Cisco UCS Director VMware vSphere Management Guide, Release 6.6

First Published: 2018-04-27

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

This preface contains the following sections:

Audience

This guide is intended primarily for data center administrators who use Cisco UCS Director and who have responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security
- Virtualization and virtual machines

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.

Text Type	Indication
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

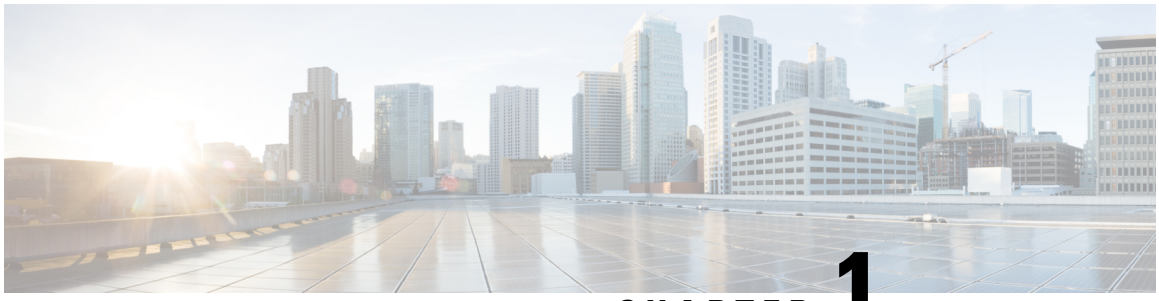
Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-director-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation.

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

New and Changed Information for this Release

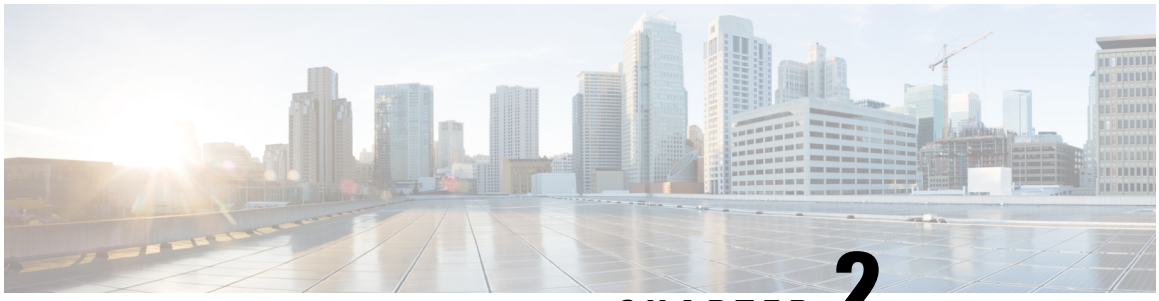
New and Changed Information for This Release

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

Table 1: New Features and Changed Behavior in Cisco UCS Director, Release 6.6.

Feature	Description	Where Documented
VMware content library support	Support for VSAN cluster configuration through Cisco UCS Central. You can create VSAN clusters from a baremetal using Cisco UCS Central.	Creating Virtual SAN Clusters Using Cisco UCS Bare Metal Servers Creating Virtual SAN Clusters

New and Changed Information for This Release



CHAPTER 2

Overview

This chapter contains the following sections:

About Cisco UCS Director for VMware vSphere

Cisco UCS Director supports the VMware vSphere product family and enables access to advanced features such as vMotion, Dynamic Resource Scheduling, and Site Recovery Manager.

Cisco UCS Director integrates with VMware vCenter server to provide automation and life cycle management of virtual infrastructure. Beginning with the physical infrastructure, Cisco UCS Director provides automated deployment of ESXi hypervisor onto compute infrastructures such as UCS, and then presents the hypervisor hosts to vCenter for hosting virtual machines.

During this process, Cisco UCS Director also provides the capability to provision physical storage and present the storage as datastores that host the data for virtual machines. You can automate the creation of virtual machines and their dependent infrastructure, such as virtual switches, port groups and datastores, as per the environmental needs of tenant users and private cloud consumers.

You can launch the virtual machine console for troubleshooting purposes. You can also create complex 3-tier applications using the application container feature.

For more information about the application container feature, see the Cisco UCS Director Application Container Guide.

You can even deploy virtual machines in a highly available environment by configuring DRS rules or HA clusters. Site level redundancy can be achieved using the SRM integration feature, which allows VMs to have site level protection.

For more information about supported VMware vSphere versions and limitations on support, see the Cisco UCS Director Compatibility Matrix.

Cisco UCS Manager Orchestration Tasks

Cisco UCS Director includes orchestration features that allow you to automate the configuration and management of tasks performed by Cisco UCS Manager in one or more workflows. The same workflow can include Cisco UCS Manager, network, and storage tasks.

For more information about orchestration in Cisco UCS Director, see the Cisco UCS Director Orchestration Guide.

Location of Orchestration Tasks

A complete list of the Cisco UCS Manager orchestration tasks is available in Workflow Designer, in the Task Library, and the **Cisco UCS Tasks** folder. The Task Library, which includes a description of the orchestration tasks, can be accessed from the following locations in Cisco UCS Director:

- **Orchestration** > **Workflows**
- `http://IP_address/app/cloudmgr/onlinedocs/cloupiaTaskLib.html` where *IP_address* is the IP address of Cisco UCS Director.

Types of Orchestration Tasks

The Cisco UCS Manager orchestration tasks include tasks to configure and manage the following:

- Servers
- Server boot
- Pools
- Policies
- VLANs
- VSANs
- vNICs
- Service profiles
- Service profile templates
- Organizations

Virtual Machine Provisioning

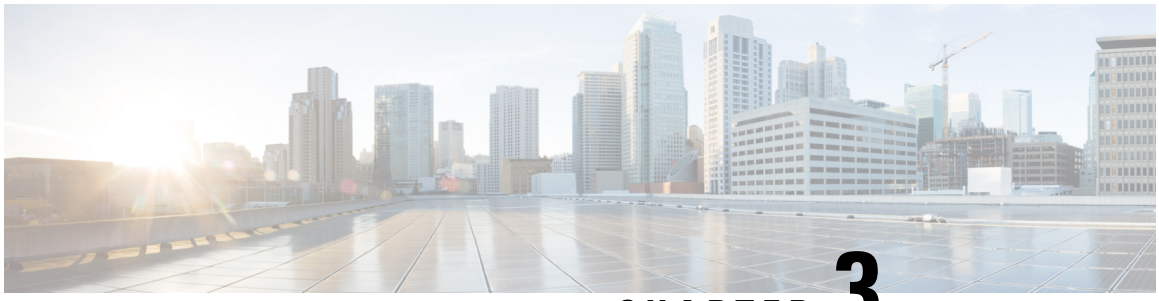
You can create reference virtual machines, which contain all the required configurations and applications to meet your business needs. These reference virtual machines are called templates, which allow for VM provisioning and standardization of software in your environment.

There are two approaches to VM provisioning:

- VM provisioning using a standardized template: All configuration is custom, which allows for rapid prototyping and standardization.

- VM provisioning using an ISO image: A base OS image is typically required in a development or QA environment, or for customers of a service provider. This can become an interactive installation.

Once a VM is provisioned using either a standardized template or ISO image, you can perform various post-provisioning actions using the VIX scripts tasks in the orchestration workflow task library.



CHAPTER 3

Managing VMware Clouds

This chapter contains the following sections:

About Managing VMware Clouds

Cisco UCS Director supports VMware through vCenter (ESX 3.5, ESX/ESXi 4.x, 5.x, 6.0 and 6.5). Cisco UCS Director automatically discovers all existing virtual machines (VMs) and images in the newly added cloud account. Typically, the discovery process takes about 5 minutes. You can also add VMware clouds

Note The term “cloud” refers to one vCenter installation.

Cisco UCS Director supports inventory collection and VM provisioning using multiple datacenters and clusters. When creating a VMware cloud, you can choose the option to discover and select multiple datacenters and clusters. Once you add a discovered datacenter and cluster to a cloud, you cannot de-select them from the cloud by editing it. However, you can edit the cloud to add extra datacenters and clusters.

Note Cisco UCS Director does not support the creation of clouds that use the same vCenter account. If there are duplicate accounts, you cannot create a VMware Cloud. In addition, if there are duplicate accounts, VM provisioning fails and an error appears in the status for the virtual account. The **Test Connectivity** function also fails with the error message. This error also occurs if the same server with the same combination of clusters is used in different clouds.

To disable this functionality, you can manually modify the `vmware.properties` file in the `cd /opt/infra/inframgr` directory to allow duplicate account IDs by setting the `allowDuplicateClouds` field to true. By default the field is set to false.

When upgrading from a previous release, all duplicate accounts display a failed connection status. Though an error message displays, all the actions can still be executed on the VMs.

Creating a VMware Cloud

When creating a VMware cloud, you can specify a datacenter and clusters in one of the following ways:

- Within the credential policy
- In the **VMware Datacenter** and **VMware Cluster** fields
- From the **Discover Datacenters / Clusters** check box

Note Either a datacenter within the credential policy or the VMware datacenter and VMware cluster can be selected. Specifying the datacenter in the **Add Cloud** screen and in the credential policy form results in an error.

Procedure

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 On the **Virtual Accounts** page, click **Virtual Accounts**.

Step 3 Click **Add**.

Step 4 On the **Add Cloud** screen, complete the required fields, including the following:

Name	Description
Cloud Type drop-down list	Displays the available cloud types. Choose VMware. **Note** The following fields are displayed when VMware is chosen. Other cloud types display fields that are specific to that cloud type.
Cloud Name field	The cloud name. The name cannot include single quotes. **Note** Each cloud requires a unique name in Cisco UCS Director. Once a cloud has been added, all reports refer to the cloud using the Cloud Name.
Server Address field	The vCenter server address
Use Credential Policy check box	Check this check box if you want to use a credential policy for this account rather than enter the information manually.

Name	Description
Use Credential Policy drop-down list	If you checked **Use Credential Policy**, choose the crednetial policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
Server User ID field	The vCenter server username.
Server Password field	The vCenter server password.
Server Access Port field	The server port number.
Server Access URL field	The server access URL.
VMware Datacenter field	The data center name on the vCenter account.
Discover Datacenters / Clusters check box	Check this check box to discover and use any VMware datacenters and associated VMware clusters.
VMware Cluster field	The name of the VMware cluster in the vCenter account. This name allows you to discover, monitor, and manage the specified pod's resources. Leave the field blank if the entire vCenter account is managed by Cisco UCS Director.
Select Datacenters / Clusters field	Check the associated datacenters and clusters you want to use. **Note** This field is visible only when you check the **Discover Datacenters / Clusters** check box.
Enable SRM check box	Check this check box to enable Site Recovery Manager (SRM) for the account.
Primary SRM Server Address field	The IP address of the primary SRM server. **Note** This field is visible only when you check the **Enable SRM** check box.
Primary SRM Server User ID field	The user ID for the primary SRM server. **Note** This field is visible only when you check the **Enable SRM** check box.
Primary SRM Server Password field	The password of the user for the primary SRM server. **Note** This field is visible only when you check the **Enable SRM** check box.

Name	Description
Primary SRM Server Access Port field	The port number for the primary SRM server. For SRM version 6.0, enter 9086 as the port number. **Note** This field is visible only when you check the **Enable SRM** check box.
Remote SRM Server User ID field	The user ID for the remote SRM server. **Note** This field is visible only when you check the **Enable SRM** check box.
Remote SRM Server Password field	The password of the user ID for the remote SRM server. **Note** This field is visible only when you check the **Enable SRM** check box.
Use SSO check box	Check this check box to use Single Sign-On (SSO) for authentication. The SSO option is only available for Virtual SAN (VSAN). SSO credentials are required for VM provisioning using storage profiles on the Virtual SAN cluster.
SSO Server Address field	The IP address of the Single-Sign On server. **Note** This field is visible only when you check the **Use SSO** check box.
SSO Server User ID field	The user ID for the SSO server. **Note** This field is visible only when you check the **Use SSO** check box.
SSO Server Password field	The password of the user ID for the SSO server. **Note** This field is visible only when you check the **Use SSO** check box.
SSO Server Access URL field	The URL for SSO server access. **Note** This field is visible only when you check the **Use SSO** check box.
SSO Server Access Port field	The port number. For vCenter version 5.x, enter 7444 as the port number. **Note** This field is visible only when you check the **Use SSO** check box.
Server Access URL field	The URL for server access.

Name	Description
Description field	The description of the cloud.
Contact Email field	The contact email address for the cloud.
Location field	The location.
Pod drop-down list	Choose the converged infrastructure pod. When you choose a pod name, the VMware cloud account is made available in the converged infrastructure stack. **Note** You cannot add more than one virtual account to a virtual SAN pod.
Service Provider field	The service provider's name.

Step 5 Click **Add**.

Testing the Connection

Procedure

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 On the **Virtual Accounts** page, click **Virtual Accounts**.

Step 3 Choose the VMware account that you want to test.

Step 4 Click **Test Connectivity**.

There is no progress bar that displays the results of the connectivity test. Use the **Summary** tab to verify that the cloud account is added and its data is collected.

Step 5 Choose **Virtual** > **Compute**.

Step 6 Click **Summary**.

It can take a few minutes to complete autodiscovery and populate the data.

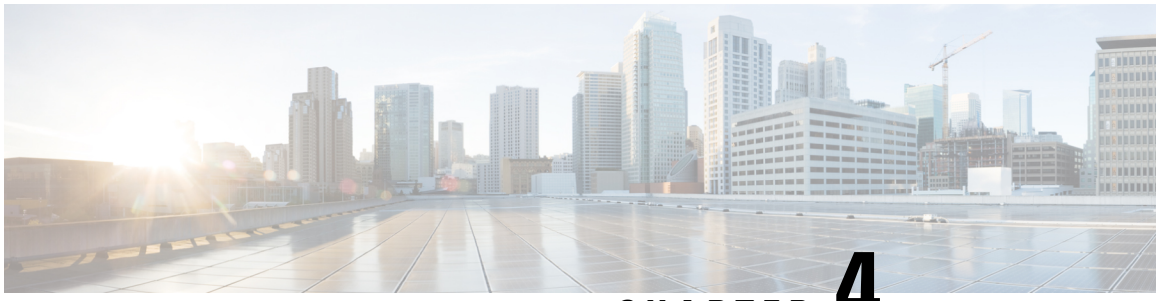
Step 7 Choose the cloud name to view its status details.

Viewing vCenter Plug-ins

Procedure

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 On the **Virtual Accounts** page, click **Plugins**.



CHAPTER 4

VMware VM Provisioning

This chapter contains the following sections:

About VMware VM Provisioning

In Cisco UCS Director you can provision new VMs in several ways, such as clone from template, clone from VM, using content library templates, and using ISO images.

See VMware Templates, on page 19 and About Virtual Machine Provisioning Using ISO Images, on page 23.

Cisco UCS Director also provides you with a predefined orchestration workflow called Provision VMware VM that you can execute to provision VMware VMs.

Creating Catalogs for Content Library-Based VM Provisioning

You can use the templates in content libraries to deploy virtual machines across VMware vCenter servers. The linked clone functionality is not supported with VM provisioning from content library VM templates. When the option to provision the new VM using a content library is selected, the **Use Linked Clone** option is disabled.

Note VMware content library discovery is only supported for VMware vCenter version 6.0 or later.

See About VMware Content Libraries, on page 17.

Cisco UCS Director supports VM provisioning using content library VM templates when a datastore or datastore cluster is selected as the target according to the following options selected in the VMware storage policy:

- Storage DRS is disabled on the datastore cluster—The datastore cluster will not be available for selection in the VMware Storage Policy and to use its datastore, you can select it as an independent datastore in the VMware Storage Policy.

- Storage DRS is enabled on the datastore cluster with the automation level set to Manual
- Storage DRS is enabled on the datastore cluster with the automation level set to Fully Automated

Note If Storage DRS is enabled on a datastore cluster with the automation level set to Fully Automated, and the allocated datastore is part of the datastore cluster, Cisco UCS Director skips the independent datastore selection during VM provisioning using the content library VM template. Instead the VM is provisioned on the datastore cluster and the following message displays in the SR log file:

```
Skipping selection of datastore for VM Provisioning using Content Library
template as given Target Datastore :{datastoreName} is attached to DRS
Enabled Datastore Cluster :{datstoreClusterName}
```

Procedure

Step 1 Choose **Policies** > **Catalogs**.

Step 2 Click **Add**.

Step 3 On the **Add Catalog** screen, choose **Standard** from the **Catalog Type** drop-down list.

Step 4 Click **Submit**.

Step 5 On the **Basic Information** screen, complete the required fields, and check **Provision new VM using Content Library VM Template**.

Step 6 Click the row with the VM template that you want to apply to the catalog.

Step 7 Complete the remaining screens in the **Add Catalog** wizard and click **Next**.

Step 8 At the final wizard screen, review the summary information and click **Submit**.

Provisioning VMs Using Orchestration Workflows

Procedure

Step 1 Choose **Orchestration**.

Step 2 On the **Orchestration** page, click **Workflows**.

Step 3 Click the row with **VMware** > **Provision VMware VM**.

Step 4 Click **Execute Now**.

Step 5 On the **Executing Workflow** screen, complete the fields including the following:

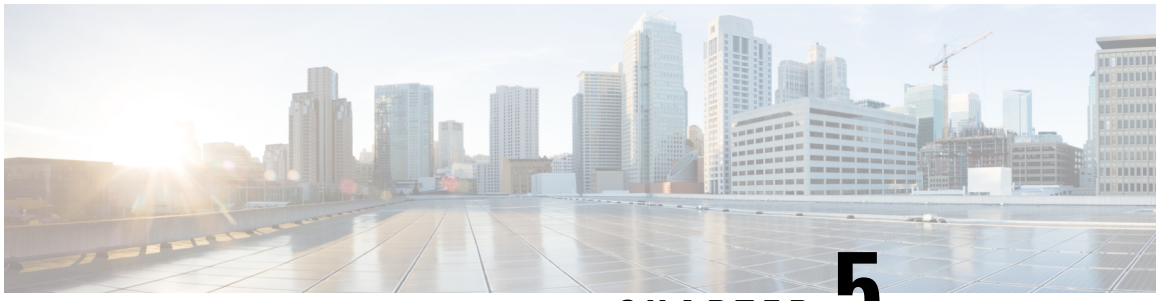
a) From the **VM Deployment Options** drop-down list, choose one of the following deployment options:

- **Clone from Template**
- **Clone from VM**
- **Move VM to VDC**

Note You can provision a VM on one datacenter by using a template available on a different datacenter under the same cloud. Likewise, you can clone a VM from one datacenter to another datacenter under the same cloud.

b) From the **Select VDC** drop-down list, choose the VDC on which the VM will be provisioned.

Step 6 Click **Submit**.



CHAPTER 5

Managing VMware Content Libraries

This chapter contains the following sections:

About VMware Content Libraries

Content libraries are container objects for VM templates and other types of files. You can create and manage a content library from a single VMware vCenter server instance. You can also share library templates to other VMware vCenter instances if HTTP(s) traffic is enabled between them.

Note VMware content library discovery is only supported for VMware vCenter version 6.0 or later.

Cisco UCS Director lets you discover and view reports for the following types of content libraries

- Local library - You can use a local library to store items in a single VMware vCenter instance. You can publish the local library so that users from other systems can subscribe to the library and access the available templates.
- Subscribed library - You can subscribe to a published local library. You must synchronize subscribed libraries to access their contents and available templates. Automatic synchronization is performed at regular intervals in VMware vCenter.

Note To perform content library inventory discovery, the Cisco UCS Director and VMware vCenter systems must have the same NTP server configured.

You can use the templates in content libraries to deploy virtual machines across VMware vCenter servers.

See Creating Catalogs for Content Library-Based VM Provisioning, on page 13.

Viewing VMware Content Library Items Reports

You can view the contents of a content library by viewing the content library items report. The content library items report displays VM templates and other files that are available in the content library.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **Content Libraries**.

Step 4 Click the row with the content library for which you want to view a report.

Step 5 Click **View Details**.

The content library items report displays all the files available in the content library including information such as the file type, size, creation date, last modified date, and last sync date.

Syncing VMware Content Libraries

Cisco UCS Director lets you synchronize a subscribed VMware content library to display the latest content and templates available.

Before you begin

Verify that the Cisco UCS Director and VMware vCenter systems have the same NTP server configured for content library inventory discovery.

Procedure

Step 1 Choose **Virtual** > **Compute**.

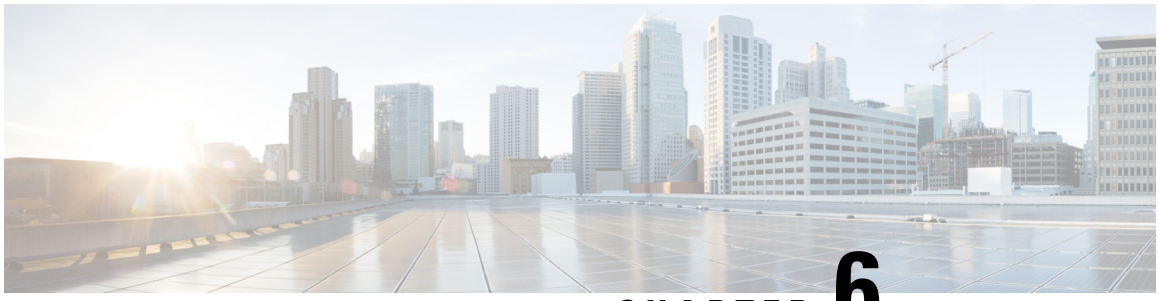
Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **Content Libraries**.

Step 4 Click the row with the subscribed content library that you want to sync.

Step 5 Click **Sync**.

Step 6 Click **Submit**.



CHAPTER 6

Managing VMware Templates

This chapter contains the following sections:

VMware Templates

A VMware Template is a master image of a virtual machine that can be used to create and provision virtual machines. A template typically includes a specified operating system and a configuration that provides virtual counterparts to hardware components. It cannot be powered on or edited, and is more difficult to alter than an ordinary virtual machine. Templates offer a more secure way of preserving a virtual machine configuration that you want to deploy multiple times.

Optionally, an administrator can create a standard catalog item on the VMware vSphere cloud that hosts a specific template. When an end user requests the catalog, a VM is provisioned based on the template that is mapped in the catalog. You can provision a VM on a datacenter by using a template available on a different datacenter under the same cloud.

Converting VMs to Images

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, click **VMs**.

Step 3 Click the row with the VM that you want to convert to an image.

Step 4 From the **More Actions** drop-down list, choose **Convert VM as Image**.

Step 5 In the **Convert VM as Image** screen, complete the fields.

Step 6 Click **Submit**.

Cloning VMs as Images

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, click **VMs**.
Step 3 Click the row with the VM that you want to clone as an image.
Step 4 From the **More Actions** drop-down list, choose **Clone VM as Image**.
Step 5 On the **Clone VM as Image** screen, complete the fields.
Step 6 Click **Submit**.

Viewing Image Reports

After you log into UCS Director, perform the following procedure to view all the images that belong to your group.

The images reports provide the following types of information:

- **Cloud**
- **Image ID**
- **Parent Node**
- **Datacenter**
- **Guest OS**
- **VMware Tools Installed**
- **VMWare Tools Version**
- **VM Version**
- **Platform**
- **Architecture**
- **Number of CPUs**
- **Provisioned Disk**
- **CPU Reservation(MHz)**

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, click **Images**.

Converting Images to VMs

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **Images**.
Step 4 Click the row with the image that you want to convert to a VM.
Step 5 Click **Convert as VM**.
Step 6 In the **Convert Image as VM** screen, click **Submit**.

Assigning Images to Groups

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **Images**.
Step 4 Click the row with the image that you want to assign to a group.
Step 5 Click **Assign Image to Group**.
Step 6 On the **Assign Image to Group** screen, choose the user and group that will be associated with the image.
Step 7 Click **Submit**.

Deploying a VM from a Template

You can deploy a VM from a template in the image report. The **Deploy VM from the Template** action provides the same functionality as the **Clone VM** action. You can quickly deploy a VM from a template, and modify any parameters necessary.

See the Cisco UCS Director Administration Guide.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **Images**.

Step 4 Click the row with the image from which you want to deploy a VM.

Step 5 Click **Deploy VM from the Template**.

Step 6 On the **Deploy VM from the Template** screen, click **Assign To User** to assign the VM to a user.

Step 7 Check **Use Linked Clone** to clone a VM from a linked clone, and choose the snapshot to associate with the linked clone.

Step 8 Click **Next**.

Step 9 On the **Customizations Option** screen, specify the option to be customized for the provisioned VM and click **Next**.

Step 10 On the **Deployment Configuration** screen, complete the fields to choose where to deploy the VM, to choose to perform provisioning now or later, and to determine how long to keep the deployed VMs running.

Step 11 Click **Next**.

Step 12 On the **Custom Specification** screen, complete the fields for custom CPU and memory parameters, if applicable.

The number of cores per socket available is specified in the VM computing policy.

Step 13 Click **Next**.

Step 14 On the **Custom Workflow** screen, click **Next**.

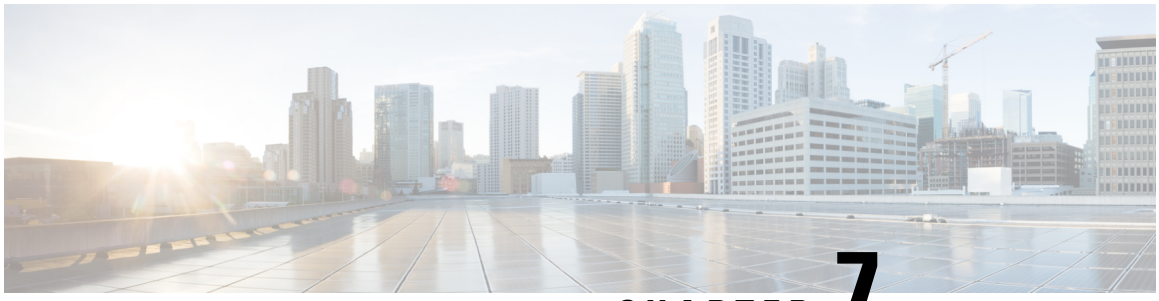
Step 15 On the **Select Datastores** screen, choose the VM disk to which you want to assign the datastores.

Step 16 Click **Next**.

Step 17 On the **Select VM Networks** screen, choose the VM network.

Step 18 Click **Next**.

Step 19 On the **Summary** screen, review the information and click **Submit**.



CHAPTER 7

VM Provisioning Using ISO Images

This chapter contains the following sections:

About Virtual Machine Provisioning Using ISO Images

In Cisco UCS Director you can provision new VMs using ISO images. Using ISO images provides more flexibility over the other methods in provisioning new VMs and installing guest operating systems.

If you provision new VMs using an ISO image, the VMs are provisioned with an ISO image that resides in a datastore. As a general convention, the datastores are exclusively used for storing ISO images, for better sharing across the environment, for centralized access, and for better file organization.

In Cisco UCS Director, you must identify and tag ISO hosting datastores, so that Cisco UCS Director can perform a deep inventory of the datastore and obtain ISO file information that resides in the datastore. Once you have a list of the ISO files, you must create ISO mapping policies to include one or more ISOs. Finally, the ISO mapping policy must be selected in the VDC computing policy to allow VM provisioning with ISO images.

In Cisco UCS Director, you can provision VMs using ISO images with the End User Portal based on the published Catalogs.

Cisco UCS Director supports collection of ISO images at any level in the datastore. The ISO images are visible when they are uploaded to any sub-folders.

Inventory containing ISO images in VSAN datastores are only supported when the ISO images are placed in any sub-folder under the root directory.

Note Folders that begin with a dot (.) are excluded from the ISO image inventory.

Viewing ISO Image Mapping Policy Reports

You can perform the following procedure to view collective information about ISO image inventory.

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **Mark DataStores for ISO Inventory Collection**.

Step 3 Click the row with the account for which you want view the associated ISO image mapping policies.

Step 4 Click **View Details**.

Marking Datastores for ISO

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **Mark DataStores for ISO Inventory Collection**.

Step 3 Click **Mark Datastores for ISO**.

Step 4 On the **Mark Datastores for ISO** dialog screen, choose the cloud and the datastores that you want to mark.

Step 5 Check the **Fetch in Account Level Inventory** check box to perform ISO inventory collection for every regular account level inventory. If unchecked, ISO inventory collection is skipped during regular account level inventory collection, reducing the regular inventory collection time.

The **Fetch in Account Level Inventory** check box lets you trigger ISO inventory collection per account on demand.

Step 6 Click **OK**.

Collecting ISO Inventory

You can perform a deep inventory of the datastore to obtain ISO file information.

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **Mark DataStores for ISO Inventory Collection**.

Step 3 Click the row with the account for which you want to collect the ISO inventory.

Step 4 Click **Collect ISO Inventory**.

Step 5 On the **Collect ISO Inventory** screen, click **OK**.

Guest OS ISO Image Mapping

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **Guest OS ISO Image Mapping**.

Step 3 Click **Add**.

Step 4 On the **Guest OS ISO Image Mapping** screen, complete the fields to add a guest OS image mapping policy.

Note If you check the **Allow End User to Select Guest OS and ISO Image** check box, you can select the guest OS and ISO image source when you create a service request. If the box is left unchecked, you can only select the guest OS when you create a service request.

Step 5 Click **Submit**.

Assigning Guest OS ISO Image Mapping Policy to VDC

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Virtual Data Centers**.

Step 2 Click the row with the VDC to which you want the guest OS ISO mapping policy to be assigned.

Step 3 Click **Edit**.

Step 4 On the **Edit VDC** screen, choose the policy from the **ISO Mapping Policy** drop-down list.

Step 5 Click **Save**.

Creating Catalogs for ISO-Based VM Provisioning

Procedure

Step 1 Choose **Policies** > **Catalogs**.

Step 2 Click **Add**.

Step 3 On the **Add Catalog** screen, choose **Standard** from the **Catalog Type** drop-down list.

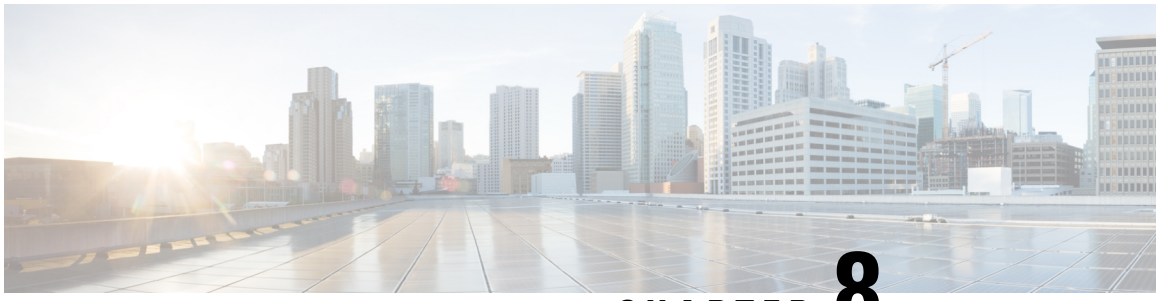
Step 4 Click **Submit**.

Step 5 In the **Basic Information** screen, check the **Provision new VM for ISO mounting** check box.
Step 6 Complete the remaining screens in the **Add Catalog** wizard and click **Next**.
Step 7 At the final wizard screen, review the summary information and click **Submit**.

Creating Service Requests for ISO-Based VM Provisioning

Procedure

Step 1 Choose **Organizations** > **Service Requests**.
Step 2 Click **Create Request**.
Step 3 On the **Create Request** screen, choose **Standard** from the **Catalog Type** drop-down list.
Step 4 Click **Submit**.
Step 5 On the **Catalog Selection** screen, choose the catalog that was published for ISO-based VM provisioning.
Step 6 Complete the remaining screens in the **Create Service Request** wizard, and click **Next**.
Step 7 At the final wizard screen, review the summary information and click **Submit**.



CHAPTER 8

Managing VMware Linked Clones

This chapter contains the following sections:

About VMware Linked Clones

A linked clone is a copy of a virtual machine that continually shares virtual disks with the parent virtual machine. This conserves disk space, and allows multiple virtual machines to use the same software installation.

A linked clone is made from a snapshot of the parent. All files available on the parent at the moment of the snapshot continue to remain available to the linked clone. Ongoing changes to the virtual disk of the parent do not affect the linked clone, and changes to the disk of the linked clone do not affect the parent. A linked clone must have access to the parent. Without access to the parent, a linked clone is disabled.

For more information on managing VM snapshots, see the Cisco UCS Director Administration Guide and the Cisco UCS Director End User Portal Guide.

The following scenarios apply for linked clone functionality:

- If a VM remains out of all the VMs being deleted from linked clone VMs, then all the VMs are brought back to the original size of the parent VM.
- If a VM is migrated to some other host and datastore, it retains the original size of the parent VM.

Using VMware Linked Clones in Cisco UCS Director

Before you begin

Before you clone a VM you must note the following:

- During storage policy creation, if you chose to use linked clones (by checking the **Use Linked Clone** check box), the clone will be a linked clone. However, if you did not check the box, the clone will be a full clone.
- During resource allocation, only those hosts that have access to the parent's images or the VM's datastores are selected as linked clones.

- You must create a new snapshot or use an existing snapshot to create the linked clone.

Note If you are creating a Standard Catalog item on the VMware vSphere Cloud using the linked clone feature, the selected VM template image must have a snapshot. If it does not have a snapshot, you need to create a new snapshot on the VM before converting it into a VM template image, and perform an inventory to sync Cisco UCS Director with vCenter.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, click **VMs**.

Step 3 Click the row with the VM for which you want to use linked clone functionality.

Step 4 From the **More Actions** drop-down list, choose **Clone**.

Step 5 On the **Clone VM** screen, complete the fields to create the linked clone from an existing snapshot or a new snapshot.

Step 6 On the **Customization Options** screen, complete the fields including the following:

a) Check the **Provision all disks in single datastore** check box to provision all disks in a single datastore.

Note The scope is the same as the system disk scope.

b) Choose the VM Application Charge Frequency, which can be hourly or monthly.

Step 7 Click **Next**.

Step 8 On the **Deployment Configuration** screen, complete the fields to choose where to deploy the VM, to choose to perform provisioning now or later, and to determine how long to keep the deployed VMs running.

Step 9 Click **Next**.

Step 10 On the **Custom Specification** screen, complete the fields for custom CPU and memory parameters, if applicable.

Step 11 Click **Next**.

Step 12 On the **Custom Workflow** screen, click **Next**.

Step 13 On the **Select Datastores** screen, choose the VM disk to which you want to assign the datastores.

Step 14 Click **Next**.

Step 15 On the **Select VM Networks** screen, choose the VM network.

Step 16 Click **Next**.

Step 17 On the **Summary** screen, review the information and click **Submit**.

Viewing Linked Clone VMs Reports

Procedure

Step 1 Choose **Virtual** > **Compute**.

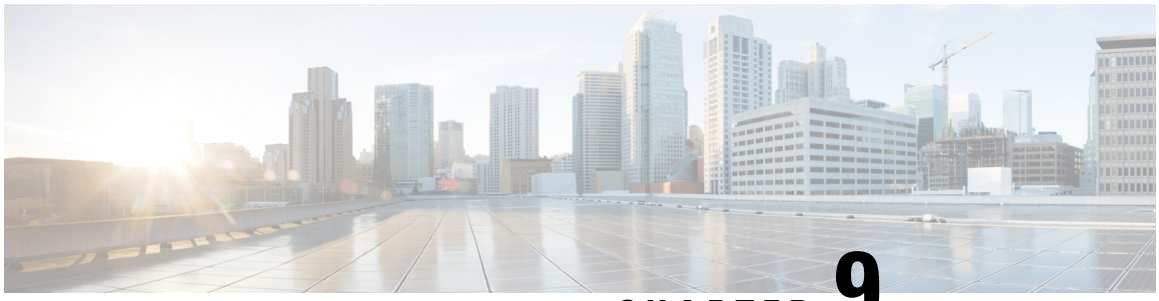
Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **Images**.

Step 4 Click the row with the image for which you want to view the linked clone VMs report.

Step 5 Click **View Details**.

Step 6 Click **Linked Clone VMs**.
You can view a report of all the linked clone VMs for each snapshot.



CHAPTER 9

Managing VMware Datastore Clusters

This chapter contains the following sections:

About VMware Datastores

A datastore is the storage repository for virtual machines and their data. A datastore can be either a Network File System (NFS) or Virtual Machine File System (VMFS). Cisco UCS Director provides a task library to create datastores from physical storage. Newly created and existing datastores are then used in VDC storage policies to provide a policy-based framework, from which you can select an appropriate datastore during VM provisioning. Datastores can also be identified as ISO image repositories to aid in ISO-based VM provisioning.

About VMware Datastore Clusters

A VMware datastore cluster is a collection of datastores with shared resources and a shared management interface. When you create a datastore cluster, you can use VMware vSphere Storage DRS to manage storage resources.

Integrating VMware Datastore Clusters With Cisco UCS Director

Cisco UCS Director allows you to manage VMware datastore clusters. You can add, edit and delete datastore clusters. Once a datastore cluster is added, the following operations are supported in Cisco UCS Director:

- The datastore clusters are available along with datastores during Clone VM, Clone Template and Create New VM operations. If datastore clusters are selected, SDRS recommends the most suited datastore for VM provisioining.
- The datastore clusters can be selected while adding a VMware Storage policy.

- DRS affinity rules can be added to the datastore cluster.

  For more information on using DRS affinity rules, see About VMware Distributed Resource Scheduler, on page 77.

Adding Datastore Clusters

Procedure

Step 1 Choose **Virtual** > **Storage**.

Step 2 On the **Storage** page, choose the cloud.

Step 3 On the **Storage** page, click **Datastore Clusters**.

Step 4 Click **Create**.

Step 5 On the **Create Datastore Cluster** screen, complete the fields including the following:

a) You can check the **Enable Storage DRS** check box to enable Storage DRS to manage storage resources for the selected datastores.

b) You can check the **Enable I/O Metric for SDRS recommendations** for Storage DRS to recommend the most suitable datastore for VM provisioning.

c) Choose the automation level. If you choose **Manual**, the placement and migration recommendations from Storage DRS are not run until you manually apply the recommendation. If you choose **Fully Automated**, the placement and migration recommendations from Storage DRS are run automatically.

Step 6 Click **Submit**.

Viewing Datastore Cluster DRS Rule Reports

Procedure

Step 1 Choose **Virtual** > **Storage**.

Step 2 On the **Storage** page, choose the cloud.

Step 3 On the **Storage** page, click **Datastore Clusters**.

Step 4 Click the row with the datastore cluster for which you want to view the associated DRS rules..

Step 5 Click **View Details**.

Step 6 Click **SDRS Rules** to view the DRS rules associated with the datastore cluster.

The DRS rules report displays the following types of rules:

- Inter VM Anti-Affinity Rules -- VM Anti Affinity.
- Intra VM Anti-Affinity Rules -- Anti Affinity.
- INTRA_VM_AFFINITY_ENABLED -- This rule represents the Intra VM Affinity enabled VMs.

- INTRA_VM_AFFINITY_DISABLED -- This rule represents the Intra VM Affinity disabled VMs.

Adding Datastore Cluster DRS Rules

Cisco UCS Director lets you add the following types of DRS affinity rules to a VMware datastore cluster:

- Inter-VM Anti-Affinity -- This rule specifies virtual machines that should never be on the same datastore.
- Intra-VM Anti-Affnity -- This rule specifies virtual disks, that are associated with a particular virtual machine, which must be on different datastores.

Note Cisco recommends that you create DRS rules with unique names. Using duplicate names causes issues with the affinity type selection when modifying the datastore cluster DRS rule.

Procedure

Step 1 Choose **Virtual** > **Storage**.

Step 2 On the **Storage** page, choose the cloud.

Step 3 On the **Storage** page, click **Datastore Clusters**.

Step 4 Click the row with the datastore cluster to which you want to add a DRS rule.

Step 5 Click **View Details**.

Step 6 Click **SDRS Rules**.

Step 7 Click **Add**.

Step 8 On the **Add Rule** screen, complete the following fields:

Name	Description
Name field	The name of the rule.
Type drop-down list	Choose the type of rule. It can be one of the following: • **VM Anti Affinity** -- Choose this option to add an inter-VM anti-affinity rule. • **VM Disk Anti Affinity** -- Choose this option to add an intra-VM anti-affinity rule.
Status drop-down list	Choose the status of the rule. It can be one of the following: • **Enabled** • **Disabled**

Name	Description
Select VM	Select the VM.
Select Disks	If the **VM Disk Anti Affinity** rule type is chosen, select the disks.
Proceed with Conflicts check box	Check the box to proceed with conflicts.

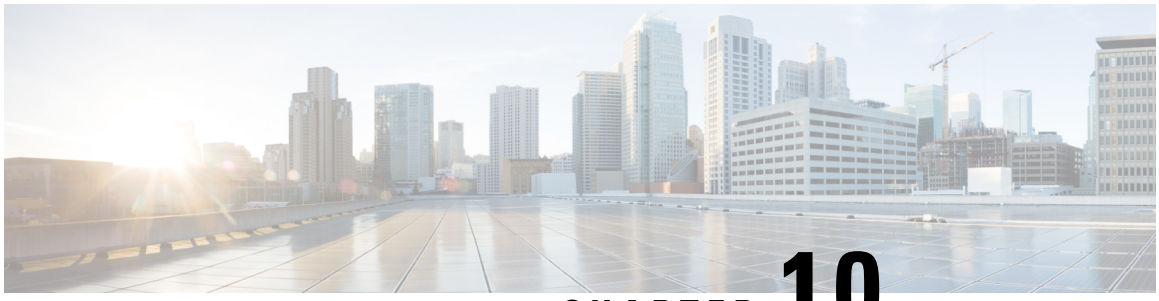
Step 9 Click **Submit**.

Enabling or Disabling Datastore Cluster DRS Rules

By default, when a Storage DRS rule is created, enabled, or disabled, the rule is created or updated, but not automatically applied. You can either run Storage DRS rules manually through VMware vSphere web client or wait until the scheduled period for the Storage DRS rule to run. You can modify the scheduled period to check imbalances under **Advanced Options** in the **Storage DRS Runtime Settings** using the VMware vSphere Web Client. By default the scheduled period is set for every 8 hours.

Procedure

Step 1 Choose **Virtual** > **Storage**.
Step 2 On the **Storage** page, choose the cloud.
Step 3 On the **Storage** page, click **Datastore Clusters**.
Step 4 Click the row with the datastore cluster for which you want to enable or disable DRS rules.
Step 5 Click **View Details**.
Step 6 Click **SDRS Rules**.
Step 7 Click **Enable Intra VM Affinity** or **Disable Intra VM Affinity**.
Step 8 On the **Enable VMDK Affinity Rule** or **Disable VMDK Affinity Rule** screens, select the VMs on which to enable or disable the rule.
Step 9 Click **Submit**.



CHAPTER 10

Managing Virtual SAN Clusters

This chapter contains the following sections:

About Virtual SAN Clusters

A virtual storage area network (Virtual SAN) cluster is a collection of virtualized local physical storage resources. A Virtual SAN cluster provides isolation among devices that are physically connected to the same fabric by abstracting them into storage pools.

Cisco UCS Director allows you to create a Virtual SAN storage profile to define the storage requirements for the files and disks of a virtual machine by specifying a set of required storage capabilities.

In Cisco UCS Director you can create Virtual SAN qualification policies. A Virtual SAN qualification policy allows you to filter a unique list of servers based on defined requirements that include server model, storage controller model, and a minimum number of solid state drives and hard disk drives. After creating a Virtual SAN qualification policy, you can use the policy to qualify Virtual SAN-capable servers based on the defined requirements.

Cisco UCS Director supports the following Virtual SAN features:

- Setup of Virtual SAN clusters for manually configured EXi nodes
- Inventory of existing Virtual SAN clusters
- Management of Virtual SAN clusters under the Cisco UCS Director tabs
- Creation of Virtual SAN storage profiles
- Mechanism to select virtual machine storage profiles
- Ability to select datastores matching storage profiles
- Virtual machine provisioning with Virtual SAN capable datastores

Creating Virtual SAN Pods

A Virtual SAN pod lets you manage your Virtual SAN with the addition of a VMware Cloud account and Cisco UCS Manager or Cisco UCS Central . The Virtual SAN Pod Wizard lets you create one pod. Each pod is limited to one VMware Cloud account and one Cisco UCS Manager or Cisco UCS Central account.

Procedure

Step 1 Choose **Administration** > **Guided Setup**.

Step 2 Double-click the **Virtual SAN Pod Configuration** icon.

Step 3 Click **Next**.

Step 4 On the **Pod** screen, create or choose an existing pod.

Note A single VSAN pod supports either a Cisco UCS Manager account or a Cisco UCS Central account.

Step 5 Click **Next**.

Step 6 On the **Cisco UCS Manager** screen, create a new Cisco UCS Manager account to add to the pod or choose an existing Cisco UCS Manager account.

You can use an existing Cisco UCS Manager account if you want the pod to reference an account that exists in Cisco UCS Director within another pod.

Step 7 Click **Next**.

Step 8 On the **Cisco UCS Central** screen, create a new Cisco UCS Central account to add to the pod or choose an existing Cisco UCS Central account.

You can use an existing Cisco UCS Central account by updating the pod.

Note You cannot edit the details in the **Cisco UCS Central** screen, if you have added Cisco UCS Manager account to the pod since a single VSAN pod supports either a Cisco UCS Manager account or a **Cisco UCS Central** account.

Step 9 Click **Next**.

Step 10 On the **VMware** screen, create a new VMware account to add to the pod or choose an existing VMware account.

You can use an existing VMware account if you want the pod to reference an account that exists in Cisco UCS Director within another pod.

While adding the VMware account, choose the **Use SSO** option and provide SSO credentials. SSO credentials are required for VM provisioning using storage profiles on the Virtual SAN cluster.

Step 11 At the final wizard screen, review the summary information.

Step 12 Click **Submit**.

Viewing Virtual SAN Pod Reports

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod for which you want to view the report.

Step 4 Click **View Details**.
The Virtual SAN pod report provides information on **Virtual SAN Clusters**, **Storage Profile**, **Service Profile Templates**, **Qualification Policies**, and **System Tasks**.

Alternately you can also view the Virtual SAN pod report by choosing the Virtual SAN pod on the **Converged** screen.

Viewing Virtual SAN Cluster Reports

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the pod associated with the Virtual SAN cluster for which you want to view a report.

Step 4 Click **View Details**.
All the Virtual SAN clusters related to the selected pod are displayed on the **Clusters** screen.

Step 5 Click the row with the Virtual SAN cluster for which you want to view a report.

Step 6 Click **View Details** to see the details of the Virtual SAN cluster.
By default, the **Summary** screen appears. The Virtual SAN cluster report includes the **Service Request**, **Datastore Capacity Report**, **Hosts**, **Disk Groups**, **Disks**, **License**, and **Topology** screen.

Configuring Virtual SAN settings at the Pod Level

You can configure Virtual SAN settings at the pod level by editing the pod settings. You can select a bare metal agent server, a UCS service profile template, a LAN boot policy, a scrub policy, and various networking policies at the pod level. The selected defined networking policies are applied while creating the cluster in the pod. The UCS service profile template, bare metal agent, LAN boot policy, and scrub policy are required to support bare metal installation of ESXi on UCS servers.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click on the row with the Virtual SAN pod for which you want to configure the pod settings.

Step 4 lick **Pod Settings**.

Step 5 On the **Pod Settings** screen, select the bare metal agent servers, and select one or more UCS service profile templates, LAN boot policies, and the scrub policies.

Step 6 Click **Next**.

Step 7 On the **Network Policies** screen, select one or more networking policies to apply at the pod level.

Step 8 Click **Submit**.

Creating Virtual SAN Clusters

Before you begin

- Configure Virtual SAN pod settings.

  See Configuring Virtual SAN settings at the Pod Level, on page 38.

- Ensure that the Virtual SAN pod is associated with a VMware account and a Cisco UCS Manager account.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod on which you want to create the Virtual SAN cluster.

Step 4 Click **View Details**.

Step 5 Click **Virtual SAN Clusters**.

Step 6 Click **Create Virtual SAN Cluster**.

Step 7 On the **Create Virtual SAN Cluster** screen, complete the fields for the host.

If you are creating a Virtual SAN cluster using ESXi, choose **ESXi Host**.

If you choose **ESXi Host**, you must provide the host node IP addresses in a comma-separated list.

The **Claim Disk Mode** drop-down list lets you expand the cluster by adding disks. If automatic mode is selected, eligible disks from all hosts will be claimed automatically to contribute to the Virtual SAN datastore capacity. Manual mode creates a Virtual SAN cluster with a capacity of 0 GB, and you will have to manually add disks to the cluster.

Step 8 Click **Next**.

Step 9 Leave the DV Switch field empty, and click **Next**.

Note If you already have a Virtual SAN cluster created using Cisco UCS Director and would like to use the DV Switch created for it, select the existing DV Switch.

Step 10 Complete the fields for the data center and cluster name, and check **Enable HA** and **Enable DRS** if you want to enable HA or DRS on the Virtual SAN cluster.

Step 11 Click **Next**.

Step 12 Select the RAID mode and choose the MTU size.

The default RAID mode is JBOD, and the default MTU size is 1500.

Step 13 Click **Next**.

Step 14 On the **Summary** screen, review the **Service Profile Template Compliance** report.

The compliance report verifies if the pre-requisites were met and if the UCS service profile template was configured properly. The compliance report verifies network configuration requirements, boot policy requirements, LAN boot policy requirements, scrub policy requirements, BIOS policy requirements, and local disk configuration policy requirements.

If any of the fields are not compliant, you should edit the corresponding policy in the UCS service profile template so that they are compliant with all requirements.

Step 15 Click **Submit**.

The Virtual SAN cluster appears on the **Virtual SAN Clusters** screen of the Virtual SAN pod report.

Expanding Virtual SAN Clusters

When expanding a Virtual SAN Cluster, the HA and DRS settings will reflect those of the existing cluster.

For information on enabling or disabling HA on a Virtual SAN cluster, see Enabling HA on Virtual SAN Clusters, on page 45 and Disabling HA on Virtual SAN Clusters, on page 45.

For information on enabling or disabling DRS on a Virtual SAN cluster, see Enabling DRS on Virtual SAN Clusters, on page 46 and Disabling DRS on Virtual SAN Clusters, on page 46.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod associated with the Virtual SAN Cluster that you want to expand.

Step 4 Click **View Details**.
All the Virtual SAN clusters associated with the pod are displayed.

Step 5 Click the row with the Virtual SAN cluster that you want to expand.

Step 6 Click **Expand Virtual SAN Cluster**.

Step 7 In the **Expand Virtual SAN Cluster** screen, complete the fields for the UCS Server, UCS Server Pool, or ESXI host.

If you are expanding a Virtual SAN cluster from a bare metal server, choose **UCS Server** or **UCS Server Pool** to install ESXi. Otherwise, choose **ESXI Host**.

By default, the RAID mode and MTU size values are automatically populated from the values selected during the initial cluster configuration.

Step 8 Click **Next**, and click **Submit**.

Virtual SAN Clusters from a Bare Metal Server

Prerequisites for Creating a Virtual SAN from a Bare Metal Server

Before you create a Virtual SAN from a bare metal server, you must meet the following prerequisites.

VMware Virtual SAN Controller Requirements

For CISCO UCS 240 M3 Rack Servers, the `storcliExtractor.sh` script will automatically create a virtual RAID 0 drive for each physical HDD that VMware Virtual SAN uses.

To configure virtual RAID 0 with the LSI controller:

- Download the MegaRAID StorCLI software from the Avago Technologies website.

  For more information, see http://www.avagotech.com/support/download-search/.

- Run the `storcliExtractor.sh` script located in the `opt/scripts` directory.

  The `storcliEstractor.sh` script extracts the downloaded MegaRAID StorCLI software and makes it available for use. The script is available with the Cisco UCS Director Bare Metal Agent, Release 5.2 patch.

UCS Service Profile Template Configuration Requirements

The following UCS service profile template configuration is required for bare metal server actions and workflows.

This configuration does not include all Cisco UCS service profile settings. The settings shown here are specific to an implementation of Cisco UCS with VMware Virtual SAN.

Note You must create a new UCS service profile template. Cisco UCS with VMware Virtual SAN implementation does not support updating an existing UCS service profile template.

When creating a Virtual SAN UCS service profile template, the template should not be associated with any server pool. You can select the **Assign Later** option in the server pool template, to assign the server pool to the Virtual SAN service profile.

For more information on creating a Virtual SAN UCS service profile template, see About Virtual SAN UCS Service Profile Templates, on page 97.

BIOS Policy Requirements

Cisco UCS C240 M3 servers require a BIOS policy with the USB UI, USBPort:SDCard advanced setting set to Enable.

Network Configuration Requirements

Make sure that three vNICs are defined in the template. Cisco UCS Director Virtual SAN workflows define the management on the first vNIC during the ESXi installation. The next two vNICs are used in explicit failover order for the Virtual SAN traffic.

Note If the vNICs have different VLANs specified, make sure that the vNICs are ordered, and that the first vNIC satisfies the PXE VLANs requirement.

Virtual SAN requires that multicast is enabled on the network. You must define a multicast policy and make sure that the Virtual SAN VLAN is set to use the defined multicast policy.

You can configure jumbo Maximum Transition Unit (MTU) end-to-end across Cisco Data Center devices in a network.

For more information on setting up Cisco uplink switches, see:

http://www.cisco.com/c/en/us/support/docs/switches/nexus-5000-series-switches/112080-config-mtu-nexus.html

http://www.cisco.com/c/en/us/support/docs/servers-unified-computing/ucs-b-series-blade-servers/117601-configure-UCS-00.html

Note VLANs and MAC pools must be created and configured prior to service profile creation, and the VLAN must have a multicast policy enabled. You must create the boot policy with a Secure Digital (SD) card as the preferred boot option, and dedicated VMkernel ports are used for VSAN and vMotion traffic.

Boot Policy Requirements

Cisco UCS Director Virtual SAN workflows support installing ESXi with an SD card. The UCS service profile template should specify the SD card as a boot device in the boot order. You must define a boot policy with the boot order SD card and set boot policy to the UCS service profile template.

Local Disk Configuration Policy Requirements

Different Mode settings are required based on the server and storage controller RAID Mode.

To use an SD card, the FlexFlash state must be set to Enable.

LAN Boot Policy Requirement for Virtual SAN

You must define a boot policy with the LAN on the first vNIC defined in the UCS service profile template configuration set first in the boot order.

Creating Virtual SAN Clusters Using Cisco UCS Bare Metal Servers

You can create a Virtual SAN cluster using a Cisco UCS bare metal server.

Before you begin

- Create a Virtual SAN pod with Cisco UCS Manager and VMware accounts if the Cisco UCS servers are managed through Cisco UCS Manager.
- Create a Virtual SAN pod with Cisco UCS Central and VMware accounts if the Cisco UCS servers are managed through Cisco UCS Central .
- Add a Cisco UCS Director Bare Metal Agent account, configure DHCP, and start services.
- Configure the pod settings with bare metal agent and UCS service profile template and policies if Cisco UCS Manager is being used within the Virtual SAN pod.
- Configure the pod settings with bare metal agent and global service profile template and global policies if Cisco UCS Central is being used within the Virtual SAN pod.
- Complete the prerequisites for creating Virtual SAN clusters using Cisco UCS bare metal servers.
- Download the ESXi install (ISO) images and run the `isoExtractor.sh` script.

  You must select ESXi 5.5, 6.0, or 6.5 VSAN template as the OS type and provide the required inputs to create an ESXi OS catalog for Virtual SAN. The created ESXi OS catalog is selected when creating a Virtual SAN cluster using a Cisco UCS bare metal server.

For more information about adding a Cisco UCS Director Bare Metal Agent account, see the Cisco UCS Director Bare Metal Agent Installation and Configuration Guide.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod on which you want to create the Virtual SAN cluster.

Step 4 Click **View Details**.

Step 5 Click **Virtual SAN Clusters**.

Step 6 Click **Create Virtual SAN Cluster**.

Step 7 On the **Create Virtual SAN Cluster** screen, complete the fields for the host.

If you are installing ESXi on a bare metal server, choose **UCS Server** or **UCS Server Pool**. The server pools and policies are listed based on the option selected.

The **Claim Disk Mode** drop-down list lets you expand the cluster by adding disks. If automatic mode is selected, eligible disks from all hosts will be claimed automatically to contribute to the Virtual SAN datastore capacity. Manual mode creates a Virtual SAN cluster with a capacity of 0 GB, and you will have to manually add disks to the cluster.

Step 8 Select an existing DV Switch, choose the network policies you want to use.

Note The selection of an existing DV Switch is optional. If a DV Switch is not selected, a new DV Switch will be created as part of the cluster.

Step 9 Click **Next**.

Step 10 Complete the fields for the data center and cluster name, and check **Enable HA** and **Enable DRS** if you want to enable HA or DRS on the Virtual SAN cluster.

Step 11 Click **Next**.

Step 12 Select the RAID mode, and click **Next**.

The default RAID mode is JBOD.

Step 13 In the **Summary** pane, review the **Service Profile Template Compliance** report.

The compliance report verifies if the pre-requisites were met and if the UCS service profile template was configured properly. The compliance report verifies network configuration requirements, boot policy requirements, LAN boot policy requirements, scrub policy requirements, BIOS policy requirements, and local disk configuration policy requirements.

If any of the fields are not compliant, you should edit the corresponding policy in the UCS service profile template so that they are compliant with all requirements.

Step 14 Click **Submit**.

The Virtual SAN cluster appears on the **Clusters** screen of the Virtual SAN pod report.

Expanding Virtual SAN Clusters from a Bare Metal Server

When expanding a Virtual SAN Cluster from a bare metal server, the HA and DRS settings will reflect those of the existing cluster.

For information on enabling or disabling HA on a Virtual SAN cluster, see Enabling HA on Virtual SAN Clusters, on page 45 and Disabling HA on Virtual SAN Clusters, on page 45.

For information on enabling or disabling DRS on a Virtual SAN cluster, see Enabling DRS on Virtual SAN Clusters, on page 46 and Disabling DRS on Virtual SAN Clusters, on page 46.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod associated with the Virtual SAN Cluster that you want to expand.

Step 4 Click **View Details**.
All the Virtual SAN clusters associated with the pod are displayed.

Step 5 Click the row with the Virtual SAN cluster that you want to expand.

Step 6 Click **Expand Virtual SAN Cluster**.

Step 7 On the **Expand Virtual SAN Cluster** screen, complete the host details field.

Choose **UCS Server** or **UCS Server Pool** to install ESXi on the bare metal server.

By default, the RAID mode and MTU size values are automatically populated from the values selected during the initial cluster configuration. You have the option to change the RAID mode from the drop-down menu.

Note A warning message appears if you change the RAID mode to a value different from the RAID mode selected during the initial cluster configuration.

Step 8 Click **Next**, and click **Submit**.

Assigning Virtual SAN Clusters to a Pod

You can discover existing Virtual SAN clusters and assign them to an existing Virtual SAN pod.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod to which you want to assign a Virtual SAN cluster.

Step 4 Click **View Details**.

Step 5 Click **Virtual SAN Clusters**.

Step 6 Click **Assign Cluster(s) to Pod**.

The **Assign Cluster(s) to Pod** screen displays all Virtual SAN clusters discovered from existing VMware vCenter accounts added in Cisco UCS Director.

Step 7 In the **Assign Cluster(s) to Pod** screen, select one or more Virtual SAN clusters and click **Submit**.
The assigned Virtual SAN cluster appears on the **Virtual SAN Clusters** details screen for the selected pod.

Enabling HA on Virtual SAN Clusters

Cisco UCS Director lets you enable VMware vSphere HA on Virtual SAN Clusters. You can enable HA when creating a new Virtual SAN cluster, or enable HA on an existing Virtual SAN cluster. When enabling HA on an existing Virtual SAN cluster, host monitoring and admission control are automatically enabled by default to ensure that there are sufficient resources available in a cluster when recovering from a failure.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod associated with the Virtual SAN cluster on which you want to enable HA.

Step 4 Click **View Details**.
All the Virtual SAN clusters associated with the pod are displayed.

Step 5 Click the row with the Virtual SAN cluster on which you want to enable HA.

Step 6 Click **Enable HA**.

Step 7 In the **Enable HA** screen, choose the **Host Isolation Response**, **VM Monitoring**, and **Datastore Heartbeating** options.

Step 8 Click **Submit**.

Disabling HA on Virtual SAN Clusters

Procedure

Step 1 \

Step 2 Choose **Hyper Converged** > **Virtual SAN**.

Step 3 On the **Virtual SAN** page, click **Pods**.

Step 4 Click the row with the Virtual SAN pod associated with the Virtual SAN cluster on which you want to disable HA.

Step 5 Click **View Details**.
All the Virtual SAN clusters associated with the pod are displayed.

Step 6 Click the row with the Virtual SAN cluster on which you want to disable HA.

Step 7 Click **Disable HA**.

Step 8 In the **Disable HA** screen, click **Submit**.

Enabling DRS on Virtual SAN Clusters

Cisco UCS Director lets you enable VMware Distributed Resource Scheduler (DRS) on Virtual SAN Clusters. You can enable DRS when creating a new Virtual SAN cluster, or enable DRS on an existing Virtual SAN cluster. When enabling DRS on an existing Virtual SAN cluster you can specify the DRS automation level.

For more information on using DRS affinity rules and automation levels, see About VMware Distributed Resource Scheduler, on page 77.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod associated with the Virtual SAN cluster on which you want to enable DRS.

Step 4 Click **View Details**.
All the Virtual SAN clusters associated with the pod are displayed.

Step 5 Click the row with the Virtual SAN cluster on which you want to enable DRS.

Step 6 Click **Enable DRS**.

Step 7 In the **Enable DRS** screen, check the **Enable DRS** checkbox and select the DRS automation level.

Step 8 Click **Submit**.

Disabling DRS on Virtual SAN Clusters

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod associated with the Virtual SAN cluster on which you want to disable DRS.

Step 4 Click **View Details**.
All the Virtual SAN clusters associated with the pod are displayed.

Step 5 Click the row with the Virtual SAN cluster on which you want to disable DRS.

Step 6 Click **Disable DRS**.

Step 7 In the **Disable DRS** screen, click **Submit**.

Viewing Virtual SAN Storage Profile Reports

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod for which you want to view the storage profile..

Step 4 Click **View Details**.

Step 5 Click **Storage Profile**.
All the Virtual SAN storage profiles displayed in Cisco UCS Director are at cloud-level and are associated with a selected pod.

Step 6 Click the row with the Virtual SAN storage profile you want to view.

Step 7 Click **View Details** to see the details of the Virtual SAN storage profile.

Creating Virtual SAN Storage Profiles

Procedure

Step 1 \

Step 2 Choose **Hyper Converged** > **Virtual SAN**.

Step 3 On the **Virtual SAN** page, click **Pods**.

Step 4 Click the row with the Virtual SAN pod.

Step 5 Click **View Details**.

Step 6 Click **Storage Profile**.

Step 7 Click **Create Virtual SAN Storage Profile**.

Step 8 In the **Create Storage Profile** screen, enter the storage profile name, the storage profile description, and complete the rule-set fields based on vendor-specific capabilities.

Step 9 Click **Submit**.

Viewing Virtual SAN UCS Service Profile Templates

Before you begin

Create a Virtual SAN UCS service profile template.

See About Virtual SAN UCS Service Profile Templates, on page 97.

See Creating Virtual SAN UCS Service Profile Templates, on page 98.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod for which you want to view the UCS Virtual SAN service profile templates.

Step 4 Click **View Details**.

Step 5 Click the **Service Profile Template**.
All the Virtual SAN UCS service profile templates associated with the pod are displayed.

Step 6 Click the row with the Virtual SAN UCS service profile template.

Step 7 Click **View Details**.

By default, the **Summary** screen appears. You can also view related local disk configuration policy, boot policy, vNIC, scrub policy and BIOS policy details, respectively, by clicking **Local Disk Configuration Policies**, **Boot Policies**, **vNICs**, **Scrub Policy**, or **BIOS Policy**.

Claiming Virtual SAN Disks

At the Virtual SAN cluster level, you can claim disks to create shared storage across multiple hosts.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod associated with the Virtual SAN cluster.

Step 4 Click **View Details**.
All the Virtual SAN clusters associated with the pod are displayed.

Step 5 Click the row with the Virtual SAN cluster.

Step 6 Click **Claim Disk**.
The dialog box displays all of the hosts with available unused data disks.

Step 7 In the **Claim Disk** screen, choose the disks you want to claim, and click **Submit**.

The all disks will appear on the **Disks** screen under the selected Virtual SAN cluster report.

Adding Disks to a Virtual SAN Disk Group

You can add a disk group to a Virtual SAN disk group.

Procedure

Step 1	Choose **Hyper Converged** > **Virtual SAN**.
Step 2	On the **Virtual SAN** page, click **Pods**.
Step 3	Click the row with the Virtual SAN pod associated with the Virtual SAN host.
Step 4	Click **View Details**. All the Virtual SAN clusters associated with the pod are displayed.
Step 5	Click the row with the Virtual SAN cluster.
Step 6	Click **View Details**.
Step 7	Click **Disk Groups**. All of the disk groups associated with the Virtual SAN cluster are displayed.
Step 8	Click the row with the disk group to which you want to add disks.
Step 9	Click **Add Disks to Disk Group**.
Step 10	In the **Add disks to Disk Group** screen, select the disks to add to the Virtual SAN disk group.
Step 11	Click **Submit**.

Viewing Virtual SAN Disk Groups

Procedure

Step 1	Choose **Hyper Converged** > **Virtual SAN**.
Step 2	On the **Virtual SAN** page, click **Pods**.
Step 3	Click the row with the Virtual SAN pod associated with the Virtual SAN cluster.
Step 4	Click **View Details**. All the Virtual SAN clusters associated with the pod are displayed.
Step 5	Click the row with the Virtual SAN cluster.
Step 6	Click **View Details**.
Step 7	Click **Disk Groups** to view the details for the disk groups associated with the Virtual SAN cluster.

Viewing Virtual SAN Qualification Policy Reports

Procedure

Step 1	Choose **Hyper Converged** > **Virtual SAN**.
Step 2	On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod for which you want to view the Virtual SAN qualification policy report.

Step 4 Click **View Details**.

Step 5 Click **Qualification Policies**.
All the Virtual SAN qualification policies associated with the pod are displayed.

Creating Virtual SAN Qualification Policies

You can create and define a qualification policy at the pod level. You can create new qualification policies with different combinations of server qualifications depending on your requirements.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod on which you want to create the Virtual SAN qualification policy and then click **View Details**.

Step 4 Click **Qualification Policies**.

Step 5 Click **Create Virtual SAN Qualification Policy**.

Step 6 On the **Create Virtual SAN Qualification Policy** screen, in the **Standard Policy** drop-down menu, choose **None**, **Standard M3 Policy**, or **Standard M4 Policy**, and complete the fields for the qualification policy. If you choose **Standard M3 Policy** or **Standard M4 Policy**, the **Server Model PID (Regex)**, **Storage Controller Model (Regex)**, **SSD count**, and **HDD Count** fields are automatically populated.

Step 7 Click **Submit**.

Qualifying Virtual SAN Capable Servers

After you create a Virtual SAN qualification policy, perform the following procedure to qualify any Virtual SAN-capable servers.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod for which you want to qualify any Virtual SAN-capable servers.

Step 4 Click **View Details**.

Step 5 Click **Qualification Policies**.

Step 6 Click **Run Qualification Task**.

Step 7 On the **Run Qualification Task** screen, click **Submit**.

The Virtual SAN-qualified servers are added to the server pool.

Viewing Virtual SAN Qualified Servers

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 Expand the pod and then click the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 Click the row with the organization that contains the server pool.
Step 5 Click **View Details**.
Step 6 Click **Server Pools**.
Step 7 Click the row with the server pool to which you have added the qualified Virtual SAN servers.
Step 8 Click **View Details**.
Step 9 Click **UCS Servers** to view all Virtual SAN servers qualified using the Virtual SAN qualification policy.

Adding Virtual SAN Qualified Servers to a Virtual SAN Cluster

After you qualify any Virtual SAN capable servers, you can add the discovered servers to a Virtual SAN cluster.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.
Step 2 On the **Virtual SAN** page, click **Pods**.
Step 3 Click the row with the Virtual SAN pod on which you want to create the Virtual SAN cluster.
Step 4 Click **View Details**.
Step 5 Click **Virtual SAN Clusters**.
Step 6 Click **Create Virtual SAN Cluster**.
Step 7 On the **Create Virtual SAN Cluster** screen, choose **UCS Server Pool** from the **Scope** drop-down menu.
Step 8 Click the **Select** button to select the discovered Virtual SAN qualified servers to add to the Virtual SAN cluster.
Step 9 Complete the fields for the host, data center, cluster details, and RAID mode.

The default RAID mode is JBOD.

Step 10 Click **Submit**.

Viewing Virtual SAN System Tasks

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Choose the row with the Virtual SAN pod for which you want to view the related Virtual SAN system tasks.

Step 4 Click **View Details**.

Step 5 Click **System Tasks**.
All the Virtual SAN system tasks for the accounts associated with the pod are displayed.

What to do next

For more information on executing, enabling, and disabling system tasks, see the Cisco UCS Director Administration Guide.

Viewing Virtual SAN Hardware Topologies

You can view the hardware topology for a Virtual SAN cluster. This topology view displays the connectivity between the cluster, hosts, and VMs.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod associated with the Virtual SAN cluster.

Step 4 Click **View Details**.
All the Virtual SAN clusters associated with the pod are displayed.

Step 5 Click the row with the Virtual SAN cluster.

Step 6 Click **View Details**.

Step 7 Click **Topology**.

Step 8 Click the row with the topology.

Step 9 Click **Sync Topology**, and click **Submit** and **Ok** to refresh the topology report.
The **Sync Status** column displays the current status of the topology sync.

Step 10 Click **View Connectivity**.
The **Topology View - Host VM Mapping** screen displays the Virtual SAN cluster and associated hosts, and the VMs associated with the host.

Step 11 If desired, you can modify the following view options:

- **View Mode** drop down list -- Adjusts the spacing and positioning of the devices. The mode determines which options are available for you to customize the topology view. You can choose between the following view modes:
  - Hierarchical
  - Concentric
  - Circular
  - Force Directed
- **Allow Item Spacing** check box -- Increases the distance between devices for the Hierarchical view mode.

Moving Virtual SAN Hosts to Maintenance Mode

Cisco UCS Director lets you move Virtual SAN hosts to the following maintenance modes:

- Ensure accessibility -- This is the default host maintenance mode. All accessible virtual machines on the host remain accessible when the host is either powered off or removed from the cluster. Partial data migration is performed.
- Full data migration -- This host maintenance mode consumes the most time and resources. VMware Virtual SAN moves all data to other hosts in the cluster and fixes availability compliance for the affected components in the cluster. This option can be used to permanently migrate a host. The host cannot enter maintenance mode if a virtual machine object has data on the host, and is not accessible and cannot be fully migrated. When migrating data from the last host in the cluster, you must make sure that you migrate the virtual machines to another datastore, and then put the host in maintenance mode.
- No data migration -- This host maintenance mode does not migrate any data from the host. If the host is powered off or removed from the cluster, some virtual machines may become inaccessible.

Before you begin

Before you move a Virtual SAN host to maintenance mode, you must note the following:

- All associated virtual machines should be powered off. The task fails if any associated virtual machines are not powered off.
- The task moves all the virtual machines to other hosts in the cluster.
- The virtual machines should migrate storage to other hosts in the cluster. You should verify the data before and after moving the host to maintenance mode.

Procedure

Step 1 On the menu bar, choose **HyperConverged** > **Virtual SAN**.

Step 2 Choose **Hyper Converged** > **Virtual SAN**.

Step 3 On the **Virtual SAN** page, click **Pods**.

Step 4 Click the row with the Virtual SAN pod associated with the Virtual SAN host.

Step 5 Click **View Details**.
All the Virtual SAN clusters associated with the pod are displayed.

Step 6 Click the row with the Virtual SAN cluster that you want to move to maintenance mode.

Step 7 Click **Move Host To Maintenance Mode**.

Step 8 On the **Move Host To Maintenance Mode** screen choose the Host Node, and in the **Maintenance Mode** drop-down menu, choose **Ensure accessibility**, **Full data migration**, or **No data migration**.

Step 9 Click **Submit**.

Decommissioning Virtual SAN Hosts

Cisco UCS Director lets you decommission a Virtual SAN host from a Virtual SAN cluster. The **Decommission Host** action completely removes a host from a cluster by performing the following tasks:

- Puts the Virtual SAN host node into maintenance mode.
- Removes the Virtual SAN host from any associated DV Switch.
- Removes the Virtual SAN host from the Virtual SAN cluster and VMware vCenter.

In the **Decommission Host** screen, you can also select the following decommission options:

- Disassociate UCS Service Profile - This option lets you decommission the Virtual SAN host from the Virtual SAN cluster, and also disassociates the respective UCS Service profile from Cisco UCS Manager.
- Delete UCS Service Profile - This option lets you decommission the Virtual SAN host from the Virtual SAN cluster, and also disassociates and deletes the respective UCS Service profile from Cisco UCS Manager.

Note You cannot decommission a Virtual SAN host from a Virtual SAN cluster that is running with the minimum number of required nodes.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod associated with the Virtual SAN host.

Step 4 Click **View Details**.
All the Virtual SAN clusters associated with the pod are displayed.

Step 5 Click the row with the Virtual SAN cluster from which you want to decommission the Virtual SAN host.

Step 6 Click **View Details**.

Step 7 Click **Hosts**.
All the Virtual SAN hosts associated with the cluster are displayed.

Step 8 Click the row with the Virtual SAN host that you want to decommission from the Virtual SAN cluster.

Step 9 Click **Decommission Host**.

Step 10 On the **Decommission Host** screen, enter the host password and check one of the following options:

- Decommission Host
- Disassociate UCS Service Profile
- Delete UCS Service Profile

Step 11 Click **Submit**.

Decommissioning Virtual SAN Clusters

Cisco UCS Director lets you decommission a Virtual SAN cluster from VMware vCenter. The **Decommission Cluster** action completely removes a Virtual SAN cluster from VMware vCenter by performing the following tasks:

- Turns off the Virtual SAN host.
- Cleans up the Virtual SAN host.
- Removes the Virtual SAN host from any associated DV Switch.
- Deletes any associated DV Switch and DV port group.
- Deregisters the host and removes the Virtual SAN cluster from VMware vCenter.
- Disassociates and deletes any associated UCS service profiles from Cisco UCS Manager.

Note You cannot decommission a Virtual SAN cluster from VMware vCenter if any VMs exist on the Virtual SAN Cluster.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **Pods**.

Step 3 Click the row with the Virtual SAN pod associated with the Virtual SAN cluster that you want to decommission from VMware vCenter.

Step 4 Click **View Details**.
All the Virtual SAN clusters associated with the pod are displayed.

Step 5 Click the row with the Virtual SAN cluster that you want to decommission from VMware vCenter.

Step 6 Click **Decommission Cluster**.

Step 7 On the **Decommission Cluster** screen, enter the host password and check one of the following options:

- Decommission Hosts

- Disassociate UCS Service Profiles
- Delete UCS Service Profiles

Note All of the hosts in the cluster should have the same host password.

Checking **Disassociate UCS Service Profiles** also checks the **Decommission Hosts** option. Checking **Delete UCS Service Profiles** also checks the **Disassociate UCS Service Profiles** and **Decommission Hosts** options.

Step 8 Check **Delete DVSwitch** to delete any associated DV Switch and DV port group.

Step 9 Click **Submit**.

Managing Infrastructure as a Service for Virtual SAN

You can manage all of your Virtual SAN infrastructure resources on the **IaaS** screen. By viewing the details of a Virtual SAN pod, you can manage the following:

- Virtual Machines (VMs)
- Virtual Data Centers (VDCs)
- Catalogs

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **IaaS**.

Step 3 Click the row with the Virtual SAN pod.

Step 4 Click **View Details**.
By default, the **VMs** page appears. You can power on, power off, or view the details of an associated VM. You can also view the VDC and catalog details by clicking **vDC** and **Catalog**. All VM-level actions are supported.

Creating a Virtual SAN Virtual Data Center

You can create a Virtual SAN Virtual Data Center (VDC) that combines Virtual SAN resources, operation details, rules, and policies to manage specific Virtual SAN group requirements. The Virtual SAN VDC creation wizard enables you to configure the policies required to provision Virtual SAN VMs in the private cloud associated with the selected pod.

Before you begin

Ensure that you have added a virtual account in the Virtual SAN pod.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **IaaS**.

Step 3 Click the row with the Virtual SAN pod.

Step 4 Click **View Details**.
By default, the **VMs** page appears. All the VMs associated with the Virtual SAN pod are displayed.

Step 5 Click **vDC**.

Step 6 Click **Virtual SAN vDC Creation Wizard**.

Using the wizard, you can create VDC virtual policies, and configure the service delivery policies. By default, this wizard automatically creates standard VDC compute, network, and storage policies for the Virtual SAN cluster. You can also select an existing or create a new system, computing, and networking policy for the Virtual SAN cluster.

If you check the **Use Linked Clone** check box to use a linked clone, the linked clone is set in the storage policy automatically created for the Virtual SAN vDC.

To edit the policies for your specific needs, choose **Policies** > **Virtual/Hypervisor Policies**.

What to do next

Once you create the Virtual SAN VDC, you can select or modify the VDC.

Creating Virtual SAN Catalogs

You can create a Virtual SAN standard catalog solely for the cloud that is associated with the selected pod. The Virtual SAN **Add Catalog** screen provides the same functionality as the **Add Catalog** screen available under **Policies**, but displays only VMware standard catalogs and it associates the catalog with the selected pod.

For more information on adding a catalog, see the Cisco UCS Director Administration Guide.

Procedure

Step 1 Choose **Hyper Converged** > **Virtual SAN**.

Step 2 On the **Virtual SAN** page, click **IaaS**.

Step 3 Click the row with the Virtual SAN pod.

Step 4 Click **View Details**.
All the VMs associated with the Virtual SAN pod are displayed.

Step 5 Click the **Catalog**.

Step 6 Click **Add**.

Step 7 On the **Basic Information** screen, complete the required fields and click **Next**.

The standard catalog type and cloud name are pre-selected. You can also choose to provision new VMs using an ISO image.

Step 8 On the **Application Details** screen, complete the fields, and click **Next**.

Step 9 On the **User credentials** screen, specify the VM user credential access options, and click **Next**.

Step 10 On the **Customization** screen, specify customization options and custom actions, and click **Next**.

Step 11 On the **VM Access** pane, specify whether end users will have access to the VM, and click **Next**.

Step 12 On the **Summary** pane, review the catalog information and click **Submit**.

What to do next

Once you create the Virtual SAN catalog, you can select the catalog and create a service request or modify the catalog.

Provisioning VMs using Virtual SAN VDC Policies

Once you create a Virtual SAN catalog, you can create a service request to provision VMs on the Virtual SAN cluster using the VDC policies defined for the cluster. The **Create Service** dialog lets you provision VMs based on values specific to the Virtual SAN clusters and VDC policies that are defined at the pod level.

For more information on creating a service request, see the Cisco UCS Director Administration Guide.

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 On the **Service Requests** page, click **Service Requests**.

Step 3 Click **Create Request**.

Step 4 Choose the catalog type, and click **Submit**.

Step 5 On the **Create Service** screen, complete the required fields and choose the Virtual SAN catalog.

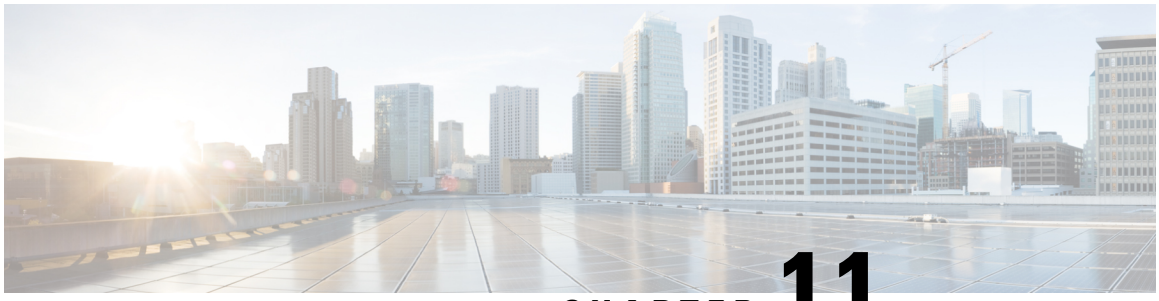
Step 6 Click **Next**.

Step 7 On the **Provisioining Configuration** screen, choose the Virtual SAN VDC and complete the required fields.

Step 8 Click **Next**.

Step 9 Review the summary for the service request.

Step 10 Click **Submit**.



CHAPTER 11

Managing VMware Host Profiles

This chapter contains the following sections:

About VMware Host Profiles

VMware host profiles allow you to take an existing host configuration and overlay it onto your ESX/i servers. They also allow you to determine if a host has changed from its original design and help to ensure that all your hosts are identically configured.

A host profile consists of two parts:

Configuration details

Describes policies that govern how a host configuration should look, including details about each specific configuration setting.

Compliance details

Describes a set of checks that are performed to ensure that the host is configured as specified in the profile.

Configuring Hosts Using Host Profiles in Cisco UCS Director

Cisco UCS Director allows you to configure hosts using host profiles. You can either perform the tasks manually using the steps listed below in the given order, or use predefined orchestration workflow tasks available in the **Task Library**:

Name	Description	Reference	Task name
1. Creating host profiles	A host profile is created by retrieving and encapsulating the configuration of an existing VMware ESX/ESXi host or reference host into a template that can used for configuring other hosts.	Creating Host Profiles, on page 61	**Create Host Profile**
2. Attaching hosts to host profiles	After you create a host profile, you can attach it to one or more hosts.	Attaching Hosts to Host Profiles, on page 61	**Attach Hosts to Host Profile**
3. (Optional) Detaching hosts from host profiles	You may detach hosts from host profiles.	Detaching Hosts from Host Profiles, on page 61	**Detach Host from Host Profile**
4. Applying host profiles	A host profile can be applied to an attached host. When applied, the configuration of the host profile is copied on the attached host.	Applying Host Profiles, on page 62	**Apply Host Profile**

Viewing Host Profile Reports

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, click **Host Profiles**.

Step 3 Click the row with the host profile for which you want to view the details.

These are the host profiles available at the cloud level.

Step 4 Click **View Details**.

Creating Host Profiles

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, click **Host Profiles**.
Step 3 Click **Create**.
Step 4 On the **Create Host Profile** screen, complete the fields.
Step 5 Click **Submit**.

Attaching Hosts to Host Profiles

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **Host Profiles**.
Step 4 Click the row with the host profile to which you want to attach a host.
Step 5 Click **Attach Host to Host Profile**.
Step 6 On the **Attach Host to Host Profile** screen, choose the host that you want to attach to the host profile.
Step 7 Click **Submit**.

Detaching Hosts from Host Profiles

Procedure

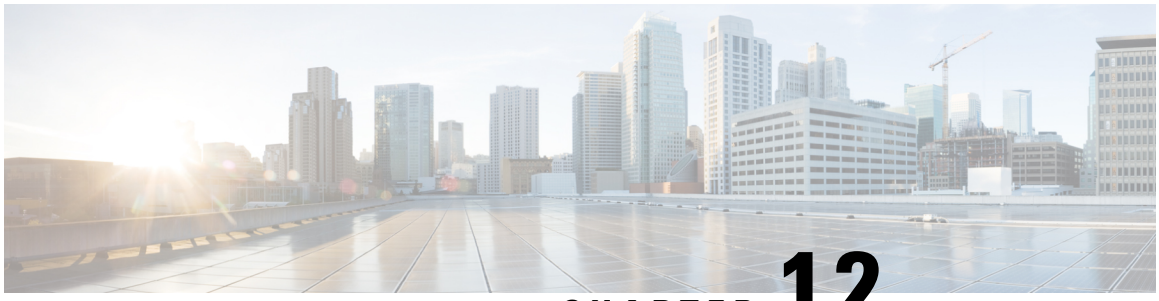
Step 1 On the menu bar, choose **Virtual** > **Compute**.
Step 2 Choose **Virtual** > **Compute**.
Step 3 On the **Compute** page, click **Host Profiles**.
Step 4 On the **Compute** page, click **Host Profiles**.
Step 5 Click the row with the host profile from which you want to detach the host.
Step 6 Click **Detach Host from Host Profile**.
Step 7 On the **Detach Host from Host Profile** screen, choose the host that you want to detach from the host profile.

Step 8 Click **Submit.**

Applying Host Profiles

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **Host Profiles**.
Step 4 Click the row with the host profile that you want to apply.
Step 5 Click **Apply Host Profile**.
Step 6 On the **Apply Host Profile** screen, choose the attached host to which you want to apply the host profile.
Step 7 Click **Submit**.



CHAPTER 12

Managing VMkernel NICs

This chapter contains the following sections:

About VMkernel NICs

The VMware VMkernel networking interface provides network connectivity for the host, and handles VMware vMotion, traffic management, and fault tolerance.

VMware vMotion, lets you migrate powered on virtual machines with no downtime.

See About VMware vMotion and vCenter Storage vMotion, on page 65.

VMware vCenter version 5.5 supports the following VMkernel traffic options:

- vMotion—Enables the VMkernel adapter to advertise itself to another host as the network connection where vMotion traffic is sent. vMotion migration to the selected host is not possible if the vMotion service is not enabled for any VMkernel adapter on the default TCP/IP stack, or if there are no adapters using the vMotion TCP/IP stack.
- Management Traffic—Enables the management traffic for the host and VMware vCenter server. A VMkernel adapter is typically created when the ESXi software is installed. You can create another VMkernel adapter for management traffic on the host to provide redundancy.
- Fault Tolerance—Enables fault tolerance logging on the host. You can use only one VMkernel adapter for fault tolerance traffic per host.
- Virtual SAN Traffic—Enables the Virtual SAN traffic on the host. Every host that is part of a Virtual SAN cluster must have a VMkernel adapter.
- vSphere Replication Traffic—Handles the outgoing replication data that is sent from the source ESXi host to the VMware vSphere replication server.

VMware vCenter versions 6.0 and later support the following VMkernel traffic options, in addition to those supported in version 5.5:

- Provisioning Traffic—Handles the data transferred for virtual machine cold migration, cloning, and snapshot creation.
- vSphere Replication NFC Traffic—Handles the incoming replication data on the target replication site.

You can view the traffic options that are enabled for a VMkernel NIC in the VMKNICs report.

Modifying VMkernel NIC Port Properties

You can modify the port properties of a VMkernel NIC. The VMKNICs report lists the traffic options that are enabled for a VMkernel NIC.

Procedure

Step 1 Choose **Virtual** > **Network**.

Step 2 On the **Network** page, choose the cloud.

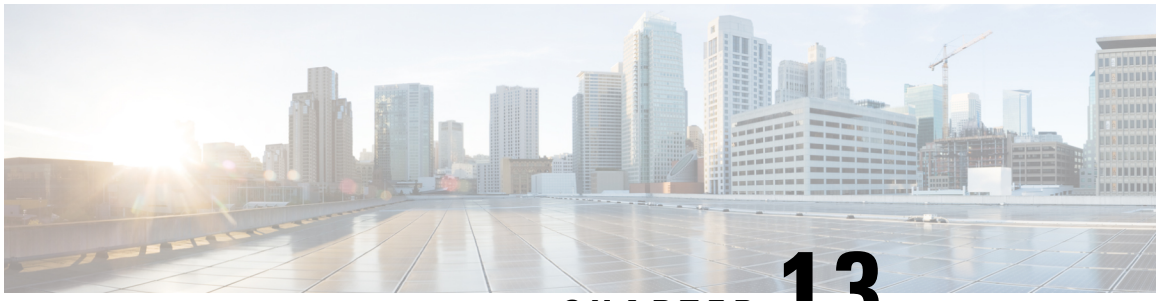
Step 3 On the **Network** page, click **vmkNICs**.

Step 4 Click the row with the VMkernel NIC for which you want to modify the port properties.

Step 5 Click **Modify Port Properties**.

Step 6 On the **Modify Port Properties** screen, click the traffic options that you want to enable on the VMkernel NIC.

Step 7 Click **Submit**.



CHAPTER 13

Managing VMware vMotion

This chapter contains the following sections:

About VMware vMotion and vCenter Storage vMotion

VMware vMotion (vMotion) technology allows users to migrate running virtual machines between compatible physical servers with zero downtime continuous service availability, and complete transaction integrity. The entire state of a VM is encapsulated by a set of files stored on shared storage, and VMware's VMFS cluster file system allows both the source and the target ESX Server to access these VM files concurrently. The active memory and precise execution state of a VM can then be rapidly transmitted over a high-speed network. Since the network is also virtualized by ESX Server, the VM retains its network identity and connections, ensuring a seamless migration process.

With VMware vCenter Storage vMotion (Storage vMotion), a VM and its disk files can be migrated from one datastore to another while the VM is running. These datastores can be on the same or separate storage arrays. The following terms are important for understanding the vMotion technology.

Host

A physical server that is part of the VMware infrastructure hardware resources pool.

Cold migration

Migration of a VM that has been powered off on the source host. The VM is powered on again on the destination host after the transfer of the VM is complete.

Hot migration

Migration of a VM that is powered on. The VM (and applications) previously running on the source host continue execution on the destination host, without being affected by changes, after the hot migration is complete.

You can enable vMotion on a VMkernel NIC using the Modify Port Properties task.

See Modifying VMkernel NIC Port Properties, on page 64.

Migration Options

Based on the running state of the VM, there are small differences in the migrations options available for the user. A *powered-off* VM provides the full range of migration options that can occur simultaneously, whereas a *powered-on* VM is restricted to migrating either the resources or the data in the same job.

Table 2: Migration options

Option	Description	Type	VM State
Change host	Move the VM to another ESX/ESXi host. You can also select and edit the network port group. Network port group modification is supported with VMware vCenter version 6.0 or later.	vMotion	Powered-off (Cold) or Powered-on (Hot)
Change datastore	Move the VM's configuration file and virtual disks.	Storage vMotion	Powered-off (Cold) or Powered-on (Hot)
Change both host and datastore	Move the VM to another ESX/ESXi host and move its configuration file and virtual disks. This option supports cross datacenter migration and lets you migrate the VM to a host with a different subnet.	Combined vMotion and Storage vMotion	Powered-off (Cold) or Powered-on (Hot) Powered-on migration is supported with VMware vSphere version 6.0 or later.

Migration Using the Migrate VM Wizard

You can migrate a VM to a new host node and datastore. You can also modify the source VM network while changing the host node. Follow the steps to execute vMotion or Storage vMotion migration.

Note VM migration is only supported within the same vCenter.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the row with the VM you want to migrate.

Step 5 From the **More Actions** drop-down list, choose **Migrate VM**.

Step 6 On the **Migrate VM** screen, choose the type of migration.

- Change host
- Change datastore
- Change host and datastore

Step 7 Expand **Host Node** or **Datastore** and check the host node or datastore to which you want to migrate the VM.

Step 8 If you are changing the host node, check **Modify Networks** to modify the source VM network.

Step 9 Expand **VM Network Mappings**, click the row with the network adapter that you want to modify, and click the edit icon.

Step 10 On the **Edit VM Network Mappings Entry**, choose the new port group from the **Target Port Group Name** drop-down list.

Step 11 Click **Submit**.

Migration using the Migrate VM Workflow Task

You can add the **Migrate VM** task from the Cisco UCS Director task library to a workflow for migration.

Note The **Migration VM** task supports VM migration for all three options discussed in Migration Options, on page 66.

Procedure

Step 1 Choose **Orchestration**.

Step 2 On the **Orchestration** page, click **Workflows**.

Step 3 Click the row with the workflow.

Step 4 From the **More Actions** drop-down list, choose **Workflow Designer**.

Step 5 Under **Available Tasks**, navigate to the **Virtualization Taks/VMware Tasks/VMware VM Tasks** folder.

Step 6 Drag and drop the **Migrate VM** folder into the **Workflow Designer** screen.

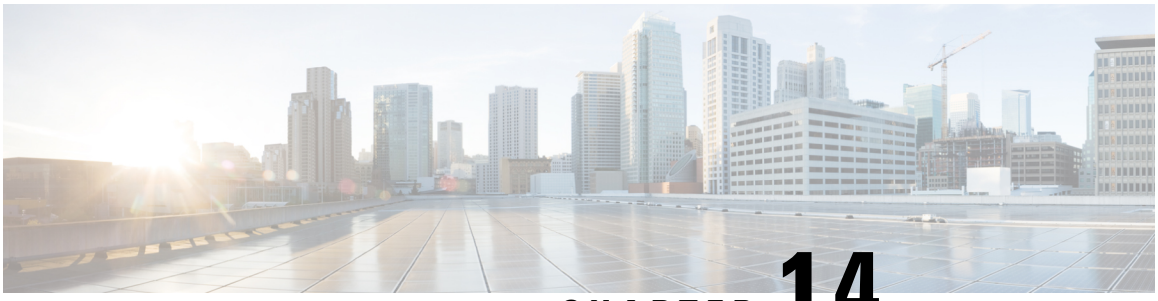
Step 7 On the **Add Task (Migrate VM)** screen, complete the fields for the workflow task basic information.

Step 8 On the **User Input Mapping** screen, choose which of the attributes you would like to use values from the workflow input fields.

Step 9 On the **Task Inputs** screen, choose the values for the task inputs that are not mapped to workflow inputs.

Step 10 On the **User Output Mappings** screen, check the **Map to User Output** check boxes for the task output attributes that you want to use for the workflow outputs.

Step 11 Click **Submit**.



CHAPTER 14

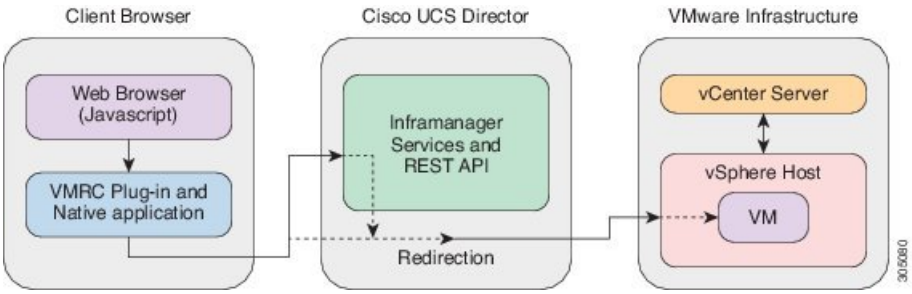
Enabling VMware Remote Console

This chapter contains the following sections:

VMware Remote Console (VMRC)

VMware vSphere contains the VMware Remote Console (VMRC) browser plug-in that can be loaded in supported web browsers. Web applications running in the browser can use the VMRC browser plug-in to access virtual machine console functions by using the VMRC JavaScript API. With a web application that uses the VMRC browser plug-in and the VMRC API, you can remotely access, and interact with, a virtual machine from any system with the appropriate web browser and operating system.

Figure 1: VMRC Topology



Note

- The VMRC console port 903 over TCP should be opened if there is a firewall between the client browser and the ESXi hosts.
- The standalone VMRC plug-in is only supported for system administrators and is not currently supported for end users.

Limitations of Using the VMRC Plug-in with Internet Explorer Browsers

When using the VMRC plug-in with Internet Explore browsers, the following limitations are observed:

- When a VM is accessed from Internet Explorer, the change in connection state is not properly displayed even after the VM is connected.
- When USB devices are connected to or disconnected from the target virtual machine, there is no response that the USB has been connected or disconnected.

This is because the VMRC browser plug-in does not properly handle events for Internet Explorer.

You can also launch a VM client to access the VM console using a standalone VMRC plug-in, if your existing VMRC browser plug-in no longer functions due to a browser update. For more information about using VMRC, refer VMware documentation.

You can also launch a VM client using remote desktop, web access, or the VNC console. For more information on launching a VM client using alternative access schemes, refer Cisco UCS Director Administration Guide.

Enabling VMRC

By default, the VMRC console is disabled for all the discovered VMs in Cisco UCS Director. Below are two ways to enable VMRC:

Name	Description	Reference
Using Catalogs	After you complete the provisioning of a VM using a Catalog that has the VM Console Configuration option enabled, the VM gets access to the VMRC console.	See Using Catalogs for Enabling VMRC, on page 71.
Enabling VM Options	You can enable the **Enable/Disable VMRC Console** option in the VMs interface under **Virtual** > **Compute**.	See Enabling VM Options for VMRC Console Access, on page 71.

After you enable VMRC Console access using any of the above methods, you can launch the VM in the VMRC console. See, Launching a VMRC-enabled Web Browser in Cisco UCS Director, on page 71.

Using Catalogs for Enabling VMRC

Procedure

Step 1 Choose **Policies** > **Catalogs**.
Step 2 Choose the Catalog in which want to enable access for the VMRC console.
Step 3 From the **More Actions** drop-down list, choose **Edit**.
Step 4 Leave the defaults and click **Next** in all the screens in the **Modify Catalog** wizard until you reach the **VM Access** screen.
Step 5 On the **VM Access** screen, under **VMRC Console Configuration** check Enable.
Step 6 Click **Next**.
Step 7 On the **Summary** screen, review the information displayed and click **Submit**.

Enabling VM Options for VMRC Console Access

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, click **VMs**.
Step 3 Click the row with the VM.
Step 4 From the **More Actions** drop-down list, choose **Enable/Disable VMRC Console**.
Step 5 On the **Enable VMRC Console Access** screen, check **Enable VMRC Console**.
Step 6 Click **Submit**.

Launching a VMRC-enabled Web Browser in Cisco UCS Director

Cisco UCS Director enables you to use VMRC, provided that your web browsers have the VMRC plug-in installed.

Note You should be able to access the VM console using VMRC through the Cisco UCS Director GUI if you are able to access the VM through the vSphere Web Client.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, click **VMs**.

Step 3 Click the row with the VM.

Step 4 Click **Launch VM Client**.

Step 5 On the **Launch Client** screen, choose **VMRC Console (Browser Plug-in)** as the access scheme for launching the VM client.

Step 6 Click **Proceed**.

For more information on launching the VM client from other access schemes, see the Cisco UCS Director Administration Guide.

Launching a VMRC Standalone Application from a Web Browser in Cisco UCS Director

Cisco UCS Director enables you to launch a VM client to access the VM console using a standalone VMRC application. The VMRC standalone application option is available only on VMware vCenter versions 5.5 and later.

Note You can use the standalone VRMC application to launch a VM client, if your existing VMRC browser plug-in no longer functions due to a browser update.

The standalone VMRC application is only supported for system administrators and is not currently supported for end users.

Before you begin

Install VMware Remote Console on your local system.

To download and install VMRC on your local system, see www.vmware.com go download-vmrc.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, click **VMs**.

Step 3 Click the row with the VM.

Step 4 Click **Launch VM Client**.

Step 5 On the **Launch Client** screen, choose **VMRC Console (Standalone Plug-in)** as the access scheme for launching the VM client.

Step 6 Click **Proceed**.

Step 7 On the **Launch Application** screen, choose **VMware Remote Console**.

Step 8 Click **OK**.

For more information on launching the VM client from other access schemes, see the Cisco UCS Director Administration Guide.

Launching an HTML5 VMRC Console in Cisco UCS Director

Cisco UCS Director enables you to launch an HTML5 based VMRC console that functions independently of web browser type and does not require a third-party plug-in or additional clients.

Note The HTML5 VMRC SDK is supported with the following versions:

- VMware vCenter version 6.0 or later
- ESxi image profile version 6.0 or later

Before you begin

- Prior to launching the VM from an HTML5 based VMRC console, you must access the VMware vSphere web client URL, such as `https://vCenterIP`, with your browser and accept the self-signed certificate. If you do not accept the self-signed certificate prior to launching the VMRC HTML5 console, an error appears stating that the console has been disconnected.

  Note This is not applicable for VMware vCenters with trusted certificates.

- You must disable VNC.

  After disabling VNC, you must power off and power on the VM before launching the VMRC console.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, click **VMs**.

Step 3 Click the row with the VM.

Step 4 Click **VMRC Console (HTML5)**.

The VM client is launched in a new browser window.

Connecting a USB Device to VMRC

You can connect a USB passthrough device to the VRMC console to access saved VM configuration files.

Note Connecting USB devices is not supported when using VMRC with VMware vCloud Director.

USB device support through the VMRC Console (Browser Plug-in) works only in Firefox.

Before you begin

- You must have a USB controller installed.
- Install a virtual machine remote console browser plug-in before accessing the VMRC console.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, click **VMs**.

Step 3 Click the row with the VM.

Step 4 Click **Launch VM Client**.

Step 5 On the **Launch Client** screen, choose **VMRC Console (Browser Plug-in)** or **VMRC Console (Standalone Plug-in)** as the access scheme for launching the VM client.

Step 6 Click **Proceed**.
The VM client is launched in a new browser window.

Step 7 In the VM client, click **Connect USB Device**.

Step 8 In the **USB Devices** dialog box, select the USB device you want to use from the list of available USB devices.

Step 9 Click **OK**.

Disconnecting a USB Device from VMRC

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, click **VMs**.

Step 3 Click the row with the VM.

Step 4 Click **Launch VM Client**.

Step 5 On the **Launch Client** screen, choose **VMRC Console (Browser Plug-in)** or **VMRC Console (Standalone Plug-in)** as the access scheme for launching the VM client.

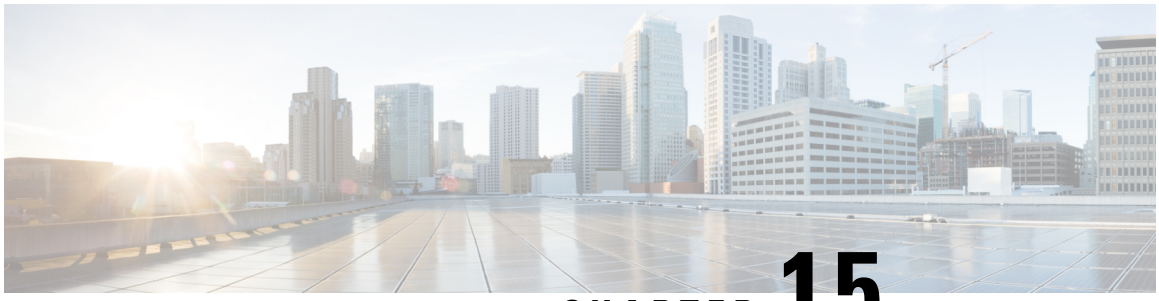
Step 6 Click **Proceed**.

The VM client is launched in a new browser window.

Step 7 In the VM client, click **Disconnect USB Device**.

Step 8 In the **USB Devices** dialog box, uncheck the selected the USB device that you want to disconnect.

Step 9 Click **OK**.



CHAPTER 15

Managing VMware Distributed Resource Scheduler

This chapter contains the following sections:

About VMware Distributed Resource Scheduler

VMware Distributed Resource Scheduler (DRS) is a utility that balances computing workloads with available resources in a virtualized environment. DRS dynamically allocates the available resources among VMs based on predefined rules called VM affinity rules. These rules are defined at the cluster level. When a VM experiences an increased load, DRS automatically allocates additional resources by redistributing VMs among the physical servers in the resource pool. In addition to VM affinity rules, the placement of VMs across the cluster is based on vMotion compatibility. vMotion has its own set of requirements to move the VMs across the hosts. For example, if a VM that has a local network (not connected to any physical adapter), it cannot be moved using VMotion.

Using DRS Affinity Rules

You can control the placement of virtual machines on hosts within a cluster by using affinity rules.

Affinity rules

An affinity rule defines a set of VMs that should run on the same host. This rule helps to keep the VMs together under a single host that is compatible within the cluster.

Anti-affinity rules

An anti-affinity rule defines a set of VMs that should run on different hosts. This rule helps to separate the VMs and make sure that they are not under a single host.

VM-Host Rules

A VM-Host rule defines affinity and anti-affinity relationships between VMs and hosts. This rule helps to either keep or separate the VMs as a group.

Viewing DRS Rules

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, click **Clusters**.
Step 3 Double-click the cluster.
Step 4 Click **DRS Rules**.

Adding DRS Rules

Procedure

Step 1 On the menu bar, choose**Virtual** > **Compute**.
Step 2 Choose **Virtual** > **Compute**.
Step 3 On the **Compute** page, click **Clusters**.
Step 4 Double-click the cluster.
Step 5 Click **DRS Rules**.
Step 6 Click **Add**.
Step 7 On the **Add Rule** screen, complete the fields, including the following:
a) Choose the type of rule. You can choose **Keep Virtual Machines Together** to add an affinity rule, **Separate Virtual Machines** to add an anti-affinity rule, or **Virtual Machines to hosts** to add a VM-Host affinity rule.
Step 8 Click **Submit**.

Enabling or Disabling DRS

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, click **Clusters**.
Step 3 Click the row with the cluster on which you want to enable or disable DRS.

Step 4 From the **More Actions** drop-down list, choose **Enable/Disable DRS**.

Step 5 On the **Enable/Disable DRS** screen, check **Enable DRS** or **Disable DRS**, and choose the type of DRS automation level, if applicable.

Step 6 Click **Submit**.

Using DRS Automation Levels

After you create a DRS cluster, you can customize the automation level for individual VMs to override the cluster's default automation level. The automation level can be set to any one of the following:

- Manual -- A DRS-enabled cluster set to manual will make recommendations to the administrator but will take no action. It is the administrator's responsibility to review and execute the recommendation.
- Partially automated -- When the VMs are powered-on, they are automatically placed on the DRS-recommended hosts. VM migrations caused by resource imbalance will be recommended by DRS but won't be moved automatically
- Fully automated -- DRS automatically places the VM on the DRS-recommended hosts during power-on and also during resource imbalance.

Editing DRS Automation Level

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, click **Clusters**.

Step 3 Click the row with the cluster on which want to enable or disable DRS.

Step 4 From the **More Actions** drop-down list, choose **Edit DRS Automation Level**.

Step 5 On the **Edit DRS Automation Level** screen, choose the type of DRS automation level.

Step 6 Click **Submit**.

About DRS Group Manager

The DRS Group Manager feature in Cisco UCS Director allows you to group a set of VMs or Hosts for bulk migration. These groups can be used when the VM-Host affinity rules are applied.

Using DRS Group Manager

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, click **Clusters**.
Step 3 Double-click the cluster.
Step 4 Click **DRS Group Manager**.
Step 5 Click **Add**.
Step 6 On the **Add Group** screen, complete the fields to group a set of VMs or hosts.
Step 7 Click **Submit**.

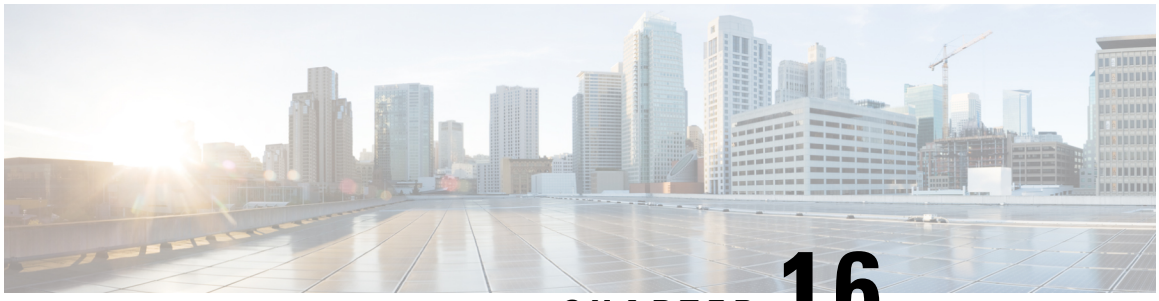
About Mapping VM Affinity Rules

In Cisco UCS Director, DRS rules can be included as part of computing policies. When you create a computing policy, you can choose to map VM affinity rules. After the computing policy is created with the VM affinity rules mapped, a VM being provisioned with the computing policy will be added using that set of VM affinity rules.

Mapping VM Affinity Rules

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Computing**.
Step 2 On the **Computing** page, click **VMware Computing Policy**.
Step 3 Click the row with the computing policy that you want to edit.
Step 4 Click **Edit**.
Step 5 On the **Edit Computing Policy** screen, complete the following fields:
a) In the **Host Node/Cluster Scope** drop-down list, choose the **Include Selected Clusters** option.
b) Select the clusters to which you want to apply the policy.
c) Check **Map VM Affinity Rules** to map VM affinity rules.
d) Optionally, choose the affinity rules to which the VM has to be mapped after provisioning.
Step 6 Click **Submit**.



CHAPTER 16

Managing VM Annotations

This chapter contains the following sections:

About VM Annotations

Annotations are a part of the VM summary that is used to describe a virrtual machine. An annotation consists of notes and Custom attributes. Custom attributes can be of the following two types:

- Virtual machine -- This is a custom attribute that can be applied to all the VMs in the inventory.
- Global -- This is a custom attribute that can be applied to all VMs and hosts in the inventory.

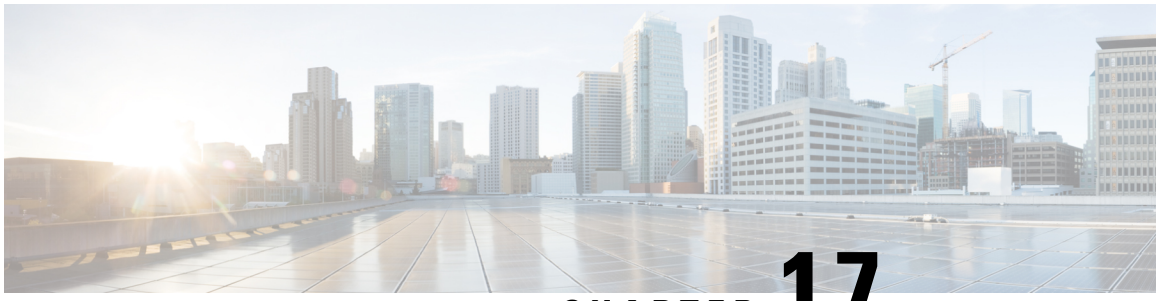
Cisco UCS Director allows you to customize the annotations of a virtual machine during VM provisioning.

Defining VM Annotations

Procedure

Step 1	Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.
Step 2	On the **Service Delivery** page, click **VMware System Policy**.
Step 3	Click the row with the policy for which you want VM annotations to be defined.
Step 4	Click **Edit**.
Step 5	On the **System Policy Information** screen, complete the fields to define VM annotations and add custom attributes.
Step 6	Click **Submit**.

Once you define annotations using this procedure, the values are saved in the VMware System Policy.



CHAPTER 17

Managing VMware vCenter Site Recovery Manager

This chapter contains the following sections:

About VMware vCenter Site Recovery Manager

VMware vCenter Site Recovery Manager (SRM) is a business continuity and disaster recovery solution that helps you to plan, test, and run the recovery of virtual machines between a protected vCenter Server site and a recovery vCenter Server site. The following terms are important for fully understanding SRM technology.

Array-based replication (ABR)

Replication of virtual machines that is managed and executed by the storage subsystem itself, rather than from inside the virtual machines, the vmkernel or the Service Console.

Failback

Reversal of direction of replication, and automatic reprotection of protection groups.

Failover

Event that occurs when the recovery site takes over operation in place of the protected site after the declaration of a disaster.

Protection group

A group of virtual machines that will be failed over together to the recovery site during testing or recovery.

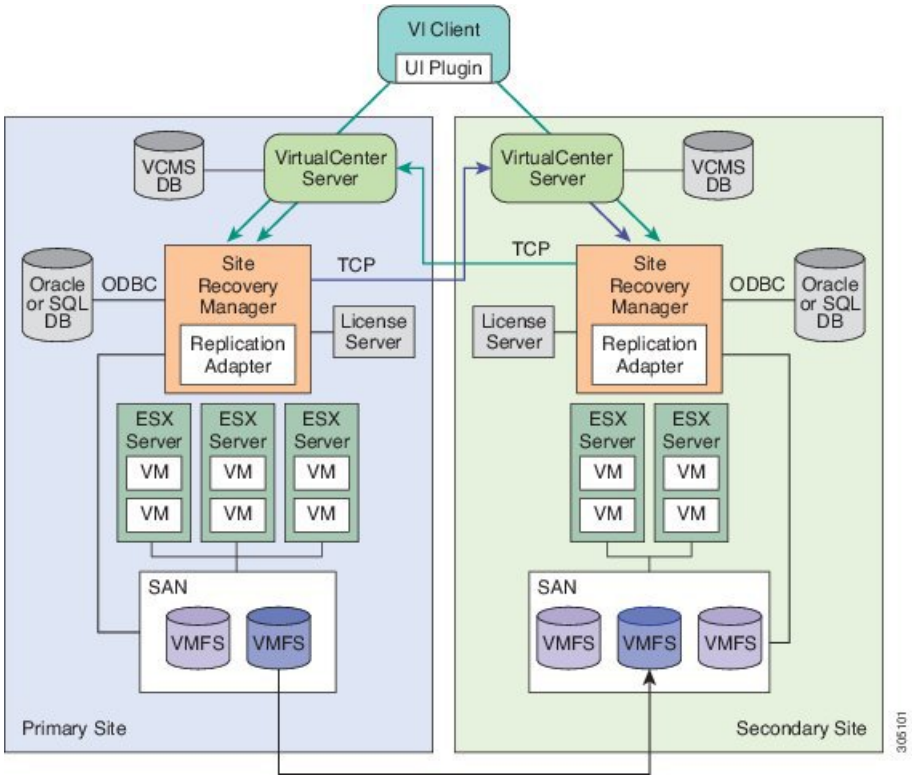
Protected site

The primary site that contains the virtual machines to be protected.

Recovery site

The secondary site to which virtual machines will fail over.

Figure 2: SRM Architecture



Overview of SRM Configuration

Configuring SRM after installation on the protected and recovery site involves the following steps:

1. Configure array managers in SRM: Array managers are identities of the storage systems at both the protected and recovery sites. Once SRM is installed, it interrogates the array managers and discovers which datastores have been marked for replication.
2. Define inventory mappings: Inventory mappings build a relationship between the folders, resource pools and networks between the protected site and recovery site. These mappings ensure that VMs are recovered to the correct location in the vCenter environment.
3. Create protection groups: Protection Groups are pointers to the replicated vSphere datastores that contain collections of virtual machines that will be failed over from the protected site to the recovery site.
4. Create recovery plans: A recovery plan is like an automated runbook. It controls every step of the recovery process, including the order in which virtual machines are powered off or powered on, the network addresses that recovered virtual machines use, and so on. A recovery plan applies to one or more protection groups. The protection groups use the inventory mappings to determine the location of placeholder VMs. These placeholder VMs are used in Recovery Plans to indicate when and where they should be recovered and allows for advanced features such as VM dependencies and scripting callouts.

Integrating SRM with Cisco UCS Director

The integration of SRM with Cisco UCS Director involves discovering and enabling the existing SRM environment in Cisco UCS Director. The various interlinked components in the SRM environment, such as inventory mappings, protection groups, and recovery plans, need to be identified and enabled in Cisco UCS Director. Identifying and enabling these components allows for the seamless communication between the primary site and recovery site when a disaster occurs.

Cisco UCS Director integration with the SRM API lets you create protection groups and initiate test, recovery, reprotect, or revert operations and collect the results. You can create a protection group, protect a VM, unprotect a VM, and add a protection group to a recovery plan using orchestration workflow tasks.

Prerequisites for Integrating SRM

Ensure that the following prerequisites are met prior to integrating SRM with Cisco UCS Director:

- Inventory mappings between protected and recovery sites, specifically resource pools, folders and networks have been configured.

  You can create folder, resource pool, and network mappings using Cisco UCS Director workflow tasks.

- Protection groups for the protected site have been created.

Note Currently, you can configure SRM to work with Cisco UCS Director by configuring array-based replication. Array-based replication surfaces replicated datastores to recover virtual machine workloads.

- A recovery plan has been created on the recovery site.

Enabling SRM in Cisco UCS Director

The following table describes the process of enabling SRM in Cisco UCS Director. Prior to completing the tasks below, ensure that the prerequisites are met. See Prerequisites for Integrating SRM, on page 85.

Task	Description
Add an SRM account	See Adding an SRM Account, on page 86.
Enable Resource Pool Mappings	Enable the resource pool mappings between protected and recovery sites in Cisco UCS Director. See Enabling Resource Pool and Folder Mappings, on page 87.
Enable Folder Mappings	Enable the folder mappings between protected and recovery sites in Cisco UCS Director. See Enabling Resource Pool and Folder Mappings, on page 87.

Task	Description
Enable Network Mappings	Enable the network mappings between protected and recovery sites in Cisco UCS Director. See Enabling Network Mappings, on page 88.
Enable Protection Groups	Enable the protected groups created in the protected site in Cisco UCS Director. See Mapping Datastores, on page 89.
Enable policies in the Virtual Datacenter (VDC)	Enable policies (computing, network and storage) in the VDC. See Enabling Policies in VDC, on page 90.

Adding an SRM Account

Before you begin

Ensure that the protection and recovery sites are configured properly.

Procedure

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 On the **Virtual Accounts** page, click **Virtual Accounts**.

Step 3 Click **Add**.

Step 4 On the **Add Cloud** screen, choose VMware as the cloud type and complete the required fields.

Step 5 In the **Cloud Name** field, enter the name for the cloud.

Each cloud requires a unique name in Cisco UCS Director. The name cannot include single quotes. Once a cloud has been added, all reports refer to the cloud using the Cloud Name.

Step 6 Choose one of the following options to specify the VMware datacenter and/or VMware cluster:

a) Check **Use Credential Policy** and select a credential policy that includes an associated VMware datacenter.

b) In the **VMware Datacenter** field, enter the data center name on the vCenter account and in the **VMware Cluster** field, enter the cluster name.

The VMware datacenter name allows you to discover, monitor, and manage the specified pod's resources. Leave the field blank if the entire vCenter account is managed by Cisco UCS Director.

When you enter a cluster name, the vCenter account displays data center cluster-level information.

c) Check **Discover Datacenters / Clusters** to discover and use any VMware datacenters and associated VMware clusters. Any associated datacenters and clusters are displayed in the **Select Datacenters / Clusters** field.

Note Either a datacenter within the credential policy or the VMware datacenter and VMware cluster can be selected. Specifying the datacenter on the **Add Cloud** screen as well as in the credential policy form results in an error.

Step 7 Check **Enable SRM**.

Step 8 Choose the converged infrastructure pod from the **Pod** drop-down list.

When you choose a pod name, the VMware cloud account appears in the converged infrastructure stack.

Step 9 Click **Add**.

Enabling Resource Pool and Folder Mappings

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Computing**.

Step 2 On the **Computing** page, click **VMware Computing Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Computing Policy** screen, complete the fields, including the following:

a) In the **Policy Name** field, enter the name of the policy.

This name is used during catalog definition.

b) In the **Host Node/Cluster Scope** drop-down list, choose the scope of deployment.

Note You can narrow the scope of deployment by specifying whether to use all, include chosen, or exclude chosen options. Depending on the choices, a new field appears where the required hosts or clusters can be chosen.

c) In the **Filter Conditions** field, check the boxes for one or more conditions that the hosts should match.

Any hosts that do not meet these criteria are excluded from consideration. If more than one condition is chosen, all of the chosen conditions must match.

d) Check **Override Template** to override the template properties.

You are provided with options to enter custom settings for CPU and memory. The specified number of vCPUs for a VM should not exceed the total cores for the chosen scope of host nodes or clusters. The CPU reservation for the VM depends upon the number of vCPUs specified. The CPU limit is based on the chosen scope of host nodes or clusters. The CPU shares determine which VM gets CPU resources when there is competition among VMs.

e) Check **Allow Resizing of VM** to allow VM resizing before provisioning, or to resize an existing VM.

You are provided with options to enter custom settings for CPU and memory. The **Permitted Values for vCPUs** field is the range of vCPUs to use while provisioning a VM or resizing an existing VM. A range of more than 8 is visible during VM provisioning or resizing, only if the chosen cloud (vCenter) is 5 or above and has VM version 8. Only the values specified in the box are visible.

The **Permitted Values for Memory in MB** field is the range of memory to use while provisioning a VM or resizing an existing VM. For example: 512, 768, 1024, 1536, 2048, 3072, 4096, and so on. Only the values specified in the box are visible.

The VMs created using this policy can be deployed into a custom folder. Cisco UCS Director allows automatic creation of folder names from group names or from the available Macro provided by Cisco UCS Director.

For more information, see the Cisco UCS Director Orchestration Guide.

By specifying ${GROUP_NAME}, folders are created from the group name that uses this policy. You can specify a new or existing folder name.

If the **Enable protection** option is checked, only the folders that are mapped to the recovery site are listed in the drop-down folder.

Step 5 Click **Submit**.

Enabling Network Mappings

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.

Step 2 On the **Network** page, click **VMware Network Policy**.

Step 3 Click **Add**.

Step 4 On the **Network Policy Information** screen, complete the fields.

Step 5 Click **Add** in the VM Networks section to add and configure multiple vNICs. These vNICs are applicable to the VM that is provisioned using this policy.

Note To add or replace vNICs for provisioned or discovered VMs using VM actions, you must configure the vNICs.

Step 6 On the **Add Entry to VM Networks** screen, complete the fields, including the following:

a) If **Allow end user to select optional NICs** in the **Network Policy** dialog box is checked, the **Mandatory** check box is pre-selected. If the **Network Policy** dialog box was not selected, and **Allow end user to select optional NICs** is not checked, then the **NIC Alias** field is optional.

Note At least one of the NICs should have the **Mandatory** option selected. The NICs that have the **Mandatory** field selected are used in VM provisioning, and you will not have the option to select the NIC during VM service request creation.

b) In the **Adapter Type** drop-down list, choose the adapter type.

Note This option is not visible if the **Copy Adapter from Template** option is chosen.

Step 7 Click **Add (+)** in the **Port Groups** section. The **Add Entry to Port Groups** screen displays.

Step 8 Click **Select** to choose the port group name.

Note All the port groups mapped in the protection site to the corresponding recovery site are displayed here.

Step 9 From the **Select IP Address Type** drop-down field, choose **DHCP** (default) or **Static**.

a) If you choose **Static**, the **Select IP Address Source** drop-down field appears. Choose **IP Pool Policy** (default) or **Inline IP Pool**.

If you choose IP Pool Policy, the **Static IP Pool** field appears. In the **Select** dialog box, choose from the list of preconfigured static IP pool(s). If no preconfigured static IP pools exist, see the Adding a Static IP Policy topic in the Cisco UCS Director Administration Guide.

b) If you choose **Inline IP Pool**, complete the fields.

Step 10 Click **Submit**.

Step 11 Click **Submit** on the **Add Entry to VM Networks** screen.

Step 12 Click **Submit** on the **Network Policy Information** screen.

Viewing SRM Protection Group Reports

You can view the collected inventory for SRM resource mappings, protection groups, and recovery plans.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **SRM Sites**.

Step 4 Click the row with the SRM site.

Step 5 Click **View Details** to see the details of the SRM site.

Step 6 Click **Protection Groups**.

Step 7 Click the row with the protection group.

Step 8 Click **View Details** to see the details of the SRM protection group.

By default, the **Unassigned Replicated VMs** page appears. You can also view the associated datastores, VMs, and recovery plans by clicking **Datastores**, **VMs**, or **Recovery Plans**.

Mapping Datastores

SRM protection groups let you group VMs to fail over from the protected site to the recovery site together as part of your recovery plan. You can enable protection groups when creating a new SRM storage policy, or when editing an existing SRM storage policy. The available datastores that you can map to your SRM storage policy is filtered based on the selected protection group. The recovery site VMs are provisioned on the selected protection group datastore.

For more information on adding a storage policy, see the Cisco UCS Director Administration Guide.

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Storage**.

Step 2 On the **Storage** page, click **VMware Storage Policy**.

Step 3 Do one of the following:

- Click **Add**.
- Choose the SRM storage policy on which you want to enable protection groups and click **Edit**.

Step 4 On the **Add Storage Resource Allocation Policy** screen, check **Enable Protection**.

Note If you are adding a new SRM storage policy, you must select an SRM cloud from the **Cloud Name** drop-down list for this option to appear.

Step 5 In the **Protection Group** field, click **Select**.

Step 6 Check the protection groups that you want to add to the storage policy, and click **Select**.

Step 7 On the **System Disk Policy** screen, if necessary, complete the required fields, and click **Next**.

Step 8 On the **Additional Disk Policies** screen, if necessary, configure a disk policy, and click **Next**.

Step 9 On the **Hard Disk Policy** screen, if necessary, specify the number of physical disks that you want to create during VM provisioning.

Step 10 Click **Submit**.

Enabling Policies in VDC

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Virtual Data Centers**.

Step 2 On the **Virtual Data Centers** page, click **vDC**.

Step 3 Click **Add**.

Step 4 On the **Add VDC** screen, select the cloud type, and click **Submit**.

Step 5 On the **Add VDC** screen, complete the fields, including:

a) Check **VDC Locked** to deny the use of the VDC for any further deployments.

Actions on existing VMs, within this VDC, are disabled. Uncheck **VDC Locked** to allow the use of the VDC for further deployments.

b) Check **Enable Protection** to enable protection.

If checked, all the policies for this account (compute, storage and network) that have SRM enabled are displayed here.

c) In the **User Action Policy** drop-down list, choose the policy that is used for execution of orchestration workflow post-provisioning of the VMs.

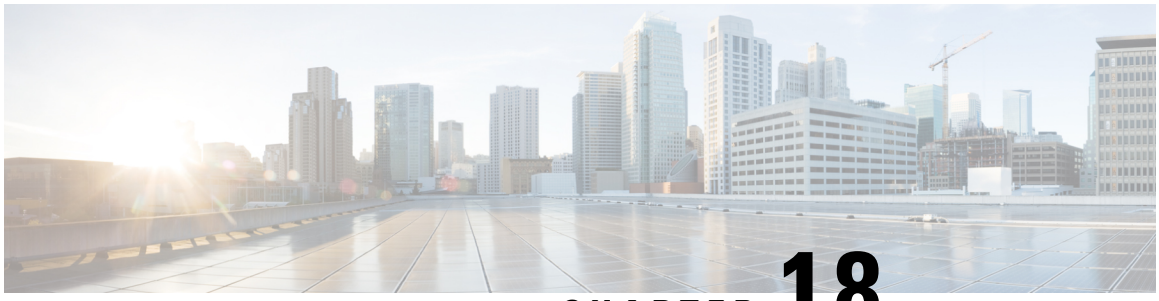
The chosen workflow appears as an action button for VMs within the VDC.

d) In the **Delete after Inactive VM days** drop-down list, choose the number of days to wait before deleting an inactive VM.

A VM that is in the inactive state is not powered-on.

Note Ensure that **Delete Inactive VMs Based on VDC Policy** is checked on the **Advanced Controls** screen under **Administration > System** for this choice to work as expected. For more information, see Enabling Advanced Controls.

Step 6 Click **Add**.



CHAPTER 18

Managing Cisco Virtual Machine Fabric Extender For VMware

This chapter contains the following sections:

About Cisco Virtual Machine Fabric Extender

A virtualized server implementation consists of one or more VMs that run as guests on a single physical server. The guest VMs are hosted and managed by a software layer called the hypervisor or virtual machine manager (VMM). Typically, the hypervisor presents a virtual network interface to each VM and performs Layer 2 switching of traffic from a VM to other local VMs or to another interface to the external network.

Working with a Cisco virtual interface card (VIC) adapter, the Cisco Virtual Machine Fabric Extender (VM-FEX) bypasses software-based switching of VM traffic by the hypervisor for external hardware-based switching in the fabric interconnect. This method reduces the load on the server CPU, provides faster switching, and enables you to apply a rich set of network management features to local and remote traffic.

Integrating Cisco VM-FEX in Cisco UCS Director

To successfully integrate Cisco VM-FEX in Cisco UCS Director, complete the tasks outlined in the table below:

Task	Description	Reference
Edit computing policy	To enable DirectPath I/O, full guest memory reservation is necessary on the VM. This can be achieved by editing the VM's computing policy.	Editing Computing Policy For Cisco VM-FEX Support, on page 94

Task	Description	Reference
Edit networking policy	The adapter type must be VMXNET3 and should be associated with the VM's DirectPath enabled portgroup.	Editing Network Policy For VM-FEX Support, on page 94

Editing Computing Policy For Cisco VM-FEX Support

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Computing**.

Step 2 On the **Computing** page, click **VMware Computing Policy**.

Step 3 Click the row with the policy that you want to edit.

Step 4 Click **Edit**.

Step 5 On the **Edit Computing Policy** screen, check **Override Template** and **Reserve all guest memory**, and specify the reserved guest memory.

Note The reserved guest memory should always be greater than 4096MB.

Step 6 Click **Submit**.

Editing Network Policy For VM-FEX Support

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.

Step 2 On the **Network** page, click **VMware Network Policy**.

Step 3 Click the row with the policy that you want to edit.

Step 4 Click **Edit**.

Step 5 On the **Network Policy Information** screen, click the + icon next to **VM Networks**.

Step 6 Click the + icon to add a new entry to the VM Networks table.

Step 7 On the **Add Entry to VM Networks** screen, choose **VMXNET3** in the **Adapter Type** drop-down list.

Step 8 Click the row with the portgroup that you want to add.

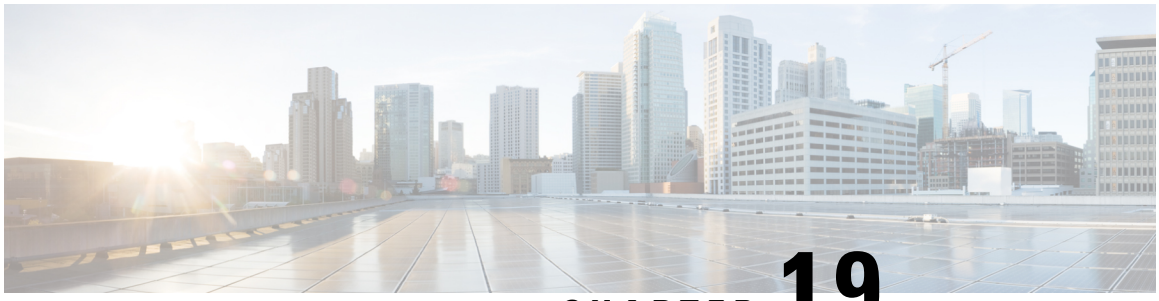
Step 9 Click the **Edit** icon.

Step 10 On the **Add Entry to Port Groups** screen, choose the VM DirectPath enabled portgroup.

Step 11 Click **Submit**.

Step 12 In the **Add VM Networks Entry** screen, click **Submit**.

Step 13 In the **Network Policy Information** screen, click **Submit**.



CHAPTER 19

Appendix

This chapter contains the following sections:

About Virtual SAN UCS Service Profile Templates

Cisco UCS Director VMware Virtual SAN implementation with UCS servers requires a standard configuration of a UCS service profile template. Cisco UCS Director workflows use the template to create service profiles with Virtual SAN specific configurations. You must make sure that the template follows the guidelines listed below.

Note Cisco UCS with VMware Virtual SAN implementation requires initiating a UCS service profile template, and it does not support updating an existing UCS service profile template.

When creating a Virtual SAN UCS service profile template, the template should not be associated with any server pool. You can select the **Assign Later** option in the server pool template, to assign the server pool to the Virtual SAN service profile.

In addition to any guidelines or recommendations that are specific to policies and pools included in service profiles and UCS service profile templates, you need to be aware of the following requirements for creating a Virtual SAN UCS service profile template.

- BIOS policy requirements
- Network configuration requirements
- Boot policy requirements
- Local disk configuration policy requirements

For an overview of requirements for setting up a Virtual SAN UCS service profile template, see Prerequisites for Creating a Virtual SAN from a Bare Metal Server, on page 40.

For more information on creating Cisco UCS Manager service profile templates, see the Cisco UCS Manager GUI Configuration Guide.

Creating Virtual SAN UCS Service Profile Templates

Summary of Steps for Setting Virtual SAN Cisco UCS Manager Service Profile Template, Network, and Policy requirements

This procedure provides a high-level summary of the steps involved to satisfy the network configuration requirements, LAN boot policy requirements, and scrub policy requirements for setting up a Virtual SAN UCS service profile template.

Note The following procedures explain only how to kick-start templates for a Virtual SAN configuration. The steps are generic and will vary depending on your Cisco UCS Manager configuration. If any option is unavailable, refer to the Cisco UCS Manager GUI for the specific Cisco UCS Manager version.

Procedure

Step 1 Define UUID suffix pools as described in Creating a UUID Suffix Pool, on page 98.

Step 2 Define MAC address pools as described in Creating a MAC Pool, on page 99.

Step 3 Define a multicast policy as described in Creating a Multicast Policy, on page 100.

Step 4 Define VLANs as described in Creating a Named VLAN, on page 100.

Step 5 Create a vNIC template with the VLANs defined as described in Creating a vNIC Template, on page 101.

Step 6 Create a QoS policy as described in Creating a QoS Policy, on page 102.

Step 7 Create and define a vNIC from the template as described in Creating a vNIC for a LAN Connectivity Policy, on page 102.

Step 8 Create a boot policy as described in Creating a Boot Policy, on page 103.

Step 9 Create a local disk configuration policy as described in Creating a Local Disk Configuration Policy, on page 104.

Step 10 Create a BIOS policy as described in Creating a BIOS Policy, on page 105.

Creating a UUID Suffix Pool

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Pools**.

Step 3 Expand the node for the organization where you want to create the pool.

If the system does not include multitenancy, expand the **root** node.

Step 4 Right-click **UUID Suffix Pools** and select **Create UUID Suffix Pool**.

Step 5 In the **Define Name and Description** page of the **Create UUID Suffix Pool** wizard, complete the required fields.

Step 6 Click **Next**.

Step 7 In the **Add UUID Blocks** page of the **Create UUID Suffix Pool** wizard, click **Add**.

Step 8 In the **Create a Block of UUID Suffixes** dialog box, complete the required fields.

Step 9 Click **OK**.

Step 10 Click **Finish** to complete the wizard.

What to do next

Include the UUID suffix pool in a service profile and/or template.

Creating a MAC Pool

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Pools**.

Step 3 Expand the node for the organization where you want to create the pool.

If the system does not include multitenancy, expand the **root** node.

Step 4 Right-click **MAC Pools** and select **Create MAC Pool**.

Step 5 In the **Define Name and Description** page of the **Create MAC Pool** wizard, complete the required fields.

Step 6 Click **Next**.

Step 7 In the **Add MAC Addresses** page of the **Create MAC Pool** wizard, click **Add**.

Step 8 In the **Create a Block of MAC Addresses** dialog box, complete the required fields.

Step 9 Click **OK**.

Step 10 Click **Finish**.

What to do next

Include the MAC pool in a vNIC template.

Creating a Multicast Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies**.

Step 3 Expand the **root** node.

Step 4 Right-click the **Multicast Policies** node and select **Create Multicast Policy**.

Step 5 In the **Create Multicast Policy** dialog box, specify the name and IGMP snooping information.

For a Virtual SAN UCS service profile template, you must click the **Enabled** radio buttons in the **IGMP Snooping State** and **IGMP Snooping Querier State** fields. The **IGMP Snooping Querier IPv4 Address** must be the same subnet as the Cisco UCS Manager subnet.

Step 6 Click **OK**.

What to do next

Specify the multicast policy for the Virtual SAN VLAN.

Creating a Named VLAN

In a Cisco UCS domain that is configured for high availability, you can create a named VLAN that is accessible to both fabric interconnects or to only one fabric interconnect.

Important You cannot create VLANs with IDs from 4030 to 4047. This range of VLAN IDs is reserved.

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 On the **LAN** tab, click the **LAN** node.

Step 3 In the **Work** pane, click the **VLANs** tab.

Step 4 On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create VLANs** dialog box, complete the required fields.

Step 6 If you clicked the **Check Overlap** button, do the following:

a) Click the **Overlapping VLANs** tab and review the fields to verify that the VLAN ID does not overlap with any IDs assigned to existing VLANs.

b) Click the **Overlapping VSANs** tab and review the fields to verify that the VLAN ID does not overlap with any FCoE VLAN IDs assigned to existing VSANs.

c) Click **OK**.

d) If Cisco UCS Manager identified any overlapping VLAN IDs or FCoE VLAN IDs, change the VLAN ID to one that does not overlap with an existing VLAN.

Step 7 Click **OK**.

Cisco UCS Manager adds the VLAN to one of the following **VLANs** nodes:

- The **LAN Cloud** > **VLANs** node for a VLAN accessible to both fabric interconnects.
- The ***Fabric_Interconnect_Name*** > **VLANs** node for a VLAN accessible to only one fabric interconnect.

What to do next

Specify the previously created multicast policy name in the **Properties** area of the Virtual SAN VLAN **General** tab.

Creating a vNIC Template

Before you begin

This policy requires that one or more of the following resources already exist in the system:

- Named VLAN
- MAC pool
- QoS policy
- LAN pin group
- Statistics threshold policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multitenancy, expand the **root** node.

Step 4 Right-click the **vNIC Templates** node and choose **Create vNIC Template**.

Step 5 In the **Create vNIC Template** dialog box, complete the required fields.

You must create two templates, specifying A and B fabrics, as your vNICs will be on separate fabrics for failover redundancy.

Step 6 Check the **Enable Failover** checkbox.

Step 7 In the **VLANs** area, use the table to select the VLANs to assign to vNICs created from this template.

Step 8 In the **Policies** area, enter an integer between 1500 and 9000 for the **MTU** field.

The MTU size must be set to 9000 for a jumbo frames network.

Step 9 Click **OK**.

What to do next

Include the vNIC template in a service profile.

Creating a QoS Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 In the **LAN** tab, expand **LAN** > **Policies**.

Step 3 Expand the node for the organization where you want to create the pool.

If the system does not include multitenancy, expand the **root** node.

Step 4 Right-click **QoS Policy** and select **Create QoS Policy**.

Step 5 In the **Create QoS Policy** dialog box, complete the required fields.

Step 6 Click **OK**.

What to do next

Include the QoS policy in a vNIC or vHBA template.

Creating a vNIC for a LAN Connectivity Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies** > *Organization_Name*.

Step 3 Expand the **LAN Connectivity Policies** node.

Step 4 Choose the policy to which you want to add a vNIC.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 On the icon bar of the **vNICs** table, click **Add**.

Step 7 In the **Create vNIC** dialog box, enter the name, select a **MAC Address Assignment**, and check the **Use vNIC Template** check box to use one the previously created vNIC templates.

Step 8 In the Adapter Performance Profile area, choose **VMware** from the **Adapter Policy** drop-down menu.

Step 9 Click **OK**.

Step 10 Click **Save Changes**.

What to do next

Create a total of three vNICs, two of which are on a separate fabric to provide failover redundancy.

Creating a Boot Policy

You can also create a local boot policy that is restricted to a service profile or service profile template. However, Cisco recommends that you create a global boot policy that can be included in multiple service profiles or service profile templates.

Cisco UCS Director Virtual SAN workflows support installing ESXi with an SD card. You must define a boot policy with an SD card specified as the first boot device in the boot order.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multitenancy, expand the **root** node.

Step 4 Right-click **Boot Policies** and select **Create Boot Policy**.

The **Create Boot Policy** wizard displays.

Step 5 Enter a unique name and description for the policy.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

Step 6 (Optional) After you make changes to the boot order, check the **Reboot on Boot Order Change** check box to reboot all servers that use this boot policy.

For boot policies applied to a server with a non-Cisco VIC adapter, even if the **Reboot on Boot Order Change** check box is not checked, when SAN devices are added, deleted, or their order is changed, the server always reboots when boot policy changes are saved.

Step 7 (Optional) If desired, check the **Enforce vNIC/vHBA/iSCSI Name** check box.

- If checked, Cisco UCS Manager displays a configuration error and reports whether one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the **Boot Order** table match the server configuration in the service profile.

- If not checked, Cisco UCS Manager uses the vNICs or vHBAs (as appropriate for the boot option) from the service profile.

Step 8 In the Boot Mode field, choose the **Legacy** or **UEFI** radio button.

Step 9 If you selected UEFI, check the **Boot Security** checkbox if you want to enable UEFI boot security.

Step 10 Click the down arrows to expand the **Local Devices** area.

Step 11 Click **Add SD Card** to add the device to the **Boot Order** table.

What to do next

Include the boot policy in a service profile and template.

After a server is associated with a service profile that includes this boot policy, you can verify the boot order in the **Boot Order Details** area on the **General** tab for the server.

Creating a Local Disk Configuration Policy

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multitenancy, expand the **root** node.

Step 4 Right-click **Local Disk Config Policies** and choose **Create Local Disk Configuration Policy**.

Step 5 In the **Create Local Disk Configuration Policy** dialog box, specify the name and choose **No Raid** from the **Mode** drop-down menu.

Step 6 Uncheck the **Protect Configuration** check box.

Step 7 Click the **Enable** radio button in the **FlexFlash State** field.

Step 8 If you are using two SD cards, click the **Enable** radio button in the **FlexFLash RAID Reporting State** field.

Step 9 Click **OK**.

What to do next

Specify the local disk configuration policy in the service profile template.

Creating a BIOS Policy

Note Cisco UCS Manager pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the Cisco Integrated Management Controller (CIMC) buffer. These changes remain in the buffer and do not take effect until the server is rebooted.

We recommend that you verify the support for BIOS settings in the server that you want to configure. Some settings, such as Mirroring Mode for RAS Memory, are not supported by all Cisco UCS servers.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multitenancy, expand the **root** node.

Step 4 Right-click **BIOS Policies** and select **Create BIOS Policy**.

Step 5 On the **Main** page of the **Create BIOS Policy** wizard, enter a name for the BIOS policy in the **Name** field.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

Step 6 In the **Create BIOS Policy** wizard, do the following to configure the BIOS settings:

a) If you want to change a BIOS setting, click the desired radio button or make the appropriate choice from the drop-down list.

For descriptions and information about the options for each BIOS setting, see the Cisco UCS Manager GUI Configuration Guide.

b) Click **Next** after each page.

Step 7 On the **USB** page, click the **enabled** radio button in the **USB PORT: SD Card** field.

Step 8 After you have configured all of the BIOS settings for the policy, click **Finish**.

Configuring a LAN Boot for a Boot Policy

You can add a LAN boot policy to use with Virtual SAN actions and workflows. the LAN boot policy is used to PXE boot for ESXi installations.

This procedure continues directly from Creating a Boot Policy, on page 103.

Procedure

Step 1 Click the down arrows to expand the **vNICs** area.

Step 2 Click the **Add LAN Boot** link.

Step 3 In the **Add LAN Boot** dialog box, enter the name of the vNIC that you want to use for the LAN boot in the **vNIC** field, then click **OK**.

The vNIC name needs to match the defined vNIC name for the UCS service profile template.

Step 4 Check the **Enforce vNIC/vHBA/iSCSI Name** check box.

Step 5 Do one of the following:

- Add another boot device to the **Boot Order** table.
- Click **OK** to finish.

Creating a Scrub Policy

You can add a FlexFlash scrub policy for use with Virtual SAN actions and workflows.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multitenancy, expand the **root** node.

Step 4 Right-click **Scrub Policies** and select **Create Scrub Policy**.

Step 5 In the **Create Scrub Policy** wizard, enter the name of the policy, and in the **FlexFlash Scrub** field, click the **Yes** radio button.

Step 6 Click **OK**.

Creating a Template for VM Provisioning

You cannot provision a Windows 2016 VM or a Windows 10 VM using an ISO image. You must create a template to provision these VMs.

Procedure

Step 1 Login to the vCenter and create a blank virtual machine.

Select **Windows** as the guest operating system, and select **Microsoft Windows Server 2016 (64-bit)** as the version.

LSI Logic SAS is automatically selected as the SCSI Controller.

Step 2 Convert the virtual machine into a template.

Step 3 Run an inventory process.

For information on how to initiate an inventory process, see Collecting ISO Inventory, on page 24

Step 4 Create a standard catalog. For information on creating a standard catalog, see Creating Catalogs for ISO-Based VM Provisioning, on page 25

Be sure to specifiy the following:

- Check the **Provision New VM for ISO Mounting** check box
- In the **Template** field, select the blank VM template you created.

Step 5 Create a service request. For more information, see Creating Service Requests for ISO-Based VM Provisioning, on page 26.

Known Issues with the Collect VMware Object Level Inventory task

Following are the known issues with the **Collect VMware Object Level Inventory** task:

- If you run the **Collect VMware Object Level Inventory** task on a host and select a virtual switch as the entity, the task initiates an inventory collection for all virtual switches present in the vCenter rather than limiting the inventory collection to the host that you selected.
- Entities selected in the **Collect VMware Object Level Inventory** task are independent of each other.

  When you run this task by selecting multiple entities, and try to filter objects, the inventory process runs at the account level of the selected entity. To elaborate, let us assume that you created two new VMs (VM11 and VM21) in two separate hosts (H1 and H2). While running this inventory task, you select the following two entities:

  - A host—in this example H1.
  - A VM but do not select a specific VM

  When the inventory process completes, instead of showing only the selected host on VM11, the report displays both VMs from both hosts (H1 and H2).