Cisco UCS Director EMC Management Guide, Release 6.7

First Published: 2019-04-09

Last Modified: 2019-06-17

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

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

Related Documentation

Cisco UCS Director Documentation Roadmap

For a complete list of Cisco UCS Director documentation, see the *Cisco UCS Director Documentation Roadmap* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-director/doc-roadmap/b_UCSDirectorDocRoadmap.html.

Cisco UCS Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Note The *Cisco UCS B-Series Servers Documentation Roadmap* includes links to documentation for Cisco UCS Manager and Cisco UCS Central. The *Cisco UCS C-Series Servers Documentation Roadmap* includes links to documentation for Cisco Integrated Management Controller.

Documentation Feedback

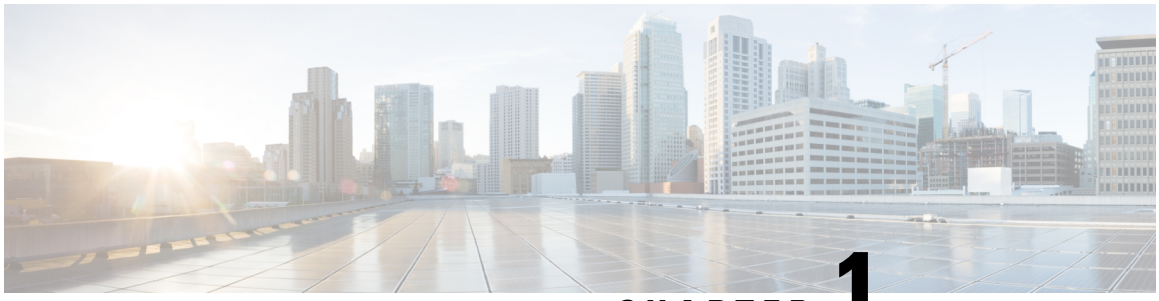
To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-director-docfeedback@cisco.com. We appreciate your feedback.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

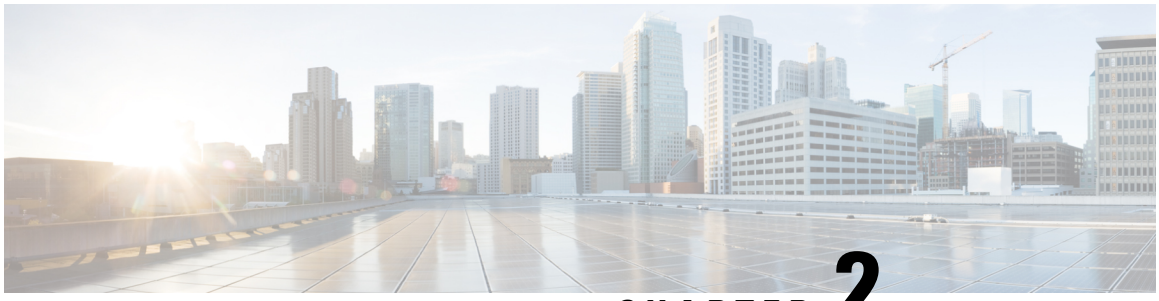
New and Changed Information for this Release

New and Changed Information in 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 6.7(1.0)

Feature	Description	Where Documented
Support for EMC Symmetrix PowerMAX	In this release, Cisco UCS Director supports EMC Symmetrix PowerMAX.	EMC Symmetrix VMAX, VMAX3, and PowerMax, on page 49



CHAPTER 2

Overview

Overview

Cisco UCS Director supports EMC storage systems and data protection systems.

Note For details about the supported versions for each of these systems, see the Cisco UCS Director Compatibility Matrix for this release.

Supported EMC Storage Systems

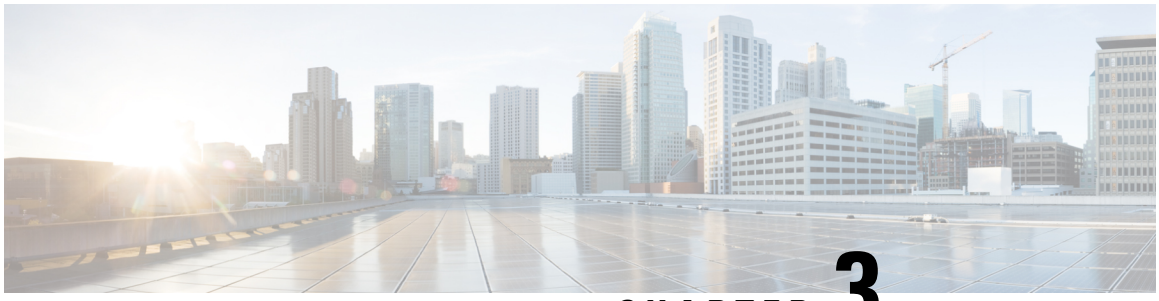
EMC Storage System	Where Documented
EMC Isilon	
EMC Unity	
EMC Symmetrix VMAX, VMAX3, and PowerMax	
EMC VNX	
EMC VNXe	
EMC VPLEX	
EMC XtremIO	

Supported EMC Data Protection Systems

EMC Data Protection System	Where Documented
EMC RecoverPoint	

PART I

EMC Storage Systems



CHAPTER 3

EMC Isilon

Cisco UCS Director Support for EMC Isilon

Cisco UCS Director manages, monitors, and does reporting for the EMC Isilon system. Data is collected through the Isilon cluster platform and namespace REST API, which is connected to Cisco UCS Director through HTTP or HTTPS. This data is parsed and bound to the output as Plain Old Java Objects (POJOs), and these objects are distributed throughout the pod.

Adding an EMC Isilon Account

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

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

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, complete the following fields:

Name	Description
Pod drop-down list	Choose the pod for this account. The pod can be one of the following types: • **Default Pod** • **Generic** • **VSPEX** • **Vblock**
Category drop-down list	Choose **Storage**.
Account Type drop-down list	Choose **EMC Isilon Cluster**.

Step 5 Click **Submit**.

Step 6 On the second **Add Account** screen, complete the following fields:

Name	Description
Account Name field	A unique name for this Isilon account. For example, **`isilon-1`**.
Description field	A description of the Isilon cluster.
Server IP field	The IP address of the Isilon cluster.
Use Credential Policy check box	Check this box if you want to use a credential policy for this account rather than enter the username and password information manually.
Credential Policy drop-down list	If you checked **Use Credential Policy**, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
Username field	The username that this account uses to access the Isilon cluster. This username must be a valid account in the Isilon cluster. This field is not displayed if you chose to use a credential policy.
Password field	The password associated with the username. This field is not displayed if you chose to use a credential policy.
Protocol drop-down list	Choose one of the following transport types that you want to use for this account: • **http** • **https** The default transport type protocol for this account is HTTPS.
Port field	The port used to access the Isilon cluster. Port 8080 is the default port for both HTTP and HTTPS.
API Version drop-down list	Choose the API verson that is supported on the Isilon cluster. The default is API version 1.

Name	Description
Connection Timeout (Seconds) field	The length of time in seconds that Cisco UCS Director will wait to establish a connection to the Isilon cluster before timing out. The default value is 30 seconds. The valid values are from 0 to 1800. An empty field or a value of 0 is interpreted as an infinite timeout.
Socket Read Timeout (Seconds) field	The length of time in seconds that Cisco UCS Director will wait for data from the Isilon cluster before timing out. The default value is 30 seconds. The valid values are from 0 to 1800. An empty field or a value of 0 is interpreted as an infinite timeout.
Contact field	The email address that you use to contact the administrator or other person responsible for this account.
Location field	The location of the contact.

Step 7 Click **Submit**.

Cisco UCS Director tests the connection to the EMC Isilon storage system. If that test is successful, it adds the Isilon account and discovers all infrastructure elements in the storage system that are associated with that account. This discovery process and inventory collection cycle takes few minutes to complete.

Storage Pool Tiers

Storage pool tiers are collections of node pools that you group to optimize storage according to need, such as a mission-critical high-speed tier that is best suited to data archiving. You can organize storage pool tiers, into logical groupings by creating policies that store or move files among these groups automatically, based on a specified criteria.

The following storage pool tiers can be created for specific purposes. Older nodes can be reduced in numerical quantity and new nodes can be added as a new tier in the same cluster.

Storage Pool Tier	Description
EMC Isilon S-Series	This platform has Input/Output Operations Per Second (IOPS) for intensive applications which process large volumes of data and devote most of their processing time to input/output (I/O) and manipulation of data. An EMC Isilon S-Series performance tier can be combined with an archive tier (EMC Isilon NL-Series) in the same cluster. An EMC Isilon S-Series with Solid State Drives (SSDs) latency tier of can be added for latency-sensitive data must meet certain time constraints in order to be acceptable to a user.
EMC Isilon X-Series	This platform is used for high concurrent and sequential throughput workflows.

Storage Pool Tier	Description
EMC Isilon NL-Series	This platform is used for cost-effective, scalable near line (NL) on-site storage of data on removable media.

Creating a Storage Pool Tier

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Isilon account where you want to create the storage pool tier.
Step 5 Click **View Details**.
Step 6 Click **Storage Pool Tiers**.
Step 7 Click **Create**.
Step 8 On the **Create Storage Pool Tier** screen, enter a unique name for the storage pool tier and click **Submit**.

These node pools are grouped to optimize storage according to need.

Storage Node Pools

Storage node pools are sets of physical nodes that are grouped by their equivalence class to optimize reliability and requested data protection settings. The OneFS operating system creates node pools automatically when you install the system and whenever you add or remove nodes. The automatic creation of node pools is referred to as automated provisioning.

You can organize storage node pools into logical groupings and create policies that store or move files among these nodes automatically, based on a specified criteria.

Creating a Node Pool

You can use a node pool to group equivalence-class nodes.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Isilon account where you want to create the node pool.
Step 5 Click **View Details**.
Step 6 Click **Node Pools**.
Step 7 Click **Create**.
Step 8 On the **Create Node Pool** screen, complete the following fields:

Name	Description
Node Pool Name field	A unique name for the node pool.
Nodes field	Expand the field, check one or more boxes for the nodes that you want to include in the pool.

Step 9 Click **Submit.**

SMB Shares

The Server Message Block (SMB) Protocol is a network file sharing protocol that was implemented by Microsoft for Windows. SMB shares provide Windows clients network access to file system resources on the cluster.

You can grant permissions to users and groups to carry out operations such as reading, writing, and setting access permissions on SMB shares.

The `/ifs` directory is configured as an SMB share and is enabled by default. OneFS supports both user and anonymous security modes. If the user security mode is enabled, users who connect to a share from an SMB client must provide a valid username with proper credentials.

The SMB protocol uses security identifiers (SIDs) for authorization data. All identities are converted to SIDs during retrieval and are converted back to their on-disk representation before they are stored on the cluster.

Creating an SMB Share

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Isilon account where you want to create the SMB share.

Step 5 Click **View Details**.

Step 6 Click **SMB Shares**.

Step 7 Click **Create**.

Step 8 On the **Create SMB Share** screen, complete the following fields:

Name	Description
SMB Share Name field	A unique name for the SMB share.
SMB Share Description field	A description of the SMB share.
Path field	The `/ifs` directory path that is configured to be an SMB share.

Name	Description
Allow Variable Expansion check box	Check the box if you want to expand Isilon path variables in the share directory path. The available path variables include the following: • `%D`—NetBIOS domain name • `%L`—Host name of the cluster, in lowercase • `%U`—User name • `%Z`—Zone name For example, if you have a user in the CISCO domain with a username of cisco1, with path varable expansion enabled, the path `/ifs/home/%D/%U` expands to `/ifs/home/CISCO/cisco1`.
Auto-Create Directories check box	Check the box if you want the share to automatically create directories when users access the share for the first time. **Note** This check box is available only if you check **Allow Variable Expansion**.

Step 9 On the **Create SMB Share** screen, expand the **User/Group Mapping** field if you want to restrict access to the SMB share.

Step 10 On the **Add Entry to User/Group Mapping** screen, complete the following fields and then click **Submit**:

Name	Description
Type drop-down list	Choose a mapping type. This can be one of the following: • **User**—Restricts access for a specific user. • **Group**—Restricts access for a group of users. • **Wellknown**—Restricts access for a well-known security identifier (SID).
Name field	The name of the user, group, or well-known SID whose access you want to restrict.
Permission drop-down list	Choose a permission option for the user, group, or well-known SID. This can be one of the following: • **No Access** • **Read Access** • **Read-Write Access** • **Full Access** • **Root Access**

The user/group mappings display in the **User/Group Mapping** table on the **Create SMB Share** screen.

Step 11 Click **Submit**.

Creating an NFS Export

Network File System (NFS) exports provide UNIX clients with network access to file system resources on the cluster.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Isilon account where you want to create the NFS export.

Step 5 Click **View Details**.

Step 6 Click **NFS Exports**.

Step 7 Click **Create**.

Step 8 On the **Create NFS Export** screen, complete the following fields:

Name	Description
Path field	The `/ifs` directory path that you want to export to UNIX clients.
Description field	A description that helps identify and document the purpose of the export.
Clients field	The UNIX clients that you want to have access to the NFS export.
Read-Only Clients field	The UNIX clients that you want to have read-only access to the NFS export.
Read-Write Clients field	The UNIX clients that you want to have read-write access to the NFS export, even if the NFS export is read-only.
Root Clients field	The uNIX clients that you want to have root access to the NFS export.
Enable Mount Access for Subdirectories check box	Check the box if you want all directories under the specified paths to be mountable.
Restrict Access to Read Only check box	Check the check box to make the NFS export read-only.
Mapping Access drop-down list	Choose the type of UNIX clients that will have mapping access to the export.
Specify Username field	One or more users that you want to have access to the NFS export.
Specify User Group(s) field	One or more user groups that you want to have access to the NFS export.

Step 9 Click **Submit**.

Viewing NFS Datastores

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Isilon account where you want to view the datastores.

Step 5 Click **View Details**.

Step 6 Click **Datastores**.

You can view information about each Network File System (NFS) datastore, including the datastore name, its NFS export path, ESXi host, NFS remote host, capacity, and free space.

Quotas

Storage quotas contain a set of resources and provide an accounting of each resource type for that set. You can use quotas ao manage storage in the following ways:

- Monitor disk storage.
- Define criteria to track or limit the amount of storage a user, group, or project uses.
- Write notification rules to trigger an action according to event thresholds. A rule can specify a schedule for executing an action or immediate notification of certain state transitions. When an event occurs, a notification trigger can execute one or more actions, such as sending an email or sending a cluster alert to the interface.

Quota types, also known as quota domains, are used to organize storage quotas. Each quota type is defined by a directory or an entity, which encapsulate the files and subdirectories to be tracked. The following identifiers are used to describe quota types:

- The directory where the quota is located
- The quota entity
- The snapshots that are to be tracked against the quota limit, if any

Creating a Quota

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Isilon account where you want to create the quota.

Step 5 Click **View Details**.

Step 6 Click **Quotas**.

Step 7 Click **Create**.

Step 8 On the **Create Quota** screen, complete the following fields:

Name	Description
Type drop-down list	Choose a quota type. This can be one of the following. • **Directory**—Specifies the directory and its subdirectories where you want to locate the quota. • **User**—Defines a specific user that you want to associate with the storage quota. • **Group**—Defines a group of users that you want to associate with the storage quota. • **All Users**——Associates all users with the storage quota. • **All Groups**—Associates all user groups with the storage quota.
Path field	The `/ifs` directory path for the storage quota.
Include Snapshots check box	Check the box if the quota governs snapshot data and head data. If you do not check the box, the quota cannot include snapshots.
Thresholds Include Overhead check box	Check the box if the thresholds that apply to the quota include the file system overhead required to store the data for physical usage. If the check box is not checked, thresholds do not include any overhead.
Enforced check box	Check the box to have the quota provide enforcement. Once checked, you can configure additional parameters, such as a hard limit and soft limit. If you do not check this box, the quota is considered to be an accounting quota.

Step 9 Click **Submit**.

Manually Generating a Quota Report

All manually generated quota reports are stored in the directory on `/ifs` that you configured in the quota report settings. For information about how to specify that directory or to set up scheduled quota reports, see Updating Quota Report Settings, on page 16.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Isilon account where you want to create the quota report.

Step 5 Click **View Details**.

Step 6 Click **Quota Reports**.

Step 7 From the **More Actions** drop-down list, choose **Create**.

Step 8 Click **Submit**.

Updating Quota Report Settings

The quota report settings allow you to configure the following:

- Manual reports—Directory where manual reports are stored and the maximum number of reports to be retained.
- Scheduled reports—Schedule that determines when the reports are run, the directory where the reports are stored, and the maximum number of reports to be retained.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Isilon account where you want to update the quota report settings.

Step 5 Click **View Details**.

Step 6 Click the **Quota Report Settings** tab.

Step 7 Click **Modify**.

Step 8 In the **Modify Quota Report Settings** dialog box, complete the following fields:

Name	Description
Live Directory field	The directory path on `/ifs` where manual or live quota reports are stored.
Live Retain field	The maximum number of manual or live quota reports to keep.
Schedule field	The schedule used to generate automated quota reports. For example, this could be **`every Sunday at 11pm`**
Schedule Directory field	The directory path on `/ifs` where scheduled quota reports are stored.
Scheduled Retain field	The maximum number of scheduled quota reports to keep.

Step 9 Click **Submit**.

Configuring a Namespace Access Point

The Isilon One FS cluster creates a single namespace and file system that is distributed across all nodes in the cluster and is accessible by clients connecting to any node in the cluster. You can assign a name to a namespace access point and the path to its file system.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Isilon account where you want to configure the namespace access point.

Step 5 Click **View Details**.

Step 6 Click the **Namespace** tab.

Step 7 Click **Create**.

Step 8 On the **Create Namespace Access Point** screen, complete the following fields:

Name	Description
Namespace Access Point Name field	A unique name for the namespace access point.
Path field	The `/ifs` home directory path for the namespace access point.

Step 9 Click **Submit**.

Viewing the Access Zones

An access zone is a context that is set up through the EMC Isilon CLI to control access to the EMC Isilon cluster based on an incoming IP address. Access zones are used to define a list of authentication providers that apply only in the context of these zones.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Isilon account where you want to view the access zones.

Step 5 Click **View Details**.

Step 6 Click **Access Zones**.

You can view all of the available information about the access zones, including the name, whether it's built-in, the SMB share use, authentication providers, system providers, and NetBIOS name.

Data Snapshots

You can take snapshots of specific data on the Isilon cluster. This data can also be backed up automatically and as frequently as required to meet your recovery point objectives. You can easily move directories, assign resources, and change directory names.

You can take up to 1,024 snapshots per directory to provide scalability and data protection in a large data environment.

Creating a Snapshot

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Isilon account where you want to create the NFS export.

Step 5 Click **View Details**.

Step 6 Click **Snapshots**.

Step 7 Click **Create**.

Step 8 On the **Create Snapshot** screen, complete the following fields:

Name	Description
Snapshot Name field	The name of the snapshot.
Snapshot Path field	The `/ifs` directory that is contained by the snapshot.
Alias check box	Check the check box if you want to create an alias for the snapshot name.
Alias Name field	An alias name for the snapshot name. This field is only available if you check the **Alias** box.
Snapshot Expiration drop-down list	Choose the expiration date for the snapshot. This can be one of the following: • **Never Expires** • **Snapshot Expires On**
Snapshot Expiration Date calendar	The expiration date for the snapshot. You can configure the expiration date as follows: • Enter the date in the field, using the MM/DD/YYYY format. • Click the calendar and choose an expiration date. This field is only visible if you chose **Snapshot Expires On**.

Step 9 Click **Submit.**

The snapshot is created and appears in the list of snapshots.

Viewing Snapshot Schedules

You must create snapshot schedules in EMC Isilon. You can view only the details of the available snapshot schedules in Cisco UCS Director.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Isilon account where you want to create the NFS export.

Step 5 Click **View Details**.

Step 6 Click **Snapshot Schedules**.

You can view all of the available information about snapshot schedules, including the snapshot name, pattern, path, expiration, description, next run, and next scheduled snapshot.

System Jobs

System jobs are maintenance functions that use system resources and can take several hours to complete. These jobs can include running a virus scan, monitoring and optimizing performance, detecting and mitigating drive and node failures, and freeing up available space. Some system jobs may run at scheduled intervals or they may be configured to only run when you manually start them.

Cisco UCS Director enables you to do the following with system jobs:

- Collect the available system jobs when you collect inventory from the EMC Isilon cluster
- View the available system jobs
- Manually run a system job
- View the details of system job policies
- View the details of system job reports

A complete list of sytem jobs is available in your EMC Isilon documentation.

Manually Running a System Job

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Isilon account where you want to run the system job.

Step 5 Click **View Details**.

Step 6 Click **System Jobs**.

Step 7 Click the row with the system job that you want to run and then click **Start**.

Step 8 On the **Start System Job** screen, complete the following fields:

Name	Description
Allow Duplicate Jobs check box	Check the box if you want to allow duplicate jobs to be run at the same time as this job.

Name	Description
Priority drop-down list	Choose a priority for this job. This can be from 1 to 10, with 1 being the highest priority job.

Step 9 Click **Submit**.

Monitoring System Jobs

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Isilon account where you want to run the system job.
Step 5 Click **View Details**.
Step 6 To view a summary of information about active jobs on the Isilon cluster, click **Job Summary**.
Step 7 To refresh the information available about active jobs, click **Collect Inventory**.

Modifying an Active Job

You can only modify an active running job. After the active job is complete, the job summary might not have any data and you cannot modify the job.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Isilon account where you want to modify the system job.
Step 5 Click **View Details**.
Step 6 Click **Job Summary**.
Step 7 Click the row with the job that you want to modify and click **Modify**.
Step 8 On the **Modify Active Job** screen, complete the following fields:

Name	Description
Impact Policy field	Check the appropriate box to choose a single Isilon policy. **Note** You can find details about the available policies on the **System Job Policy** tab to view specific details for each of these Isilon policies.
Priority drop-down list	Choose a priority for this job from 1 to 10, with 1 being the highest priority job.

Name	Description
State drop-down list	Choose a state for this job. This can be one of the following: • **Run** • **Pause** • **Cancel**

Step 9 Click **Submit**.

Viewing System Job Results

You can view all of the available information about the report, including the snapshot name, pattern, path, expiration, description, next run, and next snapshot.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Isilon account where you want to view the system job results.
Step 5 Click **View Details**.
Step 6 Click **System Job Reports**.
Step 7 Choose a report and click **View Details** to see the logged results of the system job.

Viewing Storage Efficiency Through Deduplication Results

You can use data deduplication to maximize storage efficiency by scanning the cluster for identical blocks and then eliminating the duplicates, which decreases the amount of physical storage required.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Isilon account where you want to view the deduplication results.
Step 5 Click **View Details**.
Step 6 Click **Deduplication**.
Step 7 Choose a deduplication report and click **View Details** to see the logged results of the deduplication report.

Managing EMC Isilon System Tasks

For more infomration about system tasks, see the Cisco UCS Director Administration Guide.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

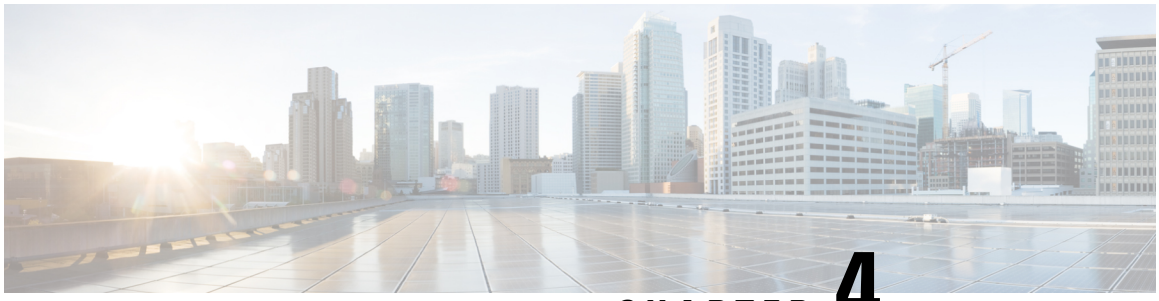
Step 4 Click the row with the EMC Isilon account where you want to manage the system tasks.

Step 5 Click **View Details**.

Step 6 Click **System Tasks**.

Step 7 Click the row with the system task and click one of the following:

- **Manage Task**—Complete the fields to update the execution, schedule, and policy configuration of the task.
- **Run Now**—Starts the system task immedialely.
- **View Details**—View the system task history, including the results of task execution, and trending reports.



CHAPTER 4

EMC Unity

Cisco UCS Director Support for EMC Unity

Cisco UCS Director provides support for orchestration automation, management, monitoring, and reporting for supported EMC Unity storage arrays.

The summary reports for EMC Unity that you can add to your Cisco UCS Director dashboard provide a system overview, free vs used system capacity, and the available capacity of storage pools. In addition, the available reports for an EMC Unity storage array include inventory information and the current status of the following:

- Storage processors
- Disk groups
- Disks
- Storage pools
- Storage tiers
- LUNs
- Consistency groups
- Hosts
- Initiators
- iSCSI portals
- iSCSI routes

- Ethernet ports
- FC (Fibre Channel) ports
- File systems
- SMB shares
- NFS shares
- NAS servers
- Snapshot schedules
- System Tasks

Adding an EMC Unity Account

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

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

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, complete the following fields:

a) From the **Pod** drop-down list, choose the one of the following types of pods for this account:

- **Default Pod**
- **Generic**
- **Vblock**
- **VSPEX**

b) From the **Category** drop-down list, choose **Storage**.

c) From the **Account Type** drop-down list, choose **EMC Unity**.

Step 5 Click **Submit**.

Step 6 On the second **Add Account** screen, complete the following fields:

a) Enter a unique name and description for the account.

b) In the **Array IP** field, enter the IP address assigned to the EMC Unity storage array.

c) Check the **Use Credential Policy** box if you want to use a credential policy for this account rather than enter the username and password information manually.

d) If you checked the **Use Credential Policy** box, choose a policy from the **Credential Policy** drop-down list.

You can also click **Add** and create a new credential policy for this account. See the Cisco UCS Director Administration Guide.

e) If you did not check **Use Credential Policy**, complete the following fields:

- Enter the username and password that this account uses to access the Unity storage array. This username must be a valid account in the Unity storage array.
- **Protocol**—Choose **https** as the transport type for this account.

- **Port**—Enter the port used to access the Unity storage array. Port 443 is the default port.
- **Connection Timeout (Seconds)**—Enter the length of time in seconds that Cisco UCS Director waits to establish a connection to the Unity storage array before timing out.

  The default value is 60 seconds. The valid values are from 0 to 1800. An empty field or a value of 0 is interpreted as an infinite timeout.
- **Socket Read Timeout (Seconds)**—Enter the length of time in seconds that Cisco UCS Director will wait for data from the Unity storage array before timing out.

  The default value is 60 seconds. The valid values are from 0 to 1800. An empty field or a value of 0 is interpreted as an infinite timeout.

f) Enter the email address and location of the administrator or other person responsible for this account.

Step 7 Click **Submit**.

Cisco UCS Director tests the connection to the EMC Unity storage array. If that test is successful, it adds the Unity account and discovers all infrastructure elements in the storage array that are associated with that account. This discovery process and inventory collection cycle takes few minutes to complete.

Storage Pools

A storage pool includes one or more drives with the same characteristics, such as the disk group, RAID type, or number of disks. An EMC Unity storage array must have at least one storage pool that you can use to create storage resources, such as LUNs and file systems.

After you create a storage pool, you can expand the pool to include additional drives and multiple drive types. However, you cannot remove drives assigned to a pool.

Creating a Storage Pool

Before you begin

- Create at least one disk group on the EMC Unity storage array. All available disk groups are added to Cisco UCS Director during inventory collection.
- Make sure the disks that you want to include in the storage pool are free and available in the appropriate storage tier.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to create a storage pool and click **View Details**.

Step 5 Click **Storage Pools**.

Step 6 Click **Create**.

Step 7 On the **Create Storage Pool** screen, complete the following fields:

a) Enter a unique name and description for the storage pool.
b) Expand **Disk Group** and check each group that you want to use.
c) From the **RAID Type** drop-down list, choose the type of RAID configured for the drives in the pool.
d) From the **RAID Stripe Width** drop-down list, choose the number of parallel stripes that can be written to or read from simultaneously.
e) In the **Number of Disks** field, enter the number of disks in the pool.
f) In the **Alert Threshold** field, enter a number between 50 and 84 to specify when the system sends an email notification about the available pool capacity.

   The alert threshold is the percentage of allocated storage from the pool. This number determines when the system sends alerts about the amount of free space remaining in the pool. For example, if you specify 84, the system sends an alert when 84% of the storage is allocated and only 16% is available.

Step 8 Click **Submit**.

Expanding a Storage Pool

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Unity account where you want to expand a storage pool and click **View Details**.
Step 5 Click **Storage Pools**.
Step 6 Click the row with the storage pool you want to expand and click **Expand**.
Step 7 On the **Expand Storage Pool** screen, complete the following fields:
a) Expand **Disk Group** and check each group that you want to add to the pool.
b) From the **RAID Type** drop-down list, choose the type of RAID configured for the drives in the pool.
c) From the **RAID Stripe Width** drop-down list, choose the number of parallel stripes that can be written to or read from simultaneously.
d) In the **Number of Disks** field, enter the number of disks that you want to add to the pool.
Step 8 Click **Submit**.

Hosts

Host configurations are logical connections that hosts or applications can use to access storage resources.

Note Cisco UCS Director supports the Host configuration type only. We do not support the Subnet or Netgroup host configuration types.

Creating a Host

Note Cisco UCS Director supports the Host configuration type only. We do not support the Subnet or Netgroup host configuration types.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to create a host and click **View Details**.

Step 5 Click **Hosts**.

Step 6 Click **Add**.

Step 7 On the **Create Host** screen, complete the following fields:

a) Enter a unique name and description for the host.

b) From the **Operating System** drop-down list, choose the operating system for the host.

Step 8 Click **Submit**.

Adding a Network Address to a Host

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to update a host and click **View Details**.

Step 5 Click **Hosts**.

Step 6 Click the row with the host you want to update and click **View Details**.

Step 7 Click **Network Addresses**.

Step 8 Choose **Create**.

Step 9 On the **Create Host IP Port** screen, complete the following fields:

a) In the **Network Address** field, enter the network address for the IP port.

You cannot change this network address after you create the IP port.

b) Check **Ignore Port While Granting Storage Access to NFS** if you want this IP port to be ignored.

Step 10 Click **Submit**.

Changing the ID for a Host LUN

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Unity account where you want to update a host and click **View Details**.
Step 5 Click **Hosts**.
Step 6 Click the row with the host you want to update and click **View Details**.
Step 7 Click **Host LUNs**.
Step 8 Click the row with the LUN that you want to modify.
Step 9 Choose **Modify**.
Step 10 On the **Modify LUN ID** screen, enter the new LUN ID and click **Submit**.

Adding an Initiator to a Host

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Unity account where you want to update a host and click **View Details**.
Step 5 Click **Hosts**.
Step 6 Click the row with the host you want to update and click **View Details**.
Step 7 Click **Initiators**.
Step 8 Choose **Add**.
Step 9 On the **Add Host Initiator** screen, complete the following fields:

a) From the **Initiator Type** drop-down list, choose either **FC** or **iSCSI**.
b) In the **iQN or WWN** field, enter the identifier for the initiator.
c) For an iSCSI initiator, if you want to use Challenge Handshake Authentication Protocol (CHAP), complete the following fields:

- **CHAP Username**
- **CHAP Secret**
- **CHAP Secret Type**

d) Check **Ignore Storage Access** if you do not want to allow this initiator to have the same storage access granted to the host.

Step 10 Click **Submit**.

Initiators

Initiators are the endpoints where Fibre Channel and iSCSI sessions originate. A Fibre Channel initiator is identified by its World Wide Name (WWN), and an iSCSI initiator by its iSCSI qualified name (IQN).

After you register an initiator and associate it with a host, all paths from the initiator are given access to the storage provisioned for the host. This ensures a high availability connection between the host and storage system.

Adding a Host Initiator

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to create a host and click **View Details**.

Step 5 Click **Initiators**.

Step 6 Click **Add**.

Step 7 On the **Add Host Initiator** screen, complete the following fields:

a) Expand **EMC Host Identity** and check the host that you want to associate with the initiator.

b) From the **Initiator Type** drop-down list, choose either **FC** or **iSCSI**.

c) In the **iQN or WWN** field, enter the identifier for the initiator.

d) For an iSCSI initiator, if you want to use Challenge Handshake Authentication Protocol (CHAP), complete the following fields:

- **CHAP Username**
- **CHAP Secret**
- **CHAP Secret Type**

e) Check the **Ignore Storage Access** box, if you do not want to allow this initiator to have the same storage access granted to the host.

Step 8 Click **Submit**.

iSCSI Interfaces

Creating an iSCSI Portal

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to configure an iSCSI interface and click **View Details**.

Step 5 Click **iSCSI Portals**.

Step 6 Click **Create**.

Step 7 On the **Create iSCSI Portal** screen, complete the following fields:

a) Expand **EMC Unity Ethernet Port** and check the port that you want to associate with the portal.

b) Enter the IP Address, Subnet Mask or Prefix Length, VLAN ID, and Gateway Address that you want to use for the portal.

Step 8 Click **Submit**.

Creating an iSCSI Route

The iSCSI route defines the destination or target node for iSCSI traffic from the iSCSI portal on the EMC Unity storage array.

Before you begin

Create an iSCSI portal.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to configure an iSCSI interface and click **View Details**.

Step 5 Click **iSCSI Routes**.

Step 6 Click **Create**.

Step 7 On the **Create iSCSI Route** screen, complete the following fields:

a) Expand the **EMC Unity iSCSI Portal** field, check the portal that you want to associate with the route, and click **Validate**.

b) In the **Destination** field, enter the IP address for the target node of the route.

The IP address can be IPv4 or IPv6.

c) Enter the Subnet Mask or Prefix Length and Gateway Address that you want to use for the portal.

Step 8 Click **Submit**.

EMC Unity Block Storage

Setting Up EMC Unity Block Storage

Note The following procedure outlines one of the ways in which you can set up EMC Unity block storage.

Step 1 Add an account for the EMC Unity storage array.

See Adding an EMC Unity Account, on page 24.

Step 2 Create at least one host.

See Creating a Host, on page 27.

Step 3 Create at least one LUN.

See Creating a LUN, on page 32.

Step 4 Map the LUN to the host that you created.

See Mapping a LUN to a Host, on page 32.

Step 5 (Optional) Add at least one initiator to the host.

See Adding a Host Initiator, on page 29.

Step 6 (Optional) If the host initiator type is iSCSI, do the following:

a) Create an iSCSI Portal.

See Creating an iSCSI Portal, on page 29.

b) Create an iSCSI Route.

See Creating an iSCSI Route, on page 30.

Step 7 (Optional) Create a consistency group that includes the LUN you created.

Use consistency groups if you want to group a set of LUNs and create snapshots that represent the same point in time for each LUN. See Creating a Consistency Group, on page 209.

LUNs

You can use Cisco UCS Director to create, configure, and map LUNs for an EMC Unity storage array.

Creating a LUN

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to create a LUN and click **View Details**.

Step 5 Click **LUNs**.

Step 6 Click **Create**.

Step 7 On the **Create LUN** screen, complete the following fields:

a) Expand **Storage Pool**, check the storage pool you want to use for the LUN, and click **Validate**.

b) Enter a unique name for the LUN.

c) In the **Size** field, enter the quantity of storage to be allocated to the LUN.

This value is combined with the capacity unit to determine the total allocated storage. After you create the LUN, you can only increase the size. You cannot decrease it.

d) From the **Capacity Units** drop-down list, choose the unit of storage.

The default capacity unit is MB.

e) Enter a description for the LUN.

f) Expand **Default Node** and check the node that you want to assign as the default.

g) Check **Thin** if you want to create a thin provisioned LUN with on-demand storage instead of dedicated storage.

h) Expand **Snapshot Schedule** and check the snapshot schedule you want to use for the LUN.

i) Check **Pause Snapshot Schedule** if you want to pause the snapshot schedule when the LUN is created.

j) Expand **Access Hosts**, check each host you want to be able to access the LUN, and click **Validate**.

k) From the **Access Type** drop-down list, choose the access for the host:

- **LUN**
- **Snapshot**
- **LUN and Snapshot**

This field is only available after you choose and validate the host that you want to map.

l) In the **HLU** field, enter the host LUN unit for the host.

This field is only available after you choose and validate the host that you want to map.

Step 8 Click **Submit**.

Mapping a LUN to a Host

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to map a LUN and click **View Details**.

Step 5 Click **LUNs**.

Step 6 Click the row with the LUN that you want to map.

Step 7 Click **Map**.

Step 8 On the **Map LUN to Host** screen, complete the following fields:

a) Expand **EMC Unity Host**, check the host that you want to map, and then click **Validate**.

b) From the **Access Type** drop-down list, choose the access for the host:

- **LUN**
- **Snapshot**
- **LUN and Snapshot**

This field is only available after you choose the host that you want to map.

c) In the **HLU** field, enter the host LUN unit for the host.

This field is only available after you choose and validate the host that you want to map.

Step 9 Click **Submit**.

Unmapping a LUN from a Host

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to unmap a LUN and click **View Details**.

Step 5 Click **LUNs**.

Step 6 Click the row with the LUN that you want to unmap.

Step 7 Click **Unmap**.

Step 8 On the **Unmap LUN from Host** screen, expand **EMC Unity Host** and check each host that you want to unmap.

Step 9 Click **Submit**.

Starting the Creation of a LUN Snapshot

In addition to setting a schedule to automate the creation of a snapshot, you can also take a snapshot of a LUN at any time.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to start a snapshot for a LUN and click **View Details**.

Step 5 Click **LUNs**.

Step 6 Click the row with the LUN where you want to create a snapshot.

Step 7 From the **More Actions** drop-down list, choose **Start Snapshot Creation**.

Step 8 On the **Start EMC Unity Snapshot Creation** screen, click **Submit**.

Pausing the Creation of a LUN Snapshot

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to pause the snapshot creation for a LUN and click **View Details**.

Step 5 Click **LUNs**.

Step 6 Click the row with the LUN where you want to pause the snapshot creation.

Step 7 From the **More Actions** drop-down list, choose **Pause Snapshot Creation**.

Step 8 On the **Pause EMC Unity Snapshot Creation** screen, click **Submit**.

Consistency Groups

Consistency groups organize the storage allocated to a specific host or a set of hosts. Each consistency group can include one or more LUNs.

You can create a snapshot for a consistency group. These snapshots provide an image for each of the LUNs in the group at the same point in time. As a result, a consistency group can help to ensure that the data across all LUNs in the group is consistent.

Creating a Consistency Group

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to create a consistency group and click **View Details**.

Step 5 Click **Consistency Groups**.

Step 6 Click **Create**.

Step 7 On the **Create Consistency Group** screen, complete the following fields:

a) Enter a unique name and description for the consistency group.

b) Expand **Snapshot Schedule** and check the snapshot schedule you want to use for the consistency group.

c) Check the **Pause Snapshot Schedule** box if you want to pause the snapshot schedule.

d) Expand **LUN**, check each LUN that you want to associate with the consistency group, and click **Validate**.

e) Expand **Access Hosts**, check each host that you want to have access to the consistency group, and click **Validate**.

f) From the **Access Type** drop-down list, choose the access for the host:

- **LUN**

- **Snapshot**
- **LUN and Snapshot**

This field is only available after you choose and validate at least one access host.

Step 8 Click **Submit**.

Adding a LUN to a Consistency Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Unity account where you want to update a consistency group and click **View Details**.
Step 5 Click **Consistency Groups**.
Step 6 Click the row for the consistency group that you want to update and click **Add LUN**.
Step 7 On the **Add LUN to Consistency Group** screen, check the box for each LUN that you want to add and then click **Validate**.
Step 8 Click **Submit**.

Removing a LUN from a Consistency Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Unity account where you want to update a consistency group and click **View Details**.
Step 5 Click **Consistency Groups**.
Step 6 Click the row for the consistency group that you want to update and click **Remove LUN**.
Step 7 On the **Remove LUN from Consistency Group** screen, check the box for each LUN that you want to remove and then click **Validate**.
Step 8 Click **Submit**.

Starting the Creation of a Consistency Group Snapshot

In addition to setting a schedule to automate the creation of a snapshot, you can also take a snapshot of a consistency group at any time.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to create a snapshot of a consistency group and click **View Details**.

Step 5 Click **Consistency Groups**.

Step 6 Click the row for the consistency group where you want to take a snapshot.

Step 7 From the **More Actions** drop-down list, choose **Start Snapshot Creation**.

Step 8 On the **Start EMC Unity Snapshot Creation** screen, click **Submit**.

Pausing a Consistency Group Snapshot

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to pause a snapshot and click **View Details**.

Step 5 Click **Consistency Groups**.

Step 6 Click the row for the consistency group where you want to pause a snapshot.

Step 7 From the **More Actions** drop-down list, choose **Pause Snapshot Creation**.

Step 8 On the **Pause EMC Unity Snapshot Creation** screen, click **Submit**.

Deleting a Consistency Group

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to delete a consistency group and click **View Details**.

Step 5 Click **Consistency Groups**.

Step 6 Click the row for the consistency group that you want to delete and click **Delete**.

Step 7 On the **Delete Consistency Group** screen, complete the following fields:

a) Check **Force Snap Deletion** if you want to delete all snapshots of the consistency group when you delete the consistency group.

b) Check **Force LUN Deletion** if you want to delete all LUNs associated with the consistency group when you delete the consistency group.

Step 8 Click **Submit**.

EMC Unity File Storage

Setting Up EMC Unity File Storage

Note The following procedure outlines one of the ways in which you can set up EMC Unity file storage.

Step 1 Add an account for the EMC Unity storage array.

See Adding an EMC Unity Account, on page 24.

Step 2 Create at least one NAS Server.

See Creating a NAS Server, on page 38.

Step 3 Create a file interface for the NAS server.

See Creating a File Interface for a NAS Server, on page 38.

Step 4 Create one or more servers to support the NAS server.

Make sure that these servers are consistent with the protocol that you plan to use for the file system.

If you plan to use the SMB (Windows) file protocol, create an SMB server. If your implementation includes Active Directory, you can also create a DNS server. See Creating an SMB Server, on page 39 and Creating a DNS Server, on page 40.

If you plan to use the NFS (Linux or Unix) file protocol, create an NFS server. See Creating an NFS Server, on page 40.

Step 5 Create at least one file system.

See Creating a File System, on page 41.

Step 6 Create one or more shares for the file system.

The shares must be consistent with the protocol you plan to use for the file system. See Creating an SMB Share, on page 45 and Creating an NFS Share, on page 46.

Step 7 (Optional) Create at least one host if you want the NFS share to allow access to the host.

See Creating a Host, on page 27.

Step 8 (Optional) Create one or more file system or directory storage quotas through user quotas or quota trees.

See Creating a User Quota for a File System, on page 43, Creating a Quota Tree, on page 44, and Creating a User Quota for a Quota Tree, on page 44.

NAS Servers

A Network-Attached Storage (NAS) server is a file server that catalogs, organizes, manages, and transfers files within the designated shares in a file storage system. A NAS server requires the following:

- Storage pool to store the server's configuration data. You can create the storage pool in Cisco UCS Director.
- Storage processor where the server runs. Cisco UCS Director imports the storage processor information from the EMC Unity storage array during inventory collection.

Creating a NAS Server

Before you begin

- Determine which storage processor you want to use for the NAS server.
- Create a storage pool.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Unity account where you want to create a NAS server and click **View Details**.
Step 5 Click **NAS Servers**.
Step 6 Click **Create**.
Step 7 On the **Create a NAS Server** screen, complete the following fields:
a) Enter a unique name for the NAS server.
b) Expand **Storage Pool**, check the pool that you want to use, and then click **Validate**.
c) Expand **Storage Processor**, check the processor that you want to use, and then click **Validate**.
Step 8 Click **Submit**.

Creating a File Interface for a NAS Server

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Unity account where you want to update a NAS server and click **View Details**.
Step 5 Click **NAS Servers**.
Step 6 Click the row with the NAS server you want to update and click **View Details**.
Step 7 Click **File Interfaces**.
Step 8 Click **Create**.
Step 9 On the **Create File Interface** screen, complete the following fields:
a) Expand **IP Port**, check the box for the port that you want to use, and then click **Validate**.

b) Enter the IP address, Subnet Mask or Prefix Length, Gateway address, and VLAN ID that you want to use for the file interface.

Step 10 Click **Submit**.

Creating an SMB Server

Create an SMB server for each NAS server that you plan to use in a Windows file system.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to update a NAS server and click **View Details**.

Step 5 Click **NAS Servers**.

Step 6 Click the row with the NAS server where you want to create the SMB server and click **View Details**.

Step 7 Click **SMB Servers**.

Step 8 Click **Create**.

Step 9 On the **Create SMB Server** screen, complete the following fields:

a) From the **SMB Server Type** drop-down list, choose one of the following:

- **Standalone**—This is the default option.
- **Active Directory**—Use this option if you plan to join the NAS server to an Active Directory domain.

b) If you chose **Standalone** as the server type, complete the following fields:

- **NetBIOS Name**
- **Description**
- **Workgroup**
- **Administrator Password**

c) If you chose **Active Directory** as the server type, complete the following fields:

- **NetBIOS Name**
- **Description**
- **Windows Domain**
- **Domain Administrator Name**
- **Domain Administrator Password**
- **Organizational Unit**

Step 10 Click **Submit**.

What to do next

For an SMB server with Active Directory, create a DNS server.

Creating an NFS Server

Create an NFS server for a NAS server that you plan to use in a Linux or Unix file system.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Unity account where you want to update a NAS server and click **View Details**.
Step 5 Click **NAS Servers**.
Step 6 Click the row with the NAS server where you want to create the NFS server and click **View Details**.
Step 7 Click **NFS Servers**.
Step 8 Click **Create**.
Step 9 On the **Create NFS Server** screen, check the **NFSv4 Enabled** box if you want to use NFSv4 with the NFS server.
Step 10 Click **Submit**.

Creating a DNS Server

Create a DNS server for each NAS server that you plan to use in a Windows file system and join to Active Directory.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Unity account where you want to update a NAS server and click **View Details**.
Step 5 Click **NAS Servers**.
Step 6 Click the row with the NAS server where you want to create the DNS server and click **View Details**.
Step 7 Click **DNS Servers**.
Step 8 Click **Create**.
Step 9 On the **Create DNS Server** screen, complete the following fields:
a) In the **Domain** field, enter the fully qualified domain name of the DNS server.
b) In the **IP Addresses** field, enter a prioritized list of one to three IPv4 or IPv6 addresses of DNS servers for the domain.

To enter more than one IP address, separate them with commas.

Step 10 Click **Submit**.

Creating an NIS Server

Network Information Service (NIS) is a unix directory service. Creating an NIS Server on a NAS Server provides ability to resolve hosts defined on NFS share access lists.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to update a NAS server and click **View Details**.

Step 5 Click **NAS Servers**.

Step 6 Click the row with the NAS server where you want to create the NIS server and click **View Details**.

Step 7 Click **NIS Servers**.

Step 8 Click **Create**.

Step 9 On the **Create NIS Server** screen, complete the following fields:

a) In the **Domain** field, enter the fully qualified domain name of the NIS server.

b) In the **IP Addresses** field, enter a prioritized list of one to ten IPv4 or IPv6 addresses of NIS servers for the domain.

To enter more than one IP address, separate them with commas.

Step 10 Click **Submit**.

File Systems

A file system represents a set of storage resources for network files. Users or hosts can connect to the file system and use it for file-based storage.

Each file system, or container for file-based storage, has the following properties:

- A pre-determined storage capacity
- A file access protocol, such as SMB, NFS, or multi-protocol
- One or more shares that network hosts or users can use to access shared files or folders

Creating a File System

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to create a file system and click **View Details**.

Step 5 Click **File Systems**.

Step 6 Click **Create**.

Step 7 On the **Create File System** screen, complete the following fields:

a) From the **Protocol** drop-down list, choose one of the following:

- **Linux/UNIX Shares (NFS)**

  Windows Shares (SMB)

b) Expand **NAS Server**, check the server that you want to use, and then click **Validate**.
c) Enter a unique name for the file system.
d) Expand **Storage Pool**, check the pool that you want to use, and then click **Validate**.
e) In the **Size** field, enter the quantity of storage to be allocated to the file system.

   This value is combined with the capacity unit to determine the total allocated storage. After you create the file system, you can only increase the size. You cannot decrease it.

f) From the **Capacity Units** drop-down list, choose the unit of storage.

   The default capacity unit is MB.

g) Check **Thin** if you want to create a thin provisioned file system with on-demand storage instead of dedicated storage.
h) Expand **Snapshot Schedule** and check the schedule that you want to use.
i) Check **Pause Snapshot Schedule** if you want to pause the snapshot schedule when the file system is created.
j) If you chose an SMB share for the protocol, check the **Advanced** box if you want to configure any of the following settings:

   - **Sync Write Enabled**—Enables synchronous writes for all storage operations. This option guarantees that any write to the share is done synchronously and reduces the chances of data loss or file corruption. This option is recommended only if you plan to use the share as storage for a database application.
   - **Opslocks Enabled**—Enables opportunistic file locking for data. This option buffers file data locally before sending it to a server. This option allows SMB clients can access the local versions of the files and communicate changes to the server periodically.
   - **Notify on Write Enabled**—Enables notifications when a write is made to the file system.
   - **Notify on Access Enabled**—Enables notifications when the file system is accessed.

Step 8 Click **Submit**.

Starting the Creation of a File System Snapshot

In addition to setting a schedule to automate the creation of a snapshot, you can also take a snapshot of a file system at any time.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Unity account where you want to create a file system snapshot and click **View Details**.
Step 5 Click **File Systems**.
Step 6 Click the row with the file system where you want to create a snapshot.
Step 7 Click **Start Snapshot Creation**.

Step 8 On the **Start EMC Unity Snapshot Creation** screen, click **Submit**.

Pausing a File System Snapshot

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Unity account where you want to pause a file system snapshot and click **View Details**.
Step 5 Click **File Systems**.
Step 6 Click the row with the file system where you want to pause a snapshot.
Step 7 From the **More Actions** drop-down list, choose **Pause Snapshot Creation**.
Step 8 On the **Pause EMC Unity Snapshot Creation** screen, click **Submit**.

Creating a User Quota for a File System

A user quota limits or tracks the amount of storage space that individual users consume on a file system. The user quota sets default hard and soft limits at the file system level.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Unity account where you want to create a user quota and click **View Details**.
Step 5 Click **File Systems**.
Step 6 Click the row with the file system where you want to create the user quota and click **View Details**.
Step 7 Click **User Quotas**.
Step 8 Click **Create**.
Step 9 On the **Create User Quota** screen, complete the following fields:
a) In the **User ID** field, enter the ID of the user whose file system storage you want to limit.
b) In the **Soft Limit** field, enter the space usage limit where the storage usage enters the grace period.

If you enter 0 in this field, the user has no limit on the amount of storage space available. This is the default value.

c) In the **Capacity Units** field, choose MB, GB, or TB as the capacity unit for the soft limit.
d) In the **Hard Limit** field, enter the space usage limit where the user no longer has any storage available.

If you enter 0 in this field, the user has no limit on the amount of storage space available. This is the default value.

e) In the **Capacity Units** field, choose MB, GB, or TB as the capacity unit for the hard limit.

Step 10 Click **Submit**.

Creating a Quota Tree

A quota tree limits the amount of storage that can be consumed on a particular directory. You can use a quota tree to set storage limits for a project where multiple users share the same directory or to track directory usage.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to create a quota tree and click **View Details**.

Step 5 Click **File Systems**.

Step 6 Click the row with the file system where you want to create a quota tree and click **View Details**.

Step 7 Click **Quota Trees**.

Step 8 Click **Create**.

Step 9 On the **Create Tree Quota** screen, complete the following fields:

a) In the **Path** field, enter the path to the directory.

The path is relative to the root system and must start with a forward slash ("/"). For example, */sample_path1/sample_path2*

b) In the **Soft Limit** field, enter the space usage limit where the storage usage on the directory enters the grace period.

If you enter 0 in this field, there is no limit to the amount of storage space available on the directory. This is the default value.

c) In the **Capacity Units** field, choose MB, GB, or TB as the capacity unit for the soft limit.

d) In the **Hard Limit** field, enter the space usage limit where the directory no longer has any storage available.

If you enter 0 in this field, the user has no limit on the amount of storage space available. This is the default value.

e) In the **Capacity Units** field, choose MB, GB, or TB as the capacity unit for the hard limit.

Step 10 Click **Submit**.

Creating a User Quota for a Quota Tree

This user quota limits the amount of storage available to an individual user on the directory associated with the quota tree.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to create a user quota and click **View Details**.

Step 5 Click **File Systems**.

Step 6 Click the row with the file system where you want to create the user quota and click **View Details**.

Step 7 Click **Quota Trees**.

Step 8 Click the row with the quota tree where you want to create the user quota.

Step 9 Click **Create User Quota**.

Step 10 On the **Create User Quota** screen, complete the following fields:

a) In the **User ID** field, enter the ID of the user whose directory storage you want to limit.

b) In the **Soft Limit** field, enter the space usage limit where the storage usage on the directory enters the grace period.

If you enter 0 in this field, there is no limit to the amount of storage space available on the directory. This is the default value.

c) In the **Capacity Units** field, choose MB, GB, or TB as the capacity unit for the soft limit.

d) In the **Hard Limit** field, enter the space usage limit where the directory no longer has any storage available.

If you enter 0 in this field, the user has no limit on the amount of storage space available. This is the default value.

e) In the **Capacity Units** field, choose MB, GB, or TB as the capacity unit for the hard limit.

Step 11 Click **Submit**.

Shares

Creating an SMB Share

An SMB share controls access to file system resources for Windows users and hosts.

Before you begin

Ensure that the file system or snapshot you choose for the share's souce is associated with a NAS server that supports the SMB profile

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to create an SMB share and click **View Details**.

Step 5 Click **SMB Shares**.

Step 6 Click **Create**.

Step 7 On the **Create SMB Share** screen, complete the following fields:

a) Expand **EMC Unity File System**, check the file system that you want to associate with the share, and then click **Validate**.

b) For the **Use Snapshot** check box, do the following:

- To use an SMB server to create the share, do not check the box.
- To use a snapshot to create the share, check the box.

c) If you chose to use an SMB server, expand **Select SMB Server** and check the server that you want to use.

d) If you chose to use a snapshot, expand **Select Snapshot of File System** and check the snapshot that you want to use.

e) In the **Path** field, enter the absolute path of the SMB share relative to the NAS server.

If you do not provide a path, the share is created in the root directory.

f) Enter a description for the SMB share.

g) Check **Access-Based Enumeration** to filter the list of available files on the share and display only those to which the user has read access.
h) Check **Branch Cache Enabled** to cache content at branch offices to enable users to access the content locally.
i) Check **Protocol Encryption** to encrypt data as it is transmitted between the array and the host.
j) Check **Continuous Availability** to provide continuous access to the share after a failover of the NAS server.
k) From the **Offline Availability** drop-down list, choose one of the following options for client-side caching of offline files:

- **Manual**—Files are cached and available offline only when caching is explicitly requested. This is the default option.
- **Programs and files opened by users**—All files that clients open from the share are automatically cached and available offline. Clients open these files from the share when they are connected to it. This option is recommended for files with shared work.
- **Programs and files opened by users, optimize for performance**—All files that clients open from the share are automatically cached and available offline. Clients open these files from the share's local cache, if possible, even if they are connected to the network. This option is recommended for executable programs.
- **None**—Client-side caching of offline files is not configured.

l) In the **UMASK** field, enter the bitmask that shows which Unix permissions are excluded for files created on the share.

The default value of 022 does not allow write access from groups and other non-user entities.

Step 8 Click **Submit**.

Creating an NFS Share

An NFS share controls access to file system resources for Linux or Unix users and hosts.

Before you begin

Ensure that the file system or snapshot you choose for the share's souce is associated with a NAS server that supports the NFS profile

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC Unity account where you want to create an NFS share and click **View Details**.
Step 5 Click **NFS Shares**.
Step 6 Click **Create**.
Step 7 On the **Create NFS Share** screen, complete the following fields:
a) Expand the **EMC Unity File System** field, check the box for the file system you want to associate with the share, and click **Validate**.
b) Check the **Use Snapshot** box if you want to use a snapshot for the share.
c) If you chose to use a snapshot, expand the **Select Snapshot of File System** field and check the box for the snapshot you want to use.

d) In the **Path** field, enter the absolute path of the NFS share relative to the NAS server.

   If you do not provide a path, the share is created in the root directory.

e) From the **Default Access** drop-down list, choose the access that you want all hosts to have.

f) From the **Minimum Security** drop-down list, choose one of the following options:

   - **Sys**—This is the default option.
   - **Kerberos**—Uses basic Kerberos user authentication.
   - **Kerberos With Integrity**—Combines Kerberos user authentication and data integrity by adding a signature to each NFS packet transmitted over the network.
   - **Kerberos with Encryption**—Combines Kerberos user authentication and data privacy by encrypting the data before sending it over the network. Data encryption requires more resources for system processing and can lead to slower performance.

g) To customize access for hosts, expand one or more of the following fields and check the desired hosts to configure the access privileges for the share:

   - **No Access Hosts**
   - **Read Only Hosts**
   - **Read Write Hosts**
   - **Root Access Hosts**

Step 8 Click **Submit**.

Mapping a Host to an NFS Share

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to map an NFS share and click **View Details**.

Step 5 Click **NFS Shares**.

Step 6 Click **Map**.

Step 7 On the **Map Host to NFS Share** screen, complete the following fields:

a) From the **Host Access Type** drop-down list, choose the access that you want the host to have.

b) Expand **Hosts** and check each host you want to map to the share.

Step 8 Click **Submit**.

Unmapping a Host from an NFS Share

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC Unity account where you want to unmap an NFS share and click **View Details**.

Step 5 Click **NFS Shares**.

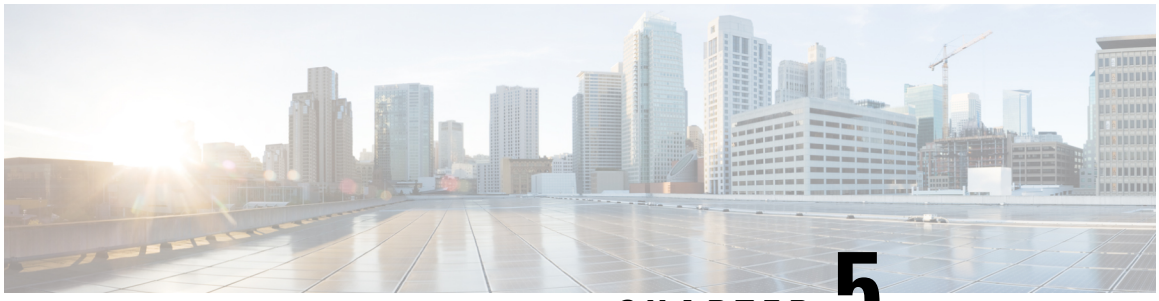
Step 6 Click **Unmap**.

Step 7 On the **Unmap Host from NFS Share** screen, complete the following fields:

a) From the **Host Access Type** drop-down list, choose the access that you do not want the host to have.

b) Expand **Hosts** and check each host you want to unmap from the share.

Step 8 Click **Submit**.



CHAPTER 5

EMC Symmetrix VMAX, VMAX3, and PowerMax

Cisco UCS Director Support for EMC Symmetrix VMAX, VMAX3, and PowerMax

Cisco UCS Director supports EMC Symmetrix VMAX, EMC Symmetrix VMAX3, and EMC Symmetrix PowerMax. Specific information on supported models, supported software, and supported management interfaces can be found in the Cisco UCS Director Compatibility Matrix for this release.

Cisco UCS Director connects to EMC VMAX using a supported EMC Solutions Enabler.

VMAX, VMAX3, and PowerMax Reports

Cisco UCS Director provides you with a view into the managed VMAX, VMAX3, and PowerMax storage systems. Some of these reports do not update automatically. You must click **Refresh** to view updated information.

VMAX and PowerMax Summary Reports

You can see at a glance the following VMAX and PowerMax summary reports:

- System capacity—Free vs. used (GB) pie chart
- System overview—Symmetrix version ID, Enginuity build version, model, Solutions Enabler IP address, and number of engines, directors, thin devices, data devices, director ports, and disks.
- Storage—Total capacity, used capacity, and free capacity

VMAX and PowerMax Component and Feature Reports

You can access reports and create VMAX and PowerMax components, such as devices, views, pools, and groups. You can drill down to view details for each component and feature, including the following:

- **Thin Pools**—Name. This is not used in VMAX3 and PowerMax.
- **Data Devices**—Device count, capacity (GB), emulation, configuration, and disk group. **Note:** This device is not used in VMAX3 and PowerMax.
- **Regular Devices**—Device count, disk group, emulation, configuration, capacity type, capacity. **Note:** This device is not used in VMAX3 and PowerMax.
- **Thin Devices**—Device count, capacity (GB), emulation, bind to thin pool (on or off), and option to preallocate 100 percent.
- **Meta Devices**—Device type, select regular or thin device, meta type, select member device. **Note:** This device is not used in VMAX3 and PowerMax.
- **Initiator Groups**—Group type (standard or cascaded), group name, type (iSCSI, FCP), and initiator name. Consistent logical unit number (LUN) can be set to on or off.
- **Storage Groups**—Storage group, storage group count, volume count, masking view, storage capacity, isparent/isccild, parent storage, child storage, masking view, FAST managed, SRP, SLO, workload type.
- **Port Groups**—Group name and director port selection (all, none, or selected).
- **Masking Views**—View name, storage group selection, host LUN ID (specified or autogenerated), initiator group selection, and port group selection.
- **Fast SRP**— Has Associated Disk Group, Storage Group Demand, and SLO Demand Report as drilldown reports. This is used only in VMAX3 and PowerMax.
- **Fast SLO**—This report contains a 'Rename' action that renames the SLO name. Has FAST SLO workload report as a drilldown report. This is used only in VMAX3 and PowerMax.
- **Tiers**—Tier name, tier type, emulation, target protection, number of ports and directors, technology, disk location, and type. This is not used in VMAX3 and PowerMax.
- **FAST Policies**—Policy name, tiers, number of tiers, number of storage groups, and emulation. **Note:** This object is not used in VMAX3 and PowerMax.

VMAX and PowerMax System Reports

The read-only VMAX and PowerMax system reports include the following information:

- **Front-End Directors**—Symmetrix ID, director module, status, type, identification, and number of ports, directors, mapped volumes, and engine ID.
- **Back-End Directors**—Symmetrix ID, director module, status, type, identification, and number of ports, directors, mapped volumes, and engine ID.
- **Director Ports**—Director module, type, port, port ID, maximum speed, node WWN, and ACLX option for each port.
- **Disk Groups**—Disk group name, technology, disk location, disks, total capacity, used capacity, free capacity, tags.

- **Features**—Name, type, capacity (GB), and Serial Advanced Technology Attachment (SATA) drive capacity (GB).
- **Licenses**—Feature name, license type, and capacity type.
- **Initiators**—Initiator group, Challenge Handshake Authentication Protocol (CHAP) enablement, user port name, user node name, initiator, type, iSCSI name, common serial number, SPC2 protocol, SCSI support, environment, volume set addressing, and other data.
- **Memory**—Slot number and capacity.

EMC Solutions Enabler for VMAX Storage

To communicate with VMAX, Cisco UCS Director uses the EMC Solutions Enabler (SE). You must install a supported Windows-based or Linux-based EMC SE before you add your VMAX or VMAX3 storage system to Cisco UCS Director. PowerMax storage system supports only Linux-based EMC SE.

Windows-Based Solutions Enabler

Guidelines for SSHD Server Configuration

To set up an SSHD server, we recommend that you install Cygwin version 1.7.27, and use the SSH daemon on the host. Cygwin provides a Linux-like environment on Microsoft Windows. See Installing a Cygwin Package, on page 51 for information on downloading Cygwin and additional information about the SSHD server.

After you install the SSHD server on the Windows-based SE, modify the Path variable under System Variables to include the Solutions Enabler bin folder so that whoever uses SSH to get into the Windows SE can immediately run VMAX commands. After you install and configure the SSHD server, set up the new default paths to enable the user-installed software to override the system software.

Installing a Cygwin Package

Ensure that you install the packages fir Cygwin version 1.7.27 on a Windows-based host.

Step 1 Download the Cygwin executable from http://www.cygwin.com/.

Step 2 While installing the Cygwin package on the package selection screen, select the **openssh** and **openssl** packages to install.

Configuring the SSHD Server

Step 1 Navigate to the `C:\<Cygwin-Install-Dir>` directory, open the `Cygwin.bat` in edit mode using any editor and add the following line: `set CYGWIN=binmode ntsec`

The following example shows the Cygwin.bat file contents after adding the line above:

```
@echo off
            C:
            chdir C:\<Cygwin-Install-Dir>\bin
```

```
set CYGWIN=binmode ntsec
bash --login -i
```

Step 2 Configure the SSHD service by running the `C:\<Cygwin-Install-Dir>\Cygwin.bat` file in a command prompt and enter the following command: `$ ssh-host-config`.

a) Answer the following questions:

Question	Recommended Response
Should privilege separation be used? <yes/no>	Select yes.
New local account 'sshd'? <yes/no>	Select yes.
Do you want to install sshd as a service? <yes/no>	Select no if SSHD is already installed as a service, otherwise select yes.
Enter the value of CYGWIN for the deamon: [ ] binmode ntsec	Enter the value as binmode ntsec
Do you want to use a different name? (yes/no)	Select yes.
Enter the new username: <new-username>	Enter the new username.
Reenter: <new-username>	Renter the new username.
Replace cloupia with new-username ? (yes/no)	Select yes.
Please enter the password: <password>	Enter the password for this account.
Reenter: <password>	Reenter the password for this account.

Configuring System Environment Variables

Step 1 Right-click the **Computer** icon and select **Properties**.

Step 2 If you don't have a computer icon on your desktop:

a) Click the **Start** button.
b) Right-click the **Computer** option in the Start menu.
c) Select **Properties**.

Step 3 Click **Advanced System Settings**.

Step 4 Under the **Advanced** tab, select **Environment Variables**.

Step 5 Under **System Variables** select the **Path** variable and append the following two binary paths: `c:\Program Files\EMC\SYMCLI\bin;c:\<Cygwin-Install-Dir>\bin`

Refer to the following example:

```
Variable Name: Path
     Variable Value: <Existing Folders Path>;c:\Program Files\EMC\SYMCLI\bin;c:\cygwin
     64\bin
```

Step 6 Add the following new **System Variable** name: `CYGWIN` and the following **Variable Value**: `binmode tty ntsec`

Starting the Cygwin SSHD Service

Step 1 Start the Cygwin SSHD service manually under Window Services.

Step 2 Configure the service to start automatically on every boot.

Verifying SSH Access

Before you begin

Ensure that you can run the SYMCLI commands without providing the absolute path at the command prompt. You can verify SSH access using any SSH client.

Step 1 Access a different machine that has an SSH client running and execute the following command: `ssh<USERNAME>@<host-ipaddress> 'date'` or `ssh-1<USERNAME>@<host-ipaddress> 'date'`

Example:

For example, execute `ssh -l pjohn@host-ipaddress 'date'`

Step 2 When the command prompts you, enter the password.

After you enter the correct password, the command returns the accurate date.

Installing and Configuring a Linux-Based Solutions Enabler

Note You can add libraries and legacy libraries, such as glibc, to the VM.

You need gatekeepers to serve as Raw Device Mappings (RDMs). Allow 6,000 to 8,000 mappings for each RDM.

Step 1 Create the base Linux image for the VM you will use.

For the base Linux image, you can use an SMC or SPA servers that run CentOS, version 5.7 x86, or x86_64. For an SMC server, allow 20 GB of space. For an SPA server, allow at least 120 GB.

Step 2 Assign a few gatekeepers as RDMs.

Step 3 Reboot the Linux VM.

Step 4 From the EMC Powerlink site, download the EMC Solutions Enabler package for Linux and the Services Management Application System (SMAS) package `se7310-Linux-i386-ni.tar.gz`.

Note See the Cisco UCS Director Compatibility Matrix to identify which version to download and install.

Use MD5 Checksum `9809ac14ed8bfcc19789d7d5671d6015`.

Step 5 Using SCP, transfer the tar file to your VM.

Step 6 At a command prompt, enter the following command to decompress the tar file: `[root@smc ~]# tar xzvf se7310-Linux-i386-ni.tar.gz`

Step 7 Install the EMC Solutions Enabler by entering the following command: `[root@smc ~]# ./se7310_install.sh -install]`

Step 8 Verify that the **`emc/symcli`** bin folder is in the Linux path, with this directory structure: `<symcli path>/bin`. An example is: **`/opt/emc/symcli/bin`**.

Step 9 To connect to the VMAX device from Cisco UCS Director, you must update the PATH variable with the SYMCLI binary dir by updating the .bashrc file for the user that logs in to VMAX.

a) Log in to the Solutions Enabler machine with the credentials that Cisco UCS Director will use.

b) Edit `.bashrc` using your editor of choice; for example, `vi .bashrc`

c) Add the following line to the .bashrc file:

```
PATH=$PATH:$HOME/bin:<symcli binary path>/bin
```

d) Save the file and exit.

Adding an EMC VMAX Account

Before you begin

You must install an EMC VMAX Solutions Enabler on a Linux or Windows Virtual Machine (VM).

Note If you have Solutions Enabler 8.0 installed, when adding an EMC VMAX account, all Symmetrix device names are padded with a zero. This may cause issues with rollback operations for tasks that were executed against an older version of Solutions Enabler.

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

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

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, complete the following fields:

Name	Description
Pod drop-down list	Choose a Pod for this account.
Category drop-down list	Choose **Storage**.

Name	Description
Account Type drop-down list	Choose **EMC VMAX** .

Step 5 Click **Submit**.

Step 6 In the second **Add Account** dialog box, complete the following fields:

Name	Description
Account Name field	A unique name for the account.
Description field	The account description.
Server Address field	The Solution Enabler IP address for the VMAX device.
Use Credential Policy check box	Check this box if you want to use a credential policy for this account rather than enter the username and password information manually.
Credential Policy drop-down list	If you checked **Use Credential Policy**, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
User ID field	The user ID that this account uses to access the VMAX or VMAX3 storage system. This user ID must be a valid account in the storage system. This field is not displayed if you chose to use a credential policy.
Password field	The password associated with the user ID. This field is not displayed if you chose to use a credential policy.
Transport Type drop-down list	Choose **SSH**.
Port field	The port number. The default port is 22.
Symmetrix id field	The Symmetrix ID can be manually entered or selected from a drop-down box that is shown if the Discover Symmetrix Arrays check box is selected.
Discover Symmetrix Arrays check box	If this box is checked, selection of the Symmetrix id can be done from the drop-down list that is shown.
Symmetrix id field	The ID of the Symmetrix array. If you checked **Discover Symmetrix Arrays**, this field becomes a drop-down list of the available arrays.
Contact field	The contact's email address.
Location field	The location for this account.

Step 7 Click **Submit**.

Cisco UCS Director tests the connection to the EMC Symmetrix VMAX or VMAX3 storage system. If that test is successful, it adds the respective VMAX account and discovers all infrastructure elements in the storage system that are associated with that account. This discovery process and inventory collection cycle takes few minutes to complete.

VMAX Management

In a Cisco UCS Director EMC VMAX account, you manage the following pools, groups, devices, and views:

- Thin pools—Create or delete, expand, bind or unbind, and view details
- Devices—data devices, thin devices, regular devices, BCV devices, and meta devices
- Initiator groups—Create or delete, rename, add or remove initiator, replace initiator, set override flags, and view details
- Storage groups—Create or delete, rename, add or remove device, associate/disassociate FAST policy, and view details
- Port groups—Create or delete, rename, add or remove port, and view details
- Masking views—Create or delete, rename, and view details

Thin Devices

The maximum size of a thin device (TDEV) in VMAX and PowerMax is 240 GB and 65536 GB respectively.

Note If you want to create a TDEV greater than this size, combine TDEVs to form a meta device. Each TDEV can be part of only one meta device.

There is no rename action for a TDEV. The device name is unique and remains the same even if the TDEV becomes a meta device and vice versa.

Creating a Thin Device

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to create a thin device.
Step 5 Click **View Details**.
Step 6 Click **Thin Devices**.
Step 7 Click **Create**.
Step 8 On the **Create Thin Device** screen, complete the following fields:

Name	Description
Device Count field	The thin device count.
Emulation drop-down list	Choose the emulation type for the thin device.
Capacity Type field	Select GB, MB, or Cylinder.
Capacity field	Number of GB, MB, or Cylinders.

Step 9 Click **Submit**.

What to do next

You can select a device and click **View Details** to see the drill-down report.

Thin Pools

An EMC VMAX thin pool is a collection of data devices that provide storage capacity for thin devices. A new thin pool requires a unique name.

Creating A Thin Pool

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to create the thin pool.
Step 5 Click **View Details**.
Step 6 Click **Thin Pools**.
Step 7 Click **Create**.
Step 8 On the **Create Thin Pool** screen, enter a name in the **Thin Pool Name** field and click **Submit**.

Binding Thin Devices to a Thin Pool

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account with the thin pool where you want to bind thin devices.
Step 5 Click **View Details**.
Step 6 Click **Thin Pools**.
Step 7 Click **Bind**.
Step 8 On the **Bind Symmetrix Device** screen, complete the following fields:

Name	Description
Select Thin Devices select list	Check the box for the thin devices that you want to bind.
Pre Allocate All check box	Check this box if you want to pre-allocate all thin devices.
Capacity Type field	Select the capacity unit in GB, MB, or Cylinder. This field is only available if you checked **Pre Allocate All**.
Pre Allocate Size field	The pre-allocation size in GB, MB, or Cylinders. **Note** The Pre Allocate Size option is not available for Symmetric CLI version 8.0, it is only available for version 7.6.1.0. This field is only available if you checked **Pre Allocate All**.

Step 9 Click **Submit**.

Unbinding a Thin Devices from a Thin Pool

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account with the thin pool where you want to unbind thin devices.
Step 5 Click **View Details**.
Step 6 Click **Thin Pools**.
Step 7 Click **UnBind**.
Step 8 On the **UnBind Thin Device from Thin Pool** screen, complete the following fields:

Name	Description
Select Thin Devices select list	Check the box for the thin devices that you want to unbind.
Force check box	Forces unbinding of the selected thin devices.

Step 9 Click **Submit**.

BCV Devices

A business continuity volume (BCV) is a symmetrix device with special attributes. A BCV device can function either as an additional mirror or as a separate host addresable volume.

Creating a BCV Device

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to create the BCV device.
Step 5 Click **View Details**.
Step 6 Click **BCV Devices**.
Step 7 Click **Create**.
Step 8 On the **Create BCV Device** screen, complete the following fields:

Name	Description
Device Count field	The BCV device count.
Emulation drop-down list	Choose the emulation type for the BCV device.
Configuration drop-down list	Choose the configuration for the BCV device.
Capacity Type field	Select GB, MB, or Cylinder.
Capacity field	Number of GB, MB, or Cylinders.

Step 9 Click **Submit**.

Data Devices

Data devices provide the physical space that is used by thin pools on a VMAX system.

Creating a Data Device

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to create a data device.
Step 5 Click **View Details**.
Step 6 Click **Data Devices**.
Step 7 Click **Create**.
Step 8 On the **Create Data Device** screen, complete the following fields:

Name	Description
Device Count field	The data device count.
Disk Group field	The disk group name.

Name	Description
Emulation drop-down list	Choose the emulation type for the data device.
Configuration field	Choose the configuration for the data device.
Capacity Type field	Choose the capacity unit in GB, MB, or Cylinder.
Capacity field	The capacity in GB, MB, or Cylinders.

Step 9 Click **Submit**.

Regular Devices

The maximum size of a VMAX regular device is approximately 240 GB.

Note If you want to create a regular device greater than this size, combine regular devices to form a meta device. Each regular device can be part of only one meta device.

There is no rename action for a regular device. The device name is unique and remains the same even if the regular device becomes a meta device and vice versa.

Creating a Regular Device

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to create a regular device.
Step 5 Click **View Details**.
Step 6 Click **Regular Devices**.
Step 7 Click **Create**.
Step 8 On the **Create Regular Device** scrreen, complete the following fields:

Name	Description
Device Count field	The regular device count.
Disk Group select button	Select the Disk Group
Emulation drop-down list	Choose the emulation type for the regular device.
Configuration drop-down	Choose the configuration.
Capacity Type field	Choose GB, MB, or Cylinder.
Capacity	Number of GB, MB, or Cylinders.

Step 9 Click **Submit**.

Meta Devices

A meta device enables you to aggregate thin devices or regular devices to increase the device size.

You can create a meta device with a thin device as the head and create other thin devices as members, or you can create a meta device with a regular device as the head and create other regular devices as members. The total meta device size is the combination of the head size and all the member device sizes.

Note There is no delete action for a meta device. Removing all of the members from a meta device results in a thin device.

Meta Member Devices

A meta member device (also referred to as a Meta LUN) is a LUN that is composed of several elements (LUNs). Meta member devices are similar to private LUNs. A meta member device is used by the system and is not available directly to any host. For example, you cannot place a meta member device into a storage group.

The following are the supported types of meta member devices:

- Concatenated Meta LUN—Creates a larger LUN from several smaller LUNs. This member device is recommended when performance is not a high priority.
- Striped Meta LUN—Creates a higher performance LUN. For example, you might want to use this type of LUN for a large file system or a database.

Creating a Meta Device

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to create a meta device.
Step 5 Click **View Details**.
Step 6 Click **Meta Devices**.
Step 7 Click **Create Meta**.
Step 8 On the **Create Meta Device**screen, complete the following fields:

Name	Description
Select Device Type drop-down list	Choose the types of devices that you want to add to the meta device. These device combinations can include the following: • Thin devices only • Regular devices only • BCV devices and thin devices (BCV+TDEV) • BCV and regular devices (BCV+R) The other fields that display on this screen depend upon which types of devices you choose.
Select Thin Device field	If you chose to include thin devices only, choose the devices you want to add to the meta device.
Select Regular Device field	If you chose to include regular devices only, choose the devices you want to add to the meta device.
Select BCV Thin Device field	If you chose BCV+TDV, choose the devices you want to add to the meta device.
Select BCV Regular Device field	If you chose BCV+R, choose the devices you want to add to the meta device.
Select Meta Type drop-down list	Choose the type of meta device you want to create.
Select Member Device(s) field	Choose the device or devices to include in the meta device.

Step 9 Click **Submit**.

Adding a Member Device to a Meta Device

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to update a meta device.
Step 5 Click **View Details**.
Step 6 Click **Meta Devices**.
Step 7 Click the row with the meta device to which you want to add a member device.
Step 8 Click **Add Device to Meta**.
Step 9 On the **Add Device to Meta** screen, choose the device that you want to add and click **Submit**.

Removing a Member Device from a Meta Device

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to update a meta device.
Step 5 Click **View Details**.
Step 6 Click **Meta Devices**.
Step 7 Click the row with the meta device from which you want to remove a member device.
Step 8 Click **Remove Device from Meta**.
Step 9 On the **Remove Device from Meta** screen, choose the device that you want to remove from the meta device and click **Submit**.

Dissolving a Meta Device

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to update a meta device.
Step 5 Click **View Details**.
Step 6 Click **Meta Devices**.
Step 7 Click the row with the meta device that you want to dissolve.
Step 8 Click **Dissolve**.
Step 9 Click **Submit**.

Adding a Member Device to a Meta Device (Striped Configuration)

If the meta device has a striped configuration, you need to complete two additional fields in the configuration.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to update a meta device.
Step 5 Click **View Details**.
Step 6 Click **Meta Devices**.
Step 7 Click the row with the striped meta device to which you want to add a member device.
Step 8 Click **Add Device to Meta**.
Step 9 On the **Add Device to Meta** screen, complete the following fields:

Name	Description
Select Member Device(s) field	Choose the member device(s) that you want to add to the meta device.
Protect Data check box	Check this box if you want to enable data protection on the devices.
Select BCV Meta Devicefield	Choose a BCV meta device head node for the meta device.

Step 10 Click **Submit**.

Initiator Groups

A VMAX or PowerMax initiator group is a collection of host bus adapters (HBAs) that work together. Initiator groups that contain other initiator groups are known as cascaded initiator groups.

Creating an Initiator Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX or EMC PowerMax account where you want to add an initiator group.
Step 5 Click **View Details**.
Step 6 Click **Initiator Group**.
Step 7 Click **Create**.
Step 8 On the **Create Initiator Group** screen, do the following:

a) From the **Initiator Group Type** drop-down list, choose one of the following initiator group types:
- **Standard**—if the initiator group will contain initiators. This is the default option.
- **Cascaded**—if the initiator group will contain other initiator groups.

b) In the **Initiator Group Name** field, enter a unique name for the initiator gorup.
c) If you chose to create a standard initiator group, complete the following fields:

Name	Description
Initiator Type drop-down list	Choose one of the following: • **iSCSI** • **FCP** **iSCSI** is the default initiator type.
Initiator Name field	A unique name for the initiator.
Consistent LUN check box	Check this box if you want to use a consistent LUN. Unchecked is the default.

d) If you chose to create a cascaded initiator group, complete the following fields:

Name	Description
Select Parent Initiator Group field	Choose the parent initiator group from the list.
Select Child Initiator Group field	Choose a child initiator group from the list.

e) Click **Submit**.

Storage Tiers

Tiered storage allows you to assign different categories of data to different types of storage media to reduce your total storage cost and maintenance.

Creating a Storage Tier

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC VMAX account where you want to create a storage tier.

Step 5 Click **View Details**.

Step 6 Click **Storage Tiers**.

Step 7 Click **Create**.

Step 8 On the **Create Storage Tier** screen, complete the following fields:

Name	Description
Storage Tier Name field	A unique name for the storage tier.
Storage Tier Type drop-down list	Choose one of the following tier types: • **Disk Group Provisioned** • **Virtual Provisioned**
Include Type drop-down list	Choose one of the following include types: • **Static** • **Dynamic**

Name	Description
Configuration Type drop-down list	Choose one of the following configuration types: • **RAID-1** • **RAID-5 (3+1)** • **RAID-5 (7+1)** • **RAID-6(6+2)** • **RAID-6(14+2)**
Select Technology drop-down list	Choose one of the following: • **EFD** • **FC** • **SATA**
Select Disk Group field	Choose a disk group.
Bind to Thin Pool field	Choose the thin pool where you want to bind the storage tier. This option is only available if you chose **Virtual Provisioned** as the Storage Tier Type.
Externally Provisioned check box	Check this box if you want to be able to externally provison the storage tier. This option is only available if you chose **Virtual Provisioned** as the Storage Tier Type.

Step 9 Click **Submit**.

Adding a Thin Pool to a Storage Tier

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to update the storage tier.
Step 5 Click **View Details**.
Step 6 Click **Storage Tiers**.
Step 7 Click the row with the storage tier that you want to update.
Step 8 Click **Add Thin Pool**.
Step 9 On the **Add Thin Pool to Storage Tier** screen, choose the thin pool that you want to add and click **Submit**.

Removing a Thin Pool from a Storage Tier

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to update the storage tier.
Step 5 Click **View Details**.
Step 6 Click **Storage Tiers**.
Step 7 Click the row with the storage tier that you want to update.
Step 8 Click **Remove Thin Pool**.
Step 9 On the **Remove Thin Pool** screen, choose the thin pool that you want to remove and click **Submit**.

Adding a Disk Group to a Storage Tier

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to update the storage tier.
Step 5 Click **View Details**.
Step 6 Click **Storage Tiers**.
Step 7 Click the row with the storage tier that you want to update.
Step 8 Click **Add Disk Group**.
Step 9 On the **Add Disk Group** dialog box, complete the following fields:

Name	Description
Select Disk Group field	Choose a disk group to be added to the storage tier.
Propogate check box	If checked, propagates changes to all storage tiers.

Step 10 Click **Submit**.

Renaming a Storage Tier

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to update the storage tier.
Step 5 Click **View Details**.
Step 6 Click **Storage Tiers**.

Step 7 Click the row with the storage tier that you want to rename.

Step 8 Click **Rename**.

Step 9 On the **Rename Storage Tier** screen, enter the new name for the storage tier and click **Submit**.

Deleting a Storage Tier

You can force the deletion of a storage tier, even if that tier includes disk groups and thin pools.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC VMAX account that contains the storage tier you want to delete.

Step 5 Click **View Details**.

Step 6 Click **Storage Tiers**.

Step 7 Click the row with the storage tier that you want to delete.

Step 8 Click **Delete**.

Step 9 On the **Delete Storage Tier** screen, check the **Force** box if you want to delete the storage tier even if it includes thin pools and disk groups, and then click **Submit**.

Storage Groups

A VMAX or PowerMax storage group is a collection of Symmetrix logical volumes that are used by an application, a server, or a collection of servers.

Storage groups present storage to hosts and are also used for FAST policies.

In Cisco UCS Director, you can create VMAX or PowerMax storage groups that are either Empty or Cascaded. A cascaded group contains other storage groups. You can contain a cascaded storage group within a masking view to present storage resources to an entire cluster.

Creating an Empty Storage Group

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the account where you want to create a storage group.

Step 5 Click **View Details**.

Step 6 Click **Storage Groups**.

Step 7 Click **Create**.

Step 8 On the **Create Storage Group** screen, complete the following fields:

Name	Description
Storage Group Type drop-down list	Choose the default option **Empty Storage Group**.
Storage Group Name field	A unituq name for the storage group.
Storage Resource Pool field	Select FAST SRP to associate to storage group. This field is required for VMAX3 or PowerMax storage groups.
Storage Level Objective field	Select SLO to associate to storage group. This field is required for VMAX3 or PowerMax storage groups.

Step 9 Click **Submit**.

Creating a Cascaded Storage Group

Before you begin

Create a parent storage group and one or more child storage groups.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the account where you want to create a storage group.
Step 5 Click **View Details**.
Step 6 Click **Storage Groups**.
Step 7 Click **Create**.
Step 8 On the **Create Storage Group** screen, complete the following fields:

Name	Description
Storage Group Type drop-down list	Choose **Cascaded Storage Group**.
Select Parent Storage Group field	The parent storage group.
Child Storage Group field	The child storage group.

Step 9 Click **Submit**.

What to do next

Add devices and associate FAST policies with the storage group.

Deleting a Storage Group

You can force the deletion of a storage group, even if that group includes devices.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the account where you want to delete a storage group.
Step 5 Click **Delete**.
Step 6 On the **Delete Storage Group** dialog box, check the **Force** box if you want to delete the storage tier even if it includes devices, and then click **Submit**.

Renaming a Storage Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the account where you want to update a storage group.
Step 5 Click **View Details**.
Step 6 Click **Storage Groups**.
Step 7 Click **Rename**.
Step 8 In the **Rename Storage Group** dialog box, enter a unique name for the storage group and click **Submit**.

Adding a Device to a Storage Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the account where you want to update a storage group.
Step 5 Click **View Details**.
Step 6 Click **Storage Groups**.
Step 7 Click the row with the storage group that you want to update.
Step 8 Click **Add Device**.
Step 9 On the **Add Devices to Storage Group** screen, complete the following fields:

Name	Description
Device Type drop-down list	Choose one of the following options: • **Thin Device** • **Regular Device**—not available for VMAX3 or PowerMax storage groups.
Select Devices field	Choose one or more devices to add to the storage group.

Name	Description
Host LUN ID field	If you do not specify a host LUN ID, it is auto generated in HEXA.

Step 10 Click **Submit**.

Removing a Device from a Storage Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the account where you want to update a storage group.
Step 5 Click **View Details**.
Step 6 Click **Storage Groups**.
Step 7 Clck the row with the storage group that you want to update.
Step 8 Click **Remove Device**.
Step 9 On the **Remove Device** screen, choose the device that you want to remove from the storage groupa and click **Submit**.

Removing a Child Storage Group from a Cascaded Storage Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the account where you want to update a storage group.
Step 5 Click **View Details**.
Step 6 Click **Storage Groups**.
Step 7 Click the row with the cascaded storage group that you want to update.
Step 8 Click **Remove Storage Group**.
Step 9 On the **Remove Child Storage from Parent Storage** screen, choose the child storage group that you wan tto remove and click **Submit**.

FAST Configuration for Storage Groups on VMAX

Associating a FAST Policy with a Storage Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the account where you want to update a storage group.
Step 5 Click **View Details**.
Step 6 Click **Storage Groups**.
Step 7 Click the row with the storage group that you want to update.
Step 8 Click**Associate FAST Policy**.
Step 9 On the **Associate FAST Policy to Storage Group** screen, complete the following fields:

Name	Description
Select FAST Policy field	Choose the FAST policy that you want to associate with the storage group.
Storage Group Priority field	Set the priority for the storage group. The valid range for the priority is from 1 to 3.

```
```

Step 10 Click **Submit**.

Disassociating a FAST Policy from a Storage Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the account where you want to update a storage group.
Step 5 Click **View Details**.
Step 6 Click **Storage Groups**.
Step 7 Click the row with the storage group that you want to update.
Step 8 Click **Disassociate FAST Policy**.
Step 9 Click **Submit**.

Reassociating a FAST Policy with a Storage Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the account where you want to update a storage group.
Step 5 Click **View Details**.
Step 6 Click **Storage Groups**.
Step 7 Click the row with the storage group that you want to update.
Step 8 Click **Reassociate FAST Policy**.
Step 9 On the **Reassociate FAST Policy to Storage Group** screen, choose the FAST policy that you want to reassociate with the storage group and click **Submit**.

Modifying the FAST Storage Group Priority

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the account where you want to update a storage group.
Step 5 Click **View Details**.
Step 6 Click **Storage Groups**.
Step 7 Click the row with the storage group that you want to update.
Step 8 Click **Modify Fast Priority**.
Step 9 On the **Modify FAST Storage Group Priority** dialog box, choose the new FAST priority for the storage group and click **Submit**.

The valid range for the priority is from 1 to 3.

Modifying FAST Settings for a Storage Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the account where you want to update a storage group.

Note This is supported only for EMC VMAX3 and EMC PowerMax.

Step 5 Click **View Details**.
Step 6 Click **Storage Groups**.
Step 7 Click the row with the storage group that you want to update.
Step 8 Click **Modify Fast Settings**.
Step 9 On the **Modify FAST Settings** screen, complete the following fields:

Name	Description
Storage Resource Pool	Select a new storage resource pool for the storage group.
Service Level Objective	Select the new service level objective for the storage group.

Step 10 Click **Submit**.

Fully Automated Storage Tiering

Fully Automated Storage Tiering (FAST) automatically moves data between storage tiers. For example, FAST can do the following:

- Move very active data to high-performance storage tiers

- Move inactive data to low-cost, high-capacity storage tiers

FAST policies dictate how the performance and cost are optimized for the associated storage tier while the automation of FAST means that your storage system has no added management constraints compared with slower and more expensive systems. A FAST system always monitors and identifies the current activity levels of your data and moves the active data and inactive data to the most appropriate storage tier (according to your policies).

FAST Policies

A FAST policy is a set of tier usage rules that you can apply to your storage groups. A FAST policy can include up to three tiers and assigns an upper usage limit for each tier. The usage limit specifies the maximum percentage of the storage group that the FAST controller can allocate to a particular tier. Policy settings allow you to control and manage automated activity.

Creating a FAST Policy

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC VMAX account where you want to create a FAST policy.

Step 5 Click **View Details**.

Step 6 Click **Fast Policies**.

Step 7 Click **Create**.

Step 8 On the **Create FAST Policy** screen, complete the following fields:

Name	Description
Fast Policy Name field	A unique name for the FAST policy.
Storage Tier Name field	Choose up to three storage tiers that you want to associate with this FAST policy.
Max Storage Group Capacity of Tier (%) field	Specify the maximum percentage of the storage group that the FAST controller can allocate to the storage tier The valid range is from 1 to 100, as a percentage of the total storage group capacity.

Step 9 Click **Submit**.

Adding Storage Tiers to a FAST Policy

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC VMAX account where you want to update a FAST policy.

Step 5 Click **View Details**.

Step 6 Click **Fast Policies**.

Step 7 Click the row with the FAST policy that you want to update.

Step 8 Click **Add Storage Tiers**.

Step 9 On the **Add Storage Tiers to Fast Policy** screen, complete the following fields:

Name	Description
Select Storage Tier field	Choose the storage tier that you want to associate with this FAST policy.
Max Storage Group Capacity of Tier (%) field	Specify the maximum percentage of the storage group that the FAST controller can allocate to the storage tier The valid range is from 1 to 100, as a percentage of the total storage group capacity.

Step 10 Click **Submit**.

Removing Storage Tiers from a FAST Policy

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC VMAX account where you want to update a FAST policy.

Step 5 Click **View Details**.

Step 6 Click **Fast Policies**.

Step 7 Click the row with the FAST policy that you want to update.

Step 8 Click **Remove Storage Tiers**.

Step 9 On the **Remove Storage Tiers From Fast Policy** screen, choose the storage tier that you want to remove and click **Submit**.

Modifying the Maximum Storage Group Capacity for a Storage Tier in a FAST Policy

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC VMAX account where you want to update a FAST policy.

Step 5 Click **View Details**.

Step 6 Click **Fast Policies**.

Step 7 Click the row with the FAST policy that you want to update.

Step 8 Click **Modify Storage Tiers**.

Step 9 On the **Modify Storage Tiers in a Fast Policy** screen, complete the following fields:

Name	Description
Select Storage Tier field	Choose the storage tier that you want to modify.

Name	Description
Max Storage Group Capacity of Tier (%) field	Change the maximum percentage of the storage group that the FAST controller can allocate to the storage tier The valid range is from 1 to 100, as a percentage of the total storage group capacity.

Step 10 Click **Submit**.

Renaming a FAST Policy

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to update a FAST policy.
Step 5 Click **View Details**.
Step 6 Click **Fast Policies**.
Step 7 Click the row with the FAST policy that you want to rename.
Step 8 Click **Rename**.
Step 9 On the **Rename FAST Policy** screen, enter the new FAST policy name and click **Submit**.

FAST Controllers

FAST can be configured to operate in the following modes:

- AUTO_APPROVE mode—Configuration change plans are generated and executed at the beginning of each inclusion device movement window based on the defined policy.
- USER_APPROVE mode—Configuration change plans are generated but not executed until they have been approved by a user. All change plans and data movements must be explicitly approved prior to being executed.

Modifying FAST Controller Settings

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to modify the FAST controller settings.
Step 5 Click **View Details**.
Step 6 Click **FAST Controller**.
Step 7 Click **Modify FAST Controller Setting**.
Step 8 On the **Modify FAST Controller Setting** screen, complete the following fields:

Name	Description
Data Movement Approval Mode drop-down list	Choose one of the following to determine how data movements will be approved: • **USER_APPROVE** • **AUTO APPROVE** USER APPROVE is the default setting.
Max Simultaneous Device Moves field	The number of maximum simultaneous device moves permitted. The valid range is 2 to 32.
Max Devices Moves Per Dayy field	The number of maximum simultaneous device moves permitted per day. The valid range is 2 to 200.
Min Initial Workload Period (hrs) field	The minimum initial workload period (in hours). The valid range is 2 to the current value.
Workload Analysis Period (hrs) field	The workload analysis period (in hours). The valid range is 2 to 672.
Swap Not Visible Devices drop-down list	Choose one of the following: • **Enable**—Permits the FAST controller to use configured but unmasked/unapped devices that are not visible to the host for FAST swaps. • **Disable**—FAST swaps can only happen between devices that belong to storage groups that are associated with a FAST policy.
Allow Only Swap drop-down list	Choose one of the following: • **Enable** the ability to swap only devices. • **Disable**
FAST VP Data Movement Mode drop-down list	Choose to enable or disable (None) the FAST VP Data Movement Mode. **Auto** is the default mode.
FAST VP Data Relocation Rate field	The FAST VP Data Relocation Rate value. The valid range is 1 to 10.
Thin Pool Reserved Capacity (%) field	The Thin Pool Reserved Capacity (%)) value. The valid range is 1 to 80.
VP Allocation By FAST policy field	Choose the Thin Pool Reserved Capacity (%) value. The default value is Enabled.
FAST VP Time to Compress (Days) field	The FAST VP Time to Compress (Days) value. The valid range is from 40 to 400 days or never.
FAST VP Compression Rate field	The FAST VP Time to Compress (Days) value. The valid range is from 1 to 10.

Step 9 Click **Submit**.

FAST Status

The FAST Status allows to you modify the FAST state of your storage tiers. You can choose one of the following types:

- Disk Group Provisioned
- Virtual Group Provisioned

Modifying the FAST State

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC VMAX account where you want to modify the FAST state.
Step 5 Click **View Details**.
Step 6 Click **FAST Status**.
Step 7 Click **Modify FAST State**.
Step 8 On the **Modify VMAX FAST State** screen, complete the following fields:

Name	Description
FAST Type drop-down list	Choose the desired **FAST Type** to change the state.
Enable check box	If checked, enables the FAST state.

Step 9 Click **Submit**.

Renaming the FAST Service Level Objective

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the account where you want to update the FAST SLO.
Step 5 Click **View Details**.
Step 6 Click **Fast Policies**.
Step 7 Click **FAST SLO**.
Step 8 Click **Rename**.
Step 9 On the **Rename FAST SLO Name** screen, enter a new SLO name and click **Submit**.

Port Groups

A VMAX or PowerMax port group is a collection of front-end ports.

Creating a Port Group

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC VMAX account where you want to create a port group.

Step 5 Click **View Details**.

Step 6 Click **Port Groups**.

Step 7 Click **Create**.

Step 8 On the **Create Port Group** screen, complete the following fields:

Name	Description
Port Group Name field	The port group name.
Select Port Group Name pop-up	Select the port(s) you want to include in the port group.
Select Items field	Chose the director port for the port group.

Step 9 Click **Submit.**

Masking Views

VMAX and PowerMax designate three types of auto-provisioning groups: storage groups, port groups, and initiator groups. These three groups work together as a masking view.

The masking view ensures that the target initiators in an initiator group can access the target storage resources in a storage group by means of the target ports in a port group.

Masking views are also useful for making changes to how the storage is presented. Changes to groups that belong to a masking view, such as adding a device or port, are automatically reflected in the masking view.

Creating a Masking View

Before you begin

You must create a storage group, initiator group, host LUN, and port group.

You must also attach devices to the storage group.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the account where you want to create a port group.

Step 5 Click **View Details**.

Step 6 Click **Masking Views**.

Step 7 Click **Create**.

Step 8 On the **Create Masking Views** screen, complete the following fields:

Name	Description
Masking View Name field	A unique name for the masking view.
Select Storage Group Name field	Choose the storage group you want to include in the masking view.
Host LUN ID field	The host LUN ID for the storage group. **Note** If you do not specify a LUN ID, the **Host LUN ID** is autogenerated.
Select Initiator Group Name field	Choose the initiator group you want to include in the masking view.
Select Port Group Namefield	Choose the port group you want to include in the masking view.

Step 9 Click **Submit**.

VMAX Properties File

You can configure certain parameters in the VMAX properties file (`vmax.properties`), which is located in the `/opt/infra/inframgr` folder.

Action or Task Retry Parameters

By default, the VMAX properties file is configured to automatically resubmit a service request or action if a workflow fails because too many tasks or actions are being executed simultaneously. This configuration reduces the level of user intervention required in this scenario.

Parameter	Description	Default Value
emc.vmax.retryMessages	The error message that displays if a workflow fails because too many tasks or actions are being executed simultaneously. If this error message is captured for a task or action, that task or action is automatically re-executed.	Default Error Message: `The SYMAPI database file is already locked by another process` **Note** To include nore than one message, enter comma-separated messages.
emc.vmax.maxIterationCount	The maximum number of attempts to be made if the VMAX response contains the message specified in the retryMessages property.	Default value: 20
emc.vmax.sleepTime	The time (in ms) that the retry operation waits before it connects to the VMAX device to execute the command.	Default value: 30000 ms (30 sec)

VMAX Sym Device Inventory Collection

By default, Cisco UCS Director collects the sym device inventory for every 500 devices. You can change this default in the VMAX properties file.

Parameter	Description	Default Value
emc.vmax.inventory.symdev.count	The number of VMAX devices for which inventory is collected. This parameter can be useful to reduce the inventory time required if the VMAX system has a large number of sym devices.	Default value: 500

Editing the VMAX Properties File

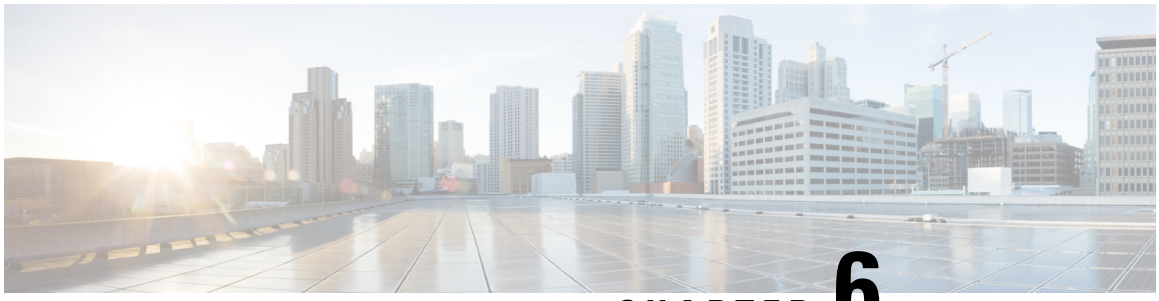
Step 1 In a terminal, log in to Cisco UCS Director with root credentials.

Step 2 Type `cd /opt/infra/inframgr` and press **Enter**.

Step 3 Type `vi vmax.properties` and press **Enter**.

Step 4 Change the desired property and save the file.

Your configuration changes are applied immediately.



CHAPTER 6

EMC VNX

About Cisco UCS Director for EMC VNX

Cisco UCS Director supports EMC VNX block, file, and unified storage accounts. Block supports block data, file supports file data, and unified supports both block and file data. See the Compatibility Matrix for all supported EMC VNX versions.

For a VNX Block account, you can manage the following:

- Block Storage Pools
- Storage Groups
- RAID Groups
- Host Initiators
- Logical Unit Numbers (LUNs)

The reports for VNX Block accounts also include details on all of these items, and on storage processors, ports, meta LUNs, hosts, ports, and disk devices.

For a VNX File account, you can manage the following:

- Data Movers
- Storage Pools for File
- Volumes
- Filesystems
- Common Internet File Servers (CIFS) servers
- Common Internet File Servers (CIFS) shares

- Network File System (NFS) exports
- Data Mover Interfaces
- DNS Domains

The reports available for VNX File accounts include details on the above items, and system overview summaries.

For a VNX File new account, you create either Common Internet File Servers (CIFS) or Network File System (NFS) Export.

For NFS Export, you create the following:

- Storage pools for files
- File systems
- Interfaces
- Volumes
- Mounts

For a VNX unified account, which combines VNX block and VNX file accounts, you can perform all the steps needed for both VNX block and VNX file accounts.

Installing EMC NaviSphere

To communicate with VNX, Cisco UCS Director supports Windows-based EMC NaviSphere and Linux-based EMC Navisphere.

Before using NaviSphere, you must install and configure a Secure Shell (SSH) server on it.

Installing and Configuring Windows-Based Navisphere

Installing a Cygwin Package

Ensure that you install the `openssh`, `openssl`, and `TCL` Cygwin packages on a Windows host.

Step 1 Download the Cygwin executable from http://www.cygwin.com/.

Step 2 While installing the Cygwin package on the package selection screen, choose the following packages:

- openssh
- openssl
- TCL

Guidelines for SSHD Server Configuration

To set up an SSHD server, we recommend that you install Cygwin version 1.7.27, and use the SSH daemon on the host. Cygwin provides a Linux-like environment on Microsoft Windows.

After you install the SSHD server on the Windows-based EMC NaviSphere, modify the Path variable under System Variables to include the NaviSphere `bin` folder. This update ensures that anyone who uses SSH to access Windows-based NaviSphere can execute VNX commands.

After you configure the SSHD server, set up new default paths to enable the user-installed software to override the system software.

Configuring the SSHD Server

Step 1 Navigate to the `C:\`*`Cygwin-Install-Dir`*`.` directory,

Step 2 Open the `Cygwin.bat` file in edit mode, using any editor, and add the following line: **`set CYGWIN=binmode ntsec`**

The following example shows the contents of the `Cygwin.bat` file after adding the above line:

```
@echo off
            C:
            chdir C:\<Cygwin-Install-Dir>\bin
            set CYGWIN=binmode ntsec
            bash --login -i
```

Step 3 Configure the SSHD service by running the `C:\`*`Cygwin-Install-Dir`*`\Cygwin.bat` file in a command prompt and enter the following command: `$ ssh-host-config`.

a) Answer the following questions:

Question	Recommended Response
Should privilege separation be used? <yes/no>	**`Yes`**
New local account 'sshd'? <yes/no>	**`Yes`**
Do you want to install sshd as a service? <yes/no>	**`No`** if SSHD is already installed as a service. **`Yes`** if SSH has not yet been installed as a service.
Enter the value of CYGWIN for the daemon: [ ] binmode ntsec	Enter the value as **`binmode ntsec`**
Do you want to use a different name? (yes/no)	**`Yes`**
Enter the new username: <new-username>	Enter the new username.
Reenter: <new-username>	Reenter the new username.
Replace cloupia with new-username? (yes/no)	**`Yes`**

Question	Recommended Response
Please enter the password: <password>	Enter the password for this account.
Reenter: <password>	Reenter the password for this account.

Configuring System Environment Variables

Step 1 On the Windows host, right-click the **Computer** icon on the desktop and choose **Properties**.

Step 2 If you don't have a computer icon on your desktop, do the following:

a) Click **Start**.
b) Right-click the **Computer** option in the Start menu.
c) Choose **Properties**.

Step 3 Click **Advanced System Settings**.

Step 4 On the **Advanced** tab, choose **Environment Variables**.

Step 5 Under **System Variables** choose the **Path** variable and append the following two binary paths: `c:\Program Files (x86)\EMC\Navisphere CLI;c:\<Cygwin-Install-Dir>\bin.`

The following is an example of the path variable with the binary paths added:

```
Variable Name: Path
     Variable Value: <Existing Folders Path>;c:\Program Files(x86)\EMC\Navisphere CLI;c:\cygwin 64\bin
```

Step 6 Add the following new system variable:

- System Variable Name: `CYGWIN`
- System Variable Value: `binmode tty ntsec`

Starting the Cygwin SSHD Service

Step 1 Start the Cygwin SSHD service manually under Window Services.

Step 2 Configure the Cygwin SSHD service to start automatically every time the computer is restarted.

Verifying SSH Access

Ensure that you can run the `naviseccli` commands without providing the absolute path at the command prompt. You can use any SSH client to verify SSH access.

Step 1 In your SSH client, access another machine that has the SSH client running and execute one of the following commands:

- `ssh USERNAME@host-ipaddress 'date'`
- `ssh -l USERNAME@host-ipaddress 'date'`

Example:

For example, `ssh -l user@host-ipaddress 'date'`

Step 2 Enter the password for the account when prompted.

After you enter the correct password, the command returns the current date.

Configuring the Navisphere Path for Windows

By default, Cisco UCS Director executes NavisecCLI commands with an explicit path that does not exist in Windows. You must create a softlink to that path through the Cygwin shell.

Step 1 Open the Cygwin shell on the Windows server where Navisphere is installed.

Step 2 In the Cygwin shell, create the following directory: `/opt/Navisphere`

Step 3 Create a softlink for the Navisphere directory.

Example:

For example. if you installed Navisphere in the `C:\Program Files (x86)\EMC\NavisphereCLI` directory, execute the following command to create a softlink:

```
ln -s /cygdrive/c/Program\ Files\ \(x86\)/EMC/NavisphereCLI /opt/Navisphere/bin
cd /opt/Navisphere/bin
chmod 775 NaviSECCli.exe
```

Installing and Configuring Linux Based NaviSphere

You must complete this step before you add a VNX Storage Array as an account in Cisco UCS Director.

Step 1 Search and download the `naviseccli` package for VNX from EMC Support for your specific platform.

For example, the package may be named:

```
NaviCLI-Linux-64-x86-en_US-7.33.2.0.51-1.x86_64.rpm
```

Step 2 If you are not logged in as root, enter the following command to switch to the root user: `su username`

Step 3 Install the `naviseccli` package using the `rpm` command.

For example, enter the following command:

```
rpm -i NaviCLI-Linux-64-x86-en_US-7.33.2.0.51-1.x86_64.rpm
```

Step 4 When you are prompted to enter a certificate verifying level, enter the verifying level as **`medium[m]`**.

Step 5 Add the `naviseccli` bin directory, which is typically `/opt/Navisphere/bin`, to your system PATH:

a) Add the following line to `~/.bash_profile & ~/.bashrc`

```
PATH=$PATH:/opt/Navisphere/bin
   export PATH
```

b) Execute this file to make the setting effective by running `source ~/.bash_profile` or `source ~/.bashrc`.

Step 6 Configure this installation of `naviseccli` to work with each storage processor on each associated array.

a) For all storage processors run the following command:

```
naviseccli -user usename -password password -h sp_ip -scope 0 -np getagent
```

b) When you reach the security prompt, choose option 2 to save the certificate.

Repeat these steps for each of the storage processors. You can use a script, if desired. The security prompt should not display again.

Step 7 With an SSH client, log in to Cisco UCS Director as the root user and run the following command against the Navisphere host where `naviseccli` is installed.

```
# ssh <navicli-user>@<navicli-host-ip> naviseccli -User sysadmin -Password <sysadmin-pass>
-Scope 0 -Address <SP-A-IP> port -list
```

Step 8 Enter the password at the login prompt (after accepting the SSH certificate)

It should list VNX Storage Array port configuration. If it first asks to save the certificate, choose option 2

Step 9 Run the same command against the SP-B IP Address to save the certificate.

```
# ssh <navicli-user>@<navicli-host-ip> naviseccli -User sysadmin -Password <sysadmin-pass>
-Scope 0 -Address <SP-B-IP> port -list
```

VNX Accounts

In Cisco UCS Director you can add the following types of VNX accounts:

- VNX file account—X-Blade enclosure, two to eight blades, configurable failover options, and flexible I/O connectivity. You can have one data mover per license.
- VNX block account—Storage or data processor enclosure, dual active storage processors, automatic failover, and flexible I/O connectivity. You can have two service providers per license.
- VNX unified account—Single platform for VNX file and VNX block. You can have two service providers per license.

Adding an EMC VNX File Account

Before you begin

- Configure a VM.
- Install the NaviSecCLI software so that all Navisphere features are supported (if it is not currently installed).
- Create a set of user credentials for the NaviCLI package with enough privileges to run NaviSecCLI commands to manage and configure VNX storage.

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

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

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, complete the following fields:

Name	Description
Pod drop-down list	Choose the pod for this account. The pod can be one of the following types: • **Default Pod** • **Generic** • **Vblock**
Category drop-down list	Choose **Storage**.
Account Type drop-down list	Choose **EMC VNX File**.

Step 5 Click **Submit**.

Step 6 On the second **Add Account** screen, complete the following fields:

Name	Description
Account Name field	A unique name for this account.
Description field	A description of this account.
Control Station IP Address	The IP address of the VNX control station that manages the file-side blades.
Use Credential Policy check box	Check if you want to use a credential policy for this account rather than enter the username and password information manually.
Credential Policy drop-down list	If you checked **Use Credential Policy**, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.

Name	Description
Control Station Username	The username that this account uses to access the VNX control station. This username must be a valid account in the control station. This field is not displayed if you chose to use a credential policy.
Password field	The password associated with the specified control station username. This field is not displayed if you chose to use a credential policy.
Transport Type drop-down list	Choose one of the following transport types that you want to use for this account: • **http** • **https** The default transport type protocol for this account is HTTPS. This field is not displayed if you chose to use a credential policy.
Port field	The port used to access the VNX control station. The default port is 443 for HTTPS. This field is not displayed if you chose to use a credential policy.
Connection Timeout (Seconds) field	The length of time in seconds that Cisco UCS Director will wait to establish a connection to the VNX control station before timing out. The default value is 40 seconds. The valid values are from 0 to 1800. An empty field or a value of 0 is interpreted as an infinite timeout. This field is not displayed if you chose to use a credential policy.
Contact Email field	The email address that you use to contact the administrator or other person responsible for this account.
Location field	The location of the contact.

Step 7 Click **Submit**.

Cisco UCS Director tests the connection to the VNX control station. If that test is successful, it adds the VNX file account and discovers all infrastructure elements in the storage system that are associated with that account. This discovery process and inventory collection cycle takes few minutes to complete.

The polling interval configured on the **System Tasks** screen on the **Administration** > **System** page specifies the frequency of inventory collection.

Adding an EMC VNX Block Account

Before you begin

- Configure a VM.

- Install the NaviSecCLI software so that all Navisphere features are supported (if it is not currently installed).
- Create a set of user credentials for the NaviCLI package with enough privileges to run NaviSecCLI commands to manage and configure VNX storage.

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

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

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, complete the following fields:

Name	Description
Pod drop-down list	Choose the pod for this account. The pod can be one of the following types: • **Default Pod** • **Generic** • **Vblock**
Category drop-down list	Choose **Storage**.
Account Type drop-down list	Choose **EMC VNX Block**.

Step 5 Click **Submit**.

Step 6 On the second **Add Account** screen, complete the following fields:

Name	Description
Account Name field	A unique name for this account.
Description field	A description of this account.
Storage Processor A IP Address field	The IP address for Storage Processor A.
Storage Processor B IP Address field	The IP address for Storage Processor B.
Use Credential Policy check box	Check if you want to use a credential policy for block access rather than enter the username and password information manually.
Credential Policy drop-down list	If you checked **Use Credential Policy**, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
Block Access User Name field	The username that this account uses to access the storage block. This username must be a valid account in the storage block. This field is not displayed if you chose to use a credential policy.

Name	Description
Block Access Password field	The password associated with the specified storage block username. This field is not displayed if you chose to use a credential policy.
Protocol drop-down list	The protocol must be **ssh**. This field is not displayed if you chose to use a credential policy.
NaviSecCLI Host IP Address field	The IP address for the secure NaviSecCLI host.
Use Credential Policy check box	Check if you want to use a credential policy for NaviSec CLI access rather than enter the username and password information manually.
Credential Policy drop-down list	If you checked **Use Credential Policy**, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
NaviSecCLI Host User Name field	The username that the account uses to access the specified secure NaviSecCLI host. This username must be a valid account in the host. This field is not displayed if you chose to use a credential policy.
NaviSecCLI Host User Password field	The password for the specified secure NaviSecCLI host. This field is not displayed if you chose to use a credential policy.
Block Access Port field	The port used to access the storage block. This field is not displayed if you chose to use a credential policy.
NaviSec CLI Path field	The path to the NaviSec CLI. For example, `/opt/Navisphere/bin`. You can leave this field empty if the path is already configured in the server. This field is not displayed if you chose to use a credential policy.
Connection Timeout (Seconds) field	The length of time in seconds that Cisco UCS Director will wait to establish a connection to the VNX block storage before timing out. The default value is 30 seconds. The valid values are from 3 to 600. This field is not displayed if you chose to use a credential policy.
Scope drop-down list	Choose one of the following scope options to limit the user access to the VNX block storage: • **Global**—Provides access to all storage systems in the domain. • **Local**—Provides access to only the storage system configured for this account. • **LDAP**—Uses LDAP authentication and provides the access configured for the username in LDAP. This field is not displayed if you chose to use a credential policy.

Name	Description
Contact field	The email address that you use to contact the administrator or other person responsible for this account.
Location field	The contact's location (user defined).

Step 7 Click **Submit**.

Cisco UCS Director tests the connection to the VNX block storage. If that test is successful, it adds the VNX file account and discovers all infrastructure elements in the storage system that are associated with that account. This discovery process and inventory collection cycle takes few minutes to complete.

The polling interval configured on the **System Tasks** screen on the **Administration** > **System** page specifies the frequency of inventory collection.

Adding an EMC VNX Unified Account

Before you begin

- Install the secure NaviSecCLI software so that all Navisphere features are supported (if it is not currently installed).
- Create a set of user credentials for the NaviSecCLI package with enough privileges to run NaviSecCLI commands to manage and configure VNX storage.

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

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

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, complete the following fields:

Name	Description
Pod drop-down list	Choose the pod for this account. The pod can be one of the following types: • **Default Pod** • **Generic** • **Vblock**
Category drop-down list	Choose **Storage**.
Account Type drop-down list	Choose **EMC VNX Unified**.

Step 5 Click **Submit**.

Step 6 On the second **Add Account** screen, complete the following fields:

Name	Description
Account Name field	A unique name for this account.
Description field	A description of this account.
File Account	
Control Station IP Address field	The IP address of the VNX control station that manages the file-side blades.
Use Credential Policy check box	Check if you want to use a credential policy for this account rather than enter the username and password information manually.
Credential Policy drop-down list	If you checked **Use Credential Policy**, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
Control Station Username	The username that this account uses to access the VNX control station. This username must be a valid account in the control station. This field is not displayed if you chose to use a credential policy.
Password field	The password associated with the specified control station username. This field is not displayed if you chose to use a credential policy.
File Access Protocol drop-down list	Choose one of the following protocols that you want to use for this account: • **http** • **https** The default protocol for this account is HTTPS. This field is not displayed if you chose to use a credential policy.
File Access Port field	The port to be used to access the VNX control station. The default port is 443 for HTTPS. This field is not displayed if you chose to use a credential policy.
Connection Timeout (Seconds) field	The length of time in seconds that Cisco UCS Director will wait to establish a connection to the VNX control station before timing out. The default value is 40 seconds. The valid values are from 0 to 1800. An empty field or a value of 0 is interpreted as an infinite timeout. This field is not displayed if you chose to use a credential policy.
Block Account	
Storage Processor A IP Address field	The IP address for Storage Processor A.
Storage Processor B IP Address field	The IP address for Storage Processor B.

Name	Description
Use Credential Policy checkbox	Check if you want to use a credential policy for block access rather than enter the username and password information manually.
Credential Policy drop-down list	If you checked **Use Credential Policy**, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
Block Access User Name field	The username that this account uses to access the storage block. This username must be a valid account in the storage block. This field is not displayed if you chose to use a credential policy.
Block Access Password field	The password associated with the specified storage block username. This field is not displayed if you chose to use a credential policy.
NaviSecCLI Host IP Address field	The IP address for the secure NaviSecCLI host.
Use Credential Policy check box	Check if you want to use a credential policy for NaviSec CLI access rather than enter the username and password information manually.
Credential Policy drop-down list	If you checked **Use Credential Policy**, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
NaviSecCLI Host User Name field	The username that the account uses to access the specified secure NaviSecCLI host. This username must be a valid account in the host. This field is not displayed if you chose to use a credential policy.
NaviSecCLI Host User Password field	The password for the specified secure NaviSecCLI host. This field is not displayed if you chose to use a credential policy.
Block Access Port field	The port used to access the storage block. The default port is 22. This field is not displayed if you chose to use a credential policy.
NaviSec CLI Path field	The path to the NaviSec CLI. For example, `/opt/Navisphere/bin`. You can leave this field empty if the path is already configured in the server. This field is not displayed if you chose to use a credential policy.
Connection Timeout (Seconds) field	The length of time in seconds that Cisco UCS Director will wait to establish a connection to the VNX block storage before timing out. The default value is 30 seconds. The valid values are from 3 to 600. This field is not displayed if you chose to use a credential policy.

Name	Description
Scope drop-down list	Choose one of the following scope options to limit the user access to the VNX block storage: • **Global**—Provides access to all storage systems in the domain. • **Local**—Provides access to only the storage system configured for this account. • **LDAP**—Uses LDAP authentication and provides the access configured for the username in LDAP. This field is not displayed if you chose to use a credential policy.
Contact field	The email address that you use to contact the administrator or other person responsible for this account.
Location field	The location of the contact.

Step 7 Click **Submit**.

Cisco UCS Director tests the connection to the VNX unified storage. If that test is successful, it adds the VNX unified account and discovers all infrastructure elements in the storage system that are associated with that account. This discovery process and inventory collection cycle takes few minutes to complete.

The polling interval configured on the **System Tasks** screen on the **Administration** > **System** page specifies the frequency of inventory collection.

VNX Block Storage Management

For VNX block (and VNX unified) accounts, you manage the following pools, groups, devices, and views:

- Storage pools—Name, description, RAID type (RAID 1/0, RAID-5, RAID-6), disks, and percentage of the full threshold
- RAID groups—RAID group ID, RAID Type (RAID 1, 0, 3, or 5, disk, hot spare), expansion, or defragmentation priority, disks. You have options to automatically destroy a RAID group after the last LUN is unbound, and for power saving.
- Host initiators—Add to new or existing host, hostname, WWN/IQN, SP port, initiator type (CLARiiON Open, HP Auto Trespass, HP No Auto Trespass, SGI, Fujitsu Siemens, Compaq Tru64), and failover mode (Active-Active mode -Failover Mode 4, Active-Passive mode (PNR)-Failover Mode 1, AIX Active-Passive mode (PAR)-Failover Mode 3, Legacy Failover Mode 2, Legacy Failover Mode 0). You add hosts to the storage groups.
- Storage groups—Name
- Logical unit numbers (LUNs)—Storage pool type (pool, RAID group), RAID type (1_0, 5), storage pool for new LUN (new or existing pool), user capacity, capacity units (MB, GB, TB, Blocks), alignment offset (LBA), default owner, initial tier placement (optimize for pool performance, highest available tier, lowest available tier), and options for automatically assigning LUN IDs as LUN names, LUN ID

autogeneration, and Thin or Maximum provisioning. You mount LUNs as Datastores and also add them to the storage groups.

The read-only report detail includes the following information:

- **System Summary**—File system allocation and system overview summary graphs
- **Data Movers**—Unique ID, account name, server name, and role
- **Storage Processors**—SP name, serial number, IP address, and faults (on or off)
- **Disk Devices**—Unique ID, account name, name, disk type, state, capacity (GB), and other data
- **Hosts**—Account name, hostname, IP address, storage group, attached to host (on or off), number of HBA ports, log in status, and status
- **Initiators**—Account name, storage group, initiator name, log in status, SP port ID, SP port type, registered (y/n), hostname, and IP address
- **Ports**—SP port, port IP address, port WWN, port type, storage processor, and fabric WWN
- **More Reports**—Tabular report for RAID groups or hosts, and instant reports for file system allocation, as well as the top five storage capacity file systems, the top five file systems file count, and the top five storage capacity volumes

Summary of Steps

Step 1 Add the VNX block account (s).

Step 2 Create the pools, groups, hosts, and LUNs needed for block management:

a) Create the storage pools.
b) Create the RAID groups.
c) Create the host initiators.
d) Create the storage groups.
e) Create the LUNs and mount them as datastores.
f) Add hosts to the storage groups.
g) Add LUNs to the storage groups.

Step 3 Review reports.

Storage Pools

A storage pool requires the following parameters:

- Storage pool name
- Description
- RAID type—1/0, 5, or 6
- Disks

- Percent full threshold

Creating a Storage Pool

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNX pod on which you want to create a storage pool and click **View details**.

Step 5 Click **Block Storage Pools**.

Step 6 Click **Create**.

Step 7 On the **Create Storage Pool** screen, complete the following fields:

Name	Description
Storage Pool Name field	The storage pool name.
Description field	The description.
RAID Type drop-down list	Choose the **RAID Type**. This can be one of the following: **1/0** **5** **8**
Disks field	Choose one or more disks to use.
Percent Full Threshold field	The percentage full threshold.

Step 8 Click **Select**.

Step 9 Click **Submit**.

RAID Groups

A RAID group has the following parameters:

- RAID Group ID—The system can specify or you can create a group ID
- RAID type—1/0, 5, or 6
- Option to automatically destroy after last LUN is unbound
- Expansion or defragmentation priority
- Option to allow power saving
- Disks

You can perform the following actions on the **RAID Groups** screen:

Button Name	Description
Create	Creates a new RAID group.
Delete	Deletes a selected RAID group.
Assign to Group	Assigns a selected RAID group to a group.
View Details	Views details about the selected RAID group.

Creating a RAID Group

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNX data center where you want to create a RAID group and click **View Details**.

Step 5 Click **RAID Groups**.

Step 6 Click **Create**.

Step 7 On the **Create RAID Group** screen, complete the following fields:

Name	Description
RAID Group ID field	Enter the RAID group ID. This can be one of the following: **1** **0** **3** **5** **disk** **hot spare**
RAID Type drop-down list	Choose the RAID type. This can be one of the following: **RAID0** **RAID1** **RAID1/0** **RAID3** **RAID5** **RAID6** **DISK**
Allow Power Saving check box	If checked, the system allows power saving for this RAID group.
Disks field	Choose one or more disks to use.

Step 8 Click **Submit**.

Host Initiators

A host initiator requires the following parameters:

- Add initiator to—You can add an initiator to a new or existing host
- Host
- WWN/IQN
- SP port
- Initiator type
- Failover mode

You can perform the following actions on the **Initiators** screen:

Button Name	Description
Register	Registers a new initiator.
View Details	Views details about the selected initiator.
Deregister	Deregisters a selected initiator.

Registering a Host Initiator

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNX data center where you want to register a host initiator and click **View Details**.
Step 5 Click **Initiators**.
Step 6 Click **Register**.
Step 7 On the **Register Host Initiator** screen, complete the following fields:

Name	Description
Add Initiator to drop-down list	Choose either **Existing Host** or **New Host**. If you chose **New Host**, you can add the initiator to a new host by specifying a **Host Name**, **Host IP Address**, and **New Host WNN**.
Host field	If you chose **Existing Host**, choose one of the hosts to add the initiator to an existing hosts.
WWN/IQN	The WWN/IQN for the new or existing host.
SP Port field	Choose one of the SP ports in the list.

Name	Description
Initiator Type drop-down list	Choose the **Initiator Type**. This can be one of the following: • CLARiiON Open • HP Auto Trespass • HP No Auto Trespass • SGI • Fujitsu Siemens • Compaq Tru64
Failover Mode drop-down list	Choose the **Failover Mode**. This can be one of the following: • Active-Active mode-Failover Mode 4 • Active-Passive mode (PNR)-Failover Mode 1 • AIX Active-Passive mode (PAR)-Failover Mode 3 • Legacy Failover Mode 2 • Legacy Failover Mode 0

Step 8 Click **Submit**.

Storage Groups

A storage group requires a name as a parameter.

You can perform the following actions on the **Storage Groups** screen:

Button Name	Description
Create	Creates a new storage group.
View Details	Views details about the selected storage group.
Delete	Deletes a selected storage group.
Add LUN	Adds a LUN to a selected storage group.
Remove LUN	Removes a LUN from a selected storage group.
Add Host	Adds a host to a selected storage group.
Remove Host	Removes a host from a selected storage group.

Creating a Storage Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNX data center where you want to create the storage group and click **View Details**.
Step 5 Click **Storage Groups**.
Step 6 Click **Create**.
Step 7 On the **Create Storage Group** screen, enter the name for the storage group in the **Name** field.
Step 8 Click **Submit**.

What to do next

Add hosts and LUNs to the storage group on the **Storage Groups** screen.

LUNs

A LUN has the following parameters:

- Option to automatically assign LUN IDs as LUN names
- Option to allow the system to specify the LUN ID
- Storage pool type
- RAID type
- Storage pool
- Thin or maximum provisioning
- User capacity (thin LUN only)
- Capacity units
- LUN ID
- Alignment offset (LBA)
- Default owner

You can perform the following actions on the **LUNs** screen:

Button Name	Description
Create	Creates a LUN.
Delete	Deletes a selected LUN.
Expand	Expands a selected LUN.
Create Meta LUN	Create a Meta LUN for a selected LUN.

Button Name	Description
Associate LUN as Datastore	Associates a LUN as a Datastore.
Assign to Group	Assigns a selected LUN to a group.
View Details	View details on a selected LUN.

Creating a LUN

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNX pod where you want to create a LUN and click **View Details**.

Step 5 Click **LUNs**.

Step 6 Click **Create**.

Step 7 On the **Create LUN** screen, complete the following fields:

Name	Description
Storage Pool Type drop-down list	Choose the storage pool type. **Restriction** If you choose **RAID Group**, the system automatically generates the LUN ID. Automatic LUN naming ensures that the LUN name conforms to a set of strict naming conventions. An incorrectly named LUN no longer functions properly. If you choose **Pool**, the default path is set to automatically assign LUN IDs as LUN names. However, you have the option to uncheck this option (not recommended).
Automatically assign LUN IDs as LUN Names check box	If you chose **Pool** as the storage pool type, the default path is set to automatically assign LUN IDs as LUN names. However, you have the option to uncheck this option (not recommended). If checked, LUN IDs are automatically assigned as LUN names. Uncheck the check box if you do not want LUN IDs to be assigned as LUN names.
Storage Pool for New LUN drop-down list	Choose the storage pool for the new LUN.
Thin check box	Check if you want a thin LUN.
Ignore Thresholds check box	Check to ignore Storage Pool threshold limits.
User Capacity field	The user capacity (applies to **Thin LUN** only).

Name	Description
Capacity Units drop-down list	Choose the capacity units type. This can be one of the following: • **GB** • **MB** • **TB** • **Blocks**
Alignment Offset (LBA) field	The alignment offset (LBA) (0 to 9999).
Default Owner drop-down list	Choose the default owner from the drop down-list: • **Auto** • **SP A** • **SP B**
Initial Tier Placement drop-down list	Choose one of the following from the drop-down list: • **Optimize for Pool Performance** • **Highest available tier** • **Lowest available tier**

Step 8 Click **Submit**.

What to do next

Mount the LUN as a Datastore.

Adding a Host to a Storage Group

Before you begin

A host and a storage group must exist in the system.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNX data center where you want to add a host and click **View Details**.
Step 5 Click **Storage Groups**.
Step 6 Click **Add Host**.
Step 7 On the **Add Host(s) to Storage Group** screen, complete the following fields:

Name	Description
Show Hosts drop-down list	Choose **Include Connected** or **Not Connected**.
Hosts field	Click **Select** and choose a host.

Step 8 Click **Submit**.

Adding a LUN to a Storage Group

Before you begin

A LUN and a storage group must exist in the system.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNX data center where you want to add a LUN and click **View Details**.
Step 5 Click **Storage Groups**.
Step 6 Click **Add LUN**.
Step 7 On the **Add LUN to Storage Group** screen, complete the following fields:

Name	Description
LUN field	If you want to choose the LUN manually, click **Select**.
Let System Specify HLU check box	If checked, the system autogenerates the Host LUN ID (HLU).

Step 8 In the **Host LUN ID** field, enter the **Host LUN ID**.
Step 9 Click **Submit**.

Creating a Meta LUN

Before you begin

Create a LUN.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with VNX Pod where you want to create a Meta LUN, and click **View Details**.

Step 5 Click **Meta LUNs**.

Step 6 Click **Create Meta LUN**.

Step 7 On the **Create Meta LUN** screen, complete the following fields:

Name	Description
Expansion Type drop-down list	Choose an expansion type. This can be one of the following: • **Stripe Expansion** • **Concatenate Expansion**
Flare LUNs drop-down list	Choose a Flare LUN that is added to the base LUN.
Meta LUN Name field	The LUN name.
MAX check box	If checked, the system creates a MAX LUN size.
User Capacity field	The LUN capacity units (applies to **Thin LUN** only).
Capacity Units drop-down list	Choose a capacity unit.
Default Owner drop-down list	Choose the default owner.
Element size Multiplier field	The element size multiplier. This field displays the strip element size multiplier for the meta LUN. The default value is 4.
Alignment Offset field	The alignment offset (LBA) value. The value range is from 0 to 9999.
Enable Auto-assign check box	If checked, the system enables **Auto-assign**. This option enables or disables Auto-assign only to a storage system that has two service providers and a LUN that is not a hot spare.
Expansion Rate drop-down list	Choose an expansion rate for making additional LUN capacity available to the host.

Step 8 Click **Submit**.

What to do next

Associate a LUN as a Datastore.

Associating a LUN as a Datastore

Before you begin

Create a LUN.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNX Pod where you want to associate a LUN as a Datastore, and click **View Details**.

Step 5 Click **LUNs**.

Step 6 Click the row with the LUN to associate as a Datastore

Step 7 Click **Associate LUN As Datastore**.

Step 8 On the **Associate LUN As Datastore** screen, complete the following fields:

Name	Description
Data store Name field	The Datastore.
Select Host Node field	The host node.
Initiator Type drop-down list	Choose the initiator type.
LUN Name field	The LUN name.
VDC Name drop-down list	Choose the VDC name.
Success Criteria drop-down list	Choose how to measure the association as successful from the drop-down.

Step 9 Click **Submit**.

What to do next

Verify that the Datastore is associated to the LUN. For example, you can choose **Virtual > Storage** and click **vCenter** to view the related data stores.

About VNX File Storage Management

For VNX File (and VNX Unified) accounts, you can use either Common Internet File System (CIFS) or Network File System (NFS) Export.

For CIFS, you create and manage the following:

- CIFS servers—Server type, computer, NetBIOS name, aliases, and domain. You can choose to join a domain, enable local users, and select interfaces.
- CIFS shares—CIFS share name, file systems, path, CIFS server, user limit, and comments.
- DNS domains—Name, DNS servers, and protocol (UDP or TCP).

For NFS Export, you create and manage the following:

- Storage pools for files—Name, description, and subnet mask for the interface. You can create from a metavolume or a storage pool. Optionally, you can slice pool volumes by default.

- Volumes—Name, type (stripe, meta, slice), stripe size (32, 64, 256), and which volumes to select. You can mount volumes to the Datastore.
- File systems—Name, storage pool, storage capacity, capacity units (GB, MB, TB). You can optionally create a file system from a storage pool or volume to contain slices. You can mount file systems to the data store.
- Data mover interfaces—Name, device name, address, subnet mask, maximum transmission unit (MTU), and VLAN ID
- NFS export—File systems, read/write hosts, root hosts, and an option to host access read-only export
- Mounts—Path, file system name, server, read-only or read/write, and access-checking policy (NT, UNIX, Secure, Native, Mixed, or Mixed and Compatible). You can choose to enable virus checking, enable CIFS oplocks, and set advanced options.

The read-only report includes the following information:

- System overview summary—Data center, account, host, role, and mode
- CIFS server and shares detail
- DNS domain detail
- For NFS, storage pool for files, file system, NFS export, and data mover detail

Summary of Steps

Step 1 Add the VNX file account(s).

Step 2 Choose either **CIFS** or **NFS Export**.

- For CIFS, create the CIFS servers, CIFS shares, and DNS domains.
- For NFS Export, create the following:

a) Storage pools for files
b) Volumes
c) File systems
d) Interfaces
e) NFS export information
f) Mounts

Step 3 Review reports.

Using CIFS

In Cisco UCS Director, you can use CIFS to export files or directories. A client can mount any server-exported directory.

To use CIFS, you create the CIFS servers, CIFS shares, and DNS domains.

CIFS Servers

A CIFS server requires the following parameters:

- Server type
- Computer name
- NetBIOS name
- Aliases
- Domain
- Option to join a domain
- Option to enable local users
- Interfaces

You can perform the following actions on the **CIFS Server** screen:

Button Name	Description
Add	Creates a new CIFS server.
Delete	Deletes a selected CIFS server.
Modify	Modifies attributes of a selected CIFS server.

Creating a CIFS Server

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNX data center where you want to create a CIFS server and click **View Details**.

Step 5 Click **Data Movers**.

Step 6 Click the row with the server and click **View Details**.

Step 7 Click **CIFS Servers**.

Step 8 Click **Add**.

Step 9 On the **Create CIFS Server** screen, complete the following fields:

Name	Description
Server Type drop-down list	Choose the server type.
Computer Name field	The computer name.
NetBIOS Name field	The NetBIOS name for this server.
Aliases field	The alias names for this server.
Domain field	The server domain name.

Name	Description
Join Domain check box	Check to enable the server to join another domain.
Enable Local Users check box	Check to enable local users on this server. If you checked this check box, go to Step 10.
Interfaces field	Click **Select** to choose an interface(s). Go to Step 11.

Step 10 If you checked **Join Domain**, complete the following additional fields:

Name	Description
Domain Admin field	The domain administrator username for this server.
Domain Password field	The server domain password.
Organizational Unit field	The server's organizational unit.

Step 11 If you checked **Enable Local Users**, complete the following additional fields:

Name	Description
Set Local Admin Password field	The local administrator password for this server.
Confirm Local Admin Password field	The confirmation of the local administrator password.

Step 12 Click **Submit**.

CIFS Shares

A CIFS share requires the following parameters:

- CIFS share name
- File system
- Path
- CIFS server
- User limit
- Comments

You can perform the following actions on the **CIFS Share** screen:

Button Name	Description
Add	Adds a new CIFS share.

Button Name	Description
Delete	Deletes a selected CIFS share.

Creating CIFS Shares

Before you begin

A CIFS server must exist in the system.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNX data center where you want to create the CIFS shares and click **View Details**.

Step 5 Click **Data Movers**.

Step 6 Click the row with the server and click **View Details**.

Step 7 Click **CIFS Shares**.

Step 8 Click **Add**.

Step 9 In the **Create CIFS Shares** dialog box, complete the following fields:

Name	Description
File Systems drop-down list	Choose the **File Systems** type.
CIFS Share Name field	The CIFS share name.
Path field	The path.
CIFS Server field	**Click Select.** Choose one or more CIFS shares.
User Limit field	The alias names for this server.
Comments field	Any comments regarding CIFS shares.

Step 10 Click **Submit**.

DNS Domains

A DNS domain requires the following parameters:

- Name
- DNS servers
- Protocol

You can perform the following actions on the **DNS Domains** screen:

Button Name	Description
Add	Adds a new DNS domain.
Delete	Deletes a selected DNS domain.

Creating a DNS Domain

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNX data center where you want to create a DNS Domain and click **View Details**.

Step 5 Click **Data Movers**.

Step 6 Click the row with the server and click **View Details**.

Step 7 Click **DNS Domain**.

Step 8 Click **Add**.

Step 9 On the **Add DNS Domain** screen, complete the following fields:

Name	Description
Name field	The DNS domain name.
DNS Servers field	The DNS server names.
Protocol drop-down list	Choose the protocol.

Step 10 Click **Submit**.

Using NFS Export

In Cisco UCS Director, you can use NFS to export files or directories. A client can mount any server-exported directory.

To use NFS Export, you create the storage pools for files, volumes, file systems, interfaces, NFS export information, and add the mounts.

Storage Pools for Files

An NFS storage pool for files requires the following parameters:

- Name
- Create from—Metavolume or storage pool
- Description
- Volumes—Subnet mask
- Slice pool volumes by default—Checked or unchecked

You can perform the following actions on the **Storage Pools for Files** screen:

Button Name	Description
Create	Creates a new NFS storage pool for files.
View Details	Views details about the selected NFS storage pool for files.
Delete	Deletes a selected storage pool for files.

Creating a Storage Pool for Files

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNX data center where you want to create a storage pool for files and click **View Details**.

Step 5 Click **Data Movers**.

Step 6 Click the row with the server and click **View Details**.

Step 7 Click **View Details**.

Step 8 Click **Storage Pools for File**.

Step 9 Click **Create**.

Step 10 On the **Create Storage Pool** screen, complete the following fields:

Name	Description
Name field	The storage pool name.
Create from drop-down list	Choose **Meta Volume** or **Storage Pool**.
Description field	The description for this storage pool.
Volumes drop-down list	The volumes for this storage pool.
Slice Pool Volumes by Default check box	Check to slice pool volumes by default.

Step 11 If you chose **Storage Pool**, complete the following additional fields to create this storage pool from another storage pool:

Name	Description
Template Pool drop-down list	Choose the template pool.
Minimum Pool Size (MB) field	The minimum pool size (MB).
Stripe Size (KB) field	The stripe size (KB).

Step 12 Click **Submit**.

Volumes

An NFS volume requires the following parameters:

- Name
- Type
- Volumes
- Stripe size—32, 64, 256

You can perform the following actions on the **Volumes** screen:

Button Name	Description
Delete	Deletes a selected volume.

Creating a Volume

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNX data center where you want to create a volume and click **View Details**.

Step 5 Click **Volumes**.

Step 6 Click **Create**.

Step 7 On the **Create Volume** screen, complete the following fields:

Name	Description
Name field	The NFS volume name.
Type drop-down list	Choose one of the following volume types for this volume: • **Stripe** • **Meta** • **Slice**
Volumes field	Choose to use one or more volumes from the list of available volumes.
Stripe Size (KB) drop-down list	Choose the **Stripe Size** from the list (256, 32, or 64 KB).

Step 8 Click **Submit**.

File Systems

An NFS file system has the following parameters:

- Name

- Create from a volume or storage pool
- Storage pool
- Storage capacity
- Capacity units
- Option to contain slices

You can perform the following actions on the **File Systems** screen:

Button Name	Description
Create	Creates a new file system.
Extend	Extends a file system.
View Details	Views details about the selected file system.
Delete	Deletes a selected file system.

Creating an NFS File System

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNX pod where you want to create an NFS File System and click **View Details**.

Step 5 Click **File Systems**.

Step 6 Click **Create**.

Step 7 On the **Create File System** screen, complete the following fields:

Name	Description
Name field	The NFS file system name.
Create from drop-down list	Choose either **Storage Pool** or **Volume** as the source for the file system.
Storage Pool field	Choose the storage pool for this file system.
Storage Capacity field	The storage capacity to allocate for this file system.
Capacity Units drop-down list	Choose the capacity units type. This can be one of the following: • **GB** • **MB** • **TB**
Contain Slices check box	Check this check box to enable the file system to contain slices.
Data Mover field	Choose the data mover account for the file system.

Step 8 Click **Submit**.

What to do next

You can mount the file system as a Datastore.

Data Mover Interfaces

An NFS data mover interface requires the following parameters:

- Name
- Device name
- Address
- Subnet mask
- MTU
- VLAN ID

You can perform the following actions on the **Interfaces** screen:

Button Name	Description
Create	Creates a data mover interface.
View Details	Views details about the selected interface.
Delete	Deletes a selected data mover interface.

Adding a Data Mover Interface

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNX pod where you want to create a Data Mover Interface and click **View Details**.
Step 5 Click **Data Movers**.
Step 6 Click the row with the server and click **View Details**.
Step 7 Click **Mover Interfaces**.
Step 8 Click **Add**.
Step 9 On the **Add Data Mover Interface** screen, complete the following fields:

Name	Description
Name field	The interface name.
Device Name drop-down list	Choose the device name for this interface.
Address field	The interface address.

Name	Description
Subnet Mask field	The subnet mask for this interface.
MTU field	The maximum transmission unit (MTU) for this interface.
VLAN ID field	The VLAN ID for this interface.

Step 10 Click **Submit**.

NFS Export

NFS Export requires the following parameters:

- File system
- Read/write hosts
- Root hosts
- Option to host access read-only export

You can perform the following actions on the **NFS Export** screen:

Button Name	Description
Create	Creates an NFS export.
Edit	Edits an NFS export.
View Details	Views details about the selected NFS export.
Delete	Deletes a selected NFS export.

Exporting an NFS File System

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNX pod where you want to add an NFS File System and click **View Details**.
Step 5 Click **Data Movers**.
Step 6 Click the row with the server and click **View Details**.
Step 7 Click **NFS Exports**.
Step 8 Click **Add**.
Step 9 On the **Add NFS Export** screen, complete the following fields:

Name	Description
File Systems drop-down list	Choose the **File Systems** type for NFS Export.
Read/Write Hosts field	The read/write hosts for NFS Export.

Name	Description
Root Hosts field	The root hosts for NFS Export.
Host Access Read-only Export check box	Check if you want host access read-only export.

Step 10 Click **Submit**.

Mounts

An NFS mount requires the following parameters:

- Path
- File system name
- Mount server
- Read-only or read and write
- Access checking policy
- Option to enable virus checking
- Option to enable CIFS oplocks
- Option to enable advanced options

You can perform the following actions on the **Mounts** screen:

Button Name	Description
Modify	Modifies the attributes of a selected mount.
Delete	Deletes a selected mount.

Modify a File System

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNX pod where the file system is located and click **View Details**.
Step 5 Click **Data Movers**.
Step 6 Click the row with the server and click **View Details**.
Step 7 Click **Mounts**.
Step 8 Click the row with file system and click **Modify**.
Step 9 On the **Modify Mount** screen, complete the following fields:

Name	Description
Path field	The path for this mount.

Name	Description
File System Name drop-down list	Choose the file system name for this mount.
Mount On drop-down list	Choose the server for this mount.
Read Only drop-down list	Choose the Read Only or Read and Write option for this mount.
Access-Checking Policy drop-down list	Choose the access-checking policy for this mount.
Virus Checking Enabled check box	Check if you want virus checking enabled.
CIFS Oplocks Enabled check box	Check if you want CIFS Oplocks enabled.
Set Advanced Options check box	Check if you want to set advanced options.

Step 10 Click **Submit**.

Deleting a File System

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNX pod containing the file system you want to delete and click **View Details**.
Step 5 Click **Data Movers**.
Step 6 Click the row with the server and click **View Details**.
Step 7 Click **Mounts**.
Step 8 Click the row with the file system and click **Delete**.

VNX Unified Storage Management

VNX unified storage combines VNX block storage with VNX file storage.

Summary of Steps

Step 1 Add the VNX block account(s).
Step 2 Create the pools, groups, hosts, and logical unit numbers (LUNs) needed for block management:
a) Create the storage pools.
b) Create the RAID groups.
c) Create the host initiators.
d) Create the storage groups.
e) Create the LUNs and mount them as datastores.

f) Add hosts to the storage groups.
g) Add LUNs to the storage groups.

Step 3 Review VNX block storage reports.

Step 4 Add the VNX file account(s).

Step 5 Choose either **CIFS** or **NFS Export**.

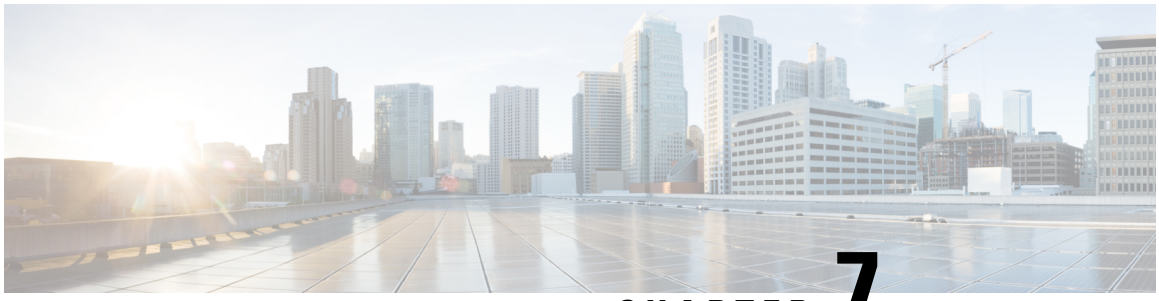
- For CIFS, create the CIFS servers, CIFS shares, and DNS domains.
- For NFS Export, create the following:

a) Storage pools for files
b) Volumes
c) File systems
d) Interfaces
e) NFS export information
f) Mounts

Step 6 Review VNX file storage reports.

What to do next

See the previous chapters on how to manage VNX block storage and VNX file storage for more details.



CHAPTER 7

EMC VNXe

• Routes Report, on page 155

About Cisco UCS Director for EMC VNXe

Cisco UCS Director supports EMC VNXe storage accounts.

Note See the Compatibility Matrix for all supported VNXe versions.

For a VNXe account, you can manage the following:

- Storage Pools
- Host Initiators
- Logical Unit Numbers (LUNs)

The reports for VNXe accounts also include details on all of these items, and on storage processors, ports, meta LUNs, hosts, ports, and disk devices.

For a VNXe account, you can manage the following:

- Filesystems
- Common Internet File Servers (CIFS) servers
- Common Internet File Servers (CIFS) shares
- Network File System (NFS) exports
- DNS Domains

The reports available for VNXe accounts include system overview summaries.

Adding an EMC VNXe Account

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

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

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, complete the following fields:

Name	Description
Pod drop-down list	Choose the pod for this account. The pod can be one of the following types: • **Default Pod** • **Generic** • **VSPEX** • **Vblock**
Category drop-down list	Choose **Storage**.

Name	Description
Account Type drop-down list	Choose **EMC VNXe**.

Step 5 Click **Submit**.

Step 6 On the second **Add Account** screen, complete the following fields:

Name	Description
Account Name field	A unique name for this account.
Description field	A description of this account.
Server IP Address field	The IP address of the VNXe server.
Use Credential Policy checkbox	Check if you want to use a credential policy for this account rather than enter the username and password information manually.
Credential Policy drop-down list	If you checked **Use Credential Policy**, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
Username field	The username that this account uses to access the VNXe server. This username must be a valid account in the server. This field is not displayed if you chose to use a credential policy.
Password field	The password associated with the specified VNXe server username. This field is not displayed if you chose to use a credential policy.
Protocol drop-down list	The protocol must be **https**.
Port field	The port to be used to access the VNXe server. The default port is 443.
Connection Timeout (Seconds) field	The length of time in seconds that Cisco UCS Director will wait to establish a connection to the VNXe server before timing out. The default value is 45 seconds. The valid values are from 0 to 1800. An empty field or a value of 0 is interpreted as an infinite timeout.
Socket Read Timeout (Seconds) field	The length of time in seconds that Cisco UCS Director will wait for data from the VNXe server before timing out. The default value is 120 seconds. The valid values are from 0 to 1800. An empty field or a value of 0 is interpreted as an infinite timeout.
Contact field	The email address that you use to contact the administrator or other person responsible for this account.
Location field	The location of the contact.

Step 7 Click **Submit**.

Cisco UCS Director tests the connection to the VNXe server. If that test is successful, it adds the VNXe account and discovers all infrastructure elements in the storage system that are associated with that account. This discovery process and inventory collection cycle takes few minutes to complete.

The polling interval configured on the **System Tasks** screen on the **Administration** > **System** page specifies the frequency of inventory collection. For more information about configuring the polling interval, see the *Cisco UCS Director Network Devices Management Guide*.

Management Overview

VNXe is managed through the use of reports that are available within UCS Director. The following sections show how each report is used to manage each function within VNXe.

System Summary Report

The System Summary report displays the following details about the VNXe device:

- Pod Name
- Account Name
- Server Address
- Model
- Software Version
- Name
- Serial Number
- MAC Address
- Connection Status

Storage Processors Report

A Storage Processor is a hardware component that provides the processing resources for performing storage operations, such as creating, modifying and monitoring storage resources. Every VNXe storage system has two storage processors.

The report contains the following information:

- Name
- Model
- BIOS Firmware Revision
- Post Firmware revision
- Serial Number
- Part Number
- Service Mode
- SAS Expander Version

Disk Groups Report

In VNXe, physical disks are grouped into three groups:

- Extreme Performance
- Performance
- Capacity

This report provides the following information:

- Name
- Part Number
- Useable Disk Capacity
- Total Disk Capacity
- Tier Type
- Disk Technology
- Total Disks
- Free Disks

Storage Pools Report

A storage pool is a homogeneous or heterogeneous grouping of physical disks with each tier being disks of similar type and speed. A homogenous storage pool is a single tier pool using one type of disk. A heterogeneous storage pool consists of multiple tiers using different types of disks.

Creating a Storage Pool

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNXe device on which you want to create a storage pool, and click **View Details**.

Step 5 Click **Storage Pools**.

Step 6 Click **Create**.

Step 7 On the **Create Storage Pool** screen, complete the following fields:

Name	Description
Name field	The storage pool name. If not specified, the name is autogenerated.
Description field	The description of the storage pool.
Extreme Performance Tier check box **Performance Tier** check box **Capacity Tier** check box	At least one tier must be configured by selecting the check box

Name	Description
RAID Type drop-down list	Choose the **RAID Type**. This can be one of the following: **RAID 5** **RAID 6** **RAID 1/0**
Stripe Width drop-down list	Choose the number of disks for the **Raid Type**. The options are: **4+1** **8+1** **12+1** **Maximum Capacity**
Disks Groups field	Choose a Disk Group from the list.
Number of Disks field	The number of disks to be used for this storage pool.
Alert Threshold field	Specify the alert threshold.
Enable FAST Cache check box	Check to enableFAST Cache, or else continue with disable option.
Enable FAST VP Schedule check box	Check to enable FAST VP Schedule, or else continue with disable option.

Step 8 Click **Submit**.

Modifying a Storage Pool

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device that contains the storage pool you want to modify, and click **View Details**.
Step 5 Click **Storage Pools**.
Step 6 Click the row with the storage pool that you want to modify.
Step 7 Click **Modify**.
Step 8 On the **Modify Storage Pool** screen, you can modify the following fields:

Name	Description
Name field	The storage pool name. Name can be modified. If not specified, the name is auto generated.
Description field	The description of the storage pool.
Alert Threshold field	Specify the alert threshold.

Name	Description
Enable FAST Cache check box	Check to enable FAST Cache.
Enable FAST VP Schedule check box	Check to enable FAST VP Schedule.

Step 9 Click **Submit**.

Expanding a Storage Pool

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device that contains the storage pool you want to expand, and click **View Details**.
Step 5 Click **Storage Pools**.
Step 6 Click the row with the storage pool that you want to expand.
Step 7 Click **Expand**.
Step 8 On the **Expand Storage Pool** screen, you can change the following fields to expand the storage pool capacity:

Name	Description
Extreme Performance Tier check box **Performance Tier** check box **Capacity Tier** check box	At least one tier must be configured by selecting the checkbox.
RAID Type drop-down list	Choose the **RAID Type**. This can be one of the following: **RAID 5** **RAID 6** **RAID 1/0**
Stripe Width drop down list	Choose the number of disks for the **Raid Type**. The options are: **4+1** **8+1** **12+1** **Maximum Capacity**
Disks Groups field	Choose a Disk Group from the list.
Number of Disks field	The number of disks to be used for this storage pool.
Enable FAST Cache check box	Check to enable FAST Cache.

Name	Description
Enable FAST VP Schedule check box	Check to enable FAST VP Schedule.

Step 9 Click **Submit**.

File Systems Report

A file system represents set of storage resources that provide network file storage. VNXe establishes a file system, either CIFS or NFS, that Windows users or Linux/UNIX hosts can connect to and use for file-based storage. Shares within the file system draw from the total storage that is allocated to the file system.

The File Systems report provides the following information:

- Name of the file system
- Storage Pool
- Type
- Total Capacity
- Used Capacity
- Protocols
- Description
- Thin Enabled
- Tiering Policy
- Deduplication

Creating a File System

Note Before you create a file system, at least one NAS server must exist on the storage system.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, choose the pod.

Step 4 On the **Storage** page, click **Storage Accounts**.

Step 5 Click the row with the VNXe device on which you want to create a file system, and click **View Details**.

Step 6 Click **File Systems**.

Step 7 Click **Create**.

Step 8 On the **Create File System** screen, complete the following fields:

Name	Description
Storage Pool field	Select the storage pool from the list.

Name	Description
Name field	Name the file system.
Protocol drop-down list	Choose NFS or CIFS from the drop-down list.
NAS Server field	Select the NAS Server from the list.
Size field	Specify a size for the file system.
Capacity Units drop-down list	Choose MB, GB, or TB from the drop-down list.
Description field	File system description.
Tiering Policy drop-down list	Choose from the following in the drop-down list: Start High Then Auto-Tier Auto-Tier Highest Available Tier Lowest Available Tier
Thin check box **FLR Enabled** check box **Enable Deduplication** check box	Check as appropriate.

Step 9 Click **Submit**.

Modifying a File System

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, choose the pod.
Step 4 On the **Storage** page, click **Storage Accounts**.
Step 5 Click the row with the VNXe device on which you want to modify file system, and click **View Details**.
Step 6 Click **File Systems**.
Step 7 Click the row with the file system that you want to modify, and choose **Modify**.
Step 8 On the **Modify File System** screen, the following fields can be changed:

Name	Description
Size field	Specify a size for the file system.
Capacity Units drop-down list	Choose MB, GB, or TB from the drop-down list.
Description field	File system description.

Name	Description
Tiering Policy drop-down list	Choose from the following in the drop-down list: Start High Then Auto-Tier Auto-Tier Highest Available Tier Lowest Available Tier
Thin check box **FLR Enabled** check box **Enable Deduplication** check box	The check boxes that were checked when the file system was created will be displayed.

Step 9 Click **Submit**.

NFS Shares Report

Shares represent mount points through which users or hosts can access file system resources. Each share is associated with a single file system and inherits the file system protocol (CIFS or NFS) established for that file system.

This report provides the following information:

- Name
- File System
- Path
- Default Access
- Read Only
- No Access Hosts
- Read Only Hosts
- Read Write Hosts
- Root Access Hosts
- Description
- Tag

Creating an NFS Share

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device on which you want to create an NFS share, and click **View Details**.
Step 5 Click **NFS Shares**.
Step 6 Click **Create**.

Step 7 On the **Create NFS Share** screen, complete the following fields:

Name	Description
File System field	Select the file system from the list.
Path field	Local path to a location within the file system.
Name field	Type a name for the share.
Description field	Type a description of the share.
Default Access drop-down list	Choose the default access for the share. The options are: **No Access** **Read-Only** **Read/Write** **Read/Write, allow Root**
No Access Hosts field	Choose a Host or Hosts from the list.
Read Only Access Hosts field	Choose a Host or Hosts from the list.
Read Write Access Hosts field	Choose a Host or Hosts from the list.
Root Access Hosts field	Choose a Host or Hosts from the list.

Step 8 Click **Submit**.

Modifying an NFS Share

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device on which you want to modify an NFS share, and click **View Details**.
Step 5 Click **NFS Shares**.
Step 6 Click the row with the NFS share that you want to modify and choose **Modify**.
Step 7 On the **Modify NFS Share** screen, the following fields can be modified:

Name	Description
Description field	Type a description of the share.

Name	Description
Default Access drop down	Choose the default access for the share. The options are: **No Access** **Read-Only** **Read/Write** **Read/Write, allow Root**
No Access Hosts field	Choose a Host or Hosts from the list.
Read Only Access Hosts field	Choose a Host or Hosts from the list.
Read Write Access Hosts field	Choose a Host or Hosts from the list.
Root Access Hosts field	Choose a Host or Hosts from the list.

Step 8 Click **Submit**.

Create an NFS Datastore

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device on which you want to create an NFS datastore, and click **View Details**.
Step 5 Click **NFS Shares**.
Step 6 Click the row with the NFS share on which you want to create an NFS datastore and choose **Create Datastore**.
Step 7 On the **Create NFS Datastore** screen, complete the following fields:

Name	Description
Host Node field	Choose the host node or nodes from the list.
Datastore Name field	Type a name for the Datastore.
Access Modedrop-down list	Choose **Read/Write** or **Read Only**.
Success Criteria drop-down list	Choose **Mount successful at least on one host** or **Mount successful on all the hosts**.

Step 8 Click **Submit**.

LUNS Report

LUN storage resources provide hosts with access to general-purpose block-level storage through network-based iSCSI or Fibre Channel (FC) connections. With LUN storage, you can manage addressable partitions of block storage resources so that host systems can mount and use these resources (LUNs) over FC or IP connections.

This report provides the following information:

- Name
- Storage Pool
- Type
- Total Capacity
- Used Capacity
- WWN
- Description
- Thin Enabled
- Tiering Policy
- Default Node
- Current Node
- Tag

Creating a LUN

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNXe device on which you want to create the LUN, and click **View Details**.

Step 5 Click **LUNs**.

Step 6 Click **Create**.

Step 7 On the **Create LUN** screen, complete the following fields:

Name	Description
Storage Pool field	Select the storage pool from the list.
Name field	Type a name for the LUN.
Size field	Specify the size of the LUN
Capacity Units drop-down list	Select from the drop-down list: **MB** **GB** **TB**
Description field	Type a description of the LUN.

Name	Description
Default Node drop-down list	Select the default node from the drop-down list: **Auto** **SP A** **SP B**
Tiering Policy drop down	Choose the tiering policy. The options are: **Start High then Auto-Tier** **Auto-Tier** **Highest Available Tier** **Lowest Available Tier**
Thin check box	Check to enable.
LUN Access Hosts field	Choose a Host or Hosts from the list.
Snapshot Access Hosts field	Choose a Host or Hosts from the list.
LUN and Snapshot Access Hosts field	Choose a Host or Hosts from the list.

Step 8 Click **Submit**.

Modifying a LUN

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device on which you want to modify a LUN, and click **View Details**.
Step 5 Click **LUNs**.
Step 6 Click the row with the LUN that you want to modify, and choose **Modify**.
Step 7 On the **Modify LUN** screen, the following fields can be modified:

Name	Description
Size field	Specify the size of the LUN
Capacity Units drop-down list	Select from the drop-down list: **MB** **GB** **TB**

Name	Description
Description field	Type a description of the LUN.
Default Node drop-down list	Select the default from the drop-down list: **Auto** **SP A** **SP B**
Tiering Policy drop-down list	Choose the tiering policy. The options are: **Start High then Auto-Tier** **Auto-Tier** **Highest Available Tier** **Lowest Available Tier**
Thin check box	Check to enable.
LUN Access Hosts field	Choose a Host or Hosts from the list.
Snapshot Access Hosts field	Choose a Host or Hosts from the list.
LUN and Snapshot Access Hosts field	Choose a Host or Hosts from the list.

Step 8 Click **Submit**.

Creating a VMFS Datastore

A VMFS datastore can be created from a LUN using the **Associate LUN As Datastore** action.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device on which you want to create a VMFS datastore, and click **View Details**.
Step 5 Click **LUNs**.
Step 6 Click the row with the LUN from which you want to create a VMFS datastore, and choose **Create Datastore**.
Step 7 On the **Associate LUN As Datastore** screen, complete the following fields:

Name	Description
Host Node field	Choose the host node or nodes from the list. **Note** V-Center account are added under Virtual Accounts to show the Host node list.
Datastore Name field	Type a name for the datastore.

Name	Description
Initiator Type drop-down list	Choose **ISCSI or FCP**.
VDC Name drop-down list	Choose from list.
Success Criteria drop-down list	Choose **Mount successful at least on one host** or **Mount successful on all the hosts**.

Step 8 Click **Submit**.

Hosts Report

Host configurations are logical connections through which hosts or applications can access storage resources. Before a network host can access storage, define a configuration for it and associate it with a storage resource.
\

VNXe supports the following types of host configurations:

- Individual host configurations: Specify access to storage resources on a host-by-host basis.
- Subnet and netgroup configurations: Configure access to storage resources for multiple hosts or network segments.
- VMware host configurations: Configure access to storage resources for individual ESX server hosts or groups of ESX servers managed by a common vCenter Server.

The Hosts report provides the following information about each host:

- Name
- Type
- OS Type
- Description

Creating a Host

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device on which you want to create a host, and click **View Details**.
Step 5 Click **Hosts**.
Step 6 Click **Create**.
Step 7 On the **Create Host** screen, complete the following fields:

Name	Description
Host Type drop-down list	Select the host type from the drop-down list.
Name field	Enter the name of the host.

Name	Description
Description field	Enter a description of the host.
OS Type field	Enter the OS type.

Step 8 Click **Submit**.

Modifying a Host

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNXe device that contains the host you want to modify, and click **View Details**.

Step 5 Click **Hosts**.

Step 6 Click the row with the host you want to modify, and click **Modify**.

Step 7 On the **Modify Host** screen, the following fields can be changed:

Name	Description
Name field	Name of the host.
Description field	Enter a description of the host.
OS Type field	Enter the OS type.

Step 8 Click **Submit**.

Host Initiators Report

Initiators are endpoints from which iSCSI sessions originate. Any host bus adapter (HBA) can have one or more initiators registered on it. Each initiator is uniquely identified by its worldwide name (WWN or IQN).

The Host Initiators report provides the following information:

- Initiator Name
- Type
- Is Bound
- ISCSI Type
- Host
- Node WWN
- Port WWN

- CHAP Secret Enabled

The **Host Initiators Report** is located under the **Hosts** screen.

Creating a Host Initiator

VNXe supports iSCSI and FC initiators. The following information is required:

- WWN of FC Host Bus Adapter of the host
- ISCSI initiators
  - IQN of the iSCSI HBA on the host
  - CHAP username and CHAP secret (optional)

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device on which you want to create the host initiator, and click **View Details**.
Step 5 Click **Hosts**.
Step 6 Click the row with the host on which you want to create the host initiator, and click **View Details**.
Step 7 Click **Host Initiators**.
Step 8 Click **Create**.
Step 9 On the **Add Host Initiator** screen, complete the following fields:

Name	Description
Initiator Type drop-down list	Choose ISCSI or FC from the drop-down list.
IQN or WWN field	Specify the IQN for ICSCI access or the WWN for FC access.
CHAP User Name field	Specify the Chap User Name.
CHAP Secret field	Specify the Chap Secret.

Step 10 Click **Submit**.

Modifying a Host Initiator

For ISCSI initiators, CHAP information can be modified.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device that contains the host intiator you want to modify, and click **View Details**.

Step 5 Click **Hosts**.
Step 6 Click the row with the host that contains the host intiator you want to modify, and click **View Details**.
Step 7 Click **Host Initiators**.
Step 8 Click the row with the host intiator you want to modify.
Step 9 Click **Modify**.
Step 10 On the **Modify Host Initiator** screen, the following fields can be modified:

Name	Description
CHAP User Name field	Specify the Chap User Name.
CHAP Secret field	Specify the Chap Secret.

Step 11 Click **Submit**.

Registering a Host Initiator

The "Register" action can be used to manually connect an initiator to its host.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device that contains the host intiator you want to register, and click **View Details**.
Step 5 Click **Hosts**.
Step 6 Click the row with the host that contains the host intiator you want to register, and click **View Details**.
Step 7 Click **Host Initiators**.
Step 8 Click the row with the host intiator you want to register.
Step 9 Click **Register**.
Step 10 On the **Register Host Initiator** screen, click **Submit**.

Unregistering a Host Initiator

The "Unregister" action can be used to remove connected initiator paths.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device that contains the host intiator you want to unregister, and click **View Details**.
Step 5 Click **Hosts**.
Step 6 Click the row with the host that contains the host intiator you want to unregister, and click **View Details**.
Step 7 Click **Host Initiators**.

Step 8 Click the row with the host intiator you want to unregister.

Step 9 Click **Unregister**.

Step 10 On the **Unregister Host Initiator** screen, click **Submit**.

Host Luns Report

The Host Luns report shows information about the relationship between the LUNs and the hosts.

The Host Luns report contains the following information:

- LUN Name
- Host
- Host LUN Identifier (HLU)
- Type
- Read Only
- Snapshot

The **Host Luns Report** is located under the **Hosts** screen.

Host Initiator Paths Report

The Host Initiator Paths report shows initiator available paths.

The Host Initiator Paths report contains the following information:

- Initiator Name
- Is Logged On
- Registration Type
- Ethernet Port
- FC Port

The **Host Initiators Paths Report** is located under the **Hosts** screen.

Host IP Ports Report

The Host IP Ports report shows the information about host connections.

The report contains the following information:

- Address
- Type

- Subnet Mask
- Host

The **Host IP Ports Report** is located under the **Hosts** screen.

Creating a Host IP Port

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device on which you want to create the host IP port, and click **View Details**.
Step 5 Click **Hosts**.
Step 6 Click the row with the host on which you want to create the host IP port, and click **View Details**.
Step 7 Click **Host IP Ports**.
Step 8 Click **Create**.
Step 9 On the **Create Host IP Port** screen, complete the following fields:

Name	Description
Network Address field	Enter the IP address or network name for the port.

Step 10 Click **Submit**.

Modifying a Host IP Port

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device contains the host IP port you want to modify, and click **View Details**.
Step 5 Click **Hosts**.
Step 6 Click the row with the host that contains the host IP port you want to modify, and click **View Details**.
Step 7 Click **Host IP Ports**.
Step 8 Click the row with the host IP port you want to modify.
Step 9 Click **Modify**.
Step 10 On the **Modify Host IP Port** screen, the following fields can be changed:

Name	Description
Network Address field	Enter the new IP address or network name for the port.

Step 11 Click **Submit**.

FC Ports Report

The FC ports report shows the available Fiber Channel ports information.

The report contains the following information:

- Name
- Storage Processor
- WWN
- Current Speed
- Requested Speed
- Available Speeds
- SFP Supported Speeds

Ethernet Ports Report

The Ethernet Ports report shows Ethernet port configuration information.

The report contains the following information:

- Name
- Storage Processor
- Current Speed
- Requested Speed
- Supported Speeds
- Port Number
- MAC Address

File Interfaces Report

The File Interfaces report contains information about network interfaces in the VNXe system. These interfaces control access to Windows (CIFS) and UNIX/Linux (NFS) file storage.

Creating a File Interface

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device on which you want to create a file interface and click **View Details**.
Step 5 Click **File Interfaces**.
Step 6 Click **Create**.

Step 7 On the **Create File Interface** screen, complete the following fields:

Name	Description
Select NAS Server field	Select the NAS Server from the list.
Ethernet Port field	Select the Ethernet Port from the list.
IP Address field	Specify an IP Address.
Gateway field	Specify a Gateway.
Net Mask field	Specify a Net Mask.
Prefix Length field	Specify a Prefix length.
VLAN ID field	Specify a VLAN ID.
Configuration drop-down list	Choose one of the following options from the drop-down list: • Global • Override • Local

Step 8 Click **Submit**.

Modifying a File Interface

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNXe device that contains the file interface you want to modify and click **View Details**.

Step 5 Click **File Interfaces**.

Step 6 Click the row with the file interface you want to modify.

Step 7 Click **Modify**.

Step 8 On the **Modify File Interface** screen, the following fields can be modified:

Name	Description
Ethernet Port field	Select the Ethernet Port from the list.
IP Address field	Specify an IP Address.
Gateway field	Specify a Gateway.
Net Mask field	Specify a Net Mask.
Prefix Length field	Specify a Prefix Length.
vlan ID field	Specify a vlan ID.

Step 9 Click **Submit.**

ISCSI Nodes Report

The ISCSI nodes report shows information about available Ethernet ports that can be used for creating a ISCSI interface.

The report contains the following information:

- Name
- Ethernet Port
- Alias

ISCSI Interface Report

The ISCSI interface is necessary in order to access LUNs from Hosts through ISCSI access.

The report contains the following information:

- Port
- Port IQN
- IP Address
- Subnet Mask
- IP Protocol Version
- Prefix Length
- VLAN ID

Creating an ISCSI Interface

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNXe device on which you want to create the ISCSI interface and click **View Details**.

Step 5 Click **ISCSI Interfaces**.

Step 6 Click **Create**.

Step 7 On the **Create ISCSI Interface** screen, complete the following fields:

Name	Description
ISCSI Node field	Select the ISCSI Node from the list.
IP Address field	Specify the IP address.
Subnet Mask field	Specify the Subnet Mask.
IPv6 Prefix Length field	Specify the IPv6 Prefix Length.

Name	Description
Gateway field	Specify the Gateway.
VLAN ID field	Specify the VLAN ID.

Step 8 Click **Submit**.

Modifying an ISCSI Interface

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device that contains the ISCSI interface you want to modify, and click **View Details**.
Step 5 Click **ISCSI Interfaces**.
Step 6 Click the row with the ISCSI interface you want to modify.
Step 7 Click **Modify**.
Step 8 On the **Modify ISCSI Interface** screen, the following fields can be modified:

Name	Description
IP Address field	Specify the IP address.
Subnet Mask field	Specify the Subnet Mask.
IPv6 Prefix Length field	Specify the IIPV6 Prefix Length.
Gateway field	Specify the Gateway.
VLAN ID field	Specify the VLAN ID.

Step 9 Click **Submit**.

Fast Cache Report

The FAST Cache is a large capacity secondary cache that uses SAS Flash disks to improve system performance by extending the storage system's existing caching capacity. You can configure individual storage pools to use the FAST Cache. When you do this, all storage resources created in those pools use the FAST Cache.

The report contains the following information:

- Name
- Description
- Number of Disks
- Free Capacity (GB)
- Total Capacity (GB)

- Raid Level
- Disk Type

Disk Report

Disks report shows the following information about available disks:

- Name
- Usuable Capacity (GB)
- Total Capacity (GB)
- Model
- Tier Type
- Disk Group
- Storage Pool
- WWN
- Manufacturer
- Disk Technology

Storage Pool FAST VP Report

The Storage Pool FAST VP report shows information about FAST VP settings for the selected storage pool.

The report contains the following information:

- Storage Pool
- Schedule Enabled
- Data Relocation State
- Data Relocation Type
- Data Relocation Rate
- Data Relocated (GB)
- Data Moving Up (GB)
- Data Moving Down (GB)
- Data Moving Within Tier (GB)
- Last Start Time
- Last End Time

Start Data Relocation

Data can be relocated using the "Start relocation" action.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNXe device with the storage pool on which you want to start data relocation and click **View Details**.

Step 5 Click **Storage Pools**.

Step 6 Click the row with the storage pool on which you want to start data relocation and click **View Details**.

Step 7 Click **Fast VP**.

Step 8 Click the row with the storage pool.

Step 9 Click **Start Relocation**.

Step 10 On the **Start Data Relocation** screen, complete the following fields:

Name	Description
Data Relocation Rate drop-down list	Choose one of the following from the drop-down list: • High • Medium • Low

Step 11 Click **Submit**.

Stop Data Relocation

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNXe device with the storage pool on which you want to stop data relocation and click **View Details**.

Step 5 Click **Storage Pools**.

Step 6 Click the row with the storage pool on which you want to stop data relocation and click **View Details**.

Step 7 Click **Fast VP**.

Step 8 Click the row with the storage pool.

Step 9 Click **Stop Relocation**.

Step 10 On the **Stop Data Relocation** screen, click **Submit** .

Storage Pools Storage Tiers Report

The Storage pool Tiers report shows information about tiering configurations of selected storage pools.

The report contains the following information:

- Name
- Storage Pool
- Raid Type
- Stripe Width

- Free Capacity (GB)
- Total Capacity
- Used Capacity
- Data Moving Up (GB)
- Data Moving Down (GB)
- Data Moving Within Tier (GB)

Jobs Report

The Jobs Report lists all requests initiated in the system. It's used to check the progress of the request and the results.

The report contains the following information:

- ID
- Job Name
- Method Name
- Start Time
- Elapsed Time
- State Change
- Submit Time
- Progress%
- Current State

FAST VP Report

Fully Automated Storage Tiering for Virtual Pools (FAST VP) enables the system to retain the most frequently accessed or important data on fast, high-performance disks. FAST VP moves the less frequently accessed and less important data to lower-performance, cost-effective disks.

The report shows the details about FAST VP settings such as its Status, scheduled days, amount of data moved to high performance/capacity tiers, amount of data within the tier, etc.

Storage Tier Report

If FAST VP is installed on your system, you can create tiered storage pools, which consist of multiple disk types, such as Flash disks and SAS disks. Using a tiered pool optimizes disk utilization.

The report contains the following information:

- ID
- Tier Type
- Total Space (GB)
- Free Space (GB)
- Total Disks
- Unused Disks
- Tag

IP Interfaces Report

This report shows the IP Interfaces available and their IP Address, Subnet Mask, and what Ethernet Port on which each interface is running.

The report contains the following information:

- ID
- IP Address
- Netmask
- IP Protocol
- Prefix Length
- Ethernet PortID
- Tag

CIFS Server Report

It shows the details about the CIFS Server such as the file interface associated with it and its domain.

The report contains the following information:

- Name
- NAS Server
- WorkGroup
- File Interface
- NetBIOS Name
- Domain
- Organization
- SMBCA Support
- SMB MultiChannel
- SMB Protocol
- Tag

Creating a CIFS Server

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNXe device on which you want to create the CIFS server, and click **View Details**.

Step 5 Click **CIFS Server**.

Step 6 Click **Create**.

Step 7 On the **Create CIFS Server** screen, complete the following fields:

Name	Description
Select NAS Server field	Select the NAS from the list.
NetBios Name field	Specify the NetBios name.
WorkGroup field	Specify a workgroup.
Local Admin Password field	Enter the Local Admin password.

Step 8 Click **Submit**.

Modifying a CIFS Server

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device that contains the CIFS server you want to modify, and click **View Details**.
Step 5 Click **CIFS Server**.
Step 6 Click the row with the CIFS server you want to modify.
Step 7 Click **Modify**.
Step 8 On the **Modify CIFS Server** screen, you can modify the following fields:

Name	Description
NetBios Name field	Specify the NetBIOS name.
WorkGroup field	Specify a workgroup.
Local Admin Password check box	Enter the Local Admin password.

Step 9 Click **Submit**.

CIFS Share Report

The report provides information about Common Internet File System (CIFS) shares in the storage system. The system uses Active Directory to authenticate user and user group access to the share.

The report contains the following information:

- ID
- CIFS Share Name
- Type
- Path
- Creation Time
- Continuous Availability

- CIFS Encrypted
- Read-Only?
- Modified Time
- File System
- CIFS Share Description

Creating a CIFS Share

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNXe device on which you want to create the CIFS share, and click **View Details**.

Step 5 Click **CIFS Share**.

Step 6 Click **Create**.

Step 7 On the **Create CIFS Share** screen, complete the following fields:

Name	Description
File System field	Select the File System from the list.
Path field	Specify a path to a location in the file system.
Name field	Specify a name for the share.
Description field	Specify a description for the share.
CIFS Server field	Select a server from the list.
Is Read Only check box	When checked, enables read-only.
Is Encryption Enabled check box	When checked, enables CIFS encryption.
Is Continuous Availability Enabled check box	When checked, enables Continuous Availability.
Is Access Entry Enabled check box	When checked, enables Access Level Permissions.

Step 8 In the **Create CIFS Shares** dialog box, click **Submit.**

Modifying a CIFS Share

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNXe device that contains the CIFS share you want to modify, and click **View Details**.

Step 5 Click **CIFS Share**.

Step 6 Click the row with the CIFS share you want to modify.

Step 7 Click **Modify**.

Step 8 On the **Modify CIFS Share** screen, the following fields can be changed:

Name	Description
Description field	Specify a description for the share.
Is Read Only check box	When checked, enables read-only.
Is Encryption Enabled check box	When checked, enables CIFS encryption.
Is Continuous Availability Enabled check box	When checked, enables Continuous Availability.
Is Access Entry Enabled check box	When checked, enables Access Level Permissions.

Step 9 Click **Submit**.

DNS Server Report

The DNS Server Report shows the DNS Configuration and list of IP addresses that correspond to the name servers in the domain.

The report contains the following information:

- ID
- DNS Domain Name
- Origin
- Addresses
- Tag

Modifying a DNS Server

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNXe device that contains the DNS server you want to modify, and click **View Details**.

Step 5 Click **DNS Server**.

Step 6 Click the row with the DNS server.

Step 7 Click **Modify**.

Step 8 On the **Modify DNS Server** screen, the following fields can be changed:

Name	Description
Addresses field	Specify an address.

Name	Description
Origin drop-down list	Choose the DNS IP origin.

Step 9 Click **Submit**

NAS Server Report

This report contains the following information:

Storage Pool

Name

Mode

Used Space (GB)

Home Node

Current Node

Replication Enabled

Default Unix User

Default Windows User

MultiProtocol Enabled

Current Unix Directory

Creating a NAS Server

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNXe device on which you want to create the NAS server, and click **View Details**.

Step 5 Click **NAS Server**.

Step 6 Click **Create**.

Step 7 On the **Create NAS Server** screen, complete the following fields:

Name	Description
Storage Pool field	Select the storage pool from the list.
Name field	Name the file system.
Mode drop-down list	Choose Normal or Destination from the drop-down list.
Storage Processor field	Select the storage processor from the list.

Step 8 Click **Submit**.

Modifying a NAS Server

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device that contains the NAS server you want to modify, and click **View Details**.
Step 5 Click **NAS Server**.
Step 6 Click the row with the NAS server you want to modify.
Step 7 Click **Modify**.
Step 8 In the **Modify NAS Server** dialog box, the following fields can be changed:

Name	Description
Name field	Enter a new name for the server.

Step 9 Click **Submit**.

NFS Server Report

The NFS Server report shows the details about NAS Server instance with NFS protocol and file interfaces supporting it.

The report includes:

- Name
- NAS Server
- File Interface
- File Interface Name

Creating an NFS Server

You create the NFS server by specifying NAS Server running NFS protocol.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the VNXe device on which you want to create the NFS server, and click **View Details**.
Step 5 Click **NFS Server**.
Step 6 Click **Create**.
Step 7 On the **Create NFS Server** screen, complete the following fields:

Name	Description
Select the NAS Server field	Select the NAS server from the list.

Step 8 Click **Submit**.

Routes Report

The Routes report contains details about the Static IP Routes.

The report shows the following information:

- ID
- Destination
- Netmask
- Gateway
- Prefix Length
- IP Interface ID
- Interface IP Address

Creating a Route

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNXe device on which you want to create the route, and click **View Details**.

Step 5 Click **Routes**.

Step 6 Click **Create**.

Step 7 On the **Create Route** screen, complete the following fields:

Name	Description
IP Interface field	Select the IP interface from the list.
Type drop-down list	Choose Default, Host, or Subnet from the drop-down list.
Destination field	Specify the destination to be connected.
Gateway field	Enter the gateway address if it is a default route.
Net Mask field	Enter the net mask.

Step 8 Click **Submit**.

Modifying a Route

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the VNXe device that contains the route you want to modify, and click **View Details**.

Step 5 Click **Routes**.

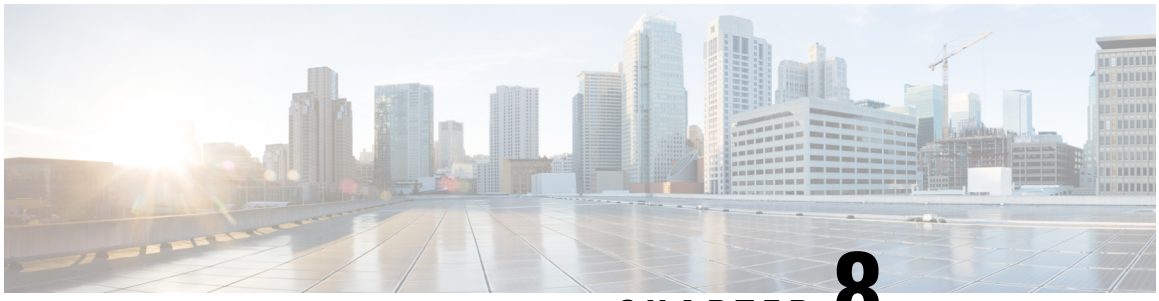
Step 6 Click the row with the route you want to modify.

Step 7 Click **Modify**.

Step 8 On the **Modify Route** screen, you can modify the following fields:

Name	Description
Type drop-down list	Choose Default, Host, or Subnet from the drop-down list.
Destination field	Specify the destination to be connected.
Gateway field	Enter the gateway address if it is a default route.
Net Mask field	Enter the net mask.

Step 9 Click **Submit**.



CHAPTER 8

EMC VPLEX

About EMC VPLEX

VPLEX is an EMC technology that provides a virtual storage system and access to data in the private cloud. A VPLEX can be implemented on Cisco UCS Director through a pod deployment such as Vblock, or as a standalone device. VPLEX has the following capabilities:

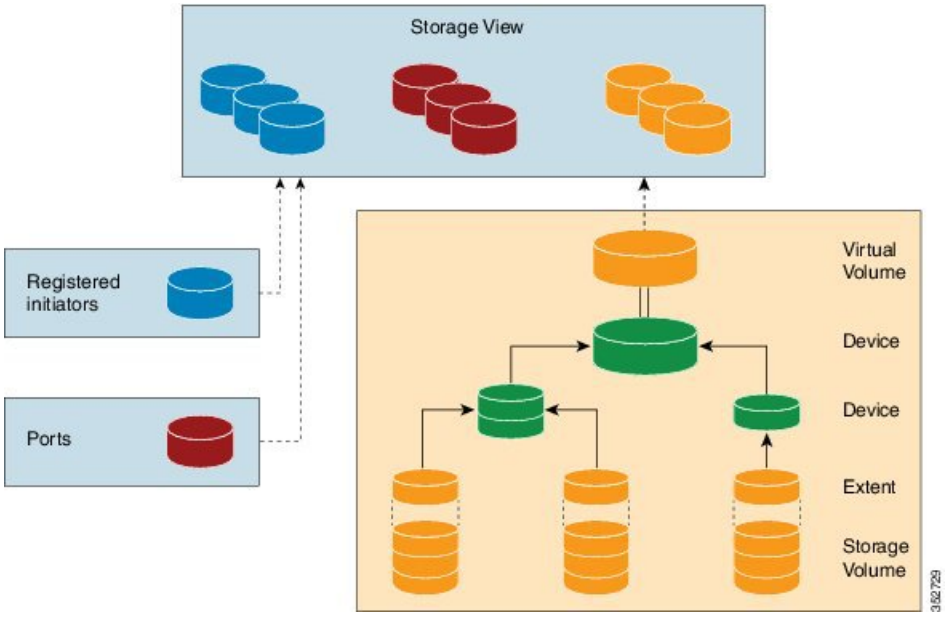
- Uses a single interface for a multi-vendor high-availability storage and compute infrastructure to dynamically move applications and data across different compute and storage locations in real time, with no outage required. VPLEX combines scaled clustering with distributed cache coherence intelligence within the same data center, across a campus, or within a specific geographical region. Cache coherency manages the cache so that data is not lost, corrupted, or overwritten.
- Dynamically makes data available for organizations. For example, a business can be sustained through a failure that would have traditionally required outages or manual restore procedures.
- Presents and maintains the same data consistently within and between sites, and enables distributed data collaboration.

- Establishes itself between ESX hosts that act as servers for virtual machines (VMs) and storage in a storage area network (SAN) where data can be extended within, between, and across pods.

EMC VPLEX Technology

EMC VPLEX encapsulates traditional physical storage array devices and applies three layers of logical abstraction to them. The logical relationships of each layer are shown in the Figure below.

Figure 1: VPLEX Logical Storage Structures



VPLEX uses extents to divide storage volumes. Extents can be all or part of the underlying storage volume. VPLEX aggregates extents and applies RAID protection in the device layer. Devices are constructed using one or more extents.

At the top layer of the VPLEX storage structures are virtual volumes, which are created by underlying devices and inherit their size. A virtual volume can be a single contiguous volume that is distributed over two or more storage volumes.

VPLEX exposes virtual volumes to hosts that need to use them with its front-end (FE) ports, which are visible to hosts. Access to virtual volumes is controlled through storage views. Storage views act as logical containers that determine host initiator access to VPLEX FE ports and virtual volumes.

VPLEX can use a Local or Metro external hardware interface depending on the network implementation described in the following sections. For more information on VPLEX solutions for VPLEX Local or Metro see the Data Center Interconnect Design Guide for Virtualized Workload Mobility with Cisco, EMC, and VMware.

VPLEX Local

Use VPLEX Local when homogeneous or heterogeneous storage systems are integrated into a pod and data mobility is managed between the physical data storage entities.

VPLEX Local has the following attributes:

- Up to four engines
- Up to 8000 logical unit numbers (LUNs)
- Single site
- Single pod

VPLEX Metro

Use VPLEX Metro when access and data mobility is required between two locations that are separated by synchronous distances. VPLEX Metro allows a remote site to present logical unit numbers (LUNs) without needing physical storage for them. VPLEX Metro configurations help users to transparently move and share workloads, consolidate a pod, and optimize resource utilization across pods.

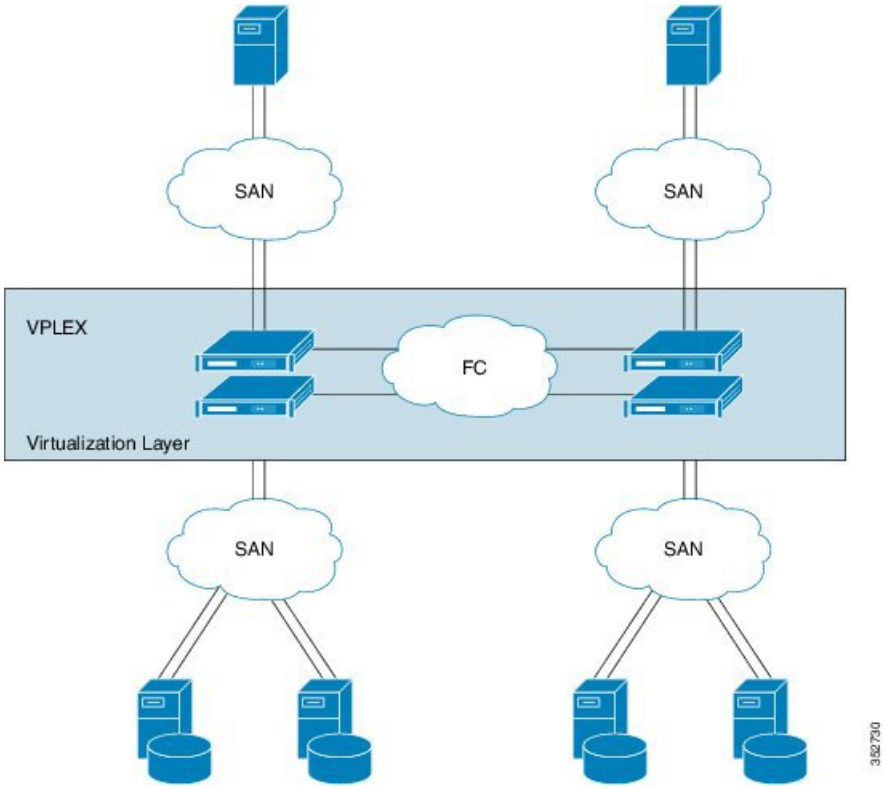
VPLEX Metro has the following attributes:

- One to eight engines
- Up to 16,000 LUNs
- Two sites
- Up to 100 kilometers

VPLEX Clustering Architecture

VPLEX uses clusters to break the boundaries of the pod and allow servers of multiple pods to have concurrent read and write access to shared block storage devices. The VPLEX cluster, shown in the Figure below is scalable. You can add up to four engines and connect multiple clusters to form a VPLEX Metro configuration. The engine is responsible for virtualizing the input and output stream and for connecting to hosts and storage using Fibre Channel connections to transfer data. VPLEX Metro currently supports up to two clusters in the same pod to provide nondisruptive data mobility, heterogeneous storage management, and improved application availability.

Figure 2: VPLEX Cluster Configuration



Managing the VPLEX Storage System for a Pod

The VPLEX virtual storage system technology for accessing data in the private cloud is associated with and supported by a pod. Cisco UCS Director collects data through the VPLEX Element Manager API and connects to the VPLEX server through HTTPS. After you establish a VPLEX account and associate a pod with a VPLEX cluster (made up of one, two, or four engines in a physical cabinet), you can configure, manage, and monitor the following VPLEX features in Cisco UCS Director:

- Cluster inventory of ESX hosts and reports for two or more VPLEX directors that form a single fault-tolerant cluster and that are deployed as one to four engines.
- VPLEX engine inventory and reports for an engine that contains two directors, management modules, and redundant power.
- Director inventory and reports for the CPU module(s) that run GeoSynchrony, the core VPLEX software. Two directors are in each engine; each has dedicated resources that can function independently.
- Port inventory and reports for Fast Ethernet ports and initiator ports.
- VPLEX (local, metro, or global) data cache report for the temporary storage of recent writes and recently accessed data.
- Storage volume inventory and reports for a logical unit number (LUN) exported from an array.
- Extent management (create, delete, report) for a slice (range of blocks) of a storage volume.

- Device management (create, delete, attach/detach mirror, report) for a RAID 1 device whose mirrors are in geographically separate locations.
- Virtual volume management (create, modify, delete, report) for a virtual volume that can be distributed over two or more storage volumes that are presented to ESX hosts.
- Storage views management (create, modify, delete, report) for a combination of registered initiators (hosts), front-end ports, and virtual volumes that are used to control host access to storage.
- Recovery point for determining the amount of data that can be lost before a given failure event.

For more information about VPLEX use cases, see the EMC VPLEX Metro Functional Overview section of the Cisco Virtualized Workload Mobility Design Considerations chapter in the Data Center Interconnect Design Guide for Virtualized Workload Mobility with Cisco, EMC, and VMware.

Adding an EMC VPLEX Account

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

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, choose **EMC VPLEX** from the **Account Type** drop-down list and click **Submit**.

Step 5 On the second **Add Account** screen, complete the following fields:

Name	Description
Account Name field	A unique name that you assign to this account.
Description field	A description of this account.
Server IP field	The IP address of the VPLEX server.
Use Credential Policy checkbox	Check this check box if you want to use a credential policy for this account rather than enter the username and password information manually.
Credential Policy drop-down list	If you checked the **Use Credential Policy** check box, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
Username field	The username that this account uses to access the VPLEX server. This username must be a valid account in the VPLEX server. This field is not displayed if you chose to use a credential policy.
Password field	The password associated with the username. This field is not displayed if you chose to use a credential policy.
Protocol drop-down list	You must use the **https** transport type protocol.
Port field	The port used to access the VPLEX server. Port 443 is the default secure HTTPS port.

Name	Description
Connection Timeout (Seconds) field	The length of time in seconds that Cisco UCS Director will wait to establish a connection to the VPLEX server before timing out. The default value is 30 seconds. The valid values are from 0 to 1800. An empty field or a value of 0 is interpreted as an infinite timeout.
Socket Read Timeout (Seconds) field	The length of time in seconds that Cisco UCS Director will wait for data from the VPLEX server before timing out. The default value is 30 seconds. The valid values are from 0 to 1800. An empty field or a value of 0 is interpreted as an infinite timeout.
Contact field	The email address that you use to contact the administrator or other person responsible for this account.
Location field	The location of the contact.

Step 6 Click **Submit**.

Cisco UCS Director tests the connection to the EMC VPLEX server. If that test is successful, it adds the VPLEX account and discovers all infrastructure elements in the storage system that are associated with that account. This discovery process and inventory collection cycle takes few minutes to complete.

The polling interval configured on the **System Tasks** tab on the **Administration** > **System** window specifies the frequency of inventory collection. For more information about configuring the polling interval, see the *Cisco UCS Director Network Devices Management Guide*.

System Requirements

Component	Requirement
Networking	Two Cisco Nexus 5000/5500 or 7000 Series switches Two Cisco UCS 6100 or 6200 Series Fabric Interconnects Cisco Nexus 1000V switch
Computing	One or multiple Cisco UCS chassis with modules that have two Fabric Extenders per chassis
Storage	EMC VNX, VMAX, Vblock, or VSPEX storage systems
Cisco UCS Director	See the Compatibility Matrix for all supported versions.
Cisco UCS Director Bare Metal Agent	See the Compatibility Matrix for all supported versions.
Cisco UCS Director —resource reservation	2 GB memory and minimum 3000-GHz CPU

Component	Requirement
Cisco UCS Director Bare Metal Agent—resource reservation	2 GB memory and minimum 2000-GHz CPU
VMware (vCenter Server/ESXI/ESXi/vSphere, or Microsoft Hyper-V Manager) server	See the Compatibility Matrix for all supported versions.

Assigning a Pod to a Cluster

You must also create a pod with each VPLEX cluster (1 and 2).

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.

Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device that you want.

Step 4 Choose **Clusters** and click the cluster that you want to assign to the pod.

Step 5 Click **Assign to Pod**.

Step 6 In the **Assign Pod to Cluster** page, complete the required field:

Name	Description
Select Pod drop-down list	Choose a pod type. This can be one of the following: • **Default Pod** • **VSPEX** • **Generic** • **Vblock**

Step 7 Click **Submit.**

Step 8 Repeat the previous steps to assign a pod to the other cluster.

Unassigning a Pod from a Cluster

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.

Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.

Step 4 Choose **Clusters** and click the cluster you want.

Step 5 Click **Unassign Pod**.

Step 6 In the **Unassign Pod from Cluster** page, click **Submit** to unassign the pod from the cluster.

Viewing VPLEX Engines

The duel VPLEX engines provide cache and processing power with redundant directors that each include two input and output (I/O) modules per director and one optional WAN COM I/O module for use in a VPLEX Metro configuration.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Engines**.
Information displays for the VPLEX engines, such as the serial numbers, engine IDs, and operational status.
Step 5 To view specific information about a specific engine, click on the engine and click **View Details**.
Information about the director, director ID, port, hostname, cluster, and so on, is displayed.

Rediscovering a Storage Array

Rediscover a storage array to view recently zoned and masked storage that has been presented to VPLEX.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Storage Arrays**.
Step 6 Click on a storage array.
Step 7 Click **Rediscover**.
Step 8 In the **Rediscover Storage Array** screen, click **Submit**.

Storage Volume Claiming

Storage volumes are logical unit numbers (LUNs) that are exported from an array. The claim process ensures that only relevant storage volumes can be processed when presented to the VPLEX cluster.

Claiming a Storage Volume

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.

Step 4 Choose **Clusters** and double-click the cluster you want to expand.

Step 5 Choose **Storage Volumes**.

Step 6 Click **Claim**.

Step 7 In the **Claim Storage Volume** screen, complete the required fields, including the following:

Name	Description
New name field	The user-defined name to be applied to the storage volume.
Thin Rebuild check box	Check the check box to set the LUN to thin provisioning upon rebuilding. Thin provisioning allocates what is needed while taking advantage of the dynamic thin allocation capabilities of the back-end storage volume. **Note** The actual storage allocated on a back-end storage volume is a function of the written portions of the storage volume, rather than the advertised capacity of the storage volume.
Application Consistent check box	Check the check box to allow the importation of existing LUNs that are one-to-one representations of existing storage volumes. These volumes can be easily imported by a host after removing VPLEX from the data path. The ability to easily move from virtualized to nonvirtualized disk storage is the main advantage to this approach. This approach limits the usable extent size to that of the underlying storage volume and imposes upper level limits on device layout and construction.

Step 8 Click **Submit.**

Unclaiming a Storage Volume

Storage volumes are logical unit numbers (LUNs) that are exported from an array. Unclaim storage volumes that are no longer relevant for processing by the VSPEX cluster.

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.

Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.

Step 4 Choose **Clusters** and double-click the cluster you want to expand.

Step 5 Choose **Storage Volumes**.

Step 6 Choose the storage volume that you want to unclaim.

Step 7 Click **Unclaim**.

Step 8 In the **Unclaim Storage Volume** screen, click **Submit** to unclaim the storage volume.

Extents

VPLEX uses extents to divide storage volumes. Extents can be all or part of the underlying storage volume. VPLEX aggregates extents and applies RAID protection in the device layer. Devices are constructed using one or more extents and can be combined into more complex RAID schemes and device structures as wanted.

Extents should be sized to match the desired capacity of the virtual volume. If the storage volume that you want to use for an extent is larger than the desired virtual volume, you should create an extent that is the size of the desired virtual volume.

Note Do not create smaller extents and then use devices to concatenate or stripe the extents.

Creating an Extent

You can create an extent for a storage volume and specify its capacity.

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.

Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.

Step 4 Choose **Clusters** and double-click the cluster you want to expand.

Step 5 Choose **Extents**.

Step 6 Click **Create**.

Step 7 In the **Create Extent** screen, complete the required fields, including the following:

Name	Description
Storage Volume field	Click **Select**. In the **Select** dialog box, chose a storage volume name and click **Select**.
Size (GB) field	The size of the extent in gigabytes.
Extent Count field	The number of extents for this storage volume.

Step 8 Click **Submit.**

Deleting an Extent

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.

Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.

Step 4 Choose **Clusters** and double-click the cluster you want to expand.

Step 5 Choose **Extents**.
Step 6 Choose the appropriate extent to delete.
Step 7 Click **Delete**.
Step 8 In the **Delete Extent** screen, click **Submit** to confirm your deletion.

VPLEX Storage Devices

A VPLEX storage device is made up of a single block storage device that uses storage from the VPLEX cluster. The following types of VPLEX devices are available:

- **RAID-0**—Provides a performance-oriented striped or dispersed data mapping technique.
- **RAID-1**—Provides a mirroring data mapping technique to keep two (or more) devices in an identical state at all times. If one device fails, the operating system (OS) can continue, using the remaining disk(s).
- **Concatenated RAID**—Shows that data is concatenated across a linear collection of disks.
- **1:1 Mapping of extents to devices**—Provides an option to create multiple devices from multiple extents with a mapping of one extent to one device.

Creating a VPLEX Storage Device

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Devices**.
Step 6 Click **Create**.
Step 7 In the **Create Device** screen, complete the required fields, including the following:

Name	Description
Type of Device drop-down list	Choose the type of storage device: • **RAID-0** • **RAID-1** • **Concatenated RAID** • **1:1 Mapping of extents to devices**
Source Extents field	Click the **Select** button. In the **Select** screen, choose one or more extents to create this local device and click **Select**. An extent is a slice (range of blocks) of a storage volume.

Name	Description
Target Extents field	Click the **Select** button. In the **Select** screen, choose a target extents to create the local device and click **Select**. An extent is a slice (range of blocks) of a storage volume. This field is displayed only when you select **RAID-1**.
Device Name field	The name of this single block storage device that is unique across all clusters.
Stripe Depth drop-down list	Choose how large you would like the stripe depth to be. The block size is 4 kilobytes. This field is displayed only when you select **RAID-0**.

Step 8 Click **Submit**.

Mirroring a VPLEX Storage Device

When a VPLEX storage device is mirrored, it creates a single view of storage data and makes this data accessible immediately to the host. This process eliminates the need for host-based mirroring, which saves the host CPU processing resources and increases high availability for critical applications.

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.

Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.

Step 4 Choose **Clusters** and double-click the cluster you want to expand.

Step 5 Choose **Devices**.

Step 6 Click **Attach Mirror**.

Step 7 In the **Attach Local/Remote Mirror** screen, complete the required fields, including the following:

Name	Description
Mirror Type drop-down list	Choose the type of storage device: • **Local**—Local storage device. • **Remote**—Remote storage device.
Mirror Device button	Click the **Select**. In the **Select** dialog box, choose the device that is to be attached to the VPLEX storage device as a mirror and click **Select**.

Step 8 Click **Submit.**

Viewing a VPLEX Storage Device

You can view VPLEX storage device information such as its total capacity in gigabytes, whether it is local or global (remote), if a rebuild is allowed, and whether it is RAID 1, RAID 0, or RAID C (concatenated).

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Devices**.
Step 6 Click **View Details**.
Step 7 Click **Submit.**

Detaching a Mirror from a VPLEX Storage Device

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Devices**.
Step 6 Click **Detach Mirror** icon.
Step 7 In the **Detach Local/Remote Mirror** dialog box, click **Select**. In the **Select** dialog box, choose the name of the mirrored device and click **Submit** to remove it from the VPLEX storage device.

Deleting a VPLEX Storage Device

You can delete a single block storage device that uses storage from the cluster.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Devices**.
Step 6 Choose the appropriate device to delete.
Step 7 Click **Delete**.
Step 8 In the **Delete Device** dialog box, click **Submit** to confirm your deletion.

Consistency Groups

Volumes are protected by consistency groups. If two data sets are dependent on one another (such as a database and a database log), they should be part of the same consistency group.

Virtual volumes are added to a consistency group when a consistency group is created. A consistency group ensures that there is application-dependent write consistency of application data on distributed virtual volumes within the system if a disaster occurs. The properties of the consistency group are then immediately applied to the added volumes.

Use the following guidelines for consistency groups:

- Only volumes with visibility and storage-at-cluster properties that match those properties of the consistency group can be added to the consistency group.
- The maximum number of volumes in a consistency group is 1000.
- You should group together volumes used by the same application or host in a consistency group.
- Only volumes with storage at both clusters (distributed volumes) are allowed in remote consistency groups.
- If any of the specified volumes are already in the consistency group, these volumes are skipped.
- When you initiate a detach rule for a consistency group, it takes 5 seconds to suspend the nonpreferred cluster and maintain input and output functions on the preferred cluster.

Creating a Consistency Group

Consistency groups allow you to group volumes together and apply a set of properties to the entire group.

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.

Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.

Step 4 Choose **Clusters** and double-click the cluster you want to expand.

Step 5 Choose **Consistency Groups**.

Step 6 Click **Create**.

Step 7 In the **Create Consistency Group** page, complete the required fields, including the following:

Name	Description
Group Name field	The group name, which is unique among all clusters.
Type drop-down list	Choose the type of virtual volumes that need to be added to the consistency group. This can be one of the following: • **Local:cluster-1** • **Global: All clusters**

Name	Description
Global Visibility check box	Check the check box to synchronize and make all global consistency groups visible to clusters.
Detach Rule drop-down list	Choose from the following detach (win) rules for each volume (cluster): • **cluster 1 detaches**—In any failure scenario, the preferred cluster for that volume is declared as cluster 1. • **cluster 2 detaches**—In any failure scenario, the preferred cluster for that volume is declared as cluster 2. • **no automatic winner**—The input/output (I/O) operation suspends at both VPLEX clusters if either the link partitions or an entire VPLEX cluster fails.
Delay field	The number of seconds after an inter-cluster link fails before the winning cluster detaches.
Virtual volume(s) field	Click **Select**. In the **Select** dialog box, choose the virtual volume(s) to add to the consistency group and click **Select**.

Step 8 Click **Submit.**

Adding a Virtual Volume to an Existing Consistency Group

You can add one or more virtual volumes to an existing consistency group.

Note You can also add virtual volumes when you create a consistency group.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Consistency Groups**.
Step 6 Choose **Add Virtual Volumes**.
Step 7 In the **Add Virtual Volume(s) to Consistency Groups** page, click **Select**.
Step 8 In the **Select** dialog box, choose the virtual volume(s) to add to the consistency group and click **Select**.
Step 9 Click **Submit.**

Removing a Virtual Volume from a Consistency Group

You can remove one or more virtual volumes from an existing consistency group.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Consistency Groups**.
Step 6 Click **Remove Virtual Volumes**.
Step 7 In the **Remove Virtual Volume(s) from Consistency Groups** page, click **Select**.
Step 8 In the **Select** dialog box, choose the virtual volume(s) to add to the consistency group and click **Select**.
Step 9 Click **Submit.**

Enabling or Disabling a RecoverPoint for a Consistency Group

A RecoverPoint can be enabled for a consistency group to provide any-point-in-time recovery for diversified storage environments both within and across pods to provide continuous data protection for operational and disaster recovery on VPLEX distributed virtual volumes within the VPLEX system. RecoverPoint can also be disabled for a consistency group.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Consistency Groups**.
Step 6 Click **Enable/Disable Recoverpoint**.
Step 7 In the **Enable/Disable Recoverpoint on Consistency Group** page, choose either **Enable** or **Disable** from the **Select Option** drop-down list.
Step 8 Click **Submit.**

Viewing a Consistency Group

You can view the virtual volumes that belong to a consistency group.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Consistency Groups**.
Step 6 Choose the consistency group that you want to view.

Note In the **Virtual Volumes** tab, you can see a list of the virtual volumes that belong to the consistency group.

Deleting an Existing Consistency Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Consistency Groups**.
Step 6 Choose the consistency group that you want to delete.
Step 7 Click **Delete**.
Step 8 In the **Delete Consistency Groups** confirmation dialog box, click **Submit**.

Distributed Devices and RuleSets

Creating a distributed device allows you to use storage from both clusters in a single VPLEX cluster (plex).

Each distributed device that spans two VPLEX clusters must have a RuleSet assigned to it. The RuleSet defines which cluster is declared a preferred cluster that maintains access to the volume and which cluster should be declared the nonpreferred cluster in a failure event. Once these roles are declared, the clusters' distributed devices detach so that they can resume normal input and output operations (I/O).

Viewing a RuleSet for a Distributed Device

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **RuleSets**.

Creating a Distributed Device

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Distributed Devices**.

Step 5 Click **Create**.

Step 6 In the **Create Distributed Device** screen, complete the required fields, including the following:

Name	Description
Souce Cluster	Click **Select**. In the **Select** dialog box, choose the source cluster to display source devices and click **Select**.
Souce Device	Click **Select**. In the **Select** dialog box, choose a local device as a source to create a distributed device and click **Select**.
Target Device field	Click **Select**. In the **Select** dialog box, choose a local device that you want to add as target to create as a distributed device and click **Select**.
Logging Volume(s) field	Click **Select**. In the **Select** dialog box, choose one or more logging volumes that you want to add to this distributed device and click **Select**.
Device Name field	The new device name that is unique across VPLEX.
RuleSet field	Click **Select**. In the **Select** dialog box, choose the RuleSet name that you previously configured and want to add to this distributed device and click **Select**.

Step 7 Click **Submit.**

Deleting a Distributed Device

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.

Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.

Step 4 Choose **Distributed Devices**.

Step 5 Choose the distributed device that you want to delete.

Step 6 Click **Delete**.

Step 7 In the **Delete Distributed Device** screen, click **Submit** to confirm your deletion.

Initiators

An initiator is a host that is registered with a port so that it can access the VPLEX storage network.

Creating an Initiator

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.

Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.

Step 4 Choose **Clusters** and double-click the cluster you want to expand.

Step 5 Choose **Initiators**.

Step 6 Click **Register**.

Step 7 In the **Register Host Initiator** screen, complete the required fields, including the following:

Name	Description
Type drop-down list	Choose the type of intiator: • **default**— Other software initiator. • **hpux**— HP (Hewlett Packard)-UX iSCSI software initiator • **sun-vcs**—Sun Microsystems, Inc and Veritas Cluster Server (VCS) software initiator • **aix**—IBM AIX software initiator • **recoverpoint**—EMC RecoverPoint initiator
Initiator Name field	The initiator hostname that is assigned to the registered port.
Port WWN	The worldwide name (WWN) in a Fibre Channel fabric that is a unique port identifier in the storage network.
Node WWN field	The WWN in a Fibre Channel fabric that is a unique node identifier in the storage network.

Step 8 Click **Submit.**

Viewing an Initiator

You can view an initiator host that has access to VPLEX storage:

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.

Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.

Step 4 Choose **Clusters** and double-click the cluster you want to expand.

Step 5 Choose **Initiators**.

Step 6 Click the initiator you want and click **View Details**.

Deleting an Initiator

You can delete an initiator that currently has VPLEX storage access.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Initiators**.
Step 6 Choose the name of the initiator host and click **Delete**.
Step 7 In the **Deregister Initiator Port** confirmation screen, click **Submit**.

Note Optionally, check **Force** to delete the initiator port if the initiator host attached to the port.

Virtual Volumes

VPLEX uses extents to divide storage volumes. Extents can be all or part of the underlying storage volume. VPLEX aggregates extents and applies RAID protection in the device layer. Devices are constructed using one or more extents.

At the top layer of the VPLEX storage structures are virtual volumes, which are created by underlying devices and inherit their size. A virtual volume can be a single contiguous volume that is distributed over two or more storage volumes.

VPLEX exposes virtual volumes to hosts that need to use them with its front-end (FE) ports, which are visible to hosts. Access to virtual volumes is controlled through storage views. Storage views act as logical containers that determine host initiator access to VPLEX FE ports and virtual volumes.

Creating a Virtual Volume

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Virtual Volumes**.
Step 6 Click **Create**.
Step 7 In the **Create Virtual Volume** screen, complete the required fields, including the following:

Name	Description
Select Local Device Name field	Click **Select**. In the **Select** dialog box, choose a local storage device and click **Select**.
Storage Tier ID field	The storage tier number that is used to manage the local storage volume as a single unit. Storage tiers are used to manage arrays based on price, performance, capacity and other attributes.

Step 8 Click **Submit**.

Enabling Remote Access on a Virtual Volume

You can allow remote access to a virtual volume for a host that needs to use it.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Virtual Volumes**.
Step 6 Choose a virtual volume name from the list.
Step 7 Click **Remote Access**.
Step 8 In the **Remote Access on Virtual Volume** screen, complete the following required field:

Name	Description
Select Access Type drop-down list	Choose from the following: • **Enable**—Activates remote access to this virtual volume. • **Disable**—Removes remote access to this virtual volume.

Step 9 Click **Submit**.

Expanding a Virtual Volume

A virtual volume is presented to a host that needs to use it.

Note A virtual volume can be expanded to include either extents or local devices.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Virtual Volumes**.
Step 6 Click **Expand**.
Step 7 In the **Expand Virtual Volume** screen, complete the required fields, including the following:

Name	Description
Device Type drop-down list	Choose from the following: • **Extent**—A slice (range of blocks) of a storage volume. • **Local Device**—One or more extents that have additional specific RAID properties. The local device must come from a cluster.
Select Extent field	This parameter is available if **Extent** was chosen as the device type. Click **Select**. In the **Select** dialog box, choose the extent that you want and click **Select**.
Select Local Device field	This parameter is available if **Local Device** was chosen as the device type. Click **Select**. In the **Select** dialog box, choose the local device that you want and click **Select**.

Step 8 Click **Submit**.

Viewing a Virtual Volume

You can view a single virtual volume from the cluster.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Virtual Volumes**.
Step 6 Choose the appropriate virtual volume to view.
Step 7 Click **View**.
Information about the virtual volume appears in a new view that describes the virtual volume attributes.

Deleting a Virtual Volume

You can delete a single block storage device that uses storage from the cluster.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Virtual Volumes**.
Step 6 Choose the appropriate virtual volume to delete.
Step 7 Click **Delete**.

Step 8 In the **Delete Virtual Volume** screen, click **Submit** to confirm your deletion.

Viewing Target Ports

Target ports are front-end (FE) ports where the director port is connected to host initiators. These ports are visible to hosts and contain such information as their name, node worldwide number (WWN), port WWN, whether they are enabled, their Director IDs, and so on.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Target Ports**.
Step 6 Click **View Details** to see more detailed information about an individual target port.

Storage Views

VPLEX allows host access to virtual volumes through storage views. Storage views act as logical containers that determine host initiator access to VPLEX front-end (FE) ports and virtual volumes.

Creating a Storage View

You can create a storage view that includes virtual volumes, and VPLEX ports to control host access to the virtual volumes.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Storage Views**.
Step 6 Click **Create**.
Step 7 In the **Create Storage View** screen, complete the following fields:

Name	Description
Select Target Port field	Click **Select**. In the **Select** dialog box, choose one or more target ports to add to the storage view and click **Select**.
Storage View Name field	The storage view that is unique across all clusters.

Step 8 Click **Submit**.

Deleting a Storage View

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Storage Views**.
Step 6 Click **Delete**.
Step 7 In the **Delete Storage View** confirmation screen, click **Submit**.

Note Optionally, check **Force** to delete the storage view if hosts are attached to this view.

Step 8 Click **Submit**.

Adding an Initiator to a Storage View

You can create a storage view that includes one or more initiator ports.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Storage Views**.
Step 6 Choose the storage view you want from the **Storage Views** panel.
Step 7 Click **Add Initiator**.
Step 8 In the **Add Initiators to Storage View** screen, click **Select**.
Step 9 In the **Select** screen, choose one or more initiator host accounts to add to the storage view and click **Select**.
Step 10 Click **Submit**.

Removing an Initiator from a Storage View

You can remove one or more initiator ports from a storage view.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.

Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Storage Views**.
Step 6 Choose the storage view you want from the **Storage Views** panel.
Step 7 Click **Remove Initiator**.
Step 8 In the **Remove Initiators from Storage View** screen, click **Select**.
Step 9 In the **Select** screen, choose one or more initiator host accounts to remove from the storage view and click **Select**.
Step 10 Click **Submit.**

Adding a Virtual Volume to a Storage View

You can create a storage view that includes virtual volumes.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choos **Storage Views**.
Step 6 Choose the storage view you want from the **Storage Views** panel.
Step 7 Click **Add Virtual Volume**.
Step 8 In the **Add Virtual Volume to Storage View** screen, complete the required fields, including the following:

Name	Description
Virtual Volume field	Click **Select**. In the **Select** dialog box, choose a virtual volume (see the **Name** column) and click **Select**.
LUN ID field	(Optional) enter the logical unit number (LUN) identifier.

Step 9 Click **Submit**.

Removing a Virtual Volume from a Storage View

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Storage Views**.
Step 6 Choose the storage view you want from the **Storage Views** panel.
Step 7 Click **Remove Virtual Volume**.

Step 8 In the **Remove Virtual Volume from Storage View** screen, click **Select** from the **Virtual volume** field.
Step 9 In the **Select** screen, choose a virtual volume and click **Select**.
Step 10 Click **Submit**.

Adding a Port to a Storage View

You can create a storage view that includes target ports. Target ports are front-end (FE) ports where the director port is connected to host initiators. These ports are visible to hosts and contain such information as their name, node worldwide number (WWN), port WWN, whether they are enabled, their Director IDs, and so on.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Storage Views**.
Step 6 Choose the storage view you want from the **Storage Views** panel.
Step 7 Click **Add Port**.
Step 8 In the **Add Target Ports to Storage View** screen, click **Select**.
Step 9 In the **Select** screen, choose one or more target ports to add to the storage view and click **Select**.
Step 10 Click **Submit.**

Removing a Port from a Storage View

You can remove target port(s) from a storage view.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Storage Views**.
Step 6 Choose the storage view you want from the **Storage Views** panel.
Step 7 Click **Remove Port**.
Step 8 In the **Remove Target Ports from Storage View** screen, click **Select**.
Step 9 In the **Select** screen, choose one or more target ports to remove from the storage view and click **Select**.
Step 10 Click **Submit**.

Logging Volumes

VPLEX uses logging volumes to track changes during a loss of connectivity or loss of a volume (mirror in a distributed device). You should create a logging volume on each cluster. Each logging volume must be large enough to contain one bit for every page of distributed storage space (approximately 10 gigabytes of logging volume space for every 320 terrabytes of distributed devices). The logging volumes can experience a lot of input and output during and after-link outages, so each logging volume should be striped across many disks for speed, and have a mirror on another fast disk to secure this information.

Creating a Logging Volume

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.

Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.

Step 4 Choose **Clusters** and double-click the cluster you want to expand.

Step 5 Choose **Logging Volumes**.

Step 6 Click **Create**.

Step 7 In the **Create Logging Volume** screen, complete the required fields, including the following:

Name	Description
Type of Device drop-down list	Choose the type of storage device: • **RAID-0**—Performance-oriented striped or dispersed data mapping technique. • **RAID-1**—Mirroring data mapping technique that keeps two (or more) devices in an identical state at all times.
Select Extents field	Click the **Select** button. In the **Select** dialog box, choose one or more extents for this device and click **Select**. An extent is a slice (range of blocks) of a storage volume.
Volume Name field	The volume name that is unique across all clusters.
Stripe Depth field	The stripe depth for a RAID-0 device.

Step 8 Click **Submit**.

Adding a Mirror to a Logging Volume

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.

Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.

Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Logging Volumes**.
Step 6 Choose a logging volume from the list.
Step 7 Click **Add Mirror**.
Step 8 In the **Select** screen, choose a storage volume and click **Select**.
Step 9 Click **Submit**.
The mirror is added to the logging storage volume.

Deleting a Logging Volume

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **Clusters** and double-click the cluster you want to expand.
Step 5 Choose **Logging Volumes**.
Step 6 Choose the appropriate logging volume to delete.
Step 7 Click **Delete**.
Step 8 In the **Delete Logging Volume** screen, click **Submit** to confirm your deletion.

Managing VPLEX System Tasks

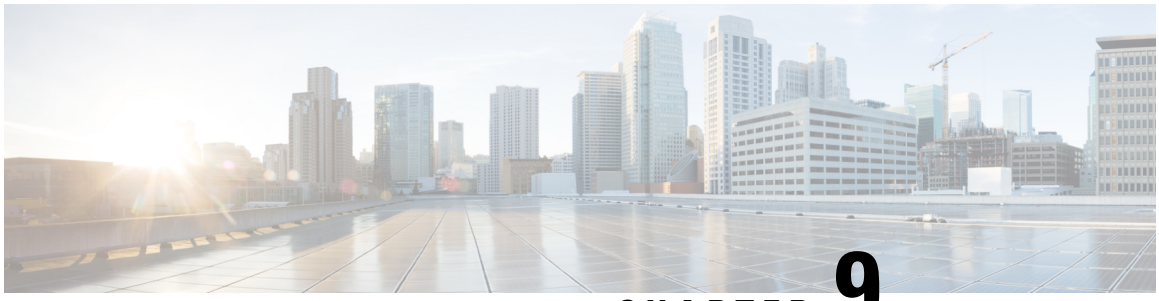
Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the account under **Multi-Domain Managers**.
Step 3 Choose **EMC VPLEX** to expand the connected VPLEX device(s) and click the VPLEX device you want.
Step 4 Choose **System Tasks**.
Step 5 Double-click the **EMC VPLEX Tasks** folder icon.
Step 6 Choose a VPLEX task and click **Manage Task**.
Step 7 In the **Manage Task** screen, complete the following fields:

Name	Description
Task Execution drop-down list	Choose **Enable** or **Disable** to enable or disable this VPLEX task.
System Task Policy drop-down list	Choose either the **default-system-task-policy** or the **local-run-policy** assigned to this VPLEX task.
Minutes drop-down list	Choose the frequency in minutes for how often the VPLEX task is executed.

Step 8 Click **Submit.**

Step 9 If you want to run this VPLEX task, click **Run Now**.

Step 10 If you want to view this VPLEX task, click **View Details**.



CHAPTER 9

EMC XtremIO

Overview

The XtremIO Storage Array is an all-flash system, based on a scale-out architecture. The system uses building blocks, called X-Bricks, which can be clustered together. The system operation, controlled by a stand-alone dedicated Linux-based server, is called the **XtremIO Management Server (XMS)**. Each XtremIO cluster requires an XMS host, which can be either a physical or a virtual server. A single XMS host can manage multiple clusters, so a single cluster may not require its own XMS host. The array continues operating if it is disconnected from the XMS, but cannot be configured or monitored.

XtremIO array architecture is designed to deliver the full performance potential of flash. Linear scaling of all resources, such as CPU, RAM, SSDs, and host ports, is done in a balanced manner. This allows the array to achieve any desired performance level, while maintaining consistency of performance that is critical to predictable application behavior. The XtremIO Storage Array provides a high level of performance that is consistent over time, system conditions, and access patterns. It is designed for high-granularity true random I/O.

Cluster performance level is not affected by capacity utilization level, number of volumes, or aging effects. Moreover, performance is not based on a "shared cache" architecture and is not affected by the data set size or data access pattern. Due to its content-aware storage architecture, XtremIO provides:

- Even distribution of data blocks, inherently leading to maximum performance and minimal flash wear
- Even distribution of metadata

- Freedom from hotspots in data or metadata
- Easy setup and no tuning
- Advanced storage functionality, including Inline Data Deduplication and Compression, thin provisioning, advanced data protection (XDP), snapshots, and more

XtremIO Connector in Cisco UCS Director

The XtremIO connector allows you to monitor and manage the XtremIO volumes, initiator groups, LUN mappings, snapshots, and basic network configurations. It connects through the HTTPS protocol. In order to manage XtremIO in Cisco UCS Director, the XMS Host IP is used when adding a physical account in Cisco UCS Director.

Orchestration

Viewing the Task Library

The Task Library contains Cisco UCS Director tasks related to Cisco EMC XtremIO. You can view the Task Library using the following steps.

Step 1 Choose **Orchestration**.
Step 2 On the **Orchestration** page, click **Workflows**.
Step 3 Click **Task Library**.
Step 4 On the **Task Library** screen, click **Submit** to launch the Task Library documentation.
Step 5 Scroll down the list to EMC XtremIO tasks.
Step 6 Clicking on any of the listed tasks takes you to the specifics of the task.

XtremIO Accounts

Adding an EMC XtremIO Account

To manage EMC XtremIO, Cisco UCS Director uses the XMS Host IP.

Step 1 Choose **Administration** > **Physical Accounts**.
Step 2 On the **Physical Accounts** page, click **Physical Accounts**.
Step 3 Click **Add**.
Step 4 On the **Add Account** screen, complete the following fields:
a) **Pod**—Choose a pod for the account from the drop-down list.
b) **Category**—Choose **Storage**.

c) **Account Type**—Choose **EMC XtremIO** from the drop-down list.

Step 5 Click **Submit**.

Step 6 On the second **Add Account** screen, complete the following fields:

a) **Account Name**—A unique name that you assign to this account.

b) **Description**—A description of this account.

c) **Management Server Address**—This can be an IPv4 or IPv6 address or the host address.

d) **Use Credential Policy**—Check this box if you want to use a credential policy for this account rather than enter the username and password information manually.

e) **Credential Policy** drop-down list—Choose the credential policy that you want to use from this drop-down list.

This field is only displayed if you choose to use a credential policy.

f) **Username**—The username that this account uses to access the XtremIO storage system. This username must be a valid account in the storage system.

This field is not displayed if you chose to use a credential policy.

g) **Password**—The password associated with the specified XtremIO username.

This field is not displayed if you chose to use a credential policy.

h) **Protocol**

Both HTTP and HTTPS are supported.

i) **Port**—The port used to access the XtremIO storage system.

Must not be Port 7225. Port number varies depending on implementation.

j) **Discover XtremIO Clusters**—Check this box if you want Cisco UCS Director to discover the available XtremIO clusters now so that you can choose the one you want to manage with this account.

If you check this box, the **Cluster Name** field becomes a drop-down list of the clusters managed by the XMS host. If you do not check this box, you must manually enter the information in the **Cluster Name** field.

k) **Cluster Name**—A valid name for the XtremIO cluster that you want to discover and manage with this account.

You must enter a valid name for an XtremIO cluster in this field if you did not check **Discover XtremIO Clusters**.

l) **Connection Timeout (Seconds)**—The length of time in seconds that Cisco UCS Director will wait to establish a connection to the XMS host before timing out.

The default value is 60 seconds The valid values are from 0 to 1800. An empty field or a value of 0 is interpreted as an infinite timeout.

m) **Socket Read Timeout (Seconds)**—The length of time in seconds that Cisco UCS Director will wait for data from the XMS host before timing out.

The default value is 50 seconds. The valid values are from 0 to 1800. An empty field or a value of 0 is interpreted as an infinite timeout.

n) **API Version**—Choose the API verson that is supported on the XtremIO storage system.

The default value is API version v2.

o) **Contact**—The email address that you use to contact the administrator or other person responsible for this account.

p) **Location**—The location of the contact.

Step 7 Click **Submit**.

Cisco UCS Director tests the connection to the EMC XtremIO storage system and XMS host. If that test is successful, it adds the XtremIO account and discovers all infrastructure elements in the storage system that are associated with that account. This discovery process and inventory collection cycle takes few minutes to complete.

The polling interval configured on the **System Tasks** tab on the **Administration** > **System** window specifies the frequency of inventory collection. For more information about configuring the polling interval, see the *Cisco UCS Director Network Devices Management Guide*.

Editing an XtremIO Account

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

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

Step 3 Click the XtremIO account that you wish to edit.

Step 4 Click **Edit**.

Step 5 On the **Edit Account** screen, you can edit the following fields:

a) **Description**

b) **Management Server Address**

c) **Use Credential Policy**

If checked, the **Credential Policy** drop-down list is shown.

d) **User Name**

e) **Password**

f) **Protocol**

Both HTTP and HTTPS are supported.

g) **Port**

Must not be 7225. Port number varies depending on implementation.

h) **Discover XtremIO Clusters** check box

If checked, a drop-down list of all of the XMS clusters is shown. You can choose the cluster to be managed.

i) **Cluster Name**

If the **Discover XtremIO Clusters** check box is not checked, enter a valid name of the cluster managed by the XMS host.

j) **Contact**

k) **Location**

Step 6 Click **Submit**.

Step 7 On the **Physical Accounts** page, choose the account.

Step 8 Click **Test Connection**.

XtremIO Volumes

A Volume is a set of blocks, presented to the operating environment as a range of consecutive logical blocks with disk-like storage and I/O semantics. It is possible to define various percentages of disk space as Volumes in an active cluster.

Creating an XtremIO Volume

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC XtremIO account for which you want to create a volume.

Step 5 Click **View Details**.

Step 6 Click **Volumes**.

Step 7 Click **Create**.

Step 8 On the **Create Volume** screen, complete the following:

a) Enter the volume name.
b) Enter the volume size.
c) From the **Capacity Type** drop-down list, choose the type of the device capacity.
d) From the **Logical Block Size** drop-down list, choose the block size of the volume. The size cannot be mofified later.
e) From the **Small Input/Output Alerts** drop-down list, choose **Enabled** to send alerts for higher number of small input or output.
f) From the **Unaligned Input/Output Alerts** drop-down list, choose **Enabled** to send alerts for higher number of unaligned input or output.
g) From the **VAAI TP Alerts** drop-down list, choose **Enabled** to send VAAI TP alerts.

Step 9 Click **Submit.**

Modifying an XtremIO Volume

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC XtremIO account for which you want to modify the volume.

Step 5 Click **View Details**.

Step 6 Click **Volumes**.

Step 7 Click the row with the volume that you wish to modify.

Step 8 Click **Modify**.

Step 9 On the **Modify Volume** screen, you can modify any or all of the following:

a) **Volume Name**
b) **Volume Size**
c) **Capacity Type**
d) Enable or disable the small input/output alerts.
e) Enable or disable the unaligned input/output alerts.
f) Enable or disable VAAI TP alerts.

Step 10 Click **Submit.**

XtremIO Initiator Groups

The XtremIO Storage Array uses the term "Initiators" to refer to ports that can access a Volume. Initiators are managed in the XtremIO Storage Array by assigning them to an Initiator Group. The Initiators within an Initiator Group share access to one or more of the cluster's Volumes.

Creating an Initiator Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC XtremIO account for which you want to create an initiator group.
Step 5 Click **View Details**.
Step 6 Click **Initiator Groups**.
Step 7 On the **Initiator Groups** page, click **Create**.
Step 8 On the **Create Initiator Group** screen, complete the following fields:
a) Enter the initiator group name.
b) Enter the initiator name in the following format: <*initiator name*>@<*port address*>. If there are multiple initiators, enter the comma separated intiator names in the specified format.
Step 9 Click **Submit.**

Renaming an Initiator Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC XtremIO account for which you want to rename the initiator group.
Step 5 Click **View Details**.
Step 6 Click **Initiator Groups**.

Step 7 Click the row with the initiator group that you wish to rename.
Step 8 Click **Rename**.
Step 9 On the **Rename Initiator Group** screen, type in a new name for the Initiator
Step 10 Click **Submit**

XtremIO Initiators

Initiators are added to the cluster by defining them in an Initiator Group. You can define Initiators when adding a group, or later define them by using the Edit Initiator Group option. To remove an Initiator, edit the group and delete the Initiator's properties.

Creating an Initiator

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC XtremIO account for which you want to create an initiator.
Step 5 Click **View Details**.
Step 6 Click **Initiators**.
Step 7 On the **Initiators** page, click **Create**.
Step 8 On the **Create Initiator** screen, complete the following fields:
a) Expand **Initiator Group Name** field and choose the group name where you wantto create an initiator.
b) Enter the initiator name.
c) Enter the initiator name in the following format: <*initiator name*>@<*port address*>. If there are multiple initiators, enter the comma separated intiator names in the specified format.
d) From the **OS** drop-down list, choose one of the following:

- Other
- Windows
- Linux
- ESX
- Solaris
- AIX
- HP-UX

Step 9 Click **Submit.**

Modifying an Initiator

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC XtremIO account for which you want to modify the initiator.

Step 5 Click **Initiators**.

Step 6 Click the row with the initiator that you want to modify.

Step 7 Click **Modify**.

Step 8 On the **Modify Initiator** screen, you can modify any or all of the following:

a) **Initiator Name**

b) **Port address**

c) From the **OS** drop-down list, choose one of the following:

- Other
- Windows
- Linux
- ESX
- Solaris
- AIX
- HP-UX

Step 9 Click **Submit.**

Volume Mapping

When you map a volume to an initiator group, a Logical Unit Number (LUN) is assigned to that volume.

You can map multiple volumes to an initiator group. The initiator group's first mapped volume is assigned a LUN of 1. Additional mapped volumes are assigned LUNs in sequential order. You can also manually enter a LUN ID during mapping. These numbers cannot be changed later so any change must be specified during LUN creation.

Mapping a Volume

Note You cannot change a LUN ID after a volume is mapped to an initiator group.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC XtremIO account for which you want to map a volume.
Step 5 Click **View Details**.
Step 6 Click **Volume Mapping**.
Step 7 Click **Map Volume**.
Step 8 On the **Map Volume** screen, do the following:
a) Expand the **Volume** field and choose the volume that you want to map.
b) Expand the **Initiator Group** and choose the initiator group where you want to map the volume.
c) In the **LUN ID** field, do one of the following:
- Enter a unique LUN ID to specify the LUN ID that you want to assign to the mapped volume.
- Leave the field empty to have the EMC XtremIO system automatically assign a LUN ID to the mapped volume.

d) Click **Submit**.

Unmapping a Volume

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC XtremIO account for which you want to unmap a volume.
Step 5 Click **View Details**.
Step 6 Click **Volume Mapping**.
Step 7 Click the row with the volume that you want to unmap.
Step 8 Click **UnMap Volume**.
Step 9 Click **Submit**.

Consistency Groups

Consistency Groups (CG) are used to create a consistent image of a set of Volumes, usually used by a single application, such as a database. With XtremIO CGs, you can create a Snapshot of all Volumes in a group, using a single command. This ensures that all Volumes are created at the same time. Many operations that are applied on a single Volume can also be applied on a CG.

Adding a Consistency Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC XtremIO account to which you want to add a consistency group.
Step 5 Click **View Details**.
Step 6 Click **Consistency Group**.
Step 7 Click **Create**.
Step 8 On the **Create EMC XtremIO Consistency Group** screen, complete the following fields:
a) Enter the consistency group name.
b) Expand the **Volume** field and check the volumes that you want to use for the Consistency Group.
Step 9 Click **Submit**.

Renaming a Consistency Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC XtremIO account for which you want to rename the consistency group.
Step 5 Click **View Details**.
Step 6 Click **Consistency Group**.
Step 7 Click the row with the consistency group that you want to rename.
Step 8 Click **Rename**.
Step 9 On the **Rename Consistency Group** screen, enter the consistency group name.
Step 10 Click **Submit**.

Viewing a Consistency Group Report

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC XtremIO account for which you want to view the consistency group report.
Step 5 Click **View Details**.
Step 6 Click **Consistency Group**.
A list of Consistency Groups available under the EMC XtremIO account is displayed.

Adding a Volume to a Consistency Group

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC XtremIO account.
Step 5 Click **View Details**.
Step 6 Click **Consistency Group**.
Step 7 Click the row with the consistency group to which you want to add a volume.
Step 8 Click **Add Volume**.
Step 9 On the **Add Volume to Consistency Group** screen, expand **Volume** and check a volume that you want to add to the consistency group.
Step 10 Click **Submit.**

Removing a Volume from a Consistency Group

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC XtremIO account.
Step 5 Click **View Details**.
Step 6 Click **Consistency Group**.
Step 7 Click the row with the consistency group from which you to remove the volume.
Step 8 Click **Remove Volume**.
Step 9 On the **Remove Volume from Consistency Group** screen, expand **Volume** and check the volumes that you want to remove from the consistency group.
Step 10 Click **Submit.**

iSCSI

To establish an iSCSI connection for transferring data, first define an iSCSI portal. An iSCSI portal is an IPv4 address and port associated with a Target port. Each iSCSI Target can be associated with multiple portals. If an IP connection requires routing to remote networks, you can define routing rules that apply to the iSCSI Target ports only.

Creating an iSCSI Portal

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC XtremIO account for which you want to create an iSCSI portal.

Step 5 Click **View Details**.

Step 6 Click **iSCSI Portals**.

Step 7 Click **Create**.

Step 8 On the **Create iSCSI Portal** screen, complete the following fields:

a) Enter the IPv4 address with the CIDR notation (*XX.XX.XX.XX/XX*).

b) Enter the VLAN number for the iSCSI portal in the range of 0 to 4094.

c) Expand **iSCSI Target** and check the target that you want to use.

Step 9 Click **Submit.**

Creating an iSCSI Route

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC XtremIO account for which you want to create an iSCSI route.

Step 5 Click **View Details**.

Step 6 Click **iSCSI Routes**.

Step 7 Click **Create**.

Step 8 On the **Create iSCSI Routes** screen, complete the following fields:

a) Enter the name of the iSCSI route.

b) Enter the destination network address of the iSCSI route with the CIDR notation.

c) Enter the gateway IP address.

Step 9 Click **Submit.**

Snapshots

Snapshots are instantaneous copy images of Volume data. The state of the data captured is exactly as it appeared at the specific point in time that the Snapshot was created. This enables you to save the Volume data state and then access the specific Volume data whenever needed, including after the source Volume has changed.

A Snapshot can be taken either directly from a source Volume or from other Snapshots within a source Volume's group (Volume Snapshot Group). XtremIO Snapshots are by default read-write, but can be created as read-only to maintain immutability.

The source data remains available without interruption, while the Snapshot can be used to perform other functions on the data. Changes made to the Snapshot's source do not affect the Snapshot data.

XtremIO Snapshots are space-efficient both in terms of metadata consumed and physical capacity. Snapshots are implemented using redirect-on-write methodology. New writes to the source Volume (or Snapshot) are

redirected to new locations, and only metadata is updated to point to the new data location. This method guarantees that there is no performance degradation while Snapshots are created.

Creating a Snapshot Scheduler

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC XtremIO account for which you want to create a snapshot scheduler.

Step 5 Click **View Details**.

Step 6 Click **Schedulers**.

Step 7 Click **Create**.

Step 8 On the **Create Snapshot Scheduler** screen, complete the following fields:

a) From the **Scheduler to be created on** drop-down list, choose **Volumes**, **Consitency Group**, or **Snapshot Set** and then do one of the following:

- Expand **Volume** and check the volume that you want to use.
- Expand **Consitency Group** and check the consistency group that you want to use.
- Expand **Snapshot Set** and check the snapshot set that you want to use.

b) From the **Schedule** drop-down list, choose either **Fixed Interval** or **Explicit Time** and then do one of the following.

- In the **Snapshot Fixed Schedule** field, enter the desired time in the following format: hh:mm:ss.
- Enter the snapshot explicit schedule and choose the snapshot explicit schedule day.

c) In the **Number of Snapshots to Keep** field, enter a number of snapshots to be saved.

d) If a suffix is required for the scheduler, enter it in the **Suffix** field.

e) From the **Snapshot Type** drop-down list, choose **Read/Write** or **Read Only**.

Step 9 Click **Submit.**

Viewing Snapshot Sets

A Snapshot Set is a group of Snapshots that were taken using a single command and represents a point in time of a group. A Snapshot Set can be the result of a Snapshot taken on a CG, on another Snapshot Set, or on a set of Volumes that were selected manually. A Snapshot Set maintains a relationship with the ancestor from which it was created.

Step 1 Choose **Physical** > **Storage**.

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

Step 3 On the **Storage** page, click **Storage Accounts**.

Step 4 Click the row with the EMC XtremIO account.

Step 5 Click **View Details**.

Step 6 Click **Snapshot Sets**.
A list of Snapshot Sets is displayed. You can also click **Snapshots** and see more information about the Snapshot Sets.

Creating a Snapshot Set

Note The **Create Snapshot Set** feature is also available under the **Snapshots** tab. The steps used to create a Snapshot Set are identical.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC XtremIO account for which you want to create a snapshot set.
Step 5 Click **View Details**.
Step 6 Click **Snapshot Sets**.
Step 7 Click **Create**.
Step 8 On the **Create Snapshot Set** screen, complete the following fields:
a) Enter a name in the **Snapshot Set Name** field.
b) (Optional). Enter a suffix for the snapshot name in the **Snapshot Suffix** field. (Optional)
c) From the **Type** drop-down list, choose **Read/Write** or **Read Only**.
d) From the **Snapshot Origin Type** drop-down list, choose **Volumes**, **Consitency Group**, or **Snapshot Set** and then do one of the following:
- Expand **Volume** and check the volumes that you want to use.
- Expand **Consitency Group** and check the consistency group that you want to use.
- Expand **Snapshot Set** and check the snapshot set that you want to use.

Step 9 Click **Submit.**

System Reports

Cisco UCS Director XtremIO provides the following System Reports:

- Clusters Report

The following reports are displayed as child reports under the Clusters Report.

- Bricks Report
- Storage Controllers Report
- SSDs Report
- Data Protection Report

- X-Env Report
- Targets Report

Viewing System Reports

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC XtremIO account for which you want to view system reports.
Step 5 Click **View Details**.
Step 6 Click **Clusters**.
Step 7 Click the row with the cluster for which you want to view system reports.
Step 8 Click **View Details**.
The child reports are available as separate tabs. Clicking the desired tab displays the details of the report.

Other Configurations

Viewing the Email Notifier

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC XtremIO account.
Step 5 Click **View Details**.
Step 6 Click **Clusters** .
Step 7 Click the row with the cluster for which you want to view the email notifier.
Step 8 Click **View Details**.
Step 9 Click **Email Notifier**.
Details about the Email Notifier are displayed.

Viewing the SNMP Notifier

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.

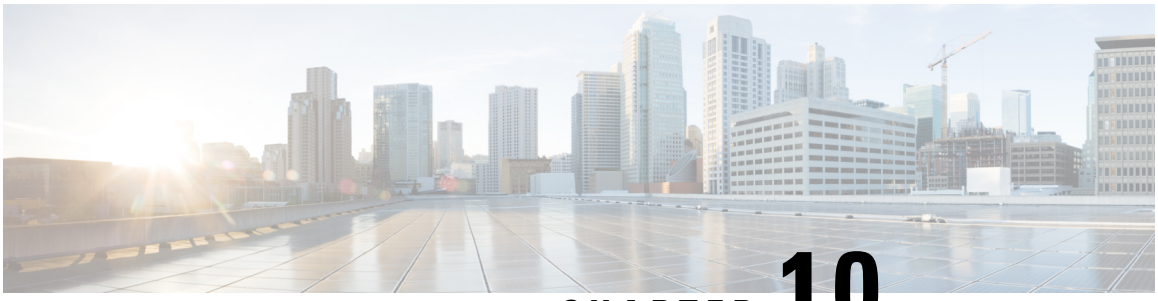
Step 4 Click the row with the EMC XtremIO account.
Step 5 Click **View Details**.
Step 6 Click **Clusters** .
Step 7 Click the row with the cluster for which you want to view the SNMP notifier.
Step 8 Click **View Details**.
Step 9 Click **SMTP Notifier**.
Details about the SMTP Notifier are displayed.

Viewing the Syslog Notifier

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Storage** page, choose the pod.
Step 3 On the **Storage** page, click **Storage Accounts**.
Step 4 Click the row with the EMC XtremIO account.
Step 5 Click **View Details**.
Step 6 Click **Clusters** tab.
Step 7 Click the row with the cluster for which you want to view the syslog notifier.
Step 8 Click **View Details**.
Step 9 Click **Syslog Notifier**.
Details about the Syslog Notifier are displayed.

PART II

EMC Data Protection Systems



CHAPTER 10

EMC RecoverPoint

EMC RecoverPoint Support

EMC RecoverPoint protects storage array logical unit numbers (LUNs) and provides concurrent local and remote data replication. RecoverPoint also provides continuous data protection for operational and disaster recovery by enabling any point-in-time recovery (PITR) for diversified storage environments both within and across pods.

RecoverPoint secures data by providing synchronous and asynchronous replication across heterogeneous arrays for block-based storage protocols. Replication improves reliability, fault-tolerance, and accessibility to data. If data becomes compromised or lost, you can look at data back in time and recover it by extending the vCenter VMware Site Recovery Manager (SRM) functionality with PITR capabilities.

RecoverPoint provides the ability to do the following:

- Enable continuous data protection for any PITR to optimize the recovery point objective (RPO) and recovery time objective (RTO).
- Ensure recovery consistency for inter-dependent applications.
- Provide synchronous or asynchronous replication policies.
- Reduce WAN bandwidth consumption and utilize available bandwidth optimally.

In Cisco UCS Director, you can access the following EMC RecoverPoint reports for Vblock clusters:

- Consistency groups that ensure that there is application-dependent write consistency of application data on VPLEX distributed virtual volumes within the VPLEX system in the event of a disaster.
- Consistency group copies of the initial consistency groups.
- Replication sets that consist of a production source volume and its local or local and remote replica volumes. One or more replication sets makes up a consistency group.

Note For more details about scalability and configuration options, see the EMC RecoverPoint documentation.

Adding an EMC RecoverPoint Account

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

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, do the following:

a) From the **Account Type** drop-down list, choose **EMC RecoverPoint**.

b) Click **Submit**.

Step 5 On the next **Add Account** screen, complete the following fields:

Name	Description
Account Name field	A unique name for this RecoverPoint account.
Description field	A description of this account.
Server IP field	The IP address of the RecoverPoint system.
Use Credential Policy checkbox	Check this check box if you want to use a credential policy for this account rather than enter the username and password information manually.
Credential Policy drop-down list	If you checked the **Use Credential Policy** check box, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
Username field	The username that this account uses to access the RecoverPoint system. This username must be a valid account in the RecoverPoint system. This field is not displayed if you chose to use a credential policy.
Password field	The password associated with the username. This field is not displayed if you chose to use a credential policy.
Protocol drop-down list	Choose one of the following transport types that you want to use for this account: • **http** • **https** The default transport type protocol for this account is HTTPS.
Port field	The port used to access the RecoverPoint system. Port 7225 is the default secure HTTPS port through which Cisco UCS Director connects to the RecoverPoint system to obtain data.

Name	Description
API Version drop-down list	Choose the API verson that is supported on the RecoverPoint server. The default is API version 4_0.
Connection Timeout (Seconds) field	The length of time in seconds that Cisco UCS Director will wait to establish a connection to the RecoverPoint server before timing out. The default value is 60 seconds. The valid values are from 0 to 1800. An empty field or a value of 0 is interpreted as an infinite timeout.
Socket Read Timeout (Seconds) field	The length of time in seconds that Cisco UCS Director will wait for data from the RecoverPoint server before timing out. The default value is 60 seconds. The valid values are from 0 to 1800. An empty field or a value of 0 is interpreted as an infinite timeout.
Contact field	The email address that you use to contact the administrator or other person responsible for this account.
Location field	The location of the contact.

Step 6 Click **Submit**.

Cisco UCS Director tests the connection to the EMC RecoverPoint server. If that test is successful, it adds the RecoverPoint account and discovers all infrastructure elements in the storage system that are associated with that account. This discovery process and inventory collection cycle takes few minutes to complete.

The polling interval configured on the **System Tasks** tab on the **Administration** > **System** window specifies the frequency of inventory collection. For more information about configuring the polling interval, see the *Cisco UCS Director Network Devices Management Guide*.

RecoverPoint Appliance Clusters

RecoverPoint Appliance (RPA) clusters are a group of two to eight physical (or virtual) RPAs at the same geographic location. These clusters work together to replicate and protect data.

Assigning a RecoverPoint Cluster to a Pod

You can assign a RecoverPoint cluster to a pod in Cisco UCS Director. This configuration is optional.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.
Step 3 Choose **EMC RecoverPoint**.
Step 4 Click the row with the EMC RecoverPoint account that contains the cluster you want to assign to a pod.
Step 5 Click **View Details**.
Step 6 Click **Clusters**.
Step 7 Click the row with the cluster that you want to assign and then click **Assign to Pod**.

Step 8 On the **Assign Pod to Cluster** screen, choose a pod type from the**Select Pod** drop-down list and click **Submit**.

Repeat the previous steps if you need to assign another cluster to a pod.

What to do next

You can double-click a RecoverPoint cluster to view the cluster summary, cluster gateway, splitters, RPAs, VMware vCenter servers and filters, the repository volume, and other cluster volume information.

Unassigning a RecoverPoint Cluster from a Pod

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Choose **EMC RecoverPoint**.

Step 4 Click the row with the EMC RecoverPoint account that contains the cluster you want to unassign.

Step 5 Click **Clusters**.

Step 6 Click the row with the cluster that you want to unassign.

Step 7 Click **Unassign from Pod** and then click **Submit**.

Replication Through Consistency Groups

In EMC RecoverPoint, volumes are protected by consistency groups. A consistency group ensures that updates to production volumes are also written to copies in a consistent and correct write-order. This configuration ensures that the copy can always be used to continue working from, or to restore the production source. The volumes must be replicated together in one consistency group to guarantee that at any point in time, the saved data is in true form. If two data sets are dependent on each other (such as a database and a database log), they should be part of the same consistency group.

EMC RecoverPoint also supports simultaneous bidirectional replication. With this type of replication, the same RecoverPoint appliance (RPA) can serve as the source RPA for one consistency group and the target RPA for another consistency group.

For more detailed guidelines about RecoverPoint consistency groups, see the *EMC RecoverPoint Administrator's Guide*, which can be obtained from EMC.

Setting Up Replication

This procedure provides an overview of how to set up replication with a RecoverPoint consistency group in Cisco UCS Director.

Step 1 Create a consistency group with a production copy.

See Creating a Consistency Group, on page 209.

Step 2 Create a consistency group copy to act as the replica for the production copy.

See Creating a Consistency Group Copy, on page 213.

Step 3 Create a replication set for each production volume that you want to replicate.

See Creating a Replication Set, on page 217.

Step 4 Add one or more user volumes to the consistency group copy in a replication set.

The user volume is the primary volume in a replication set that contains the data you want to protect. See Adding a User Volume to a Consistency Group Copy, on page 218.

Step 5 Add one or more journal volumes to the consistency group copy in a replication set

Journal volumes hold system information or point in time history and can be either a copy journal or a production journal. See Adding a Journal Volume to a Consistency Group Copy, on page 219.

Step 6 Add a link to a consistency group copy.

This link is used to transfer data between the production copy and the replication copies. See Adding a Link Between Consistency Group Copies, on page 220.

Step 7 Enable the consistency group.

See Enabling a Consistency Group, on page 211.

Step 8 Enable the consistency group copy.

See Enabling a Consistency Group Copy, on page 215.

Step 9 Start the data transfer.

You must initiate the first data transfer. It does not start automatically. See Starting Data Transfer for a Consistency Group, on page 222 and Starting a Transfer for a Consistency Group Copy, on page 222.

Creating a Consistency Group

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Choose **EMC RecoverPoint**.

Step 4 Click the row with the EMC RecoverPoint account where you want to create the consistency group.

Step 5 Click **View Details**.

Step 6 Click **Consistency Groups**.

Step 7 Click **Create**.

Step 8 On the **Create Consistency Group** screen, complete the following fields:

Name	Description
Consistency Group Name	A group name that is unique among all clusters.
Production Name	A descriptive name for the production copy.

Name	Description
Cluster	Choose the RecoverPoint cluster where you want to create the group and then click **Validate**.
Modify Group Policy check box	(Optional) Check this check box if you want to modify the default group policy options and choose the primary and secondary RPAs for the consistency group.
Modify Copy Policy check box	(Optional) Check this check box if you want to modify the default production copy policy options.
Group Policy—Displayed only if you checked the **Modify Group Policy** check box.	
Primary RPA	Choose the primary RecoverPoint appliance for this group.
Priority drop-down list	Choose the priority for the consistency group.
Distribute Group check box	Check this box if you want to create a group that can write across multiple RPAs. Each RecoverPoint system allows a maximum of eight distributed consistency groups.
Secondary RPAs	If you checked the **Distribute Group** check box, choose one or more secondary RPAs that you want to distribute data writes to.
Copy Policy—Displayed only if you checked the **Modify Copy Policy** check box.	
Host OS drop-down list	Choose the host operating system.
Journal Policy—Displayed only if you checked the **Modify Copy Policy** check box.	
Journal Compression drop-down list	Choose the journal compression level.
Maximum Journal Lag drop-down list	Choose the maximum journal lag.
Required Protection Window check box	Check this check box if you want to enable a protection window.
Protection Window	If you checked the **Required Protection Window** check box, enter the length of time for the protection window.
Window unit drop-down list	If you checked the **Required Protection Window** check box, choose the window time unit.
Enable Snapshot Consolidation check box	Check this box if you want to enable snapshot consolidation.
Do not consolidate snapshots for at least below period	If you checked the **Enable Snapshot Consolidation** check box, enter the length of time for which snapshot consolidation should not be performed.
Unit (Consolidation Period) drop-down list	If you checked the **Enable Snapshot Consolidation** check box, choose the consolidation period unit.

Name	Description
consolidate to one snapshot per day	If you checked the **Enable Snapshot Consolidation** check box, enter the number of days to consolidate snapshots that are older than the consolidation period.
Indefinitely check box	If you checked the **Enable Snapshot Consolidation** check box, check this check box if you want to consolidate snapshots for an indefinite number of days.
consolidate to one snapshot per week	If you checked the **Enable Snapshot Consolidation** check box, enter the number of weeks to consolidate snapshots that are older than the consolidation period.
Indefinitely check box	If you checked the **Enable Snapshot Consolidation** check box, check this check box if you want to consolidate snapshots for an indefinite number of weeks.

Step 9 Click **Submit**.

Enabling a Consistency Group

Enable each consistency group after you add the links between the consistency group copies.

Before you begin

Add the links between the consistency group copies. See Adding a Link Between Consistency Group Copies, on page 220.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.
Step 3 Choose **EMC RecoverPoint**.
Step 4 Click the row with the EMC RecoverPoint account with the consistency group that you want to enable.
Step 5 Click **Consistency Groups**.
Step 6 Click the row with the consistency group that you want to enable.
Step 7 From the **More Actions** drop-down list, choose **Enable**.
Step 8 On the **Enable Consistency Group** screen, click **Submit**.

Applying a Bookmark to a Consistency Group

A bookmark is a text label that uniquely identifies a consistency group. You can bookmark a consistency group at any time. However, you cannot bookmark a disabled consistency group. Bookmarks are useful to mark particular points in time, such as an event in an application, or a point in time to fail over.

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Choose **EMC RecoverPoint**.

Step 4 Click the row with the EMC RecoverPoint account with the consistency group you want to bookmark.

Step 5 Click **View Details**.

Step 6 Click **Consistency Groups**.

Step 7 Click the row with the consistency group that you want to bookmark.

Step 8 From the **More Actions** drop-down list, choose **Apply Bookmark**.

Step 9 On the **Apply Bookmark** screen, complete the following fields:

Name	Description
Bookmark Name field	A unique name for the bookmark.
Consistency Type drop-down list	Choose one of the following consistency types: • **Crash-Consistent**—Creates snapshots (points in time) that are crash-consistent for data files, control files, and logs that are in the same RecoverPoint consistency group. This is the default type. • **Application-Consistent**—Used to bookmark Microsoft Volume Shadow Copy Service (VSS)-aware applications in many consistency groups. VSS guarantees that the applications are in a consistent state at the point-in-time when each bookmark is applied to an image. As a result, recovery using an image with a KVSS bookmark is faster than recovering from normal RecoverPoint images. The RecoverPoint KVSS utility is a command-line utility that enables applying bookmarks to Windows 2003 and 2008-based applications that support Microsoft Volume Shadow Copy Service (VSS).
Consistency Policy drop-down list	Choose from the following consistency policies applied to this snapshot: • **Never Consolidate**—The snapshot is never consolidated. • **Daily**—The snapshot policy is applied daily. • **Weekly**—The snapshot policy is applied weekly. • **Monthly**—The snapshot policy is applied monthly. • (Default) **Always Consolidate**—The snapshot is consolidated the next time that the consolidation process runs.

Step 10 Click **Submit**.

Updating a Snapshot for a Consistency Group

You can collect the latest snapshot image for a consistency group.

A snapshot is a point in time marked by the system for recovery purposes. A snapshot includes only the data that has changed from the previous snapshot. Once the system distributes the snapshot to the remote storage system, the snapshot creates a new current image on the remote storage system. A snapshot is the difference between one consistent image of stored data and the next consistent image of stored data.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.
Step 3 Choose **EMC RecoverPoint**.
Step 4 Click the row with the EMC RecoverPoint account where you want to update the snapshots for a consistency group.
Step 5 Click **View Details**.
Step 6 Click **Consistency Groups**.
Step 7 Click the row with the consistency group where you want to update the snapshots.
Step 8 From the **More Actions** drop-down list, choose **Update Snapshots**.
Step 9 On the **Update Snapshots** screen, click **Submit**.

Consistency Group Copies

A consistency group copy includes all volumes in a consistency group. The volumes can be one of the following types:

- Production copy—A volume that is the source of the data you want to replicate.
- Local copy—A volume that is the target for the data replication.

Creating a Consistency Group Copy

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.
Step 3 Choose **EMC RecoverPoint**.
Step 4 Click the row with the EMC RecoverPoint account where you want to create the consistency group copy.
Step 5 Click **Consistency Groups Copies**.
Step 6 Click **Create**.
Step 7 On the **Create Consistency Group Copy** screen, complete the following fields:

Name	Description
Consistency Group field	Expand the field, check the box for the consistency group that you want to copy, and click **Validate**.
Copy Name field	A unique name for the consistency group copy.

Name	Description
Cluster field	Expand the field, check the box for the cluster where the consistency group copy will be created, and click **Validate**. The consistency group copy does not need to be on the same cluster as the production copy.
Copy Policy	
Host OS drop-down list	Choose the host operating system.
Journal Policy	
Journal Compression drop-down list	Choose the journal compression level.
Maximum Journal Lag drop-down list	Choose the maximum journal lag.
Required Protection Window check box	Check this check box if you want to enable a protection window.
Protection Window	If you checked the **Required Protection Window** check box, enter the value of time for the protection window.
Window unit drop-down list	If you checked the **Required Protection Window** check box, choose the window time unit.
Enable Snapshot Consolidation check box	Check this check box if you want to enable snapshot consolidation.
Do not consolidate snapshots for at least below period	If you checked the **Enable Snapshot Consolidation** check box, enter the value of time for which snapshot consolidation should not be performed.
Unit (Consolidation Period) drop-down list	If you checked the **Enable Snapshot Consolidation** check box, choose the consolidation period unit.
consolidate to one snapshot per day	If you checked the **Enable Snapshot Consolidation** check box, enter the number of days to consolidate snapshots that are older than the consolidation period.
Indefinitely check box	If you checked the **Enable Snapshot Consolidation** check box, check this check box if you want to consolidate snapshots for an indefinite number of days.
consolidate to one snapshot per week	If you checked the **Enable Snapshot Consolidation** check box, enter the number of weeks to consolidate snapshots that are older than the consolidation period.
Indefinitely check box	If you checked the **Enable Snapshot Consolidation** check box, check this check box if you want to consolidate snapshots for an indefinite number of weeks.

Step 8 Click **Submit.**

Enabling a Consistency Group Copy

Enable each consistency group copy after you add the links between the consistency group copies.

Before you begin

Add the links between the consistency group copies. See Adding a Link Between Consistency Group Copies, on page 220.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.
Step 3 Choose **EMC RecoverPoint**.
Step 4 Click the row with the EMC RecoverPoint account with the consistency group copy that you want to enable.
Step 5 Click **Consistency Groups Copies**.
Step 6 Click the row with the consistency group copy that you want to enable.
Step 7 Click **Enable** or **Disable**.
Step 8 From the **More Actions** drop-down list, choose **Enable**.
Step 9 On the **Enable Consistency Group Copy** screen, click **Submit**.

Enabling Image Access

You can enable image access to verify, backup, clone, or analyze data in a consistency group copy before failover or production recovery.

Note You cannot enable image access on production copies.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.
Step 3 Choose **EMC RecoverPoint**.
Step 4 Click the row with the EMC RecoverPoint account where you want to enable image access.
Step 5 Click **View Details**.
Step 6 Click **Consistency Groups Copies**.
Step 7 From the **More Actions** drop-down list, choose **Enable Image Access**.
Step 8 On the **Enable Image Access** screen, complete the following fields:

Name	Description

Select an Image to Access drop-down list	Choose an image to access:
	• **The latest image**—The last snapshot that was created at the production copy and transferred to the copy journal. This image is at the top of the image list and is the most current snapshot sent from production.
	• **An image from the image list**—Choose one of the images from the list of images in the copy journal.
	• **A specific point in time or bookmark**—This option displays advanced search criteria and lets you specify the image based on one of the following:
	  • **Point in Time**, including date, time, and seconds.
	  • **Bookmark** with the option of **Exact** text, **Image Type**, **Max Range**, and **Max Range Units**.

Select Image Access Mode drop-down list	Choose the image access mode by selecting one of the following options: • **Logged Access**—After disabling image access, any writes made to the copy while image access is enabled are undone. The distribution of images from the copy journal to the copy storage continues from the accessed image forward. The state of the copy storage is restored to **No access**. • **Virtual Access**—After disabling image access, the virtual volume and any writes made to it are undone faster than in logged access mode. The distribution of images from the copy journal to the copy storage continues from the last image that was distributed before image access was enabled. The state of the copy storage is restored to **No access**. • **Virtual Access With Roll**—After disabling image access, the virtual volume, any changes to it, and any writes made directly to the copy are discarded. The distribution of images from the copy journal to the copy storage continues from the image which the system has rolled to. The state of the copy storage is restored to **No access**.

Step 9 Click **Submit**.

Note Choose **Disable Image Access** to disable image access on the selected consistency group copy.

Editing a Consistency Group Copy Policy

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Choose **EMC RecoverPoint**.

Step 4 Click the row with the EMC RecoverPoint account where you want to update a consistency group copy.

Step 5 Click **View Details**.

Step 6 Click **Consistency Groups Copies**.

Step 7 Click the row with the consistency group copy that you want to update and click **View Details**.

Step 8 Click **Copy Policy**.

Step 9 From the **More Actions** drop-down list, choose **Edit Copy Policy**.

Step 10 On the **Edit Consistency Group Copy Policy** dialog box, update the **Copy Policy** and **Journal Policy** fields as needed.

For information about the fields, see Creating a Consistency Group Copy, on page 213.

Step 11 Click **Submit**.

Replication Sets

Consistency groups include one or more replication sets. Each replication set contains a production volume and the local or remote copy volumes (LUNs) where the production volume is replicated.

The number of replication sets in your system must be equal to the number of production volumes being replicated.

Creating a Replication Set

The number of replication sets in your system must be equal to the number of production volumes being replicated.

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Choose **EMC RecoverPoint**.

Step 4 Click the row with the EMC RecoverPoint account where you want to create the replication set.

Step 5 Click **Replication Sets**.

Step 6 Click **Create**.

Step 7 In the **Create Replication Set** dialog box, complete the following fields:

Name	Description
Consistency Group Name field	Expand the field, check the box for the consistency group where you want to create the replication set, and click **Validate**.
Replication Set Name field	A unique name for the replication set.

Step 8 Click **Submit**.

Renaming a Replication Set

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Choose **EMC RecoverPoint**.
Step 4 Click the row with the EMC RecoverPoint account where you want to rename the replication set.
Step 5 Click **Replication Sets**.
Step 6 Click the row with the replication set that you want to rename.
Step 7 Click **Edit**.
Step 8 On the **Edit Replication Set** screen, enter the new name for the replication set.
Step 9 Click **Submit**.

User Volumes and Journal Volumes

The consistency group copy in a replication set contains at least one user volume and one journal volume. These volumes hold the data for replication.

User Volumes

The user volume is the primary volume in a replication set. This volume contains the data you want to protect.

Journal Volumes

Each consistency group copy must include one or more journal volumes that are dedicated to holding system information or point in time history. The type of information contained in a journal volume depends upon the journal type.

You can add one of the following types of journals:

- Copy journal—Copy journals are dedicated to holding point-in-time information for each image on the production storage. They also hold bookmarks for significant points in time. The copy journals hold all changes to data, so that the copy storage can be rolled back to a previous point in time (PIT).
- Production journal—Production journals are dedicated to storing information about the replication process. This marking information makes synchronization between the production and copy volumes more efficient. A production journal does not contain snapshots. Since this volume is used for failover, we recommend that you configure journal protection policies for the production journal.

Adding a User Volume to a Consistency Group Copy

The user volume is the primary volume in a replication set. This volume contains the data you want to protect.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.
Step 3 Choose **EMC RecoverPoint**.
Step 4 Click the row with the EMC RecoverPoint account that contains the consistency group copy and replication set.
Step 5 Click **Replication Sets**.
Step 6 Click the row with the replication set where you want to add the user volume.
Step 7 From the **More Actions** drop-down list, choose **Add User Volume**.
Step 8 On the **Add User Volume to Group Copy** screen, complete the following fields:

Name	Description
Consistency Group Copy field	Expand the field, check the box for the consistency group copy that includes the replication set where you want to add the user volume, and click **Validate**.
User Volume field	Expand the field, check the box for the user volume that you want to add to the replication set, and click **Validate**.

Step 9 Click **Submit.**

Adding a Journal Volume to a Consistency Group Copy

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Choose **EMC RecoverPoint**.

Step 4 Click the row with the EMC RecoverPoint account that contains the consistency group copy where you want to add the volume.

Step 5 Click **Consistency Groups Copies**.

Step 6 Click the row with the consistency group copy where you want to add the volume.

Step 7 From the **More Actions** drop-down list, choose **Add Journal Volume**.

Step 8 On the **Add Journal Volume to Group Copy** screen, do the following:

a) Expand the **Journal Volume** field and choose the journal volume that you want to add to the group copy.

b) Click **Submit**.

Data Transfers

EMC RecoverPoint transfers data across a communication connection between the production copy and the replication copies in the replication set of a consistency group. When the link is open, data can be transferred between consistency group copies.

You can start the transfer of data from a production copy to all other replication copies in a consistency group within a RecoverPoint appliance (RPA) cluster.

When you configure the link for the data transfer, you choose the replication mode that you want to use for the transfer. This mode can be one of the following:

- Asynchronous—Replication in asynchronous mode creates a data copy that is synchronized automatically at specified intervals. The Recoverry Point Objective (RPO) that you configure for the link determines the length of these intervals. The default RPO is 25 seconds. In this mode, the host application initiates the data transfer, but does not wait for an acknowledgment from the remote vRPA before it initiates the next write. This is the default replication mode.
- Synchronous—Replication in synchronous mode creates a data copy that is always in sync with the production source. In this mode, the host application initiates the data transfer, then it waits for acknowledgment from the remote vRPA before starting the next transfer.

Adding a Link Between Consistency Group Copies

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Choose **EMC RecoverPoint**.

Step 4 Click the row with the EMC RecoverPoint account with the consistency group copy where you want to add the link.

Step 5 Click **Consistency Groups Copies**.

Step 6 Click **Add Link**.

Step 7 On the **Add Link Between Consistency Group Copies** screen, complete the following fields:

Name	Description
First Copy field	Expand the field, check the box for the first consistency group copy to be linked.
Second Copy field	Expand the field, check the box for the second consistency group copy to be linked, and click **Validate**.
Replication Mode drop-down list	Choose the replication mode by selecting one of the following options: • **Asynchronous**—Use this mode when you want the data between the production volume and the copy to be synchronized automatically at specified intervals, based on the recovery point objective (RPO). This is the default mode. • **Synchronous**—Use this mode when you want the data between the production volume and the copy to always be in sync.
Protection Settings for Synchronous Mode	
Dynamic by Latency check box	If you check this box, RecoverPoint alternates between synchronous and asynchronous replication modes, as necessary. The latency conditions determine when this occurs. If you enable this option, you must configure the RPO values for asynchronous mode.
Start Async Replication Above in Milliseconds field	When the specified latency limit is reached, RecoverPoint starts replicating asynchronously. The default is 5 milliseconds. This field is only displayed if you enable dynamic replication by latency.
Resume Sync Replication Below in Milliseconds field	When the specified latency limit is reached, RecoverPoint resumes synchronous replication. The default is 3 milliseconds. This field is only displayed if you enable dynamic replication by latency.
Dynamic by Throughput check box	If you check this box, RecoverPoint alternates between synchronous and asynchronous replication modes, as necessary. The throughput conditions determine when this occurs. If you enable this option, you must configure the RPO values for asynchronous mode.

Name	Description
Start async replication above Throughput	When the specified throughput limit is reached, RecoverPoint starts replicating asynchronously. The throughput limit is a combination of this value and the throughput unit. This field is only displayed if you enable dynamic replication by throughput.
Throughput Unit	The unit of measure for the throughput limit. This field is only displayed if you enable dynamic replication by throughput.
Resume sync replication below	When the specified throughput limit is reached, RecoverPoint resumes synchronous replication. The throughput limit is a combination of this value and the throughput unit in the field below. This field is only displayed if you enable dynamic replication by throughput.
Throughput Unit	The unit of measure for the throughput limit. This field is only displayed if you enable dynamic replication by throughput.
Protection Settings for Asynchronous Mode—These fields are also displayed if you choose to enable dynamic replication by latency or throughput in synchronous mode.	
RPO	The recovery point objective defines the maximum time period over which you can tolerate data loss or corruption. The RPO determines the interval between data transfers across the link The default value is 25, which combined with the default value for the RPO Unit of seconds, configures an interval of 25 seconds.
RPO Unit drop-down list	The RPO unit can be one of the following: • **Bytes** • **KB** • **MB** • **GB** • **TB** • **Writes** • **Seconds** • **Minutes** • **Hours**
Protection Settings for Both Modes	

Name	Description
Snapshot Granularity drop-down list	Choose the following snapshot granularity for the link: • **Dynamic** - The system determines the snapshot granularity of a specific (local or remote) link, according to the available resources. • **Fixed (per second)** - Creates one snapshot per second, over a specific (local or remote) link. • **Fixed (per write)** - Creates a snapshot for every write operation, over a specific (local or remote) link.

Step 8 Click **Submit.**

Starting Data Transfer for a Consistency Group

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Choose **EMC RecoverPoint**.

Step 4 Click the row with the EMC RecoverPoint account with the consistency group where you want to start a data transfer.

Step 5 Click **Consistency Groups**.

Step 6 Click the row with the consistency group for which you want to transfer data.

Step 7 From the **More Actions** drop-down list, choose **Start Transfer** and then click **Submit**.

The message on the **Submit Result** screen tells you whether the data transfer was successful.

Note Click **Pause Transfer** to temporarily pause the transfer of data from the production host. If you pause transfers to copies of a lower-priority consistency group when WAN bandwidth is limited, you can make more bandwidth available for a higher-priority transfer.

Starting a Transfer for a Consistency Group Copy

You can transfer data in a consistency group copy only if it is a replication copy and not a production copy. The production copy consists of a single consistency group.

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Choose **EMC RecoverPoint**.

Step 4 Click the row with the EMC RecoverPoint account with the consistency group copy where you want to start a data transfer.

Step 5 Click **Consistency Groups Copies**.

Step 6 Click the row with the consistency group copy for which you want to transfer data.

Step 7 From the **More Actions** drop-down list, choose **Start Transfer** and then click **Submit**.

The message on the **Submit Result** screen tells you whether the data transfer was successful.

Note Click **Pause Transfer** to temporarily pause the transfer of data from the production host. If you pause transfers to copies of a lower-priority consistency group when WAN bandwidth is limited, you can make more bandwidth available for a higher-priority transfer.

Getting the Transfer Status for a Consistency Group

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Choose **EMC RecoverPoint**.

Step 4 Click the row with the EMC RecoverPoint account with the consistency group where you want to get the transfer status.

Step 5 Click **Consistency Groups**.

Step 6 Click the row with the consistency group for which you need the transfer status.

Step 7 From the **More Actions** drop-down list, choose **Get Transfer Status**.

Step 8 On the **Get Transfer Status** screen, click **Submit**.

The message on the **Submit Result** screen tells you whether or not the data transfer was successful.

Group Sets

In RecoverPoint, group sets let you automatically bookmark a set of consistency groups at pre-defined intervals to manage consistency. The bookmark represents the same recovery point in each consistency group in the group set. It allows you to define consistent recovery points for consistency groups that are distributed across different RecoverPoint appliances. Group sets provide automatic management of consistent points in time across consistency groups that are dependent on each other, or that must work together.

For more detailed guidelines about group sets, see the *EMC RecoverPoint Administrator's Guide*, which can be obtained from EMC.

Creating a Group Set

Before you begin

Before you create a group set, note the following:

- All consistency groups in the group set must be replicating in the same direction, from the same source.
- All consistency groups in the group set must be enabled.
- The interval between automatic bookmarks should not be less than 30 seconds.

Step 1 Choose **Physical** > **Storage**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.
Step 3 Choose **EMC RecoverPoint**.
Step 4 Click the row with the EMC RecoverPoint account where you want to create the group set.
Step 5 Click **View Details**.
Step 6 Click **Group Sets**.
Step 7 Click **Create**.
Step 8 On the **Create RecoverPoint Group Set** screen, complete the following fields:

Name	Description
Group Set Name field	A unique name for the group set.
Consistency Group Name	Expand the field, choose one or more consistency groups to add to the group set, and then click **Validate**.
Frequency field	The frequency that the bookmark is added to the consistency groups in the group set.
Unit drop-down list	The unit of time for the bookmark frequency. This unit can be minutes or seconds.

Step 9 Click **Submit**.

Deleting a Group Set

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.
Step 3 Choose **EMC RecoverPoint**.
Step 4 Click the row with the EMC RecoverPoint account where you want to create the group set.
Step 5 Click **View Details**.
Step 6 Click **Group Sets**.
Step 7 Click the row with the group set that you want to delete.
Step 8 Click **Delete**.
Step 9 On the **Delete RecoverPoint Group Set** screen, click **Submit**.

System Tasks

Assigning a Policy to a RecoverPoint System Task

For more information about system tasks, see the Cisco UCS Director Administration Guide.

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.
Step 3 Choose **EMC RecoverPoint**.
Step 4 Click the row with the EMC RecoverPoint account where you want to update the system task.
Step 5 Click **View Details**.
Step 6 Click **System Tasks**.
Step 7 Expand the **EMC RecoverPoint Tasks** folder.
Step 8 Click the EMC RecoverPoint system task (EMCRecoverPointCollector).
Step 9 From the **More Actions** drop-down list, choose **Manage Task**.
Step 10 On the **Manage Task** screen, complete the following fields:

Name	Description
Task Execution drop-down list	Choose **Enable** or **Disable** to enable or disable this RecoverPoint system task.
System Task Policy drop-down list	Choose either the **default-system-task-policy** or the **local-run-policy** to assign to this RecoverPoint system task.
Minutes drop-down list	Choose the frequency in minutes to determine how often this RecoverPoint system task is executed.

Step 11 Click **Submit**.
Step 12 If you want to run this RecoverPoint task, click **Run Now**.
Step 13 If you want to view this RecoverPoint task, click **View Details**.

Viewing RecoverPoint Task History and Reports

Step 1 Choose **Physical** > **Storage**.
Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.
Step 3 Choose **EMC RecoverPoint**.
Step 4 Click the row with the EMC RecoverPoint account where you want to view the system task information.
Step 5 Click **View Details**.
Step 6 Click **System Tasks**.
Step 7 In the System Tasks panel, click the **EMC RecoverPoint Tasks** folder icon to expand the folder.
Step 8 Expand the **EMC RecoverPoint Tasks** folder.
Step 9 Double-click the EMC RecoverPoint system task (EMCRecoverPointCollector).
Step 10 Click one of the following to view reporting information for this system task:

- **System Task History**
- **More Reports**