their subcomponents
- The VMware software stack that implements a software-defined data center:
  - vSphere Enterprise Plus Edition
  - Platform Services Controller, used as the identity provider
  - vCenter Server Standard
  - Virtual SAN
  - NSX for vSphere
  - vRealize Operations
  - vRealize Log Insight

Depending on the system configuration that is installed in your data center and the types of workload infrastructure deployed in your system, the following VMware software components might be available.

- View, the software components from the Horizon 6 product that provides virtual desktop infrastructure
- App Volumes

For the exact versions of the VMware products that are in your system after its initial bring-up, see the EVO SDDC Release Notes document for your version of EVO SDDC. If your system has been updated after its initial bring-up using the Life Cycle Management features, see “View Inventory Component Versions,” on page 121 for details on how to view the versions of the VMware products that are within your system.

**CAUTION** Do not manually change any of the settings that the system sets automatically by default. If you change system-generated settings, unpredictable results might occur. Do not change settings for the resources that the system automatically creates and deploys during the system deployment process, the workload domain processes, assigned IP addresses or names, and so on.

Some of the system-default configuration settings can be customized using the EVO SDDC Manager Web interface. See Chapter 8, “Settings Configuration Using the EVO SDDC Manager Web Interface,” on page 95.

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

- vSphere Enterprise Edition
- Platform Services Controller, used as the identity provider
- vCenter Server Standard
- Virtual SAN
- NSX for vSphere
- vRealize Operations
- vRealize Log Insight
- View, a component of the VMware Horizon product
- App Volumes
Client Web Interfaces Used When Administering an EVO SDDC System

You use the EVO SDDC Manager Web interface in a browser for the single-point-of-control management of your EVO SDDC system. The EVO SDDC Manager provides centralized access to and an integrated view of the physical and virtual infrastructure of the system.

EVO SDDC Manager does not mask the individual component management products. Along with the EVO SDDC Manager Web interface, 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 EVO SDDC Manager Web interface.

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 EVO SDDC Manager Web interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere Web Client</td>
<td>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>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>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 environment is deployed in your system, you might also use the following Web interfaces for administration tasks involving the associated VMware software components in such an environment:

- View Administrator Web interface
- App Volumes Manager Console

Launch links are not provided in the EVO SDDC Manager Web interface 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 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 EVO SDDC Manager Web Interface

You use the EVO SDDC Manager Web interface to perform administration tasks on the system. This 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 EVO SDDC Manager Web interface by using an industry-standard Web browser. For the list of supported Web browser types and versions, see the VMware EVO SDDC 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 EVO SDDC Manager Web Interface,” on page 11
- “Tour of the EVO SDDC Manager Web Interface,” on page 12
- “Log out of the EVO SDDC Manager Web Interface,” on page 17

**Log in to the EVO SDDC Manager Web Interface**

You access the EVO SDDC Manager Web interface 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 your EVO SDDC system. The system uses role-based access control (RBAC) to determine what operations a user can perform, including logging in. For details about the system’s RBAC, see “Role-Based Access Control,” on page 36.

During the system’s bring-up process, a name and password are entered to create a superuser account. If this is the first time you are logging in to the system after running the system’s 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 system’s 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 EVO SDDC Manager. This name typically has a form like vrm.sddc.example.com, where sddc.example.com is the value that was specified in the EVO SDDC Sub-Domain field in the system's bring-up wizard. The FQDN and the numeric virtual IP (VIP) for the EVO SDDC Manager are listed in the Component IP Allocation step in the bring-up wizard. Then during the system's bring-up process, the system associates that name with the numeric virtual IP (VIP). See the EVO SDDC Overview and Bring-Up Guide for details about the addresses that are assigned during the bring-up process.

Procedure

1. In a Web browser, open the login screen by navigating to https://VRM-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 accessing your system.

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

Tour of the EVO SDDC Manager Web Interface

The EVO SDDC Manager Web interface is your single point of control for managing and monitoring your EVO SDDC software-defined data center and for provisioning virtual environments.

In the EVO SDDC Manager Web interface, you use the Navigation bar to move between the main areas of the 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.
Dashboard

The Dashboard page is the home page that provides the overall administrative view of your system. The Dashboard page provides a top-level view of the physical and logical resources across all of the physical racks in your system, including available CPU, memory, and storage capacity. From this page, you can start the process of creating a workload domain.
You use the links on the dashboard to drill-down and examine details about the physical resources and the virtual environments that are provisioned for the management and workload domains. For more information about each area, see:

- Chapter 5, “Managing Physical Resources,” on page 39
- Chapter 6, “Working with Management Domains and Workload Domains,” on page 41

**System Status**

Use this page to check on the health of the system. You can view alerts, examine historical and current information about the tasks running in the system, and examine the system events and audit events that are raised by the system's problem detection and monitoring components. From these event lists, you can access the Event Catalog to see descriptions of the pre-configured events that the system generates through EVO SDDC Manager. From the alerts listing, you can access the Alert Catalog to see descriptions of the alerts that the system raises.
Your EVO SDDC system has event-driven problem detection. The system records an event for system conditions that are potentially significant or interesting to you, such as a degradation, a failure, or a user-initiated configuration change. The system raises an alert when it determines a problem, based on an analysis of the event or combination of events.

See Chapter 7, “Monitoring Your EVO SDDC System,” on page 71 for the information about using alerts and events to monitor the health of your system.

User Management

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

- In the Users & Groups screen, grant or revoke the ability for users and groups to use the system.
- In the Roles & Permissions screen, examine the roles that provide the privileges associated with the available operations in the system. Your system uses role-based access control (RBAC).
Two roles are defined by default. One is an administrator-level role that provides full administrative privileges. The other provides read-only privileges.

See Chapter 4, “Managing Users and Groups,” on page 29.

**Life Cycle Management**

Use this page to manage the patching and maintenance of the software components that are installed in your system. The system notifies you when an update is available and provides the ability to download the bundles and begin the update process. For details, see Chapter 10, “Lifecycle Management,” on page 109.

**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 system. For details about setting defaults used for VDI environments, see “Customize Default Values Used When Creating VDI Workload Domains,” on page 95.

- Initiate the process for adding a new rack to the system.

- Work with network settings, such as editing uplink connectivity settings, reviewing the IP address distribution in the system, excluding IP addresses, entering data center network configurations, and associating those configurations with workload domains.

- Manage license keys for your system’s VMware software components.

**Log out of the EVO SDDC Manager Web Interface**

Log out of the EVO SDDC Manager Web interface when you have completed your tasks.

**Procedure**

1. In the EVO SDDC Manager Web interface, 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 EVO SDDC System

To ensure security in your system, you can rotate the passwords for the built-in accounts that are used by the physical and logical entities in your EVO SDDC 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 the system have built-in accounts and their passwords are managed by the system using the vrm-cli tool. At the end of the system bring-up process on a physical rack, the system requires you rotate the account passwords by logging in to that rack’s EVO SDDC Manager virtual machine 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 system’s ability to manage the physical and logical entities.

When you rotate passwords on-demand in a steady-state system, you must run the `./vrm-cli.sh rotate-all` command in turn on each physical rack in the system. When the command is run on the first 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 first rack, you run the command on the subsequent racks, which changes the passwords for entities local to that rack.
You run the `vrm-cli.sh rotate-all` command by logging in to a rack's EVO 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 EVO SDDC Manager VM's root account, see “Credentials for Logging In To the EVO SDDC Manager (vrm) Virtual Machine,” on page 20.

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

- No failed workflows exist in the system. Use the Workflows area of the System page to verify the system has no workflows in a failure state.
- No active workflows, such as creating or deleting workload domains, are running in the system or are expected to run during the password rotation process. Schedule a window of time when you expect no active workflows running in the system before performing on-demand password rotation.

This chapter includes the following topics:

- “Credentials for Logging In To the EVO SDDC Manager (vrm) Virtual Machine,” on page 20
- “Look Up Account Credentials Using the Lookup-Password Command,” on page 20
- “Rotate All Passwords On-Demand for the Managed Physical and Logical Entities,” on page 21
- “vrm-cli Command Reference,” on page 23

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

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

When the hardware partner images a physical rack for delivery to you, a randomized password is generated for the root account for that rack’s EVO SDDC Manager virtual machine. The hardware partner sends you this system-generated password when the physical rack is shipped to you.

The `./vrm-cli.sh rotate-all` command does not change the password of the EVO 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 EVO 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 EVO SDDC Manager virtual machine's root and `vrack` accounts, they are not retrievable from the system. 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 the EVO SDDC system, you log in to the EVO 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 EVO SDDC Manager VM and run the `vrm-cli.sh lookup-password` command. See “Credentials for Logging In To the EVO SDDC Manager (vrm) Virtual Machine,” on page 20.

**Procedure**

1. Using the root account, connect and log in, for example by SSH, to the EVO SDDC Manager VM.
2. Change to the `/home/vrack/bin` directory.
3 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 that are managed by the system by the vrm-cli tool. The username and password for each account is displayed.

What to do next
Save the lookup command’s output to a secure location so that you can access it later and use it to log in to the components as needed.

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 EVO SDDC Manager virtual machine to rotate all of the passwords that are managed by the system. After running it on the first rack, run the ./vrm-cli.sh rotate-all command on the second rack, then on the third rack, and so on.

Prerequisites
Verify the following prerequisites are met:

- No failed workflows exist in the system. Use the Workflows area of the System page to verify the system has no workflows in a failure state.
- No active workflows, such as creating or deleting workload domains, are running in the system or are expected to run during the password rotation process. Schedule a window of time when you expect no active workflows running in the system before performing on-demand password rotation.
- You have the root account credentials to log in to each rack's EVO SDDC Manager VM. For details, see “Credentials for Logging In To the EVO SDDC Manager (vrm) Virtual Machine,” on page 20.

Procedure

1 For the first physical rack, using the root account, connect and log in, for example by SSH, to the rack's EVO SDDC Manager VM.
2 Stop the vrm-watchdogserver and vrm-tcserver services:
   
   
   service vrm-watchdogserver stop
   service vrm-tcserver stop
3 Change to the /home/vrack/VMware/vRack directory.
4 Save a copy of the /home/vrack/VMware/vRack/vrm.properties file to a secure location where you can access it later if necessary.
5 Change to the /home/vrack/bin directory.
6 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.
7 Save the output to a secure location so that you can compare it to the post-rotated listing.
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 is run on the first 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`.

```
./vrm-cli.sh rotate-password-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 EVO 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-tcserver service.

   service vrm-watchdogserver start

25 Repeat steps Step 13 through Step 24 for each physical rack in your system.

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 EVO 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

Lookup Commands

Use these commands to look up information about entities managed by the system.

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 system's logical inventory for the management and workload domains and lists their names.</td>
</tr>
<tr>
<td>lookup-history</td>
<td>store latest timestamp</td>
<td>Manages and retrieves the password history recorded in Zookeeper.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>./vrm-cli.sh lookup-history store records the local rack's current password state into Zookeeper.</td>
</tr>
<tr>
<td></td>
<td></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></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>lookup-password</td>
<td>None</td>
<td>Retrieves and lists the account credentials for the built-in accounts that are managed and rotated by the system. See also “Look Up Account Credentials Using the Lookup-Password Command,” on page 20.</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 EVO SDCC 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 system-generated randomized passwords for the accounts that are managed by the system, set up ESXi host passwords, and generate passwords that adhere to the system’s password policies.

**Note** Because some items in the system’s inventory are managed across all racks in the system 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 EVO 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 EVO SDDC Manager in which the command is run. When run from a specific rack’s EVO 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 EVO SDDC System,” on page 19.

<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-lsvm</td>
<td>None</td>
<td>Rotates passwords of the visible ISVM virtual appliances.</td>
</tr>
<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>Command</td>
<td>Subcommands and Input</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</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 the system 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 the system. 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 system'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 the system. 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>
<thead>
<tr>
<th>Command</th>
<th>Subcommands and Input</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure-snmp</td>
<td>full-path-to-input-json-file</td>
<td>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 the system has two ToR switches. Additionally, the second rack in a multirack system has the two spine switches for the system. 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</td>
</tr>
</tbody>
</table>

```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": [  # Users that the system will connect to the SNMP server with
    {
      "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
    },
    {
      "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, the system uses port 162 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 3-3. vrm-cli Configuration-Related Commands (Continued)

<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 management switch for the rack in which the command is run. See “Configure Syslog from the Switches to vRealize Log Insight,” on page 92.</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 system. See the Bringing-Up EVO SDDC on Additional Racks topic in the EVO SDDC Overview and Bring-Up Guide.</td>
</tr>
</tbody>
</table>
Managing Users and Groups

You can manage users and groups using the User Management page of the EVO SDDC Manager Web Interface. Your EVO SDDC system provides role-based access control.

For an overview of the User Management page, see “Tour of the EVO SDDC Manager Web Interface,” on page 12.

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

EVO 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 Your EVO SDDC System,” on page 29
- “Add Local Users and Groups,” on page 33
- “Assign Permissions to Users and Groups,” on page 35
- “Add a System Administrator,” on page 35
- “Role-Based Access Control,” on page 36
- “User Passwords in Your EVO SDDC System Environment,” on page 36

Active Directory and Your EVO SDDC System

To allow the users and groups in your Microsoft Active Directory domain to use their Active Directory credentials to log in to the EVO SDDC Manager Web interface as well as the vCenter Server instances that are deployed in your system, 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 deployment of your system, 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 your EVO SDDC system 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 system is deployed, you can log in to the system using the administrator@vsphere.local account that is generated by the system deployment 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 EVO SDDC Manager Web interface by assigning roles provided by your EVO SDDC system's role-based access control capabilities. See “Assign Permissions to Users and Groups,” on page 35 and “Role-Based Access Control,” on page 36.
- 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 your system 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 EVO SDDC System,” on page 32.

### Configure an Active Directory Domain as an Identity Source for your EVO SDDC System

Use the vSphere Web Client to log in to the management domain's vCenter Server Appliance and configure your Active Directory domain as an identity source used by the authentication service. When your Active Directory domain is configured as an identity source, you can grant permissions to those users and groups to log in to the EVO SDDC Manager client and access the system, 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 EVO SDDC Manager client as an administrator. You can launch the vSphere Web Client from the EVO 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 EVO 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>
<tr>
<td>Organizational unit</td>
<td>Optional. The canonical name of the organizational unit, for example, mydomain.com/MyOrganizationalUnit/mycomputer. <strong>IMPORTANT</strong> Use this field only if you are familiar with LDAP.</td>
</tr>
<tr>
<td>User name</td>
<td>User name in User Principal Name (UPN) format, for example, <a href="mailto:jchin@mydomain.com">jchin@mydomain.com</a>. This user must have a minimum of read access. <strong>IMPORTANT</strong> 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.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the user.</td>
</tr>
</tbody>
</table>

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 EVO SDDC Manager client to grant the appropriate permissions to the Active Directory domain’s users and groups for accessing your system using their Active Directory credentials. See “**Assign Permissions to Users and Groups**,” on page 35.

- 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](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 EVO SDDC System**

To allow your Active Directory users and groups to log in to the vSphere Web Client using their Active Directory credentials and access the vCenter Server objects and the objects from the vSphere products that integrate with the vSphere Web Client, you can use the Global Permissions area in the vSphere Web Client to grant them the appropriate permissions.

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 EVO SDDC System**,” on page 30.

**Procedure**

1. Open the view of the management domain’s vCenter Server resources in the vSphere Web Client.
   a. In the EVO 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 (').'</span> 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.


### Add Local Users and Groups

Use the vSphere Web Client to add local users and groups to the management domain. These users and groups are internal to the vCenter Single Sign-On authentication service for your EVO SDDC system and belong to the system’s management domain.

The Platform Services Controller component provides the single sign-on capability for the VMware SDDC components, including EVO SDDC Manager. Before you can authorize users and groups to perform operations using the EVO SDDC Manager Web interface, 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 to the management domain or adding them as users and groups to the management domain’s 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 system.

**Prerequisites**

Verify that you are logged in to the EVO SDDC Manager Web interface as an administrator. You access the management domain by launching the vSDDC Manager Web Client from the EVO SDDC Manager Web interface.
Procedure

1. Open the view of the management domain’s vCenter Server resources in the vSphere Web Client.
   a. In the EVO 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 system. <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 system. Perform one of the following next steps.

- Add the local user to a group using the Platform Services Controller Web interface. When users are added to a group, you can assign permissions to the group so that all of the users in the group receive the same permissions for performing operations in the system. Then use the User Management page in the EVO SDDC Manager Web interface to assign a role to that group.
- Use the User Management page to authorize the local user for performing operations in the system by assigning an appropriate role to that user. See “Assign Permissions to Users and Groups,” on page 35.
Assign Permissions to Users and Groups

Your EVO SDDC system uses roles, and their associated rights, to determine which users and groups can perform which operations in the system.

System administrators assign roles to users and groups using the Permissions area of the User Management page. The ability to perform operations in the system 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 EVO SDDC system. See “Active Directory and Your EVO SDDC System,” on page 29, “Configure an Active Directory Domain as an Identity Source for your EVO SDDC System,” on page 30, and “Add Local Users and Groups,” on page 33.

Procedure

1. In the EVO SDDC Manager Web interface, navigate to User Management > Users & Groups.
2. Click Add User/Group.
   The window displays fields to select users and groups that are known to your system.
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 in the system. 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 a System Administrator

You can add a system administrator for your EVO SDDC system by giving a user account the Admin role.

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

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 access the EVO SDDC system. See “Active Directory and Your EVO SDDC System,” on page 29, “Configure an Active Directory Domain as an Identity Source for your EVO SDDC System,” on page 30, and “Add Local Users and Groups,” on page 33.
Procedure

1. In the EVO SDDC Manager Web interface, 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 EVO SDDC Manager Web interface and perform system administrator operations.

Role-Based Access Control

Your EVO SDDC system uses roles and rights to determine what operations a user can perform in the system. EVO SDDC 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 EVO SDDC Manager and access the system.

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 operations in the EVO SDDC system. 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 EVO SDDC System Environment

The password restrictions, lockout, and expiration for a user’s password in your EVO SDDC system 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 EVO SDDC Manager Web interface 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 system’s single sign-on (SSO) domain’s internal identity source that is created during system setup 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 EVO SDDC system 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 system setup. If you have configured your system to use another identity provider, the password policy of that identity provider applies instead. The name of your system’s SSO domain was specified in the configuration wizard during the system bring-up process.

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 EVO SDDC Manager Web interface as an administrator. You access the internal identity source by launching the vSphere Web Client from the EVO SDDC Manager Web interface.

Procedure

1. Open the view of the management domain’s vCenter Server resources in the vSphere Web Client.
   a. In the EVO 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 system setup, the default password policy parameters are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum lifetime</strong></td>
<td>Password must be changed every 90 days</td>
</tr>
<tr>
<td><strong>Restrict re-use</strong></td>
<td>Users cannot reuse any previous 5 passwords</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: Special characters, such as &amp; # % Alphabetic characters, such as A b c D Uppercase characters, such as A B C Lowercase characters, such as a b c Numeric characters, such as 1 2 3 The minimum number of alphabetic characters must be no less than the combined uppercase and lowercase requirements.</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 EVO SDDC Manager, you can work with the physical resources in your EVO SDDC system.

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

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 this system. To see detailed information about the physical switches and hosts for a particular rack in the list, click the rack’s name. For an alternative view of the physical rack information, you can use the Map view.

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

- “Switch Details and Operations,” on page 40
- “ESXi Host Details and Operations,” on page 40

EVO 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 system calculates the hardware health state of the resource based on the current set of alerts that the EVO 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 EVO SDDC alerts reported of warning, error, or critical severity.</td>
</tr>
<tr>
<td>🚨</td>
<td>The resource has EVO SDDC alerts reported with warning severity.</td>
</tr>
<tr>
<td>🚨</td>
<td>The resource has EVO SDDC alerts reported with error severity.</td>
</tr>
<tr>
<td>🚨</td>
<td>The resource has EVO SDDC 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 the system and information about its built-in monitoring capabilities, see:

- “EVO SDDC System Alerts Raised During Ongoing System Operations,” on page 84
- Chapter 7, “Monitoring Your EVO SDDC System,” on page 71

**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
- Hardware health status

The hardware health status reflects the severities of the EVO SDDC 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 a system of two or more racks. Spine switches are installed when a second rack is added to the first rack in the system.

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

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

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

By default, the system’s 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](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](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](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 as part of your EVO SDDC system. The system chooses the appropriate number of hosts required to accommodate redundancy capabilities and VMware SDDC best practices. When the system provisions a management domain, it automatically provisions and configures the management domain with the necessary SDDC virtual infrastructure: vSphere, vCenter Server, Virtual SAN, NSX for vSphere,
vRealize Operations, and vRealize Log Insight. The appropriate management packs and content packs are deployed in the vRealize Operations and vRealize Log Insight components and are automatically configured for the management domain’s virtual infrastructure. For more information about the management domain, see the EVO SDDC Overview and Bring-Up Guide.

The two pre-packaged environments you can deploy in your EVO SDDC system are named Virtual Infrastructure (VI) and Virtual Desktop Infrastructure (VDI). To provision one of these pre-packaged environments, you use an EVO SDDC Manager workflow to carve a pool of capacity out of the system’s available capacity, and the system provisions the environment, called the workload domain, using that carved-out pool of capacity. The system automatically determines the required amount of capacity to carve out based on your input for:

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

The system provides this policy-driven approach to capacity deployment. Based on the levels you specify, your system reserves the necessary hardware resources out of the physical infrastructure available in the system. Then using those reserved hardware resources, the system deploys the appropriate number of vCenter Server instances, 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 system 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 vRealize Log Insight and vRealize Operations Manager

The result is a workload-ready SDDC environment.

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

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

This chapter includes the following topics:

- “Creating and Provisioning Workload Domains,” on page 42
- “Expanding Management and Workload Domains,” on page 65
- “Delete a Workload Domain,” on page 67
- “Enabling Virtual SAN Space Efficiency Features in All-Flash Systems,” on page 68
- “Manually Update the Credentials for the vRealize Operations for Horizon Broker Agent When Account Credentials Change for the Connection Server Administrator Account,” on page 69

**Creating and Provisioning Workload Domains**

The flexibility of the software-defined data center provided by an EVO SDDC system gives you the ability to offer virtual infrastructure to your consumers with minimal overhead. Your EVO SDDC system comes with the ability to provision pre-packaged environments on which you can base service offerings.

The two pre-packaged environments you can deploy in your EVO SDDC system 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 EVO SDDC Manager client. When you create a VI workload domain, your EVO SDDC system reserves the necessary pool of capacity from the system’s resources and deploys the VMware SDDC software stack appropriate for the VI infrastructure.

The pre-packaged VMware software components that support the deployment of the virtual infrastructure include vCenter Server, Virtual SAN, NSX Manager and the required controllers, vRealize Operations, and vRealize Log Insight. As the system creates and provisions the VI workload domain, it deploys one or more vCenter Server instances, associates the ESXi hosts with those instances and performs the appropriate configuration of the hosts, virtual networks, and integration with vRealize Operations and vRealize Log Insight.

The system uses the information you provide in each step of the VI workload domain creation wizard to determine the virtual environment it will 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 the system’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 system’s 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 system 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 46.

Procedure

1. **Start the Wizard to Create a VI Workload Domain** on page 44
   
   You start the Configure VI wizard from the Dashboard page of the EVO SDDC Manager Web interface.
2 Specify General Information about the VI Workload Domain on page 44
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 45
At the Workload step of the creation wizard, you specify the levels of performance, availability, and hardware capacities you want the system to provision for this VI workload domain.

4 Specify the Networking Information for the Virtual Infrastructure Workload Domain on page 46
Specify the networking information for the VI workload domain.

5 Review the Details and Start the Creation Workflow on page 49
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 49 section of “Review the Details and Start the Creation Workflow,” on page 49.

Start the Wizard to Create a VI Workload Domain
You start the Configure VI wizard from the Dashboard page of the EVO SDDC Manager Web interface.

Prerequisites
Verify that you have met the prerequisites described in “Create a Virtual Infrastructure Workload Domain,” on page 43.

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. You can also select steps in that top wizard progress line to move between steps.

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
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 the system to provision for this VI workload domain.

Based on your selections, the system will determine:
- The number of hosts that it needs to fulfill those selections
- Which specific hosts in the system 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>
</table>
| Low    | With this choice, the following Virtual SAN parameters are used:  
- Number of failures to tolerate: zero (0).  
Because Virtual SAN requires a minimum of three hosts by default, three hosts are assigned to the virtual infrastructure. |
| Normal | With this choice, the following Virtual SAN parameters are used:  
- Number of failures to tolerate: one (1).  
Because Virtual SAN requires a minimum of three hosts by default, three hosts are assigned to the virtual infrastructure. |
| High   | With this choice, the following Virtual SAN parameters are used:  
- Number of failures to tolerate: two (2).  
Because Virtual SAN requires a minimum of five hosts by default for this setting, five hosts are assigned to the virtual infrastructure. |

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 system uses the management network that was configured during the system’s bring-up process. During deployment of the VI workload domain’s infrastructure, the system 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 system 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 the system bring-up process for that subnet. See “About Excluding IP Address from System Use,” on page 100.

**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 system’s 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 system’s bring-up process. If you choose to use this default, but the system 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 system’s bring-up process and allocates a VLAN ID from its pool. If you choose to use this default, but the system 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>
</tbody>
</table>
Table 6-1. VI Workload Domain Network Configurations (Continued)

<table>
<thead>
<tr>
<th>Network Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 system’s bring-up process. If you choose to use this default, but the system detects inadequate IP address space in the existing VXLAN network, you must specify a new configuration at that step in the wizard.</td>
</tr>
<tr>
<td>Data Center connection</td>
<td>Used for access from outside the system to the workloads that you run in the workload domain. In the wizard, you can select the network configuration that was configured during the system’s bring-up process, one that was configured in advance using the Data Center Connections settings screen, or enter a new configuration at that wizard step. 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.</td>
</tr>
</tbody>
</table>

**Prerequisites**

Verify that you have met the networking prerequisites as described in “Create a Virtual Infrastructure Workload Domain,” on page 43.

**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 in your system. 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 the system’s 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 system 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 when your EVO SDDC system was deployed. 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 system bring-up process. See “About Excluding IP Address from System Use,” on page 100.

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 when your system was deployed, 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 system 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 when your system was deployed, 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 system 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 the system bring-up process. See “About Excluding IP Address from System Use,” on page 100.

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

- To use the same VXLAN network configuration that was specified when your system was deployed, 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 existing configurations that is already saved in this system. During ongoing system operations, Data Center configurations can be saved 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 system 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 system creates and deploys the virtual infrastructure for this workload domain.

The hosts that will be added to the workload domain are listed along with the names of the physical racks in which those hosts are located. Unless you chose High availability, the hosts can be located in different physical racks.

This page also displays the IP addresses of the vCenter Server instances that will be deployed to manage the resources assigned to the virtual environment.

Procedure

1. Scroll down the page to review the information.
2. (Optional) Print the information or download a printable version to print later.
3. Click Finish to begin the creation process.

The VI Workload Triggered window appears, letting you know that the system 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 Setup 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 present in the system. From the Dashboard page, you can use the View Details button 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 49.

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 your system creates a VI workload domain, it creates and configures the required VMware SDDC environment within your EVO SDDC system. Within that SDDC environment, you can perform the typical workload-related tasks that you would typically do in a virtual environment built on a vSphere data center.

Note All of the capabilities of a VMware SDDC are available to you in the VI workload domain’s environment, such as creating, provisioning, and deploying virtual machines, configuring the software-defined networking features, and so on.

Procedure

1. From the EVO 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 EVO SDDC Manager Web interface. When you create a VDI workload domain, your EVO SDDC system 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, the EVO SDDC system 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. The system first runs the VI workload domain creation workflow, to create a virtual infrastructure (VI) environment. For a description of VI workload domains and the pre-packaged VMware SDDC software that makes up a virtual infrastructure environment, see “Create a Virtual Infrastructure Workload Domain,” on page 43. The system sizes this VI workload domain 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 system deploys and configures the additional pre-packaged 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 by the system during 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. In the VDI environment creation process, the system 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 the system 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 54.

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 54.

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 system places the virtual desktops on this network and configures the network to carry traffic between the EVO SDDC system and the environment external to the EVO SDDC system. Prior to starting the VDI workload domain creation wizard, contact your organization’s Data Center Network Administrator to determine the correct vlan ID, subnet, subnet mask, default gateway, and DNS server information to use for this VDI environment’s data center network.

Your Data Center Network administrator must ensure that the settings for the data center network provide for secure traffic and is routable outside the EVO SDDC system. Your Data Center Network administrator must also ensure that this EVO SDDC system’s public management network is able to communicate with that secure data center network. Otherwise, the VDI workload domain creation workflow will fail. This EVO SDDC system’s management network must be able to communicate with that secure data center network to provision and manage the VDI environment. This management network’s information is specified during the system’s bring-up process. By the time you are creating VDI workload domains, the management network is already configured in the system.

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 into the system. 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 101.

To review the details of networks already configured in this system, 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 EVO SDDC. 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 the EVO SDDC system and the virtual desktops within the system.
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. With this 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 (http://pubs.vmware.com/horizon-62-view/topic/com.vmware.horizon-view.installation.doc/GUID-3446495C-FEC8-425C-AFF8-A6CAABAE973.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 54
   Using the **Deploy Desktops** option in the VDI workload domain creation wizard means that the system will deploy the virtual machines that are the virtual desktops as part of the VDI environment creation process. 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 57
   You start the Configure VDI wizard from the Dashboard page of the EVO SDDC Manager Web interface.

3. **Specify the General Configuration Information for the VDI Workload Domain** on page 58
   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 59
   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 60
   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 61
   Specify the networking information for the VDI workload domain.

7 Specify the Windows Images for the VDI Environment on page 62
   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 the system deploy desktops 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 63
   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 64
   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 64, 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 system will deploy the virtual machines that are the virtual desktops as part of the VDI environment creation process. 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, the EVO SDDC system 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 EVO SDDC release, the Windows operating system can be Windows 7, Windows 8, or Windows 10. The EVO SDDC system 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 system-generated 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 Desks 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](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 Desks 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 EVO SDDC supports using for virtual desktops. The OSOT is available at [https://labs.vmware.com/flings/vmware-os-optimization-tool](https://labs.vmware.com/flings/vmware-os-optimization-tool)

To achieve successful results in the VDI environment in your EVO SDDC system, 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 EVO SDDC 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](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 EVO SDDC system, the virtual desktops that are created based on the prepared Windows image will be unusable.

This requirement is determined by the View Composer software that is deployed in the VDI environment. As described in VMware KB article 1026556, by default the View Composer QuickPrep process uses KMS to activate Windows guest operating systems. To ensure linked-clone desktops are properly activated, you must use KMS license activation on the parent virtual machine. QuickPrep does not use other volume activation methods such as Multiple Activation Key (MAK) licensing.

You must 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

For example, disabling certain Windows 7, Windows 8/8.1, and Windows 10 services and tasks can result in performance benefits for the virtual desktops, as described in the Horizon 6 product documentation topic Optimizing Windows for Linked-Clone Virtual Machines at pubs.vmware.com/horizon-62-view/topic/com.vmware.horizon-view.desktops.doc/GUID-E938922D-7FD4-41E7-A774-0C811CA6595D.html.

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 EVO SDDC Manager Web interface.

Prerequisites

Verify that you have met the prerequisites described in “Create a VDI Workload Domain,” on page 50.

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. You can also select steps in that top wizard progress line to move between steps.
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 system 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 system 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 system 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 system 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 50 for the type of Active Directory infrastructure you want to use with this VDI environment.
Procedure

1. Select whether to use your organization's existing Active Directory domain or to have the system 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.  
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 EVO SDDC system does not install DHCP for the desktops. The system expects that you have DHCP installed and reachable by broadcast from the Data Center network configuration. |
| Internal | When you select this choice, the system 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 50.
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

Specify the networking information for the VDI workload domain.

The servers created for the VDI infrastructure will be installed on the system’s existing management network and the virtual desktops will be installed on the data center network. The data center network specified in this step is 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 provide a DMZ network configuration.

**Important**  Ensure that the configuration for the data center network, the DMZ network configuration, and the system’s management network meets the networking prerequisites described in “Create a VDI Workload Domain,” on page 50. 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 50.

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 saved in this system. During ongoing system 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 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 the system deploy desktops 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 54.

If the Windows Server 2012 ISO file and Windows OVA files have already been uploaded into the system 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 50 and “Prepare the OVA for the Virtual Desktops,” on page 54.

Procedure

   - 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 system for this purpose, because it was previously uploaded into the system 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 in the system for this purpose, because it was previously uploaded into the system 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 system 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 system 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 Setup page and click **Tasks**. When the VDI workload domain is created, the Dashboard page refreshes to indicate the new domain present in the system. 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 launch the View Administrator Web interface to 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 64.
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 View Details 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 your system’s integrated 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 integrated vRealize Log Insight instance 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 that is integrated in your system, see “Get Started Using the Integrated vRealize Log Insight,” on page 91.</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>
</tbody>
</table>

Implement App Volumes | 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. |
### 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. |

### 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 EVO SDDC system has a management domain. When the system expands a management domain, it 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 EVO 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.
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>Expand Method - By Capacity</td>
<td>Type the amount of CPU, memory, and storage capacity to add to the management domain.</td>
</tr>
</tbody>
</table>

Proceed to the next step by clicking Next.

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 system 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 system 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 Setup page and click Tasks.

**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 EVO 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>

Proceed to the next step by clicking Next.

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 system 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 Setup 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 EVO 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 Specify the topology details to use for these virtual desktops and click Next.

4 Specify the details of the Active Directory that you want associated with these virtual desktops and click Next.

5 At the Virtual Desktops step, specify whether to use App Volumes to manage the added virtual desktops and click Next.

6 At the Virtual Desktops step, specify details about the virtual desktops and click Next.

7 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 Setup page and click Tasks.

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 EVO SDDC system.

**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.

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 EVO 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.

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 Setup page and click Tasks.
Enabling Virtual SAN Space Efficiency Features in All-Flash Systems

Your EVO SDDC system might be an all-flash storage environment. For all-flash storage, the system's Virtual SAN space efficiency features enable you to reduce the amount of space for storing data in your workload domains.

As provided by the Virtual SAN features installed in an all-flash EVO SDDC system, 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 Virtual SAN 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 Virtual SAN 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 Virtual SAN policy to enable these features.

For detailed information about these Virtual SAN space efficiency features, see the Virtual SAN 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 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 Virtual SAN 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: http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.virtualsan.doc/GUID-6D818555-8DE8-4F06-9498-66903FB9C775.html

You enable these features on a workload domain's underlying environment by using the vSphere Web Client to edit the Virtual SAN 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 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-FE72F6CD6227.html, 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 integrated in your system.

When you create a VDI workload domain in the system, the system configures the VDI environment to use the features of vRealize Operations® for Horizon® to collect performance data from the VDI environment and provide that data in the vRealize Operations Manager instance integrated in your system. 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 system installs the broker agent, credentials are paired between the broker agent and the account credentials the system sets up for the Horizon Administrator account when it deploys 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 the VDI environments in your system, 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 59.

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.
Monitoring Your EVO SDDC System

Your EVO SDDC system provides built-in capabilities to help you perform effective operations monitoring, troubleshooting, performance management, infrastructure capacity planning, and compliance monitoring and auditing.

You use the built-in monitoring capabilities of the system 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</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 of your system 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 the EVO SDDC system, an audit event is an event raised for a user-initiated or system-generated action. 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 EVO SDDC Manager client
- Users performing actions involving workflows, such as creating a workload domain
- User actions involving system 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 EVO SDDC system

Examples of system-initiated actions that raise audit events:

- System validation activity, such as powering on of the system
- All system workflows and tasks, including successful and failed actions
- All system actions 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. The system has a built-in capability for detecting problems using events raised at a system or device level, and generating alerts that warn you about problems that would impact workload Service Level Agreements (SLAs) or which require human intervention. In the system, 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 the system that changes the state of a system resource. A workflow is a long-running group of tasks that perform an overall goal, such as creating a workload domain.

Integration with vRealize Log Insight

Events and log content for the system's physical resources and the VMware SDDC virtual infrastructure are sent to the vRealize Log Insight software product that is integrated in the system by default. As a result, you can log in to the integrated vRealize Log Insight Web interface and obtain a unified view of event and syslog information to assist with troubleshooting. Data from the events and audit events raised by the EVO SDDC system 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 the vRealize Log Insight Capabilities in Your System,” on page 89.

Note: In this release, the integrated vRealize Log Insight software is configured for monitoring of the EVO SDDC system only. Configuring the integrated vRealize Log Insight to monitor additional applications or VMs is not supported in this release.

Integration with vRealize Operations Manager

The vCenter Adapter that is used to connect vRealize Operations Manager to one or more instances of vCenter Server is automatically installed and configured into the integrated vRealize Operations Manager. The management and workload domains' vCenter Server instances send their event and metric data into vRealize Operations Manager using that
Managing Workflows and Tasks

From the System Status page of the EVO SDDC Manager Web interface, you can work with the workflows and tasks that have been reported by your EVO SDDC system. A task is a unit of work performed by the system that changes the state of a system 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>Workflow Tasks</th>
<th>ALL</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORLFDROWS</td>
<td>TASKS</td>
</tr>
<tr>
<td>2</td>
<td>167</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 system. 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 its tasks and detailed information. When you expand a workflow in the list, you can click View Sub Tasks to see detailed information about each of the tasks involved in that workflow. If a task is in a failed state, you can have the system attempt to rerun it by clicking RERUN.
Task Details

When you click the View Sub Tasks link 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 workflow to see its tasks and detailed information. When you expand a workflow in the list, you can click View Sub Tasks to see detailed information about each of the tasks involved in that workflow. If a task is in a failed state, you can have the system attempt to rerun it by clicking RERUN.

Managing Alerts, Events, and Audit Events

From the System Status page of the EVO SDDC Manager Web interface, you can work with the alerts, events, and audit events that have been reported by your EVO SDDC system.

On the System Status page, you can see the total count of alerts, events, and audit events at a glance, and then use the View Details links to drill-down for details about each type.

The integrated vRealize Log Insight is the final destination for all events. EVO 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 the system has 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.

![Alert Details](image)

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 “EVO SDDC System Alerts Raised During Ongoing System Operations,” on page 84.

**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 system.

This screen includes events that have been raised by EVO 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 integrated 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 EVO SDDC Manager that have not yet been forwarded to the integrated vRealize Log Insight. Because this count does not include events that have already been forwarded to the integrated vRealize Log Insight, 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 the vRealize Log Insight Capabilities in Your System,” on page 89.

- Click Catalog to open the Event Catalog and view the definitions of all of the events that the system monitors and records as part of its event-driven problem detection capabilities. See “Event Catalog,” on page 78.

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 the vRealize Log Insight Capabilities in Your System,” on page 89.
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 system 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 EVO SDDC Manager dashboard by navigating to the System Status page and clicking on the View Details button in the Events area.

<table>
<thead>
<tr>
<th>SEVERITY</th>
<th>ALL ▼</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVER_DOWN ▶</td>
<td></td>
</tr>
<tr>
<td>USER_LOG_OUT_FAILED ▶</td>
<td></td>
</tr>
<tr>
<td>STORAGE_CONTROLLER_UP ▶</td>
<td></td>
</tr>
</tbody>
</table>

Expand an event to see its definition, containing details such as its severity, description, resource hierarchy, categories, and type.

**HDD_EXCESSIVE_WRITE_ERRORS ▶**

<table>
<thead>
<tr>
<th>Severity</th>
<th>WARNING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Hierarchy</td>
<td>RACK, SERVER, STORAGE</td>
</tr>
<tr>
<td>Categories</td>
<td>SERVER, HARDWARE</td>
</tr>
<tr>
<td>Type</td>
<td>NORMAL</td>
</tr>
<tr>
<td>Description</td>
<td>Storage drive for rack [RACK_NAME] server [SERVER] and HDD [STORAGE] has excessive write errors</td>
</tr>
</tbody>
</table>

You can filter the displayed list by the event severity.
Hardware Operational Events

The system raises these events that are related to hardware operations. The event is raised when the system 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 by the EVO SDDC System

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Severity</th>
<th>Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMC_AUTHENTICATION_FAILURE</td>
<td>ERROR</td>
<td>The system is unable to authenticate to the server's out-of-band (OOB) management port.</td>
</tr>
<tr>
<td>BMC_MANAGEMENT_FAILURE</td>
<td>ERROR</td>
<td>The system failed to perform a management operation using the server's OOB management port.</td>
</tr>
<tr>
<td>BMC_NOT_REACHABLE</td>
<td>ERROR</td>
<td>The system 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 system 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 system 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_READ_ERRORS</td>
<td>WARNING</td>
<td>Excessive read errors reported 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>HDD_TEMPERATURE_ABOVE_THRESHOLD</td>
<td>WARNING</td>
<td>HDD storage drive temperature has reached its maximum safe operating temperature.</td>
</tr>
<tr>
<td>HDD_UP</td>
<td>INFO</td>
<td>Operational status is up for an HDD storage drive.</td>
</tr>
<tr>
<td>HDD_WEAROUT_ABOVE_THRESHOLD</td>
<td>WARNING</td>
<td>Wear-out state of an HDD storage drive is above its defined threshold.</td>
</tr>
<tr>
<td>HMS_AGENT_DOWN</td>
<td>CRITICAL</td>
<td>A physical rack's Hardware Management Services agent is down.</td>
</tr>
<tr>
<td>HMS_AGENT_UP</td>
<td>INFO</td>
<td>A physical rack's Hardware Management Services agent is operational.</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>MANAGEMENT_SWITCH_DOWN</td>
<td>CRITICAL</td>
<td>Operational status is down for a physical rack’s management switch.</td>
</tr>
<tr>
<td>MANAGEMENT_SWITCH_PORT_DOWN</td>
<td>WARNING</td>
<td>Operational status is down for a switch port in a physical rack’s management switch.</td>
</tr>
<tr>
<td>MANAGEMENT_SWITCH_PORT_UP</td>
<td>INFO</td>
<td>Operational status is up for a switch port in a physical rack’s management switch.</td>
</tr>
<tr>
<td>MANAGEMENT_SWITCH_UP</td>
<td>INFO</td>
<td>Operational status is up for a physical rack’s management switch.</td>
</tr>
<tr>
<td>NIC_LINK_DOWN</td>
<td>WARNING</td>
<td>Deprecated. NIC_PORT_DOWN event is used instead.</td>
</tr>
<tr>
<td>NIC_PACKET_DROP_ABOVE_THRESHOLD</td>
<td>WARNING</td>
<td>A NIC’s packet drop is above its defined threshold.</td>
</tr>
<tr>
<td>NIC_PORT_DOWN</td>
<td>ERROR</td>
<td>Operational status is down for a NIC port.</td>
</tr>
<tr>
<td>NIC_PORT_UP</td>
<td>INFO</td>
<td>Operational status is up for a NIC port.</td>
</tr>
<tr>
<td>PCH_TEMPERATURE_ABOVE_THRESHOLD</td>
<td>WARNING</td>
<td>Platform controller hub [PCH] temperature has reached its maximum safe operating temperature.</td>
</tr>
<tr>
<td>SERVER_DOWN</td>
<td>ERROR</td>
<td>Server is in the powered-down state.</td>
</tr>
<tr>
<td>SERVER_PCIE_ERROR</td>
<td>ERROR</td>
<td>A server’s system has PCIe errors.</td>
</tr>
<tr>
<td>SERVER_POST_ERROR</td>
<td>ERROR</td>
<td>A server’s system has POST failures.</td>
</tr>
<tr>
<td>SERVER_UP</td>
<td>INFO</td>
<td>Server is in the powered-up state.</td>
</tr>
<tr>
<td>SPINE_SWITCH_DOWN</td>
<td>ERROR</td>
<td>Operational status is down for a physical rack’s spine switch.</td>
</tr>
<tr>
<td>SPINE_SWITCH_PORT_DOWN</td>
<td>WARNING</td>
<td>Operational status is down for a switch port: in a physical rack’s spine switch.</td>
</tr>
<tr>
<td>SPINE_SWITCH_PORT_UP</td>
<td>INFO</td>
<td>Operational status is up for a switch port: in a physical rack’s spine switch.</td>
</tr>
<tr>
<td>SPINE_SWITCH_UP</td>
<td>INFO</td>
<td>Operational status is up for a physical rack’s spine switch.</td>
</tr>
<tr>
<td>SSD_DOWN</td>
<td>ERROR</td>
<td>Operational status is down for an SSD storage device.</td>
</tr>
<tr>
<td>SSD_EXCESSIVE_READ_ERRORS</td>
<td>WARNING</td>
<td>Excessive read errors reported for an SSD storage drive.</td>
</tr>
<tr>
<td>SSD_EXCESSIVE_WRITE_ERRORS</td>
<td>WARNING</td>
<td>Excessive write errors reported for an SSD storage drive.</td>
</tr>
<tr>
<td>SSD_TEMPERATURE_ABOVE_THRESHOLD</td>
<td>WARNING</td>
<td>SSD storage drive temperature has reached its maximum safe operating temperature.</td>
</tr>
<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 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 switch.</td>
</tr>
<tr>
<td>TOR_SWITCH_PORT_DOWN</td>
<td>WARNING</td>
<td>Operational status is down for a switch port in a physical rack’s ToR switch.</td>
</tr>
</tbody>
</table>
Table 7.1. Hardware Operational Events Raised by the EVO SDDC System (Continued)

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Severity</th>
<th>Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOR_SWITCH_PORT_UP</td>
<td>INFO</td>
<td>Operational status is up for a switch port in a 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 switch.</td>
</tr>
</tbody>
</table>

**Audit Events**

In the EVO SDDC system, an audit event is an event raised for a user-initiated or system-generated action. The audit event is raised when the system 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 by the EVO SDDC System

<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 system has added a new subtask to a workload-domain-related workflow. The system creates workflows for certain user actions and this event is raised when the system 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 system.</td>
</tr>
<tr>
<td>DOMAINVIRTUAL_INFRASTRUCTURE_ADD</td>
<td>INFO</td>
<td>User has initiated the operation to create a Virtual Infrastructure workload domain in the system.</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 succeeded.</td>
</tr>
<tr>
<td>PERMISSION_REVOKE_FAILED</td>
<td>WARNING</td>
<td>The user-initiated action to remove a role from a user and revoke 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 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 to another 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 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 system has failed.</td>
</tr>
</tbody>
</table>
### Table 7-2. Audit Events Raised by the EVO SDDC System (Continued)

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Severity</th>
<th>Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROLE_ADD_SUCCEEDED</td>
<td>INFO</td>
<td>The user-initiated action to create a new role in the system has completed 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 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 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 EVO SDDC Manager failed for the user.</td>
</tr>
<tr>
<td>USER_LOG_IN_SUCCEEDED</td>
<td>INFO</td>
<td>Log in to EVO SDDC Manager succeeded for the user.</td>
</tr>
<tr>
<td>USER_LOG_OUT_FAILED</td>
<td>WARNING</td>
<td>Log out from EVO SDDC Manager failed for the user.</td>
</tr>
<tr>
<td>USER_LOG_OUT_SUCCEEDED</td>
<td>INFO</td>
<td>Log out from EVO SDDC Manager succeeded for the user.</td>
</tr>
</tbody>
</table>

### Life Cycle Management Events

The system raises these events that are related to the life cycle management operations that are available in your system. As appropriate for the particular event, when the event is raised, the event report includes information such as the type of operation that was performed, whether the operation succeeded or failed, and the condition for which the event was raised. For details about using the life cycle management features available in your system, see Chapter 10, “Lifecycle Management,” on page 109.

### Table 7-3. Life Cycle Management Events Raised by the EVO SDDC System

<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 system failed to download a bundle from the remote source location. The exact cause of the failure could not be detected by the system.</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>Event Name</td>
<td>Severity</td>
<td>Short Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------------</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 system 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 system 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 system failed to retrieve the bundle manifest file from the remote source location. The exact cause of the failure could not be detected by the system.</td>
</tr>
<tr>
<td>BUNDLE_MANIFEST_INVALID</td>
<td>ERROR</td>
<td>The system has determined that the bundle manifest which was retrieved from the remote source location and written to the system's 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 system 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 system cannot locate the specified bundle at the expected location within the system's bundle repository.</td>
</tr>
<tr>
<td>BUNDLE_REPO_WRITE_FAILURE</td>
<td>ERROR</td>
<td>Problems with the system's 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 system has automatically cancelled a scheduled upgrade because a workflow is taking place in the system, 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 system has determined all of the system 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>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 system 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 system cannot locate an index file at the remote source location.</td>
</tr>
</tbody>
</table>
Table 7-3. Life Cycle Management Events Raised by the EVO SDDC System (Continued)

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Severity</th>
<th>Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMWARE_DEPOT_INSUFFICIENT_PERMISSION</td>
<td>ERROR</td>
<td>The system 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 system cannot locate a manifest file at the remote source location.</td>
</tr>
<tr>
<td>VMWARE_DEPOT_MISSING_BUNDLE</td>
<td>ERROR</td>
<td>The system 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 system 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 EVO SDDC system’s 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 “EVO SDDC System Alerts Raised During Ongoing System Operations,” on page 84.

EVO SDDC System Alerts Raised During Ongoing System Operations

An alert is a stateful record for a problem. The EVO SDDC system 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 system’s bringup process and during ongoing system operations.

During ongoing system operations, the system raises alerts for problems detected as a result of its periodic polling of hardware status or from alert-raising events. Alerts are not generated for fleeting conditions or for problems that the system can resolve itself. The system raises alerts for issues that:

- Persist
- Require human intervention to resolve

The system 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 system polls the servers and switches 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 system polls the hardware resources 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 on the system 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 system’s manifest.
After each polling interval, the system calls its built-in problem-detection service to analyze the updated status and inventory information and determine whether a persistent condition exists. If a problem that requires human intervention exists, the system raises an alert. Even though the system can generate multiple events for a particular outstanding problem, it creates only one alert about the persistent problem. You then verify and resolve the reported problem and clear the alert using the EVO SDDC Manager Web interface.

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 78 for a list of the event definitions that you can view in the Event Catalog user interface.

Some of the EVO SDDC system alerts are more likely to be raised during the Power On System Validation (POSV) portion of the system’s bringup process. As an example, the alert named EVO_SDDC_BUNDLE_INCOMPLETE_ALERT is raised during POSV if the system detects the EVO SDDC ISO file is missing some elements. For the list of alerts that are raised during POSV, see the EVO SDDC Overview and Bring-Up Guide.

You can use the Alerts Catalog page in the EVO SDDC Manager Web interface to view the EVO SDDC system’s 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 84.

Table 7-4. EVO SDDC System 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>ERROR</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>ERROR</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>ERROR</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 first rack. The system 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>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>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_TEMPERATURE_ABOVE_UPPER_THRESHOLD_ALERT</td>
<td>A CPU temperature has reached its maximum safe operating temperature.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td></td>
<td>This alert is initiated by the CPU_TEMPERATURE_ABOVE_UPPER_THRESHOLD event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU_TEMPERATURE BELOW_LOWER_THRESHOLD_ALERT</td>
<td>A CPU temperature has reached its minimum safe operating temperature.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td></td>
<td>This alert is initiated by the CPU_TEMPERATURE BELOW_LOWER_THRESHOLD event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU_THERMAL_TRIP_ERROR_ALERT</td>
<td>A server CPU has shut down due to thermal error.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td></td>
<td>This alert is initiated by the CPU_THERMAL_TRIP_ERROR event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU_UNDETECTTED_ALERT</td>
<td>The polling did not detect a CPU that matches what is expected according to the</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td></td>
<td>manifest.</td>
<td></td>
<td></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</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td></td>
<td>memory. This alert is initiated by the DIMM_ECC_MEMORY_ERROR event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIMM_TEMPERATURE ABOVE_THRESHOLD_ALERT</td>
<td>Memory temperature has reached its maximum safe operating temperature.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td></td>
<td>This alert is initiated by the DIMM_TEMPERATURE ABOVE_THRESHOLD event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIMM_THERMAL_TRIP_ALERT</td>
<td>Memory has shut down due to thermal error.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td></td>
<td>This alert is initiated by the DIMM_THERMAL_TRIP event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EVO_SDDC_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>EVO_SDDC_BUNDLE_INVALID_alert</td>
<td>Checksum validation for the ISO file failed.</td>
<td>CRITICAL</td>
<td>Event</td>
</tr>
<tr>
<td>EVO_SDDC_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>
<tr>
<td>HDD_DOWN_ALERT</td>
<td>Operational status is down for an HDD.</td>
<td>ERROR</td>
<td>Event</td>
</tr>
<tr>
<td></td>
<td>This alert is initiated by the HDD_DOWN event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDD_EXCESSIVE_READ_ERRORS_ALERT</td>
<td>Excessive read errors reported for an HDD.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td></td>
<td>This alert is initiated by the HDD_EXCESSIVE_READ_ERRORS event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDD_EXCESSIVE_WRITE_ERRORS_ALERT</td>
<td>Excessive write errors reported for an HDD.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td></td>
<td>This alert is initiated by the HDD_EXCESSIVE_WRITE_ERRORS event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDD_EXTRA_ALERT</td>
<td>The polling found an additional HDD that does not match what is expected according</td>
<td>WARNING</td>
<td>24-hour poll</td>
</tr>
<tr>
<td></td>
<td>to the manifest.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDD_INVALID_ALERT</td>
<td>The polling detected a type of HDD that does not match what is expected according</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td></td>
<td>to the manifest.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDD_TEMPERATURE ABOVE_THRESHOLD_ALERT</td>
<td>HDD temperature has reached its maximum safe operating temperature.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td></td>
<td>This alert is initiated by the HDD_TEMPERATURE ABOVE_THRESHOLD event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDD_UNDETECTTED_ALERT</td>
<td>The polling did not detect an HDD that matches what is expected according to the</td>
<td>ERROR</td>
<td>24-hour poll</td>
</tr>
<tr>
<td></td>
<td>manifest.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDD_WEAROUT ABOVE_THRESHOLD_ALERT</td>
<td>Wear-out state of an HDD is above its defined threshold.</td>
<td>WARNING</td>
<td>Event</td>
</tr>
<tr>
<td></td>
<td>This alert is initiated by the HDD_WEAROUT ABOVE_THRESHOLD event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HMS_AGENT_DOWN_ALERT</td>
<td>The Hardware Management Services (HMS) aggregator cannot communicate with the HMS</td>
<td>CRITICAL</td>
<td>30-minute poll</td>
</tr>
<tr>
<td></td>
<td>agent on the rack's management switch through the private management network,</td>
<td></td>
<td>24-hour poll</td>
</tr>
<tr>
<td></td>
<td>either because the agent is down or the network is not available. This alert is</td>
<td></td>
<td>Event</td>
</tr>
<tr>
<td></td>
<td>initiated by the HMS_AGENT_DOWN event or by polling.</td>
<td></td>
<td></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 EVO 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>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>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>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>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>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_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, 24-hour 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, 30-minute poll, 24-hour poll</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>
<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>
</tbody>
</table>
Using the vRealize Log Insight Capabilities in Your System

By default, vRealize Log Insight is installed and integrated in your deployed EVO SDDC system. 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 in the system.

vRealize Log Insight is a log aggregator that provides simplified log viewing and analysis. Events and log content for the system’s physical resources and the virtual infrastructure are collected by the integrated vRealize Log Insight, 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 integrated 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 the EVO SDDC system is also sent to vRealize Log Insight, 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 integrated vRealize Log Insight for remote syslog forwarding to an instance of vRealize Log Insight that is external to the EVO SDDC system or to another syslog server. You configure vRealize Log Insight to forward incoming events to a syslog target in 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 the topic in the vRealize Log Insight 3.3 documentation center at http://pubs.vmware.com/log-insight-33/topic/com.vmware.log-insight.administration.doc/GUID-956EC67B-44B4-44BB-AF24-0DE4377F725C.html.

For the steps to log in to the vRealize Log Insight Web interface from the EVO SDDC Manager Web interface, see “Get Started Using the Integrated vRealize Log Insight,” on page 91.

**Note** In this release, the integrated vRealize Log Insight software is configured for monitoring of the EVO SDDC system only. Configuring the integrated vRealize Log Insight to monitor additional applications or VMs is not supported in this release.

Automatically Installed Content Packs

The integrated vRealize Log Insight 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
By default, your EVO SDDC system’s vRealize Log Insight instance includes a number of VMware content packs, including an EVO SDDC content pack. For a detailed description of the EVO SDDC content pack, see “EVO SDDC Content Pack,” on page 90. 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>EVO SDDC</td>
<td>This content pack includes an overview dashboard that gives overall summary views of the data sent by the EVO SDDC Manager, 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 Horizon View servers is collected and consolidated.</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.

**Note** Using the vRealize Log Insight Web interface to update the automatically installed content packs or to install additional content packs is not supported in this release.

### EVO SDDC Content Pack

The EVO SDDC content pack provides graphical summary views for various EVO SDDC Manager events that are sent to vRealize Log Insight. The content pack organizes the views into multiple tabs that display collected information about various aspects of the system. The top **Overview** tab includes high-level overview of all system 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 EVO SDDC system, such as the rack-level, server-level, switch-level, component-level, and so on. As a result, this set of tabs gives you the ability to get an overall cross-system view using the **Overview** tab, and then drill-down into the hardware level you are interested in by using the other tabs.

The **Audits - Summary** tab provides views of the collected audit event data by severity, by system audit event and user audit event, and a timeline view of audit events.
Get Started Using the Integrated vRealize Log Insight

By default, vRealize Log Insight is integrated in your EVO SDDC system. vRealize Log Insight delivers real-time log management for VMware environments, providing system-wide visibility of logs and easier troubleshooting across the physical and virtual infrastructure in your EVO SDDC system.

During the setup and configuration process of your EVO SDDC system, the vRealize Log Insight virtual appliance is deployed and configured as an integrated part of the VMware SDDC software stack in your system. 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** In this release, the integrated vRealize Log Insight software is configured for monitoring of the EVO SDDC system only. Configuring the integrated vRealize Log Insight to monitor additional applications or VMs is not supported in this release.

As part of the EVO SDDC system deployment and configuration process, content packs are automatically installed and configured in vRealize Log Insight. 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 available and ready for you to use. For an overview of these content packs that are installed by default, see “Using the vRealize Log Insight Capabilities in Your System,” on page 89. 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.

In the EVO SDDC Manager Web interface, you can open the vRealize Log Insight Web interface using the following methods. During an EVO SDDC Manager logged-in session, 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 system.

If this is the first time after your system was deployed 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 EVO 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 EVO SDDC Manager (vrm) Virtual Machine,” on page 20 and “Look Up Account Credentials Using the Lookup-Password Command,” on page 20.

**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 EVO 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 deployment of your EVO SDDC system, 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 EVO SDDC System,” on page 19.

The vRealize Log Insight Web interface appears with the display filtered to show the events that meet the criteria for the launch context from EVO SDDC Manager.

What to do next

Examine the descriptions of the content packs that are available by default by selecting **Content Packs** in the upper right corner menu.

Examine the data available in the content packs. To display the dashboards from the installed content packs, click **Dashboards** and use the drop-down menu at the upper left to select the content pack.

Enable login accounts for additional users. See the Managing User Accounts in vRealize Log Insight topic and its subtopics in the vRealize Log Insight product documentation available at the following locations:

   - From the **Help** menu choice in the vRealize Log Insight Web interface.
   
   - In the vRealize Log Insight product documentation online at http://pubs.vmware.com/log-insight-33/index.jsp.

For detailed information about how to use the content packs and other capabilities of the vRealize Log Insight Web interface, see the vRealize Log Insight product documentation available at those two locations also.

Configure Syslog from the Switches to vRealize Log Insight

Your system’s integrated vRealize Log Insight instance is a syslog collector. In this release, you manually configure the switches to export their log files to the integrated vRealize Log Insight instance.

Prerequisites

Verify that you have the root account credentials to log in remotely to the EVO SDDC Manager virtual machines on each rack. The root account credentials are managed by your organization. See “Credentials for Logging In To the EVO SDDC Manager (vrn) Virtual Machine,” on page 20.
Procedure

1. On the first rack, using the root account, connect and log in, for example by SSH, to the EVO SDDC Manager VM.

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

3. Configure ability to export the switches’ log files to the system’s integrated 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 system.
- 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 Integrated vRealize Log Insight,” on page 91.

Using the vRealize Operations Manager Capabilities of Your System

By default, vRealize Operations Manager is installed and integrated in your deployed EVO SDDC system. You can use the capabilities of vRealize Operations Manager to work with the 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. In your EVO SDDC system, data from the management and workload domains’ propagates to vRealize Operations Manager and you get a unified view of the event data and metrics for the virtual infrastructure. As part of the EVO SDDC system deployment and configuration process, the vCenter Adapter for vRealize Operations Manager is automatically installed and configured in vRealize Operations Manager. Additionally, when you create a VDI workload domain, the Horizon View Adapter for vRealize Operations Manager is automatically 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** In this release, the integrated vRealize Operations Manager software is configured for monitoring of the EVO SDDC system only. Configuring the integrated vRealize Operations Manager to monitor additional applications or VMs is not supported in this release.

vRealize Operations Manager Multiple-Node Cluster

In a single-rack EVO SDDC system, 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 system, 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

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 EVO SDDC Manager Web interface, you can launch the Web interface using the following methods. During an EVO SDDC Manager logged-in session, 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 Log Insight Web interface.

Procedure

1. Open the vRealize Operations Manager Web interface by clicking the vROPS launch link located on the Management Info area of the domain details for the management and workload domains.

   The vRealize Operations Manager login screen appears.

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

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

   Those account credentials are 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 system’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 EVO SDDC Manager Web interface to review and configure settings for parameters that are used in various system features.

This chapter includes the following topics:

- “Customize Default Values Used When Creating VDI Workload Domains,” on page 95
- “Additional Rack Settings Screen,” on page 98
- “Managing Network Settings,” on page 98

**Customize Default Values Used When Creating VDI Workload Domains**

You can set default values for some of the parameters the system 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 EVO SDDC system creates those VDI-specific resources for a View infrastructure that are appropriate for the selections you make in the Configure VDI wizard. The system uses default values for the View infrastructure’s required parameters. You can customize those default values using the VDI Settings page.

**Procedure**

1. In the EVO SDDC Manager Web interface, 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 96.
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 the system uses when creating VDI workload domains.

VDI Parameters

If you do not customize these values for your system, when you configure a new VDI workload domain, the system default values are used for the VDI parameters. To see the steps for customizing these system default values, see “Customize Default Values Used When Creating VDI Workload Domains,” on page 95.

<table>
<thead>
<tr>
<th>Type</th>
<th>System 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>DCI</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>System 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, the system deploys a Replica Connection server 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, the system deploys a Replica Security server in the VDI environment.</td>
</tr>
<tr>
<td>Type</td>
<td>System Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Max Desktops per vCenter Server</td>
<td>1200</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. If the total number of virtual desktops exceeds this number, a new VDI workload domain is deployed, including the vCenter server that manages that workload domain.</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>Shared Memory [%]</td>
<td>20</td>
<td>Specifies the percentage of the transparent pages value that is set in the VDI workload domain’s vCenter servers.</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 EVO SDDC system.

As described in the *EVO SDDC Overview and Bring-Up Guide*, when you follow the steps in the Bringing-Up on Additional Racks procedure to power on a new rack and use the spine switches to connect it to the system’s existing racks, the thumbprint of the added rack is displayed in this screen. Then you start the Add Rack wizard to verify the identity of the new rack using its thumbprint and bootstrap password.

See the Bringing-Up on Additional Racks procedure in the *EVO SDDC Overview and Bring-Up Guide* for the detailed steps for adding a new rack to your system.

**Managing Network Settings**

Use the Network Settings screen to examine and make changes to network-related settings in your EVO SDDC system.
Manage Uplink Connectivity Settings Using the EVO SDDC Manager Web Interface

After system deployment, you can use the Uplink screen in the EVO SDDC Manager Web interface 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 EVO 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 Virtual Router Redundancy Protocol (VRRP) or Hot Standby Router Protocol (HSRP), and so on.

The ToR uplink settings are entered during the system bringup process. The ToR uplink connectivity can be either L2 or L3 to the upstream network. After the system bringup process, you use this screen to change the settings that were entered during bringup.

**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 EVO SDDC Manager Web interface 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 EVO 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 EVO SDDC Manager Web interface, 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 uplinks 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. |
Option | Description
--- | ---
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 System Use

You can exclude IP addresses in the subnets used in the system to prevent the system from assigning those addresses to system resources.

The system allocates IP addresses to its internal resources from the subnets you enter during the system bring-up process or 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.

The system 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 100.

- **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 system’s bring-up process and the VI workload domain creation workflow.

  For example, during the system bring-up process on the first rack, specifying excluded IP addresses in the management subnet screen of the bring-up wizard prevents the system 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 to the system.

  Then, during creation of a VI workload domain, the system uses the same management network subnet that was used during system bring-up. 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 system’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 system as excluded addresses. The system is prevented from assigning the IP addresses in this set to system 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.
The system allocates IP addresses to its internal resources from the subnets you enter during the system bringup process or the Virtual Infrastructure workload domain creation process. When those subnets include IP address that are already used in your corporate network for other purposes, or which you want to reserve for another use, you exclude those IP addresses to prevent IP conflicts. Using this screen, you can add those IP addresses or ranges of addresses that you want to prevent the system from automatically assigning to resources in the system. Excluding such IP addresses helps to prevent IP conflicts.

When you make a change in this screen, you must use the Update button to confirm the change in the system.

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 in the system, such as:

- Information about each subnet in the system, such as the subnet address, broadcast address, and so on
- Number of IPs currently available in each subnet
- The distributed port group associated with each subnet

### Data Center Screen

You use the Data Center screen to manage the relationships between workload domains and the data center network connections that are defined in your EVO SDDC system. You can review the information for the existing connections, add new data center connections, associate and disassociate data center connections with workload domains, and remove data center connections that are no longer associated with a workload domain.

### 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 defined in the system. In your EVO SDDC system, a data center connection specifies the network that carries traffic between the system and the networking environment external to the system, such as your corporate network. During the system’s bringup 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.
Adding or Replacing a Server

You can add capacity to your EVO SDDC system by adding one or more servers to a rack or replace a faulty server in a rack with a new server. The inserted server behaves just as the existing servers in the rack.

This chapter includes the following topics:

- “Add a Server,” on page 103
- “Replace a Faulty Server, CPU, Memory, SAS, BMC, or NIC,” on page 105
- “Replace SSD or HDD on a Server,” on page 108

Add a Server

You can increase the capacity of your EVO SDDC system by adding a new server.

Prerequisites

The new server should be from the same vendor and of the same model number as the other servers in the rack. It should be physically at your site before you begin this procedure.

Procedure

1. Print your BoM.
2. Identify the firmware versions on the new server.
   For information on how to identify the version, refer to the documentation from your vendor.
3. Compare the firmware versions on the new server to your BoM. If there is a delta, the firmware on the replacement server needs to be updated to match the BoM. This process of upgrading the firmware on a server is referred to as true-up.
   To true-up of the new server, refer to the documentation from your vendor.
4. Install ESXi on the new server. For information on the ESXi version that works with EVO SDDC, refer to the Release Notes. For more information, see VMware vSphere Documentation.
5. Set the password on the server to EvoSddc!2016.
6. 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.
   See VMware vSphere 6.0 Documentation.
Enable the Secure Shell (SSH) for the ESXi host:

- Open the vSphere Web Client.
- Right-click **Host** in the VMware Host Client.
- Click **SSH Enable**.

Mount the new server in an empty slot on the rack and connect it to the management and ToR switches according to the wiremap. See Chapter 13, “Rack Wiring,” on page 129.

Power on the new server.

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

In a command line window, SSH to the EVO SDDC Manager on the rack where you are adding the server.

Open the \(/home/vrack/VMware/vRack/server-commission.properties\) file and specify values for `hms.host.bmc.username` and `hms.host.bmc.password`.

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

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

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

You need administrator credentials to run this command. The command window displays the task progress.

During server commissioning, the system does the following:

- HMS recognizes the new server.
- Adds the new server to PRM inventory.
- EVO SDDC Manager adds the new server to the capacity pool.

Note the hostId displayed in the output.

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

```
Server Commissioning SUCCEEDED
```

Retrieve the IP address of the commissioned server.

- On the EVO SDDC Manager Dashboard, click **Physical Resources**.
- Click the rack on which the server was commissioned.
- Click the host corresponding to the hostId you noted down in step 13.
- Note down the inband IP address.

Change the password on the new server to the common password for ESXi servers.

- Log in to the EVO SDDC Manager VM on the rack on which you added the new server.
- Navigate to the \(/home/vrack/bin\) directory.
- Type the following command:

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

where `hostIPAddress` is the IP address you noted down in step 13d.

The IP address of the new server is 192.168.100.xxx, which is not in range you assigned to it in step 6. The new server is now available for addition to workload domains.
Replace a Faulty Server, CPU, Memory, SAS, BMC, or NIC

If a server in your EVO SDDC system goes bad, you can replace it with a new server. Use this procedure to replace any of the following in a physical rack:

- CPU
- iDRAC or BMC
- memory
- motherboard or server
- NIC card
- SAS controller
- SAS expander

Prerequisites

- Ensure that the new server should be from the same vendor and of the same model number as the server it is replacing. It should be at your site before you begin this procedure. This applies to other components as well.
- Expand the cluster to which the faulty part belongs by adding a server from the capacity pool. When the replacement server is added to the EVO SDDC rack, the newly added server is added to the capacity pool and is available for workload domain creation and workload expansion.

Procedure

1. If the host does not belong to a workload domain, retrieve the password of the host.
   a. In a command line window, SSH to the EVO SDDC Manager on the rack.
   b. Navigate to /home/vrack/bin.
   c. Type the following command:
      ```
      ./vrm-cli.sh lookup-password
      ```
   d. Note the ESXi and IPMI passwords of the host that is to be decommissioned.
2. From the Dashboard page, navigate to Physical Resources > Rack Details.
3. 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.
4. Click Decommission.

   The sever decommission task is scheduled. During this task, the faulty server is removed from all workload domains to which it was allocated and the system’s available capacity is updated to reflect the reduced capacity.

   **Note** If this host belongs to a workload, there must be more than 3 hosts in that workload domain. If there are only 3 hosts in that workload domain, you will not be able to decommission this host. If one of the 3 hosts is dead, click Force Decommission to decommission the host.

5. To watch the progress of the decommission task, click STATUS in the left navigation pane. Data on the host is transferred according to the following rules.
   - Decommissioning a healthy host (which is up and running in vSphere) in a workload
The host is put in maintenance mode. Data from the host is transferred to the other hosts in the workload domain. The host is cleaned up and is put in the state that it was after imaging - it only has the vswitch0 with a non-routable IP address, disks that were used for Virtual SAN are cleaned up, and there is no vDS.

- Decommissioning a dead host (which is powered off in vSphere) in a workload
  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.

- Decommissioning a host that does not belong to a workload
  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.

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

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

Table: ESXi Credentials

<table>
<thead>
<tr>
<th>IPMI/BMC Credentials</th>
<th>User name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Depends on server type and vendor</td>
<td>D3c0mm1ss10n3d!</td>
</tr>
</tbody>
</table>

When the server is decommissioned, the chassis-identification LED on the host starts to beacon (flashing on and off). This helps you identify the server that has been decommissioned.

7 Power off the decommissioned server and remove it from the physical rack.

8 Follow the appropriate step depending on the component that needs to be upgraded or replaced.

- If you are replacing a faulty server or motherboard, follow these steps.
  a Print your BoM.
  b Identify the firmware versions on the replacement server.
     For information on how to identify the version, refer to the documentation from your vendor.
  c Compare the firmware versions on the replacement server to your BoM. If there is a delta, the firmware on the replacement server needs to be updated to match the BoM. This process of upgrading the firmware on a server is referred to as true-up.
     To true-up of the replacement server, refer to the documentation from your vendor.
  d Install ESXi on the replacement server. For information on the ESXi version that works with EVO SDDC Manager, refer to the Release Notes. For more information, see VMware vSphere Documentation.
  e Set the password on the server to EvoSddc!2016.
  f Enable Secure Shell (SSH) for the ESXi host using vSphere Web Client or the host client. The steps below apply if you are using the vSphere Web Client.
     1 Open the vSphere Web Client.
     2 Right-click Host in the VMware Host Client.
3 Click SSH **Enable**.

Ensure that the host’s IP address is from the following range:

192.168.100.50 - 192.168.100.73

If the IP address is outside this range, assign a new IP address to the host from this range. The subnet is 255.255.252.0 and gateway is 192.168.100.1.

- If you are upgrading or replacing a FRU, follow the documentation from your vendor to complete this task.
- If you are upgrading the BIOS or BMC, follow the documentation from your vendor to complete this task.

9 Mount the replacement server or server with the upgraded FRU or BIOS on the rack and connect it to the same ports of the management and ToR switches as the old server.

10 Power on the server.

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

11 In a command line window, SSH to the EVO SDDC Manager on the rack where you are adding the server.

12 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. The command window displays the task progress.

During server commissioning, the system does the following:

- HMS recognizes the new server.
- Adds the new server to PRM inventory.
- EVO SDDC Manager adds the new server to the capacity pool.

13 Note the hostId displayed in the output.

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

**Server Commissioning SUCCEEDED**

14 Retrieve the IP address of the replacement server.

- On the EVO SDDC Manager Dashboard, click **Physical Resources**.
- Click the rack on which the server was commissioned.
- Click the host corresponding to the hostId you noted down in step 13.
- Note down the inband IP address.

15 Rotate the password on the replacement server.

- Log in to the EVO SDDC Manager VM on the rack on which you added the new server.
- Navigate to the `/home/vrack/bin` directory.
- Type the following command:

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

where `hostIPAddress` is the IP address you noted down in step 13d.
Replace SSD or HDD on a Server

You can replace the SSD or HDD on a host by placing the host in maintenance mode.

Virtual machines that are running on a host entering maintenance mode need to be migrated to another host (either manually or automatically by DRS) or shut down. The host is in a state of **Entering Maintenance Mode** until all running virtual machines are powered down or migrated to different hosts. You cannot power on virtual machines or migrate virtual machines to a host entering maintenance mode.

When no more running virtual machines are on the host, the host’s icon changes to **under maintenance** and the host’s Summary panel indicates the new state. While in maintenance mode, the host does not allow you to deploy or power on a virtual machine.

**NOTE** DRS does not recommend (or perform, in fully automated mode) any virtual machine migrations off of a host entering maintenance or standby mode if the vSphere HA failover level would be violated after the host enters the requested mode.

**Procedure**

1. In the vSphere Client inventory, right-click a host and select **Enter Maintenance Mode**.
   - If the host is part of a partially automated or manual DRS cluster, a list of migration recommendations for virtual machines running on the host appears.
   - If the host is part of an automated DRS cluster, virtual machines are migrated to different hosts when the host enters maintenance mode.

   **NOTE** While the host is in maintenance mode, do not delete the management domain that the host belongs to.

2. If applicable, click **Apply Recommendations**.

3. Replace the SSD or HDD.

4. Right-click the host and select **Exit Maintenance Mode**.
Lifecycle Management (LCM) enables you to perform automated updates on EVO SDDC components (EVO SDDC Manager, HMS, and LCM) as well as VMware components (vCenter Server, ESXi, and NSX). EVO SDDC Manager is pre-configured to communicate with the VMware software repository. The high level update workflow is described below.

1. Notification of update availability.
2. Download update bundle.
3. Select update targets and schedule update.
4. Update is applied to the selected targets at the scheduled time.

**Note** VMware recommends that you do not create, modify, or delete a workload domain during an update.

Even though EVO 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 chapter includes the following topics:

- “Set VMware Depot User,” on page 110
- “Download Update Bundle,” on page 111
- “Select Targets and Schedule Update,” on page 114
- “View Inventory Component Versions,” on page 121
- “Display Backup Locations,” on page 121
Set VMware Depot User

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

Procedure

1. In the EVO 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.

Download Update Bundle

When an update bundle is available, a notification is displayed on the EVO 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 EVO SDDC with the EVO SDDC Manager NTP server.

Procedure

1 Do one of the following:

- Click the bundle notification on the EVO SDDC Manager dashboard.
- In the EVO 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 EVO SDDC drop-down to see the available updates for EVO SDDC components and the VMware Software Update drop-down to see vCenter Server and ESXi updates.

3 Do one of the following:
   - Click **DOWNLOAD** to download the bundle right away.
   - Click ** schedule to schedule the download. Select the date and time and then click **SCHEDULE**.
4 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.

<table>
<thead>
<tr>
<th>BUNDLE TYPE</th>
<th>BUNDLE VERSION</th>
<th>RELEASE DATE</th>
<th>BUNDLE SIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVORACK</td>
<td>11.5.2751336</td>
<td>Apr 14, 2016</td>
<td>123 MB</td>
</tr>
</tbody>
</table>

**Dependency Bundle**: The selected bundle is dependent on the following bundles and they will also be downloaded.

<table>
<thead>
<tr>
<th>BUNDLE TYPE</th>
<th>BUNDLE VERSION</th>
<th>RELEASE DATE</th>
<th>BUNDLE SIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMWARE_SOFTWARE</td>
<td>11-A-568943-VMWARE</td>
<td>Apr 14, 2016</td>
<td>365 MB</td>
</tr>
</tbody>
</table>

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).
5 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 EVO 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**. Contact VMware support for such errors.

### 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 EVO SDDC Manager may be available while the update is applied, it is recommended that you schedule the update at a time when EVO SDDC Manager is not being heavily used.

**Note**  Do not create, modify, or delete a workload domain while an update is being installed.

### Prerequisites

1. You must have downloaded the appropriate bundle so that it is available in the local repository.

2. Ensure that the EVO SDDC Manager and HMS are at the same version. In a dual rack scenario, the EVO 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 EVO SDDC update.

3 Click **UPDATE**.

The **UPDATE** button is enabled only for one update at a time. Once you schedule a EVO SDDC update, the UI allows you to schedule a VMware software update. However, VMware recommends that you schedule only one update at a time. Wait for the scheduled update to be installed successfully before scheduling another update.

The system validates that update pre-requisites are met before displaying the target selection.

4 On the TARGET page, select the domains where the update is to be applied.

When a new version of the software is available, it must be installed on the management domain. So the management domain is automatically selected for update and the checkbox next to it grayed out.
Click **EXPAND** next to the domain to see the areas of your datacenter that will be updated.

The targets on the primary rack (the rack that contains the PSCs) are updated before the targets on additional racks.

**NOTE** If you select only a subset of the domains in your datacenter to be updated, the update will be displayed in both the Available Updates section (since some domains are yet to be updated) as well the Scheduled Updates section. You cannot schedule an update on a failed domain. If the system does not let you select a domain, click the **INVENTORY** tab to check the status of the domain. Resolve the issue and then re-schedule the update.

5. Click **NEXT**.
6 On the SCHEDULE page, select the date and time for the update to be applied to the target domains and click NEXT. You can select a date within a year from the present date.

![EVO SDDC Update]

Select Update Schedule

- April 2016

SUN MON TUE WED THU FRI SAT
27 28 29 30 31 01 02
02 03 04 05 06 07 08 09
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
01 02 03 04 05 06 07

DATE: 2018-04-14
TIME: 03:15 PM

Note Do not reboot the physical racks, any devices on the rack, or the EVO 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.
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 EXPAND 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.

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 ![undo](image) to the right of the component name and then click **GET BACKUP LOCATION**.

   The backup file name and location is displayed.
Managing Licenses Used in Your System

You manage the required licenses using the Licensing screen available from the Settings page in the EVO SDDC Manager client.

This chapter includes the following topics:

- “EVO SDDC Licensing Model,” on page 123
- “Manage License Keys for the Software in Your EVO SDDC System,” on page 124

EVO SDDC Licensing Model

The EVO SDDC Manager software is licensed under the EVO SDDC license. As part of the EVO SDDC product, EVO SDDC Manager deploys specific VMware software products, some of which are licensed under the EVO SDDC license and some are licensed separately.

The following VMware software deployed by EVO SDDC Manager is licensed under the EVO SDDC license:

- VMware vSphere
- VMware Virtual SAN
- VMware NSX for vSphere

The following VMware software deployed by EVO 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 EVO SDDC license, use the information resources at the EVO SDDC product information page at http://www.vmware.com/products/cloud-foundation.html.

All physical processors in the EVO SDDC system are licensed using the base EVO SDDC license.
Manage License Keys for the Software in Your EVO SDDC System

Use the Licensing screen of the EVO SDDC Manager Web interface to work with the license keys for the system’s software.

In the Licensing screen, you can:

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

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 the system 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 system.</td>
</tr>
</tbody>
</table>
Troubleshooting EVO SDDC Systems for Data Center System Administrators

You can troubleshoot issues that you might experience after you install and deploy your EVO SDDC system. This chapter includes the following topics:

- “Unable to Browse to the VMware SDDC Software Components' Web Interfaces Using their Fully Qualified Domain Names,” on page 125
- “Decommission Workflow Stops Responding at Task Named Enter Hosts Maintenance Mode,” on page 126
- “VDI Workload Creation Fails at the Import DHCP Relay Agents Task,” on page 127

Unable to Browse to the VMware SDDC Software Components' 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 your EVO SDDC system, but the login screen for that product does not appear in the browser.

Problem

In the EVO SDDC Manager Web interface, 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 into the system configuration wizard for the EVO SDDC Subdomain field. 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 EVO SDDC Subdomain field in the system's bring-up wizard.

The EVO SDDC Manager runs an internal DNS server so that it can guarantee that FQDN resolution works within the system. If a delegation record was not configured in the specified root domain to point to the EVO SDDC Manager DNS server for the specified EVO SDDC 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 during configuration of your EVO SDDC system, 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.

VMware, Inc.
### 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 type the subdomain portion for your EVO SDDC system 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 EVO SDDC Manager virtual machine.
   
   The New Name Server Record window appears.

6. Type the EVO 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 EVO 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 system 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 system 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 EVO 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 EVO 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 the EVO SDDC system’s management network and the data center network specified in the VDI workload domain creation wizard, the creation workflow fails at the Import DHCP Relay Agents task.

**Problem**

In the Workflows screen, you see that the creation workflow for your VDI workload domain environment has failed in the task Import DHCP Relay Agents.

**Cause**

When the system’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, the system 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 EVO 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 system’s 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 EVO SDDC Manager VM can communicate with the data center network.
  
  One way to verify is to remotely log in to the EVO 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.
Connect cables according to the wiremaps.
Rack 1

Figure 13-1. Wiremap for rack 1 with Dell Components

- Jump VM
- Private Managed Switch
- 16 switch serial console switch. For Connections, see port connectivity table
- Spine 2 on Rack 2
- Spine 1 on Rack 2
- ToR 2
- ToR 1
- Management switch
- Management port
- Node 1
- Node 13
- Node 1
- Node 13
- public network
- Management port
- Management port
- Management port
- Management port
- Management port
Figure 13-2. Wiremap for rack 2 with Dell Components

Jump VM

Private Managed Switch

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

Spine 2

Spine 1

ToR 2

ToR 1

Management switch

Node 1

Node 12

Node 24

Node 2

Node 13

Node 2

Node 12

Node 24

Node 1

Node 13

Node 1

Node 13

Management port

Management port

Management port

Management port

Management port

Management port

public network

public network
Figure 13-3. Wiremap for rack 1 with Quanta Components

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

Refer to the tables below for port connectivity information.

**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>
<tr>
<td>4</td>
<td>Spine 1 console port</td>
</tr>
</tbody>
</table>
### Port Number

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Connects To</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Spine 2 console port</td>
</tr>
<tr>
<td>6</td>
<td>PDU 1</td>
</tr>
<tr>
<td>7</td>
<td>PDU 2</td>
</tr>
<tr>
<td>8</td>
<td>PDU 3</td>
</tr>
<tr>
<td>9</td>
<td>PDU 4</td>
</tr>
<tr>
<td>10 - 16</td>
<td>Not connected</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>
<tr>
<td>Port Number</td>
<td>Speed</td>
<td>Connects To</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>11</td>
<td>40 Gbps</td>
<td>Rack 6 ToR 1 port 49</td>
</tr>
<tr>
<td>12</td>
<td>40 Gbps</td>
<td>Rack 6 ToR 1 port 49</td>
</tr>
<tr>
<td>13</td>
<td>40 Gbps</td>
<td>Rack 7 ToR 1 port 49</td>
</tr>
<tr>
<td>14</td>
<td>40 Gbps</td>
<td>Rack 7 ToR 1 port 49</td>
</tr>
<tr>
<td>15</td>
<td>40 Gbps</td>
<td>Rack 8 ToR 1 port 49</td>
</tr>
<tr>
<td>16</td>
<td>40 Gbps</td>
<td>Rack 8 ToR 1 port 49</td>
</tr>
</tbody>
</table>

**ToR 2**

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Speed</th>
<th>Connects To</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 24</td>
<td>10 Gbps</td>
<td>node 1 - node 24 where port 1 connects to node 1, port 2 connects to node 2, and so on</td>
</tr>
<tr>
<td>25-38</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>43-46</td>
<td>10 Gbps</td>
<td>Public network</td>
</tr>
<tr>
<td>47</td>
<td>NA</td>
<td>Not connected</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>Not connected</td>
</tr>
<tr>
<td>Management</td>
<td>1 Gbps</td>
<td>Management switch port 42</td>
</tr>
</tbody>
</table>

**ToR 1**

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Speed</th>
<th>Connects To</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 24</td>
<td>10 Gbps</td>
<td>Node 1 - node 24 where port 1 connects to node 1, port 2 connects to node 2, and so on</td>
</tr>
<tr>
<td>25-38</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>43-46</td>
<td>10 Gbps</td>
<td>Public network</td>
</tr>
<tr>
<td>47</td>
<td>NA</td>
<td>Not connected</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>Not connected</td>
</tr>
<tr>
<td>Management</td>
<td>1 Gbps</td>
<td>Management switch port 41</td>
</tr>
</tbody>
</table>
## Management Switch

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Speed</th>
<th>Connects To</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 24</td>
<td>1 Gbps</td>
<td>Node 1 - Node 24 where port 1 connects to node 1, port 2 connects to node 2, and so on</td>
</tr>
<tr>
<td>25 - 40</td>
<td>NA</td>
<td>Not connected</td>
</tr>
<tr>
<td>41</td>
<td>1Gbps</td>
<td>ToR 1 management port</td>
</tr>
<tr>
<td>42</td>
<td>1Gbps</td>
<td>ToR 2 management port</td>
</tr>
<tr>
<td>43</td>
<td>1Gbps</td>
<td>Spine 1 management port</td>
</tr>
<tr>
<td>44</td>
<td>1Gbps</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>1Gbps</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>
</tbody>
</table>

Management port Private managed switch

**Note**: PDU ports are not reflected in the table above.
Index

A
about this information 5
Active Directory
and your system 29
when creating a VDI workload domain 59
Active Directory users and groups, granting
vSphere Web Client access 32
add server 103
adding physical racks to the system 98
Alert Catalog 84
alert definitions 84
alerts, system-defined list 84
alerts based on system-detected problems 74
B
browser support for the EVO SDDC Manager
interface 11
C
client interfaces 9
clients, administrative web interfaces 9
compression 68
configuring settings 95
Connection Server administrator account 69
corporate network, connections to 101
creating a VDI workload domain,
troubleshooting 127
creating VDI workload domains 50
D
Dashboard page 12
data center connections, working with 101
decommissioning hosts, troubleshooting 126
deduplication 68
deleting workload domains 67
desktop OVA requirements 54
domains, management and workload 41
E
Event Catalog 78
event-driven problem detection 74
EVO SDDC, VMware software components 8
EVO SDDC Manager Web interface
logging in 11
logging out 17
tour of 12
excluding IP addresses, about 100
expand, management domain 65
expand a management domain 65
expanding management and workload
domains 65
expanding workload domain 66
external networks, networking to 101
G
glossary 5
groups
adding locally 33
assigning permissions for operations 35
I
identity sources, verifying 30
intended audience 5
interfaces, administrative Web clients 9
introduction to administering EVO SDDC
systems 7
IP addresses, excluding 100
IP addresses exclusions 100
IP Distribution screen 100
J
joining an Active Directory domain 30
L
license keys, entering in the system 124
licenses, managing 123
licensing model 123
lifecycle management
backup location 121
download update 111
inventory version 121
schedule update 114
Lifecycle Management page 12
list view of resources 39
log in to the EVO SDDC Manager Web
interface 11
log out of the EVO SDDC Manager Web
interface 17
look up built-in account credentials 20
management domain, about 41
management switch, syslog 92
managing users and groups 29
map view of resources 39
monitoring your system 71

names, VI workload domains 44
network settings, managing 98
networking
to external networks 101
to your corporate network 101

operations, assigning permissions to perform 35

password policy 37
passwords, rotating 19
permissions, assigning to users and groups 35
physical resources, views of 39
physical rack, port connectivity 133
physical resources, managing 39
problem detection 74
RAID 5 erasure coding 68
RAID 6 erasure coding 68
RBAC 36
replace
BMC 105
CPU 105
memory 105
NIC 105
SAS 105
server 105
rights in the system 36
role-based access control (RBAC) 36
roles, about 36
root account credentials for the VRM virtual machine 20
rotating passwords 19
rotating all passwords 21

security, password rotation 19
server
add 103
replace 105
setting default values, for VDI workload domains 95
setting up environment, rack wiring 129
settings, uplink connectivity 99

settings configuration 95
Settings page 12
software components 8
Support Resources page 12
switches, syslog 92
syslog, switches 92
system health, examining 94
system status, workflows and tasks 73
system administrator account 35
System Status page 12

tasks, working with troubleshooting
logging in to Web interfaces 125
VDI workload domains 127

update
download 111
inventory versions 121
schedule 114
uplink connectivity settings, configuring 99
User Management page 12
user interface, EVO SDDC Manager 11
users
adding locally 33
assigning permissions for operations 35
using vRealize Log Insight 91

vCenter Server Single Sign-On, Active Directory 29
VDI offering 42
VDI infrastructure settings 96
VDI workload domains
creating 50
creation wizard 57
desktop OVA requirements 54
post-deployment tasks 64
setting default values 95
VDI workload domain creation Active Directory 59
General Topology step 58
networking information 61
parent desktop template 62
Review step 63
Virtual Desktops step 60
Windows Server ISO 62

VI offering 42
VI workload domain
accessing the infrastructure using the vSphere Web Client 49
naming 44
network configurations 46
selecting performance and availability settings 45
start creation wizard 44
start deployment 49
VI workload domains, about creating 43
views of physical resources 39
Virtual SAN features in all-flash storage systems 68
Virtual Desktops step, VDI workload domain creation 60
vRealize Log Insight 89
vRealize Operations Manager, examining system health with 94
vrm-cli utility 23

W
Web interface, EVO SDDC Manager 11
workflows, working with 73
workload domains
about 41
deleting 67
expanding 65, 66
VDI 50
Virtual Infrastructure 43