<table>
<thead>
<tr>
<th>Date</th>
<th>Vblock System</th>
<th>Document revision</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2015</td>
<td>Gen 4.3</td>
<td>4.8</td>
<td>Updated to include support for VMware vSphere 6.0 with Cisco Nexus 1000V Switch. Removed support for VMware vSphere 5.0.</td>
</tr>
<tr>
<td>August 2015</td>
<td>Gen 4.3</td>
<td>4.7</td>
<td>Added support for VMware vSphere 6.0 with VMware VDS.</td>
</tr>
<tr>
<td>February 2015</td>
<td>Gen 4.2</td>
<td>4.6</td>
<td>Added support for Cisco B200 M4 Blade.</td>
</tr>
<tr>
<td>December 2014</td>
<td>Gen 4.2</td>
<td>4.5</td>
<td>Updated to support Vblock System Release 5.0.</td>
</tr>
<tr>
<td>July 2014</td>
<td>Gen 4.2</td>
<td>4.4</td>
<td>Added external hosts, VDS, vSphere</td>
</tr>
<tr>
<td>December 2013</td>
<td>Gen 4.1</td>
<td>4.3</td>
<td>Added TPM, removed Data Protection information, and added link to new Data Protection Guide.</td>
</tr>
<tr>
<td>April 2013</td>
<td>Gen 4.1</td>
<td>4.2</td>
<td>Added VCE Vision™ Intelligent Operations Updated VMware vSphere information Integrated into Gen 3.1 release</td>
</tr>
<tr>
<td>March 2013</td>
<td>Gen 4.0</td>
<td>4.1</td>
<td>Updated for VCE rebranding.</td>
</tr>
<tr>
<td>February 2013</td>
<td>Gen 4.0</td>
<td>4.0</td>
<td>Gen 4.0 release</td>
</tr>
</tbody>
</table>
## Contents

### Introduction

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About this document</td>
<td>10</td>
</tr>
<tr>
<td>Accessing VCE documentation</td>
<td>11</td>
</tr>
<tr>
<td>Related documentation</td>
<td>12</td>
</tr>
<tr>
<td>Intelligent Physical Infrastructure appliance</td>
<td>13</td>
</tr>
<tr>
<td>Managing compute resources</td>
<td>14</td>
</tr>
<tr>
<td>Starting Cisco UCS Manager</td>
<td>14</td>
</tr>
<tr>
<td>Upgrading Cisco UCS software</td>
<td>14</td>
</tr>
<tr>
<td>Activating a Cisco UCS Manager Capability Catalog</td>
<td>15</td>
</tr>
<tr>
<td>Activating a port license</td>
<td>16</td>
</tr>
<tr>
<td>Adding a UUID range</td>
<td>17</td>
</tr>
<tr>
<td>Deleting a UUID pool</td>
<td>18</td>
</tr>
<tr>
<td>Adding a WWNN range</td>
<td>18</td>
</tr>
<tr>
<td>Deleting a WWNN range</td>
<td>20</td>
</tr>
<tr>
<td>Adding a WWPN range using Cisco UCS Manager</td>
<td>20</td>
</tr>
<tr>
<td>Deleting a WWPN range</td>
<td>22</td>
</tr>
<tr>
<td>Adding a MAC address range</td>
<td>22</td>
</tr>
<tr>
<td>Deleting a MAC pool</td>
<td>23</td>
</tr>
<tr>
<td>Adding an IP pool using Cisco UCS Manager</td>
<td>24</td>
</tr>
<tr>
<td>Modifying the time zone setting</td>
<td>25</td>
</tr>
<tr>
<td>Adding a network time protocol server</td>
<td>26</td>
</tr>
<tr>
<td>Removing a network time protocol server</td>
<td>27</td>
</tr>
<tr>
<td>Adding a syslog server</td>
<td>27</td>
</tr>
<tr>
<td>Adding an SNMP server</td>
<td>28</td>
</tr>
<tr>
<td>Removing an SNMP server</td>
<td>29</td>
</tr>
<tr>
<td>Using the Cisco Trusted Platform Module</td>
<td>30</td>
</tr>
<tr>
<td>Managing service profiles</td>
<td>32</td>
</tr>
<tr>
<td>Configuring service profile templates</td>
<td>32</td>
</tr>
<tr>
<td>Configuring service profile templates for disjoint layer 2</td>
<td>44</td>
</tr>
<tr>
<td>Assigning a management IP address to the service profile</td>
<td>53</td>
</tr>
<tr>
<td>Modifying the management IP address on a service profile</td>
<td>53</td>
</tr>
<tr>
<td>Assigning service profiles</td>
<td>54</td>
</tr>
<tr>
<td>Renaming service profiles</td>
<td>55</td>
</tr>
<tr>
<td>Managing networking resources</td>
<td>56</td>
</tr>
</tbody>
</table>
## Managing Cisco MDS switches

- Upgrading Cisco MDS switch software .................................................. 77
  - Reversing the procedure ................................................................. 78
- Configuring a VSAN ............................................................................. 79
  - Reversing the procedure ................................................................. 80
- Configuring a domain ID and priority for VSAN ................................. 80
  - Reversing the procedure ................................................................. 81
- Enabling Fibre Channel interfaces ...................................................... 81
  - Reversing the procedure ................................................................. 82
- Moving licenses between Fibre Channel interfaces ............................ 82
- Creating Fibre Channel aliases ......................................................... 83
  - Reversing the procedure ................................................................. 83
- Creating Fibre Channel zones ............................................................ 84
  - Reversing the procedure ................................................................. 84
- Creating modifying and activating zone sets .................................... 85
- Creating Fibre Channel port channels .............................................. 85
  - Reversing the procedure ................................................................. 87

## Managing storage resources

- Logging into a storage array ............................................................... 88
- Creating devices and pools .............................................................. 88
  - Creating TDATs, TDEVs, and pools .............................................. 89
  - Creating a meta device ................................................................. 90
  - Adding TDATs to a pool ............................................................... 91
  - Binding TDEVs to a pool ............................................................. 92
  - SYMCLI commands for managing devices and pools ..................... 92
- Creating a VSAN ............................................................................ 93
  - Reversing the procedure ............................................................... 93
Mapping the CIFS share ................................................................................................................................. 130
Unmapping a CIFS share ................................................................................................................................. 131
Deleting a CIFS share ........................................................................................................................................ 131

Managing VMware vSphere ESXi 5.1 5.5 and 6.0 .......................................................................................... 133
Installing the latest VMware vSphere ESXi patch .......................................................................................... 133
Configuring advanced settings for VMware vSphere ESXi .......................................................................... 134
Reversing the procedure ................................................................................................................................. 137
Hardening security on VMware vSphere ESXi hosts .................................................................................... 137

Managing VMware vSphere virtual machines ............................................................................................. 138
Increasing the disk timeout on Microsoft Windows virtual machines .......................................................... 138
Setting up Java and Internet Explorer on the management virtual machine .............................................. 138

Managing VMware vCenter Single Sign-On accounts for VMware vSphere 6.0 ..................................... 140
Unlocking and resetting the VMware vCenter Single Sign-On administrator password (vSphere 6.0) .... 140
Managing the lockout status of VMware vCenter Single Sign-On account (vSphere 6.0) ...................... 140
Managing VMware vCenter Single Sign-On default password policies (vSphere 6.0) ....................... 141
Managing VMware vCenter Single Sign-On lockout policies (vSphere 6.0) ............................................ 141
Adding an Active Directory identity source to VMware vCenter Single Sign-On (vSphere 6.0) ........ 142
Back up or restoring the VMware external Platform Services Controller configuration (vSphere 6.0) ....... 144
Redirecting VMware vCenter Server to the secondary external Platform Services Controller (vSphere 6.0) 144
Enabling fault tolerance for external Platform Services Controller (vSphere 6.0) .................................... 145

Managing VMware vCenter Single Sign-On accounts for VMware vSphere 5.5 .................................... 146
Unlocking and resetting the VMware vCenter Single Sign-On administrator password ......................... 146
Managing the lockout status of VMware vCenter Single Sign-On account ............................................... 146
Managing VMware vCenter Single Sign-On default password policies .................................................. 147
Managing VMware vCenter Single Sign-On lockout policies ................................................................ 147
Adding an Active Directory identity source to VMware vCenter Single Sign-On ................................ 148
Back up the VMware vCenter Single Sign-On configuration .................................................................. 149
Restoring a VMware vCenter Single Sign-On single or primary node .................................................... 151
Restoring from a VMware vCenter Server 5.5 database backup ............................................................... 152

Managing VMware vCenter Single Sign-On for VMware vSphere 5.1 ....................................................... 155
Unlocking and resetting the VMware vCenter Single Sign-On administrator password ........................ 155
Managing the lockout status of a VMware vCenter Single Sign-On account ............................................ 155
Managing VMware vCenter Single Sign-On default password policies ............................................... 156
Managing the VMware vCenter Single Sign-On lockout policies .......................................................... 156
Adding an Active Directory identity source to VMware vCenter Single Sign-On .................................. 157
Back up the VMware vCenter Single Sign-On configuration ................................................................. 158
Restoring a VMware vCenter Single Sign-On single or primary node instance ........................................ 159

Managing virtualization .......................................................................................................................... 162
Patching VMware vSphere ESXi hosts with the VMware Update Manager ........................................ 162
Supported guest operating systems .................................................................................................... 164
Using VMware Enhanced vMotion Compatibility with Cisco UCS blade servers .................................. 165
Enabling EVC within a cluster .............................................................................................................. 166
Configuring the Virtual Flash Read Cache .......................................................................................... 166

Managing VMware vSphere Distributed Switch ................................................................................ 168
Managing licenses ............................................................................................................................... 168
Provisioning a VMware VDS configuration ......................................................................................... 168
    Modifying an existing distributed port group .................................................................................... 168
    Creating a distributed port group .................................................................................................... 171
    Configuring a VMkernel distributed port group .............................................................................. 172
    Associating VMware vSphere ESXi hosts to an existing VMware VDS ........................................... 173
    Configuring jumbo frames on VMware VDS .................................................................................... 174
    Configuring jumbo frames on distributed port groups .................................................................... 175
    Modifying class of service settings .................................................................................................. 176
Decommissioning a VMware VDS configuration .................................................................................. 177
    Deleting a distributed port group ..................................................................................................... 177
    Disassociating the VMware vSphere ESXi host ............................................................................... 180
    Removing a VMware VDS ................................................................................................................ 186
Using disjoint layer 2 configuration on VMware VDS ........................................................................ 189
    Creating a VMware VDS for disjoint layer 2 configuration ............................................................ 189
    Creating distributed port groups for disjoint layer 2 configuration ............................................... 190
    Adding VMware vSphere ESXi hosts to VMware VDS .................................................................. 191
Backing up and restoring a VMware VDS data configuration ................................................................ 193
    Exporting a backup of a VMware dvSwitch configuration ............................................................... 193
    Importing a backup of a VMware dvSwitch configuration ............................................................... 194
    Restoring a backup of a VMware dvSwitch configuration ............................................................... 194
Basic troubleshooting .......................................................................................................................... 195

Managing the Cisco Nexus 1000V Series Switch ................................................................................. 196
Managing licenses ............................................................................................................................... 196
Adding hosts .......................................................................................................................................... 196
Creating a port profile .......................................................................................................................... 196
Modifying the uplink port profile ......................................................................................................... 197
    Reversing the procedure .................................................................................................................. 199
Modifying vEthernet data port profiles ............................................................................................... 200
Modifying the QoS settings ................................................................................................................. 203
Upgrading the VEM software ............................................................................................................... 204
Troubleshooting the Cisco Nexus 1000V switch .................................................................................. 205

Deploying and provisioning a service offering .................................................................................... 206
Introduction

This guide contains instructions for managing the Vblock® System after installation at the customer site.

The target audience for this document includes those responsible for managing the Vblock System, including the system administrator and VCE personnel responsible for remote management of the Vblock System. The document assumes that the person administering the Vblock System:

- Is familiar with VMware, EMC storage technologies, and Cisco compute and networking technologies
- Is familiar with Vblock System concepts and terminology
- Has Vblock System troubleshooting skills

The VCE Glossary provides terms, definitions, and acronyms that are related to VCE.

To suggest documentation changes and provide feedback about this book, send an email to docfeedback@vce.com. Include the name of this book, the topic name where your comment applies, and your feedback.
About this document

This document contains instructions for managing the Vblock System 720 after it has been installed. Information is organized by component - compute, networking, storage, the management platform, and virtualization.

The document also includes guidelines for backing up applications, data, and Vblock System 720 configuration files.
Accessing VCE documentation

Select the documentation resource that applies to your role.

<table>
<thead>
<tr>
<th>Role</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer</td>
<td>support.vce.com</td>
</tr>
<tr>
<td></td>
<td>A valid username and password are required. Click VCE Download Center to access the technical documentation.</td>
</tr>
<tr>
<td>Cisco, EMC, VMware employee, or VCE Partner</td>
<td>partner.vce.com</td>
</tr>
<tr>
<td></td>
<td>A valid username and password are required.</td>
</tr>
<tr>
<td>VCE employee</td>
<td>sales.vce.com/saleslibrary</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>vblockproductdocs.ent.vce.com</td>
</tr>
</tbody>
</table>
Related documentation

This section provides information about other documents that support the administration guide.

For more information, refer to the following:

- **VCE Release Certification Matrix** for lists of the certified versions of software, firmware, and hardware for VCE Systems.

- **VCE Systems Powering On and Off Guide** for instructions on how to power VCE Systems on and off.

- **VCE Vision™ Intelligent Operations Administration Guide** to manage your VCE Systems.

- **VCE Integrated Data Protection Guide** contains information on advanced planning and backup guidelines using VCE Integrated Data Protection.
Intelligent Physical Infrastructure appliance

The Intelligent Physical Infrastructure (IPI) appliance provides an intelligent gateway to gather information about power, thermals, security, alerts, and all components in the physical infrastructure for each cabinet.

VCE Vision™ Intelligent Operations uses Simple Network Management Protocol (SNMP) to poll the status of the IPI appliance and then passes the results to VMware vCenter.

For cabinet-related operations such as adding users or cabinet access cards, refer to the VCE Intelligent Physical Infrastructure (IPI) Appliance User Manual.

Refer to the VCE Systems Management Release Certification Matrix (RCM) to identify the recommended firmware version for your IPI appliance. Contact VCE Support with any questions.

Accessing the IPI appliance

To access the IPI appliance in a given cabinet, connect a laptop to the appropriate subnet and use a browser to access the IPI appliance.

The following default settings apply:

- **IP address**: 192.168.0.253
- **Mask**: 255.255.255.0
- **Gateway**: 192.168.0.1

Related information

[Accessing VCE documentation](#) (see page 11)
Managing compute resources

Starting Cisco UCS Manager

Use this procedure to start Cisco UCS Manager.

About this task
The default HTTP or HTTPS web link for Cisco UCS Manager GUI is http(s)://UCSManager_IP.

Procedure

1. Open a web browser.
2. Type the virtual cluster IP of the management port on the fabric interconnect.
3. If a Security Alert dialog box appears, click Yes to accept the security certificate and continue.
4. In the Cisco UCS Manager window, click Launch UCS Manager.
   
   Note: Depending upon the web browser, you may be prompted to download or save the .JNLP file.
5. If a banner window appears, review the message and click OK.
6. If a Security dialog box appears, perform the following:
   
   a. Check the box to accept all content from Cisco.
   b. Click Yes to accept the certificate and continue.
7. In the Login dialog box, perform the following:
   
   a. Type your username and password.
   b. If your Cisco UCS implementation includes multiple domains, select the appropriate domain from the Domain drop-down list.
   c. Click Login.

Upgrading Cisco UCS software

You can upgrade an existing instance of Cisco UCS software using the manual upgrade procedure or the Cisco UCS Firmware Auto Install procedure.
Cisco UCS Manager Capability Catalog

The Cisco UCS Manager Capability Catalog is a set of tunable parameters, strings, and rules. The Cisco UCS Manager uses the catalog to update the display and configure components such as newly qualified dual in-line memory modules (DIMMs) and disk drives for servers.

About this task

The catalog is divided by hardware components such as the chassis, CPU, local disks, and the I/O module. There is one provider per hardware component. Use the catalog to view the list of providers available for that component. Each provider is identified by the vendor, model (PID), and revision. For each provider, you can view details of the equipment manufacturer and the form factor.

Cisco UCS Manager Capability Catalog updates are included in each Cisco UCS Manager update. Unless otherwise instructed by Cisco Technical Support, only activate the Capability Catalog update after you have downloaded, updated, and activated a Cisco UCS Infrastructure Software Bundle.

When you activate a Capability Catalog update, the Cisco UCS Manager immediately updates to the new baseline catalog. You do not need to perform any further tasks or reboot any component in the Cisco UCS instance or reinstall the Cisco UCS Manager when you perform an update.

Each Cisco UCS Manager release contains a baseline catalog. In rare cases, Cisco releases an update to the Capability Catalog and makes it available on the same site where you download firmware images.

The catalog update is compatible with Cisco UCS Manager, Release 1.3(1), and later.

Before you begin

Before activating a capability catalog, download, update, and activate a Cisco UCS infrastructure software bundle.

Procedure

Refer to the Cisco UCS Manager upgrade documentation for your release to update the Cisco UCS Manager Capability Catalog.

Related information

Cisco UCS Manager upgrade documentation
Activating a port license

Port licenses for each Cisco UCS fabric interconnect are factory installed and shipped with the hardware. Activate a port license using the Cisco UCS Manager (UCSM).

About this task

The Cisco UCS 6296UP Fabric Interconnect has pre-installed licenses for the first eighteen unified ports enabled in Cisco UCSM.

Expansion modules come with eight licenses that can be used on the expansion module or the base module.

Note:  The eight default licenses that come with the Cisco UCS 6248UP Fabric Interconnect expansion module can be used to enable ports on the base module, but will travel with the expansion module if it is removed. Upon removal of an expansion module, any default expansion module licenses used by the base module are removed from the ports on the base module, resulting in unlicensed ports.

Port licenses are not bound to physical ports. When a licensed port is disabled, the license is retained for use with the next enabled port. To use additional fixed ports, purchase and install licenses for those ports. If you use an unlicensed port, the Cisco UCSM initiates a 120-day grace period measured from the first use of the unlicensed port and is paused when a valid license file is installed. The amount of time used in the grace period is retained by the system.

Note:  Each physical port has its own grace period. Initiating the grace period on a single port does not initiate the grace period for all ports.

If a licensed port is not configured, that license is transferred to a port functioning within a grace period. If multiple ports are acting within grace periods, the license is moved to the port whose grace period is closest to expiring.

To avoid inconsistencies during failover, VCE recommends that both fabric interconnects in the cluster have the same number of licensed ports. If symmetry is not maintained and failover occurs, Cisco UCS enables the missing licenses and initiates the grace period for each port used on the failover node.

The Vblock System ships with the appropriate number of fabric interconnect licenses installed. If additional licenses are needed, request a chassis activation kit (CAK).

Procedure

To view, obtain, download, install, and uninstall a fabric interconnect license, refer to the Cisco UCS Manager Configuration Guide for your release.

Related information

Cisco UCS Manager GUI Configuration Guide
Adding a UUID range

Use this procedure to add a range to a universally unique identifier (UUID) pool using the Cisco UCS Manager.

Before you begin

Obtain UUID information.

Procedure

1. Log in to the Cisco UCS Manager.
2. In the Navigation window, select the Servers tab.
4. Expand the node for the organization where you want to create the pool. If the system does not include multi-tenancy, expand the root node.
5. Right-click UUID Suffix Pools and select Create UUID Suffix Pool.
6. In the Define Name and Description window of the Create UUID Suffix Pool wizard, perform the following:
   a. In the Name field, type the name of the UUID pool.
   b. In the Description field, type a description of the pool.
   c. In the Prefix field, either select Derived (the system creates the suffix) or Other (allows you to specify the suffix).
7. In the Add UUID Blocks window of the Create UUID Suffix Pool wizard, click Add.
8. From the Create a Block of UUID Suffixes window:
   a. Type the first UUID suffix in the pool and the number of UUID suffixes to include in the pool.
   b. Click OK.
9. Click Finish.

What to do next

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

Related information

Accessing VCE documentation (see page 11)
Deleting a UUID pool

Use this procedure to delete a universally unique identifier (UUID) pool using the Cisco UCS Manager.

About this task

If you delete a pool, the addresses are not reallocated from the pool that have been assigned to vNICs or vHBAs. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until:

- Associated service profiles are deleted
- vNIC or vHBA to which the address is assigned is deleted or assigned to a different pool

Procedure

1. Log in to the Cisco UCS Manager.
2. In the Navigation window, select the Servers tab.
3. On the Servers tab, expand Servers > Pools > Organization_Name.
4. Expand the UUID Suffix Pools node.
5. Right-click the pool and select Delete.
6. If a confirmation dialog box appears, click Yes.

Related information

Adding a UUID range (see page 17)

Adding a WWNN range

Use this procedure to add a range to the world wide node names (WWNN) pool using the Cisco UCS Manager. A WWNN pool is a world wide name (WWN) pool that contains only WW node names.
About this task

A WWN pool only includes WWNNs or world wide port name (WWPNs) in the following ranges:

- 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF
- 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF.

All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, VCE recommends using WWN prefix 20:00:00:25:B5:XX:XX:XX for all blocks in a pool.

Before you begin

Obtain the WWNN information.

Procedure

1. Log in to the Cisco UCS Manager.
2. In the **Navigation** window, select the **SAN** tab.
3. In the **SAN** tab, expand **SAN > Pools**.
4. Expand the node for the organization where you want to create the pool. If the system does not include multi-tenancy, expand the root node.
5. Right-click **WWNN Pools** and select **Create WWNN Pool**.
6. From the **WWNN Pool** window, perform the following:
   a. In the **Define Name and Description** window, type a unique name and description for the WWNN pool.
   b. Click **Next**.
7. In the **Add WWN Blocks** window, click **Add**.
8. In the **Create WWN Block** window, perform the following:
   a. In the **From** field, type the first WWNN in the pool.
   b. In the **Size** field, type the number of WWNNs to include in the pool.
   c. Click **OK**.
9. Click **Finish**.

What to do next

Include the WWNN pool in a vHBA template.
Related information

Accessing VCE documentation (see page 11)
Deleting a WWNN range (see page 20)
Cisco UCS Manager GUI Configuration Guide

Deleting a WWNN range

Use this procedure to delete a range from the world wide node names (WWNN) pool using the Cisco UCS Manager.

About this task

If you delete a pool, the addresses are not reallocated from the pool that have been assigned to vNICs or vHBAs. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until:

- Associated service profiles are deleted
- vNIC or vHBA to which the address is assigned is deleted or assigned to a different pool

Procedure

1. Log in to the Cisco UCS Manager.
2. In the Navigation window, select the SAN tab.
3. In the SAN tab, expand SAN > Pools > Organization_Name.
4. Expand the WWNN Pools node.
5. Right-click the WWNN pool you want to delete and select Delete.
6. If a confirmation dialog box appears, click Yes.

Related information

Adding a WWNN range (see page 18)
Cisco UCS Manager GUI Configuration Guide

Adding a WWPN range

Use this procedure to add a range to the world wide port names (WWPN) pool using the Cisco UCS Manager.
About this task
A world wide name (WWN) pool only includes world wide node names (WWNNs) or WWPNs in the following ranges:

- 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF
- 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF

All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, VCE recommends using the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX

VCE also recommends creating separate WWPN pools for SAN Fabric A and SAN Fabric B.

Before you begin
Obtain the WWPN information.

Procedure

1. Log in to the Cisco UCS Manager.
2. In the Navigation window, select the SAN tab.
3. Expand SAN > Pools.
4. Expand the node for the organization where you want to create the pool. If the system does not include multi-tenancy, expand the root node.
5. Right-click WWPN Pools and select Create WWNN Pool.
6. From the WWNN Pool window, perform the following:
   a. In the Define Name and Description window, type a unique name and description for the WWNN pool.
   b. Click Next.
7. In the Add WWN Blocks window, click Add.
8. In the Create WWN Block window, perform the following:
   a. In the From field, type the first WWPN in the pool.
   b. In the Size field, type the number of WWPNs to include in the pool.
   c. Click OK.
9. Click Finish.
What to do next

Include the WWPN pool in a vHBA template.

Related information

Accessing VCE documentation (see page 11)
Cisco UCS Manager GUI Configuration Guide

Deleting a WWPN range

Use this procedure to delete a world wide port name (WWPN) range from the WWPN pool using the Cisco UCS Manager.

About this task

If you delete a pool, the addresses are not reallocated from the pool that have been assigned to vNICs or vHBAs. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until:

- Associated service profiles are deleted
- vNIC or vHBA to which the address is assigned is deleted or assigned to a different pool

Procedure

1. Log in to the Cisco UCS Manager.
2. In the Navigation window, select the SAN tab.
3. In the SAN tab, expand SAN > Pools > Organization_Name > WWPN Pools > WWPN_Pool_Name.
4. Expand the WWPN Pools node.
5. Right-click the WWPN pool you want to delete and select Delete.
6. If a confirmation dialog box appears, click Yes.

Adding a MAC address range

Use this procedure to add a range to the media access control (MAC) address pool using the Cisco UCS Manager.
Procedure

1. Log in to the Cisco UCS Manager.
2. In the Navigation window, select the LAN tab.
3. Expand LAN > Pools.
4. Expand the node for the organization where you want to create the pool. If the system does not include multi-tenancy, expand the root node.
5. Right-click MAC Pools and select Create MAC Pool.
6. In the first window of the Create MAC Pool wizard, perform the following:
   a. In the Define Name and Description window, type a unique name and description for the MAC pool.
   b. Click Next.
7. In the Add MAC Addresses window, click Add.
8. In the Create a Block of MAC Addresses window, type the first MAC address in the pool and the number of MAC addresses to include in the pool.
9. Click Finish.

What to do next

Include the MAC pool in a vNIC template.

Related information

Accessing VCE documentation (see page 11)
Deleting a MAC pool (see page 23)
Cisco UCS Manager GUI Configuration Guide

Deleting a MAC pool

Use this procedure to delete a media access control (MAC) pool using the Cisco UCS Manager.
Before you begin

If you delete a pool, the addresses are not reallocated from the pool that have been assigned to vNICs or vHBAs. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until:

- Associated service profiles are deleted
- vNIC or vHBA to which the address is assigned is deleted or assigned to a different pool

Procedure

1. Log in to the Cisco UCS Manager.
2. In the Navigation window, select the LAN tab.
3. Expand LAN > Pools > Organization_Name.
4. Expand the MAC Pools node.
5. Right-click the MAC pool you want to delete and select Delete.
6. If a confirmation dialog box appears, click Yes.

Related information

 Adding a MAC address range  (see page 22)

Adding an IP pool using Cisco UCS Manager

Use this procedure to create an IP address block in the management IP pool with Cisco UCS Manager.

About this task

The management IP pool is a collection of external IP addresses. Cisco UCS Manager reserves each block of IP addresses in the management IP pool for external access that terminates in the CIMC on a server. You can configure service profiles and service profile templates to use IP addresses from the management IP pool. You cannot configure servers to use the management IP pool. All IP addresses in the management IP pool must be in the same subnet as the IP address of the fabric interconnect.

Note: The management IP pool must not contain any static IP addresses assigned for a server or service profile.

Procedure

1. In the Navigation window, select the LAN tab.
2. Expand Pools > IP Pools.
3 Right-click IP Pool (ext-mgmt) and select Create Block of IP Addresses.

4 In the Create a Block of IP Addresses window, perform the following:
   a In the From field, type the first IP address in the block.
   b In the Size field, type the number of IP addresses in the pool.
   c In the Subnet Mask field, type the subnet mask associated with the IP addresses in the block. All IP addresses in the management IP pool must be in the same subnet as the IP address of the fabric interconnect.
   d In the Default Gateway field, type the default gateway associated with the IP addresses in the block.
   e In the Primary DNS field, type the IP address of the primary DNS server.
   f In the Secondary DNS field, type the IP address of the secondary DNS server.

5 Click OK.

What to do next

Configure one or more service profiles or service profile templates to obtain the CIMC IP address from the management IP pool.

Related information

Cisco UCS Manager GUI Configuration Guide

Modifying the time zone setting

Use this procedure to modify the time zone setting in a Cisco UCS instance.

About this task

Cisco UCS requires both an instance-specific time zone setting and a network time protocol (NTP) server to ensure the correct time appears in Cisco UCS Manager. Accurate time settings are beneficial in situations where logs are being viewed for troubleshooting.

VCE recommends that all devices in a Vblock System are set to the same time.

Before you begin

Refer to the Logical Configuration Survey for the correct time zone setting.
Procedure

1. Log in to the Cisco UCS Manager.
2. On the Navigation window, select the Admin tab.
3. Expand All.
4. Click Timezone Management.
5. On the Work window, select the General tab.
6. From the Timezone drop-down list, select the time zone you want to use for the Cisco UCS instance.
7. Click Save Changes.

Adding a network time protocol server

Use this procedure to add network time protocol (NTP) server using the Cisco UCS Manager.

About this task

Cisco UCS requires both an instance-specific time zone setting and an NTP server to ensure the correct time appears in the Cisco UCS Manager. When you add an NTP server, devices receive time from the same source.

VCE recommends that all devices in a Vblock System are set to the same time.

Before you begin

Set up the NTP server to be reachable using an IP address from the Cisco UCSM.

Procedure

1. Log in to the Cisco UCS Manager.
2. On the Navigation, select the Admin tab.
3. On the Admin tab, expand All.
4. Click Timezone Management.
5. On the Work window, select the General tab.
6. In the NTP Servers area, click the + on the table icon bar.
7. In the Add NTP Server dialog box, type the IP address or hostname of the NTP server you want to use for this Cisco UCS instance in the NTP Server field, and click OK.
Results
The accurate time appears in the lower right corner of the Cisco UCS Manager.

What to do next
After you add an NTP server, verify the time is accurate. View the time settings in the lower right corner of the Cisco UCS Manager.

Related information

Removing a network time protocol server (see page 27)

Removing a network time protocol server
Use this procedure to remove a network time protocol (NTP) server using the Cisco UCS Manager.

Procedure

1. Log in to the Cisco UCS Manager.
2. In the Navigation window, select the Admin tab.
3. From the Admin tab, expand All.
4. Select Timezone Management.
5. In the Work window, select the General tab.
6. In the NTP Servers area, right-click the server you want to delete and click Delete.
7. If a confirmation dialog box appears, click Yes.
8. Click Save Changes.

Related information

Adding a network time protocol server (see page 26)

Adding a syslog server
Use this procedure to add a syslog server to the Cisco UCS domain using the Cisco UCS Manager.
About this task

When you add a syslog server, logs are sent to the server to facilitate reporting alerts and troubleshooting. VCE recommends using the syslog server to facilitate the reporting of alerts and troubleshooting.

Before you begin

Deploy a syslog server so that it is reachable from the Cisco UCS management IP address using an IP address.

Procedure

1. Log in to the Cisco UCS Manager.
2. From the Admin tab, select Faults, Events and Audit Log > Syslog.
3. Under File, for Admin State, click Enabled.
4. In the Level menu, click Debugging.
5. Under File, in the Level menu, click Critical.
6. In the Server 1 section, for Admin State, click Enabled.
7. In the Level menu, click Critical.
8. In the Hostname field, type the primary syslog server IP address or hostname.
9. In the Facility field, select the appropriate facility.
10. Verify that the logs have been received on the syslog server.

Adding a syslog server

Use this procedure to add a syslog server using the Cisco Integrated Management Controller (CIMC).

Before you begin

Deploy a syslog server so that it is accessible.

Procedure

1. Log in to the CIMC.
2. From the Admin tab, select CIMC Log.
3. From the CIMC Log window, select the Logging Controls tab.
4. In the **Remote Syslog Server 1** section, click **Enabled**.

5. In the **IP Address** field, type the IP address of the syslog server on which the CIMC log should be stored.

6. Verify that the logs have been received on the syslog server.

### Adding an SNMP server

Use this procedure to add an SNMP server to the Cisco UCS domain using the Cisco UCS Manager.

#### About this task

Configuring an SNMP server allows the monitoring of Cisco UCS Manager and the ability to receive SNMP traps.

VCE recommends the use of an SNMP server to aid in report alerting, monitoring and troubleshooting. SNMP v3 is recommended as the most secure option in using the SNMP protocol.

#### Before you begin

Before performing this task, verify that an SNMP server is reachable using a hostname or IP address from the Cisco UCS Manager IP address.

#### Procedure

1. Log in to the Cisco UCS Manager.

2. From the **Navigation** window, select the **Admin** tab.

3. From the **Admin** tab, expand **All > Communication Management > Communication Services**.

4. Select the **Communication Services** tab.

5. In the **Admin State** field, click **Enabled**.

6. In the **Port** field, type the port on which the Cisco UCS Manager communicates with the SNMP host.

   **Note:** You cannot change the default port.

7. In the **Community/Username** field, type an alphanumeric string between 1 and 32 characters. Do not use @, \, " , ? or an empty space. The default is public.

8. In the **System Contact** field, type a contact.

   **Note:** A system contact entry can be up to 255 characters and can be an email address, name or number.

9. In the **System Location** field, type the location of the host on which the SNMP server runs.
10 Click **Save Changes**.

**What to do next**

Verify that the SNMP server is able to poll the Cisco UCS Manager and receive traps.

**Related information**

[Cisco UCS Manager GUI Configuration Guide](#)

**Adding an SNMP server**

Use this procedure to add an SNMP server using Cisco Integrated Management Controller (CIMC).

**Before you begin**

Log in with administrator privileges.

**Procedure**

1. Log in to CIMC.
2. From the **Navigation** window, select the **Admin** tab.
3. On the **Admin** tab, click **Communications Services**.
4. In the **Communications Services** window, select the **SNMP** tab.
5. In **SNMP Properties**, edit the following properties:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enabled checkbox</strong></td>
<td>Check if this server sends SNMP traps to the designated host.</td>
</tr>
<tr>
<td><strong>SNMP Port field</strong></td>
<td>The port that the server uses to communicate with the SNMP host. This value cannot be changed.</td>
</tr>
<tr>
<td><strong>Access Community String field</strong></td>
<td>The default SNMP v1 or v2c community name or SNMP v3 username that CIMC includes on any trap messages it sends to the SNMP host. The name can include up to 18 characters.</td>
</tr>
<tr>
<td><strong>System Contact field</strong></td>
<td>Name of the person responsible for the SNMP implementation. This name or information can include up to 254 characters, such as an email address or a name and telephone number.</td>
</tr>
<tr>
<td><strong>System Location field</strong></td>
<td>Location of the host where the SNMP agent (server) runs. The location can include up to 254 characters.</td>
</tr>
</tbody>
</table>
6 In **SNMP Users**, edit the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Change as follows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add button</td>
<td>Click an available row in the table then click <strong>Add</strong> to add a new SNMP user.</td>
</tr>
<tr>
<td>ID column</td>
<td>The system-assigned identifier for the SNMP user.</td>
</tr>
<tr>
<td>Name column</td>
<td>SNMP username.</td>
</tr>
<tr>
<td>Auth Type column</td>
<td>User authentication type.</td>
</tr>
<tr>
<td>Privacy Type column</td>
<td>User privacy type.</td>
</tr>
</tbody>
</table>

7 In the **Common Trap Destination Settings** area, complete the following fields:

<table>
<thead>
<tr>
<th>Property</th>
<th>Change as follows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap Community String field</td>
<td>Name of the SNMP community group to which trap information should be sent.</td>
</tr>
<tr>
<td>SNMP Version drop-down list</td>
<td>SNMP version used for the trap.</td>
</tr>
<tr>
<td>Type field</td>
<td>If you select V2c for the version, select the type of trap to send.</td>
</tr>
</tbody>
</table>

8 In the **Trap Destinations** area, complete the following fields:

<table>
<thead>
<tr>
<th>Property</th>
<th>Change as follows</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID column</td>
<td>Type the trap destination ID. This value cannot be modified.</td>
</tr>
<tr>
<td>Enabled column</td>
<td>For each desired SNMP trap destination, check the associated checkbox in this column.</td>
</tr>
<tr>
<td>Trap Destination IP Address</td>
<td>IP address where SNMP trap information is sent.</td>
</tr>
</tbody>
</table>

9 Click **Save Changes**.

**Removing an SNMP server**

Use this procedure to remove an SNMP server from the Cisco UCS domain using the Cisco UCS Manager.

**Procedure**

1 Log in to the Cisco UCS Manager.

2 From the **Navigation** window, select the **Admin** tab.

3 From the **Admin** tab, expand **All > Communication Management > Communication Services**.

4 Select the **Communication Services** tab.

5 In the **Admin State** field, click **Disabled**.
6 Click **Save Changes**.

**Cisco Trusted Platform Module**

Cisco TPM provides authentication and attestation services that provide safer computing in all environments. Cisco TPM is a computer chip that securely stores artifacts such as passwords, certificates, or encryption keys that authenticate the Vblock System. Cisco TPM provides authentication and attestation services that provide safer computing in all environments.

Cisco TPM is available by default within the Vblock System as a component within the Cisco UCS B-Series M3 Blade Servers and Cisco UCS B-Series M4 Blade Servers, and is shipped disabled. The *Vblock System Blade Pack Reference* contains additional information about Cisco TPM.

VCE supports only the Cisco TPM hardware. VCE does not support the Cisco TPM functionality. Because making effective use of the Cisco TPM involves the use of a software stack from a vendor with significant experience in trusted computing, VCE defers to the software stack vendor for configuration and operational considerations relating to the Cisco TPMs.

Related information

[www.cisco.com](http://www.cisco.com)

**Managing service profiles**

**Configuring service profile templates**

This profile allows you to override the identity values on the server at the time of association and use resource pools and policies set up in the Cisco UCS Manager to automate administration tasks.

**About this task**

Use this procedure to create four service profile templates for production blades that will run VMware. You can disassociate the service profile from one server and then associate it with another manually or through an automated server pool policy. The burned-in settings, such as the universally unique identifier (UUID) and media access control (MAC) address on the new server are overwritten with the configuration in the service profile. The change in server is transparent to your network so there is no need to reconfigure any component or application on your network to use the new server.
This profile allows you to manage and use the following system resources through resource pools and policies:

- Virtualized identity information, including pools of MAC addresses, world wide name (WWN) addresses, and UUIDs
- Ethernet and Fibre Channel (FC) adapter profile policies
- Firmware package policies
- Operating system boot order policies

Before you begin

Assign a minimum of four vNICs to each compute blade for VMware vSphere Distributed Switch (VDS) deployments.

Procedure

1. Launch the Cisco UCS Manager.
2. From the **Navigation** window, select the **Servers** tab and navigate to **Service Profile Templates**.
3. Right-click **Service Profile Templates** and select **Create Service Profile Template**.
4. From the **Identify Service Template** window, perform the following:
   a. In the **Name** field, type a name in the following format: `<Service Profile Template Identifier>_<Blade Type>_<VCE System or Vblock_System ID>`
      - Service Profile Template Identifier = 1
      - Blade Type = **B200** if installing B200 blades or **B250** if installing B250 blades
      - Vblock System
      - ID = **01** for first system or **02** for second system

For example, if full-width blades (B250 or B440) with dual mezzanine cards are installed:
   - 1_B250-DualVIC-01 and 2_B250-DualVIC-01
   - 2_B250-DualVIC-01 or 2_B440-DualVIC-01
b In the Type field, click **Updating Template**.

**Important:** Updating Templates requires a *UserAck Maintenance Policy*. Create the policy if it doesn’t exist and apply it to the **Service Profile Updating Template**. Failure to apply a *UserAck Maintenance Policy* may result in unexpected service profile reboots when modifying the **Updating Service Profile Template**. If the *UserAck Maintenance Policy* is not created or used, create a **Service Profile Initial Template**.

c In the **UUID Assignment** field, select the previously created pool, and click **Next**.

5 On the Networking page, in the How would you like to configure LAN Connectivity? field, select **Expert**, and click **Add**.

6 On the **Create vNIC** window, perform the following:

   a In the **Name** field, type **vNIC-0**.
   
   b Click **Use vNIC Template**.
   
   c In the **vNIC Template** field, click **vNIC-0-Fabric-A**.
   
   d In the **Adapter Policy** field, click **VMware** and click **OK**.

7 Click **Add** to create **vNIC-1**.

8 On the **Create vNIC** window, perform the following:

   a In the **Name** field, type **vNIC-1**.
   
   b Select **Use vNIC Template**.
   
   c In the **vNIC Template** field, click **vNIC-1-Fabric-B**.
   
   d In the **Adapter Policy** field, click **VMware** and click **OK**.
9 Complete this step **ONLY** if installing or deploying:

- Cisco B460 quad blades or Cisco B250, B260, B440, or B420 full-width blades with dual mezzanine cards
- Cisco B200 M3, B22 M3, or B200 M4 with dual mezzanine cards
- VMware VDS 5.5 or later

**Important:** For the Cisco B460 M4 blade with a mezzanine adapter combination of two 1240-VICs and two 1280-VICs, do not add vNIC2/3 to the service profile template. vNIC2/3 must be added manually to the service profile.

- Install VMware vSphere ESXi with vNIC 0/1 and reboot.
- Add vNIC-2-Fabric-A to the service profile and reboot.
- Add vNIC-3-Fabric-B to the service profile and reboot.
- After each reboot, verify the new vNIC number and associated MAC address is correctly enumerated in both Cisco UCS Manager and VMware vSphere ESXi.

**Important:** For a Cisco B200 M4 blade with dual mezzanine cards, do not add vNIC2/3 to the service profile template. vNIC2/3 must be added manually to the service profile.

- Install VMware vSphere ESXi with vNIC0/1 and reboot.
- Add vNIC-2-Fabric-A to the service profile and reboot.
- Add vNIC-3-Fabric-B to the service profile and reboot.
- After each reboot, verify the new vNIC number and associated MAC address is correctly enumerated in both Cisco UCSM and VMware vSphere ESXi.

- From the **Networking** window, select **Add** to create vNIC-2.
- On the **Create vNIC** window, in the **Name** field, type **vNIC-2**.
- Select **Use vNIC Template**.
- In the **vNIC Template** field, click **vNIC-2-Fabric-A**.
- In the **Adapter Policy** field, click **VMware** and click **OK**.
- On the **Networking** window, click **Add** to create vNIC-3.
- On the **Create vNIC** window, in the **Name** field, type **vNIC-3**
- Select **Use vNIC Template**.
- In the **vNIC Template** field, click **vNIC-3-Fabric-B**.
j In the Adapter Policy field, click VMware and click OK.

10 On the Storage window, perform the following:
   a In the Local Storage field, click the UIM_nodisk policy that was previously created.
   b In the SAN Connectivity field, click Expert.
   c In the WWNN Assignment field, click Global-WWNN-Pool and click Add.

11 On the Create vHBA window, perform the following:
   a In the Name field, type vHBA-0.
   b Select Use vHBA Template.
   c In the vHBA Template field, click vHBA-0-Fabric-A.
   d In the Adapter Policy field, click VMware, then click OK and Add.

12 On the Create vHBA window, perform the following:
   a In the Name field, type vHBA-1.
   b Select Use vHBA Template.
   c In the vHBA Template field, click vHBA-1-Fabric-B.
   d In the Adapter Policy field, click VMware.
   e Click OK and Next.

13 From the Storage page, for the B460 M4 blade with the following mezzanine adapter combination (two 1240-VICs and two 1280-VICs), click Add.

14 From the Create vHBA window, perform the following:
   a In the Name field, type vHBA-2.
   b Select Use vHBA Template.
   c In the vHBA Template field, click vHBA-2-Fabric-A.
   d In the Adapter Policy field, click VMware.
   e Click OK and Next.

15 From the Create vHBA window, perform the following:
   a In the Name field, type vHBA-3.
   b Select Use vHBA Template.
c In the vHBA Template field, click vHBA-3-Fabric-A.

d In the Adapter Policy field, click VMware.

e Click OK and Next.

16 On the Zoning window, click Next.
For the vNIC/vHBA Placement window, refer to the vNIC/vCON placement table.

For the Cisco Nexus 1000V Switch, the following configuration notes apply:

- If a Vblock System is configured to use the Cisco Nexus 1000V Switch, and the server only has one mezzanine adapter, the assignment of the two vNICs and two vHBAs to vCONs is system managed.

- If a Vblock System is configured to use the Cisco Nexus 1000V Switch and the server has more than one mezzanine adapter, the assignment of the four vNICs and two vHBAs to vCONs is statically mapped.

- In a Cisco B460 with four mezzanine adapters, four vHBAs can be configured.

- For the Cisco B200 M4 blade, regardless of the number of mezzanine adapters, vNICs are statically mapped to a vCON.

For VMware VDS, the following configuration notes apply:

- If a Vblock System is configured to use the VMware VDS and the server only has one mezzanine adapter, the assignment of the four vNICs and two vHBAs to vCONs is system managed.

- Configurations with a VMware VDS always have a minimum of four vNICs.

- If a server with more than one mezzanine adapter is configured to use VMware VDS, the assignment of the four vNICs and two vHBAs to vCONs is statically mapped.

- In a Cisco B460 with four mezzanine adapters, four vHBAs can be configured.

- For the Cisco B200 M4 blade, regardless of the number of mezzanine adapters, vNICs are statically mapped to a vCON.

Add the four vNICs and two vHBAs to the vCON in the order indicated shown in the following table:

<table>
<thead>
<tr>
<th>Blade type</th>
<th>Mezzanine adapter</th>
<th>One mezzanine adapter vNICs/vCONs</th>
<th>Two mezzanine adapter vNICs/vCONs</th>
<th>Four mezzanine adapter vNICs/vCONs (statically mapped)</th>
<th>Mezzanine adapter supported combinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco B22 M3</td>
<td>1240</td>
<td>System managed</td>
<td>Statically mapped</td>
<td>vNIC0 &gt; vCON1 vNIC1 &gt; vCON1 vHBA0 &gt; vCON1 vNIC2 &gt; vCON2 vNIC3 &gt; vCON2</td>
<td>1240 only 1240 and 1280</td>
</tr>
<tr>
<td>Blade type</td>
<td>Mezzanine adapter</td>
<td>One mezzanine adapter vNICs/ vCONs</td>
<td>Two mezzanine adapter vNICs/ vCONs</td>
<td>Four mezzanine adapter vNICs/ vCONs (statically mapped)</td>
<td>Mezzanine adapter supported combinations</td>
</tr>
<tr>
<td>------------</td>
<td>------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------</td>
<td>----------------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vHBA1 &gt; vCON2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1280</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Cisco B200 M3</td>
<td>1240</td>
<td>System managed</td>
<td>Statically mapped</td>
<td>N/A</td>
<td>1240 and 1280</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td>vNIC0 &gt; vCON1</td>
<td>vNIC1 &gt; vCON1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vHBA0 &gt; vCON1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vNIC2 &gt; vCON2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vNIC3 &gt; vCON2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1280</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Cisco B200 M4</td>
<td>1340</td>
<td>Statically mapped</td>
<td>Statically mapped</td>
<td>N/A</td>
<td>1340 only 1340 and 1380</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
<td>vNIC0 &gt; vCON1</td>
<td>vNIC1 &gt; vCON1</td>
<td>vHBA0 &gt; vCON1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>vNIC2 &gt; vCON1</td>
<td>vNIC3 &gt; vCON2</td>
<td>vHBA1 &gt; vCON2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>vHBA0 &gt; vCON1</td>
<td>vNIC2 &gt; vCON2</td>
<td>vHBA1 &gt; vCON2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1380</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Cisco B230 M2</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>1280 only</td>
</tr>
<tr>
<td>Cisco B250 M2 (EoS)</td>
<td>Pal</td>
<td>System managed</td>
<td>N/A</td>
<td>N/A</td>
<td>Palo only</td>
</tr>
<tr>
<td>Cisco B260 M4</td>
<td>1240</td>
<td>System managed</td>
<td>Statically mapped</td>
<td>N/A</td>
<td>1240 and 1280</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vNIC0 &gt; vCON1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vNIC1 &gt; vCON1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vHBA0 &gt; vCON1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vNIC2 &gt; vCON2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vNIC3 &gt; vCON2</td>
<td></td>
</tr>
<tr>
<td>Blade type</td>
<td>Mezzanine adapter</td>
<td>One mezzanine adapter vNICs/vCONs</td>
<td>Two mezzanine adapter vNICs/vCONs</td>
<td>Four mezzanine adapter vNICs/vCONs (statically mapped)</td>
<td>Mezzanine adapter supported combinations</td>
</tr>
<tr>
<td>------------</td>
<td>------------------</td>
<td>----------------------------------</td>
<td>----------------------------------</td>
<td>--------------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>1280</td>
<td>System managed</td>
<td>Statically mapped</td>
<td>N/A</td>
<td>1280 only 1240 and 1280</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC0 &gt; vCON1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC1 &gt; vCON1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vHBA0 &gt; vCON1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC2 &gt; vCON2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC3 &gt; vCON2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vHBA1 &gt; vCON2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco B420 M3</td>
<td>1240</td>
<td>System managed</td>
<td>Statically mapped</td>
<td>N/A</td>
<td>1240 1240 and 1280</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC0 &gt; vCON1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC1 &gt; vCON1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vHBA0 &gt; vCON1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC2 &gt; vCON3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC3 &gt; vCON3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vHBA1 &gt; vCON3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1280</td>
<td>System managed</td>
<td>vNIC0 &gt; vCON1</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC1 &gt; vCON1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vHBA0 &gt; vCON1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC2 &gt; vCON3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC3 &gt; vCON3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vHBA1 &gt; vCON3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco B440 M2</td>
<td>2 x 1280</td>
<td>N/A</td>
<td>Statically mapped</td>
<td>N/A</td>
<td>2 x 1280 only</td>
</tr>
<tr>
<td>with VMware vSphere 5.5</td>
<td></td>
<td></td>
<td>vNIC0 &gt; vCON1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC1 &gt; vCON1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vHBA0 &gt; vCON1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC2 &gt; vCON2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC3 &gt; vCON2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vHBA1 &gt; vCON2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco B460 M4</td>
<td>2 x 1240</td>
<td>N/A</td>
<td>Statically mapped</td>
<td>Statically mapped</td>
<td>2 x 1240 ((2 x 1240) + (2 x 1280))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC0 &gt; vCON1</td>
<td>vNIC0 &gt; vCON1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC1 &gt; vCON1</td>
<td>vNIC1 &gt; vCON3</td>
<td></td>
</tr>
<tr>
<td>Blade type</td>
<td>Mezzanine adapter</td>
<td>One mezzanine adapter vNICs/vCONs</td>
<td>Two mezzanine adapter vNICs/vCONs</td>
<td>Four mezzanine adapter vNICs/vCONs (statically mapped)</td>
<td>Mezzanine adapter supported combinations</td>
</tr>
<tr>
<td>------------</td>
<td>------------------</td>
<td>-----------------------------------</td>
<td>----------------------------------</td>
<td>------------------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vHBA0 &gt; vCON1 vNIC2 &gt; vCON2 vNIC3 &gt; vCON2 vHBA1 &gt; vCON2</td>
<td>vHBA0 &gt; vCON2 vNIC2 &gt; vCON2 vNIC3 &gt; vCON4 vHBA1 &gt; vCON4 vHBA2 &gt; vCON3 vHBA3 &gt; vCON1</td>
<td>vHBA0 &gt; vCON2 vNIC2 &gt; vCON2 vNIC3 &gt; vCON4 vHBA1 &gt; vCON4 vHBA2 &gt; vCON3 vHBA3 &gt; vCON1</td>
<td>2 x 1280 ((2 x 1240) + (2 x 1280))</td>
</tr>
<tr>
<td>2 x 1280</td>
<td>N/A</td>
<td>Statically mapped</td>
<td>Statically mapped</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>vNIC0 &gt; vCON1 vNIC1 &gt; vCON1 vHBA0 &gt; vCON1 vNIC2 &gt; vCON2 vNIC3 &gt; vCON2 vHBA1 &gt; vCON2</td>
<td>vNIC0 &gt; vCON1 vNIC1 &gt; vCON3 vHBA0 &gt; vCON3 vHBA1 &gt; vCON4 vHBA2 &gt; vCON3 vHBA3 &gt; vCON1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Important:** For a Cisco B460 M4 blade with a mezzanine adapter combination of two 1240-VICs and two 1280-VICs, install VMware vSphere ESXi with vNIC 0/1 and reboot. Add vNIC-2-Fabric-A, reboot. Add vNIC-3-Fabric-B and reboot. After each reboot, verify the new vNIC number and associated MAC address is correctly enumerated in both Cisco UCS Manager and VMware vSphere ESXi. Do not add vNIC2/3 to the service profile template. vNIC2/3 must be added manually to the service profile.

For a B200 M4 with dual mezzanine cards, install VMware vSphere ESXi with vNIC0/1 and reboot. Add vNIC-2-Fabric-A, reboot, followed by adding vNIC-3-Fabric-B and reboot. After each reboot, verify the new vNIC number and associated MAC address is correctly enumerated in both Cisco UCSM and VMware vSphere ESXi. Do not add vNIC2/3 to the service profile template. vNIC2/3 must be added manually to the service profile.

18 On the vMedia Policy window, click Next.
19 On the **Server Boot Order** window, click `1_storagesystem_serialnumber` and then click **Next**.

20 On the **Maintenance Policy** page, click **VCE-UserAck** in the **Maintenance Policy** field and then click **Next**.

21 On the **Server Assignment** window, perform the following:
   a Select **Up** for the power state.
   b In the **Host Firmware** field, click the appropriate firmware package.
   c Click **Next**.

22 On the **Operational Policies** window, select the following:
   a For **Bios Policy**, click **VCE_Default**.
   b For **Scrub Policy**, click **default**.
   c Select **External IPMI Management Configuration**.
   d For **IPMI Access Profile**, click the appropriate profile.

23 Click **Finish**.

24 To clone this service profile template, perform the following:
   a Right-click the service profile template that was just created.
   b Select **Create a Clone**.
   c For **Clone Name**, type an appropriate name for the service profile template. For example: `2_B200-01` or `2_B250-DualVIC01`.
   d For **Org**, click the appropriate organization. For example: **Root**.
   e Click **OK**.

25 To modify the service profile template that you just cloned, perform the following:
   a Select the service profile template that you just cloned and navigate to the **Boot Order** tab.
   b Select **Modify Boot Policy**.
   c Select the correct boot policy. For example: `2_storagesystem_serialnumber`.
   d Click **OK**.

26 To clone this service profile template, perform the following:
   a Right-click the service profile template that was just created.
b  Click **Create a Clone**.

c  For **Clone Name**, type an appropriate name for Service Profile Template 3. For example: 3_B200-01- or 3_B250-DualVIC-01.

d  For **Org**, select the appropriate organization. For example: *Root*.

e  Click **OK**.

27 To modify the service profile template that you just cloned, perform the following:

a  Select the service profile template that was just cloned and navigate to the **Boot Order** tab.

b  Select **Modify Boot Policy**.

c  Select the correct boot policy. For example: *3_storagesystem_serial number*

d  Click **OK**.

28 For FC Bandwidth Option only, to clone this service profile template, perform the following:

a  Right-click the service profile template that was just created.

b  Select **Create a Clone**.

c  For **Clone Name**, type an appropriate name for Service Profile Template 4. For example: 4_B200-01- or 4_B250-DualVIC-01.

d  For **Org**, click the appropriate organization. For example: *Root*.

e  Click **OK**.

29 To modify the service profile template that you just cloned, perform the following:

a  Select the service profile template that was just cloned and navigate to the **Boot Order** tab.

b  Select **Modify Boot Policy**.

c  Select the correct boot policy. For example: *4_storagesystem_serialnumber*

d  Click **OK**.

30 For FC Bandwidth Option only, to clone this service profile template, perform the following:

a  Right-click the service profile template that was just created.

b  Select **Create a Clone**.

c  For **Clone Name**, type an appropriate name for Service Profile Template 5. For example: 5_B200-01- or 4_B250-DualVIC-01.
d  For Org, click the appropriate organization. For example: Root.
e  Click OK.

31  To modify the service profile template that you just cloned, perform the following:
a  Select the service profile template that was just cloned and navigate to the Boot Order tab.
b  Select Modify Boot Policy.
c  Select the correct boot policy. For example: 5_storagesystem_serialnumber
d  Click OK.

Configuring service profile templates for disjoint layer 2

Use this procedure to configure four service profile templates for disjoint layer 2 for production blades that will run VMware.

About this task

You can disassociate the service profile from one server and then associate it with another manually or through an automated server pool policy. The burned-in settings, such as universally unique identifier (UUID) and media access control (MAC) address on the new server are overwritten with the configuration in the service profile. The change in server is transparent to your network and there is no need to reconfigure any component or application on your network to begin using the new server.

This profile allows you to manage and use the following system resources through resource pools and policies:

- Virtualized identity information, including pools of MAC addresses, world wide name (WWN) addresses, and UUIDs
- Ethernet and Fibre Channel (FC) adapter profile policies
- Firmware package policies
- Operating system boot order policies

Before you begin

Assign a minimum of four vNICs to each compute blade for VMware vSphere Distributed Switch (VDS) deployments.

To support disjoint layer 2 on certain blade types with multiple network physical ports additional to the onboard mLom ports, add vNICs 4 and 5 to the service profile individually between reboots AFTER you install VMware vSphere ESXi with the initial vNICs 0-3. With VMware vSphere 5.5, it is possible to re-map vmNICs after hypervisor installation. However, VMware does not support re-mapping the vmNICs after the hypervisor is installed without first submitting a support ticket.
Procedure

1. Launch the Cisco UCS Manager.

2. From the Navigation window, select the Servers tab and navigate to Service Profile Templates.

3. Right-click Service Profile Templates and select Create Service Profile Template.

4. From the Identify Service Template window, perform the following:
   a. In the Name field, type a name in the following format: `<Service Profile Template Identifier>_<Blade Type>_<VCE System or Vblock System ID>`
      - Service Profile Template Identifier = 1
      - Blade Type = B200 if installing B200 blades or B250 if installing B250 blades
      - Vblock System ID = 01 for first system or 02 for second system
   
      For example, if full-width blades (B250 or B440s) with dual mezzanine cards are installed:
      - 1_B250-DualVIC-01 and 2_B250-DualVIC-01
      - 2_B250-DualVIC-01 or 2_B440-DualVIC-01
   b. In the Type field, click Updating Template.
   c. In the UUID Assignment field, select the previously created pool, and click Next.

5. On the Networking page, in the How would you like to configure LAN Connectivity? field, select Expert, and click Add.

6. On the Create vNIC window, perform the following:
   a. In the Name field, type vNIC-0.
   b. In the vNIC Template field, click vNIC-0-Fabric-A.
   c. In the Adapter Policy field, click VMware and click OK.

7. Click Add to create vNIC-1.

8. On the Create vNIC window, perform the following:
   a. In the Name field, type vNIC-1.
   b. Select Use vNIC Template.
   c. In the vNIC Template field, click vNIC-1-Fabric-B.
   d. In the Adapter Policy field, click VMware and click OK.
9 Complete this step ONLY if installing or deploying:

- Cisco B460 quad blades or Cisco B250, B260, B440, or B420 full-width blades with dual mezzanine cards
- Cisco B200 M3, B22 M3, or B200 M4 with dual mezzanine cards
- VMware VDS 5.5 or later

**Important:** For the Cisco B460 M4 blade with a mezzanine adapter combination of two 1240-VICs and two 1280-VICs, do not add vNIC2/3 to the service profile template. vNIC2/3 must be added manually to the service profile.

- Install VMware vSphere ESXi with vNIC 0/1 and reboot.
- Add vNIC-2-Fabric-A to the service profile and reboot.
- Add vNIC-3-Fabric-B to the service profile and reboot.
- After each reboot, verify the new vNIC number and associated MAC address is correctly enumerated in both Cisco UCS Manager and VMware vSphere ESXi.

**Important:** For a Cisco B200 M4 blade with dual mezzanine cards, do not add vNIC2/3 to the service profile template. vNIC2/3 must be added manually to the service profile.

- Install VMware vSphere ESXi with vNIC0/1 and reboot.
- Add vNIC-2-Fabric-A to the service profile and reboot.
- Add vNIC-3-Fabric-B to the service profile and reboot.
- After each reboot, verify the new vNIC number and associated MAC address is correctly enumerated in both Cisco UCSM and VMware vSphere ESXi.

a From the Networking window, select Add to create vNIC-2.

b On the Create vNIC window, in the Name field, type vNIC-2.

c Select Use vNIC Template.

d In the vNIC Template field, click vNIC-2-Fabric-A.

e In the Adapter Policy field, click VMware and click OK.

f On the Networking window, click Add to create vNIC-3.

g On the Create vNIC window, in the Name field, type vNIC-3

h Select Use vNIC Template.

i In the vNIC Template field, click vNIC-3-Fabric-B.
In the Adapter Policy field, click VMware and click OK.

To assign the disjoint layer 2 vNICs to a service profile after the disjoint layer 2 service profile has been created, perform the following steps:

a. Verify that each service profile has VMware vSphere ESXi installed.

b. Verify that the correct vNIC number and associated MAC address is correctly enumerated in Cisco UCS Manager and VMware vSphere ESXi. vNIC and MAC address assignments must be consistent before adding disjoint layer 2 vNICs.

c. Add vNIC-4 to the service profile using vNIC-4-Fabric-A vNIC template and assign it to the correct vCON placement based on the disjoint layer 2 placement table.

d. Reboot the server and verify the new vNIC number and associated MAC address is correctly enumerated in both Cisco UCS Manager and VMware vSphere ESXi. vNIC and MAC address assignments must be consistent before adding disjoint layer 2 vNICs.

e. Add vNIC-5 to the service profile using the vNIC-5-Fabric-B vNIC template and assign it to the correct vCON placement based on the disjoint layer 2 placement table.

f. Reboot the server. Verify the new vNIC number and associated MAC address is correctly enumerated in both the Cisco UCS Manager and VMware vSphere ESXi. vNIC and MAC address assignments must be consistent before adding disjoint layer 2 vNICs.

On the Storage window, perform the following:

a. In the Local Storage field, click the UIM_nodisk policy that was previously created.

b. In the SAN Connectivity field, click Expert.

c. In the WWNN Assignment field, click Global-WWNN-Pool and click Add.

On the Create vHBA window, perform the following:

a. In the Name field, type vHBA-0.

b. Select Use vHBA Template.

c. In the vHBA Template field, click vHBA-0-Fabric-A.

d. In the Adapter Policy field, click VMware, then click OK and Add.

On the Create vHBA window, perform the following:

a. In the Name field, type vHBA-1.

b. Select Use vHBA Template.

c. In the vHBA Template field, click vHBA-1-Fabric-B.

d. In the Adapter Policy field, click VMware.
e Click OK and Next.

14 From the Networking page, for the B460 M4 blade with the following mezzanine adapter combination (two 1240-VICs and two 1280-VICs), click Add.

15 From the Create vHBA window, perform the following:
   a In the Name field, type vHBA-2.
   b Select Use vHBA Template.
   c In the vHBA Template field, click vHBA-2-Fabric-A.
   d In the Adapter Policy field, click VMware.
   e Select OK and Next.

16 From the Create vHBA window, perform the following:
   a In the Name field, type vHBA-3.
   b Click Use vHBA Template.
   c In the vHBA Template field, click vHBA-3-Fabric-A.
   d In the Adapter Policy field, click VMware.
   e Click OK and Next.

17 On the Zoning window, click Next.
For the vNIC/vHBA Placement window, refer to the following disjoint layer 2 vNIC/vCON placement table. For the placement of vNICs 0-3 and vHBAs 0-3, refer to the vNIC/vCON placement table.

For the Cisco Nexus 1000V Switch, the following configuration notes apply:

- If a Vblock System is configured to use the Cisco Nexus 1000V Switch, and the server has only one mezzanine adapter, the assignment of the four vNICs and two vHBAs to vCONs is system managed.

- If a Vblock System is configured to use the Cisco Nexus 1000V Switch and the server has more than one mezzanine adapter, the assignment of the six vNICs and two vHBAs to vCONs is statically mapped.

- In a Cisco B460 with four mezzanine adapters, four vHBAs can be configured.

- For the Cisco B200 M4 blade, regardless of the number of mezzanine adapters, vNICs are statically mapped to a vCON.

For VMware VDS, the following configuration notes apply:

- If a Vblock System is configured to use the VMware VDS and the server has only one mezzanine adapter, the assignment of the six vNICs and two vHBAs to vCONs is system managed.

- A Vblock System configuration with a VMware VDS always has a minimum of four vNICs.

- If a server with more than one mezzanine adapter is configured to use VMware VDS, the assignment of the six vNICs and two vHBAs to vCONs is statically mapped.

- In a Cisco B460 with four mezzanine adapters, four vHBAs can be configured.

- For the Cisco B200 M4 blade, regardless of the number of mezzanine adapters, vNICs are statically mapped to a vCON.

Add the four vNICs and two vHBAs to the vCON in the order indicated shown in the following table:

<table>
<thead>
<tr>
<th>Blade type</th>
<th>Mezzanine adapter</th>
<th>One mezzanine adapter</th>
<th>Two mezzanine adapters</th>
<th>Four mezzanine adapters</th>
<th>Mezzanine adapter supported combinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>B22 M3</td>
<td>1240</td>
<td>System managed</td>
<td>vNIC4 &gt; vCON1</td>
<td>N/A</td>
<td>1240 only, 1240 and 1280</td>
</tr>
<tr>
<td></td>
<td>1280</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>B200 M3</td>
<td>1240</td>
<td>System managed</td>
<td>vNIC4 &gt; vCON1</td>
<td>N/A</td>
<td>1240 only, 1240 and 1280</td>
</tr>
<tr>
<td></td>
<td>1280</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Blade type</td>
<td>Mezzanine adapter</td>
<td>One mezzanine adapter</td>
<td>Two mezzanine adapters</td>
<td>Four mezzanine adapters</td>
<td>Mezzanine adapter supported combinations</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------</td>
<td>-----------------------</td>
<td>------------------------</td>
<td>-------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>B200 M4</td>
<td>1340</td>
<td>vNIC4 &gt; vCON1</td>
<td>vNIC4 &gt; vCON1</td>
<td>N/A</td>
<td>1340 only&lt;br&gt;1340 and 1380</td>
</tr>
<tr>
<td></td>
<td>1380</td>
<td>N/A</td>
<td>vNIC5 &gt; vCON2</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>B230 M2</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>1280 only</td>
</tr>
<tr>
<td></td>
<td>1280</td>
<td>System managed</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>B250 M2 (EoS)</td>
<td>Palo</td>
<td>System managed</td>
<td>N/A</td>
<td>N/A</td>
<td>Palo only</td>
</tr>
<tr>
<td></td>
<td>1240</td>
<td></td>
<td>vNIC4 &gt; vCON1</td>
<td></td>
<td>1240 only</td>
</tr>
<tr>
<td>B260 M4</td>
<td>1240</td>
<td>System managed</td>
<td>vNIC4 &gt; vCON1</td>
<td>N/A</td>
<td>1240 only&lt;br&gt;1240 and 1280</td>
</tr>
<tr>
<td></td>
<td>1280</td>
<td>System managed</td>
<td>vNIC4 &gt; vCON1</td>
<td>N/A</td>
<td>1280 only&lt;br&gt;1240 and 1280</td>
</tr>
<tr>
<td>B420 M3</td>
<td>1240</td>
<td>System managed</td>
<td>N/A</td>
<td>N/A</td>
<td>1240 only</td>
</tr>
<tr>
<td></td>
<td>1280</td>
<td>System managed</td>
<td>N/A</td>
<td>N/A</td>
<td>1240 and 1280</td>
</tr>
<tr>
<td>B440 M2 w/ VMware vsphere 5.5</td>
<td>2 x 1280</td>
<td>N/A</td>
<td>vNIC4 &gt; vCON1</td>
<td>N/A</td>
<td>2 x 1280 only</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC5 &gt; vCON2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B460 M4</td>
<td>2 x 1240</td>
<td>N/A</td>
<td>vNIC4 &gt; vCON1</td>
<td>TBD</td>
<td>2 x 1240&lt;br&gt;((2 x 1240) + (2 x 1280))</td>
</tr>
<tr>
<td></td>
<td>2 x 1280</td>
<td>N/A</td>
<td>vNIC4 &gt; vCON1</td>
<td></td>
<td>2 x 1280&lt;br&gt;((2 x 1240) + (2 x 1280))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vNIC5 &gt; vCON2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** For the Cisco B460 M4 blade with the following mezzanine adapter combination (two 1240-VICs and two 1280-VICs), install VMware vSphere ESXi with vNIC 0/1, add vNIC-2-Fabric-A, reboot, and add vNIC-3-Fabric-B and reboot. After each reboot, verify the new vNIC number and associated MAC address is correctly enumerated in both Cisco UCS Manager and VMware vSphere ESXi.

For a Cisco B200 M4 with dual mezzanine cards, install VMware vSphere ESXi with vNIC0/1 and reboot. Then add vNIC-2-Fabric-A and reboot. Add vNIC-3-Fabric-B and reboot. After each reboot, verify the new vNIC number and associated MAC address is correctly enumerated in both Cisco UCSM and VMware vSphere ESXi.

19 On the vMedia Policy window, click Next.

20 On the Server Boot Order window, click 1_ storagesystem_serialnumber, and then click Next.
21 On the Maintenance Policy page, click VCE-UserAck in the Maintenance Policy field and then click Next.

22 On the Server Assignment window, perform the following:
   a. Select Up for the power state.
   b. In the Host Firmware field, select the appropriate firmware package.
   c. Click Next.

23 On the Operational Policies window, select the following:
   a. For Bios Policy, click VCE_Default.
   b. For Scrub Policy, click default.
   c. Select External IPMI Management Configuration.
   d. For IPMI Access Profile, click the appropriate profile.

24 Click Finish.

25 To clone this service profile template, perform the following:
   a. Right-click the service profile template that was just created.
   b. Select Create a Clone.
   c. For Clone Name, type an appropriate name for the service profile template. For example: 2_B200-01 or 2_B250-DualVIC01.
   d. For Org, click the appropriate organization. For example: Root.
   e. Click OK.

26 To modify the service profile template that you just cloned, perform the following:
   a. Click the service profile template that you just cloned and navigate to the Boot Order tab.
   b. Click Modify Boot Policy.
   c. Click the correct boot policy. For example: 2_storagesystem_serialnumber.
   d. Click OK.

27 To clone this service profile template, perform the following:
   a. Right-click the service profile template that was just created.
   b. Select Create a Clone.
c For **Clone Name**, type an appropriate name for Service Profile Template 3. For example: 3_B200-01- or 3_B250-DualVIC-01.

d For **Org**, select the appropriate organization. For example: **Root**.

e Click **OK**.

28 To modify the service profile template that you just cloned, perform the following:

a Select the service profile template that was just cloned and navigate to the **Boot Order** tab.

b Select **Modify Boot Policy**.

c Select the correct boot policy. For example: **3_storagesystem_serial number**

d Click **OK**.

29 For FC Bandwidth Option only, to clone this service profile template, perform the following:

a Right-click the service profile template that was just created.

b Select **Create a Clone**.

c For **Clone Name**, type an appropriate name for service profile template 4. For example: 4_B200-01- or 4_B250-DualVIC-01.

d For **Org**, click the appropriate organization. For example: **Root**.

e Click **OK**.

30 To modify the service profile template that you just cloned, perform the following:

a Select the service profile template that was just cloned and navigate to the **Boot Order** tab.

b Select **Modify Boot Policy**.

c Select the correct boot policy. For example: **4_storagesystem_serialnumber**

d Click **OK**.

31 For FC Bandwidth Option only, to clone this service profile template, perform the following:

a Right-click the service profile template that was just created.

b Select **Create a Clone**.

c For **Clone Name**, type an appropriate name for service profile template 5. For example: 5_B200-01- or 5_B250-DualVIC-01.

d For **Org**, click the appropriate organization. For example: **Root**.
To modify the service profile template that you just cloned, perform the following:

- Select the service profile template that was just cloned and navigate to the **Boot Order** tab.
- Select **Modify Boot Policy**.
- Select the correct boot policy. For example: `5_storagesystem_serialnumber`
- Click **OK**.

### Assigning a management IP address to the service profile

Assigning the management IP address to the service profile instead of the blade ensures that if the service profile moves to another blade, the IP address follows the service profile to the new blade.

**About this task**

Cisco UCS management software provides two options for connecting to a Cisco UCS cluster. The first option provides existing connectivity to the Cisco UCS Manager; the second option provides access to a Cisco KVM Manager.

The option to use static or pooled management IP addresses appears on the **Equipment > Chassis > Server > Inventory > CIMC** tab.

**Procedure**

1. On the **Navigation** window, select the **Servers** tab.
2. On the **Servers** tab, select **Servers > Service Profiles > Root**.
3. Select the first service profile, then on the right window, select **Change Management IP Address**.
4. Click **Static**.
5. Type the **IP Address**, **Subnet Mask**, and **Gateway**. Refer to the *Logical Configuration Survey* for the IP address for the CIMC IP address for the server.

**What to do next**

Repeat this process for all service profiles.

### Modifying the management IP address on a service profile

Use this procedure to change the management IP address on a service profile using the Cisco UCS Manager.
About this task

The Cisco UCS management software provides two options for connecting to a Cisco UCS cluster. The first option provides existing connectivity to the Cisco UCS Manager and the second provides access to a Cisco KVM Manager. The option to use static or pooled management IP addresses appears on the Equipment > Chassis > Server > Inventory > CIMC tab.

Before you begin

Obtain the:

- IP address
- Subnet mask
- Gateway to assign to the service profile

Procedure

1. On the Servers tab, select Servers > Service Profiles > Root.
2. Select the desired Service Profile.
4. In the Management IP Address Policy field, select Static.
5. Type the IP Address, Subnet Mask, and Default Gateway for the Cisco Integrated Management Controller (CIMC) IP address for the server.
6. Repeat this process for all service profiles.

Results

Verify the KVM functionality by initiating a KVM session to the blade from the service profile.

Assigning service profiles

Use this procedure to assign service profiles to the Cisco UCS servers using the Cisco UCS Manager.

Procedure

1. From the Navigation window, select the Servers tab.
2. On the Servers tab, click Service Profile Host-01-1.
3. Click Change Service Profile Association.
4. For Server Assignment, click Select Existing Server.
Choose the appropriate blade for this profile.

Evenly distribute service profiles within a VMware cluster across available chassis. The arrangement depends on the number of chassis and blades installed and the number of hosts in the VMware cluster. Coordinate with the person installing VMware to complete this procedure.

For example, four chassis with eight blades per chassis equals 32 blades. Four 8-node VMware clusters equals two blades per chassis:

- Assign service profiles 1 and 2 to chassis 1, blades 1 and 2.
- Assign service profiles 3 and 4 to chassis 2, blades 1 and 2.
- Assign service profiles 5 and 6 to chassis 3, blades 1 and 2.
- Assign service profiles 7 and 8 to chassis 4, blades 1 and 2.

Hosts in a VMware cluster should always belong to the same service profile template. For example, hosts 1 through 8 belong to template 1, hosts 9 through 16 belong to template 2.

Select **Restrict Migration** and click **OK**.

Repeat this procedure for all service profiles.

### Renaming service profiles

Use this procedure to rename service profiles using the Cisco UCS Manager.

**Procedure**

1. From the **Navigation** window, select the **Servers** tab.
2. On the **Servers** tab, right-click the existing service profile.
3. Select **Rename Service Profile**.
4. Type the desired service profile name.
5. Click **OK**.
Managing networking resources

Creating a named VLAN on both fabric interconnects

Add a named VLAN to both fabric interconnects in the Cisco UCS instance to create a connection to a specific external LAN.

About this task

A named VLAN creates a connection to a specific external LAN. The VLAN isolates traffic to that external LAN, including broadcast traffic. To ensure proper failover and load-balancing, VCE recommends adding VLANs to both fabric interconnects.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. VLANs with IDs in the range of 3968 to 4048 are reserved and cannot be used. Ethernet traffic is dropped on any VLAN that has an ID that overlaps with an FCoE VLAN ID.

Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN.

Before you begin

Obtain a unique VLAN name and VLAN ID.

Procedure

1. Log on to the Cisco UCS Manager and select the LAN tab.
2. Expand LAN > LAN CLOUD, right-click on LAN Cloud and select Create VLANs.
3. In the Create VLANs window:
   a. Type the name of the VLAN in the Name field.
   b. Select Common/Global to apply the VLANs to both fabrics and use the same configuration parameters in both cases.
   c. Type the VLAN ID.
4. Click Check Overlap to ensure that the VLAN ID does not overlap with any other IDs on the system.
5. Click OK.

What to do next

After creating the VLAN, add the VLAN to a service profile using Cisco UCS Manager.
Adding a VLAN to a service profile template

Add VLAN to a service profile template for both Ethernet interfaces.

Procedure

1. Log in to the Cisco UCS Manager and select the **Servers** tab.
2. Expand **Servers > Service Profiles Templates** and select the service profile template to which you want to add a VLAN.
3. Expand the service profile and select **vNICs**.
4. On the right side of the vNICs window, select an Ethernet interface and click **Modify**.
5. If the **Use vNIC Template** option is selected, de-select this option to modify this single service profile.
6. From the list of VLANs, select the VLAN you created and click **OK**.
7. Repeat these steps for the other Ethernet interface.

What to do next

Add the VLANs to the Cisco Nexus 55xx Series switches, Cisco Nexus 1000V Series virtual switch, and any other switching infrastructure that is required.

Adding a VLAN to the Cisco Nexus 1000V Switch

This procedure provides an example of how to add a VLAN to the Cisco Nexus 1000V Switch using Cisco NX-OS commands.

Before you begin

- Verify that the Cisco Nexus 1000V Virtual Supervisor Modules are up and reachable through the console or the management connection.
- Obtain VLAN IDs and names.

**Important:** Obtain approval from VCE before changing management settings.
Procedure

1. To view VLANs, type: `show vlan`
2. To create a VLAN, type: `configure terminal`
3. To assign an ID to the VLAN, type: `vlan vlan_id`
4. To assign a name to the VLAN, type: `name vlan_name`
5. To view information about the new VLAN, type: `show vlan vlan_id`

Related information

Cisco Nexus 1000V Port Profile Configuration Guide

Adding a VLAN to the Cisco Nexus series switches

Use this procedure to add a VLAN to the Cisco Nexus series switches using Cisco NX-OS commands.

About this task

VCE recommends that naming VLANs to identify usage. For example, for VLAN 109: NFS-VLAN-109.

Before you begin

Verify that the Cisco Nexus series switches are up and reachable through the console or the management connection.

Verify connectivity information for the Cisco Nexus series switches, such as:

- Console information
- Login credentials
- IP address
- Access method (SSH/TELNET)
- VLAN names

Procedure

1. To view all VLANs, type: `show vlan`
2. To create a VLAN, type: `configure terminal`
3. To assign an ID to the VLAN, type: `vlan vlan_id`
4. To assign a name to the VLAN, type: `name vlan_name`

5. To view information about the new VLAN, type: `show vlan vlan_id`

Related information

Configuring a virtual port channel (see page 59)

Reversing the procedure

Procedure

To reverse this procedure, type `no vlan vlan_id`

Configuring a virtual port channel

Use this procedure to configure a Cisco virtual port channel (vPC) on the Cisco Nexus series switches.

About this task

When configuring a Cisco vPC, you can use any available Ethernet port to form a Cisco vPC enabled port-channel. VCE recommends that the spanning tree mode on the port channels be configured appropriately. For example, spanning tree mode on port channels towards the aggregation switches can be configured as normal and towards servers and other non-network devices as edge.

Default Vblock System port channels are:

- PO1 for the network uplink
- PO50 between the switches
- PO101 and PO102 from the switch to the fabric interconnects
- 47 and 48 for the AMP
- PO201 and PO202 for the X-Blades

To view ports reserved by VLANs, type: `show vlan brief`

Before you begin

- Verify that the Cisco Nexus series switches can be reached through the console or the management connection
- Verify that the vPC, link aggregation control protocol (LACP) features are enabled on the Cisco Nexus series switches.
• Verify that LACP is enabled on the peering device doing port channeling with the Cisco Nexus series switches
• Verify that the appropriate member Ethernet ports are physically cabled
• Verify the Ethernet ports that will become members of this port channel
• Create a VLAN
• Obtain required vPCs, IDs, and the VLANs that need to be in each vPC
• Obtain Cisco Nexus series switches connectivity information (IP address/console information), login credentials and access method (SSH/TELNET)

Procedure

1. Log in to the primary Cisco Nexus series switch.
2. To start the configuration, type: `Switch-A# config terminal`
3. To specify the port channel, type: `Switch-A(config)# interface port-channel port_channel_number`
4. To add a description, type: `Switch-A(config-if)# description description`
   
   **Note:** The description should include to, from, and a purpose.
   
   **For example:** description To X-Blade Server 2 for NFS
5. To specify the switchport mode, type: `Switch-A(config-if)# switchport mode mode`
   
   where `mode` is **Trunk** or **Access**.
6. To specify the Cisco vPC ID, type: `Nexus5548-A(config-if)# vpc vPC_ID`
7. To specify the access VLAN or the VLANs that need to be trunked, type one of the following:
   
   — `Switch-A(config-if)# switchport access vlan_id`
   
   — `Switch-A(config-if)# switchport trunk allowed vlan vlan_id`
8. To set the spanning tree port, type: `Switch-A(config-if)# spanning-tree port type type`
   
   where `type` specifies the type: `normal/network/edge` trunk/etc.
9. To set the state, type: `Nexus5548-A(config-if)# no shut`
10 To add the appropriate Ethernet ports as members of the port channel:
   a Type Switch-A(config)# interface ethernet port_number
   b Type Switch-A(config-if)# switchport mode mode where mode is Trunk or Access (same as the port channel).
   c Type Switch-A(config-if)# channel group channel_number mode active

11 To set the state, type: Switch-A(config-if)# no shut

12 To save the configuration, type: Switch-A# copy run start

13 Repeat this procedure on the peer switch.

Related information

Adding a VLAN to the Cisco Nexus series switches (see page 58)
Deleting a virtual port channel (see page 61)
Cisco Nexus 5000 Series NX-OS Software Configuration Guide

Deleting a virtual port channel

Use this procedure to delete a virtual port channel (vPC).

Procedure

1 Log in to the Cisco Nexus series switch.

2 To start the configuration, type: Switch-A# config terminal

3 To remove the appropriate Ethernet port as members of the port channel, type: Switch-A#interface ethernet port_number

4 Type: Switch-A(config-if)# no channel group channel_number mode active

5 To delete the port channel, type: Switch-A(config)# no interface port-channel port_channel_number

Related information

Configuring a virtual port channel (see page 59)
Cisco Nexus 5000 Series Switches Virtual PortChannel Quick Configuration Guide
Adding VLANs to the trunk of a virtual port channel

Use this procedure to add VLANs to the trunk of an existing Cisco virtual port channel (vPC) on the Cisco Nexus series switch.

About this task

Additional VLANs are added to the trunk of an existing virtual port channel when it is modified.

Before you begin

- Verify that the Cisco Nexus series switch is reachable through the console or the management connection
- Verify that the Cisco vPC that needs to be modified is up
- Obtain the required Cisco vPC ID and VLANs that need to be added to the Cisco vPC
- Cisco Nexus series switch connectivity information (IP address/console information), login credentials and access method (SSH/TELNET)

Procedure

1 Log in to the primary Cisco Nexus series switch.
2 To run the configuration, type: Switch-A# config terminal
3 To specify the port channel, type: Switch-A(config)# interface port-channel port_channel_number
4 To add the VLANs, type: Switch-A(config)# switchport trunk allowed vlan add VLAN_IDs
5 Repeat this procedure on the peer Cisco Nexus series switch.

Related information

Removing VLANs from the trunk of a virtual port channel (see page 62)

Removing VLANs from the trunk of a virtual port channel

Use this procedure to remove VLANs from a Cisco virtual port channel (vPC).

Procedure

1 Log in to Cisco Nexus series switch.
2 To run the configuration, type: `Switch-A# config terminal`

3 Type: `Switch-A(config)# interface port-channel port_channel_number`

4 To remove the VLAN ID, type: `Switch-A(config-if)# switchport trunk allowed vlan remove VLAN_IDs`

Related information

Adding VLANs to the trunk of a virtual port channel (see page 62)
Cisco Nexus 5000 Series Switches Virtual PortChannel Quick Configuration Guide
Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide

Adding port channels to VLANs for disjoint layer 2 networks

Adding port channels to VLANs for disjoint layer 2 networks defines the VLANs that pass over specific uplinks using the Cisco UCS Manager.

About this task

The procedure shows an example scenario for adding port channels to VLANs for disjoint layer 2 networks.

All VLANs must be explicitly assigned to an uplink, including VLANs added after initial deployment. Otherwise, a VLAN is allowed to travel over all uplinks, which breaks the disjoint layer 2 concept.

Cisco virtual port channels (vPCs) 101 and 102 are production uplinks that connect to Cisco Nexus Switch. Cisco vPCs 105 and 106 are customer uplinks that connect to the customer's switches. If you use
Ethernet performance port channels (103 and 104 by default), port channels 101 through 104 should have the same VLANs assigned.

Before you begin
Obtain the port channels, VLANs, and VLAN-to-port channel assignments.

Procedure

1. Log in to the Cisco UCS Manager.
2 To assign VLANs to port channels 101 and 105 in fabric A, perform the following:
   a  Select the LAN tab.
   b  Select the LAN node.
   c  From the LAN Uplinks Manager tab, select VLANs > VLAN Manager.
   d  Select Fabric A.
   e  In the Port Channels and Uplinks tab, select Port-Channel 101.
   f  In the VLANs table, select the VLANs to assign to port channel 101. Use the CTRL key to select more than one VLAN.
   g  Click Add to VLAN and OK
   h  In the Port Channels and Uplinks tab, select Port-Channel 105.
   i  In the VLANs table, select the VLANs to assign to port channel 105.
   j  Click Add to VLAN and OK.
   k  Verify that port channels 101 and 105 (Fabric B) display under all required VLANs. Refer to Viewing port channels assigned to VLANs for disjoint layer 2 networks.

3 To assign VLANs to port channels 102 and 106 in fabric B, perform the following:
   a  In VLAN Manager Navigation window, select the LAN tab.
   b  Select the LAN node.
   c  In the Work window, select the LAN Uplinks Manager link on the LAN Uplinks tab.
   d  In the LAN Uplinks Manager, select VLAN Manager.
   e  Select Fabric B.
   f  In the Port Channels and Uplinks tab, select Port-Channel 102.
   g  In the VLANs table, select the VLANs to assign to port channel 102. Use the CTRL key to select more than one VLAN.
   h  Select Add to VLAN and click OK.
   i  In the Port Channels and Uplinks tab, select Port-Channel 106.
   j  In the VLANs table, select the VLANs to assign to port channel 106.
   k  Select Add to VLAN and click OK.
Verify that port channels 102 and 106 (Fabric B) display under all required VLANs. Refer to Viewing port channels assigned to VLANs for disjoint layer 2 networks.

Related information

Viewing port channels assigned to VLANs for disjoint layer 2 networks (see page 66)
Removing port channels from VLANs for disjoint layer 2 networks (see page 66)
Cisco UCS Manager Configuration Guide: Configure upstream disjoint layer 2 network

**Viewing port channels assigned to VLANs for disjoint layer 2 networks**

Use this procedure to verify that port channels have been assigned to VLANs.

**Procedure**

1. Log in to the Cisco UCS Manager.
2. In the **Navigation** window, select the **LAN** tab.
3. On the **LAN** tab, select the **LAN** node.
4. In the **Work** window, select the **LAN Uplinks Manager** link on the **LAN Uplinks** tab.
5. In the **LAN Uplinks Manager**, select **VLANs** > **VLAN Manager**.
6. Click Fabric A or Fabric B to view the port channels and VLANs on that fabric interconnect.
7. In the VLANs table, expand the appropriate node and the VLAN for which you want to view the assigned ports or port channels.

Related information

Adding port channels to VLANs for disjoint layer 2 networks (see page 63)
Removing port channels from VLANs for disjoint layer 2 networks (see page 66)
Cisco UCS GUI Configuration Guide: Configuring upstream disjoint layer 2 networks

**Removing port channels from VLANs for disjoint layer 2 networks**

Use this procedure in a disjoint layer 2 network configuration to remove port channels from VLANs.
About this task

If you remove all port or port channel interfaces from a VLAN, the VLAN returns to the default behavior and data traffic on that VLAN flows on all uplink ports and port channels. Depending upon the configuration in the Cisco UCS domain, this default behavior can cause Cisco UCS Manager to drop traffic for that VLAN. To avoid this, VCE recommends that you either assign at least one interface to the VLAN or delete the VLAN.

Procedure

1. Log in to the Cisco UCS Manager.
2. In the Navigation window, select the LAN tab.
3. On the LAN tab, select the LAN node.
4. In the Work window, select the LAN Uplinks Manager link on the LAN Uplinks tab.
5. In the LAN Uplinks Manager, select VLANs > VLAN Manager.
6. Click Fabric A or Fabric B to view the port channels and VLANs on that fabric interconnect.
7. In the VLANs table, expand the appropriate node and the VLAN from which you want to remove the assigned ports or port channels.
8. Click the port or port channel that you want to remove from the VLAN.
   Note: Hold down the Ctrl key to click multiple ports or port channels.
9. Click Remove from VLAN.
10. If a confirmation dialog box appears, click Yes.
11. Click Apply if you want to continue to work in the VLAN Manager or click OK to close the window.

Related information

Viewing port channels assigned to VLANs for disjoint layer 2 networks (see page 66)

Adding port channels to VLANs for disjoint layer 2 networks (see page 63)

Cisco UCS Manager GUI Configuration Guide: Configuring upstream disjoint layer 2 networks

Upgrading Cisco Nexus 9000 Series Switch software

Use this procedure to upgrade the system image on the Cisco Nexus 9000 Series Switch.
About this task

- Back up the original configuration by typing: `copy running-config startup-config`
- Verify that the configuration has been updated and back up the new configuration
- There are two switches that require upgrades. Some operational checking is recommended after the first switch is upgraded to ensure that a platform outage does not occur before upgrading the second switch

Before you begin

Refer to the Cisco website to access the software upgrade code.

Obtain:

- Console (terminal) access
- Management IP access
- Cisco account to download images
- An SCP, TFTP, FTP or SFTP server to upload the Cisco NX-OS image to the switch

Review Cisco release notes before any upgrade.

Procedure

1. Go to the [Cisco Support](https://www.cisco.com) website to download the Cisco NX-OS bin file system software for the Cisco Nexus series switch.
2. Upload the file to the switch with the copy server (TFTP, SCP, FTP, or SFTP) being used.
3. To back up the switch running the configuration, type: `copy running-config startup-config`
4. To verify the switch has enough space for the new image, type: `VSJ3X2N9396B# dir bootflash:`
5. If there is not enough space, type: `delete bootflash:filename`
6. To copy the updated images to the switch, type: `VSJ3X2N9396A(config)# copy ftp: bootflash:
   a. Type the filename of the kickstart bin file from the Cisco download site. For example, `n9000-dk9.6.1.2.I2.2(1).bin`
   b. For VRF, type: `management`
   c. Type the hostname of the FTP server.`
Type the username and password. The system copies the images to the switch, and the following message appears:

```
***** Transfer of file Completed Successfully *****
```

7. To view the impact of the upgrade, type: `VSJ3X2N9396A(config)# show install all impact kickstart bootflash:n9000-dk9.6.1.2.I2.2(1).bin`

8. If you are performing a disruptive upgrade, following warning appears:

```
Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)? [n] y
Install is in progress, please wait.
Performing runtime checks.
[############################] 100% -- SUCCESS
Setting boot variables.
[############################] 100% -- SUCCESS
Performing configuration copy.
[############################] 100% -- SUCCESS
Module 1: Refreshing compact flash and upgrading bios/loader/bootrom/power-seq.
Warning: please do not remove or power off the module at this time.
Note: Power-seq upgrade needs a power-cycle to take into effect.
On success of power-seq upgrade, SWITCH OFF THE POWER to the system and then, power it up.
Note: Micro-controller upgrade needs a power-cycle to take into effect.
On success of micro-controller upgrade, SWITCH OFF THE POWER to the system and then, power it up.
[############################] 100% -- SUCCESS
Finishing the upgrade, switch will reboot in 10 seconds.
VSJ3X2N9396A(config)# 2011 Sep 8 18:16:43 VSJ3X2N9396A Sep 8 18:16:43 %KERN-0-
SYSTEM_MSG: Shutdown Ports.. - kernel
2011 Sep 8 18:16:43 VSJ3X2N9396A Sep 8 18:16:43 %KERN-0-SYSTEM_MSG: writing reset
reason 49, - kernel
Broadcast message from root (Thu Sep 8 18:16:43 2011):
The system is going down for reboot NOW!
```

9. Type `Y` to continue with the installation.

10. When the switch reboots, to verify that the updated version of the software is running, type: `show version`

11. In the version information that is returned, check that the kickstart image file and system image file are the correct version.

What to do next

Some operational checking is recommended after upgrading the first switch to ensure that a platform outage is not experienced before upgrading the second switch.

When you have verified that the configuration has been updated successfully, create a backup of the new configuration.
Reversing the procedure

Procedure

To reverse the procedure, perform the upgrade steps using the earlier version of the software.

Upgrading Cisco Nexus 5500 Series Switch software

Use this procedure to upgrade both the Cisco NX-OS Kickstart and Cisco NX-OS System images on the Cisco Nexus 5500 series switch.

About this task

Always upgrade the two images together and verify that the version numbers of the images are the same. After verifying that the configuration has been updated successfully, create a backup of the new configuration. There are two switches that must be upgraded. Some operational checking is recommended after upgrading the first switch to ensure that a platform outage is not experienced before upgrading the second switch.

Before you begin

- Review Cisco release notes before any upgrade
- Back up the switch running the configuration by typing: `copy running-config startup-config`
- Obtain:
  - Console (terminal) access
  - Management IP access
  - Cisco account to download images
  - An SCP, TFTP, FTP or SFTP server to upload the Cisco NX-OS image to the switch

Procedure

1. Go to the Cisco Support website and download the Cisco NX-OS Kickstart and Cisco NX-OS System Software for the Cisco Nexus 5500 Series Switch.
2. Upload the two files to the switch with the copy server (TFTP, SCP, FTP, or SFTP) being used.
3. To back up the switch running the configuration, type: `copy running-config startup-config`
4 To verify the switch has enough space for the new image, type: **VSJ3X2N5548B# dir bootflash:**

```plaintext
495    Apr 06 03:47:56 2011  license_XXXXXXXX.lic
49152   Apr 06 03:51:08 2011  lost+found/
1893    May 26 23:14:43 2011  mts.log
25164288  Apr 06 03:41:50 2011  n5000-uk9-kickstart.5.0.2.N2.1.bin
156932426  Apr 06 03:42:36 2011  n5000-uk9.5.0.2.N2.1.bin
4096    Jan 01 03:45:25 2009  vdc_2/
4096    Jan 01 03:45:25 2009  vdc_3/
4096    Jan 01 03:45:26 2009  vdc_4/
```

Usage for bootflash://sup-local

- 299823104 bytes used
- 1351081984 bytes free
- 1650905088 bytes total

**VSJ3X2N5548B#**

5 If there is not enough space, type: **delete bootflash:filename**

6 To copy the updated images to the switch, from VSJ3X2N5548A(config)#, type: **VSJ3X2N5548A(config)# copy ftp: bootflash:**

   a Type the filename of the kickstart bin file from the Cisco download site. For example, **n5000-uk9-kickstart.5.0.3.N1.1c.bin**

   b For the VRF, type: **management**

   c Type the hostname of the FTP server.

   d Type the username and password. The system copies the images to the switch, and the following message appears:

```
***** Transfer of file Completed Successfully *****
```
To view the impact of the upgrade, from VSJ3X2N5548A(config) #, type: `show install all impact kickstart bootflash:n5000-uk9-kickstart.5.0.3.N1.1c.bin`

Verifying image bootflash:/n5000-uk9-kickstart.5.0.3.N1.1c.bin for boot variable "kickstart". [################################] 100% -- SUCCESS
Verifying image bootflash:/n5000-uk9.5.0.2.N2.1.bin for boot variable "system". [################################] 100% -- SUCCESS
Verifying image type. [########################] 100% -- SUCCESS
50%

Verifying image bootflash:/n5000-uk9-kickstart.5.0.3.N1.1c.bin for boot variable "kickstart". [################################] 100% -- SUCCESS
Verifying image bootflash:/n5000-uk9.5.0.2.N2.1.bin for boot variable "system". [################################] 100% -- SUCCESS
Verifying image type. [########################] 100% -- SUCCESS
50%

Extracting "system" version from image bootflash:/n5000-uk9.5.0.2.N2.1.bin.
[################################] 100% -- SUCCESS
Extracting "kickstart" version from image bootflash:/n5000-uk9-kickstart.5.0.3.N1.1c.bin.
[################################] 100% -- SUCCESS
Extracting "bios" version from image bootflash:/n5000-uk9.5.0.2.N2.1.bin.
[################################] 100% -- SUCCESS
Performing module support checks. [################################] 100% -- SUCCESS
Notifying services about system upgrade. [################################] 100% -- SUCCESS
Compatibility check is done:

<table>
<thead>
<tr>
<th>Module</th>
<th>bootable</th>
<th>Impact</th>
<th>Install-type</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>no</td>
<td>n/a</td>
<td>n/a</td>
<td>Incompatible image</td>
</tr>
</tbody>
</table>

Images will be upgraded according to following table:

<table>
<thead>
<tr>
<th>Module</th>
<th>Image</th>
<th>Running-Version</th>
<th>New-Version</th>
<th>Upg-Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>system</td>
<td>5.0(2)N2(1)</td>
<td>5.0(2)N2(1)</td>
<td>no</td>
</tr>
<tr>
<td>1</td>
<td>kickstart</td>
<td>5.0(2)N2(1)</td>
<td>5.0(3)N1(1c)</td>
<td>no</td>
</tr>
<tr>
<td>1</td>
<td>bios</td>
<td>v1.8.0(10/06/2010)</td>
<td>v1.8.0(10/06/2010)</td>
<td>no</td>
</tr>
<tr>
<td>1</td>
<td>power-seq</td>
<td>v3.0</td>
<td>v3.0</td>
<td>no</td>
</tr>
<tr>
<td>2</td>
<td>power-seq</td>
<td>v1.0</td>
<td>v1.0</td>
<td>no</td>
</tr>
<tr>
<td>1</td>
<td>uC</td>
<td>v1.1.0.1</td>
<td>v1.0.0.14</td>
<td>no</td>
</tr>
</tbody>
</table>

Additional info for this installation:

Port: port-channel52 in VLAN0001 is Designated. Topology change could occur during ISSU.
Upgrade needs to be disruptive!!!
To install the new Cisco NX-OS images, type:

```
VSJ3X2N5548A(config)# install all
kickstart bootflash:n5000-uk9-kickstart.5.0.3.N1.1c.bin system
bootflash:n5000-uk9.5.0.3.N1.1c.bin.
```

To view installation progress, any time during the installation process, type: `show install all`

```
Verifying image bootflash:/n5000-uk9-kickstart.5.0.3.N1.1c.bin for boot variable "kickstart".
[########################] 100% -- SUCCESS
Verifying image bootflash:/n5000-uk9.5.0.3.N1.1c.bin for boot variable "system".
[########################] 100% -- SUCCESS
Verifying image type.
[########################] 100% -- SUCCESS
Extracting "system" version from image bootflash:/n5000-uk9.5.0.3.N1.1c.bin.
[########################] 100% -- SUCCESS
Extracting "kickstart" version from image bootflash:/n5000-uk9-kickstart.5.0.3.N1.1c.bin.
[########################] 100% -- SUCCESS
Extracting "bios" version from image bootflash:/n5000-uk9.5.0.3.N1.1c.bin.
[########################] 100% -- SUCCESS
Performing module support checks.
[########################] 100% -- SUCCESS
Notifying services about system upgrade.
[########################] 100% -- SUCCESS
Compatibility check is done:

<table>
<thead>
<tr>
<th>Module</th>
<th>bootable</th>
<th>Impact</th>
<th>Install-type</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>1</td>
<td>yes</td>
<td>disruptive</td>
<td>reset</td>
<td>STP ISSU preupgrade check failed</td>
</tr>
</tbody>
</table>

- Upgrade needs to be disruptive!

Images will be upgraded according to following table:

```
<table>
<thead>
<tr>
<th>Module</th>
<th>Image</th>
<th>Running-Version</th>
<th>New-Version</th>
<th>Upg-Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>system</td>
<td>5.0(2)N2(1)</td>
<td>5.0(3)N1(1c)</td>
<td>yes</td>
</tr>
<tr>
<td>1</td>
<td>kickstart</td>
<td>5.0(2)N2(1)</td>
<td>5.0(3)N1(1c)</td>
<td>yes</td>
</tr>
<tr>
<td>1</td>
<td>bios</td>
<td>v1.8.0(10/06/2010)</td>
<td>v3.5.0(02/03/2011)</td>
<td>yes</td>
</tr>
<tr>
<td>1</td>
<td>power-seq</td>
<td>v3.0</td>
<td>v3.0</td>
<td>no</td>
</tr>
<tr>
<td>2</td>
<td>power-seq</td>
<td>v1.0</td>
<td>v1.0</td>
<td>no</td>
</tr>
<tr>
<td>1</td>
<td>uC</td>
<td>v1.1.0.1</td>
<td>v1.0.0.14</td>
<td>no</td>
</tr>
</tbody>
</table>
```

Additional info for this installation:

- Port: port-channel52 in VLAN0001 is Designated. Topology change could occur during ISSU.
- Upgrade needs to be disruptive!!!
If you are performing a disruptive upgrade, following warning appears:

Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)? [n] y
Install is in progress, please wait.
Performing runtime checks.
[####################] 100% -- SUCCESS
Setting boot variables.
[####################] 100% -- SUCCESS
Performing configuration copy.
[####################] 100% -- SUCCESS
Module 1: Refreshing compact flash and upgrading bios/loader/bootrom/power-seq.
Warning: please do not remove or power off the module at this time.
Note: Power-seq upgrade needs a power-cycle to take into effect.
On success of power-seq upgrade, SWITCH OFF THE POWER to the system and then, power it up.
Note: Micro-controller upgrade needs a power-cycle to take into effect.
On success of micro-controller upgrade, SWITCH OFF THE POWER to the system and then, power it up.
[####################] 100% -- SUCCESS
Finishing the upgrade, switch will reboot in 10 seconds.

Type y to continue with the installation.
11 When the switch reboots, to verify that the updated version of the software is running, type: `show version`

```
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at http://www.gnu.org/licenses/gpl.html.
Software
BIOS:      version 3.5.0
loader:    version N/A
kickstart: version 5.0(3)N1(1c)
system:    version 5.0(3)N1(1c)
power-seq: Module 1: version v3.0
           Module 2: version v1.0
           Module 3: version v2.0
uC:        version v1.1.0.1
BIOS compile time:       02/03/2011
kickstart image file is: bootflash:/n5000-uk9-kickstart.5.0.3.N1.1c.bin
kickstart compile time:  5/4/2011 3:00:00 [05/04/2011 10:43:31]
system image file is:    bootflash:/n5000-uk9.5.0.3.N1.1c.bin
system compile time:     5/4/2011 3:00:00 [05/04/2011 12:35:20]
Hardware
cisco Nexus5548 Chassis ("O2 32X10GE/Modular Supervisor")
Intel(R) Xeon(R) CPU         with 8299528 kB of memory.
Processor Board ID JAF1513CCCF
Device name: VSJ3X2N5548A
bootflash: 2007040 kB
Kernel uptime is 0 day(s), 0 hour(s), 8 minute(s), 43 second(s)
Last reset at 696441 usecs after Thu Sep  8 18:16:43 2011
   Reason: Disruptive upgrade
System version: 5.0(2)N2(1)
Service:
plugin
Core Plugin, Ethernet Plugin
```

12 In the version information that is returned, check that the kickstart image file and system image file are the correct version.

What to do next
Some operational checking is recommended after upgrading the first switch to ensure that a platform outage is not experienced before upgrading the second switch.

When the configuration has been updated successfully, create a backup of the new configuration.

Related information

Cisco Support
Reversing the procedure

Procedure

To reverse the procedure, perform the upgrade steps using the earlier version of the software.
Managing Cisco MDS switches

Upgrading Cisco MDS switch software

Use this procedure to upgrade or downgrade the firmware on the Cisco MDS series switches.

Before you begin

There are two switches that must be upgraded. Perform operational checking after upgrading the first switch to ensure that a platform outage does not occur before upgrading the second switch. Obtain:

- Console (terminal) access
- Management IP access
- A Cisco account to download any images
- A SCP, TFTP, FTP, or SFTP server to upload the Cisco NX-OS image to the switch
- Obtain access to software upgrade code on the Cisco website

Review Cisco release notes before any upgrade.

Procedure

1. To log in to the Cisco MDS switch and save the running configuration, type: `copy run tftp://tftp-server/filename` or `copy run ftp://ftp server/filename`

2. From the Cisco Support website, under Select a Task, select Download Software.

3. From the Products list, select Cisco IOS and NX-OS Software.

4. Select Download Software.

5. Select the switch and required software version, and select Download Now. Kickstart file names are as follows:
   - MDS9513: m9500-sf2ek9-kickstart-mz.5.2.2d.bin
   - MDS9148: m9100-s3ek9-kickstart-mz.5.2.2d.bin

   NX-OS file names:
   - MDS9513: m9500-sf2ek9-mz.5.2.2d.bin
   - MDS9148: m9100-s3ek9-mz.5.2.2d.bin
6 Download Kickstart and system software with the copy server (TFTP, SCP, FTP, SFTP) is being used.

7 While in the bootflash directory, copy Kickstart and the system files from the FTP copy server to the fabric switch as follows:

   a Type MDS# cd bootflash:
   b To verify there is enough free space, type MDS# dir
   c Type MDS# copy ftp://ftp_server_addr/filename.bin filename.bin
   d Type MDS# copy ftp://ftp_server_addr/filename.bin filename.bin

8 To verify that there is enough storage on the standby supervisor, perform the following:

   a Type MDS# cd bootflash:
   b Type MDS# dir

9 While in configure mode, type: VSJ3X2M9148B# configure terminal

    Type configuration commands, one per line. End with CNTL/Z.
    VSJ3X2M9148B(config)# no logging level all

10 To check the impact of the firmware upgrade, type: VSJ3X2M9148B# show install all

     impact kickstart m9100-s5ek9-kickstart-mz.6.2.9a.bin system m9100-
     s5ek9-mz.6.2.9a.bin

11 To ensure that you can view the entire upgrade process, perform the upgrade using the console port. You can log your session to a file for future reference.

12 To install system and Kickstart software, type: VSJ3X2M9148B# install all

     kickstart m9100-s5ek9-kickstart-mz.6.2.9a.bin system m9100-s5ek9-mz.6.2.9a.bin

13 After the update completes, to view the status of the install, type: show install all status

Reversing the procedure

Procedure

Refer to the release notes section Downgrading Your Cisco MDS SAN-OS Software Image and follow the guidelines before downgrading the software.

Related information

Cisco.com
Configuring a VSAN

Use this procedure to configure a VSAN and to assign Fibre Channel (FC) interfaces.

About this task
VCE recommends that the VSANs be named to identify usage. For example, for VSAN 10: SAN_A.

Before you begin

- Verify that the Cisco MDS switch is up and reachable through the console or management connection
- Obtain required VSANs, names, and FC interfaces that need to be assigned to the VSANs
- Obtain Cisco MDS switch connectivity information (IP address/console information), login credentials and access method (SSH/TELNET)

Procedure

1. Log in to the Cisco MDS switch.
2. To view VSANs, type: show vsan
3. To enter the global configuration mode and start the configuration, type: switch# configure terminal
4. To configure the database for VSAN, type: switch(config)# vsan database
5. To specify the VSAN being created, type: switch(config-vsan-db)# vsan vsan_id
6. To specify the VSAN name, type: switch(config-vsan-db)# vsan vsan_id name vsan_name
7. To assign an FC interface to the VSAN, type: switch(config-vsan-db)# vsan vsan_id interface fc slot
8. To update the interface with the VSAN, type: switch(config-vsan-db)# vsan vsan_id fc slot

Related information

Cisco: Configuring and Managing VSANs
Reversing the procedure

Procedure

1. To enter the global configuration mode and start the configuration, type: `switch# configure terminal`

2. Type: `switch(config)# vsan database`

3. To delete a VSAN, type `no vsan vsan_id`

Configuring a domain ID and priority for a VSAN

A unique domain ID must be assigned to the new VSAN added to the switch.

About this task

When a new VSAN is added to a switch in a fabric, the domain manager is used to assign a domain ID and priority to the VSAN. When a switch boots up or joins a new fabric, it can request a specific domain ID or take any available domain_ID.

Before you begin

- Verify that the Cisco MDS switch is up and reachable through the console or management connection
- Obtain required VSANs, names, and FC interfaces that need to be assigned to the VSANs
- Verify that the domain ID of the new VSAN matches the domain ID of the existing VSAN for this switch
- Obtain Cisco MDS switch connectivity information (IP address/console information), login credentials and access method (SSH/TELNET)

Procedure

1. Log in to the Cisco MDS switch.

2. To view VSANs, type: `show vsan`

3. To view the domain ID of the existing VSAN on the switch, type: `switch#show fcdomain domain-list`

4. To enter the global configuration mode and start the configuration, type: `switch# configure terminal`

5. To assign a domain ID, type: `switch# fcdomain domain domain_id static vsan vsan_id`
To assign a priority, type: `switch# fcdomain priority 2 vsan vsan_id`

Results
Setting the domain ID and priority ensures that the switch takes a role of a principal switch in that VSAN and that the domain ID in that VSAN does not get changed during a fabric merge process.

Reversing the procedure

Procedure

1 To enter the global configuration mode and start the configuration, type: `switch# configure terminal`

2 Type: `switch(config)# vsan database`

3 To delete a VSAN, type `no vsan vsan_id`

Enabling Fibre Channel interfaces

Use this procedure to enable Fibre Channel (FC) interfaces.

Before you begin

- Verify that the Cisco MDS switch is up and reachable through the console or management connection.
- Obtain the FC interfaces IDs
- Obtain Cisco MDS switch connectivity information (IP address/console information), login credentials and access method (SSH/TELNET)

Procedure

1 Log in to the Cisco MDS switch.

2 To start the configuration, type: `switch-A# config terminal`

3 To configure the interface, type: `switch-A(config)# interface fc interface_id`

4 To apply for a license, type: `switch-A(config-if)# port-license acquire`

5 To enable the interface, type: `switch-A(config-if)# no shutdown`

6 To verify that the interface is up, type: `show interface fc interface_id`
Reversing the procedure

Procedure

To disable the interface, type: `switch-A(config-if)# shutdown`

Moving licenses between Fibre Channel interfaces

Use this procedure to move licenses between Fibre Channel (FC) interfaces.

Before you begin

- Verify that the Cisco MDS switch is up and reachable through the console or management connection
- Obtain the FC interfaces IDs
- Obtain Cisco MDS switch connectivity information (IP address/console information), login credentials and access method (SSH/TELNET)

Procedure

1. Log in to the Cisco MDS switch.
2. To view the port licenses, type: `show port-license`
3. To start the configuration, type: `Switch-A# config terminal`
4. To configure the interface where license is being moved from, type: `Switch-A(config)# interface fc interface_id`
5. To disable the license on that interface, type: `Switch-A(config-if)# no port-license`
6. To exit, type: `Switch-A(config-if)# exit`
7. To configure the interface where the license is being moved to, type: `Switch-A(config)# interface fc interface_id`
8. To acquire the license on that interface, type: `Switch-A(config-if)# port-license acquire`
9. To end the configuration, type: `Switch-A(config-if)# end`
10. To verify that appropriate ports have enabled licenses, type: `show port-license`
Creating Fibre Channel aliases

Use this procedure to create Fibre Channel (FC) aliases.

Before you begin

- Verify that the Cisco MDS switch is up and reachable through the console or management connection
- Obtain:
  - Required port world wide name (PWWN) of the device
  - VSAN ID of the device
  - Cisco MDS switch connectivity information (IP address/console information), login credentials, and access method (SSH/TELNET)

Procedure

1. Log into the Cisco MDS switch.
2. To start the configuration, type: `switch-A# config terminal`
3. To configure the FC alias, type: `switch-A (config)# fcalias name alias_name vsan vsan_id`
4. To add the device to the FC alias, type: `switch-A (config-fcalias)# member pwnn device_pwnn`
5. To verify that the FC alias is configured, type: `show fcalias name alias_name`

Reversing the procedure

Procedure

1. To start the configuration, type: `switch-A# config terminal`
2. To disable the FC alias, type: `switch-A(config)# no fcalias name alias_name vsan vsan_id`
Creating Fibre Channel zones

Use this procedure to create a Fibre Channel (FC) zone.

Before you begin

Verify that the Cisco MDS switch is up and reachable through the console or management connection. Obtain:

- FC alias for members of the zone
- VSAN ID of the device
- Cisco MDS switch connectivity information (IP address/console information), login credentials, and access method (SSH/TELNET)

Procedure

1. Log into the Cisco MDS switch.
2. To start the configuration, type: `switch-A# config terminal`
3. To create the FC zone, type: `switch-A(config)# zone name zone_name vsan vsan_id`
4. To add the members to the FC zone, type: `switch-A(config-zone)# member fcalias fcalias_name`
5. To add additional members to the FC zone, type: `switch-A(config-zone)# member fcalias fcalias_name`
6. To commit the VSAN to the FC zone, type: `switch-A(config)# zone commit vsan vsan_id`
7. To exit, type: `switch-A(config-zone)# end`
8. To verify that the zone is configured, type: `switch-A(config)# show zone name zone_name`

Reversing the procedure

Procedure

1. To start the configuration, type: `switch-A# config terminal`
2. To delete the FC zone, type: `switch-A(config)# no zone name zone_name vsan vsan_id`
Creating modifying and activating zone sets

Use this procedure to create and activate zone sets.

Before you begin

- Verify that the Cisco MDS switch is up and reachable through the console or management connection
- Obtain:
  - Names of the zones to be added or removed
  - Name of the zone set to be modified or created
  - VSAN ID of the zone set
  - Cisco MDS switch connectivity information (IP address/console information), login credentials, and access method (SSH/TELNET)

Procedure

1. Log in to the Cisco MDS switch.
2. To start the configuration, type: `switch-A# config terminal`
3. To create or modify the zone set, type: `switch-A(config)# zoneset name zoneset_name vsan vsan_id`
4. To add members to the zone set, type: `switch-A(config-zone)# member zone_name`
5. To remove members from the zone set, type: `switch-A(config-zone)# no member zone_name`
6. To activate the zone set: `switch-A(config)# zoneset activate name zoneset_name vsan vsan_id`
7. To exit: `switch-A(config-zone)# end`
8. To verify that the zone is configured, type: `show zoneset name zoneset_name vsan vsan_id`
9. To verify the active zone set, type: `show zoneset active vsan vsan_id`

Creating Fibre Channel port channels

Use this procedure to create a Fibre Channel (FC) port channel.
Before you begin

- Verify that the Cisco MDS switch is up and reachable through the console or management connection
- Obtain:
  - Required FCI interface IDs of port channel members
  - The VSAN IDs of the interfaces
  - The Cisco MDS switch connectivity information (IP address/console information), login credentials, and access method (SSH/TELNET)

Procedure

1. Log into the Cisco MDS switch.
2. To start the configuration, type: `switch-A# config terminal`
3. To create the port channel interface, type:
   a. `switch-A(config)# interface port-channel port-channel_id`
   b. `switch-A(config-if)# channel mode active`
   c. `switch-A(config-if)# switchport mode F`
   d. `switch-A(config-if)# switchport rate-mode dedicated`
   e. `switch-A(config-if)# switchport trunk mode off`
4. To add port channel to the VSAN, type: `switch-A(config)# vsan vsan_id interface port-channel port-channel_id`
5. To add an FC interface to the port channel, type:
   a. `switch-A(config)# interface fc interface_id`
   b. `switch-A(config-if)# channel-group port-channel_id force`
6. To exit, type: `switch-A(config-zone)# end`
7. To verify that the port channel is configured, type: `switch-A(config)# show interface port-channel port-channel_id`
Reversing the procedure

Procedure

1. To start the configuration, type: `switch-A# config terminal`

2. To remove an FC interface from the port channel, type: `switch-A(config)# interface fcinterface_id`

3. Type: `switch-A(config-if)# no channel-group`

4. To remove a port channel, type: `switch-A(config)# no interface port-channel port-channel_id`
Managing storage resources

Logging into a storage array

Use this procedure to log into the storage array using EMC Unisphere for VMAX3.

Before you begin

- From the active directory (AD) account or local EMC Unisphere for VMAX3 account, ensure that there are proper audit trails for any changes made to the storage array
- Verify that you have the proper IP addresses of the storage management VMs
- Obtain the username and password for EMC Unisphere for VMAX3

Procedure

1. Use Remote Desk Protocol (RDP) to access the storage management VM using your AD/Windows credentials.
2. To launch EMC Unisphere for VMAX3, from your browser type: `https://host IP:8443`
3. Log in with user credentials.

Creating devices and pools

Use these procedures to create devices and pools in the storage array.

About this task

TDATs and pools are normally created by the bin file load.

VCE recommends using drives in multiples of RAID group sizes. Only create new virtual provisioning (VP) pools to support new application requirements.

Bare metal hosts require separate disk drives. The boot LUNs and data LUNs for bare metal cannot coexist with the same disk groups or VP pools used for VMware vSphere ESXi boot and VMware vSphere ESXi data volumes.

Bare metal applications require a dedicated storage pool.

EMC RecoverPoint Replica Journals and Replica Volumes must be placed in a dedicated disk group and VP pool. For example, for RAID 1/0 or RAID 6, add drives in multiples of eight. For RAID 5, add drives in multiples of four.

Before you begin

Verify that there are available drives in the storage array to create the TDATs and VP pools.
Procedure

1. Using the SYMCLI commands, create TDATS, TDEVS and pools.
2. Create a meta device.
3. Add TDATs to the pool.
4. Bind TDEVs to the pool.
5. To verify that the new pool was created, from EMC Unisphere, select Storage > Storage Configuration > Storage Pools.

What to do next
Creating TDATs, TDEVs, and pools (see page 89)

Related information
Deleting a virtual provisioning pool (see page 108)
Monitoring a virtual provisioning pool (see page 109)

Creating TDATs, TDEVs, and pools

Use this procedure to create TDATs, TDEVS and pools using SYMCLI commands or EMC Unisphere for VMAX.

Procedure

1. Log on to the storage management VM and select the storage array to create the storage pool.
2. Type the `symconfigure` command with the prepare flag: `symconfigure -sid xxx -cmd your_command prepare -nop`
3. If no errors occur, type: `symconfigure -sid xxx -cmd your_command commit -nop`
4. To create a TDAT (completed using the bin file load), type: `create dev count=8, attribute=datadev, size=240GB, emulation=fba, config=raid-5, data_member_count=3, disk_group=0`
5. To create a TDEV, type: `create dev count=8, size=240GB, emulation=fba, config=TDEV`
The three types of pools that you can create are:

- Enterprise flash drive (EFD) for high performance
- Fibre Channel (FC) for general purpose
- Serial advanced technology attachment (SATA) for archiving

To create an EFD, type: `create pool Prod-HP-01, type=thin, max_subs_percent=400`

To create an FC, type: `create pool Prod-GP-01, type=thin, max_subs_percent=400`

To create a SATA, type: `create pool Prod_AR-01, type=thin, max_subs_percent=400`

Related information

- Creating devices and pools (see page 88)
- Creating a meta device (see page 90)

### Creating a meta device

Use this procedure to create a meta device using the `symconfigure` SYMCLI command.

**Before you begin**

Verify that TDATs, TDEVs, and pools have already been created.

**Procedure**

1. To create a meta device, type: `symconfigure -sid xxx -file filename prepare -nop`

2. If no errors occur, type: `symconfigure -sid xxx -file filename commit -nop`
To add the commands for meta creation to a text file, type:

```
Form meta from dev 02d3 config=striped
Add dev 02d4 to meta 02d3
Add dev 02d5 to meta 02d3
Add dev 02d6 to meta 02d3
Add dev 02d7 to meta 02d3
Add dev 02d8 to meta 02d3
Add dev 02d9 to meta 02d3
Add dev 02da to meta 02d3
```

Related information

- Creating devices and pools (see page 88)
- Adding TDATs to a pool (see page 91)

### Adding TDATs to a pool

Use this procedure to add TDATs to the pool using SYMCLI commands.

**About this task**

This information is provided for informational purposes only. The bin file load applies all TDATs to VP pools.

**Procedure**

To add everything between the start and end, including the start/end devices, type:

```
add dev start:end to pool Prod_HP_01 type=thin,member_state=enable
add dev start:end to pool Prod_GP_01 type=thin,member_state=enable
add dev start:end to pool Prod_AR_01 type=thin,member_state=enable
```

Related information

- Creating devices and pools (see page 88)
- Binding TDEVs to a pool (see page 92)
**Binding TDEVs to a pool**

Use this procedure to bind TDEVs to the pool.

**About this task**

These commands bind an already existing TDEV to a VP pool.

**Procedure**

To bind TDEVs to the pool, type:

- `Bind tdev xxx to pool Prod_HP_01 preallocate size=20 GB`
- `Bind tdev xxx to pool Prod_AR_01 preallocate size=20 GB`
- `Bind tdev xxx to pool Prod_GP_01 preallocate size=20 GB`

**Related information**

[[Creating devices and pools](#) (see page 88)]

**SYMCLI commands for managing devices and pools**

This topic contains SYMCLI commands for managing devices and pools.

<table>
<thead>
<tr>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>List devices</td>
<td><code>symdev -sid xxx list -tdev</code></td>
</tr>
<tr>
<td>View LUN and the disk group details</td>
<td><code>symdev -sid xxx show lunid</code></td>
</tr>
<tr>
<td>View data devices from disk group 2 (FC)</td>
<td><code>symdev -sid xxx list -disk_group 2 -datadevs</code></td>
</tr>
<tr>
<td>List pools</td>
<td><code>symcfg list -pool -thin symcfg show -pool pool name -thin -mb</code></td>
</tr>
<tr>
<td>View details</td>
<td><code>symcfg -sid xxx -pool list -v</code></td>
</tr>
<tr>
<td>View data devices and pool status</td>
<td><code>symcfg -sid xxx -datadev list -v</code></td>
</tr>
<tr>
<td>View thin pool and enabled devices size</td>
<td><code>symcfg -sid xxx show -pool Prod_GP_01 -thin -detail -gb</code></td>
</tr>
<tr>
<td>View thin devices and bound pools status</td>
<td><code>symcfg -sid xxx -tdev list</code></td>
</tr>
</tbody>
</table>
Creating a VSAN

Use this procedure to create a VSAN for the Cisco Nexus 5548UP Switch.

Before you begin

- Verify that the switch is up and reachable through the console or management connection
- Obtain:
  - Required VSANs, names, and Fibre Channel (FC) interfaces to be assigned to the VSANs
  - Cisco MDS switch connectivity information (IP address/console information), login credentials and access method (SSH/TELNET)
- Name the VSANs to identify usage (for example, for VSAN 10: SAN_A)

For more information, see the Cisco Nexus 5500 Series NX-OS SAN Switching Configuration Guide

Procedure

1. Log in to the switch.
2. To view VSANs, type: `show vsan vsan 1 informationname:VSAN0001 state:activeinteroperability mode:defaultloadbalancing:src-id/dst-id/oxidoperational state:down`
3. To start the configuration, type: `config terminal`
4. To configure the database for VSAN, type: `(config)# vsan database`
5. To specify the VSAN being created, type: `(config-vsan-db)# vsan vsan_id`
6. To assign an FC interface to the VSAN, type: `(config-vsan-db)# vsan vsan_id interface fcinterface_id`
7. To view the VSANs, type: `show vsan`

Reversing the procedure

Procedure

To delete the zone, type: `switch-A(config)# no zone name zone_name vsan vsan_id`
Creating Fibre Channel interfaces

Use this procedure to enable Fibre Channel (FC) interfaces.

Before you begin

- Verify that the Cisco Nexus switch is up and reachable through the console or management connection
- Obtain:
  - Required FC interfaces IDs
  - Cisco Nexus switch connectivity information (IP address/console information), login credentials and access method (SSH/TELNET)

Procedure

1. Log into the Cisco Nexus switch.

2. To start the configuration, type: `switch-A# config terminal`

3. To configure the interface, type: `switch-A(config)# interface fcinterface_id`

4. To enable the interface, type: `switch-A(config-if)# no shutdown`

5. To verify that the interface is up, type: `switch-A# show interface fcinterface_id`

Reversing the procedure

Procedure

To disable the interface, type: `switch-A(config-if)# shutdown`

Creating boot and data LUNs

For information about configuring Symmetrix storage, refer the Storage Management chapter of the *EMC Unisphere for VMAX Product Guide*.

Related information

[EMC Unisphere for VMAX Product Guide](#)
Host front-end connectivity standards for EMC Symmetrix VMAX 10K

Each engine is connected to each SAN fabric. Odd directors are connected to SAN A and even directors are connected to SAN B.

EMC Ionix UIM should be limited to the designated cluster EMC Symmetrix FA ports. Disable the non-host cluster ports on the Cisco MDS 9148 Switches and place them in a separate VSAN. Ports E1, F1, H0, and H1 on directors 1 through 4 are reserved as follows and should not be used:

- E1 ports are reserved for X-Blade connectivity.
- F1 ports are reserved for backup or migration connectivity.
- H0 and H1 ports are reserved for EMC Symmetrix Remote Data Facility (SRDF) and EMC RecoverPoint connectivity.

Note: AMP hosts are zoned to front end ports 1g1 and 2g1 (single-engine) or 2g1 and 3g1 (more than one engine).

As a best practice, if beginning with two or more engines, assign a cluster across two engines, one port per director for a total of four ports. For example, assign cluster 1 hosts to port E0 on directors 1, 2, 3, and 4 in a two-engine configuration:

- Cluster 2 assigned G0
- Cluster 3 assigned F0
- Cluster 4 assigned G1
- Cluster 5 assigned E0
- Cluster 6 assigned G0

The following table identifies the EMC Symmetrix FA ports used for front end host connectivity:

<table>
<thead>
<tr>
<th>Fabric B</th>
<th>Fabric A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Engine 1</strong></td>
<td><strong>Director 2</strong></td>
</tr>
<tr>
<td>Engine 1</td>
<td>Director 2</td>
</tr>
<tr>
<td>F1</td>
<td>MIG/BRS</td>
</tr>
<tr>
<td>F0</td>
<td>C2</td>
</tr>
<tr>
<td>E1</td>
<td>XB Slot 0 P1</td>
</tr>
<tr>
<td>E0</td>
<td>C1</td>
</tr>
</tbody>
</table>

| **Engine 2** | **Director 4** | **Director 3** |
| Engine 2 | Director 4 | Director 3 |
| F1 | MIG/BRS | H1 | REP/brs | F1 | MIG/BRS | H1 | REP/brs |
| F0 | C4 | H0 | C4 | F0 | C4 | H0 |
### Fabric B

<table>
<thead>
<tr>
<th></th>
<th>XB Slot 0 P1</th>
<th>Fabric A</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>G1 C4</td>
<td>E1</td>
</tr>
<tr>
<td>E0</td>
<td>C3 G0 C3</td>
<td></td>
</tr>
</tbody>
</table>

### Engine 3

<table>
<thead>
<tr>
<th>Director 6</th>
<th>Director 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1 H1</td>
<td>F1 H1</td>
</tr>
<tr>
<td>F0 C6 H0 C6</td>
<td>F0 C6 H0 C6</td>
</tr>
<tr>
<td>E1 G1</td>
<td>E1 G1</td>
</tr>
<tr>
<td>E0 C5 G0 C5</td>
<td>E0 C5 G0 C5</td>
</tr>
</tbody>
</table>

### Engine 4

<table>
<thead>
<tr>
<th>Director 8</th>
<th>Director 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1 H1</td>
<td>F1 H1</td>
</tr>
<tr>
<td>F0 C8 H0 C8</td>
<td>F0 C8 H0 C8</td>
</tr>
<tr>
<td>E1 G1</td>
<td>E1 G1</td>
</tr>
<tr>
<td>E0 C7 G0 C7</td>
<td>E0 C7 G0 C7</td>
</tr>
</tbody>
</table>

### X-Blade notes

- X-Blade ports and designated front-end ports are placed in a separate VSAN (for example, 20/21).
- All X-Blades are zoned to the same front end ports on the array.
- As a best practice, use a 4:1 ratio of X-Blades to FA ports.
- In a single-engine configuration, all X-Blades with slot 0 port 0 are zoned to FE 1E1 and all X-Blades with slot 0 port 2 are zoned to FE 2E1.
- In configurations with more than two engines, you can expand the X-Blades as necessary.

The following example shows a two-engine configuration:

- X-Blades 2/4/6/8 slot 0 port 0 WWPNs are zoned to Symmetrix FE 1E1
- X-Blades 2/4/6/8 slot 0 port 1 WWPNs are zoned to Symmetrix FE 4E1
- X-Blades 3/5/7/9 slot 0 port 0 are zoned to FE 3E1
- X-Blades 3/5/7/9 slot 0 port 1 are zoned to FE 2E1
- For VMware vSphere ESX clusters, if you have a single engine or two-engine EMC Symmetrix VMAX 10K, place odd clusters across C1/C3 designated ports and even clusters on C2/C4 ports.
Bare metal notes

- There is no segmentation of bare metal and VMware vSphere ESX blades from a SAN configuration perspective.
- With a bare metal configuration, there is no dedicated VSAN, no dedicated FI ports, and no dedicated FA ports.
- Apply the WWPN to Cisco UCS host mapping as if the bare metal hosts were a cluster.

Required FA port settings

To develop a bin file request, the following FA port settings are required:

- Common Serial Number (C)
- SCSI 3 (SC3)
- SPC 2 (SPC2)
- SCSI Support 1 (OS2007)
- Init Point to Point (PP)
- Unique WWN (UWN)
- Access Logix (ACLX)
- Auto Negotiate (EAN)

Host front-end connectivity standards for EMC Symmetrix VMAX 20K and 40K

Eight hosts/eight engines

Engine 8

<table>
<thead>
<tr>
<th>Director 16 (Even)</th>
<th>Director 15 (Odd)</th>
<th>Director 14 (Even)</th>
<th>Director 13 (Odd)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
<td>SIB-1B</td>
<td>SIB-1A</td>
</tr>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
<td>SIB-1B</td>
<td>SIB-1A</td>
</tr>
<tr>
<td>E0</td>
<td>E1</td>
<td>F0</td>
<td>Oracle 5</td>
</tr>
</tbody>
</table>
### Engine 7

<table>
<thead>
<tr>
<th>Director 14 (Even)</th>
<th>Director 13 (Odd)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
</tr>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E0</th>
<th>E1</th>
<th>F0</th>
<th>F1</th>
<th>G0</th>
<th>G1</th>
<th>H0</th>
<th>H1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle 5</td>
<td>Oracle 6</td>
<td>Oracle 7</td>
<td>Oracle 8</td>
<td>Oracle 9</td>
<td>Oracle 10</td>
<td>Oracle 11</td>
<td>Oracle 12</td>
</tr>
</tbody>
</table>

### Engine 6

<table>
<thead>
<tr>
<th>Director 12 (Even)</th>
<th>Director 11 (Odd)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
</tr>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E0</th>
<th>E1</th>
<th>F0</th>
<th>F1</th>
<th>G0</th>
<th>G1</th>
<th>H0</th>
<th>H1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle 1</td>
<td>Oracle 2</td>
<td>Oracle 3</td>
<td>Oracle 4</td>
<td>Oracle 5</td>
<td>Oracle 6</td>
<td>Oracle 7</td>
<td>Oracle 8</td>
</tr>
</tbody>
</table>

### Engine 5

<table>
<thead>
<tr>
<th>Director 10 (Even)</th>
<th>Director 9 (Odd)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
</tr>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E0</th>
<th>E1</th>
<th>F0</th>
<th>F1</th>
<th>G0</th>
<th>G1</th>
<th>H0</th>
<th>H1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle 1</td>
<td>BRS</td>
<td>Oracle 2</td>
<td>X-Blade</td>
<td>Oracle 3</td>
<td>App SVR/SE host</td>
<td>REP</td>
<td>MIG</td>
</tr>
</tbody>
</table>

### Engine 4

<table>
<thead>
<tr>
<th>Director 8 (Even)</th>
<th>Director 7 (Odd)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
</tr>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E0</th>
<th>E1</th>
<th>F0</th>
<th>F1</th>
<th>G0</th>
<th>G1</th>
<th>H0</th>
<th>H1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle 4</td>
<td>BRS</td>
<td>Oracle 2</td>
<td>X-Blade</td>
<td>Oracle 3</td>
<td>App SVR/SE host</td>
<td>REP</td>
<td>MIG</td>
</tr>
</tbody>
</table>
### Engine 3

<table>
<thead>
<tr>
<th>Director 6 (Even)</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
<td>SIB-1B</td>
<td>SIB-1A</td>
<td>SIB-2A</td>
<td>SIB-2B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Director 5 (Odd)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
<td>SIB-1B</td>
<td>SIB-1A</td>
<td>SIB-2A</td>
<td>SIB-2B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Director 6 (Even)</td>
<td>E0</td>
<td>E1</td>
<td>F0</td>
<td>F1</td>
<td>G0</td>
<td>G1</td>
<td>H0</td>
<td>H1</td>
<td></td>
</tr>
<tr>
<td>Director 5 (Odd)</td>
<td>E0</td>
<td>E1</td>
<td>F0</td>
<td>F1</td>
<td>G0</td>
<td>G1</td>
<td>H0</td>
<td>H1</td>
<td></td>
</tr>
</tbody>
</table>

### Engine 2

<table>
<thead>
<tr>
<th>Director 4 (Even)</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
<td>SIB-1B</td>
<td>SIB-1A</td>
<td>SIB-2A</td>
<td>SIB-2B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Director 3 (Odd)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
<td>SIB-1B</td>
<td>SIB-1A</td>
<td>SIB-2A</td>
<td>SIB-2B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Director 4 (Even)</td>
<td>E0</td>
<td>E1</td>
<td>F0</td>
<td>F1</td>
<td>G0</td>
<td>G1</td>
<td>H0</td>
<td>H1</td>
<td></td>
</tr>
<tr>
<td>Director 3 (Odd)</td>
<td>E0</td>
<td>E1</td>
<td>F0</td>
<td>F1</td>
<td>G0</td>
<td>G1</td>
<td>H0</td>
<td>H1</td>
<td></td>
</tr>
</tbody>
</table>

### Engine 1

<table>
<thead>
<tr>
<th>Director 2 (Even)</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
<td>SIB-1B</td>
<td>SIB-1A</td>
<td>SIB-2A</td>
<td>SIB-2B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Director 1 (Odd)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
<td>SIB-1B</td>
<td>SIB-1A</td>
<td>SIB-2A</td>
<td>SIB-2B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Director 2 (Even)</td>
<td>E0</td>
<td>E1</td>
<td>F0</td>
<td>F1</td>
<td>G0</td>
<td>G1</td>
<td>H0</td>
<td>H1</td>
<td></td>
</tr>
<tr>
<td>Director 1 (Odd)</td>
<td>E0</td>
<td>E1</td>
<td>F0</td>
<td>F1</td>
<td>G0</td>
<td>G1</td>
<td>H0</td>
<td>H1</td>
<td></td>
</tr>
</tbody>
</table>

### Four hosts/four engines

### Engine 3

<table>
<thead>
<tr>
<th>Director 6 (Even)</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
<td>SIB-1B</td>
<td>SIB-1A</td>
<td>SIB-2A</td>
<td>SIB-2B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Director 5 (Odd)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
<td>SIB-1B</td>
<td>SIB-1A</td>
<td>SIB-2A</td>
<td>SIB-2B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Even Director 6</td>
<td>E0</td>
<td>E1</td>
<td>F0</td>
<td>F1</td>
<td>G0</td>
<td>G1</td>
<td>H0</td>
<td>H1</td>
<td></td>
</tr>
<tr>
<td>Odd Director 5</td>
<td>E0</td>
<td>E1</td>
<td>F0</td>
<td>F1</td>
<td>G0</td>
<td>G1</td>
<td>H0</td>
<td>H1</td>
<td></td>
</tr>
</tbody>
</table>
Engine 4

<table>
<thead>
<tr>
<th>Director 8 (Even)</th>
<th>Director 7 (Odd)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
</tr>
<tr>
<td>F0 Oracle 4</td>
<td>E1 BRS</td>
</tr>
<tr>
<td>E1 Oracle 2</td>
<td>F0 Oracle 3</td>
</tr>
<tr>
<td>F1 X-Blade</td>
<td>G0 Oracle 3</td>
</tr>
<tr>
<td>G1 App SVR/SE host</td>
<td>H0 REP</td>
</tr>
<tr>
<td>H1 REP</td>
<td>E0 Oracle 1</td>
</tr>
<tr>
<td>SIB-1B</td>
<td>E1 BRS</td>
</tr>
<tr>
<td>SIB-1A</td>
<td>F0 Oracle 4</td>
</tr>
<tr>
<td>SIB-2A</td>
<td>F1 X-Blade</td>
</tr>
<tr>
<td>SIB-28</td>
<td>G0 Oracle 3</td>
</tr>
<tr>
<td></td>
<td>G1 App SVR/SE host</td>
</tr>
</tbody>
</table>

Engine 5

<table>
<thead>
<tr>
<th>Director 10 (Even)</th>
<th>Director 9 (Odd)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
</tr>
<tr>
<td>F0 Oracle 1</td>
<td>E1 BRS</td>
</tr>
<tr>
<td>E1 Oracle 2</td>
<td>F0 Oracle 3</td>
</tr>
<tr>
<td>F1 X-Blade</td>
<td>G0 Oracle 3</td>
</tr>
<tr>
<td>G1 App SVR/SE host</td>
<td>H0 REP</td>
</tr>
<tr>
<td>H1 REP</td>
<td>E0 Oracle 1</td>
</tr>
<tr>
<td>SIB-1B</td>
<td>E1 BRS</td>
</tr>
<tr>
<td>SIB-1A</td>
<td>F0 Oracle 4</td>
</tr>
<tr>
<td>SIB-2A</td>
<td>F1 X-Blade</td>
</tr>
<tr>
<td>SIB-28</td>
<td>G0 Oracle 3</td>
</tr>
<tr>
<td></td>
<td>G1 App SVR/SE host</td>
</tr>
</tbody>
</table>

Engine 6

<table>
<thead>
<tr>
<th>Director 12 (Even)</th>
<th>Director 11 (Odd)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM A0-B1</td>
<td>IOM C0-D1</td>
</tr>
<tr>
<td>F0 Oracle 1</td>
<td>E1 BRS</td>
</tr>
<tr>
<td>E1 Oracle 2</td>
<td>F0 Oracle 3</td>
</tr>
<tr>
<td>F1 X-Blade</td>
<td>G0 Oracle 3</td>
</tr>
<tr>
<td>G1 Oracle 4</td>
<td>H0 Oracle 4</td>
</tr>
<tr>
<td>H1</td>
<td>E0 Oracle 1</td>
</tr>
<tr>
<td></td>
<td>E1 BRS</td>
</tr>
<tr>
<td></td>
<td>F0 Oracle 4</td>
</tr>
<tr>
<td></td>
<td>F1 X-Blade</td>
</tr>
<tr>
<td></td>
<td>G0 Oracle 3</td>
</tr>
<tr>
<td></td>
<td>G1 Oracle 4</td>
</tr>
<tr>
<td></td>
<td>H0 REP</td>
</tr>
</tbody>
</table>

Disk group standards

There is a minimum of three disk groups, depending upon the workload configuration that is selected. Refer to Storage disk group configuration options (see page 102) to understand the different disk groups used based on the configuration purchased.

You might need additional disk groups to support bare metal and network attached storage (NAS), depending on the configuration.

Bare metal and RecoverPoint Journal disks are in separate disk groups no matter which workload configuration is selected.

Disk groups should typically contain a number of disks that can be divisible by 4 or 8 (RAID-1, RAID-5 (3+1) and (7+1), RAID-6 (6+2) and (14+2)).
When building devices (TDATs, symdevice, etc.), EMC lays out the hyper volumes or splits across all disks in the group. EMC also maximizes the size and number of the hyper volumes per disk to best use the disks (less wasted space), with minimum splits per drive.

Hyper volumes are combined to provide a protection scheme. TDATs in a RAID-5(3+1) are shown below:
Storage disk group configuration options

Two options are available from which customers can choose.

The array configuration and bin file requirements change depending on which option is selected:

**Segregated workload configuration**
In this configuration, drives are separated into disk groups based on their intended use. This separation allows dedication of drive spindles to particular applications, which provides better performance to the applications. Each disk group is then used to configure one or more VP pools.

**Mixed workload configuration**
In this configuration, the total number of disk groups is reduced. Each disk group supports multiple VP pools. This arrangement improves drive utilization efficiency by supporting multiple applications from the same set of drive spindles.

**Note:** Using the mixed workload configuration requires that EMC FAST VP be configured in order to provide the most optimal usage of disk.

Bare metal configurations always require separate disk groups, regardless of which configuration is chosen by the customer.

Before beginning the bin file request, confirm which option has been selected by the customer. The customer’s choice is detailed in the Logical Build notes section of the BOM.
Disk group and VP pools: segregated workload configuration

The customer might require specific disk groups and VP pools to be configured for their application. This information should be identified prior to submitting the bin file request.

However, the VMware vSphere ESXi boot LUNs disk group, the Bare Metal disk groups, the NAS data disk groups, and the RP Journal disk group must ALWAYS be configured in separate disk groups. They must never be combined in the segregated workload configuration.

<table>
<thead>
<tr>
<th>Disk Group</th>
<th>Base/Optional</th>
<th>VP Pool</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot_luns</td>
<td>Base</td>
<td>esx-boot</td>
<td>esx_boot</td>
</tr>
<tr>
<td>boot_luns</td>
<td>Optional</td>
<td>NAS-control</td>
<td>NAS control volumes configured from the boot LUNs disk group</td>
</tr>
<tr>
<td>flash_hp</td>
<td>Base</td>
<td>Prod-HP-Rxx</td>
<td>EFD disk group</td>
</tr>
<tr>
<td>fc_gp</td>
<td>Base</td>
<td>Prod-GP-Rxx</td>
<td>FC disk group</td>
</tr>
<tr>
<td>sata_ar</td>
<td>Base</td>
<td>Prod-AR-Rxx</td>
<td>SATA disk group</td>
</tr>
<tr>
<td>boot_baremetal</td>
<td>Optional</td>
<td>BM-boot</td>
<td>Bare metal boot LUN</td>
</tr>
<tr>
<td>flash_baremetal</td>
<td>Optional</td>
<td>BM-HP-Rxx</td>
<td>EFD for Bare metal</td>
</tr>
<tr>
<td>fc_baremetal</td>
<td>Optional</td>
<td>BM-GP-Rxx</td>
<td>FC for Bare metal</td>
</tr>
<tr>
<td>sata_baremetal</td>
<td>Optional</td>
<td>BM-AR-Rxx</td>
<td>SATA for Bare metal</td>
</tr>
<tr>
<td>flash_nas</td>
<td>Optional</td>
<td>NAS-HP-Rxx</td>
<td>EFD NAS data</td>
</tr>
<tr>
<td>fc_nas</td>
<td>Optional</td>
<td>NAS-GP-Rxx</td>
<td>FC NAS data</td>
</tr>
<tr>
<td>sata_nas</td>
<td>Optional</td>
<td>NAS-AR-Rxx</td>
<td>SATA NAS data</td>
</tr>
<tr>
<td>RP_journal</td>
<td>Optional</td>
<td>RP_Journal</td>
<td>RecoverPoint Journal</td>
</tr>
</tbody>
</table>

Disk group and VP pools: mixed workload configuration

The customer might require specific disk groups and VP pools to be configured for their application. This information should be identified prior to submitting the bin file request.

However, the esx-boot VP pool, the bare metal VP pools, the NAS VP pools, and RP-Journal VP pool must ALWAYS be configured in separate VP pools. They must never be combined in the mixed workload configuration.

<table>
<thead>
<tr>
<th>Disk Group</th>
<th>Base/Optional</th>
<th>VP Pool</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>fc_gp</td>
<td>Base</td>
<td>Prod-GP-Rxx</td>
<td>FC disk group</td>
</tr>
<tr>
<td>fc_gp</td>
<td>Base</td>
<td>esx-boot</td>
<td>esx_boot</td>
</tr>
<tr>
<td>fc_gp</td>
<td>Optional</td>
<td>NAS-control</td>
<td>NAS control volumes</td>
</tr>
</tbody>
</table>
### Disk Group Table

<table>
<thead>
<tr>
<th>Disk Group</th>
<th>Base/Optional</th>
<th>VP Pool</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>fc_gp</td>
<td>Optional</td>
<td>NAS-GP-Rxx</td>
<td>FC NAS data</td>
</tr>
<tr>
<td>flash_hp</td>
<td>Base</td>
<td>Prod-HP-Rxx</td>
<td>EFD disk group</td>
</tr>
<tr>
<td>flash_hp</td>
<td>Optional</td>
<td>NAS-HP-Rxx</td>
<td>EFD NAS data</td>
</tr>
<tr>
<td>sata_ar</td>
<td>Base</td>
<td>Prod-AR-Rxx</td>
<td>SATA disk group</td>
</tr>
<tr>
<td>sata_ar</td>
<td>Optional</td>
<td>NAS-AR-Rxx</td>
<td>SATA NAS data</td>
</tr>
<tr>
<td>flash_baremetal</td>
<td>Optional</td>
<td>BM-HP-Rxx</td>
<td>EFD for Bare metal</td>
</tr>
<tr>
<td>fc_baremetal</td>
<td>Optional</td>
<td>BM-boot</td>
<td>Bare metal boot LUN</td>
</tr>
<tr>
<td>fc_baremetal</td>
<td>Optional</td>
<td>BM-GP-Rxx</td>
<td>FC for Bare metal</td>
</tr>
<tr>
<td>sata_baremetal</td>
<td>Optional</td>
<td>BM-AR-Rxx</td>
<td>SATA for Bare metal</td>
</tr>
<tr>
<td>RP_journal</td>
<td>Optional</td>
<td>RP_Journal</td>
<td>RecoverPoint Journal</td>
</tr>
</tbody>
</table>

### Meta volume standards

The maximum LUN size on an EMC Symmetrix VMAX 10K/20K/40K is 240GB.

The EMC best practice is to create meta devices with four or eight members; therefore: 8 * 240GB = 1920GB (roughly 2TB).

The VCE best practice is to create a striped meta volume.

### VP pool standards

All devices must be placed in VP pools on EMC Symmetrix VMAX 10K.

All virtual devices must be placed in VP pools on EMC Symmetrix VMAX 20K/40K.

VP pool oversubscription ratio of 3:1 is the EMC Symmetrix VMAX 10K maximum.

There are a minimum of four VP pools configured:

- Esxi-boot for boot LUNs
- Prod-HP-Rxx for EFD devices
- Prod-GP-Rxx for FC devices
- Prod-AR-Rxx for SATA devices

VMware vSphere ESXi Boot volumes must be placed in a separate dedicated VP pool.
NAS control volumes require a separate dedicated VP pool. NAS data volumes should be placed in separate dedicated VP pools.

Bare metal boot volumes must be placed in a separate dedicated VP pool.

Bare metal data volumes must be placed in separate dedicated VP pools.

For RecoverPoint implementations, an additional pool will be created called RP-Journal.

Refer to the *EMC Symmetrix VMAX 10K/20K/40K Bin Config Template* for pool naming conventions.

TDATs (datadevs) are assigned to a virtual pool.

Each TDAT must be of the same protection type and technology.

TDEVs are then created. TDEVs are actual devices that are in turn presented to the servers as storage.

TDEVs do not have any real storage behind them until they are bound to a virtual pool. They are pre-allocated 5% to 10% of the overall size during the bind process (refer to SYMCLI commands).

Again, the maximum size of any LUN is 240GB. Meta devices must be utilized to create larger devices.

TDEV meta devices must be created BEFORE they are bound to a virtual pool.

Once a TDEV is bound to a pool, its data is distributed across the TDATs that make up the virtual pool (represented by the slices 1-6). Note that this is an example and not necessarily how it would get laid out in the pool:
Boot LUN standards

Each VMware vSphere ESXi server and/or bare metal blade boots from a SAN-attached boot drive presented from the EMC Symmetrix array. The boot LUNs have the following characteristics:

- The boot drives are thin devices with pre-allocated capacity of a full device on the EMC VMAX 10K and are thick devices on the EMC VMAX 20K/40K.
- Boot drives are 20GB TDEVs - ESXi.
  
  Bare metal boot LUNs might be a different size depending on operating system requirements.
- Boot drive TDEVs are configured from the VMware vSphere ESX-boot VP pool for VMware vSphere ESXi hosts or BM-boot VP pool for bare metal hosts.

Data drive standards

EMC VMAX 10K

Data devices are thin devices (TDEV), but can be fully pre-allocated or partially pre-allocated depending on the customer requirements. The default is 5% to 10% pre-allocated capacity. Do not create TDEV
volumes larger than 1920 GB. TDEV volumes that exceed the maximum can result in a TDEV too large for pre-VMware vSphere ESXi 5.x.

**Note:** VCE standard is still a 2 TB maximum (1920 GB in the case of EMC Symmetrix) until VCE no longer supports versions of VMware prior to VMware vSphere ESXi 5.x as part of initial deployments.

**EMC VMAX 20K/40K**

Data devices can be thick or thin devices as required by the customer. Thin devices (TDEV), can be fully pre-allocated or partially pre-allocated depending on the customer requirements. The default is 5% to 10% pre-allocated capacity.

Do not create DEV or TDEV volumes larger than 1920 GB. TDEV volumes that exceed the maximum can result in a TDEV too large for pre-VMware ESXi 5.x.

**Note:** The VCE standard is a 2 TB maximum (1920 GB in the case of EMC Symmetrix), until VCE no longer supports versions of VMware prior to VMware vSphere ESXi 5.x as part of initial deployments.

**Hot spare drive standards**

**EMC Symmetrix VMAX 20K**

The hot spare drive standard for the EMC Symmetrix VMAX 20K is two spares per 100 drives per drive type with a minimum of eight spares per system.

Flash sparing rules are as follows:

- If there are fewer than 33 flash drives of a given type, use one flash drive spare per flash drive type.
- If there are more than 32 flash drives of a given type, use two flash drive spares per 100 flash drives for each flash drive type.
- Enterprise Flash Drives (EFD) do not count toward the minimum of eight spares per system.

**EMC Symmetrix VMAX 10K**

EMC determines the rules for the quantities and types of spares after careful analysis of field data. To provide the best possible protection, configure spare drives on every loop and for every drive type of data drive in the loop.

Use the following guidelines:

- Use two spares per 100 drives per drive type with a minimum of four spares per system.
• Flash sparing rules:
  — If there are fewer than 33 flash drives of a given type, use one flash drive spare per flash drive type.
  — If there are more than 32 flash drives of a given type, use two flash drive spares per 100 flash drives for each flash drive type.
• Enterprise Flash Drives (EFD) do not count toward the minimum of four spares per system.

Deleting a virtual provisioning pool

Use this procedure to delete a virtual provisioning (VP) pool using EMC Unisphere for VMAX.

About this task
Available storage is removed from the host allocation when the pool is deleted.

Before you begin
Obtain:
• Storage devices in the storage pool that have been removed from storage groups
• Members of the storage pool

Procedure

1 Log on to the EMC Unisphere for VMAX management tool.
2 Select Storage > Thin Pools to open the Thin Pools list view.
3 Unbind all thin devices from the storage pool as follows:
   a Select the thin pool and click View Details to open the thin pool’s details view.
   b In Related Objects, click Bound Volumes to open the Bound Volumes for Thin Pool view.
   c To unbind members, select them and click Unbind.
   d Click OK in the confirmation message.
4 Disable all pool members as follows:
   a Select the thin pool and click View Details to open the thin pool’s details view.
   b In Related Objects, click Data Volumes to open the Data Volumes for Thin Pool view.
   c To disable members, select them and click Disable.
   d Click OK in the confirmation message.
5 Remove pool members as follows:
   a In the Data Volumes for Thin Pool view, select all pool members and click Remove.
   b Click OK in the confirmation message

6 Delete the device pool as follows:
   a Select the storage pool and click Delete.
   b Click OK in the confirmation message.

7 To verify that the pool was deleted, list the available pools as follows:
   a To view a list of pools, type: symcfg list -pool -thin
   b Type: symcfg show -pool pool_name -thin -mb

Related information

Monitoring a virtual provisioning pool (see page 109)
Creating devices and pools (see page 88)

Expanding a storage pool

Procedure

If new disk drives are purchased to support the expansion of a VP pool, ensure that EMC includes this expansion in the new bin file load.

Monitoring a virtual provisioning pool

Use this procedure to monitor pools in a storage array using EMC Unisphere for VMAX.

About this task
Monitoring the virtual provisioning (VP) pool use helps to ensure that the Vblock System applications have available disk space.

Before you begin
Create a storage pool.

Procedure

1 Log into Unisphere for VMAX.
2 Select the VP pool.
3 Click Properties > View Details.

Related information

Deleting a virtual provisioning pool (see page 108)
Creating devices and pools (see page 88)

Managing licenses

Use this procedure to apply licenses to the EMC Symmetrix Array for the Vblock System using EMC Unisphere for VMAX.

Procedure

1 Select System > Settings > Electronic Licenses.
2 For EMC Symmetrix-based licenses, perform the following:
   a Click Symmetrix Entitlements to open the Symmetrix Entitlements list view.
   b Click Get File to open the EMC Powerlink website.
   c Follow the instructions on the website to obtain new license files (by downloading or through email). Be sure to download or copy the license file to a location on the SMAS server.
   d Click Load File to open the Load License File dialog box.
   e Click Browse and select the license file.
   f Click OK to load the license file onto the EMC Symmetrix system.
3 For host-based licenses, perform the following:
   a Click Solutions Enabler to open the Solutions Enabler License Key list view.
   b Click Load Key to open the Load License Key dialog box.
   c Type the license key.
   d Click Apply to load additional license keys.
   e Click OK when done.
Managing EMC Symmetrix storage provisioning

On the EMC Symmetrix Enginuity 5876, auto-provisioning groups are the exclusive mechanism for storage provisioning. Auto-provisioning is implemented using the `symaccess` command with Solutions Enabler 7.0 and later, or using EMC Unisphere for VMAX.

The fundamental concept of auto-provisioning groups is the logical grouping of related objects and the creation of a view that associates the related groups together.

Creating an initiator group

Follow this procedure to create initiator groups (hosts) using EMC Unisphere for VMAX.

About this task
To create initiator groups (hosts) using EMC Unisphere for VMAX, use the **Create Host** wizard under **Host Management**.

Procedure

1. Select the EMC Symmetrix storage system.
2. To open the **Initiator Groups** list view, select **Hosts** > **Initiator Groups**.
3. To view details, select an initiator group and click **View Details**.
4. To open the **Create Host** wizard, click **Create**.
5. Select the EMC Symmetrix system on which to create the group.
6. Type a name for the host (name for the initiator group).
7. Select an initiator or initiator group to associate with the host and click **Add**. Repeat this step for each initiator/group you want associate with the host. Initiators can only belong to one initiator group at a time; therefore, any initiators that do not appear in the list are already part of a group.

   **Note:** You can filter the list by starting to type the name. In addition, you can also use an asterisk as a wildcard.

8. Click **Finish** to create the initiator group or **Show Advanced** to continue setting the advanced options.

Related information

- [Modifying an initiator group](#) (see page 112)
- [Deleting an initiator group](#) (see page 113)
- [EMC Unisphere for VMAX Online Help](#)
Modifying an initiator group

Use this procedure to modify an initiator group using EMC Unisphere for VMAX from the Initiator Groups list view.

About this task

There are two methods for modifying an initiator group. You can modify from the Initiator Groups list view or from the Host Management wizard, located in the Common Tasks panel.

Procedure

1. From the Initiator Group view, select the EMC Symmetrix storage system.
2. Select Hosts > Initiator Groups.
3. From the Initiator Groups list, select the initiator group and click View Details.
4. From the Details view, to change the name of the initiator group, highlight the name in the Properties panel, and type a new name over it.
5. To override the port attributes, perform the following:
   a. Click Set Flags. The Set Initiator Group Flags dialog box opens.
   b. Optional: Select an initiator group whose flag settings you want to copy.
   c. Optional: Modify any of the attributes. To modify an attribute:
      i. Select the corresponding Override option. The Enable option is enabled.
      ii. Enable (select) or disable (clear) the flag.
   d. Optional: Select Consistent LUNs to specify that LUN values for the initiator group must be kept consistent for all volumes within each masking view of which this initiator group is part. When set, any masking operation involving this initiator group is rejected if it would result in inconsistent LUN values. When not set, the Symmetrix system will attempt to keep LUN values consistent, but will deviate from consistency if LUN conflicts occur during masking operations.
   e. Click OK. The Set Initiator Group Flags dialog box closes.
6. Click Apply.

Related information

Creating an initiator group (see page 111)
Deleting an initiator group (see page 113)
Modifying an initiator group from the Host Management wizard

Use this procedure to modify an initiator group using EMC Unisphere for VMAX from the Host Management wizard.

Procedure

1. From the Host Management wizard, in the Common Task panel, click Manage Host.
2. Select the EMC Symmetrix system on which the group is defined.
3. Select the Host (name for the initiator group).
4. Click Next.
5. Perform either of the following:
   - To add an initiator or initiator group, select one and click Add.
   - To remove an initiator or initiator group, select one and click Remove.
6. Click Finish to create the initiator group or Show Advanced to continue setting the advanced options.

Related information

Deleting an initiator group

Use this procedure to delete a host or initiator group using EMC Unisphere for VMAX.

About this task
You cannot delete a host or initiator group that is part of a masking view.

Procedure

1. Select the EMC Symmetrix storage system.
2. Select Hosts > Hosts.
3. When the Hosts list opens, select the host or initiator group from the list and click Delete.
When the **Delete Initiator Group** confirmation dialog box appears, click **OK**.

Related information

- Creating an initiator group (see page 111)
- Modifying an initiator group (see page 112)
- EMC Unisphere for VMAX Online Help

## Creating a port group

Use this procedure to create a port group using EMC Unisphere for VMAX.

### About this task

This procedure should only be needed when adding a new engine or adding backup/replication hosts.

### Procedure

1. Select the EMC Symmetrix storage system.
2. Select **Hosts > Port Groups**.
3. From the **Port Groups** list view, click **Create Port Group**.
4. When the **Create Port Group** dialog box opens, type a port group name. Port group names must be unique from other port groups on the EMC Symmetrix system and cannot exceed 64 characters. Only alphanumeric characters, underscores ( _ ), and (-) are allowed. Port group names are case-insensitive.
5. Select the available ports from the **Ports** list and click **Add**. The following properties appears:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dir:Port</td>
<td>EMC Symmetrix system director and port in the port group</td>
</tr>
<tr>
<td>Identifier</td>
<td>WWPN of the port</td>
</tr>
<tr>
<td>Port Groups</td>
<td>Number of port groups where the port is a member</td>
</tr>
<tr>
<td>Masking Views</td>
<td>Number of masking views where the port is associated</td>
</tr>
<tr>
<td>Volumes</td>
<td>Number of volumes in the port group</td>
</tr>
<tr>
<td>VSA Flag</td>
<td>Indicates if Volume Set Addressing is set for the port</td>
</tr>
</tbody>
</table>
6. Click **OK**.
Related information

Adding ports to a port group (see page 115)
Deleting a port group (see page 116)
EMC Unisphere for VMAX Online Help

**Renaming a port group**

Use this procedure to rename a port group.

**Procedure**

1. Select the EMC Symmetrix system.
2. Select **Hosts > Port Groups**.
3. From the **Port Groups** list view, select the port group and click **View Details**.
4. When the **Details** view opens, type the new port group **Name** and click **Apply**.

**Adding ports to a port group**

Use this procedure to add ports to a port group using EMC Unisphere for VMAX.

**Procedure**

1. Select the EMC Symmetrix storage system.
2. Select **Hosts > Port Groups**.
3. From the **Port Groups** list view, select the port group and click **View Details**.
4. From the **Related Objects** window, click **Ports**.
5. When the list view opens showing the ports in the port group, click **Add Ports**.
6. From the **Add Ports** dialog box, select from the available ports and click **OK**.

Related information

Creating a port group (see page 114)
Deleting a port group (see page 116)
EMC Unisphere for VMAX Online Help
Removing ports from a port group

Use this procedure to remove ports from a port group

Procedure

1. To remove ports from port group, select the EMC Symmetrix system.
2. Select Hosts > Port Groups. The opens.
3. When the Port Groups list view opens, select the port group and click View Details.
4. From the Related Objects window, click Ports to open from the Ports list view.
5. Select the port to remove or hold down the shift key to multi-select the ports to be removed from the port group.
6. Click Remove.
7. Click Close.

Related information

EMC Unisphere for VMAX Online Help

Deleting a port group

Use this procedure to delete a port group using EMC Unisphere for VMAX.

About this task
You cannot delete a port group that is part of a masking view.

Procedure

1. Select the EMC Symmetrix storage system.
2. Select Hosts > Port Groups.
3. From the Port Groups list view, select the port group and click Delete.
4. Click Close.

Related information

Creating a port group (see page 114)
Adding ports to a port group (see page 115)
EMC Unisphere for VMAX Online Help

Creating a storage group

Use this procedure to create a storage group using EMC Unisphere for VMAX.

Procedure

1. Select the EMC Symmetrix storage system.
2. Select Storage > Storage Groups Dashboard.
3. In the Storage Group Management window, select Provision Storage to Host.
4. In the Provision Storage wizard, type a storage group name.
5. Select the appropriate storage resource pool.
6. Select your first desired service level, workload type, number of volumes, and volume capacity.
7. Select Add Service Level to create volumes of different response time characteristics in the same storage group.
   Note: If you create a multiple service level volumes, child storage groups will automatically be created and associated with the indicated service levels. It is recommended that you specify the service level in the name of the children storage groups. For example, cluster2_Gold 8.
8. After all of the desired storage groups and service levels have been entered, click Next to specify the host and port groups, or click Add to Job List to create the storage group(s) without provisioning to a host.

Related information

Modifying a storage group (see page 117)
Deleting a storage group (see page 118)
EMC Unisphere for VMAX Online Help

Modifying a storage group

Use this procedure to modify a storage group using EMC Unisphere for VMAX.
Procedure

1. Select the EMC Symmetrix storage system.

2. Select Storage > Storage Groups Dashboards.

3. In the Storage Group Management window, double-click the storage group to view details.

4. From the Details view, make changes in the Properties window and click Apply.

5. In the Related Object window, click Volumes.

6. When the Volumes list view appears, if you are adding volumes, perform the following:
   
   a. Click Add Volumes.
   
   b. Locate and select the volumes to add to the storage group.
   
   c. Optional: If adding volumes to a storage group that is part of a masking view:
      
      i. Click Set Dynamic LUN Addresses. The Set LUN Address - Storage Group dialog box opens.
      
      ii. Manually assign the host LUN addresses for all the volumes you are adding to the group.
      
      iii. Click OK.
   
   d. Click OK in the Add Volumes to Storage Group dialog box.

7. If removing volumes, perform the following:
   
   a. Select the volumes to remove from the storage group and click Remove Volumes.
   
   b. Select Unmap, if required.
   
   c. Click OK.

Related information

Creating a storage group (see page 117)
Deleting a storage group (see page 118)
EMC Unisphere for VMAX Online Help

Deleting a storage group

Use this procedure to delete a storage group using EMC Unisphere for VMAX.
About this task
You cannot delete a storage group that is part of a masking view.

Procedure

1. Select the EMC Symmetrix storage system.
2. Select Storage > Storage Groups Dashboard.
3. From the Storage Group Management window, double-click the storage group and click Delete.
4. Click OK when the confirmation message appears.

Related information

Creating a storage group (see page 117)
Modifying a storage group (see page 117)
EMC Unisphere for VMAX Online Help

Creating a masking view

Use this procedure to create a masking view using EMC Unisphere for VMAX.

Procedure

1. Select the EMC Symmetrix storage system.
2. Select Hosts > Masking view.
3. From the Masking view list view, click Create Masking view.
4. In the Create Masking View dialog box, type the masking view name.
5. Select the Initiator Group.
6. Select the Port Group.
7. Select the Storage Group.
8. Click OK.

Related information

Renaming a masking view (see page 120)
Deleting a masking view (see page 120)
Renaming a masking view

Use this procedure to rename a masking view using EMC Unisphere for VMAX.

Procedure

1. Select the EMC Symmetrix storage system.
2. Select **Hosts** > **Masking view**.
3. Select the masking view from the list and click **View Details**.
4. When the **Details** view appears, type the new name, and click **Apply**.

Related information

- [Creating a masking view](#) (see page 119)
- [Deleting a masking view](#) (see page 120)

Deleting a masking view

Use this procedure to rename a masking view using EMC Unisphere for VMAX3.

Procedure

1. Select the EMC Symmetrix storage system.
2. Select **Hosts** > **Masking view**.
3. When the **Masking Views** list view opens, select the masking view from the list and click **Delete**.
4. To unmap volumes in the masking view from their mapped ports, select **Unmap**.
5. Click **OK**.

Related information

- [Creating a masking view](#) (see page 119)
- [Renaming a masking view](#) (see page 120)
Managing NFS

Creating a file system on a storage array

Use this procedure to create a file system on a storage array.

About this task

VCE recommends the following guidelines for file system slicing:

- When using virtual provisioning (VP) pool volumes (TDEVs/Thin LUNs), slicing is permitted, except with EMC CLARiiON VP pools, which are FAST VP enabled. Slicing is permitted on thick VP pool LUNs or RAID group LUNs on EMC CLARiiON.

- Be familiar with replication requirements that may restrict slicing.
  - TF/SRDF require full volumes; slicing is not permitted.
  - EMC Celerra Replicator replicates the file system, regardless of the underlying storage volume configuration. Slicing is permitted.
  - When using traditional volumes (STDs/thick LUNs on RAID groups), slicing is permitted.

- Do not use a thin file system with a thin (TDEV or thin VP Pool LUN) backend volume. Use a thin file system only with a thick volume on the backend. A backend volume is a traditional thick LUN (STD, fully allocated or thick VP Pool LUN, or RG volume).

- Do not use auto-extend unless specifically requested by the customer.
  - The auto-extended file system displays the maximum size of the file system on the NFS client.
  - Use of auto-extend on many file systems can decrease the performance of the file systems due to the Control Station managing the file system extension rather than the storage array.
  - Use of auto-extend does reduce the possibility of a file system full event, but does require more monitoring and space management.

- The recommended file system size is no larger than what can be backed up and restored while maintaining SLAs. The maximum size is 16 TB.

- Enable uncached write on the NFS file systems that are to be used as VMware datastores.
  - You can increase performance by caching writes in the data mover and not requiring downstream acknowledgements from the array before acknowledging the write to the host. These techniques create data integrity issues. The data mover is not designed to preserve cached writes if an extended power outage occurs.
If the customer desires increased performance by not bypassing the data mover cache, make sure that they understand the risks involved.

Before you begin

Verify that there is sufficient space in the NAS pool to create the file system.

Procedure

1. Log in to the primary Control Station using EMC Unisphere on the storage management VM.
2. From the main menu, select Storage > Storage Configuration > File Systems.
3. When the File Systems list appears, to create a new file system, click Create.
4. In the Create File System window, perform the following:
   a. From the Create from field, select Storage Pool.
   b. Type a File System Name.
   c. From the Storage Pool field, select a storage pool.
   d. Type the Storage Capacity.
      
      Note: The Auto Extend Enabled, Thin Enabled, Slice Volumes, Deduplication Enabled, and Mount Point fields are set by default and should not be changed.
   e. Select the data mover that you want to use.
      
      Note: A mount point can be customized. Using the default mount point results in a mount point with the same name as the file system.
   f. Click Apply.

A message confirming the creation of the file system appears in the top of the window.

5. Click Cancel if you are done creating file systems.

6. To verify that Uncached Write is enabled, perform the following:
   a. Log into the Primary Control Station using PuTTY/SSH from the storage management VM.
   b. If the file system is mounted, type: \texttt{#server_unmount movername -perm fs_name \_fs\_mountpoint}
   c. To mount the system with Uncached Write enabled, type: \texttt{#server_mount movername -option rw, uncached fs_name fs_mountpoint}
   d. To verify the setting, type: \texttt{#server_mount ALL}
Select Storage > Storage Configuration > File Systems. From the list of file systems, verify that the new file system appears.

What to do next

Create an NFS export on the storage array. Mount the NFS export.

Related information

Creating an NFS export on a storage array (see page 123)

Reversing the procedure

Procedure

To reverse this procedure, from the File Systems list, select the file system and click Delete.

Creating an NFS export on a storage array

Use this procedure to create an NFS export on a storage array.

Before you begin

Create a file system on the storage array.

Procedure

1. Log in to the primary Control Station using EMC Unisphere on the storage management VM.
2. Select Storage > Shared Folders > NFS.
3. When the NFS Exports window appears, all of the NFS exports that already exist in the storage array appear. To create a new NFS export, click Create.
4. From the Create NFS Export window, perform the following:
   a. From the Choose Data Mover field, select a data mover.
   b. From the File System field, select a File System and type a path.
   c. In the Host Access field, type the IP addresses of the hosts that require access to the NFS export.

   Note: In this example, all of the hosts in the 192.168.X.X range have full access to the NFS export. This type of access is specific to a lab environment and should not be set in other environments. These formats can be used as guidance for enabling host access: 192.168.109.0/255.255.255.0 (109 subnet) 192.168.109.101,192.168.109.102 (specific hosts)
Click **Apply**. A confirmation message appears in the top of the window.

5 Click **Cancel** if you are done creating exports.

6 Select **Storage > Shared Folders > NFS**. From the list of exported file systems, verify that the exported file system appears.

What to do next

Mount the NFS export.

Related information

Creating a file system on a storage array (see page 121)

### Mounting the NFS export

Use this procedure to mount the NFS export on VMware vSphere ESXi.

Before you begin

- Create an NFS export on the storage array
- Set export permissions on the storage array to allow the host to access the export
- Verify that there is network connectivity between the storage array and the host where the NFS export is to be mounted

Procedure

1 From the VMware vCenter Server, select **Home > Inventory > Hosts and Clusters**.

2 From the host list, select the host on which to mount the NFS export.

3 From the **Configuration** tab, under **Hardware**, select **Storage**. A list of data stores appears.

4 Select **Add Storage** from the top menu.

5 When the **Add Storage** wizard appears, select **Network File System** and click **Next**.

6 On the **Locate Network File System** page, perform the following:

   a In the **Server** field, type the IP address of the NFS virtual interface of the data mover where the NFS export exists.

   b In the **Folder** field, type the path of the NFS export.

   c In the **Data store Name** field, type a name for NFS export to be listed in the data stores.
d Click Next.

7 From the Summary window, review the information and click Finish.

8 Verify the procedure as follows:

a Right-click on the data store, and select Browse Data store. The lost + found and etc directories appear in the data store.

b Create a test directory and copy the data to the directory to verify that you have read/write access to the data store.

Related information

Creating a file system on a storage array (see page 121)
Creating an NFS export on a storage array (see page 123)
Unmounting the NFS export (see page 125)

Unmounting the NFS export

Use this procedure to unmount the NFS export on VMware vSphere ESXi.

Procedure

1 From the Data stores window, right-click the datastore and select Unmount. A warning message appears that you are about to unmount the data store.

2 Click Yes to unmount the NFS export.

Related information

Mounting the NFS export (see page 124)
Creating a file system on a storage array (see page 121)

Deleting the NFS Export

Use this procedure to delete the NFS export.

Before you begin
Unmount the NFS export.
Procedure

1. Log in to the primary Control Station using EMC Unisphere on the storage management VM.
2. Select **Storage > Shared Folders > NFS**.
3. From the list of NFS exports, right-click the NFS export and select **Delete**.
4. If a message appears indicating a problem with the website’s security certificate, click **Continue to this website**.
5. When the **Confirm Delete** window appears, click **OK**.
6. Verify that the unmounted data store no longer appears.
Managing CIFS

Creating a CIFS

Use this procedure to create a CIFS.

About this task

VCE recommends the following guidelines for file system slicing:

- When using VP pool volumes (TDEVs/Thin LUNs), slicing is permitted except with EMC CLARiiON VP pools that are FAST VP enabled. Slicing is permitted on thick VP pool LUNs or RAID group LUNs on EMC CLARiiON.

- TF/SRDF requires full volumes; slicing is not permitted

- EMC Celerra Replicator replicates the file system, regardless of the underlying storage volume configuration. Slicing is permitted

- When using traditional volumes (STDs/thick LUNs on RAID groups), slicing is permitted

- Do not create a thin file system with a thin (TDEV or Thin VP Pool LUN) backend volume. Create a thin file system with a thick volume on the backend. A backend volume is a traditional thick LUN (STD, fully allocated or thick VP pool LUN, or RG volume)

- The auto-extended file system displays the maximum size of the file system on the NFS client

- Do not use auto-extend unless specifically requested by the customer

- Use of auto-extend on many file systems can decrease file system performance due to the Control Station managing the file system extension rather than the storage array

- Use of auto-extend reduces the possibility of a file system full event, but requires additional monitoring and space management

- The recommended file system size is no larger than what can be backed up and restored while maintaining SLAs. The maximum size is 16 TB

Before you begin

Be familiar with replication requirements that may restrict slicing.

Procedure

1. Log in to the primary Control Station using EMC Unisphere on the storage management VM.
3. From the File Systems list, to create a new file system, click Create.
4 From the **Create File System** window, perform the following:
   
   a From the **Create from** field, select **Storage Pool**.
   
   b Type a **File System Name**.
   
   c From the **Storage Pool** field, select a storage pool.
   
   d Type the **Storage Capacity**.
   
   e Do NOT select:
      
      - **Auto Extend Enabled** unless specifically requested by the customer.
      - **Thin Enabled** unless using STD volumes on the back end.
      - **Slice Volumes** unless using RAID groups or disk groups.
      - **Deduplication Enabled** unless specifically requested by customer.
   
   f From the **Data Mover (R/W)** field, select the data mover on which the CIFS server resides. If the CIFS server resides on a VDM (Virtual data mover), select the VDM name.
   
   g For the **Mount Point** field, select **Default** to use the file system name as the mount point or click **Custom** to designate a specific mount point.
      
      **Note:** VCE typically uses **Default**.
   
   h Click **OK**.

5 Click **OK** to confirm.

6 Verify the procedure as follows:
   
   a From the main menu, select **Storage > Storage Configuration > File Systems**.
   
   b From the list of file systems, verify that the new file system appears.
   
   c Verify the following:
      
      - A CIFS server exists and is licensed on the storage array.
      - CIFS services are up and running.
      - The CIFS server is joined with an **Active Directory** domain, or a different authentication method must be used to access the CIFS share.

**What to do next**

Create a CIFS share.
Creating a CIFS share
(see page 129)

Reversing the procedure

Procedure

To delete a file system, from the File Systems list, select the file system and click Delete.

Creating a CIFS share

Use this procedure to create a CIFS share.

Before you begin

- Verify that a CIFS server exists and is licensed on the storage array and that CIFS services are up and running.
- Verify that the CIFS server is joined with an Active Directory domain, or a different authentication method must be used to access the CIFS share.
- Verify that NTP is running on the X-Blades and the time on the X-Blades is in sync with the Active Directory (AD) servers. NTP configuration is performed on the Control Station CLI.
  - To check if NTP is running, type: server_date ALL timesvc stats ntp
  - To check time on the X-Blades, type: server_date ALL
- Create a CIFS file system.

Procedure

1. Log in to the primary Control Station using EMC Unisphere on the storage management VM.
2. From the main menu, select Storage > Shared Folders > CIFS.
3. From the Shares list, to create a CIFS share, click Create.
4. If a warning message appears indicating a problem with the website’s security certificate, click Continue to this website.
5. From the Create CIFS Shares window, perform the following:
   a. From the Choose Data Mover field, select the data mover that you want to create the CIFS share on.
   b. Type a CIFS Share Name.
c From **File System** field, select the file system.

d Check the **CIFS server** box to create the CIFS share on.

e In the **Path** field, type a new path if you do not want to use the default path.

f Optional: Type a **User Limit**.

g Click **Apply**. A confirmation message appears at the top of the page indicating that a new CIFS share was created successfully.

6 Click **Cancel** if you are finished.

7 To verify the procedure, from the main menu, select **Storage > Shared Folders > CIFS**. From the list of shares, verify that the new share appears.

**What to do next**

Map the CIFS share.

**Related information**

[Mapping the CIFS share](#) (see page 130)

**Mapping the CIFS share**

Use this procedure to map a CIFS share.

**Before you begin**

- Verify that the guest operating system where the share is being mapped has access to the CIFS share using an authentication method such as Active Directory (AD)

- Create a CIFS share

**Procedure**

1 From the guest operating system where the CIFS share is to be mapped, right-click on **My Computer**, and select **Map Network Drive**.

2 Select a **Drive** letter to map the CIFS share.

3 In the **Folder** field, type the IP address of the CIFS server, and the full path name of the CIFS share.

4 If not already checked, select **Reconnect at logon**, and click **Finish**.

**Note:** You may have to re-type user credentials when the drive is being mapped.
To verify the procedure:

a. Open **My Computer** to view the mapped CIFS share.

b. Open the Y drive.

*Note:* The new share is mapped to the Y drive in this example.

As a root-level share, the `.etc` and `lost+found` directories already exist.

c. Create a new test directory to verify that you have read-write privileges to this share.

Related information

**Unmapping a CIFS share** (see page 131)

**Unmapping a CIFS share**

Use this procedure to disconnect a CIFS share.

**Before you begin**

- Verify that the share is mapped.
- Verify that the guest operating system on which the share is being mapped has access to the CIFS share using an authentication method such as Active Directory.

**Procedure**

1. On the system which you want to disconnect from the CIFS share, right-click on **My Computer** and select **Disconnect Network Drive**.

2. Select the drive that you wish to disconnect, and click **OK**.

3. To verify that the CIFS share was unmapped properly, go to **My Computer** and verify that the CIFS share does not appear.

Related information

**Mapping the CIFS share** (see page 130)

**Deleting a CIFS share**

Use this procedure to delete a CIFS share.
Procedure

1. Log in to the primary Control Station using EMC Unisphere on the storage management VM.
2. From the main menu, select Storage > Shared Folders > CIFS.
3. From the listing of CIFS Shares, right-click on the CIFS share and select Delete.
4. When Confirm Delete message appears, click OK.
5. Select Storage > Shared Folders > CIFS.

What to do next

From the list of shares, verify that the deleted share does not appear.

Related information

Creating a CIFS share (see page 129)
Managing VMware vSphere ESXi 5.1, 5.5, and 6.0

Installing the latest VMware vSphere ESXi patch

Use this procedure to install the latest supported VMware vSphere ESXi patch.

About this task

The following releases of VMware vSphere ESXi are supported:

- 6.0
- 5.5
- 5.1

After you install the latest patch, when you update a VMware vSphere ESXi host to a newer supported build, the host no longer shares the same build.

VCE recommends that you use the VMware Update Manager (VUM) if upgrading to a newer supported build, however, you can use the CLI to install the patch.

Do not use this procedure for major upgrades.

Before you begin

- Verify that the host is in Maintenance mode and all the VMs are evacuated.
- Verify the software compatibility for the Cisco Nexus 1000V Series Switch or VDS, EMC PowerPath VE, and the build to which you are upgrading. You might need to upgrade third-party software prior to updating to the latest release of VMware vSphere ESXi.
- Obtain the VCE Release Certification Matrix with the version to which you want to update. Look for the supported version of the VMware patch (build) in the Virtualization section.
- Determine which patch to install. For supported versions, refer to the appropriate VCE Release Certification Matrix.

Procedure

1. Download the latest VMware vSphere ESXi patch supported for this release.
3. In the Search by Product menu, select ESXi (Embedded and Installable) | 5.x.0 or 6.0.
4. Click Search.
5  Select and download the latest supported VMware vSphere ESXi patch. For example, ESXi5X0-2012XXXXX.zip

6  Install the patch as described in *Patching VMware vSphere ESXi hosts with the VMware Update Manager*.

7  To verify the installation, on the VMware vSphere ESXi host Splash Screen (through Cisco UCS vKVM), confirm that the build number matches the update just applied.

8  Reboot the VMware vSphere ESXi host.

### Configuring advanced settings for VMware vSphere ESXi

Use this procedure to configure advanced VMware vSphere ESXi settings.

**About this task**
The following advanced settings are available:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk.UseDeviceReset</td>
<td>0</td>
</tr>
<tr>
<td>NFS.MaxVolumes</td>
<td>256</td>
</tr>
<tr>
<td>Net.TcpipHeapSize</td>
<td>30</td>
</tr>
<tr>
<td>Net.TcpipHeapMax</td>
<td>512 for VMware vSphere 6.0</td>
</tr>
<tr>
<td>Net.TcpipHeapMax</td>
<td>512 for VMware vSphere 5.5</td>
</tr>
<tr>
<td>Net.TcpipHeapMax</td>
<td>128 for VMware vSphere 5.1</td>
</tr>
</tbody>
</table>

NFS performance is enhanced when advanced configuration options are set. VCE recommends applying NFS options before connecting any NFS share to the VMware vSphere ESXi hosts.

You can configure the settings on each host individually using the VMware vSphere client or run the VMware vSphere PowerCLI script to configure the settings on all VMware vSphere ESXi hosts.

**Before you begin**

- If configuring with the script, verify that the VMware PowerCLI is installed on a workstation with administrative access to VMware vCenter
- Obtain the IP address and local root user credentials for the VMware vSphere ESXi host or appropriate administrative credentials to the VMware vCenter

**Procedure**

1. Within the VMware vSphere client, select the host.

2. Select the **Configuration** tab.
3 In the **Software** section, select **Advanced Settings**.

4 Set the parameters in the window.

5 To configure the settings on each VMware vSphere ESXi host in the VMware vCenter using the script:
   
   a Verify that VMware vSphere PowerCLI is installed on a Microsoft Windows machine.
   
   b Verify that you have network access to the VMware vCenter server.
   
   c Copy the script to a `.ps1` file on your hard drive.
   
   d Modify the `$vcenter` variable.
Execute the script in the VMware vSphere PowerCLI environment.

**Note:** This script does NOT set jumbo frames on the vmknics. You must perform jumbo frame settings manually or using another tool.

```powershell
# Set NFS advanced settings for all servers in vCenter. If hosts were built using EMC UIM, or built manually, this script can be run to assist with the configuration of NFS. It does NOT set jumbo frames on the vmknics: you must do this by using the command line or another tool.

$vcenter = Read-Host "What is the name/IP of the vCenter Server?"

connect-viserver $vcenter

$esxHosts = Get-VMHost | Sort Name

foreach($esx in $esxHosts){
  Write-Host "Updating TCP and NFS advanced configuration Settings on $esx"
  # Update TCP settings
  if((Get-VMHostAdvancedConfiguration -VMHost $esx -Name Net.TcpipHeapSize).Values -ne "30"){
    Set-VMHostAdvancedConfiguration -VMHost $esx -Name Net.TcpipHeapSize -Value 30 -Confirm:$false
  }
  if((Get-VMHostAdvancedConfiguration -VMHost $esx -Name Net.TcpipHeapMax).Values -ne "128"){
    Set-VMHostAdvancedConfiguration -VMHost $esx -Name Net.TcpipHeapMax -Value 512 -Confirm:$false
  # for vSphere 5.5 or 6.0
    # Set-VMHostAdvancedConfiguration -VMHost $esx -Name Net.TcpipHeapMax -Value 128 -Confirm:$false
    # for vSphere 5.1
  }
  # Update NFS settings
  if((Get-VMHostAdvancedConfiguration -VMHost $esx -Name NFS.MaxVolumes).Values -ne "256"){
    Set-VMHostAdvancedConfiguration -VMHost $esx -Name NFS.MaxVolumes -Value 256 -Confirm:$false
  }
  if((Get-VMHostAdvancedConfiguration -VMHost $esx -Name NFS.HeartbeatTimeout).Values -ne "5"){
    Set-VMHostAdvancedConfiguration -VMHost $esx -Name NFS.HeartbeatTimeout -Value 5 -Confirm:$false
  }
}
```

**Results**

To verify the procedure, review the modified **Advanced Settings** in the **Advanced Settings** section under the **Configuration** tab using the VMware vSphere Client on each VMware vSphere ESXi host.

**What to do next**

Reboot the VMware vSphere ESXi host(s).
Reversing the procedure

Procedure

To reverse this procedure, modify the Advanced Settings back to their default values.

Hardening security on VMware vSphere ESXi hosts

About this task

For information on hardening security on the VMware vSphere ESXi hosts, refer to the VMware vSphere Security Hardening Guides.
Managing VMware vSphere virtual machines

Increasing the disk timeout on Microsoft Windows virtual machines

Use this procedure to increase the amount of time for a Microsoft Windows VM to wait for unresponsive disk I/O operations.

About this task

- VCE recommends increasing the disk timeout value to 190 seconds. VMware tools, version 3.0.2 and later sets the value to 60 seconds.
- VCE recommends including this registry setting on all Microsoft Windows VMs and templates to accommodate unresponsive disk I/O operations.
- For more information, refer the VMware Knowledge Base entry 1014.

Procedure

1. Using the Microsoft regedit application, navigate to HKEY_LOCAL_MACHINE > /System > /CurrentControlSet > Services > /Disk.
2. Right-click and select New > DWORD (32-bit) Value.
3. Type the value name TimeOutValue. The name is case sensitive.
4. Set the data type to REG_DWORD.
5. Set the data to 190 (decimal).
6. Reboot the virtual machine.

Setting up Java and Internet Explorer on the management workstation or virtual machine

Use this procedure to set up Java and Internet Explorer version 11 on the management workstation or virtual machine (element manager) if EMC Unisphere or other web-based applications fail to launch. You configure the Java security setting to support web-based applications.

Before you begin

- Ensure Java version 7 Update 51 or later is installed on the management workstation or virtual machine.
• Ensure that the Java security level complies with your corporate security policy.

Procedure

1 Using administrative privileges, log into Microsoft Windows on the management workstation or virtual machine.

2 Navigate to the Java Windows Control Panel.

3 Select the Security tab.

4 Set the security level to the lowest setting (least secure).

5 Click Edit Site List..., which opens in the Exception Site List popup window.

6 Add the URLs of web-based applications. For example: https://ip_address_of_web_based_application

7 Click OK to close the Exception Site List popup window.

8 Click OK to close the Java Windows Control Panel.
Managing VMware vCenter Single Sign-On for VMware vSphere 6.0

VMware vCenter Single Sign-On overview

VMware vCenter Single Sign-On (SSO) is an authentication mechanism that allows you to configure security policies and lock out or disable an account for VMware vSphere 6.0. Usually, the default policies do not need to be modified. However, you might have to modify policies or accounts if regulations require different policies or if you are troubleshooting a problem.

Unlocking and resetting the VMware vCenter Single Sign-On administrator password (VMware vSphere 6.0)

Use the procedure in the VMware knowledge base article KB 2034608 to unlock a VMware vCenter Single Sign-On (SSO) administrator account.

About this task

For security purposes, the VMware vCenter administrator account is locked after three failed login attempts.

Procedure

Follow the procedure in the VMware knowledge base article 2034608.

Managing the lockout status of VMware vCenter Single Sign-On (VMware vSphere 6.0)

Use this procedure to view the lockout status of a VMware vCenter Single Sign-On (SSO) account.

Procedure

1. Log on to the VMware vSphere Web Client as an SSO administrator.
   
   Note: By default, the user is administrator@vsphere.local.

2. From the home page, select Administration > Single Sign-On > Users and Groups.

3. Each tab shows information from the identity sources about configured accounts that are on the system. Select the Users tab.
4 The Locked or Disabled columns show the status of each configured SSO account. Right-click the appropriate account and select Enable/Disable or Unlock.

**Note:** The Locked Users and Disabled Users tabs show information for the identity sources only.

5 Click Yes to confirm.

Managing VMware vCenter Single Sign-On default password policies (VMware vSphere 6.0)

Use this procedure to manage the VMware vCenter Single Sign-On default password policies.

**About this task**

By default, the SSO passwords expire after 365 days, including the SSO administrator password. You can modify the expiration policy to manage administrative passwords.

**Procedure**

1 Log on to the VMware vSphere Web Client as an SSO administrator.

   **Note:** By default, this user is administrator@vsphere.local.

2 From the home page, select Administration > Single Sign-On > Configuration.

3 To view current SSO password policies, select the Policies tab and click Password Policies.

4 To modify the password policy, click Edit.

5 Make the required changes and click OK.

Managing VMware vCenter Single Sign-On lockout policies (VMware vSphere 6.0)

Use this procedure to modify the strict lockout policy of VMware vCenter Single Sign-On.

**Procedure**

1 Log on to the VMware vSphere Web Client as an SSO administrator.

   **Note:** By default, this user is administrator@vsphere.local.

2 From the home page, select Administration > Single Sign-On > Configuration.

3 Select the Policies tab and then select Lockout Policy to view the current lockout policies.
4. To modify the lockout policy, select Edit.

5. Make the required changes and click OK.

**Adding an Active Directory identity source to VMware vCenter Single Sign-On (VMware vSphere 6.0)**

Use this procedure to associate Windows Active Directory to the VMware vCenter Single Sign-On 6.0 service on the Platform Services Controller(s).

**About this task**

Follow this procedure for each Active Directory domain you wish to associate with VMware SSO, unless otherwise indicated.

**Note:** This procedure may not be available during the VCE Manufacturing process.

**Before you begin**

You must have network access to the vCenter Web Client and Active Directory Domain Admin privileges.

**Procedure**

1. Join the SSO Virtual Machine to the appropriate Windows Active Directory Domain. Restart the server.

2. Log on to the VMware vSphere 6.0 Web Client on the vCenter virtual machine via this URL:
   https://localhost:9443/vsphere-client/

3. Log on using the `administrator@vsphere.local` administrator account (username & password are case-sensitive). For credentials information, see VCE Systems usernames and passwords.

4. Click Administration on the left pane.

5. Click System Configuration under Deployment.

6. Click the Nodes icon under System Configuration.

7. Select Platform Services Controller 2's hostname, click the Manage tab and click the Settings button.

8. Click Active Directory under Advanced.

9. Click the Join... button.
10 Type the Active Directory **Domain**, **User name**, and **Password** (with appropriate AD domain administrative rights).

   **Note:** Leave Organizational unit blank.

11 Click **OK**.

12 **Reboot** the Platform Service Controller Node under the **Actions** menu.

13 Select **Platform Services Controller 1’s hostname**, click the Manage tab and click the **Settings** button.

14 Click **Active Directory** under **Advanced**.

15 Click the **Join…** button.

16 Type the Active Directory **Domain**, **User name**, and **Password** (with appropriate AD domain administrative rights).

   **Note:** Leave Organizational unit blank.

17 Click **OK**.

18 **Reboot** the **Platform Service Controller Node** under the **Actions** menu.

   **Note:** Rebooting the (primary) Platform Service Controller Node 1 affects the following:
   
   — All running tasks on the node will be cancelled or interrupted.
   
   — All users currently accessing this node will temporarily lose connectivity.
   
   — If this node is a vCenter Server, features such as DRS and vMotion will temporarily become unavailable.
   
   — If this node is a Platform Services Controller, services such as Single Sign-On, licensing and certificate, running on this node will temporarily go down.

19 Click **Administration** on the left pane.

20 Click **Configuration** under **Single Sign-On**.

21 Click the **Identity Sources** tab.

22 Click the green + icon to type the details for the Active Directory domain that is to be added.

23 Select the **Active Directory** (Integrated Windows Authentication) radio button under **Identity source type**.

24 Verify the **domain name** that was previously registered to the Platform Services Controller will be assigned to this AD domain registration.

25 Select the **Use machine account** radio button and click **OK**.
26  The Active Domain registration is complete.

   **Note:** While logged into vCenter through the Web Client or vSphere Client as the administrator@vsphere.local administrative user, you must assign Administrator roles/permissions for domain user accounts or groups that will require access to vCenter 6.0. By default, only the administrator@vsphere.local administrator account can access vCenter until additional permissions are explicitly assigned to domain users.

---

**Backing up or restoring the VMware external Platform Services Controller configuration (VMware vSphere 6.0)**

Use this procedure to back up or restore the VMware vCenter Platform Services Controller (PSC).

**About this task**

Maintaining a back-up of the PSC configuration ensures continued VMware vSphere access for VMware vCenter Server components.

**Procedure**

1. Follow the back up and restore procedure in the VMware knowledge base article [KB 2110294](https://kb.vmware.com/kb/2110294).

2. Refer to the *Backing Up and Restoring vCenter Server* section in the [VMware vSphere 6.0 Documentation Center](https://www.vmware.com/support/vsphere/doc/), which you can find here:

   ESXi and vCenter Server 6.0 Documentation > vSphere Installation and Setup > Backing Up and Restoring vCenter Server

**Redirecting VMware vCenter Server to the secondary external Platform Services Controller (VMware vSphere 6.0)**

If the primary external Platform Services Controller fails and there are multiple PSCs that are replicating without fault tolerance configured, you need to repoint the vCenter Server for authentication.

**Procedure**

Refer to the *Repointing the Connections Between vCenter Server and Platform Services Controller* section of the [vSphere Installation and Setup Guide](https://docs.vmware.com/en/vsphere/6.0/standard/configuration/guides/installation-and-setup/index.html). You can find the section here: ESXi and vCenter Server 6.0 Documentation > vSphere Installation and Setup > After You Install vCenter Server or Deploy the vCenter Server Appliance

For more information, see the [VMware Platform Services Controller 6.0 FAQs](https://www.vmware.com/support/doclib/vsphere60/index.html)
Enabling fault tolerance for the external Platform Services Controller (VMware vSphere 6.0)

Use the following procedure to enable fault tolerance on the external PSC.

About this task

If you have multiple PSCs, you can create fault tolerant pairing, which provides continuous availability for VMware vCenter Server instance authentication.

Before you begin

Perform the following tasks before enabling fault tolerance:

1. Read the Providing Fault Tolerance for Virtual Machines section in the vSphere Availability Guide of the VMware vSphere 6.0 Documentation Center.
2. Review and resolve all validation and compliance checks needed to ensure fault tolerance is operational.
3. Confirm the PSC virtual machine CD/DVD drive is set to Client Device.
4. Confirm that the VMKernel flagged for fault tolerance logging is created on all appropriate ESXi hosts.

Procedure

Follow the Turn On Fault Tolerance procedure in the VMware vSphere Availability Guide of the VMware vSphere 6.0 Documentation Center.
Managing VMware vCenter Single Sign-On for VMware vSphere 5.5

VMware vCenter Single Sign-On (SSO) is an authentication mechanism that allows you to configure security policies and lock out or disable an account for VMware vSphere 5.5.

Usually, the default policies do not need to be modified. However, you might have to modify policies or accounts if regulations require different policies or if you are troubleshooting a problem.

Unlocking and resetting the VMware vCenter Single Sign-On administrator password

Use the procedure to unlock a VMware vCenter Single Sign-On (SSO) administrator account.

About this task

For security purposes, the VMware vCenter administrator account is locked after three failed login attempts.

Procedure

Follow the procedure in the VMware knowledge base article KB 2034608.

Managing the lockout status of VMware vCenter Single Sign-On account

Use this procedure to view the lockout status of a VMware vCenter Single Sign-On (SSO) account.

Procedure

1. Log on to the VMware vSphere Web Client as an SSO administrator.
   
   **Note:** By default, the user is administrator@vsphere.local.

2. From the home page, select Administration > Single Sign-On > Users and Groups.

3. Each tab shows information from the identity sources about configured accounts that are on the system. Select the Users tab.

4. The Locked or Disabled columns show the status of each configured SSO account. Right-click the appropriate account and select Enable/Disable or Unlock.

   **Note:** The Locked Users and Disabled Users tabs show information for the identity sources only.
Click Yes to confirm.

Managing VMware vCenter Single Sign-On default password policies

Use this procedure to manage the VMware vCenter Single Sign-On (SSO) default password policies.

About this task

By default, the SSO passwords expire after 365 days, including the SSO administrator password. You can modify the expiration policy to manage administrative passwords.

Procedure

1. Log on to the VMware vSphere Web Client as an SSO administrator.
   
   **Note:** By default, this user is administrator@vsphere.local.

2. From the home page, select Administration > Single Sign-On > Configuration.

3. To view current SSO password policies, select the Policies tab and click Password Policies.

4. To modify the password policy, click Edit.

5. Make the required changes and click OK.

Managing VMware vCenter Single Sign-On lockout policies

Use this procedure to modify the strict lockout policy of VMware vCenter Single Sign-On (SSO).

Procedure

1. Log on to the VMware vSphere Web Client as an SSO administrator.
   
   **Note:** By default, this user is administrator@vsphere.local.

2. From the home page, select Administration > Single Sign-On > Configuration.

3. Select the Policies tab and then select Lockout Policy to view the current lockout policies.

4. To modify the lockout policy, select Edit.

5. Make the required changes and click OK.
Adding an Active Directory identity source to VMware vCenter Single Sign-On

Use this procedure to associate an Windows Active Directory (AD) identity source to the VMware vCenter Single Sign-On (SSO) 5.5 service.

About this task
This procedure joins the Windows server running VMware vCenter Server to the domain and adds the AD (Integrated Windows Authentication) identity source to SSO. This procedure is not required if the VMware vCenter SSO server was joined to the AD domain and logged on to with a domain admin account prior to installation.

Before you begin
Obtain network access to the VMware vCenter Web Client and Windows AD domain with administrator privileges.

If the VMware vCenter Server and SSO are installed in separate systems from a custom installation, join both systems to the domain.

Procedure

1. Join the Microsoft Windows server running the VMware vCenter Server to the domain.
2. Reboot the server for the changes to take effect.
3. After the system is up and the services are started, to add the AD (Integrated Windows Authentication) identity source to SSO, perform the following:
   a. Log on to the vSphere Web Client as the SSO administrator (administrator@vsphere.local).
   b. Select Administration.
   c. If closed, expand Single Sign-On.
   d. Click Configuration.
   e. Select the Identity Sources tab.
   f. Click Add Identity Source (+) under the Options menu.
   g. Select Active Directory (Integrated Windows Authentication). If the domain name field is not automatically propagated with the proper Windows DNS domain, type the proper DNS domain.
   h. Select Use machine account and click OK.
What to do next

After the AD identity source is configured, users from that domain can be added to the VMware vCenter Server.

Related information

www.vmware.com

Backing up the VMware vCenter Single Sign-On configuration

Back up the VMware vCenter Single Sign-On (SSO) configuration as a Single Sign On.zip on the desktop of the host machine.

About this task

This procedure modifies the Windows registry. Before making any registry modifications, verify that you have a current and valid backup of the registry and the VM. The Microsoft Knowledge Base - article 136393 contains information on backing up and restoring the registry.

Maintaining a backup of the SSO configuration ensures continued VMware vSphere access for VMware vCenter Server components. For a complete backup, back up your SSO database. Refer to the documentation for your database type.

Back up the SSO configuration:

- After installing, updating, or changing the location of a VMware vCenter SSO instance
- Before the VMware vCenter Server VM is restored from a snapshot
- Before the VMware vCenter Server VM is installed from a backup of the database from a prior VMware vCenter Server instance

Procedure

1. To generate a log bundle on the desktop of the user logged into the VMware vCenter SSO server, perform the following:
   
   a. Select Programs > VMware.
   
   b. Right-click Generate vCenter Single Sign-On log bundle and select Run as administrator. To redirect where the log bundle is to be generated, from an elevated command prompt, replace <Absolute Path To Folder> with your preferred path: cscript "C:\Program Files\VMware\Infrastructure\VMware\cis\vmware-sso\vm-support\sso-support.wsf" /s:<Absolute Path To Folder>
2 To back up associated Windows registry keys, perform the following:
   a Select Start > Run, and type regedit.
   b Press Enter.
   c From the Registry Editor window, back up the registry folder: HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\services\VMwareDirectoryService

3 To back up SSL certificates, certificate server data, and KDC data folders, perform the following:
   a For the SSL certificates, back up: C:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf.
   b For the certificate server data, back up: C:\ProgramData\VMware\CIS\data\vmca.
   c For the KDC data, back up:
      ■ C:\ProgramData\VMware\CIS\cfg\vmkdc
      ■ C:\ProgramData\MIT\Kerberos5

4 To back up the VMware directory service (VMdir) database, open a command prompt to perform the following:
   a To create a new directory to store the database backup, type: mkdir C:\MDBBackup
   b To change the directory, type: cd C:\Program Files\VMware\Infrastructure\VMware\CIS\vmdird
   c To back up the database using the vdcbackup, type: vdcbackup C:\ProgramData\VMware\cis\data\vmdird C:\MDBBackup
      Note: This creates a copy of the data.mdb and lock.mdb files and places them in the C:\MDBBackup directory.
   d Back up the MDBBackup folder where the copies of the two database files were stored.

Related information

VMware vSphere 5.5 Upgrade Guide
Restoring a VMware vCenter Single Sign-On single or primary node

Use this procedure to restore a VMware vCenter Single Sign-On (SSO) single or primary node instance to a new host machine.

About this task

This procedure manually restores a VMware vCenter SSO single node or primary node instance from a full operating system level vCenter Server 5.5 backup. If the VMware vCenter SSO single node or primary node instance is corrupt, restore a backup to ensure continued VMware vSphere access for VMware vCenter Server.

Before you begin

- Restore the VMware vCenter Server 5.5 from backup according to vendor best practices
- Back up the VMware vCenter SSO configuration and shut down the corrupt vCenter Server

Procedure

1. Install the VMware vCenter Server 5.5 on a new VM.
2. Stop VMware vCenter SSO services on the restored VMware vCenter Server in the following order:
   - VMware Secure Token Service
   - VMware Identity Management Service
   - VMware Certificate Service
   - VMware KDC Service
   - VMware Directory Service
   
   Note: The VMware Knowledge Base contains information about how to start or stop VMware vCenter Services.
3. To restore the VMware Directory Service (VMdir) database, perform the following:
   a. Verify the VMdir has stopped.
   b. Navigate to the VMdir at: \ProgramData\VMware\cis\data\vmdird
   c. Copy the backed up data.mdb and lock.mdb files to the VMdir directory.
4 In a multi-site SSO deployment, type **VMdir** in restore mode to import the database files and replicate with the other nodes.

   a. Open a command prompt and change directory to C:\Program Files\VMware\Infrastructure\VMware\CIS\vmdird.

   b. To start the restore operation, type: `vmdird.exe -m restore`

   VMdir starts in restore mode and terminates when the restore is complete.

5 Start VMware vCenter SSO services on the restored VMware vCenter Server in the following order:

   - VMware Directory Service
   - VMware Kdc Service
   - VMware Certificate Service
   - VMware Identity Management Service
   - VMware Secure Token Service

Related information

**VMware Knowledge Base article 1003895 - starting, stopping or restarting VMware vCenter services**

**Restoring from a VMware vCenter Server 5.5 database backup**

Use this procedure to manually restore a VMware vCenter Single Sign-On (SSO) single node or primary node instance from a database backup.

**Before you begin**

- This procedure modifies the Windows registry. Before making any registry modifications, ensure that you have a current and valid backup of the registry and the VM.

- Prepare a host machine for the restored VMware vCenter SSO instance. The host machine can be a physical machine or a VM and must satisfy the hardware requirements for VMware vCenter SSO.

- Download the VMware vCenter Server installer from the [VMware Download Center](#) to the new host machine.

- Name the new host machine with the same name as the failed VMware vCenter SSO instance.
Procedure

1. Install only VMware vCenter SSO 5.5.x on a new VM.

2. Stop all VMware vCenter SSO services on the restored VMware vCenter Server system in this order:
   - VMware Secure Token Service
   - VMware Identity Management Service
   - VMware Certificate Service
   - VMware KDC Service
   - VMware Directory Service

3. To restore the VMwareDirectoryService registry folder, perform the following:
   a. Select Start > Run.
   b. Type regedit and press Enter.
   c. When the Registry Editor opens, select File > Import and select the backup key.

4. Restore the SSL certificates by restoring the backup copy of the conf folder and its contents to this directory: C:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf

5. Restore the certificate server data by restoring the backup copy of the vmca folder and its contents to this directory: C:\ProgramData\VMware\CIS\data\vmca

6. Restore the KDC data by restoring the backup copy of the vmkdc and Kerberos5 folders to these directories:
   - C:\ProgramData\VMware\CIS\cfg\vmkdc
   - C:\ProgramData\MIT\Kerberos5

7. To restore the VMdir database, perform the following:
   a. Verify that the VMware Directory Service has stopped.
   b. Navigate to the VMdir directory at: C:\ProgramData\VMware\cis\data\vmdird
   c. Copy the backed up data.mdb and lock.mdb files to the VMdir directory.
In a multi-site VMware vCenter SSO deployment, to run VMDir in restore mode to allow it to import the database files and replicate with the other nodes, open a command prompt and perform the following:

a. To change the directory, type: `cd C:\Program Files\VMware\Infrastructure\VMware\CIS\vmdird`

b. To start the restore, type: `vmdird.exe -m restore`

Start all VMware vCenter SSO services on the restored VMware vCenter Server in following order:

- VMware Directory Service
- VMware KDC Service
- VMware Certificate Service
- VMware Identity Management Service
- VMware Secure Token Service

What to do next

Continue with the VMware vSphere 5.5 installation.
Managing VMware vCenter Single Sign-On for VMware vSphere 5.1

VMware vCenter Single Sign-On (SSO) is an authentication mechanism that allows you to configure security policies and lock out or disable an account for VMware vSphere 5.1.

Usually, the default policies do not need to be modified. However, you might have to modify policies or accounts if regulations require different policies or if you are troubleshooting a problem.

Unlocking and resetting the VMware vCenter Single Sign-On administrator password

Use the procedure to unlock a VMware vCenter Single Sign-On (SSO) administrator account.

About this task

For security purposes, the VMware vCenter administrator account is locked after three failed login attempts.

Procedure

Follow the procedure in the VMware knowledge base article KB 2034608.

Managing the lockout status of a VMware vCenter Single Sign-On account

Use this procedure to view the lockout status of a VMware vCenter Single Sign-On (SSO) account.

Procedure

1. Log in to the VMware vSphere Web Client as an SSO administrator.
   
   **Note:** By default, the user is `admin@system-domain`.

2. In the home page, select **Administration > Access > SSO Users and Groups**.

   Each tab shows information from the identity sources about accounts that are configured on the system.

3. Select the **Users** tab. The **Locked** or **Disabled** columns display the status of each configured SSO account.

   **Note:** The **Locked Users** and **Disabled Users** tabs show information for the identity sources only. They can also be locked or disabled, therefore, based on the account being used, click the appropriate tab.
4 Right-click the appropriate account and click either **Enable/Disable** or **Unlock** the account.

5 Click **Yes** to confirm.

**Managing VMware vCenter Single Sign-On default password policies**

Use this procedure to manage the VMware vCenter Single Sign-On (SSO) default password policies.

**About this task**

By default, the SSO passwords expire after 365 days, which includes the SSO administrator password. You can modify the expiration policy to ensure that administrative passwords do not expire unexpectedly.

**Procedure**

1 Log in to the VMware vSphere Web Client as an SSO administrator. By default, this user is `admin@system-domain`.

2 In the home page, click **Administration > Sign-On and Discovery > Configuration**.

3 Select the **Policies** tab and then click **Password Policies** to see the current password policies for SSO.

4 To modify the password policy, click **Edit**.

5 Make the required changes and then click **OK**.

**Managing the VMware vCenter Single Sign-On lockout policies**

Use this procedure to modify the strict lockout policy of VMware vCenter Single Sign-On (SSO) for your organizational requirements.

**Procedure**

1 Log in to the VMware vSphere Web Client as an SSO administrator.

   **Note:** By default, this user is `admin@system-domain`.

2 On the home page, click **Administration > Sign-On and Discovery > Configuration**.

3 Select the **Policies** tab and then click **Lockout** policy to view the current password policies for SSO.

4 To modify the password policy, click **Edit**.

5 Make the required changes and then click **OK**.
Adding an Active Directory identity source to VMware vCenter Single Sign-On

Use this procedure to associate Windows Active Directory (AD) to the VMware vCenter Single Sign-On (SSO) service.

About this task
This procedure is not required if someone joined the VMware vCenter SSO server to the AD domain and logged in with a domain admin account prior to its installation.

Before you begin
Obtain network access to the VMware vCenter Web Client and Windows AD domain with administrative privileges.

Procedure

1. To log into the VMware vSphere 5.1 Web Client on the VMware vCenter VM, navigate to: https://localhost:9443/vsphere-client/
2. Log in using the admin@System-Domain administrator account.
3. Select Administration.
4. Select Configuration under Sign-On and Discovery.
5. Verify that the AD domain you wish to add is not included in the Identity Sources listing.
6. Click the green plus sign (+) to access the details for the AD domain you want to add.
7. Click Active Directory under Identity source type.
8. Type a name to assign to this AD domain registration.
9. Type the primary server URL. For example, ldap://ad01.location.company-name.com:3268
10. Type the secondary server URL. For example, ldap://ad02.location.company-name.com:3268
11. Type the base domain name for users. For example, DC=LOCATION,DC=COMPANY-NAME,DC=COM
12. Type the domain name. For example, location.company-name.com
13. Type the domain (NETBIOS) alias. For example, LOCATION
14. Type the base domain name for groups. For example, DC=LOCATION,DC=COMPANY-NAME,DC=COM
15 Select password from the Authentication Type pull-down menu.

16 Provide the domain admin credentials for the domain being added in the Username and Password fields.

   **Note:** You can use the appropriate AD KDC SSL security certificate and select Reuse Session.

17 Click Test Connection.

18 If the test is successful, click OK.

   **Note:** While logged in to VMware vCenter through the Web Client or VMware vSphere Client as the admin@System-Default administrative user, you must assign administrator roles/permissions for domain user accounts or groups that require access to VMware vCenter 5.1. By default, only the admin@System-Default administrator account can access VMware vCenter until additional permissions are explicitly assigned to domain users.

### Related information

**VMware documentation**

### Backing up the VMware vCenter Single Sign-On configuration

Use this procedure to back up the VMware vCenter Single Sign-On (SSO) configuration.

#### About this task

Maintaining a backup of the SSO configuration ensures continued VMware vSphere access for VMware vCenter Server components. For a complete backup, you must also back up your SSO database. Refer to the documentation for your database type.

Back up the SSO configuration when you:

- Install, update, or change the location of a VMware vCenter SSO instance.
- Modify the node.pkg file. This includes changing the SSO database information, such as database host name or port, or changing the SSO password that was created for the administrator user admin@System-Domain when SSO was originally installed.

   **Note:** This original password is required when you restore a SSO backup.

- Need to maintain a point-in-time copy of the SSO configuration.

#### Procedure

1 Log in to the VMware vCenter SSO host machine.
2 You can back up the Single Sign On configuration using the Microsoft Windows user interface or the command prompt. To back up using the user interface, go to step 3. Otherwise, go to step 4 for the command prompt.

3 To back up the Single Sign On configuration from the Microsoft Windows user interface, perform the following:
   a Select Start > Programs > VMware.
   b Right-click the Generate vCenter Single Sign On backup bundle and select Run as administrator.

4 From a command prompt, perform the following:
   a Right-click the Command Prompt icon or menu item, and select Run as administrator.
   b Change directory to D:\Program Files\VMware\Infrastructure\SSOServer\scripts.
   c If you installed SSO in a location other than the default C:\Program Files, adjust the path.
   d Type cscript sso-backup.wsf /z and press Enter.

Results
The VMware vCenter SSO configuration is backed up as Single Sign On.zip on the desktop of the host machine.

Related information
VMware vSphere 5.1 Upgrade Guide

Restoring a VMware vCenter Single Sign-On single or primary node instance

Use this procedure to restore a VMware vCenter Single Sign-On (SSO) single or primary node instance to a new host machine.

About this task
If the VMware vCenter SSO single node or primary node instance is corrupted, you can restore a backup to ensure continued VMware vSphere access for VMware vCenter Server.

Before you begin
   • Verify that you have a current backup of the VMware vCenter SSO configuration
Prepare a host machine for the restored SSO instance. The host machine can be a physical or VM but must satisfy the SSO hardware requirements

Verify access to the VMware vCenter SSO database from the host machine

Verify that you have the original administrator password for the VMware vCenter SSO instance that you are restoring

Verify that you have the account name and password for the RSA SSPI service and VMware vCenter SSO service of the VMware vCenter SSO instance that you are restoring

Download the VMware vCenter Server installer to the new host machine

Procedure

1. Copy the backup file `Single Sign On.zip` to the new host machine in the directory `C:\Temp\SSO Recovery`.

2. Rename the new host with the same Fully Qualified Domain Name (FQDN) as the SSO server from which you created the backup.

3. If the SSO instance from which you created the backup was in a workgroup and installed using its IPv4 address, verify that the new host machine has the same static IP address.

   **Note:** DHCP is not supported.

4. Verify that the DNS of the new host is forward and reverse resolvable.

5. On the VMware vCenter SSO host machine, in the VMware vCenter Server installation directory, double-click the `autorun.exe` file to start the installer.

6. Select **vCenter™ Single Sign On** and click **Install**.

7. Follow the prompts in the installation wizard to choose the installer language and to agree to the end user patent and license agreements.

8. Select **Recover installed instance of vCenter Single Sign-On from a backup**.


10. Type the original administrator password for the old SSO instance. Use the password that was created for the admin@System-Domain user when SSO was originally installed, even if you have changed that password.

11. Make sure that the RSA SSPI service is logged on to the same account as in the SSO instance from which you created the backup.

12. Follow the prompts to complete the SSO restoration.

**Results**
The VMware vCenter SSO single or primary node instance is restored.
What to do next

If there are SSO high-availability backup nodes associated with the primary node that you restored, ensure that the RSA SSPI service logs on to the same account in the primary node and all high availability backup nodes.

From the VMware vSphere Web Client, log in to the VMware vCenter Server instances that are registered to the SSO instance to verify that you have working access to them.

Related information

VMware ESXi and vCenter Server 5.1 documentation: Hardware Requirements for vCenter and vSphere
Managing virtualization

Patching VMware vSphere ESXi hosts with the VMware Update Manager

Use this procedure to patch the VMware vSphere ESXi hosts with VMware Update Manager (VUM).

About this task
Complete this procedure when a new VMware vSphere ESXi host is deployed or requires an update.

Before you begin
Verify that the patch bundle is listed on the latest version of the VCE Systems Release Certification Matrix.

Procedure

1. Set the VMware vSphere ESXi host to Maintenance mode.
2. In the VMware vSphere client, select a host and go to Update Manager > Admin View > Configuration > Patch Download Settings.
3. From the Patch Download Sources window, click Import Patches.
4. From the Select Patches window of the Import Patches wizard, browse to where you saved the patch or package software bundle, and select the file.
5. Click Next and wait until the file upload successfully completes. If the upload fails, verify that the structure of the zip file is correct or verify that the VUM settings are correct.
6. Click Next.
7. From the Confirm Import window, verify that the package imported into the VUM repository, and click Finish.
8. Select the Patch Repository tab and search for the package and verify that the import worked.
9. Select the Baselines and Groups tab and click Create to create a new baseline.
10. From the New Baseline wizard, in the Name field, type the package name. For example, PowerPath.
11. For Host Baselines, click Host Extension.
12. Click Next.
13. Find the package extension and click the down arrow to add it to the Extensions to Add field.
15 You can attach the package baseline to individually selected VMware vSphere ESXi hosts or to multiple hosts at a time by selecting the cluster.

To attach the package baseline to several VMware vSphere ESXi hosts:

a  Go to the Compliance view and highlight the desired host in the list to the left of the vSphere client window, and select a folder, cluster, or data center.

b  In the right window, select Update Manager and then click Attach.

c  From the Attach Baseline or Group window, under Name, select the package baseline that you created.

d  Click Attach.

16 Select Scan and check the circle in the Compliance box at the top right side of the screen.

<table>
<thead>
<tr>
<th>If the circle is...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>This is the first time attached the baseline to the VMware vSphere ESXi host.</td>
</tr>
<tr>
<td>Green</td>
<td>You have already attached baselines to the VMware vSphere ESXi host and remediated them. The 100% compliant indicator shows that the extension is already installed.</td>
</tr>
<tr>
<td>Red</td>
<td>You must stage and remediate the baseline (as described in the following step) to achieve compliance. To verify the remediation, review the information in the Recent Tasks window, or click the Tasks/Event tab.</td>
</tr>
</tbody>
</table>

17 Staging is the process of pushing the package onto individual VMware vSphere ESXi hosts from the VUM server. To stage the baseline:

a  In the Update Manager tab, in the Attached Baselines list in the middle of the screen, highlight the package baseline that you created, and click Stage.

b  Click Stage. When the Stage Wizard appears, under the Name column in the Baselines list, the package baseline that you created is selected by default.

Note: The default Name selection should not be changed. In the Host column, all the VMware vSphere ESXi hosts to which you attached the package baseline are selected by default.

c  If desired, change the default Host selection to stage the baseline to only one or some of the VMware vSphere ESXi hosts.

d  Click Next.

e  From the Patch and Extension Exclusion window, verify the information and click Next.

f  From the Ready to Complete window, verify the information and click Finish.
To remediate the package baseline, perform the following:

a Highlight the VMware vSphere ESXi host to remediate.

**Note:** When you remediate the package baseline, packages are installed on hosts that do not have the package. The package is updated on hosts that have an outdated package.

b In the Attached Baselines area, highlight the package baseline that you created and click Remediate. From the Remediate window, in the Baseline Groups and Types area, Extension Baselines is selected by default. In the Baselines list, the package baseline that you created is selected by default.

**Note:** Default selections should not be altered. Under Host, all the VMware vSphere ESXi hosts to which you staged the package baseline are selected by default.

c If desired, change the default Host selection to remediate the baseline to only one or some of the VMware vSphere ESXi hosts and click Next.

d From the Patches and Extensions window, verify the information and click Next.

e From the Host Remediation Options window, in the Task Name field, type a task name. For example, PowerPath/VE install.

f In the Task Description field, type a description. For example, PP/VE 5.9 install.

g Change or maintain remediation time and failure options values in the Remediation Time and Failure Options fields as needed to suit your environment.

h Click Next. The Ready to Complete window appears with your remediation selections.

i Verify the information and click Finish.

Related information

Accessing VCE documentation (see page 11)

**Supported guest operating systems**

Use this procedure to install supported guest operating systems in VMware VMs.

For information about installing supported guest operating systems in VMware VMs, refer to the VMware Guest Operating System Installation Guide.

Related information

Guest Operating System Installation Guide
Using VMware Enhanced vMotion Compatibility with Cisco UCS blade servers

Use these guidelines to ensure Enhanced vMotion Compatibility (EVC) when upgrading Cisco UCS blade servers in a Vblock System.

Use this information with the Vblock System Blade Packs Reference.

VCE does not recommend mixing Cisco UCS blade server types within a cluster. However, there are instances when it is necessary to mix blade types, including upgrades.

When upgrading Cisco UCS blade servers in a Vblock System, consider the following guidelines:

- Cisco UCS Blade Servers B200 M1 through B200 M3 support Enhanced vMotion Compatibility (EVC) mode Intel® "Nehalem" Generation (Xeon® Core™ i7). Individual Cisco UCS blade servers support several EVC modes, but only Xeon Core i7 is a commonly supported mode across all three Cisco UCS blade servers. If the CPU feature sets are greater than the EVC mode you are enabling, you may need to power down all VMs in the cluster, and enable or modify the EVC mode.

- Cisco UCS Blade Servers B200 M1 and M2 support some additional CPU features (such as those provided in 32-nanometer EVC mode), but some of those features might not be enabled in the BIOS due to U.S. export rules. To ensure complete and reliable vMotion compatibility when mixing blade types in a single cluster, use Intel Xeon® Core™ i7 EVC mode.

- If all the Cisco UCS blade servers in the cluster have the same CPU type, set the EVC mode to CPU architecture. For example, if the cluster contains all Cisco UCS Blade Servers B200 M1, select Intel Xeon® Core™ i7 EVC mode. This allows vMotion compatibility between Cisco UCS Blade Servers B200 M1 and other hosts.

  **Note:** EVC mode should only be enabled if you are adding, or planning to add hosts with newer CPUs to an existing cluster.

- Set the EVC mode before you add Cisco UCS blade servers with newer CPUs to the cluster. This eliminates the need to power down the VMs running on the blade servers. Setting a lower EVC mode than the CPU can support may hide some CPU features, which may impact performance. Proper planning is needed if performance or future compatibility within the cluster is desired.

**Related information**

- [Enhanced vMotion Compatibility (EVC) processor support (KB1003212)](Enhanced_vMotion_Compatibility_(EVC)_processor_support_(KB1003212))
- [Enable EVC on an Existing Cluster](Enable_EVC_on_an_Existing_Cluster)
Enabling VMware Enhanced vMotion Compatibility within a cluster

Use this procedure to enable VMware Enhanced vMotion Compatibility (EVC) within a cluster.

About this task
The VMware EVC ensures vMotion compatibility for hosts in a cluster. VMware EVC verifies that all hosts in a cluster present the same CPU feature set to the VMs, even if the CPUs on the hosts are different. The EVC feature uses the Intel FlexMigration technology to mask processor features so that hosts can present the feature set of an earlier generation of processors. This feature is required if hosts in a cluster use both Cisco UCS C200 and C220 Rack Servers.

Before you begin
Before enabling VMware EVC on an existing cluster, ensure that the hosts in the cluster meet the requirements listed in EVC Requirements in the VMware vSphere ESXi and vCenter Server 5 Documentation.

Procedure

1. You can optionally create an empty cluster. If you have already created a cluster, skip this step.
   
   **Note:** This is the least disruptive method of creating and enabling a VMware EVC cluster.

2. Select the cluster for which you want to enable VMware EVC.

3. If the VMs are running with more features than the EVC mode you intend to set, power off the VMs, enable EVC, and migrate them back into the cluster after enabling VMware EVC.

4. Power off all the VMs on the hosts with feature sets greater than the VMware EVC mode.

5. Migrate the cluster’s VMs to another host.

6. Edit the cluster settings and enable EVC.

7. Select the CPU vendor and feature set appropriate for the hosts in the cluster.

8. If you powered off and migrated virtual machines out of the cluster, power on the VMs in the cluster and migrate the VMs back into the cluster.

Related information

VMware vSphere ESXi and vCenter Server 5 Documentation

Configuring the Virtual Flash Read Cache

Use this procedure to configure the Virtual Flash Read Cache (VFRC) for each VM.
Procedure

1. Using the VMware vSphere web client, open the Hosts and Clusters view.
2. Right-click the virtual machine and select Edit Settings.
3. In the Virtual Hardware tab, expand the VMDK to be configured with the VFRC.
4. In the Virtual Flash Read Cache field, enter a value for the read cache configuration size for the VMDK. Specify the block size using the Advanced option.
5. Repeat Steps 1 - 4 for each virtual machine and associated VMDK that requires VFRC.

Note: VMware vSphere does NOT prevent over provisioning. Consider the total available Virtual Flash Read Cache capacity when configuring the cache size.
Managing VMware VDS

The section provides the most common procedures for managing an existing VMware vSphere Distributed Switch (VDS).

Managing licenses

Use this procedure for an overview of how to manage VMware vSphere Distributed Switch (VDS) licenses.

About this task

The VMware VDS is an enterprise feature of VMware vSphere vCenter Server 5.5 and requires that the VMware vSphere ESXi hosts are licensed with the VMware vSphere Enterprise Plus edition. A non-Enterprise Plus edition will not support VMware VDS functionality. No additional license is required to be installed or managed for the VMware VDS.

Provisioning a VMware VDS configuration

This section provides procedures for provisioning an existing VMware vSphere Distributed Switch (VDS) configuration.

Modifying an existing distributed port group

Use this procedure to modify distributed port group settings for the VMware vSphere Distributed Switch (VDS) from the VMware vSphere Web Client.

About this task

From the VMware vSphere Web Client, you can modify distributed port group settings such as the name, VLAN ID, teaming and failover policy, traffic filtering and marking policies. VCE standard configuration settings must not be changed to ensure proper Vblock System operation.

Using the VMware vSphere Web Client, only one distributed port group can be edited at a time. If several port groups require modification, VCE recommends using VMware PowerCLI or vSphere vCLI command line/script tools.

Before you begin

Identify the VMware VDS containing the distributed ports. The default switch name used throughout this guide is DVSswitch01-A.
Procedure

1. To launch the VMware vSphere Web Client from VMware vCenter Server, open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client

   **Note:** You can also launch the VMware vSphere Web Client by selecting **Start Menu > All Programs > VMware > VMware vSphere Web Client.**

2. Log on to the VMware vSphere Web Client with the `administrator@vsphere.local` user account (Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3. On the **VMware vSphere Web Client Home** tab, under **Inventories**, click **Networking**.

4. Expand **DVSwitch01-A** and right-click the distributed port group that you want to modify and click **Edit Settings**.
The following table shows the VCE recommended settings:

<table>
<thead>
<tr>
<th>Edit option</th>
<th>Field: VCE recommended setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name: the name chosen for the distributed port group</td>
</tr>
<tr>
<td></td>
<td>Port binding: Static Binding</td>
</tr>
<tr>
<td></td>
<td>Port allocation: Elastic</td>
</tr>
<tr>
<td></td>
<td>Number of ports: 8 (increases automatically as long as Elastic is selected for port allocation)</td>
</tr>
<tr>
<td></td>
<td>Network resource pool: use default setting</td>
</tr>
<tr>
<td></td>
<td>Description: Add details about distributed port groups</td>
</tr>
<tr>
<td>Advanced</td>
<td>Configure reset at disconnect: Enabled</td>
</tr>
<tr>
<td></td>
<td>Override port policies: use default setting</td>
</tr>
<tr>
<td>Security</td>
<td>Promiscuous mode: Reject</td>
</tr>
<tr>
<td></td>
<td>MAC address changes: Reject</td>
</tr>
<tr>
<td></td>
<td>Forged transmit: Reject</td>
</tr>
<tr>
<td>Traffic shaping</td>
<td>Ingress traffic shaping: Disabled</td>
</tr>
<tr>
<td></td>
<td>Egress traffic shaping: Disabled</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN type: VLAN</td>
</tr>
<tr>
<td></td>
<td>VLAN ID: Refer to the Logical Configuration Survey</td>
</tr>
<tr>
<td>Teaming and failover</td>
<td>Load balancing: Route based on physical NIC load. The vMotion port group only has one active uplink (associated with vNIC2 fabric A). The other uplink should be in standby mode</td>
</tr>
<tr>
<td></td>
<td>Network failure detection: Link status only</td>
</tr>
<tr>
<td></td>
<td>Notify switches: Yes</td>
</tr>
<tr>
<td></td>
<td>Failback: Yes</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Netflow: default</td>
</tr>
<tr>
<td>Traffic filtering and marking</td>
<td>Status: enable this option for vMotion NFS distributed port groups. All other port groups should be disabled</td>
</tr>
<tr>
<td></td>
<td>vMotion Traffic Rule Enabled - use the + sign to make edits</td>
</tr>
<tr>
<td></td>
<td>Action tag</td>
</tr>
<tr>
<td></td>
<td>COS value checkbox is selected</td>
</tr>
<tr>
<td></td>
<td>Set CoS to 4</td>
</tr>
<tr>
<td></td>
<td>Set traffic direction to Egress</td>
</tr>
<tr>
<td></td>
<td>Type System Traffic and set Protocol/Traffic Type to vMotion</td>
</tr>
<tr>
<td></td>
<td>NFS Traffic Rule Enabled - use the + sign to make edits</td>
</tr>
<tr>
<td></td>
<td>Action tag</td>
</tr>
<tr>
<td></td>
<td>COS value checkbox is selected</td>
</tr>
<tr>
<td></td>
<td>Set CoS to 2</td>
</tr>
<tr>
<td></td>
<td>Set traffic direction to Egress</td>
</tr>
<tr>
<td></td>
<td>Type IP and set Protocol/Traffic Type to Any</td>
</tr>
</tbody>
</table>
Creating a distributed port group

Use this procedure to create a distributed port group on an existing VMware vSphere Distributed Switch (VDS).

About this task

You can use the VMware vSphere Web Client to create and add virtual and VMKernel distributed port groups to an existing VMware VDS. After you create a distributed port group, you must configure the port group.

Procedure

1. To launch the VMware vSphere Web Client from the VMware vCenter Server, open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client.

   **Note:** You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Right-click DVSwitch01-A and select New Distribution Port Group.

5. From the New Distributed Port Group wizard, to create the distributed port group, perform the following:
   
a. Type the name of the distributed port group and click Next.

   b. Leave Port binding and Port allocation to the default settings Static binding and Elastic.

   c. Leave the Number of Ports to the default setting of eight.

   d. Set the VLAN type to VLAN and change the VLAN ID.

   e. Leave Customize default policies configuration unchecked.

   f. Click Next.

   g. Review and verify the settings for the new distributed port group and click Finish.

Virtual distributed port groups can be assigned to the VMs. VMKernel distributed port groups require configuration.
What to do next

As an option, assign VMKernel distributed port groups to the VMware vSphere ESXi hosts. Refer to Configuring a VMkernel distributed port group (see page 172).

Configuring a VMKernel interface

Use this procedure to configure a VMKernel (vMotion or NFS) interface using the Add and Manage Host wizard.

Before you begin

Create a VMkernel distributed port group.

Procedure

1. From the VMware vSphere Web Client Home tab, under Inventories, click Networking.
2. Right-click DVSwitch01-A and select Add and Manage Hosts.
3. From the Add and Manage Hosts wizard, perform the following:
   a. Select Manage host networking and click Next.
   b. Select Attach hosts.
   c. From the Select member hosts window, select the VMware vSphere ESXi host, and click OK.
      
      Note: You can add multiple VMware vSphere ESXi hosts at the same time.
   d. Verify that the selected host(s) have been added to the list and click Next.
   e. From the Select network adapter tasks window, deselect Manage physical adapters and verify that Manage VMKernel adapters is selected.
   f. Click Next.
   g. Select the VMware vSphere ESXi host and click New adapter.
   h. From the Add Networking window, verify that Select an existing Distributed Port Group is selected and click Browse.
   i. Select VMKernel (vMotion or NFS) distributed port group and click OK.
   j. Click Next.
   k. For the vMotion distributed port group only, select vMotion traffic and click Next.
l For the NFS distributed port group only, verify that Enable services is unchecked and click Next.

m Select Use static IP4 settings, apply IPv4 address/Subnet Mask, and click Next.

n When the Analyze impact window appears, click Next.

o From the Ready to complete window, validate the settings and click Finish.

p Select the new VMKernel.

q Select Edit adapter.

r Select NIC settings.

s Verify that the MTU setting is set to 1500.

   Note: The NFS MTU setting is 9000.

t Click OK and Finish.

u Repeat steps g through s for each additional VMware vSphere ESXi host to create a new network adapter.

v Click Next.

w Verify that the No Impact message appears and click Next.

x Review and verify the Summary results and click Finish.

**Associating VMware vSphere ESXi hosts to an existing VMware VDS**

Use this procedure to associate a new VMware vSphere ESXi host to an existing VMware vSphere Distributed Switch (VDS).

**About this task**

Associating a new VMware vSphere ESXi host to an existing VMware VDS requires adding the vmnics to the VMware VDS uplinks. From the Add and Manage Hosts wizard, you can:

- Add two physical adapters (vmnic2 and vmnic3) to the VMware VDS
- Associate the VMware vSphere ESXi hosts to the VMware VDS

**Before you begin**

Verify which VMware VDS the VMware vSphere ESXi host will be added.
Procedure

1. To launch the VMware vSphere Web Client from VMware vCenter Server, open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client.

   **Note:** You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Right-click DVSwitch01-A and select Add and Manage Hosts.

5. From the Add and Manage Hosts wizard, perform the following:
   a. Select Add Hosts and click Next.
   b. Select New Hosts.
   c. From the Select new hosts window, select the VMware vSphere ESXi host to be added and click OK.
      
      **Note:** You can modify multiple VMware vSphere ESXi hosts at a time using the Add and Manage Hosts wizard.
   d. Validate the selected host appears in the list and click Next.
   e. From the Select network adapter tasks window, deselect Manage VMKernel adapters.
   f. Verify that Manage physical adapters is selected and click Next.
   g. Select vmnic2 and click Assign uplink.
   h. Select Uplink 1 and click OK.
   i. Select vmnic3 and click Assign uplink.
   j. Select Uplink 2 and click OK.
   k. Click Next.
   l. Verify that the status message displays no impact and click Next.

6. Review the Summary results and click Finish.

**Configuring jumbo frames on VMware VDS**

Use this procedure to configure jumbo frames on an existing VMware vSphere Distributed Switch (VDS).
Procedure

1. Open a browser and type the following URL: `https://<vCenterIP>:9443/vsphere-client`  
   **Note:** You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

2. Log on to the VMware vSphere Web Client with the `administrator@vsphere.local` user account (VMware vSphere Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Right-click `DVSwitch01-A` and select Edit Settings.

5. On the Properties tab, select Advanced.

6. Change the MTU value from 1500 to 9000.

7. Click OK.

**Configuring jumbo frames on distributed port groups**

Use this procedure to configure jumbo frames on the NFS distributed port group.

Procedure

1. Open a browser and type the following URL: `https://<vCenterIP>:9443/vsphere-client`  
   **Note:** You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

2. Log on to the VMware vSphere Web Client with the `administrator@vsphere.local` user account (VMware vSphere Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, select Hosts and Clusters.

4. Select the first host.  
   **Note:** Each NFS distributed port group must be modified for each VMware vSphere ESXi host.

5. Under Manage, select Networking, and then select VMKernel adapters.

6. From the table, select the adapter with the `vcesys_esx_nfs` listed under the network label.

7. Click the edit icon to select NIC settings and change the MTU value from 1500 to 9000.
8 Click OK.

9 Repeat this procedure for each VMware vSphere ESXi host as needed.

Modifying class of service settings

Use this procedure to modify class of service (CoS) settings for the VMware vSphere Distributed Switch (VDS).

About this task

The CoS marking is leveraged as part of the VCE standard configuration and configured with the Traffic Filtering and marking policy on VMware VDS.

Procedure

1 Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client

   Note: You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

2 Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3 On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4 Expand the DVswitch01-A to view all port groups.

5 Right-click vcesys_esx_vmotion distributed port group and click Edit settings.

6 Select Traffic filtering and marking.

7 From the Status drop-down box, select Enable.

8 Select the green plus (+) icon to open the New Network Traffic Rule wizard, and perform the following:

   a For the Name, type: vMotionCOS.

   b For Action, select Tag.

   c Check CoS value, and change value to 4.

   d Change the Traffic direction to Egress only.

   e Select the green plus (+) and select New System Traffic Qualifier.

   f Verify that the type is set System traffic and the Protocol/Traffic type is set to vMotion.
g  Click OK.

9  Right-click the `vcesys_esx_nfs` distributed port group, click Edit settings.

10 From the wizard, perform the following:
   a  For the Name, type: NFSCOS
   b  For Action, select Tag.
   c  Check Update CoS tag, and change value to 2.
   d  Change the Traffic direction to Egress only.
   e  Select the green plus (+) and select New IP Qualifier.
   f  From the Protocol drop-down, select Any.
   g  Leave the Type as IP.
   h  Click OK.

Decommissioning VMware VDS components

This section describes the steps necessary to decommission all the VMware vSphere Distributed Switch (VDS) components.

This section covers the following procedures for decommissioning VMware VDS components:

- Deleting distributed port groups
- Disassociating the VMware vSphere ESXi host from an existing VMware VDS
- Removing a VMware VDS

Deleting a distributed port group

This section describes how to delete a distributed port group from an existing VMware vSphere Distributed Switch (VDS).

Before you begin

- Before deleting a distributed port group, reassign all powered-on VMs to a different distributed port group. If the VMs are powered off, you can delete the distributed port group.

  Note: If you delete a distributed port group with powered-on VMs and network adapter numbers assigned to the distributed port group, the system returns an error.
• Migrate the VMKernel ports from the VMware vSphere ESXi host attached to the VMware VDS.

Perform the following procedures:

• If there are powered-on VMs on the distributed port group, refer to Migrating VM distributed port group assignments.

• If there are no powered on VMs on the distributed port group, refer to Deleting a distributed port group from a VMware VDS

Migrating VM distributed port group assignments to a different switch

Use this procedure to migrate VM distributed port group assignments to a different distributed or standard switch.

About this task

This procedure is not required if there are no powered-on VMs on the distributed port group. VMs connected to the distributed port group can be powered-off to remove the distributed port group.

You can use the VM migration wizard to migrate any port group types. However, use caution when migrating the VMware vCenter Server VMs, because a disconnect can cause the loss of the VMware vCenter Server, which could prevent the VM port group from migrating.

You can use the VM migration wizard to migrate from a VMware vSphere Standard Switch (vSS) to a VMware vSphere Distributed Switch (VDS), a VMware VDS to a VMware vSS or a VMware VDS to a VMware VDS seamlessly.

Before you begin

Verify that the powered-on VMs on all VMware vSphere ESXi hosts that are attached to an existing VMware VDS are not assigned to any distributed port groups.

Verify that there is an available distributed port group to which to migrate the powered-on VMs.

Create another switch with the following criteria:

• If migrating to a different VMware vSphere Distributed Switch:
  – Attach at least one VMNIC as an uplink for a new distributed or standard switch.
  – Create the distributed port groups with the same name and VLAN ID as the existing switch.

• If migrating to a standard switch:
  – Create a new standard switch and attach at least one VMNIC as an uplink for the standard switch.
vNIC0 and vNIC1 connect to a different set of physical switches than vNIC2 and vNIC3. Do not add vNIC2 and/or vNIC3 to vSwitch0, because it could cause the VMware vSphere ESXi host to lose network connectivity if management traffic gets switched.

If no VMNICs are available, migrate one VMNIC from the VMware VDS. Keep the second VMNIC on the Distributed Switch for VM traffic to continue to communicate.

Create the VM port group with correct VLAN ID to the new standard switch.

Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client

   **Note:** You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Right-click DVswitch01-A and select Migrate VM to Another Network.

5. From the Migrate Virtual Machine Networking wizard, perform the following:

   a. Verify that Specific network is selected and click Browse.

   b. Select the Source network distributed port group or standard port group and click OK.

   c. Select Browse for the destination network.

   d. Select the distributed port group or port group where the VMs will be reassigned and click OK.

   e. Click Next.

   f. When the list of VMs appear, select the checkbox on each VM, and click Next.

   g. Validate that the source and destination is correct and click Finish. The selected VMs distributed port groups migrate to a new distributed or standard switch.

Deleting the distributed port group from the VMware VDS

Use this procedure to delete the distributed port group from the existing VMware vSphere Distributed Switch (VDS).
Before you begin

- Verify that there are no powered-on VMs on any of the distributed port groups.
- Verify that none of the VMs have a port assignment connected to any of the distributed port group.

Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client.

   **Note:** You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Select the drop-down Array on DVswitch01-A to list the distributed port groups.

5. Right-click the distributed port group and select All vCenter Action > Remove from Inventory.

6. Click OK.

**Disassociating the VMware vSphere ESXi host**

This section describes how to disassociate the VMware vSphere ESXi host from an existing VMware vSphere Distributed Switch (VDS).

**Before you begin**

- Reassign all the VMs to a port group on a different distributed switch or standard switch. Otherwise, an error occurs when you attempt to delete the VMware vSphere ESXi host from the VMware VDS.
- Migrate all VMKernel ports to a different distributed switch or standard switch.
- Distributed port groups and uplink adapters do not need to be removed.

VMs network adapters assigned to a distributed port group will force an error when attempted to delete the ESXi host from the VMware VDS. All the VMs are assigned to the distributed port group need to be reassigned to a port group on a different distributed or standard switch. The VMware VDS that is being removed must have all the VMKernel ports either migrated to a different standard Switch or VMware VDS or be removed.
After reviewing the prerequisites, perform the following procedures:

1. **vMotion/evacuate all powered on VMs from the VMware vSphere ESXi host**
2. **Migrate VM distributed port group assignments**
3. **Migrate the VMkernel ports to a different switch**

**vMotion/evacuating all powered-on VMs from the VMware vSphere ESXi host**

Use this procedure to evacuate/vMotion all powered-on VMs to a different VMware vSphere ESXi host to free up the ports on the VMware vSphere Distributed Switch (VDS). VMs can still point to the same distributed port groups from a different VMware vSphere ESXi host, because there are no assigned VMs on the host.

**About this task**

This procedure requires using the migration VM network wizard that migrates all the VMs port assignments to a different switch with no downtime. If this option is not possible due to the number of VMs or a shortage of system resource capacity, refer to *Migrating powered-on VMs distributed port group assignments to a different switch*.

**Before you begin**

Ensure that sufficient system capacity exists on other VMware vSphere ESXi hosts to migrate all the powered-on VMs.

**Procedure**

1. Open a browser and type the following URL: `https://<vCenterIP>:9443/vsphere-client`
   
   **Note:** You can also launch the VMware vSphere Web Client by selecting **Start Menu > All Programs > VMware > VMware vSphere Web Client**.

2. Log on to the VMware vSphere Web Client with the **administrator@vsphere.local** user account (VMware vSphere Single Sign On (SSO) account) or other administrative account with appropriate permissions.

3. On the **VMware vSphere Web Client Home** tab, under **Inventories**, select **Hosts and Clusters**.

4. From the left window, select the appropriate VMware vSphere ESXi host and select the **Related Objects** tab.

5. From the right window, click **Virtual Machines**. Using the **CTRL** key, select all of the VMs.

6. Select **Actions > Migrate** to open the migration wizard.

7. Verify that **Change host** is selected and click **Next**.
8 Select the destination resource (cluster or VMware vSphere ESXi host) to migrate the VMs and click Next.

9 Verify that Resource CPU for optimal vMotion performance (Recommended) is selected and click Next.

10 Review the summary window and click Finish. The VMs migrate to a different VMware vSphere ESXi host. If the cluster was chosen as the destination with DRS enabled, VMware vCenter automatically places the VMs with a different VMware vSphere ESXi host.

Migrating VM distributed port group assignments to a different switch

Use this procedure to migrate VM distributed port group assignments to a different distributed or standard switch.

About this task

This procedure is not required if there are no powered-on VMs on the distributed port group. VMs connected to the distributed port group can be powered-off to remove the distributed port group.

You can use the VM migration wizard to migrate any port group types. However, use caution when migrating the VMware vCenter Server VMs, because a disconnect can cause the loss of the VMware vCenter Server, which could prevent the VM port group from migrating.

You can use the VM migration wizard to migrate from a VMware vSphere Standard Switch (vSS) to a VMware vSphere Distributed Switch (VDS), a VMware VDS to a VMware vSS or a VMware VDS to a VMware VDS seamlessly.

Before you begin

Verify that the powered-on VMs on all VMware vSphere ESXi hosts that are attached to an existing VMware VDS are not assigned to any distributed port groups.

Verify that there is an available distributed port group to which to migrate the powered-on VMs.

Create another switch with the following criteria:

- If migrating to a different VMware vSphere Distributed Switch:
  - Attach at least one VMNIC as an uplink for a new distributed or standard switch.
  - Create the distributed port groups with the same name and VLAN ID as the existing switch.

- If migrating to a standard switch:
  - Create a new standard switch and attach at least one VMNIC as an uplink for the standard switch.
vNIC0 and vNIC1 connect to a different set of physical switches than vNIC2 and vNIC3. Do not add vNIC2 and/or vNIC3 to vSwitch0, because it could cause the VMware vSphere ESXi host to lose network connectivity if management traffic gets switched.

- If no VMNICS are available, migrate one VMNIC from the VMware VDS. Keep the second VMNIC on the Distributed Switch for VM traffic to continue to communicate.
- Create the VM port group with correct VLAN ID to the new standard switch.

Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client

   **Note:** You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Right-click DVswitch01-A and select Migrate VM to Another Network.

5. From the Migrate Virtual Machine Networking wizard, perform the following:
   a. Verify that Specific network is selected and click Browse.
   b. Select the Source network distributed port group or standard port group and click OK.
   c. Select Browse for the destination network.
   d. Select the distributed port group or port group where the VMs will be reassigned and click Ok.
   e. Click Next.
   f. When the list of VMs appear, select the checkbox on each VM, and click Next.
   g. Validate that the source and destination is correct and click Finish. The selected VMs distributed port groups migrate to a new distributed or standard switch.

Migrating the VMKernel ports to a different switch

Use this procedure to migrate the VMKernel ports to a different distributed or standard switch.
Before you begin

Do not associate the VMware vSphere ESXi host with VMKernel ports to the VMware vSphere Distributed Switch (VDS). Create another distributed or standard switch to migrate the VMKernel ports.

The standard or distributed switch must have the minimum support criteria:

- Attach at least one VMNIC to an uplink port for a new distributed or standard switch
- Create the distributed port group with the same name and VLAN ID of what is created in the existing distributed or standard switch
- If a VMware VDS is created, add the VMware vSphere ESXi host to it so that the VMKernel port can be migrated between the two distributed switches. This does not apply for a standard switch

**Note:** VMKernel ports can be deleted from the VMware vSphere ESXi host if a VMNIC is not available to use for an uplink on the new distributed or standard switch.

Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client

   **Note:** You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, select Hosts and Clusters.

4. Left-click ESXi host and select the Manage tab.

5. Left-click Networking and select Virtual switches.

6. Left-click the distributed or standard switch to which the VMKernel adaptor will be migrated.

7. Left-click Migrate a VMKernel network adaptor to selected switch.

8. From the Migrate VMKernel Network Adapter wizard, perform the following:
   a. Select vcesys_esx_vmotion and click Next.
   b. Change the Network label to VCESys_esx_vmotion.
   c. Change the VLAN ID to 106 and click Next.
   d. Verify that the No Impact status appears and then click Next.
   e. Verify Ready to complete pages for correct results and click Finish.
f Wait 60 seconds and then select the VMKernel adapter link under Networking to ensure that the VCESys_esx_vmotion adapter is on the new switch.

g Repeat this step for each VMKernel network adapter.

Disassociating the VMware vSphere ESXi host from a VMware VDS

Use this procedure to disassociate the VMware vSphere ESXi host from an existing VMware vSphere Distributed Switch (VDS).

Before you begin

Verify that there are no VMs, vNIC uplinks and VMKernel ports attached to the existing VMware vSphere Distributed Switch coming from each VMware vSphere ESXi host.

Procedure

1 Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client.

   **Note:** You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

2 Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3 On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4 Right-click DVSwitch01-A and select Add and Manage Hosts.

5 From the Add and Manage Hosts wizard, perform the following:
   
a Select Remove hosts and click Next.

b Select Attached hosts.

c From the Select member hosts window, select the VMware vSphere ESXi host to be deleted and click OK.

   **Note:** You can modify multiple VMware vSphere ESXi hosts at a time using the Add and Manage Hosts wizard.

d Validate that the selected host appears in the list and click Next.

e Review the summary results window and click Finish.
Removing a VMware VDS

This section describes the required procedures for removing a VMware vSphere Distributed Switch (VDS).

Before you begin

- Uplink adapters and VMware vSphere ESXi hosts do not need to be removed to delete the VMware VDS.
- Powered on VMs cannot be attached to any distributed port groups. No VMs are permitted on any VMware vSphere ESXi hosts connect to the VMware VDS and attached to the distributed port groups.

Perform the following procedures:

1. **Migrate VM distributed port group assignments to a different switch.**
2. **Migrate VMKernel ports to a different switch.**

Migrating VM distributed port group assignments to a different switch

Use this procedure to migrate VM distributed port group assignments to a different distributed or standard switch.

About this task

This procedure is not required if there are no powered-on VMs on the distributed port group. VMs connected to the distributed port group can be powered-off to remove the distributed port group.

You can use the VM migration wizard to migrate any port group types. However, use caution when migrating the VMware vCenter Server VMs, because a disconnect can cause the loss of the VMware vCenter Server, which could prevent the VM port group from migrating.

You can use the VM migration wizard to migrate from a VMware vSphere Standard Switch (vSS) to a VMware vSphere Distributed Switch (VDS), a VMware VDS to a VMware vSS or a VMware VDS to a VMware VDS seamlessly.

Before you begin

Verify that the powered-on VMs on all VMware vSphere ESXi hosts that are attached to an existing VMware VDS are not assigned to any distributed port groups.

Verify that there is an available distributed port group to which to migrate the powered-on VMs.

Create another switch with the following criteria:

- If migrating to a different VMware vSphere Distributed Switch:
  - Attach at least one VMNIC as an uplink for a new distributed or standard switch.
Create the distributed port groups with the same name and VLAN ID as the existing switch.

- If migrating to a standard switch:
  - Create a new standard switch and attach at least one VMNIC as an uplink for the standard switch.
  - vNIC0 and vNIC1 connect to a different set of physical switches than vNIC2 and vNIC3. Do not add vNIC2 and/or vNIC3 to vSwitch0, because it could cause the VMware vSphere ESXi host to lose network connectivity if management traffic gets switched.
  - If no VMNICs are available, migrate one VMNIC from the VMware VDS. Keep the second VMNIC on the Distributed Switch for VM traffic to continue to communicate.
  - Create the VM port group with correct VLAN ID to the new standard switch.

Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client

   **Note:** You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Right-click DVswitch01-A and select Migrate VM to Another Network.

5. From the Migrate Virtual Machine Networking wizard, perform the following:
   a. Verify that Specific network is selected and click Browse.
   b. Select the Source network distributed port group or standard port group and click OK.
   c. Select Browse for the destination network.
   d. Select the distributed port group or port group where the VMs will be reassigned and click OK.
   e. Click Next.
   f. When the list of VMs appear, select the checkbox on each VM, and click Next.
   g. Validate that the source and destination is correct and click Finish. The selected VMs distributed port groups migrate to a new distributed or standard switch.
Removing VMKernel ports

Use this procedure to remove VMKernel ports after the VMs have been migrated from the VMware vSphere Distributed Switch (VDS).

Before you begin

Verify that all VMs have been migrated off the VMware VDS.

Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client

   Note: You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere Single Sign-On (SSO) account) or another administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Right-click DVswitch01-A and select Add and Manage Hosts.

5. From the Add and Manage Hosts wizard, perform the following:
   a. Select Manage host networking and click Next.
   b. Click Attach hosts.
   c. From the Select member hosts window, select the VMware vSphere ESXi hosts and click OK.
   d. Verify that the selected host has been added and click Next.
   e. From the Select network adapter tasks window, deselect Manage physical adapters so that only Manage VMKernel adapters is selected and click Next.
   f. Under On this switch, select the VMKernel port by selecting the VMKernel adapter and click Assign port group.
   g. If you need to delete VMKernel ports, under the VMKernel adapter list, select the VMKernel port and click Remove.
   h. Select the port group that belongs to a different vSwitch and click OK.
   i. Validate the VMKernel port destination and click Next.
   j. Verify that a No impact message appears and click Next.
Review the summary results and click Finish.

**Using disjoint layer 2 configuration on VMware VDS**

This section contains procedures necessary to configure disjoint layer 2 on VMware vSphere Distributed Switch (VDS).

**About this task**

To support disjoint layer 2 configurations, the following must be assigned to the VMware VDS:

- Cisco UCS vNIC 4 (10 Gb or more depending on virtual interface card (VIC) hardware)
- Cisco UCS vNIC 5 (10 Gb or more depending on VIC hardware)

A separate VMware VDS is created with two dedicated uplinks to isolate disjoint layer 2 traffic from all other primary VDS traffic. There must be a single VMware VDS created for each data center, but not for each cluster. Disjoint layer 2 is not a mandatory configuration for VMware VDS.

To configure a disjoint layer 2 configuration on a VMware VDS, perform the following:

- [Creating a VMware VDS for disjoint layer 2 configuration](#) (see page 189)
- [Creating distributed port groups for disjoint layer 2 configuration](#) (see page 190)
- [Adding the VMware vSphere ESXi hosts to the VMware VDS](#) (see page 191)

**Creating a VMware VDS for disjoint layer 2 configuration**

Use this procedure to create a VMware vSphere Distributed Switch (VDS) for disjoint layer 2 configuration.

**About this task**

On full-width blades with additional network physical ports to the onboard modular LAN on motherboard (mLOM) ports, add vNICs 4 and 5 to the service profile. This must be done individually between reboots, after installing VMware vSphere ESXi with vNIC 0-3. This is required because of the way VMware vSphere ESXi interprets the Cisco peripheral component interconnect (PCI) bus enumeration of the vNICs during installation. VMware does not support remapping the vNICs after the hypervisor is installed beginning with VMware vSphere 5.5 without a support ticket.

**Procedure**

1. From the VMware vSphere Web Client **Home** tab, under **Inventories**, select **Networking**.
2 Right-click Datacenter01 (Logical Configuration Survey (LCS) default name) and select New Distributed Switch.

**Note:** The disjoint layer 2 Cisco DVswitch naming scheme is as follows: DVswitch<VCE System ID>-DJL2

3 From the New Distributed Switch wizard, perform the following:

   a Change the name of the distributed switch to DVswitch01-DJL2 unless a different cluster name is used in the LCS.
   b Validate that the cluster location is Cluster01.
   c Click Next.
   d Select Distributed switch: 5.5.0C.
   e Click Next.
   f From the Edit Settings window, change Number of uplinks to 2.
   g Leave Network I/O Control enabled.
   h Uncheck Default port group
   i Click Next to view the Ready to complete window.
   j Review the settings and click Finish if everything is correct. Otherwise, click Back to edit changes.

4 Repeat this procedure to create a new VMware VDS for each additional workload type.

What to do next

Creating distributed port groups for disjoint layer 2 configuration (see page 190)

**Creating distributed port groups for disjoint layer 2**

Use this procedure to create distributed port groups for disjoint layer 2.

About this task

Change the load balancing policy from Route based on originating virtual port to Route based on physical NIC load for all the VMKernel distributed port groups. Disjoint layer 2 traffic is commonly virtual distributed port groups only so it would typically be configured with the default settings.

If vcesys_esx_vmotion is configured as disjoint layer 2, configure teaming and failover with vmnic4 in active state and vmnic5 in standby state.
Procedure

1. From the VMware vSphere Web Client Home tab, under Inventories, select Networking.

2. Right-click DVswitch01-DJL2 (LCS default name) and select New Distribution Port Group.

3. From the New Distributed Port Group wizard, perform the following:
   a. Change the name of the distributed port group as provided in the Logical Configuration Survey (LCS).
   b. Click Next to configure port group settings.
   c. Under Configure Settings, leave Port binding and Port allocation as default.
   d. Leave Number of Ports at 8.
   e. For VLAN type, select VLAN and change the VLAN ID to what was specified in the LCS.
   f. Click Next to view the Ready to complete window.
   g. Review the settings and click Finish if everything is correct. Otherwise, click Back to edit changes.

4. Repeat this procedure for each distributed port group that belongs to the disjoint layer 2 configuration for the VMware VDS.

What to do next

Adding the VMware vSphere ESXi hosts to the VMware VDS (see page 191)

Adding VMware vSphere ESXi hosts to VMware VDS

Use this procedure to add VMware vSphere ESXi hosts and attach a pair of VMNICs as uplinks to the disjoint layer 2 VMware vSphere Distributed Switch (VDS).

Procedure

1. From the VMware vSphere Web Client Home tab, under Inventories, select Networking.

2. Right-click DVswitch01-DJL2 (Logical Configuration Survey default name) and select Add and Manage Hosts.

3. From the Add and Manage Hosts wizard, perform the following:
   a. Select Add Hosts and click Next.
   b. Click (+) New Hosts.
   c. Select the VMware vSphere ESXi host for VMware VDS and click OK.
d Validate that the selected host appears and then click Next.

e From the Select network adapter tasks window, verify that Manage physical adapters and Manage VMKernel adapters are checked and click Next.

f Select vmnic4 and click Assign uplink.

g Select Uplink 3 and click OK.

h Select vmnic5 and click Assign uplink.

i Select Uplink 4 and click OK.

j Click Next.

k Click Next to view the Ready to complete window.

l Review the settings and click Finish if everything is correct. Otherwise, click Back to edit changes.

4 Add the VMkernel distributed port groups (vMotion, NFS) only if they belong to the disjoint layer 2 traffic. Otherwise, click Next and go to step 5.

a From the Manage VMKernel network adapters window, verify that the host is selected and click (+) New adapter.

b From the Add Networking wizard, select a distributed port group and click Browse.

c Select vcesys_esx_vmotion and click OK.

d Click Next.

e Check vMotion traffic and click Next.

f Select Use static IP4 settings and apply IPv4 address/Subnet Mask as specified in the LCS.

g Click Next to view the Ready to complete window.

h Review the settings and click Finish if everything is correct. Otherwise, click Back to edit changes.

i Repeat this step to create the vcesys_esx_nfs port group. Do not select any checkboxes.

Note: vcesys_esx_nfs port group has a default MTU of 1500. The MTU must be set to 9000.

j Click Next.

5 Verify that the status appears as: No Impact and click Next. If there is a problem with the output, click Back to return to the previous window.

6 Review the Summary results and click Finish.
7 Repeat this procedure for the remaining VMware vSphere ESXi hosts.

Back up and restore a VMware VDS data configuration

When you export a backup of the DVswitch configurations, a zip file is created. The import feature will not overwrite the existing dvSwitch(s) and instead create a separate one. The restore feature will overwrite the existing dvSwitch currently in use. Each feature is broken out by administrative procedures.

Exporting a backup of a VMware dvSwitch configuration

Use this procedure to export the configuration of the VMware vSphere Distributed Switch (VDS) dvSwitch configuration into a zip file.

About this task

The VMware dvSwitch configuration includes all the VMware VDS and distributed port group’s configuration settings.

Before you begin

Verify that the VMware VDS is configured.

Procedure

1 Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client

   Note: You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

2 Login to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3 On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4 Right-click DVSwitch01-A and select All vCenter Action > Export Configuration.

5 Choose one of the following:
   – Distributed switch configuration and all port groups
   – Distributed switch only

6 In the Descriptions field, type DVswitch01-A and click OK.

7 Click Yes to save the configuration file.
Importing a backup of a VMware dvSwitch configuration

This procedure creates a VMware vSphere Distributed Switch (VDS) from an exported configuration file using the same switch and distributed port group configuration. This does not override the existing VMware VDS.

Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client

   Note: You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

2. Login to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere Single Sign-On (SSO) account) or another administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Right-click Datacenter and select All vCenter Actions > Import Distributed Switch.

5. Click Browse to select Select a distributed switch backup file.

6. Select Preserve original distributed switch and port group identifiers.

7. Click Next.

8. Review the import settings and click Finish.

Restoring a backup of a VMware dvSwitch configuration

This procedure resets the configuration of an existing VMware vSphere Distributed Switch (VDS) to the settings in the configuration file.

About this task

Restoring a VMware VDS changes the settings on the selected switch back to the settings saved in the configuration file. Restoring a backup of the VMware dvSwitch configuration resets the existing VMware VDS configuration to the settings in the configuration file and destroy the existing VMware VDS.

Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client

   Note: You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.
2. Login to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Right-click the VMware VDS to be restored and select All vCenter Actions > Restore Configuration.

5. Select Restore distributed switch or port groups or Restore distributed switch only.

6. Click Browse to select Select a distributed switch backup file and click Next.

7. Review the import settings and click Finish.

**Basic troubleshooting**

This section provides a list of procedures that can be used to troubleshoot a VMware vSphere Distributed Switch (VDS).

For network health check, refer to the following procedures:

- Enable vSphere Distributed Switch Health Check
- View vSphere Distributed Switch Health Check Information

For managing network rollback, refer to the following procedures:

- Host Networking Rollback
- vSphere Distributed Switch Rollback
- Disable Rollback

For managing network recovery, refer to Resolve Errors in the Management Network Configuration on a vSphere Distributed Switch.

**Related information**

VMware vSphere Networking guide
Managing the Cisco Nexus 1000V Series Switch

Managing licenses

Use this procedure to manage licenses for the Cisco Nexus 1000V Switch.

For instructions on how install and configure a license for the Cisco Nexus 1000V Switch, refer to the *Cisco Nexus 1000V License Configuration Guide* for your release.

Related information

*Cisco Nexus 1000V License Configuration Guide*

Adding hosts

Use this procedure to add hosts to the Cisco Nexus 1000V Switch.

For instructions on how to add hosts, refer to the *Cisco Nexus 1000V VEM Software Installation and Upgrade Guide* for your release.

Related information

*Cisco Nexus 1000V VEM Software Installation and Upgrade Guide*

Creating a port profile

Use this procedure to create a port profile on the Cisco Nexus 1000V Switch.

About this task

Management settings should not be changed without VCE approval. This content is for example purposes only.

Procedure

1. Log on to the Cisco Nexus 1000V VSM.
2. To start the configuration, type: `n1000v# config t`
3. To specify the port profile name, type: `n1000v(config)# port-profile type vethernet port-profile-name`
4. To designate the interfaces as an access port, type: `n1000v(config-port-prof)# switchport mode access`
To grant access, type: `n1000v(config-port-prof)# switchport access vlan vlan-id`

To specify the port group, type: `n1000v(config-port-prof)# vmware port-group`

To confirm that the port profile is created, type: `n1000v(config-port-prof)# show port-profile name name`

You can view the port profile in VMware vCenter by navigating to Inventory > Networking. The left side of the window displays the port profile you created.

To save the configuration: `n1000v(config)# copy run start`

Related information

Cisco Nexus 1000V Port Profile Configuration Guide

Modifying the uplink port profile

Use this procedure to modify the uplink port profile.

About this task

This procedure modifies the trunk that runs northbound from the Cisco Nexus 1000V Switch through the Cisco UCS vNICs to the Cisco UCS fabric interconnect. This carries VSM to Virtual Ethernet Module (VEM) traffic, service console and VMKernel, and VM data traffic. VLAN numbers and IP addresses referenced in this procedure are recommended by VCE. If the customer uses a naming convention that differs from what is recommended, refer to the Logical Configuration Guide.

When you modify the uplink port profile, northbound traffic from the Cisco Nexus 1000V Switch through the Cisco UCS fabric interconnect is affected.

Before you begin

- Verify that VLANs on uplinks exist in Cisco UCS and in the aggregation switches.
- Verify the use of jumbo frames.
- Obtain the IP address of the Cisco Nexus 1000V Switch VSM.

Procedure

1. Log on to the VSM.
2. Type: `configure terminal`
To use jumbo frames, type:

```
    system mtu 9000
    port-profile type ethernet DATA-UPLINK
    vmware port-group
```

Type `port-profile type ethernet DATA-UPLINK`

Type: `vmware port-group`

Depending on your Vblock System, perform the following:

<table>
<thead>
<tr>
<th>For this Vblock System...</th>
<th>Type the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified</td>
<td><code>switchport trunk allowed vlan 105-107, 109, 116-117, 201, 209</code></td>
</tr>
<tr>
<td></td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td><code>&lt;ESX mgmt vlan number&gt;, &lt;vMotion vlan number&gt;, &lt;ESX Fault Tolerance vlan number&gt;, &lt;ESX NFS vlan number&gt;, &lt;N1K L3 Control VLAN number&gt;, &lt;L3 vmotion VLAN number&gt;, &lt;Customer Data vlan number&gt;, &lt;customer CIFS vlan&gt;</code></td>
</tr>
<tr>
<td>Block</td>
<td><code>switchport trunk allowed vlan 105-107, 116-117, 201</code></td>
</tr>
<tr>
<td></td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td><code>&lt;ESX mgmt vlan number&gt;, &lt;vMotion vlan number&gt;, &lt;ESX Fault Tolerance vlan number&gt;, &lt;N1K L3 Control VLAN number&gt;, &lt;L3 vmotion VLAN number&gt;, &lt;Customer Data VLAN number&gt;</code></td>
</tr>
</tbody>
</table>

Type:

```
    channel-group auto mode on mac-pinning
    no shutdown
```
8 Perform the following:

<table>
<thead>
<tr>
<th>For this Vblock System...</th>
<th>Type the following...</th>
</tr>
</thead>
</table>
| Unified                   | system vlan 105-107, 109, 116-117  
OR  
<ESX mgmt vlan number>, <vMotion vlan number>, <FT vlan number>, <ESX NFS vlan number>, <N1K L3 Control VLAN number>, <L3 vmotion VLAN number> |
| Block                     | system vlan 105-107,116-117  
OR  
<ESX mgmt vlan number>, <vMotion vlan number>, <FT vlan number>, <N1K L3 Control VLAN number>, <L3 vmotion VLAN number> |

9 Perform the following:

<table>
<thead>
<tr>
<th>For this Vblock System...</th>
<th>Type the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified</td>
<td>mtu 9000</td>
</tr>
<tr>
<td>Block</td>
<td>mtu 9000 (to use jumbo frames)</td>
</tr>
</tbody>
</table>

10 Type:

state enabled

copy run start

11 To verify this procedure, view the uplinks created under the Cisco Nexus 1000V Switch in the production VMware vCenter. Select Inventory > Networking.

Reversing the procedure

Procedure

1 Log on to the VSM.

2 Type:

configure terminal

no port-profile type ethernet DATA-UPLINK

copy run start

deck
Modifying vEthernet data port profiles

Use this procedure to modify data port profiles for VMware VM traffic, MGMT, VMotion, Fault Tolerance, NFS, and VSM Layer 3 Control.
Procedure

1. To modify the data port profiles for VMware VM traffic, MGMT, VMotion, Fault Tolerance, NFS, and VSM Layer 3 Control, type the following commands:

    port-profile type vethernet VM-DATA-201
    vmware port-group
    switchport mode access
    switchport access vlan 201 or <Customer Data VLAN number>
    no shutdown
    state enabled
    copy run start

    port-profile type vethernet VCESYS_ESX_MGMT
    vmware port-group
    switchport mode access
    switchport access vlan 105 or <ESX mgmt vlan number>
    no shutdown
    pinning id 0
    system vlan 105 or <ESX mgmt vlan number>
    service-policy type qos input SET_COS_6
    state enabled
    copy run start

    /* For vSphere 5.x only */

    port-profile type vethernet VCESYS_ESX_VMOTION
    vmware port-group
    switchport mode access
    switchport access vlan 106 or <vMotion vlan number>
    no shutdown
    pinning id 0
    system vlan 106 or <vMotion vlan number>
    service-policy type qos input SET_COS_4
    state enabled
    copy run start

    /*******************************

    /* For vSphere 6.0 or later */

    port-profile type vethernet VCESYS_ESX_L3VMOTION
    vmware port-group
    switchport mode access
    switchport access vlan 117 or <L3 vMotion vlan number>
    no shutdown
    pinning id 0
    system vlan 117 or <L3 vMotion vlan number>
    service-policy type qos input SET_COS_4
    state enabled
    copy run start

    port-profile type vethernet VCESYS_ESX_FT
    vmware port-group
    switchport mode access
    switchport access vlan 107 or <FT vlan number>
    no shutdown
    pinning id 0
    system vlan 107 or <FT vlan number>
    state enabled
copy run start

/***********************/

/* For Unified Systems */

port-profile type vethernet VCESYS_ESX_NFS-Fab-A
vmware port-group
switchport mode access
switchport access vlan 109 or <ESX NFS vlan number>
no shutdown
pinning id 0
system vlan 109 or <ESX NFS vlan number>
service-policy type qos input SET_COS_2
state enabled

port-profile type vethernet VCESYS_ESX_NFS-Fab-B
vmware port-group
switchport mode access
switchport access vlan 109 or <ESX NFS vlan number>
no shutdown
pinning id 1
system vlan 109 or <ESX NFS vlan number>
service-policy type qos input SET_COS_2
state enabled

/*********************/

port-profile type vethernet VCESYS_N1K_L3CONTROL
vmware port-group
switchport mode access
switchport access vlan 116 or <N1K_L3_Control vlan number>
no shutdown
pinning id 0
capability l3control
system vlan 116 or <N1K_L3_Control vlan number>
state enabled

copy run start
To verify the procedure, view the (VM facing) port groups in VMware VCenter. In the following example, the green icon represents UPLINK, and the blue icon represents the VM facing port group:

![Port Groups Screenshot](image)

Modifying the QoS settings

Use this procedure to modify QoS settings on the Cisco Nexus 1000V Switch and mark the service console and VMKernel traffic with the appropriate QoS.

About this task

Policing and prioritization of traffic are implemented only when a policy map is applied to an interface. The only exception is that by default, the QoS value for control and packet VLAN traffic is set to six. This value can be overridden with an explicit QoS policy configured on the interface that carries the control and packet VLAN traffic.

If the VSM VMs are not hosted on the VEM in an VMware vSphere ESXi host that it is managing (for example, the VSM VMs are hosted on separate VMware vSphere ESXi hosts running the regular VMware vSwitch), packets from the VSM are not covered by the QoS policies configured on the Cisco Nexus 1000V DVS. To ensure proper QoS treatment, the VSM packets configure and attach QoS policy on the switchports of the physical switches connected the VMware vSphere ESXi hosts where the VSM VMs are hosted.

This QoS policy colors and marks the control packets only. The upstream switches must be configured with the proper QoS per-hop-behavior to ensure differentiated services.

Procedure

1. Log on to the Cisco Nexus 1000V Switch.
2 Type: `config t`

3 Perform the following:

<table>
<thead>
<tr>
<th>For the Vblock System:</th>
<th>Type:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified</td>
<td>policy-map type qos SET_COS_2</td>
</tr>
<tr>
<td></td>
<td>class class-default</td>
</tr>
<tr>
<td></td>
<td>set cos 2</td>
</tr>
<tr>
<td></td>
<td>policy-map type qos SET_COS_4</td>
</tr>
<tr>
<td></td>
<td>class class-default</td>
</tr>
<tr>
<td></td>
<td>set cos 4</td>
</tr>
<tr>
<td></td>
<td>policy-map type qos SET_COS_6</td>
</tr>
<tr>
<td></td>
<td>class class-default</td>
</tr>
<tr>
<td></td>
<td>set cos 6</td>
</tr>
<tr>
<td>Block</td>
<td>policy-map type qos SET_COS_4</td>
</tr>
<tr>
<td></td>
<td>class class-default</td>
</tr>
<tr>
<td></td>
<td>set cos 4</td>
</tr>
<tr>
<td></td>
<td>policy-map type qos SET_COS_6</td>
</tr>
<tr>
<td></td>
<td>class class-default</td>
</tr>
<tr>
<td></td>
<td>set cos 6</td>
</tr>
</tbody>
</table>

**Upgrading the VEM software**

Use this procedure to upgrade the Cisco Nexus 1000V Switch virtual Ethernet module (VEM) software.

For instructions on performing the upgrade, refer to *Cisco Nexus 1000V VEM Software Installation and Upgrade Guide* for your release.

**Related information**

*Cisco Nexus 1000V VEM Software Installation and Upgrade Guide*
Troubleshooting the Cisco Nexus 1000V Switch

Use this procedure to obtain troubleshooting information the Cisco Nexus 1000V Switch.

For troubleshooting information and procedures for the Cisco Nexus 1000V Switch, refer to the Cisco Nexus 1000V Troubleshooting Guide for your release.

Related information

Cisco Nexus 1000V Troubleshooting Guide
Deploying and provisioning a service offering

Use this procedure to deploy and provision a host for the service offering.

About this task

Note: This procedure is applicable to EMC Ionix UIM/P 3.0 only.

EMC Ionix UIM/P services are managed through service profiles comprised of Server, Network, and Storage profiles. The service offerings are the templates for the service profiles and provide the default settings for the Server, Network, and Storage profiles contained within the profile. The service offering further defines whether the service can be used to install a supported operating system on the blades once the service is activated.

When the service offering is complete and marked available, it is added to the Service Catalog for service planning. After the service is created, service profiles can be customized from the Service Manager and the service can be provisioned.

Before you begin

Before you can manage a service offering, refer to EMC® Ionix™ Unified Infrastructure Manager/ Provisioning Version 3.0 Online Help (Administration and User Guide) P/N 300-012-615 REV A01 at support.emc.com to:

- Verify that the VMware vSphere ESXi Operating System ISO has already been uploaded into EMC Ionix UIM.
- Successfully discover the Vblock System. During discovery EMC Ionix UIM/P pulls in the Cisco UCS blade (servers) information and the storage pools created in Unisphere for VMAX into the EMC Ionix UIM/P database.
- Grade the blades and mark them available for EMC Ionix UIM/P to use in services.
- Grade the storage pools and mark them available for EMC Ionix UIM/P to use in services.
- Define the network profiles.
- To create the pools, use EMC UIM/P 3.x to:
  - Add a MAC address range.
  - Add a UUID range.
  - Add a WWNN range.
  - Add a WWPN range.
  - EMC Ionix UIM/P 3.1: add IP pools and ranges (required)
- Create the service offering and mark it available.
Procedure

1. Log in to EMC Ionix UIM.
2. From the Administration view, select the Service Catalog tab.
3. Select an available server offering and click Create Service.
4. From the Create Service from Service Offering window, type a Service Name and Description, select the Discovered Vblock and click OK. You are automatically redirected to the Edit Service window.
5. To change the service, click Edit.
6. Select a tab and click Edit to make changes to those sections of the service.
   
   Note: On the vCenter Cluster tab, the Set Password button is for changing the password for accessing vCenter. This is different from the Set Password button used within the Operating System tab.

7. Click Close when you are done making edits.
8. To provision the host, from the Administration view, select the Service Manager tab.
9. Select the desired service and click Provision.
10. After a service has provisioned successfully, select the service and click the Activate button to activate the host.

What to do next

Refer to the EMC® Ionix™ Unified Infrastructure Manager/Provisioning Online Help Administration Guide to establish connectivity to the VMware vCenter servers and vCloud directors.

Related information

- Adding a MAC address range (see page 22)
- Adding a UUID range (see page 17)
- Adding a WWNN range (see page 18)
- Adding a WWPN range (see page 20)
- Accessing VCE documentation (see page 11)
Managing the AMP

Upgrading the Cisco UCS C220 Server

Use this procedure to prepare the ISO for a remote upgrade using KVM.

Before you begin

If upgrading a Cisco UCS C220 Server in an HA AMP, migrate VMs off the host being upgraded before running the upgrade procedure. Refer to the Cisco Host Upgrade Utility Release 1.4(4) Quick Start Guide for Cisco UCS C-Series Rack Servers.

Find the ISO file download for your server online and download it to a temporary location accessible from the Cisco UCS C220 Server being upgraded.

**Note:** If upgrading a Cisco UCS Server on a mini-AMP, management access to the Vblock System is lost. Verify that the AMP VMs come back up and specific application services restart for database servers, the VMware vCenter server, and associated VUM servers.

Procedure

1. Use a browser to navigate to the CIMC Manager software on the server that you are upgrading.
   a. Type the CIMC IP address for the server in the address field of the browser.
   b. Type your username and password.
   c. From the toolbar, click **Launch KVM Console**.
   d. The access method for the virtual media depends on the version of the KVM console that you are using. If the KVM Console window has a virtual media (VM) tab, select that tab. Otherwise, select **Tools** > **Launch Virtual Media**.
   e. Click **Add Image** and select the downloaded ISO file.
   f. In the **Client View**, select the checkbox in the **Mapped** column for the ISO file that you added and then wait for mapping to complete. The KVM displays the progress in the Details section.
   g. Verify the ISO file appears as a mapped remote device.
   h. Boot the server and press **F6** when prompted to open the **Boot Menu** screen.

2. On the **Boot Menu** screen, select **Cisco vKVM-Mapped vDVD1.22** and press **Enter**. The server reboots from the selected device.

3. When the server BIOS and CIMC firmware versions appear, at the **Have you read the Cisco EULA?** prompt, select **I agree**.

**Note:** EULA=end user license agreement.
4 From the Host Upgrade Menu, select Update All.

5 At the Confirmation screen, select Yes.

6 From the Confirmation screen for the BIOS Update, select Yes.

7 After reboot is complete, verify that all VMs are powered up and have access to the VMware vCenter Server.

Related information

Cisco Host Upgrade Utility Release 1.4(4) Quick Start Guide for Cisco UCS C-Series Rack Servers

Cisco Host Upgrade Utility 1.5(1) User Guide

Upgrading the Cisco Catalyst switch software on the AMP

Use this procedure to upgrade the Cisco IOS software on a Cisco switch.

Before you begin

- Verify that you have a Cisco account to download images.
- Review the release notes before any upgrade.
- An SCP, TFTP, FTP, or SFTP server is required to upload the IOS image to the router.

VCE recommends that you:

- Back up the original configuration.
- After you have verified that the configuration has been updated successfully, create a backup of the new configuration.

Procedure

1 Request Cisco access and a username for the Cisco Support website.

2 After access is granted, go to the Cisco Support website.

3 From the Select a Task list, click Download Software.

4 Select the switch series and model, and then select IOS Software.

5 Select the supported software version, and click Download Now.

6 Download the file to the appropriate copy server (TFTP, SCP, FTP, or SFTP).
7 To create a backup of the running configuration and save it on a remote file copy server, type:
Switch# copy startup-config [tftp:|SCP|FTP|SFTP]

8 To verify that the router has sufficient RAM space for the new image, type: show flash

The system lists the contents of the flash:

```
Directory of flash:
  440  -rwx        6505  Aug 19 1993 16:50:47 -07:00  config.text
  2   -rwx        1216  Aug 15 1993 16:34:24 -07:00  vlan.dat
  441  -rwx 18629690  Sep 14 1993 16:48:22 -07:00  c3560e-universalk9-mz.150-
        1.SE.bin
  442  -rwx        3096  Aug 19 1993 16:50:47 -07:00  multiple-fs
  443  -rwx        1931  Aug 19 1993 16:50:47 -07:00  private-config.text
 3 drwx         512  Feb 28 1993 16:14:01 -08:00  c3560e-universalk9-mz.122-
        55.SE1
57671680 bytes total (20904960 bytes free)
VSJ3X2C3560A#
```

9 If there is not enough space, delete the current image.

10 To save the configuration, type: copy run start

11 To copy the new image to the flash directory in router, type: VSJ3X2C3560A# copy ftp://ftp://

```
Address or name of remote host [10.10.1.39]?
Source filename [c3560e-universalk9-mz.150-1.SE.bin]?
Destination filename [c3560e-universalk9-mz.122-55.SE1]
```

12 To update the configuration to boot from the new image, type: VSJ3X2C3560A# config t

```
Enter configuration commands, one per line. End with CNTL/Z.
VSJ3X2C3560A(config)#boot system flash:/c3560e-universalk9-mz.150-1.SE.bin]
```
To verify the configuration register is 0x2102 (or 0xF for the 3560 model) use the show version command and view the last line of the output, type: VSJ3X2C3560A# sh ver
14 Create a backup of the new configuration.

15 Restart the switch.

16 To verify the upgrade, type: `Show Version`

### Reversing the procedure

**Procedure**

1. To remove the boot system flash command for the new image, type:

   ```
   no boot system flash:/newimagename
   ```

2. Type the boot system flash command for the old image:

   ```
   boot system flash:/oldimagename
   ```

### Backing up the AMP

#### Creating an instance of the configuration repository

Use this procedure to build the environment to support capture of Vblock System configuration files for change management and recovery.

**About this task**

This process is required to support the recovery of the Cisco network devices that comprise the Vblock System.

VCE recommends that you establish a process to perform network device configuration backups and that you place the repository on the AMP VM that hosts the fabric manager service.

**Before you begin**

- Access a copy of the PuTTY software used to verify device connectivity and login credentials
- Access a copy of the TFTP server software that provides a method to accept a remote copy of device configuration files
- Identify the VM within the AMP deployment where the repository is to be created
Monitor disk storage resources to prevent overuse issues and data unavailability

Procedure

1. To create the backup directory, type: \Cisco.

   VCE recommends using the D:\ drive, however, if the D:\ drive is not available, use the C:\ drive. This drive is referenced throughout these instructions.

2. Create the named devices and data subdirectories. It is recommended that you create one set of empty subdirectories and then copy them to the other device directories. The directory names are the major model numbers with 00 substituted for the last two digits of the device model.

   Note: The list of device models is provided as an example. Create only the entries needed to support the Vblock System being deployed.

3. Install the TFTP server.

4. To configure the TFTP server, in the home directory is the location created above \Cisco, restrict read/write access to the IP range of devices sending configuration files.

5. To verify the procedure, monitor the config directories for entries copied from the network devices in the Vblock System.

What to do next

Initiate network device configuration backups.

Creating a backup of a configuration repository

Use this procedure to create a backup of the host(s) where Cisco network device configuration files are stored.

About this task

When you create a backup of a configuration repository, the recovery of the Cisco network devices such as Cisco fabric interconnect and Cisco switches are supported.

VCE recommends establishing a process to perform host backups that allow file-level restores.

Before you begin

- Verify that the configuration backup repository exists with regularly scheduled tasks to keep it up to date
- Verify the location of the host repository.

Make sure to monitor disk storage resources to prevent overuse issues and data unavailability.
Procedure
Refer to the documentation supplied by the backup vendor for this procedure.

What to do next
Establish a procedure to restore a single configuration file, the entire repository, and the supporting process to populate it, or restore the complete host where the repository exists.

Restoring a configuration file
Use this procedure to restore a network or storage device configuration file in the event of failure, corruption, or other data loss event.

About this task
VCE recommends following the vendor recommended restore processes for the device.

Before you begin
- Verify that local or remote connectivity exists to the impacted device.
- Access the configuration file needed to restore operational status.
- Obtain a method to transfer the configuration file from the source location to the impacted device whether it be FTP, or copy and paste.

Procedure
To restore a configuration file, refer to the documentation provided with the vendor to restore the device.

Backing up targets
Use this procedure to back up targets that are in AMP and the Vblock System.

About this task
VCE recommends that you:
- Perform daily backups of all VMs at 7 A.M. and 7 P.M.
- Perform daily backups of the VMware vCenter SQL Server database every four hours. This coincides with server daily backups at 3, 7, 11 A.M. and 3, 7, 11 P.M.
- Set the retention value set to 35 days.

Disk storage resources should be monitored to prevent overuse issues and data unavailability.
If for some reason AMP is lost, the AMP servers must be stored on the backup media to be installed otherwise you will be unable, or severely limited, in the ability to manage or recover the Vblock System. AMP servers are:

- VMware vCenter Server
- VMware vCenter SQL database
- VMware vCenter Update Manager
- Jump
- Array management
- Fabric manager services
- Other Servers created to manage Vblock System
- Other VMs identified as part of the Core or VCE Optional workloads to manage the Vblock System

You must perform configuration backups for these AMP devices:

- Cisco network (28xx/29xx) router (optional)
- Cisco network (35xx/37xx) switches
- EMC storage: VNXe

To back up targets in AMP and the Vblock System, refer to the documentation provided with the backup tool vendor.
Configuring external hosts

This section describes how to configure external hosts to the Vblock System 700 series.

The Vblock System provides predictable and scalable performance as a proven, converged infrastructure system. Vblock System 700 series components such as network switches, SAN switches, or storage arrays are not designed to be shared outside the Vblock System. However, customers may want to leverage the Vblock System 700 series storage infrastructure with external hosts.

Risks and considerations

This section describes the risks and considerations for configuring external hosts.

Vblock System environments are designed and engineered for optimal performance by dedicating and leveraging internal components for the exclusive use of the Vblock System. While it is technically feasible to permanently leverage Vblock System resources by systems that are external to the Vblock System as outlined in this document, it will add complexity to the environment and may limit the performance, expandability, and supportability of the Vblock System.

If permanent, external connectivity is established, VCE can only provide reasonable effort support for troubleshooting Vblock System performance issues. VCE may need to disconnect external connectivity to determine if the Vblock System is functioning correctly.

VCE reasonable effort support enables VCE to accept seamless support customer calls where VCE will determine the Vblock System is operating correctly, and assist in problem resolution to the best possible extent. It should be noted that VCE has not certified any external use of Vblock System resources and customers will need to address external support issues with the appropriate vendor.

The VCE System Release Certification Matrix contains information about the supported code levels for the Vblock System.

External component compatibility

Before external hosts can connect to the Vblock System, verify with the customer that the following items are compatible:

- SAN switch hardware and firmware
- Server HBA/firmware/drivers
- Server operating system

When external hosts connect to the Vblock System, unsupported components within the external host may be inconsistent with the design and testing of the Vblock System. Customers risk that their external applications will be incompatible with Vblock System code levels if there is an upgrade to the Vblock System.

The VCE System Release Certification Matrix contains information about the supported code levels.
Vblock System management

Customers must consider the risk of managing external hosts from a single interface and the potential negative impact on the common hardware resources.

EMC VMAX is managed with EMC SMC/Unisphere. EMC SMC/Unisphere provides a single interface that can be partitioned with users and roles. However, VCE has not tested the impact of adding users and roles within the EMC SMC/Unisphere interface on provisioning tools such as EMC UIM.

In a Vblock System configuration, external hosts can access any device, even devices assigned to the Vblock System. You could simultaneously allocate a device to a Vblock System host and an external host thereby causing a risk to data integrity. This could corrupt Vblock System application data or the external host application data.

Hardware isolation

The Vblock System shares common hardware resources that are not easily isolated and managed. Isolating hardware can add complexity to growth and scalability of the Vblock System storage resources and external host storage. Use dynamic cache partitioning and EMC Symmetrix priority controls to segregate cache resources. If dynamic cache partitioning and EMC Symmetrix priority controls are incorrectly applied, there can be an adverse impact on the performance of the Vblock System and external hosts. Controls need to be understood and applied to external host workloads.

Each Vblock System and external host is unique. There is no consistent rule to apply to the Vblock System for external host connectivity. Once controls are in place, active monitoring is essential so that fine tuning adjustments can be made. Support from EMC Professional Services may be required for Dynamic Cache Partitioning.

External host connectivity

This section describes the rules for external host connectivity.

External host connectivity is not consistent with the design of the Vblock System. If a customer wants to connect the Vblock System to an external host in a manner inconsistent with the design, testing, and current RCM, VCE will acknowledge the request. In order for VCE to do this, the customer must accept the rule sets outlined in the following sections.

Ports

VCE recommends the following rule sets for ports:

- A determined number of director CPU pairs and their front-end ports will be dedicated on the EMC VMAX array in a Vblock System for external host access. Other director CPUs are dedicated and assigned to Vblock System hosts.
  - A single director CPU consists of two ports. For example, 1h:0, 1h:1. (1 indicates the director number, h indicates the CPU, and 0 or 1 indicates the port)
  - An example of a pair of director CPUs is: 1h:0, 1h:1, 2h:0, 2h:1 (a total of four front-end ports per a pair of director CPUs)
• CPU pairs should come from different engines and be assigned to different SAN fabrics. An understanding of the EMC VMAX engine layout is required.

• Front-end ports dedicated to the external host will be connected to the customer's existing SAN. The customer is responsible for:
  — Ensuring that the SAN and the EMC Enginuity code are compatible with the Vblock System as specified by the VCE RCM
  — Ensuring that all configurations within their SAN allow proper access to the dedicated, front-end ports (for example, SAN switch settings and zoning)
  — Specific configuration of the dedicated, front-end ports (for example, port flags such as virtual bus addressing or SPC2)

• Front-end ports dedicated to the Vblock System will be connected to the internal SAN of the Vblock System

**Dedicated disk groups**

VCE recommends the following rules for dedicated disk groups:

• Dedicated disk groups are allocated to, and used exclusively by the Vblock System. The storage LUNs presented from the dedicated disk groups will be accessed exclusively through the dedicated, front-end ports

• Dedicated disk groups are allocated to non-Vblock System or external servers, and used exclusively by non-Vblock System servers. Storage LUNs presented from these groups shall be accessed exclusively through the previously dedicated, front-end ports for external servers. The customer is responsible for the configuration of the storage within these dedicated disk groups (for example, storage pool creation, TDAT creation and assignment, TDEV creation and assignment, masking views)

**SAN connections**

VCE recommends the following rules sets for SAN connections:

• Use of Inter Switch Links (ISLs) between the Vblock System SAN and external SAN is prohibited. Non-Vblock System or external servers directly connected to the Vblock System SAN switch for purposes not specifically authorized by VCE, is prohibited.

• The external IP network or SAN components serving the external servers must be maintained at a code level compatible with the RCM.

The *VCE System Release Certification Matrix* contains information about the supported code levels for the Vblock System.

**Storage array**

The Vblock System storage array must be maintained at a compatible level of firmware (EMC Enginuity).
The VCE System Release Certification Matrix contains information about the supported code levels for the Vblock System.

**Third party tools**

Third party provisioning tools such as EMC UIM/P may have limited functionality or restrictions within this shared environment. Third party provisioning tools behavior may differ in an environment where storage devices are maintained exclusively for the Vblock System.

**Open systems**

Only open systems are allowed for external host connectivity. IBM System z and IBM iSeries hosts are not supported because of the levels of expertise and support that cannot be provided by VCE within a Vblock System. IBM iSeries requires specially formatted disk drives not sold by VCE and cannot be used by resources. Both IBM Mainframe and IBM iSeries hosts are characterized by very high input/output rates that can be counterproductive to the resource needs of the internal Vblock System hosts.

**Overall support criteria**

This section describes the overall support criteria for configuring external hosts.

For VCE to support external hosts on the Vblock System:

- No more than 25 percent of the overall storage capacity of the Vblock System can be allotted for external hosts.
- No more than 25 percent of the overall workload on the array can be used for external hosts. This includes metrics such as IOPS and front-end adapter (FA) port assignments.
- The following table shows the maximum allowed external connectivity FA CPU allocation limited for engines:

<table>
<thead>
<tr>
<th>Engines</th>
<th>Maximum external connectivity FA CPU allocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single</td>
<td>Requires an exception</td>
</tr>
<tr>
<td>Two</td>
<td>2 FA CPU (for example, 7h:0/1 and 10h:0/1)</td>
</tr>
<tr>
<td>Three</td>
<td>2 FA CPU</td>
</tr>
<tr>
<td>Four</td>
<td>4 FA CPU</td>
</tr>
<tr>
<td>Five</td>
<td>4 FA CPU</td>
</tr>
<tr>
<td>Six</td>
<td>6 FA CPU</td>
</tr>
<tr>
<td>Seven</td>
<td>6 FA CPU</td>
</tr>
<tr>
<td>Eight</td>
<td>6 FA CPU</td>
</tr>
</tbody>
</table>

- Only Fibre Channel (FC) connectivity is supported for external hosts. iSCSI, FICON, and FCoE are not supported
• The Vblock System 720 with EMC VMAX 10K single engine requires an impact assessment from VCE, including a review of the proposed connectivity and workload

• Two engine configurations with external host connectivity will have required scalability limitations and may not provide future connectivity for EMC VG Gateway or EMC RecoverPoint. If this is an issue, consider adding more engines. Obtain an RPQ so that the customer understands that they cannot connect these components without support or instruction

• **NO** support or SLAs (performance or availability) will be provided for external hosts or switches

• All storage resources should be considered in the same manner as done with bare metal (separate disk groups, pools, LUNs)
Guidelines for backing up applications and data
Guidelines for backing up configuration files

Backing up configuration files


For information about performing these tasks, refer to:

Procedure

- VCE Vision™ Intelligent Operations Administration Guide
- VCE Vision™ Intelligent Operations online help that is bundled with the software

Related information

Accessing VCE documentation (see page 11)

Backing up network devices running Cisco NX-OS software

Use this procedure to create a configuration file to back up network devices using Cisco NX-OS operating systems.

About this task
This procedure does not apply to the Cisco Catalyst switches. To back up those devices, use a method such as an expect script or CatTools.

Before you begin
This solution is based on the presence of the TFTP service and therefore, must be installed, configured, and active, on the AMP or AMP-2 server where the configuration repository exists.

- Verify that an instance of the configuration repository exists.
- Obtain:
  - Login credentials for device configuration backup
  - Network IP address of the configuration backup repository
  - Device name and type that matches the model abbreviation used to create the repository sub-directory structure (for example, 9500, 4900, 2900)
Procedure

1. Log in to the device account using administrator privileges.

2. To confirm that the scheduler feature is enabled, type: `SWITCH# show feature | include scheduler`

   | scheduler     | 1       | enabled |

3. From the network device, to create the backup task, type:

   ```
   SWITCH# conf t
   SWITCH(config)# scheduler aaa-authentication username login password
   SWITCH(config)# scheduler job name cfgBackup
   SWITCH(config-job)# copy startup-config tftp://IP/device/config/ cdevice_startup_$(TIMESTAMP).cfg
   SWITCH(config-job)# copy running-config tftp://IP/device/config/ name_running_$(TIMESTAMP).cfg
   SWITCH(config-job)# end
   ```

   `SWITCH#`

   **Note:** Because of routing requirements, it may be necessary to add VPN routing and forwarding (VRF) management to the end of each copy command. The variable `$(TIMESTAMP)` included in the file name inserts the date/time into the file name when the tasks are executed.
4 To schedule the backup task, type:

```
SWITCH# conf t
SWITCH(config)# scheduler schedule name Daily0600
SWITCH(config-schedule)# time daily 06:00
SWITCH(config-schedule)# job name cfgBackup
SWITCH(config-schedule)# end
SWITCH#
```

```
SWITCH# conf t
SWITCH(config)# scheduler schedule name Daily1800
SWITCH(config-schedule)# time daily 18:00
SWITCH(config-schedule)# job name cfgBackup
SWITCH(config-schedule)# end
SWITCH#
```

5 To confirm the scheduler update, type: SWITCH# show scheduler config

```text
config terminal
feature scheduler
scheduler logfile size 16
end
cfg terminal
scheduler job name cfgBackup
copy startup-config tftp://192.168.1.93/9500/config/D01-9500-01_startup_$(TIMESTAMP).cfg
copy running-config tftp://192.168.1.93/9500/config/D01-9500-01_running_$(TIMESTAMP).cfg
end
cfg terminal
scheduler schedule name Daily0600
time daily 06:00
job name cfgBackup
da
```

```text
cfg terminal
scheduler schedule name Daily1800
time daily 18:00
job name cfgBackup
da
```
6 Verify that the copy statements work by running each individually:

```
V00101MD9502# copy running-config tftp://192.168.101.93/9500/config/
   V00101MD9502_running_$TIMESTAMP.cfg
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
TFTP put operation was successful
```

7 To save the configuration updates, type: SWITCH# copy running-config startup-config

```
[########################################] 100%
```

8 To verify the procedure, run each statement individually: V00101MD9502# copy running-config tftp://192.168.101.93/9500/config/V00101MD9502_running_$TIMESTAMP.cfg

---

**Backing up Cisco UCS fabric interconnects**

Use this procedure to back up the Cisco UCS fabric interconnects.

**About this task**

You can restore a system configuration from any full state backup file exported from Cisco UCS Manager. The file does not need to be exported from the Cisco UCS Manager on the system that you are restoring.

The restore function is only available for a full state backup file. You cannot import a full state backup file. A restore is performed through the initial system setup.

**Before you begin**

This solution is based on the presence of the trivial file transfer protocol (TFTP) service and therefore, must be installed, configured, and active on the AMP or AMP-2 server where the configuration repository exists.

Obtain:

- Administrator login credentials
- Network IP address of the configuration backup repository
- Name of the device name and type to match the model abbreviation used to create the repository sub-directory structure (for example, \\6100\config\filename)

**Procedure**

Create and run the backup using the Cisco UCS Manager GUI or CLI.
Related information

Creating and running the fabric interconnect backup using the Cisco UCS Manager GUI (see page 226)
Creating and running the fabric interconnect backup using the Cisco UCS Manager CLI (see page 227)

Creating and running the fabric interconnect backup using the Cisco UCS Manager GUI

Use this procedure to back up the Cisco UCS fabric interconnects configuration in Vblock System by using the Cisco UCS Manager GUI.

Procedure

1 Create the backup as follows:

   Note: The creation of the backup is a one-time only task.

   a Using a browser, navigate to the Cisco UCS Manager.
   b Log in to the account using administrator privileges.
   c From the Navigation window, select the Admin tab.
   d Click the All node.
   e From the Work window, select the General tab.
   f In the Actions area, select Backup.
   g In the Backup Configuration window, select Create Backup Operation.
   h Set Admin State to Disabled.
   i Set Type to Full State.
   j Select the Preserve Identifies checkbox.
   k Click OK.
   l If the Cisco UCS Manager displays a confirmation window, click OK.

2 Run the backup as follows:

   a Using a browser, navigate to the Cisco UCS Manager.
   b Log in to the account using administrator privileges.
   c From the Navigation window, select the Admin tab.
d  Select the All node.

e  From the Work window, select the General tab.

f  In the Actions area, select Backup.

g  From the Backup Operations table of the Backup Configuration window, select the backup operation that you want to run. The details of the selected backup operation appear in the Properties area.

h  In the Admin State field, select Enabled.

i  For all protocols except TFTP, type the password in the Password field.

j  You can optionally change the content of the other available fields.

k  Click Apply. The Cisco UCS Manager takes a snapshot of the configuration type that you selected and exports the file to the network location. The backup operation displays in the Backup Operations table in the Backup Configuration window.

l  View the progress of the backup operation by clicking the down arrows on the FSM Details bar. The FSM Details area expands and displays the operation status.

m  To close the Backup Configuration window, click OK.

n  The backup operation continues to run until it is completed. To view the progress, reopen the Backup Configuration window.

Related information

Creating and running the fabric interconnect backup using the Cisco UCS Manager GUI (see page 226)
Creating and running the fabric interconnect backup using the Cisco UCS Manager CLI (see page 227)

Creating and running the fabric interconnect backup using the Cisco UCS Manager CLI

Before you begin

Log in to the Cisco UCS Manager using SSH administrator privileges. Note that the creation of the backup is performed only once.
Procedure

1. To create the backup, set the system mode, create the backup operation and commit the transaction. To do this, type:

   UCS-A# scope system

   UCS-A /system* # create backup tftp://v00001vmfm01/6100/config/ device_name_full-state.tar.gz full-state disabled

   Password:

   UCS-A /system* # commit-buffer

   UCS-A /system #

2. To run the backup, set the system node, run the backup operation, and commit the transaction. To do this, type:

   UCS-A# scope system

   UCS-A /system* # scope backup v00001vmfm01

   UCS-A /system* # enable

   Password:

   UCS-A /system* # commit-buffer

   UCS-A /system #

Related information

Creating and running the fabric interconnect backup using the Cisco UCS Manager GUI (see page 226)

Creating and running the fabric interconnect backup using the Cisco UCS Manager CLI (see page 227)

Backing up network devices running Cisco IOS software

Use this procedure to back up the network devices that use the Cisco IOS 12.x operating system version, or later.

Before you begin

This solution is based on the presence of the trivial file transfer protocol (TFTP) service and therefore, must be installed, configured, and active, on the AMP or AMP-2 server where the instance of the configuration repository exists.
Obtain:

- Login credentials for the device configuration backup
- Network IP address of the configuration backup repository
- Device name and type to match the model abbreviation used to create the repository sub-directory structure

Procedure

1. Log in to the device account using administrator privileges.
2. From the network device, to create the backup task and specify commands, type:

   ```
   SWITCH# enable
   SWITCH# config t
   SWITCH(config)# kron policy-list cfgBackup
   SWITCH(config-kron-policy)# cli show startup-config | redirect tftp://IP/deviceconfig/name_startup_TIMESTAMP.cfg
   SWITCH(config-kron-policy)# cli show running-config | redirect tftp://IP/device/config/name_running_TIMESTAMP.cfg
   SWITCH(config-policy)# end
   ```

**Note:** The static placeholder, TIMESTAMP, in the configuration filename is used because a variable is not available that inserts the date and time into the filename when the tasks are executed. VCE recommends that a script be deployed that processes the files with the TIMESTAMP string present and transforms it into the date and time that the file was created. Otherwise, subsequent executions of the configuration captures overlay the prior versions.
3 From the network device, to schedule the backup task, type:

```
SWITCH# conf t
SWITCH(config)# kron occurrence Daily0600 at 06:00 recurring
SWITCH(config-kron-occurrence)# policy-list cfgBackup
SWITCH(config-kron-occurrence)# end
SWITCH# conf t
SWITCH(config)# kron occurrence Daily1800 at 18:00 recurring
SWITCH(config-kron-occurrence)# policy-list cfgBackup
SWITCH(config-kron-occurrence)# end
```

4 To confirm scheduler update, type: `SWITCH# show kron schedule`

```
Kron Occurrence Schedule
Daily0600 inactive, will run again in 0 days 19:08:36 at 6:00 on
Daily1800 inactive, will run again in 0 days 07:08:36 at 18:00 on
```

5 To save the configuration updates, type: `SWITCH# copy running-config startup-config`

```
[########################################] 100%
```

**Backing up the VMware vCenter SQL server database**

Use this procedure to create backup jobs within a Microsoft SQL server configuration.

**About this task**

VCE recommends that you perform this backup process on a daily basis. Frequency depends upon the client recovery point objective (RPO).

**Before you begin**

- Confirm that the Microsoft SQL server sa login is enabled and a password is set for account
- Ensure that server authentication mode is set to the SQL Server and Windows Authentication mode
- Obtain:
  - Administrator login credentials
– AMP jump server or AMP-2 element manager server network address
– VMware vCenter SQL server network address
– SQL server login credentials

Procedure

1. Connect to the client AMP environment jump server.

2. From the jump server, use remote desktop protocol (RDP) to access the SQL database server, and log in as administrator.

3. To run the SQL Server Management Studio application, navigate to the application and for VMware vSphere 5.5, select Start > All Programs > Microsoft SQL Server 2012 > SQL Server Management Studio or for VMware vSphere 5.1, select Start > All Programs > Microsoft SQL Server 2008 > SQL Server Management Studio.

4. To log in to the application, perform the following:
   a. In the Server type field, verify that Database Engine appears. If not, select it.
   b. If the Server name field is not auto-filled, select (local). If no matching account exists, log in with administrator privileges.
   c. In the Authentication field, verify that Windows Authentication appears. If not, select it, and click Connect.

5. To confirm the list of databases that require backup, from the Object Explorer window, expand Databases > System Databases. The databases that require backup are in the System Databases (master, model, msdb) and the vcenter and vum databases that appear after the Database Snapshots folder.

   Note: Depending on the naming standard that has been followed (client or VCE), they should appear as xmgmtvcneter and xmgmtvum, where x is a unique identifier. The tempdb database should be excluded from the backup process creation tasks.

6. Navigate to and expand SQL Server Agent > Jobs.

7. To create a backup job, right-click Jobs and select New Job.
   a. From the New Job window, in the Name field, type a value to correspond with the backup to be performed.
   b. In the Owner field, remove the default login and type sa.
   c. Change the Category field to Database Maintenance.
   d. Type a description in the Description field.
   e. Verify Enabled is checked.
To create a new job step entry, under **Select a page**, select **Procedure (Steps)**, and then click **New**.

- From the **New Job Step** window, in the **Step name** field, type **Backup** or other text.
- Verify that the default value is set in the **New Job Step window** **Type** field.
- Leave the **Run as** field empty.
- In the **Database** field, select the database to be processed.
- Copy and paste this text into the **Command** area, and modify the **@DIRNAME** and **@DBNAME** variables accordingly:

```sql
DECLARE @DIRNAME VARCHAR(40), @DBNAME VARCHAR(40), @SUFFIX VARCHAR(48), @FILENAME VARCHAR(128);

SET @DIRNAME = 'I:\Backups\';
SET @DBNAME = 'master';

SET @SUFFIX = '_FULL_' + convert(varchar(8),getdate(),112) + '_' + replace(convert(varchar(8),getdate(),108),':','') + '.bak';
SET @FILENAME = @DIRNAME+@DBNAME+@SUFFIX;
BACKUP DATABASE @DBNAME TO DISK=@FILENAME WITH NAME=@DBNAME,SKIP,STATS=20;
```

- Under **Select a page**, select the **Advanced** tab.
- For the **On success action** field, select **Quit the job reporting success**.
- Under **Select a page**, select the **Advanced** tab.

**Note:** You can optionally type a directory location and file name into the **Output file** field to capture script log messages. For example, `I:/Backups/master.log`

- Click **OK**.

To create the job schedule, under **Select a page**, select **Schedules**, and then click **New**.

- From the **New Job Schedule** window, type a **Name** for the job schedule. For example, **Daily Backup**.
To set the schedule, use the following table to create the settings:

<table>
<thead>
<tr>
<th>For these databases</th>
<th>Make the following settings</th>
</tr>
</thead>
</table>
| master, model, msdb | 1. In the Frequency section, set the **Occurs** field to **Daily**.  
2. Verify that the **Recurs** field is set to **1 day(s)**.  
3. In the Daily Frequency section, check **Occurs once at** and set to **06:30 AM**.  
4. In the Duration section, confirm that the **Start date** is set to the current date and **No end date** is selected. |
| vcenter, vum       | 1. In the Frequency section, set the **Occurs** field to **Daily**.  
2. Verify that the **Recurs** field is set to **1 day(s)**.  
3. In the Daily Frequency section, check **Occurs every**, type **4**, and select **hours**.  
4. Set **Starting at** to **06:30:00 AM** and **Ending at** to **06:29:59 AM**.  
5. In the Duration section, confirm that the **Start date** is set to the current date and **No end date** is selected. |

- Verify that the **Schedule Type** is set to **Recurring** and confirm **Enabled** is checked.
- Click OK to accept the schedule update.
- Click OK to complete backup job creation.

Repeat the above steps starting with step 8 until all databases (excluding tempdb) have a backup job.

To create an SQL Server backup file management job, go to step 8 and perform the following:

- As the job description, type **BAK file management**.
- For the **database** field, select **master**.
For the **Command** field, use this text:

```
-- SQL Server Transact SQL script to perform backup file management
--
-- Use this script to manage the BAK files created by the backup jobs. Modify
-- the following variable for the shared location of the backup files –
--
-- DIRNAME - Set location of the backup files
--
DECLARE @dt datetime, @DIRNAME VARCHAR(40)
--
SET @DIRNAME = 'I:\Backups\';
--
select @dt = getdate() - 1
EXECUTE master.dbo.xp_delete_file 0,@DIRNAME,N'BAK',@dt
```

**Note:** You can optionally type a directory location and file name into the **Output file** field to capture script log messages. For example, *Filemgmt.log*

**d**  Use the same schedule as the master database.

12 To test a backup, right-click on a backup job and choose **Start Job at Step**.

**What to do next**
Monitor the backup location to confirm creation is being performed on schedule.

**Related information**

Microsoft Developer Network article for SQL Server 2012: Change Server Authentication Mode

**Back up the EMC Symmetrix configuration**

You can back up the EMC Symmetrix configuration by using a script.
Procedure

To back up the EMC Symmetrix configuration, run this script:

```bash
REM VMax backup script
REM
SET BACKUPDIR=\EMC\VMax
IF EXIST %BACKUPDIR% GOTO LBL1
MKDIR %BACKUPDIR%
:LBL1
cd %BACKUPDIR%
symdev list > symdev-list.txt
symdev list -datadev > symdev-list-datadev.txt
symcfg authorization list > symcfg-auth-list.txt
symcfg list -pool > symcfg-list-pool.txt
symcfg list -pool -thin -detail > symcfg-list-pool-thin.txt
symcfg list -fa all -v > symcfg-list-fa-all.txt
symcfg list -fa all -port > symcfg-list-fa-ports.txt
symcfg list -applications > symcfg-list-applications.txt
symcfg list -connections > symcfg-list-connections.txt
symcfg list -features > symcfg-list-features.txt
symaccess -sid %1 backup -f symaccess-backup.vmax -nop
REM EXIT 0.
```

**Back up the EMC VNXe configuration**

Use this procedure to backup the EMC VNXe storage array used as the AMP shared storage.

About this task

EMC Unisphere requires a current version of Microsoft® Internet Explorer® or Mozilla Firefox with Adobe Flash Player 9 or above.

Before you begin

Obtain the:

- Network IP address and/or URL of the EMC VNXe management address.
- Administrator login credentials for service accounts.

Procedure

1. To log into EMC Unisphere, using a browser, open a URL to the EMC VNXe management address.

2. From the EMC VNXe login screen, type the username and password for the account with advanced administrator privileges for the EMC VNXe system. If you are using an LDAP-based account, type the domain/username for the account. For more information, refer to the *Configuring User Access to Unisphere*. 

© 2013-2015 VCE Company, LLC.  
All Rights Reserved.
3 Click Login.

**Note:** If you cannot remember the passwords for the EMC VNXe default administrator or service user accounts, you can set the passwords back to the default passwords that shipped with your EMC VNXe system.

4 To initiate configuration backup task, select **Settings > Service System**.

5 Type the service password to access the **Service System** page.

6 Under **System Components**, select **Storage System**.

7 Under **Service Actions**, select a service action and click **Execute service action**.

8 If you click **Save Configuration**, you can save details about the configuration settings on the EMC VNXe system to a local file. Service personnel can use this file to assist you with reconfiguring your system after a major system failure or a system reinitialization.

The configuration details include information about:

- System specifications
- Users
- Installed licenses
- Storage resources
- Storage servers
- Hosts

**Note:** The file only contains details about your system configuration settings. You cannot restore your system from this file.

Use this file to record system configuration changes. Save the configuration settings after each major configuration change to ensure you have a current copy of the file.
Backing up Cisco MDS Switches

Creating backups of startup and running configuration files

Use this procedure to create a backup of the Cisco MDS switch startup and running configuration files.

About this task

The backups are stored on the Cisco UCS C220 Vblock System Management Server.

Before you begin

- Start the trivial file transfer protocol (TFTP) service on each of the management servers
- If it does not already exist, create the following folder on each management server:
  D:\Cisco\MDS\switch-model\config
- Obtain the int-mdsbackup login and password to log in to the Cisco MDS switches

Procedure

1. Log on to the switch via PuTTY using your int-mdsbackup login on the Vblock System.
2. Use the copy command to create the configuration file backups.

What to do next

Schedule the backup to run on a regular basis.

Related information

Scheduling backups of the startup and running configuration files (see page 237)

Scheduling backups of the startup and running configuration files

Use this procedure to create and schedule a job to back up the Cisco MDS switch startup and running configuration files.

Procedure

1. From the host, type: config t
2 Type the following commands, one per line. At the end of each line, type Ctrl-Z:

```
scheduler aaa-authentication username login password password
scheduler job_name switchBackup
```

3 To create a backup for the startup-config and running-config files, for example, type:

```
copy startup-config tftp://192.168.101.93/9502/config/
V00101MDxxxx_startup_$(TIMESTAMP).config

copy running-config tftp://192.168.101.93/9502/config/
V00101MDxxxx_running_$(TIMESTAMP).config
```

```
end
```

**Note:** This adds the date and timestamp to filenames.

4 Type the following commands, one per line. At the end of each line, type Ctrl+Z.

```
scheduler schedule name Daily
time daily 23:00
job name switchBackup
```

```
end
```
To verify the action, type:

```
show schedule config
config terminal
feature scheduler
scheduler logfile size 16
end
config terminal
scheduler job name switchBackup

copy startup-config tftp://192.168.101.93/xxxx/config/
V00101MDxxxx_startup_$ (TIMESTAMP).config

copy running-config tftp://192.168.101.93/xxxx/config/
V00101MDxxxx_running_$ (TIMESTAMP).config
end

config terminal
Scheduler schedule name Daily
Time daily 23:00
Job name switchBackup
end
```

Creating a script to purge older copies of the backup files

Use the script in this procedure to delete old backups of the startup and configuration files.
Procedure

To create a script that deletes old backups of the startup and configuration files, copy the VBS script below and save it as \D:\scripts\delete_old_backups.vbs.

```
Option Explicit
On Error Resume Next
Dim oFSO, oFolder, sDirectoryPath
Dim oFileCollection, oFile, sDir
Dim iDaysOld
' Specify Directory Path for File Deletion
sDirectoryPath = "D:\Cisco\9xxx\config"
' Specify Number of Days Old File to Delete
iDaysOld = 7
Set oFSO = CreateObject("Scripting.FileSystemObject")
Set oFolder = oFSO.GetFolder(sDirectoryPath)
Set oFileCollection = oFolder.Files
For Each oFile In oFileCollection
    Specify File Extension
    'Specify number with Number of characters in the file extension
    If LCase(Right(CStr(oFile.Name), 6)) = "config" Then
        If oFile.DateLastModified < (Date() - iDaysOld) Then
            oFile.Delete(True)
        End If
    End If
Next
Set oFSO = Nothing
Set oFolder = Nothing
Set oFileCollection = Nothing
Set oFile = Nothing
```

Scheduling the task to purge older backup files

Use this procedure to create a task to purge older backup files.

About this task

In Creating a script to purge older backup files, you created a script called \D:\scripts\delete_old_backups.vbs that deletes older backups. Complete the following steps to schedule that script to run on a daily basis.

```
Option Explicit
On Error Resume Next
Dim oFSO, oFolder, sDirectoryPath
Dim oFileCollection, oFile, sDir
Dim iDaysOld
' Specify Directory Path for File Deletion
sDirectoryPath = "D:\Cisco\9xxx\config"
' Specify Number of Days Old File to Delete
iDaysOld = 7
Set oFSO = CreateObject("Scripting.FileSystemObject")
Set oFolder = oFSO.GetFolder(sDirectoryPath)
Set oFileCollection = oFolder.Files
For Each oFile In oFileCollection
    Specify File Extension
    'Specify number with Number of characters in the file extension
    If LCase(Right(CStr(oFile.Name), 6)) = "config" Then
        If oFile.DateLastModified < (Date() - iDaysOld) Then
            oFile.Delete(True)
        End If
    End If
Next
Set oFSO = Nothing
Set oFolder = Nothing
Set oFileCollection = Nothing
Set oFile = Nothing
```

Before you begin

Obtain the password for the [Domain]\svc-vmfms01 account from your VMware administrator.
Procedure

1. To create a task within the VMFMS01 server to run the .vbs script daily at 01:00, select Start > Programs > Accessories > System Tools > Scheduled Tasks

2. Browse to D:\scripts\delete_old_backups.vbs.

3. Use the credentials for the [Domain]\svc-vmfms01 account to run the task.

4. On the Schedule tab, schedule the task to run daily at 1:00 AM.
About VCE

VCE, an EMC Federation Company, is the world market leader in converged infrastructure and converged solutions. VCE accelerates the adoption of converged infrastructure and cloud-based computing models that reduce IT costs while improving time to market. VCE delivers the industry's only fully integrated and virtualized cloud infrastructure systems, allowing customers to focus on business innovation instead of integrating, validating, and managing IT infrastructure. VCE solutions are available through an extensive partner network, and cover horizontal applications, vertical industry offerings, and application development environments, allowing customers to focus on business innovation instead of integrating, validating, and managing IT infrastructure.

For more information, go to http://www.vce.com.