<table>
<thead>
<tr>
<th>Date</th>
<th>VCE System</th>
<th>Document revision</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2015</td>
<td>Gen 3.3</td>
<td>3.7</td>
<td>Updated to include support for VMware vSphere 6.0 with Cisco Nexus 1000V Switches.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Removed support for VMware vSphere 5.0.</td>
</tr>
<tr>
<td>February 2015</td>
<td>Gen 3.2</td>
<td>3.6</td>
<td>Added support for Cisco B200 M4 Blade.</td>
</tr>
<tr>
<td>July 2014</td>
<td>Gen 3.2</td>
<td>3.5</td>
<td>Added VMware vSphere 5.5. Added VMware EVC information.</td>
</tr>
<tr>
<td>December 2013</td>
<td>Gen 3.1</td>
<td>3.4</td>
<td>Added TPM, removed Data Protection information, and a link to Data Protection Guide.</td>
</tr>
<tr>
<td>April 2013</td>
<td>Gen 3.1</td>
<td>3.3</td>
<td>Added VCE Vision Intelligent Operations. Updated VMware vSphere information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Integrated into Gen 3.1 release.</td>
</tr>
<tr>
<td>March 2013</td>
<td>Gen 3.0</td>
<td>3.2</td>
<td>Updated for VCE rebranding.</td>
</tr>
<tr>
<td>February 2013</td>
<td>Gen 3.0</td>
<td>3.1</td>
<td>Updated for VCE rebranding. Added information about service profiles, VMware 5.0 and 4.1, boot and data LUNs.</td>
</tr>
<tr>
<td>December 2012</td>
<td>Gen 3.0</td>
<td>3.0</td>
<td>Gen 3.0 release</td>
</tr>
</tbody>
</table>
# Contents

**Introduction** ............................................................................................................................................... 8  
Copyrights and trademarks ........................................................................................................................... 8

**About this document** .................................................................................................................................... 9

**Accessing VCE documentation** .............................................................................................................. 10

**Related documentation** .......................................................................................................................... 11

**Managing compute resources** .................................................................................................................. 12  
Starting Cisco UCS Manager .......................................................................................................................... 12  
Starting EMC Ionix UIM/P ............................................................................................................................ 12  
Upgrading Cisco UCS software ...................................................................................................................... 13  
Activating a Cisco UCS Manager Capability Catalog .................................................................................. 13  
Activating a port license ............................................................................................................................... 14  
Adding a UUID range using EMC UIM/P 3.x ............................................................................................... 14  
Adding a UUID range ................................................................................................................................... 16  
Editing or excluding a UUID range using EMC UIM/P 3.x ....................................................................... 17  
Reversing the procedure .............................................................................................................................. 19  
Deleting a UUID range using EMC UIM/P 3.x ............................................................................................ 19  
Deleting a UUID pool .................................................................................................................................. 20  
Adding a WWNN range using EMC UIM/P 3.x ............................................................................................ 20  
Adding a WWNN range ............................................................................................................................... 22  
Editing or excluding a WWNN range using EMC UIM/P 3.x .................................................................... 23  
Reversing the procedure .............................................................................................................................. 25  
Deleting a WWNN range using EMC UIM/P 3.x .......................................................................................... 25  
Deleting a WWNN range ............................................................................................................................. 26  
Adding a WWPN range using EMC UIM/P 3.x ........................................................................................... 26  
Editing or excluding a WWPN range using EMC UIM/P 3.x .................................................................... 28  
Reversing the procedure .............................................................................................................................. 30  
Deleting a WWPN range using EMC UIM/P 3.x .......................................................................................... 31  
Deleting a WWPN range ............................................................................................................................. 31  
Adding a MAC address range using EMC UIM/P 3.x .............................................................................. 32  
Adding a MAC address range ..................................................................................................................... 34  
Editing or excluding a MAC address range using EMC UIM/P 3.x ......................................................... 34  
Reversing the procedure .............................................................................................................................. 36  
Deleting a MAC address range using EMC UIM/P 3.x ............................................................................ 37  
Deleting a MAC pool ................................................................................................................................... 37  
Adding an IP pool and range of addresses using EMC UIM/P 3.x ............................................................... 38  
Adding an IP pool ....................................................................................................................................... 39  
Deleting an IP pool or range of addresses using EMC UIM/P 3.x .............................................................. 40  
Creating an isolation zone service using EMC UIM/P 3.x ........................................................................ 41  
Modifying the time zone setting .................................................................................................................. 41  
Adding a network time protocol server .................................................................................................... 42  
Removing a network time protocol server ................................................................................................ 43  
Adding a syslog server ............................................................................................................................... 43
Managing networking resources.................................................................69
  Creating a named VLAN on both fabric interconnects...............................69
  Adding a VLAN to a service profile template.............................................70
  Adding a VLAN to a service profile using EMC UIM/P...............................70
  Adding a VLAN to the Cisco Nexus 1000V Switch......................................71
  Adding a VLAN to the Cisco Nexus series switches....................................72
    Reversing the procedure...........................................................................73
  Configuring a virtual port channel............................................................73
  Deleting a virtual port channel.................................................................75
  Adding VLANs to the trunk of a virtual port channel.................................75
  Removing VLANs from the trunk of a virtual port channel........................76
  Adding port channels to VLANs for disjoint layer 2 networks.....................76
  Viewing port channels assigned to VLANs for disjoint layer 2 networks........79
  Removing port channels from VLANs for disjoint layer 2 networks..............79
  Upgrading Cisco Nexus 5500 Series Switch software.................................80
    Reversing the procedure...........................................................................85
  Upgrading Cisco MDS switch software......................................................86
    Reversing the procedure...........................................................................87
Managing Cisco MDS switches.....................................................................88
  Upgrading Cisco MDS switch software......................................................88
  Reversing the procedure...........................................................................89
  Configuring a VSAN..................................................................................89
    Reversing the procedure...........................................................................90
  Configuring a domain ID and priority for a VSAN.....................................90
    Reversing the procedure...........................................................................91
  Enabling Fibre Channel interfaces............................................................92
    Reversing the procedure...........................................................................92
  Moving licenses between Fibre Channel interfaces....................................92
  Disabling port licenses............................................................................93
Managing storage resources........................................................................94
  Logging on to a storage array.................................................................94
  Creating storage pools.............................................................................94
  Expanding a storage pool.........................................................................96
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing VMware vCenter Single Sign-On for VMware vSphere 6.0</td>
<td>123</td>
</tr>
<tr>
<td>Managing VMware vSphere virtual machines</td>
<td>121</td>
</tr>
<tr>
<td>Managing VMware vSphere ESXi 6.0, 5.5, and 5.1</td>
<td>117</td>
</tr>
<tr>
<td>Managing NFS</td>
<td>106</td>
</tr>
<tr>
<td>Managing CIFS</td>
<td>111</td>
</tr>
<tr>
<td>Creating a VSAN</td>
<td>96</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>97</td>
</tr>
<tr>
<td>Monitoring a storage pool</td>
<td>97</td>
</tr>
<tr>
<td>Creating a storage group</td>
<td>98</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>98</td>
</tr>
<tr>
<td>Connecting a host to a storage group</td>
<td>99</td>
</tr>
<tr>
<td>Creating a boot LUN</td>
<td>102</td>
</tr>
<tr>
<td>Creating a data LUN</td>
<td>104</td>
</tr>
<tr>
<td>Expanding a LUN</td>
<td>104</td>
</tr>
<tr>
<td>Monitoring a RAID group</td>
<td>105</td>
</tr>
<tr>
<td>Creating a file system on a storage array</td>
<td>106</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>108</td>
</tr>
<tr>
<td>Creating an NFS export on a storage array</td>
<td>108</td>
</tr>
<tr>
<td>Mounting the NFS export</td>
<td>109</td>
</tr>
<tr>
<td>Unmounting the NFS export</td>
<td>110</td>
</tr>
<tr>
<td>Deleting the NFS Export</td>
<td>110</td>
</tr>
<tr>
<td>Creating a CIFS</td>
<td>111</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>113</td>
</tr>
<tr>
<td>Creating a CIFS share</td>
<td>113</td>
</tr>
<tr>
<td>Mapping the CIFS share</td>
<td>114</td>
</tr>
<tr>
<td>Unmapping a CIFS share</td>
<td>115</td>
</tr>
<tr>
<td>Deleting a CIFS share</td>
<td>115</td>
</tr>
<tr>
<td>Installing the latest VMware vSphere ESXi patch</td>
<td>117</td>
</tr>
<tr>
<td>Configuring advanced settings for VMware vSphere ESXi</td>
<td>118</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>120</td>
</tr>
<tr>
<td>Hardening security on VMware vSphere ESXi hosts</td>
<td>120</td>
</tr>
<tr>
<td>Increasing the disk timeout on Microsoft Windows virtual machines</td>
<td>121</td>
</tr>
<tr>
<td>Setting up Java and Internet Explorer on the management virtual machine</td>
<td>121</td>
</tr>
<tr>
<td>Deleting a CIFS</td>
<td>115</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>115</td>
</tr>
<tr>
<td>Creating a CIFS share</td>
<td>114</td>
</tr>
<tr>
<td>Mapping the CIFS share</td>
<td>114</td>
</tr>
<tr>
<td>Unmapping a CIFS share</td>
<td>115</td>
</tr>
<tr>
<td>Deleting a CIFS share</td>
<td>115</td>
</tr>
<tr>
<td>Creating a CIFS</td>
<td>111</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>113</td>
</tr>
<tr>
<td>Creating a CIFS share</td>
<td>113</td>
</tr>
<tr>
<td>Mapping the CIFS share</td>
<td>114</td>
</tr>
<tr>
<td>Unmapping a CIFS share</td>
<td>115</td>
</tr>
<tr>
<td>Deleting a CIFS share</td>
<td>115</td>
</tr>
<tr>
<td>Installing the latest VMware vSphere ESXi patch</td>
<td>117</td>
</tr>
<tr>
<td>Configuring advanced settings for VMware vSphere ESXi</td>
<td>118</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>120</td>
</tr>
<tr>
<td>Hardening security on VMware vSphere ESXi hosts</td>
<td>120</td>
</tr>
<tr>
<td>Monitoring a storage pool</td>
<td>97</td>
</tr>
<tr>
<td>Creating a storage group</td>
<td>98</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>98</td>
</tr>
<tr>
<td>Connecting a host to a storage group</td>
<td>99</td>
</tr>
<tr>
<td>Creating a boot LUN</td>
<td>102</td>
</tr>
<tr>
<td>Creating a data LUN</td>
<td>104</td>
</tr>
<tr>
<td>Expanding a LUN</td>
<td>104</td>
</tr>
<tr>
<td>Monitoring a RAID group</td>
<td>105</td>
</tr>
<tr>
<td>Creating a file system on a storage array</td>
<td>106</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>108</td>
</tr>
<tr>
<td>Creating an NFS export on a storage array</td>
<td>108</td>
</tr>
<tr>
<td>Mounting the NFS export</td>
<td>109</td>
</tr>
<tr>
<td>Unmounting the NFS export</td>
<td>110</td>
</tr>
<tr>
<td>Deleting the NFS Export</td>
<td>110</td>
</tr>
<tr>
<td>Creating a CIFS</td>
<td>111</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>113</td>
</tr>
<tr>
<td>Creating a CIFS share</td>
<td>113</td>
</tr>
<tr>
<td>Mapping the CIFS share</td>
<td>114</td>
</tr>
<tr>
<td>Unmapping a CIFS share</td>
<td>115</td>
</tr>
<tr>
<td>Deleting a CIFS share</td>
<td>115</td>
</tr>
<tr>
<td>Installing the latest VMware vSphere ESXi patch</td>
<td>117</td>
</tr>
<tr>
<td>Configuring advanced settings for VMware vSphere ESXi</td>
<td>118</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>120</td>
</tr>
<tr>
<td>Hardening security on VMware vSphere ESXi hosts</td>
<td>120</td>
</tr>
<tr>
<td>Increasing the disk timeout on Microsoft Windows virtual machines</td>
<td>121</td>
</tr>
<tr>
<td>Setting up Java and Internet Explorer on the management virtual machine</td>
<td>121</td>
</tr>
<tr>
<td>Deleting a CIFS</td>
<td>115</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>115</td>
</tr>
<tr>
<td>Creating a CIFS</td>
<td>114</td>
</tr>
<tr>
<td>Mapping the CIFS share</td>
<td>114</td>
</tr>
<tr>
<td>Unmapping a CIFS share</td>
<td>115</td>
</tr>
<tr>
<td>Deleting a CIFS share</td>
<td>115</td>
</tr>
<tr>
<td>Installing the latest VMware vSphere ESXi patch</td>
<td>117</td>
</tr>
<tr>
<td>Configuring advanced settings for VMware vSphere ESXi</td>
<td>118</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>120</td>
</tr>
<tr>
<td>Hardening security on VMware vSphere ESXi hosts</td>
<td>120</td>
</tr>
<tr>
<td>Monitoring a storage pool</td>
<td>97</td>
</tr>
<tr>
<td>Creating a storage group</td>
<td>98</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>98</td>
</tr>
<tr>
<td>Connecting a host to a storage group</td>
<td>99</td>
</tr>
<tr>
<td>Creating a boot LUN</td>
<td>102</td>
</tr>
<tr>
<td>Creating a data LUN</td>
<td>104</td>
</tr>
<tr>
<td>Expanding a LUN</td>
<td>104</td>
</tr>
<tr>
<td>Monitoring a RAID group</td>
<td>105</td>
</tr>
<tr>
<td>Creating a file system on a storage array</td>
<td>106</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>108</td>
</tr>
<tr>
<td>Creating an NFS export on a storage array</td>
<td>108</td>
</tr>
<tr>
<td>Mounting the NFS export</td>
<td>109</td>
</tr>
<tr>
<td>Unmounting the NFS export</td>
<td>110</td>
</tr>
<tr>
<td>Deleting the NFS Export</td>
<td>110</td>
</tr>
<tr>
<td>Creating a CIFS</td>
<td>111</td>
</tr>
<tr>
<td>Reversing the procedure</td>
<td>113</td>
</tr>
<tr>
<td>Creating a CIFS share</td>
<td>113</td>
</tr>
<tr>
<td>Mapping the CIFS share</td>
<td>114</td>
</tr>
<tr>
<td>Unmapping a CIFS share</td>
<td>115</td>
</tr>
<tr>
<td>Deleting a CIFS share</td>
<td>115</td>
</tr>
</tbody>
</table>
Managing the AMP .......................................................................................................................... 164
Upgrading the Cisco UCS C220 Server .............................................................................................. 164
Upgrading the Cisco Catalyst switch software .................................................................................. 165
    Reversing the procedure ............................................................................................................ 168
Backing up the AMP ....................................................................................................................... 168
    Creating an instance of the configuration repository .............................................................. 168
    Restoring a configuration file .................................................................................................. 169
    Backing up targets .................................................................................................................. 169

Guidelines for backing up VCE Systems configuration files ............................................................ 171
    Backing up VCE System configuration files ............................................................................. 171
    Backing up network devices running Cisco NX-OS software .................................................... 171
    Backing up Cisco UCS fabric interconnects .............................................................................. 173
        Creating and running the fabric interconnect backup by using the Cisco UCS Manager GUI .. 174
        Creating and running the fabric interconnect backup by using the Cisco UCS Manager CLI .. 175
    Backing up network devices running Cisco IOS software ......................................................... 176
    Backing up the VMware vCenter SQL server database .............................................................. 178
    Backing up the EMC VNX configuration .................................................................................... 182
        Reversing the procedure ........................................................................................................ 182
    Backing up the EMC VNXe configuration ................................................................................. 183

Backing up Cisco MDS Switches ....................................................................................................... 185
    Creating backups of startup and running configuration files ...................................................... 185
    Scheduling backups of the startup and running configuration files .......................................... 185
    Creating a script to purge older copies of the backup files ....................................................... 187
    Scheduling the task to purge older backup files ....................................................................... 188
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.

Related information

Accessing VCE documentation (see page 10)

Copyrights and trademarks

Copyright 2012-2015 VCE Company, LLC. All Rights Reserved. VCE, VCE Vision, VCE Vscale, Vblock, VxBlock, VxRack, and the VCE logo are registered trademarks or trademarks of VCE Company LLC. All other trademarks used herein are the property of their respective owners.
About this document

This document contains instructions for managing the VCE System 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 VCE System 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 <a href="#">VCE Download Center</a> 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>

[Accessing VCE documentation](#)
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.
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.

Starting EMC Ionix UIM/P

Use the following steps to launch EMC Ionix UIM/P.

Procedure

1. Open a web browser.
2. Navigate to https://Hostname/, where Hostname is the fully qualified host name of the appliance. The login screen appears.
3. Type your username and password and then click Enter.
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.

Related information

Cisco UCS Manager upgrade documentation

Activating a 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

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 using EMC UIM/P 3.x**

Use this procedure to add a range to a Universally Unique Identifier (UUID) pool.
About this task

**NOTE:** This procedure is applicable to EMC Ionix UIM/P version 3.0, and later. Refer to the VCE Release Certification Matrix to verify what version of UIM/P you are running.

EMC Ionix UIM/P 3.0 is installed with one UUID pool that is empty until you add ranges of addresses to the pool. The pool cannot be used if it does not have a range of addresses. Also, provisioning cannot be performed until the ranges have been defined.

During provisioning, EMC Ionix UIM/P uses the addresses included in the pool and assigns the UUIDs to the blades.

A UUID pool uses a unique identifier to identify each computer system on an individual blade. A UUID pool can be designated as **Global** or **Vblock** (identifies a Vblock System) by selecting a tag used by EMC Ionix UIM/P for selection precedence.

EMC Ionix UIM/P performs UUID pool selection in this order:

1. EMC Ionix UIM/P allocates resources from a range that matches the specified Vblock System.
2. If not found, EMC Ionix UIM/P allocates resources from the global range.
3. If not found, provisioning fails.

**NOTE:** Provisioning can also fail if EMC Ionix UIM/P finds a range, but the resources are allocated.

Addresses from the pool are not used until all of the addresses in the existing pools have been allocated. Each pool provides a range of identifiers from which EMC Ionix UIM/P pulls to assign to system resources when it provisions a service. The pools automate the resource assignments ensuring that a unique identifier is used for each resource and eliminate the need for infrastructure administrators to track the identifiers used during resource allocation.

Additionally, EMC Ionix UIM/P ensures that the identifiers are unique for all resources managed through multiple Vblock Systems discovered by the same instance of EMC Ionix UIM/P.

VCE recommends that you:

- Select ranges that minimize or eliminate the risk of conflict with existing devices in the current network environment.
- Identify the UUID currently used in the environment and create ranges to exclude them from EMC Ionix UIM/P resource allocation.

Before you begin

Obtain the UUID information.

Procedure

1. Log in to EMC Ionix UIM/P.
2. From the **Administration** view, select the **UUID Pool** tab.
3. Click **Add**.
4. Type a **Name**.
5 Type a **Start** and **End** range of UUIDs that are available to allocate to each computer system on each blade at the time the service is provisioned.

**NOTE:** The UUID is 32 digits and is formatted as: 8-4-4-4-12.

For example, 00000000-0000-0000-0000-000000000000

6 Select either the **Global** or **Vblock** tag.

7 Click **OK**.

**Results**

If the range was added successfully, it appears on the appropriate tab.

**What to do next**

When all the addresses from the existing ranges have been allocated, use the UUID pool for resource allocation.

**Related information**

[Deleting a UUID range using EMC UIM/P 3.x](#) (see page 19)

[Editing or excluding a UUID range using EMC UIM/P 3.x](#) (see page 17)

## 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.

3 On the **Servers** tab, expand **Servers > 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 **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
Deleting a UUID pool (see page 20)
Cisco UCS Manager GUI Configuration Guide

Editing or excluding a UUID range using EMC UIM/P 3.x

Follow this procedure to edit or exclude a UUID range using EMC UIM/P 3.x.

About this task

⚠️ NOTE: This procedure is applicable to EMC Ionix UIM/P 3.0, and later only. Refer to the VCE Release Certification Matrix to verify what version of UIM/P that you are running.

Included ranges containing values that were previously issued can only be expanded to include additional values. Only existing ranges that have not been allocated can be excluded. If you attempt to exclude part of a range that has previously been allocated for use, the application returns an error.

A UUID pool can be designated as Global or Vblock (identifies a Vblock System) by selecting a tag used by EMC Ionix UIM/P for selection precedence.

Addresses from the pool are not used until all the addresses in the existing pools have been allocated. Each pool provides a range of identifiers from which EMC Ionix UIM/P pulls to assign to system resources when it provisions a service. The pools automate the resource assignments ensuring that a unique identifier is used for each resource and eliminate the need for infrastructure administrators to track the identifiers used during resource allocation.

Additionally, EMC Ionix UIM/P ensures that the identifiers are unique for all resources managed through multiple Vblock Systems discovered by the same instance of EMC Ionix UIM/P.

When you exclude a UUID range, the pool is no longer available for use in deployed services.

VCE recommends that you:

- Select ranges that minimize or eliminate the risk of conflict with existing devices in the current network environment.
• Identify the UUID currently used in the environment and create ranges to exclude them from EMC Ionix UIM/P resource allocation.

**Before you begin**

**Obtain the:**

- UUID range currently being used.
- UUID range that you want to add.

**Procedure**

**To edit a range:**

1. Log in to EMC Ionix UIM/P.
2. From the **Administration** view, select the **UUID Pool** tab.
3. Select a range, and click **Edit**.
4. From here, you can:
   a. Change the **Name**.
   b. Change a **Start** and **End** range of UUIDs that are available to allocate to the Fiber Channel vHBAs in UCS at the time the service is provisioned.

   ★ **NOTE:** The UUID is 32 digits and is formatted as follows: 8-4-4-4-12.

   For example, 00000000-0000-0000-0000-000000000000.
   c. Change the tag to either **Global** or **Vblock**.

   ★ **NOTE:** You cannot change the tag if any UUIDs in the range are allocated.
5. Click **OK**.

**To exclude a range:**

1. From the **Administration** view, select the **MAC Pool** tab.
2. Click **Exclude**.
3. Edit the **Start** or **End** range of MAC addresses to be excluded from resource allocation.
4. Click **OK**.
5. To verify that a pool was expanded successfully, verify that the free and total addresses are increased in the pool. To verify that a range was excluded, verify that the range you excluded from the pool does not display in the list of available addresses.

**What to do next**

When all the addresses from the existing ranges have been allocated, use the UUID pool for resource allocation.
Related information

Adding a UUID range using EMC UIM/P 3.x (see page 14)
Deleting a UUID range using EMC UIM/P 3.x (see page 19)

Reversing the procedure

Procedure

To reverse this procedure, repeat it and type the original values in the Start and End fields, or select the exclusion range of addresses and click OK.

Deleting a UUID range using EMC UIM/P 3.x

Use this procedure to delete an existing UUID range from the UUID pool.

About this task

小心: This procedure is applicable to EMC Ionix UIM/P version 3.0, and later. Refer to the VCE Release Certification Matrix to verify what version of EMC Ionix UIM/P you are running.

The range is no longer available to a resource. You cannot delete any range in the pool that is allocated to a resource.

Before you begin

Obtain the UUID information.

Procedure

1 Log in to EMC Ionix UIM/P.
2 From the Administration view, select the UUID Pool tab.
3 Select a range, and click Delete.
4 Click Yes.

Results

If the procedure is successful, the range no longer exists in the pool.

Related information

Adding a UUID range using EMC UIM/P 3.x (see page 14)
Editing or excluding a UUID range using EMC UIM/P 3.x (see page 17)
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 16)
Cisco UCS Manager GUI Configuration Guide

Adding a WWNN range using EMC UIM/P 3.x

Use this procedure to add a range to the World Wide Node Names (WWNN) pool.

About this task

NOTE: This procedure is applicable to EMC Ionix UIM/P version 3.0, and later. Refer to the VCE Release Certification Matrix to verify what version of UIM/P you are running.

EMC Ionix UIM/P 3.0 is installed with one WWNN pool that is empty until you add ranges of addresses to the pool. The pool cannot be used if it does not have a range of addresses. Also, provisioning cannot be performed until the ranges have been defined.

During provisioning, EMC Ionix UIM/P uses the addresses included in the pool and assigns the WWNNs to the fiber channel vHBAs.

A WWNN pool uses unique identifiers assigned to servers in Cisco UCS. A WWNN pool can be designated as Global or Vblock (identifies a Vblock System) by selecting a tag used by EMC Ionix UIM/P for selection precedence.
EMC Ionix UIM/P performs WWNN pool selection in this order:

1. EMC Ionix UIM/P allocates resources from a range that matches the specified Vblock System.
2. If not found, EMC Ionix UIM/P allocates resources from the global range.
3. If not found, provisioning fails.

**NOTE:** Provisioning can also fail if EMC Ionix UIM/P finds a range, but the resources are allocated.

Addresses from the pool are not used until all the addresses in the existing pools have been allocated. Each pool provides a range of identifiers from which EMC Ionix UIM/P pulls to assign to system resources when it provisions a service. The pools automate the resource assignments to ensure that a unique identifier is used for each resource and to eliminate the need for infrastructure administrators to track the identifiers that are used during resource allocation.

Additionally, EMC Ionix UIM/P ensures that the identifiers are unique for all resources managed through multiple Vblock Systems discovered by the same instance of EMC Ionix UIM/P.

VCE recommends that you:

- Select ranges that minimize or eliminate the risk of conflict with existing devices in the current network environment.
- Identify the WWNN currently used in the environment and create ranges to exclude them from EMC Ionix UIM/P resource allocation.
- Create separate pools for the WWNN assigned to servers.
- Since most ranges are reserved, only use the following ranges:
  - 20:00:00:00:00:00:00:00 through 20:FF:FF:FF:FF:FF:FF:FF
  - 50:00:00:00:00:00:00:00 through 5F:FF:FF:FF:FF:FF:FF:FF

**NOTE:** To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, VCE recommends using the following WWNN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX

**Before you begin**

Obtain the WWNN information.

**Procedure**

1. Log in to EMC Ionix UIM/P.
2. From the **Administration** view, select the **WWNN Pool** tab.
3. Click **Add**.
4. Type a **Name**.
Type a **Start** and **End** range of WWNNs that are available to be allocated to the fiber channel vHBAs in UCS at the time the service is provisioned.

**NOTE:** The format is 8 pairs of hexadecimal digits with each pair separated by a colon.

For example: `20:00:00:25:B5:AB:CD:EF`

Select either the **Global** or **Vblock** tag.

Click **OK**.

**Results**
If the range was added successfully, it appears on the appropriate tab.

**What to do next**
When all the addresses from the existing ranges have been allocated, use the WWNN pool for resource allocation.

**Related information**
- Deleting a WWNN range using EMC UIM/P 3.x (see page 25)
- Editing or excluding a WWNN range using EMC UIM/P 3.x (see page 23)

### 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
Deleting a WWNN range (see page 26)
Cisco UCS Manager GUI Configuration Guide

Editing or excluding a WWNN range using EMC UIM/P 3.x

Use this procedure to edit or exclude a WWNN range.

About this task

NOTE: This procedure is applicable to EMC Ionix UIM/P version 3.0, and later. Refer to the VCE Release Certification Matrix to verify what version of EMC UIM/P you are running.

Included ranges containing values that were previously issued can only be expanded to include additional values.

A WWNN pool uses unique identifiers assigned to servers in Cisco UCS. A WWNN pool can be Global or Vblock (identifies a Vblock System) by selecting a tag used by EMC Ionix UIM/P for selection precedence.

Addresses from the pool are not used until all the addresses in the existing pools have been allocated. Each pool provides a range of identifiers from which EMC Ionix UIM/P pulls to assign to system resources when it provisions a service. The pools automate the resource assignments ensuring that a unique
identifier is used for each resource and eliminates the need for infrastructure administrators to track the identifiers used during resource allocation.

Additionally, EMC Ionix UIM/P ensures that the identifiers are unique for all resources managed through multiple Vblock Systems discovered by the same instance of EMC Ionix UIM/P.

VCE recommends that you:

- Select ranges that minimize or eliminate the risk of conflict with existing devices in the current network environment.
- Identify the WWNN currently used in the environment and create ranges to exclude them from EMC Ionix UIM/P resource allocation.
- Create separate pools for the WWNN assigned to servers.
- Since most ranges are reserved, only use the following ranges:
  - 20:00:00:00:00:00:00:00 through 20:FF:FF:FF:FF:FF:FF:FF
  - 50:00:00:00:00:00:00:00 through 5F:FF:FF:FF:FF:FF:FF:FF

**NOTE:** To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, VCE recommends using the following WWNN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX

Before you begin

Obtain the:

- WWNN range currently being used.
- WWNN range that you want to add.

Procedure

1. Log in to EMC Ionix UIM/P.
2. From the Administration view, open the WWNN Pool tab.
3. Select a range, and click Edit.
4. From here, you can:
   a. Change the Name.
   b. Change a Start and End range of WWNNs that are available to allocate to the Fibre Channel vHBAs in UCS at the time the service is provisioned.

   **NOTE:** The format is 8 pairs of hexadecimal digits with each pair separated by a colon.

   For example: 20:00:00:25:B5:AB:CD:EF.

   c. Change the tag to either Global or Vblock.

   **NOTE:** You cannot change the tag if any WWNNs in the range are allocated.
To verify that a pool was expanded successfully, verify that the free and total addresses are increased in the pool. To verify that a range was excluded, verify that the range you excluded from the pool does not display in the list of available addresses.

What to do next

When all the addresses from the existing ranges have been allocated, use the WWNN pool for resource allocation.

Related information

Adding a WWNN range using EMC UIM/P 3.x (see page 20)
Deleting a WWNN range using EMC UIM/P 3.x (see page 25)

Reversing the procedure

Procedure

To reverse this procedure, repeat it and type the original values in the Start and End fields or select the exclusion range of addresses and click OK.

Deleting a WWNN range using EMC UIM/P 3.x

Use this procedure to delete an existing WWNN range from the WWNN pool.

About this task

aretNote: This procedure is applicable to EMC Ionix UIM/P version 3.0, and later. Refer to the VCE Release Certification Matrix to verify what version of EMC UIM/P you are running.

The range is no longer available to a resource. You cannot delete any range in the pool that is allocated to a resource.

Before you begin

Obtain the WWNN information.

Procedure

1. Log in to EMC Ionix UIM/P.
2. From the Administration view, select the WWNN Pool tab.
3. Select a range, and click Delete.
4. Click Yes.

Results

If the procedure was successful, the range no longer exists in the pool.
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 WWPN range using EMC UIM/P 3.x (see page 22)
Cisco UCS Manager GUI Configuration Guide

Adding a WWPN range using EMC UIM/P 3.x

Use this procedure to add a range to the World Wide Port Names (WWPN) pool.

About this task

NOTE: This procedure is applicable to EMC Ionix UIM/P 3.0, and later only. Refer to the VCE Release
Certification Matrix to verify what version of EMC UIM/P that you are running.
EMC Ionix UIM/P 3.0 is installed with one WWPN pool that is empty until you add ranges of addresses to the pool. The pool cannot be used if it does not have a range of addresses. Also, provisioning cannot be performed until the ranges have been defined.

During provisioning, EMC Ionix UIM/P uses the addresses included in the pool and assigns the WWPNs to the vHBAs.

A WWPN pool has unique identifiers assigned to vHBA’s in UCS. A WWPN pool can be designated as **Global** or **Vblock**, and as **Fabric A**, **Fabric B** or both, by selecting a tag used by EMC Ionix UIM/P for selection precedence.

<table>
<thead>
<tr>
<th>If you designate a pool as...</th>
<th>Then it identifies...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vblock</td>
<td>A Vblock System</td>
</tr>
<tr>
<td>Vblock_Fabric_A</td>
<td>A Vblock System and fabric</td>
</tr>
<tr>
<td>Vblock_Fabric_B</td>
<td>A Vblock System and fabric</td>
</tr>
<tr>
<td>Global</td>
<td>A global Vblock System and fabric</td>
</tr>
</tbody>
</table>

EMC Ionix UIM/P performs WWPN pool selection in this order:

1. EMC Ionix UIM/P allocates resources from a range that matches the specified Vblock System and the particular fabric.
2. If not found, EMC Ionix UIM/P allocates resources from a range that matches the specified Vblock System.
3. If not found, EMC Ionix UIM/P tries to allocate resources from the global range.
4. If not found, provisioning fails.

**NOTE:** Provisioning can also fail if EMC Ionix UIM/P finds a range but the resources are allocated.

Addresses from the pool are not used until all the addresses in the existing pools have been allocated. Each pool provides a range of identifiers from which EMC Ionix UIM/P pulls to assign to system resources when it provisions a service. The pools automate the resource assignments ensuring that a unique identifier is used for each resource and eliminate the need for infrastructure administrators to track the identifiers used during resource allocation.

Additionally, EMC Ionix UIM/P ensures that the identifiers are unique for all resources managed through multiple Vblock Systems discovered by the same instance of EMC Ionix UIM/P.

VCE recommends that you:

- Select ranges that minimize or eliminate the risk of conflict with existing devices in the current network environment.
- Identify the WWPN currently used in the environment and create ranges to exclude them from EMC Ionix UIM/P resource allocation.
- Create separate pools for the WWPN assigned to vHBA ports.
- Since most ranges are reserved, only use the following ranges:
  - 20:00:00:00:00:00:00:00 through 20:FF:FF:FF:FF:FF:FF:FF
To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, VCE recommends using the following WWPN prefix for all blocks in a pool:

20:00:00:25:B5:XX:XX:XX

Before you begin

Obtain the WWPN information.

Procedure

1. Log in to EMC Ionix UIM/P.
2. From the Administration view, select the WWPN Pool tab.
3. Click Add.
4. Type a Name.
5. Type a Start and End range of WWPNs that are available to be allocated to the fiber channel vHBAs in UCS at the time the service is provisioned.

   | NOTE: The range format is eight pairs of hexadecimal digits with each pair separated by a colon.

   For example: 20:00:00:25:B5:AB:CD:EF

6. Select either the Global or Vblock tag. If you select Vblock, you can also select Fabric A, Fabric B, or Both.
7. Click OK.

Results

If the range was added successfully, it appears on the appropriate tab.

What to do next

After all the addresses from the existing ranges have been allocated, use the WWPN pool for resource allocation.

Related information

Deleting a WWPN range using EMC UIM/P 3.x (see page 31)
Editing or excluding a WWPN range using EMC UIM/P 3.x (see page 28)

Editing or excluding a WWPN range using EMC UIM/P 3.x

Use this procedure to edit or exclude a WWPN range.
About this task

**NOTE:** This procedure is applicable to EMC Ionix UIM/P version 3.0, and later. Refer to the VCE Release Certification Matrix to verify what version of EMC UIM/P you are running.

Included ranges containing values that were previously issued can only be expanded to include additional values. Only existing ranges that have not been allocated can be excluded.

A WWPN pool has unique identifiers assigned to vHBA’s in a Cisco UCS. A WWPN pool can be **Global** or **Vblock**, and designated as **Fabric A**, **Fabric B** or both, by selecting a tag used by EMC Ionix UIM/P for selection precedence.

<table>
<thead>
<tr>
<th>If you designate a pool as...</th>
<th>Then it identifies...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vblock</td>
<td>A Vblock System</td>
</tr>
<tr>
<td>Vblock_Fabric_A</td>
<td>A Vblock System and fabric</td>
</tr>
<tr>
<td>Vblock_Fabric_B</td>
<td>A Vblock System and fabric</td>
</tr>
<tr>
<td>Global</td>
<td>A global Vblock System and fabric</td>
</tr>
</tbody>
</table>

Addresses from the pool are not used until all the addresses in the existing pools have been allocated. Each pool provides a range of identifiers from which EMC Ionix UIM/P pulls to assign to system resources when it provisions a service. The pools automate the resource assignments ensuring that a unique identifier is used for each resource and eliminates the need for infrastructure administrators to track the identifiers used during resource allocation.

Additionally, EMC Ionix UIM/P ensures that the identifiers are unique for all resources managed through multiple Vblock Systems discovered by the same instance of EMC Ionix UIM/P.

VCE recommends that you:

- Select ranges that minimize or eliminate the risk of conflict with existing devices in the current network environment.
- Identify the WWPN currently used in the environment and create ranges to exclude them from EMC Ionix UIM/P resource allocation.
- Create separate pools for the WWPN assigned to vHBA ports.
- Since most ranges are reserved, only use the following ranges:
  - 20:00:00:00:00:00:00:00 through 20:FF:FF:FF:FF:FF:FF:FF
  - 50:00:00:00:00:00:00:00 through 5F:FF:FF:FF:FF:FF:FF:FF

**NOTE:** To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, VCE recommends using the following WWPN prefix for all blocks in a pool:

20:00:00:25:B5:XX:XX:XX

Before you begin

Obtain the:

- WWPN range currently being used.
• WWPN range that you want to add.

Procedure

1 Log in to EMC Ionix UIM/P.

2 From the Administration view, open the WWPN Pool tab.

3 Select a range, and click Edit.

4 From here, you can:
   a Change the Name.
   b Change a Start and End range of WWPNs that are available to allocate to the Fiber Channel vHBAs in UCS at the time the service is provisioned.
      
      ![NOTE:](image)
      The format is 8 pairs of hexadecimal digits with each pair separated by a colon.
      
      For example: 20:00:00:25:B5:AB:CD:EF
   c Change the tag to either Global or Vblock. If you select Vblock, you can also select Fabric A, Fabric B, or Both.
      
      ![NOTE:](image)
      You cannot change the tag if any WWPNs in the range are allocated.

5 Click OK.

6 To verify that a pool was expanded successfully, verify that the free and total addresses are increased in the pool. To verify that a range was excluded, verify that the range you excluded from the pool does not display in the list of available addresses.

What to do next

When all the addresses from the existing ranges have been allocated, use the WWPN pool for resource allocation.

Related information

Adding a WWPN range using EMC UIM/P 3.x (see page 26)
Deleting a WWPN range using EMC UIM/P 3.x (see page 31)

Reversing the procedure

Procedure

To reverse this procedure, repeat it and type the original values in the Start and End fields, or select the exclusion range of addresses and click OK.
Deleting a WWPN range using EMC UIM/P 3.x

Use this procedure to delete an existing WWPN range from the WWPN pool.

About this task

**NOTE:** This procedure is applicable to EMC Ionix UIM/P version 3.0, and later. Refer to the VCE Release Certification Matrix to verify what version of EMC UIM/P you are running.

The range is no longer available to a resource. You cannot delete any range in the pool that is allocated to a resource.

Before you begin

Obtain the WWPN information.

Procedure

1. Log in to EMC Ionix UIM/P.
2. From the Administration view, select the WWPN Pool tab.
3. Select a range, and click Delete.
4. Click Yes.

Results

If the procedure is successful, the range no longer exists in the pool.

Related information

- Adding a WWPN range using EMC UIM/P 3.x (see page 26)
- Editing or excluding a WWPN range using EMC UIM/P 3.x (see page 28)

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 using EMC UIM/P 3.x

Use this procedure to add a range to the Media Access Control (MAC) address pool.

About this task

**NOTE:** This procedure is applicable to EMC Ionix UIM/P version 3.0, and later. Refer to the VCE Release Certification Matrix to verify what version of EMC Ionix UIM/P you are running.

EMC Ionix UIM/P 3.0 is installed with one MAC address pool that is empty until you add ranges of addresses to the pool. The pool cannot be used if it does not have a range of addresses. Also, provisioning cannot be performed until the ranges have been defined.

During provisioning, EMC Ionix UIM/P uses the addresses included in the pool and assigns the MAC addresses to the service vNICs.

A MAC address pool can be **Global** or **Vblock**, and designated as **Fabric A**, **Fabric B** or both, by selecting a tag used by EMC Ionix UIM/P for selection precedence.

<table>
<thead>
<tr>
<th>If you designate a pool as...</th>
<th>Then it identifies...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vblock</td>
<td>A Vblock System</td>
</tr>
<tr>
<td>Vblock_Fabric_A</td>
<td>A Vblock System and fabric</td>
</tr>
<tr>
<td>Vblock_Fabric_B</td>
<td>A Vblock System and fabric</td>
</tr>
<tr>
<td>Global</td>
<td>A global Vblock System and fabric</td>
</tr>
</tbody>
</table>

EMC Ionix UIM/P performs MAC address pool selection in this order:

1. EMC Ionix UIM/P allocates resources from a range that matches the specified Vblock System and the particular fabric.
2. If not found, EMC Ionix UIM/P allocates resources from a range that matches the specified Vblock System.
3. If not found, EMC Ionix UIM/P tries to allocate resources from the global range.
4. If not found, provisioning fails.
Provisioning can also fail if EMC Ionix UIM/P finds a range but the resources are allocated.

Addresses from the pool are not used until all the addresses in the existing pools have been allocated. Each pool provides a range of identifiers from which EMC Ionix UIM/P pulls to assign to system resources when it provisions a service. The pools automate the resource assignments ensuring that a unique identifier is used for each resource and eliminate the need for infrastructure administrators to track the identifiers used during resource allocation.

Additionally, EMC Ionix UIM/P ensures that the identifiers are unique for all resources managed through multiple Vblock Systems discovered by the same instance of EMC Ionix UIM/P.

VCE recommends that you:

- Select ranges that minimize or eliminate the risk of conflict with existing devices in the current network environment.
- Identify the MAC addresses currently used in the environment and create ranges to exclude them from EMC Ionix UIM/P resource allocation.
- Use ranges starting with 00:25:B5, for example: 00:25:B5:AA:00:01.

Before you begin

Obtain the MAC address information.

Procedure

1. Log in to EMC Ionix UIM/P.
2. From the Administration view, click the MAC Pool tab.
3. Click Add.
4. Type a Name.
5. Type a Start and End range of MAC addresses that are available to allocate to each interface port on an Ethernet network at the time the service is provisioned.
   
   **NOTE:** The range format is six pairs of hexadecimal digits, where each pair is separated by a colon. It is recommended to use ranges starting with 00:25:B5.

   For example, 00:25:B5:AA:00:01.

6. Select either Global or Vblock. If you select Vblock, you can also select Fabric A, Fabric B, or Both.
7. Click OK.

Results

If the range was added successfully, it appears on the appropriate tab.

What to do next

When all the addresses from the existing ranges have been allocated, use the MAC address pool for resource allocation.
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

Deleting a MAC pool (see page 37)
Cisco UCS Manager GUI Configuration Guide
About this task

**NOTE:** This procedure is applicable to EMC Ionix UIM/P version 3.0, and later. Refer to the VCE Release Certification Matrix to verify what version of EMC UIM/P you are running.

Included ranges containing values that were previously issued can only be expanded to include additional values. Only existing ranges that have not been allocated can be excluded. If you attempt to exclude part of a range that has previously been allocated for use, the application returns an error.

A MAC address pool can be **Global** or **Vblock**, and designated as **Fabric A**, **Fabric B** or both, by selecting a tag used by EMC Ionix UIM/P for selection precedence.

<table>
<thead>
<tr>
<th>If you designate a pool as...</th>
<th>Then it identifies...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vblock System</td>
<td>A Vblock System</td>
</tr>
<tr>
<td>Vblock System_Vblock_Fabric_A</td>
<td>A Vblock System and fabric</td>
</tr>
<tr>
<td>Vblock System_Vblock_Fabric_B</td>
<td>A Vblock System and fabric</td>
</tr>
<tr>
<td>Global</td>
<td>A global Vblock System and fabric</td>
</tr>
</tbody>
</table>

Addresses from the pool are not used until all the addresses in the existing pools have been allocated. Each pool provides a range of identifiers from which EMC Ionix UIM/P pulls to assign to system resources when it provisions a service. The pools automate the resource assignments ensuring that a unique identifier is used for each resource and eliminate the need for infrastructure administrators to track the identifiers used during resource allocation.

Additionally, EMC Ionix UIM/P ensures that the identifiers are unique for all resources managed through multiple Vblock Systems discovered by the same instance of EMC Ionix UIM/P.

When you exclude a MAC address range, the pool is no longer available for use in deployed services.

VCE recommends that you:

- Select pool ranges that minimize or eliminate the risk of conflict with existing devices in the current network environment.
- Identify the MAC addresses currently used in the environment and create ranges to exclude them from EMC Ionix UIM/P resource allocation.
- Use ranges starting with 00:25:B5, for example: 00:25:B5:AA:00:01.

**Before you begin**

Obtain the:

- MAC address range currently being used.
- MAC address range that you want to add.

**Procedure**

To edit a range:

1. Log in to EMC Ionix UIM/P.
2 From the **Administration** view, select the **MAC Pool** tab.

3 Select a range, and click **Edit**.

4 From here, you can:
   a Change the **Name**.
   b Change a **Start** and **End** range of MAC addresses that are available to allocate to each interface port on an Ethernet network at the time the service is provisioned.

   ① **NOTE**: The format is 6 pairs of hexadecimal digits, where each pair is separated by a colon. It is recommended to use ranges starting with 00:25:B5.

   For example, **00:25:B5:AA:00:01**.

c Change the tag either **Global** or **Vblock**. If you select **Vblock**, you can also select **Fabric A**, **Fabric B**, or **Both**.

   ① **NOTE**: You cannot change the tag if any MAC addresses in the range are allocated.

5 Click **OK**.

To exclude a range:

1 From the **Administration** view, select the **MAC Pool** tab.

2 Click **Exclude**.

3 Edit the **Start** or **End** range of MAC addresses to be excluded from resource allocation.

4 Click **OK**.

5 To verify that a pool was expanded successfully, verify that the free and total addresses are increased in the pool. To verify that a range was excluded, verify that the range you excluded from the pool does not display in the list of available addresses.

**What to do next**

When all the addresses from the existing ranges have been allocated, use the MAC address pool for resource allocation.

**Related information**

- **Adding a MAC address range using EMC UIM/P 3.x** (see page 32)
- **Deleting a MAC address range using EMC UIM/P 3.x** (see page 37)

**Reversing the procedure**

**Procedure**

To reverse this procedure, repeat it and type the original values in the **Start** and **End** fields or select the exclusion range of addresses and click **OK**.
Deleting a MAC address range using EMC UIM/P 3.x

Use this procedure to delete an existing MAC address range from the MAC address pool.

About this task

NOTE: This procedure is applicable to EMC Ionix UIM/P version 3.0, and later. Refer to your Release Certification Matrix to verify what version of EMC UIM/P you are running.

The range is no longer available to a resource. You cannot delete any range in the pool that is allocated to a resource.

Before you begin

Obtain the MAC address information.

Procedure

1. Log in to EMC Ionix UIM/P.
2. From the Administration view, select the MAC address Pool tab.
3. Select a range, and click Delete.
4. Click Yes.
5. Verify that the range no longer exists in the pool.

Related information

Adding a MAC address range using EMC UIM/P 3.x (see page 32)
Editing or excluding a MAC address range using EMC UIM/P 3.x (see page 34)

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 34)

Adding an IP pool and range of addresses using EMC UIM/P 3.x

Use this procedure to add or edit IP pool general attributes.

About this task

**NOTE:** This procedure is applicable to EMC Ionix UIM/P version 3.x. Refer to the VCE Release Certification Matrix to verify what version of EMC UIM/P you are running.

IP pools are used for NFS data storage (NFS is available only on VCE System).

Before you begin

Obtain the IP address information.

Procedure

1 From the Administration view, click the Identity Pools tab.
2 Click the IP Pools tab.
3 Click Add to create a new IP pool.
4 Click the General tab.
5 Click Edit.
6 Type a Name.
7 Type a Description.
8 Type the Netmask address.
9 Type the Gateway address.
10 Select either the Global or Vblock tag.
11 Click Save.
12 Click **Range Definitions** tab.

13 Click **Add**.

14 Type **Start** IP address and **End** IP address.

15 Click **OK**.

**Results**

If the range was added successfully, it appears on the appropriate tab.

**Related information**

- Deleting an IP pool or range of addresses using EMC UIM/P 3.x (see page 40)
- Creating an isolation zone service using EMC UIM/P 3.x (see page 41)

**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.
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

Deleting an IP pool or range of addresses using EMC UIM/P 3.x

Use this procedure to delete an IP pool or range of addresses.

Procedure

Use this procedure to delete an IP pool.

NOTE: You can only delete IP pools that have no allocated identifiers.

1 From the Administration view, click the Identity Pools tab.
2 Click the IP Pools tab.
3 Select a pool, and click Delete.
4 Click Yes.

Use this procedure to delete a range from an IP pool:

1 From the Administration view, click the Identity Pools tab.
2 Click the IP Pools tab.
3 Select an IP Pool, and click Edit.
4 Click the Range Definitions tab.
5 Select a range, and click Delete.

Related information

Adding an IP pool and range of addresses using EMC UIM/P 3.x (see page 38)
Creating an isolation zone service using EMC UIM/P 3.x

Use this procedure to create a service for isolation zones when using NFS storage.

About this task

**NOTE:** This procedure is applicable to EMC Ionix UIM/P version 3.1, and later. Refer to the VCE Release Certification Matrix to verify what version of EMC UIM/P you are running.

Isolation zones allow for multiple VSAN and VLAN support. Isolation zones isolate two or more groups using the same Vblock System. Isolation zones apply only when using NFS storage.

Before you begin

Obtain the Isolation zone information.

Procedure

1. From the Service Catalog view, highlight the service offering.
2. Click Create Service.
3. Type the Service Name.
4. Type the Description.
5. Select the Discovered Vblock.
6. Select the Isolation Zone.
7. Click OK. The Edit Service window displays.
8. Highlight the server.
9. If necessary, you can edit Host Name, Grade, Use DHCP, IP Address, Status and Description.
10. Type the Netmask address.
11. Type the Gateway address.
12. Select or deselect Enable Activation Ping Test.
13. Select the BIOS Policy.
14. Click OK.

Related information

[Adding an IP pool and range of addresses using EMC UIM/P 3.x](#) (see page 38)

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.
On the Work window, select the General tab.

In the NTP Servers area, click the + on the table icon bar.

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 43)

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 42)

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

Removing an SNMP server (see page 47)
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>Enabled checkbox</td>
<td>Check if this server sends SNMP traps to the designated host.</td>
</tr>
<tr>
<td>SNMP Port field</td>
<td>The port that the server uses to communicate with the SNMP host. This value cannot be changed.</td>
</tr>
<tr>
<td>Access Community String field</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>System Contact field</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>System Location field</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 Add 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>
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>

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 column</td>
<td>IP address where SNMP trap information is sent.</td>
</tr>
</tbody>
</table>

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**.

**Related information**

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

**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

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

Important: Do not use this procedure if EMC Ionix UIM/P is used for provisioning.

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 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.

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>_ <Vblock ID>
      ■ Service Profile Template Identifier = 1
      ■ Blade Type = B200 if installing B200 blades or B250 if installing B250 blades
      ■ Vblock ID = 01 first Vblock System or 02 second Vblock 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.
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

**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 UCSM 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**.

**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**.
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.

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</td>
<td>1240 only 1240 and 1280</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vNIC2 &gt; vCON2, vNIC3 &gt; vCON2, vHBA1 &gt; vCON2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1280</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco B200 M3</td>
<td>1240</td>
<td>System managed</td>
<td>Statically mapped</td>
<td></td>
<td>1240 only 1240 and 1280</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vNIC0 &gt; vCON1, vNIC1 &gt; vCON1, vHBA0 &gt; vCON1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vNIC2 &gt; vCON2, vNIC3 &gt; vCON2, vHBA1 &gt; vCON2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1280</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco B200 M4</td>
<td>1340</td>
<td>Statically mapped</td>
<td>Statically mapped</td>
<td></td>
<td>1340 only 1340 and 1380</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vNIC0 &gt; vCON1, vNIC1 &gt; vCON1, vHBA0 &gt; vCON1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>N/A</td>
<td>vNIC0 &gt; vCON1</td>
<td>vNIC2 &gt; vCON1</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vHBA0 &gt; vCON1</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>vNIC3 &gt; vCON1 vHBA0 &gt; vCON1 vHBA1 &gt; vCON1</td>
<td>vNIC2 &gt; vCON2 vNIC3 &gt; vCON2 vHBA1 &gt; vCON2</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>1380</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco B230 M2</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td>1280 only</td>
</tr>
<tr>
<td>1280</td>
<td>System managed</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco B250 M2 (EoS)</td>
<td>Palo</td>
<td>System managed</td>
<td>N/A</td>
<td></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>vNIC0 &gt; vCON1 vNIC1 &gt; vCON1 vHBA0 &gt; vCON1 vNIC2 &gt; vCON2 vNIC3 &gt; vCON2 vHBA1 &gt; vCON2</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1280</td>
<td>System managed</td>
<td>Statically mapped</td>
<td>N/A</td>
<td></td>
<td>1280 only</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>N/A</td>
<td></td>
<td>1240 and 1280</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 and 1280</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vNIC0 &gt; vCON1 vNIC1 &gt; vCON1 vHBA0 &gt; vCON1 vNIC2 &gt; vCON3 vNIC3 &gt; vCON3 vHBA1 &gt; vCON3</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1280</td>
<td>System managed</td>
<td>vNIC0 &gt; vCON1 vNIC1 &gt; vCON1 vHBA0 &gt; vCON1 vNIC2 &gt; vCON3 vNIC3 &gt; vCON3</td>
<td>N/A</td>
<td></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></td>
<td>vHBA1 &gt; vCON3</td>
<td>N/A</td>
<td>2 x 1280 only</td>
</tr>
<tr>
<td>Cisco B440 M2 with VMware vSphere 5.1</td>
<td>2 x 1280</td>
<td>N/A</td>
<td>Statically mapped</td>
<td>vNIC2 &gt; vCON1, vNIC3 &gt; vCON1, vHBA1 &gt; vCON1, vNIC0 &gt; vCON2, vNIC1 &gt; vCON2, vHBA0 &gt; vCON2</td>
<td>N/A</td>
</tr>
<tr>
<td>Cisco B440 M2 with VMware vSphere 5.5</td>
<td>2 x 1280</td>
<td>N/A</td>
<td>Statically mapped</td>
<td>vNIC0 &gt; vCON1, vNIC1 &gt; vCON1, vHBA0 &gt; vCON1, vNIC2 &gt; vCON2, vNIC3 &gt; vCON2, vHBA1 &gt; vCON2</td>
<td>N/A</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>vNIC0 &gt; vCON1, vNIC1 &gt; vCON1, vHBA0 &gt; vCON1, vNIC2 &gt; vCON2, vNIC3 &gt; vCON2, vHBA1 &gt; vCON2</td>
</tr>
<tr>
<td></td>
<td>2 x 1280</td>
<td>N/A</td>
<td>Statically mapped</td>
<td>Statically mapped</td>
<td>vNIC0 &gt; vCON1, vNIC1 &gt; vCON1, vHBA0 &gt; vCON1, vNIC2 &gt; vCON2, vNIC3 &gt; vCON2, vHBA1 &gt; vCON2</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; vCON4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vhBA2 &gt; vCON3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vhBA3 &gt; vCON1</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**.
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.

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.

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.

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_serialnumber.

d. Click OK.

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.
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 create four Service Profile templates for creating production blades that will run VMware.

**About this task**

**Important**: This procedure cannot be used if EMC Ionix UIM/P is used for provisioning.

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

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 ID
      ■ Service Profile Template Identifier = 1
      ■ Blade Type = B200 if installing B200 blades or B250 if installing B250 blades
      ■ VCE System ID = 01 first VCE System or 02 second VCE 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.
   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

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 UCS Manager 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.
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 in Configuring service profile templates.

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

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

- If a VCE 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.

Add the four vNICs and two vHBAs to the vCON in the order 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>Cisco 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>vNIC5 &gt; vCON2</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Cisco B200 M3</td>
<td>1240</td>
<td>System managed</td>
<td>vNIC4 &gt; vCON1</td>
<td>N/A</td>
<td>1240 1240 and 1280</td>
</tr>
<tr>
<td></td>
<td>1280</td>
<td>N/A</td>
<td>vNIC5 &gt; vCON2</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Cisco B200 M4</td>
<td>1340</td>
<td>vNIC4 &gt; vCON1</td>
<td>vNIC4 &gt; vCON1</td>
<td>N/A</td>
<td>1340 only 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></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></td>
<td>1280</td>
<td>System managed</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Cisco B250 M2 (EoS)</td>
<td>1240</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>vNIC4 &gt; vCON1</td>
<td>vNIC4 &gt; vCON1</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Cisco B260 M4</td>
<td>1240</td>
<td>System managed</td>
<td>vNIC4 &gt; vCON1 vNIC5 &gt; vCON2</td>
<td>N/A</td>
<td>1240 1240 and 1280</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></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco B420 M3</td>
<td>1240</td>
<td>System managed</td>
<td>N/A</td>
<td>N/A</td>
<td>1240</td>
</tr>
<tr>
<td></td>
<td>1280</td>
<td>System managed</td>
<td>vNIC4 &gt; vCON1 vNIC5 &gt; vCON2</td>
<td>N/A</td>
<td>1280 only 1240 and 1280</td>
</tr>
<tr>
<td>Cisco B440 M2 with VMware vSphere 5.1</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>Cisco B440 M2 with VMware vSphere 5.5</td>
<td>2 x 1280</td>
<td>N/A</td>
<td>vNIC4 &gt; vCON1 vNIC5 &gt; vCON2</td>
<td>N/A</td>
<td>2 x 1280 only</td>
</tr>
<tr>
<td>Cisco B460 M4</td>
<td>2 x 1240</td>
<td>N/A</td>
<td>vNIC4 &gt; VCON1 vNIC5 &gt; vCON2</td>
<td>TBD</td>
<td>2 x 1240 ((2 x 1240) + (2 x 1280))</td>
</tr>
<tr>
<td></td>
<td>2 x 1280</td>
<td>N/A</td>
<td>vNIC4 &gt; VCON2 vNIC5 &gt; vCON4</td>
<td>vNIC4 &gt; vCON2 vNIC5 &gt; vCON4</td>
<td>2 x 1280 ((2 x 1240) + (2 x 1280))</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.
   e  Click OK.

32  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.

### Cloning the service profile templates

Follow this procedure to clone and modify the service profile templates.

**Procedure**

1  Right-click the service profile template that was just created.
2 Click **Create a Clone**.

3 For **Clone Name**, type a name for the service profile template.

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

5 Click **OK**.

6 To modify the cloned service profile template, select the service profile template and navigate to the **Boot Order** tab.

7 Select **Modify Boot Policy**.

8 Select the correct boot policy. For example: **2_ VX_6215**

9 Click **OK**.

**What to do next**

Repeat these steps as needed to clone more templates.

**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.
5 Choose the appropriate blade for this profile.

6 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.

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

8 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.

⚠️ CAUTION: 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.

Related information

Adding a VLAN to a service profile template (see page 70)

Adding a VLAN to a service profile using EMC UIM/P (see page 70)
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 a service profile using EMC UIM/P

The following procedure adds a VLAN using EMC UIM/P.

About this task

For more information on EMC UIM/P, see the *EMC Ionix Unified Infrastructure Manager/Provisioning Product Overview Guide*.

**NOTE:** EMC UIM/P only supports a single domain.

Procedure

1. Log in to EMC UIM/P.
2. Navigate to the **Service Manager** and select the service offering to which you want to add the VLAN. This step adds the VLAN to all the blades that were provisioned with this service offering.
3. Click **Edit**.
4. In the **Edit Services** window, select the **Networks** tab. Two or four Ethernet interfaces appear.
5. Select the first interface and click **Edit**.
6 In the **Edit VNIC** window, select a VLAN from the **Available VLANs** list and click **Add** and **Save**.

7 Repeat these steps for the other Ethernet interfaces. The **Edit Services** window shows the status of the Ethernet interfaces as **Changes Pending**.

8 Close the **Edit Services** window. The UIM/P Dashboard shows the provisioning status as **Partially Provisioned**.

9 Click **Apply** to initiate the changes to the service profiles. The UIM/P Dashboard shows the provisioning status as **Workflow in Progress**. Depending on the number of blades, the provisioning can take some time to finish.

**Results**

Once provisioning is finished, the new VLAN appears and the EMC UIM/P Dashboard shows the provisioning status as **Provisioned**.

**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.

**Related information**

[EMC Ionix Unified Infrastructure Manager/Provisioning Product Overview Guide](#)

### 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`
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 73)
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`

   \(\text{NOTE}\): 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`

   \(\text{NOTE}\): `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`

   \(\text{NOTE}\): `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 72)
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 73)
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.
To run the configuration, type: `Switch-A# config terminal`

To specify the port channel, type: `Switch-A(config)# interface port-channel port_channel_number`

To add the VLANs, type: `Switch-A(config)# switchport trunk allowed vlan add VLAN_IDs`

Repeat this procedure on the peer Cisco Nexus series switch.

Related information

---

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

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**.
l 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 79)
- Removing port channels from VLANs for disjoint layer 2 networks (see page 79)

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 76)

Removing port channels from VLANs for disjoint layer 2 networks (see page 79)

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

Adding port channels to VLANs for disjoint layer 2 networks (see page 76)

Viewing port channels assigned to VLANs for disjoint layer 2 networks (see page 79)

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

### 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:
   ```
   ![Dir output]

   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.
[50%]
[############################] 100% -- SUCCESS
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%] 100% -- SUCCESS
Notifying services about system upgrade.
[100%] 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-channel152 in VLAN0001 is Designated. Topology change could occur during ISSU.
Upgrade needs to be disruptive!!!
To install the new Cisco NX-OS images, type: `VSJ3X2N554BA(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`
9 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.
VSJ3X2N5548A(config)# 2011 Sep  8 18:16:43 VSJ3X2N5548A Sep  8 18:16:43 %KERN-0-
SYSTEM_MSG: Shutdown Ports.. - kernel
2011 Sep  8 18:16:43 VSJ3X2N5548A 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!

10 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.
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:
   - Type `MDS# cd bootflash:`
To verify there is enough free space, type `MDS# dir`.

Type `MDS# copy ftp://ftp_server_addr/ filename.bin filename.bin`.

type `MDS# copy ftp://ftp_server_addr/ filename.bin filename.bin`.

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

- Type `MDS# cd bootflash:`
- Type `MDS# dir`.

While in configure mode, type: `VSJ3X2M9148B# configure terminal`.

Type configuration commands, one per line. End with CNTL/Z.

`VSJ3X2M9148B(config)# no logging level all`.

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`.

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.

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`.

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

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

a. Type `MDS# cd bootflash:

b. Type `MDS# dir`

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

Type configuration commands, one per line. End with CNTL/Z.

`VSJ3X2M9148B(config)# no logging level all`

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`

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.

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`

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`. 

89  |  Managing Cisco MDS switches
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`
6. 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.
To view the port licenses, type: `show port-license`

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

To configure the interface where license is being moved from, type: `Switch-A(config)# interface fcinterface_id`

To disable the license on that interface, type: `Switch-A(config-if)# no port-license`

To exit, type: `Switch-A(config-if)# exit`

To configure the interface where license is being moved to, type: `Switch-A(config)# interface fcinterface_id`

To acquire the license on that interface, type: `Switch-A(config-if)# port-license acquire`

To end the configuration, type: `Switch-A(config-if)# end`

To verify that appropriate ports have enabled licenses, type: `show port-license`

Related information

Disabling port licenses (see page 93)

Cisco MDS 9000 Family NX-OS Licensing Guide, Release 6.x

Disabling port licenses

Use this procedure to disable port licenses.

Procedure

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

2. To configure the interface where license is being moved, type: `Switch-A(config)# interface fcinterface_id`

3. To disable the license on that interface, type: `Switch-A(config-if)# no port-license`

4. To exit, type: `Switch-A(config-if)# end`
Managing storage resources

Logging on to a storage array

Use this procedure to log into the storage array.

Before you begin

Obtain the:

- IP addresses of the two storage processors.
- IP address of the primary Control Station (unified only).
- Username and password for the storage array.

Procedure

1. Open a browser and type the IP address of either storage processor or the primary Control Station.
2. From the EMC Unisphere window, click Start a new EMC Unisphere session.
3. Type your username and password for the storage array, or type the LDAP user ID (select Use LDAP in this instance) and click Login.
4. From the NAT Mode window, type the required IP addresses, and click Add IP.
   
   **NOTE:** The NAT Mode window does not appear when connecting from within a VCE System or when using the native IP addresses of the storage processors or the Control Station. The NAT window appears only when connecting to EMC Unisphere from outside of a VCE System.
5. When the Agreement window appears, click Accept.
6. From the EMC Unisphere window, under the list of storage arrays, click on a storage array. From the main menu of the storage array, the remaining tasks that require action appear. The menu bar at the top lists all of the options available for the array.
7. Click on any of the main menu options to view available sub-menus.

Creating storage pools

Use this procedure to create a storage pool in the storage array.

About this task

VCE recommends that you use drives in multiples of RAID group sizes. Only create new virtual provisioning (VP) pools if needed 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.
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 five.

Bare metal applications require a dedicated storage pool.

Thin pools may reach an oversubscription ratio of 4:1. When a pool reaches 60 percent of capacity a warning event is generated. When a pool reaches 80 percent, more drives must be added to bring the pool below 60 percent utilized.

Before you begin

Verify that unused drives are available in the storage array.

Procedure

1. Log into the EMC storage device on which you want to create the storage pool.
2. Select Storage > Storage Configuration > Storage Pools.
3. When the Storage Pools window appears, click Create.
4. From the Create Storage Pool window, select Pool for the Storage Pool Type, type the name of the pool, and select a RAID type.
5. Under Disks, click Manual for disk selection and click Select. In the Disk Selection window, a list of available disks appears.
6. Highlight the disks you want to use for the storage pool and use the arrow key to add them to the list of selected disks. Click OK. When the Create Storage Pools window appears, the list of added disks appears.
7. Select Scheduled Auto-Tiering to enable FAST VP automated data movement if desired.
8. Select the Advanced tab to change the pool threshold from 70 percent to 60 percent.
9. Verify that all of the information is correct and click Apply.
10. When the confirmation window appears, click Yes. A confirmation message appears or, if you selected a number of drives that is not a multiple of the RAID group size, this warning appears:
11. Click OK to confirm the success or No to go back and reselect disks. In the Pools menu, the last entry is the pool that has just been created and is in the process of being initialized. Once complete, the State appears as Ready.
12. Select Storage > Storage Configuration > Storage Pools. From the list of storage pools, verify that the new pool appears.

What to do next

After the storage pool has been created, you can create LUNs in the storage pool.
Expanding a storage pool

Use this procedure to expand a storage pool.

About this task
VCE recommends that you expand the storage group in multiples of the RAID group size.

NOTE: A storage pool cannot be reduced to its previous size.

Before you begin

Before performing this task, verify that storage pools exist and disk drives are available to expand the storage pool. Best practice is for the pool to be expanded by the same number of drives in the pool, but this is not always feasible.

Procedure

1. Log on to the EMC storage device to create the storage pool.
2. Select Storage > Storage Configuration > Storage Pools.
3. When the Pools window appears, select the storage pool and click Expand.
4. From the Expand Storage Pool window, under Disks, select Manual and click Select.
5. When the Disk Selection window appears, verify that All Cabinets is selected.
6. Under Available Disks, highlight a disk and use the arrow key to add it to the Selected Disks field. Click OK.
7. From the Expanded Storage Pool window, view your pool, and click OK.
8. If your selection does not support best practices, an error message appears. You can click Yes to continue, or No to cancel out and repeat the procedure.
9. When the confirmation window appears, click OK.
10. Right-click the storage pool and select Properties. Select the Disks tab and view the storage pool. The list of disks should include the old disks as well as the new ones that were added.

What to do next
Use the expanded capacity to grow existing LUNs or create new ones.

Creating a VSAN

Use this procedure to create a VSAN for the Cisco Nexus 55xxUP Switches.

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
   information: name: VSAN0001
   state: active
   interoperability mode: default
   loadbalancing: src-id/dst-id/
   oxid: operational 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 fc interface_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`

**Monitoring a storage pool**

Use this procedure to monitor pools in a storage array.

**Before you begin**

Create a storage pool.

**Procedure**

1. Log in to EMC Unisphere and select the storage array you want to monitor.

2. Select *Storage > Storage Configuration > Storage Pools*. 
When the **Pools** window appears, select the storage pool you want to monitor and click **Properties**. The **Storage Pool Properties** window appears. In the window, there are four tabs that can be used to monitor different aspects of the storage pool. The **General** tab shows the physical and virtual capacities, including total capacity, consumed capacity and the percentage full.

Select the **Disks** tab to view the state of the individual drives that make up the storage pool.

Click **OK** when done.

**Related information**

[Creating storage pools](#) (see page 94)

## Creating a storage group

Use this procedure to create a storage group.

**About this task**

The information in this procedure is specific to environments or situations where EMC UIM/P is not used. If EMC UIM/P manages the VCE Systems resources, refer to the **EMC UIM/P User Guide** procedures to provision a new service.

**Procedure**

1. Log into EMC Unisphere and select a storage array to create the storage group.
2. Select **Hosts > Storage Groups**. In the **Storage Groups** window, a list of existing storage groups in the storage array appears.
3. To create a new group, click **Create**.
4. When the **Create Storage Group** window appears, type a name and click **Apply**.
5. When the confirmation window appears, click **Yes**.
6. Click **No** to end the procedure or **Yes** to add LUNs. Refer to the appropriate procedure for adding LUNs and hosts.
7. Select **Storage > Storage Groups**, and verify that the new storage group appears in the list.

**What to do next**

Connect the hosts and the LUNs to the storage group.

**Reversing the procedure**

**Procedure**

1. To reverse this procedure, select **Hosts > Storage Groups**.
2. From the list of storage groups, select the storage group and click **Delete**.
Connecting a host to a storage group

Use this procedure to connect hosts to a storage group.

Before you begin
Before performing this task, the storage group must exist and the hosts that you want to connect to should appear in the list of hosts seen by the storage array.

Procedure

1. Log into EMC Unisphere and select the storage array on which you want to connect the host.
2. Select Hosts > Storage Groups.
3. When the Storage Groups window appears, select the storage group you wish to connect the host to and click Connect Hosts.
4. From the Storage Group Properties window, select the Hosts tab.
   
   ✅ NOTE: By default, Show Hosts: Not connected is already selected. This setting should not be changed unless you want to add a host to more than one storage group.
5. From the list of available hosts, use the arrow key to select the host you want to add to the Hosts to be Connected field, and click Apply.
6. When the confirmation messages appear, click Yes and OK.
7. From the Storage Groups menu, right-click on the Storage Group and select Properties. Select the Hosts tab to view that the hosts you connected the storage group to appear in the list on right.

What to do next
Connect a LUN to the storage group.

Related information

Connecting a LUN to a storage group (see page 104)

Creating a boot LUN

Use this procedure to install VMware vSphere ESXi on Cisco UCS hosts without using the deployment appliance.

Before you begin

Verify that you have access to the VMware vSphere ESXi ISO file, or a custom VMware vSphere ESXi ISO file created using VMware Image Builder. For version information and download links, refer to the appropriate Release Certification Matrix.
Procedure

To create RAID Group 0, type:

```
naviseccli -h <10.251.101.40> createrg 0 <0_0_9 0_0_10 0_0_11 0_0_12 0_0_13> -pri medium -rm no -raidtype r5
```
Create boot LUNs on RAID group 0. The following example is for 32 hosts in four VMware vSphere ESXi clusters.

```bash
naviseccli -h 1<10.251.101.40> bind r5 0 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0
naviseccli -h 1<10.251.101.40> bind r5 1 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0
naviseccli -h 1<10.251.101.40> bind r5 2 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0
naviseccli -h 1<10.251.101.40> bind r5 3 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0
naviseccli -h <10.251.101.40> bind r5 4 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0
naviseccli -h <10.251.101.40> bind r5 5 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0
naviseccli -h <10.251.101.40> bind r5 6 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0
naviseccli -h <10.251.101.40> bind r5 7 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0
naviseccli -h <10.251.101.40> bind r5 8 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0
naviseccli -h <10.251.101.40> bind r5 9 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0
naviseccli -h <10.251.101.40> bind r5 10 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0
naviseccli -h <10.251.101.40> bind r5 11 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0
naviseccli -h <10.251.101.40> bind r5 12 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0
naviseccli -h <10.251.101.40> bind r5 13 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0
naviseccli -h <10.251.101.40> bind r5 14 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0
naviseccli -h <10.251.101.40> bind r5 15 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0
naviseccli -h <10.251.101.40> bind r5 16 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0
naviseccli -h <10.251.101.40> bind r5 17 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0
```
navisecci -h <10.251.101.40> bind r5 18 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0

navisecci -h <10.251.101.40> bind r5 19 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0

navisecci -h <10.251.101.40> bind r5 20 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0

navisecci -h <10.251.101.40> bind r5 21 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0

navisecci -h <10.251.101.40> bind r5 22 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0

navisecci -h <10.251.101.40> bind r5 23 -rg 0 -cap 20 -rc 1 -sp a -sq gb -wc 1 -fastcache 0

navisecci -h <10.251.101.40> bind r5 24 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0

navisecci -h <10.251.101.40> bind r5 25 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0

navisecci -h <10.251.101.40> bind r5 26 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0

navisecci -h <10.251.101.40> bind r5 27 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0

navisecci -h <10.251.101.40> bind r5 28 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0

navisecci -h <10.251.101.40> bind r5 29 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0

navisecci -h <10.251.101.40> bind r5 30 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0

navisecci -h <10.251.101.40> bind r5 31 -rg 0 -cap 20 -rc 1 -sp b -sq gb -wc 1 -fastcache 0

Related information

Accessing VCE documentation (see page 10)

Creating a data LUN

Use this procedure for examples for how to create data LUN inside the general VP pool.
Procedure

Modify the following example commands for your specific configuration using the `lun -create` command. The commands create a 3 x 2 TB LUN for each cluster, with a total of four clusters.

**NOTE:** LUNs alternate SP ownership; even LUNs are owned by SP A and odd LUNs are owned by SP B. Data LUN IDs should start at 132 and increase as needed.

```bash

naviseccli -h <10.251.101.40> lun -create -type thin -poolName <Prod-FAST> -sp b -capacity 2000 -sq gb -name <Prod-FAST>-133 -l 133 -tieringPolicy autoTier -initialTier highestAvailable

naviseccli -h <10.251.101.40> lun -create -type thin -poolName <Prod-FAST> -sp a -capacity 2000 -sq gb -name <Prod-FAST>-134 -l 134 -tieringPolicy autoTier -initialTier highestAvailable


naviseccli -h <10.251.101.40> lun -create -type thin -poolName <Prod-FAST> -sp b -capacity 2000 -sq gb -name <Prod-FAST>-137 -l 137 -tieringPolicy autoTier -initialTier highestAvailable

naviseccli -h <10.251.101.40> lun -create -type thin -poolName <Prod-FAST> -sp a -capacity 2000 -sq gb -name <Prod-FAST>-138 -l 138 -tieringPolicy autoTier -initialTier highestAvailable

naviseccli -h <10.251.101.40> lun -create -type thin -poolName <Prod-FAST> -sp b -capacity 2000 -sq gb -name <Prod-FAST>-139 -l 139 -tieringPolicy autoTier -initialTier highestAvailable

naviseccli -h <10.251.101.40> lun -create -type thin -poolName <Prod-FAST> -sp a -capacity 2000 -sq gb -name <Prod-FAST>-140 -l 140 -tieringPolicy autoTier -initialTier highestAvailable

naviseccli -h <10.251.101.40> lun -create -type thin -poolName <Prod-FAST> -sp b -capacity 2000 -sq gb -name <Prod-FAST>-141 -l 141 -tieringPolicy autoTier -initialTier highestAvailable

naviseccli -h <10.251.101.40> lun -create -type thin -poolName <Prod-FAST> -sp a -capacity 2000 -sq gb -name <Prod-FAST>-142 -l 142 -tieringPolicy autoTier -initialTier highestAvailable

naviseccli -h <10.251.101.40> lun -create -type thin -poolName <Prod-FAST> -sp b -capacity 2000 -sq gb -name <Prod-FAST>-143 -l 143 -tieringPolicy autoTier -initialTier highestAvailable
```
Connecting a LUN to a storage group

Use this procedure to connect a LUN to a storage group.

Before you begin

Verify that the LUNs and storage groups exist.

Procedure

1. Log into EMC Unisphere and select the storage array on which you want to connect the LUN.
2. Select Hosts > Storage Groups.
3. From the Storage Groups window, select a storage group and click Connect LUNs.
4. When the Storage Group Properties window appears, select the LUNs tab.
5. In the Show LUNs field, select ALL.
6. Under Available LUNs, expand the list, select the LUN you want to connect, and click Add.
7. When the LUN appears in the Selected LUNs field, modify the host LUN ID (HLU) if necessary, and click Apply.

**NOTE:** VCE recommends using the LUN ID as the HLU except in case of boot LUNs.

8. When the confirmation windows appear, click Yes and OK.
9. From Hosts > Storage Groups, select the Storage Group > Properties. Select the LUNs tab and view the LUN.

What to do next

Connect a host to the storage group.

Related information

Connecting a host to a storage group (see page 99)

Expanding a LUN

Use this procedure to expand a LUN.

About this task

⚠️ **CAUTION:** Do not use this procedure if EMC Ionix UIM/P manages the VCE Systems resources.
Before you begin

Before performing this task, verify that the LUN you intend to expand exists and that there is enough space in the storage pool or RAID group to expand the LUN.

Procedure

1. Log into EMC Unisphere and select a storage array.
2. Select Storage > LUNs > LUNs.
3. When the LUN window appears, right-click on the LUN and select Expand.
4. Type the new user capacity which is the total capacity, not the capacity by which to expand the LUN. Click OK.
5. Select Storage > LUNs > LUNs and verify the capacity of the LUN.

Monitoring a RAID group

About this task

Use this procedure to monitor a RAID group.

Before you begin

Verify that at least one RAID group exists.

Procedure

1. Log into EMC Unisphere and select the storage array to monitor.
2. Select Storage > Storage Configuration > Storage Pools.
3. When the next screen appears, select the RAID Group tab.
4. Right-click the RAID group to monitor and select Properties.
5. In the RAID Group Properties window, the General, Disks, and Partitions tabs can be used to monitor different aspects of the RAID group such as total capacity and free capacity.
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: 
      ```
      #server_unmount movername -perm fs_name fs_mountpoint
      ```
   c. To mount the system with Uncached Write enabled, type: 
      ```
      #server_mount movername -option rw, uncached fs_name fs_mountpoint
      ```
   d. To verify the setting, type: 
      ```
      #server_mount ALL
      ```

7. 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 108)
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)
   d. 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 106)
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 106)
Creating an NFS export on a storage array (see page 108)
Unmounting the NFS export (see page 110)
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 109)
Creating a file system on a storage array (see page 106)

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.

Related information

Creating a CIFS share (see page 113)
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 114)

### 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.

5 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.
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.

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 113)
Managing VMware vSphere ESXi 6.0, 5.5, and 5.1

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, 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.

Related information

Accessing VCE documentation (see page 10)
Patching VMware vSphere ESXi hosts with the VMware Update Manager (see page 148)

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></td>
<td>512 for VMware vSphere 5.5</td>
</tr>
<tr>
<td></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.
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 "512"){
        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.
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/s/article/2110294).

2. Refer to the Backing Up and Restoring vCenter Server section in the VMware vSphere 6.0 Documentation Center, 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. 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

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.

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.

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.

Related information

Unlocking by using another session or account (see page 140)

Unlocking by resetting the administrator password (see page 141)
Unlocking by using another session or account

Use this procedure to unlock an account by using another session or account.

Before you begin

Obtain network access and administrative privileges to the VMware vCenter server and VMware vSphere ESXi hosts.

Procedure

1. Log on to the VMware Web Client as an SSO administrator.
2. Select Home.
3. Select Administration.
5. Select the Users tab.
6. Right-click the affected user account and click Unlock.

Unlocking by resetting the administrator password

In emergency situations or if the default policies have been changed, reset the SSO administrator password to unlock the account. Resetting the password also unlocks the administrator account.

About this task

The following characters are not supported in SSO passwords:

- Non-ASCII characters
- Ampersand (&)
- Semicolon ( ; )
- Double quotation mark ( " )
- Single quotation mark ( ' )
- Circumflex ( ^ )
- Backslash ( \ )
- Special characters such as $ and @ work in the SSO password
- An exclamation character (!) in the SSO password for the administrator@vsphere.local user when installing SSO is valid. The SSO installation is successful, but repointing the VMware vSphere Web Client to a different SSO instance fails.
Before you begin

Obtain network access and administrator privileges to the VMware vCenter server and VMware vSphere ESXi hosts.

Procedure

1. Log on to the VMware vCenter Server with a domain administrator account. If VMware vCenter SSO is installed separate from the VMware vCenter Server, log on to the VMware vCenter SSO server.

2. Open an elevated command prompt.

3. To navigate to the vmdird directory where SSO was installed and type:
   ```
   cd Program Files\VMware\Infrastructure\VMware\CIS\vmdird
   ```

4. To open the vdcadmintool service tool, type:
   ```
   c:\Program Files\VMware\Infrastructure\VMware\CIS\vmdird>vdcadmintool.exe
   ```

5. Type 3 to select Reset account password.

6. When prompted for the Account DN, type:
   ```
   cn=Administrator,cn=users,dc=vSphere,dc=local
   ```

7. Use the newly generated password to log on to the administrator@vSphere.local account.

   **NOTE:** If the generated password contains an exclamation mark (!), perform the regeneration process a second time.

What to do next

After the password is regenerated, log on to the VMware vSphere Web Client and change the password to be compliant with the VMware list of unsupported characters.

**Resetting the local password on the VMware vCenter Server Appliance**

Use this procedure to reset the administrator@vsphere.local password on the VMware vCenter Server Appliance.

Procedure

1. Connect to the vCenter Server Appliance using SSH.

   **NOTE:** The Enable or Disable SSH Administrator Login on the VMware vCenter Server Appliance section in the vCenter Server and Host Management Guide contains additional information.

2. To open the vdcadmintool service tool, type:
   ```
   /usr/lib/vmware-vmdir/bin/vdcadmintool
   ```

3. Type 3 to select Reset account password.
When prompted for the Account DN, type:
cn=Administrator,cn=users,dc=vSphere,dc=local

Use the generated password to log on to the administrator@vSphere.local account. If the generated password contains an exclamation mark (!), perform the regeneration process a second time.

What to do next

After the password is regenerated, log on to the VMware vSphere Web Client and change the password to comply with the VMware list of unsupported characters.

Related information

VMware vCenter Server and Host Management Guide

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.

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, 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\vmkdcd`
      - `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
- VMware vSphere 5.1 Upgrade Guide
- Microsoft Knowledge Base article136393

**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: C:\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`d 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.

8 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`

9 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.
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.

Related information

Unlocking by using another session or account
Unlocking by resetting the administrator password

Unlocking by using another session or account

Follow these steps to unlock an account by using another session or account.

Before you begin

You must have network access and administrative privileges to the VMware vCenter server and VMware vSphere ESXi hosts.

Procedure

1. Select Home > Administration > SSO Users and Groups.
2. Right-click the affected user account, such as admin, and click Unlock.

Related information

Unlocking by using another session or account
Unlocking by resetting the administrator password
Unlocking by resetting the administrator password

In emergency situations or if the default policies have been changed, reset the Single Sign-On (SSO) administrator password to unlock the account.

About this task
Resetting the password also unlocks the administrator account.

Before you begin
Obtain network access and administrative privileges to the VMware vCenter server and VMware vSphere ESXi 5.1 hosts.

Procedure

1. Log in to the VMware vCenter SSO server as an administrator.
2. Select Start > Run, type cmd, and click OK.
3. From the Command Prompt window, navigate to: SSOInstallDirectory\utils.
   
   **NOTE:**
   By default, the installation directory is D:\Program Files\ VMware\Infrastructure\SSOServer.
4. Type: rsautil reset-admin-password
5. Type the master password when prompted.
   
   **NOTE:** Use the password selected for the SSO administrator during the SSO installation. If you changed the SSO administrator password after installation, the master password is still the original password.
6. Type the SSO administrator name for which you want to reset the password. For example, admin.
7. Type the new password for the user and then confirm it a second time. The message Password reset successfully appears.

Related information

- Unlocking by using another session or account (see page 140)
- Unlocking by resetting the administrator password (see page 141)

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**

**Back 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.
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.
14. Click **Next** and **Finish**.
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.

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>

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 10)

**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)
- 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 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`
5. To grant access, type:  
   `n1000v(config-port-prof)# switchport access vlan vlan-id`
6. 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`

**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 Nexus 55xxUP switches. 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 is affected.

**Before you begin**

- Verify that VLANs on uplinks exist in Cisco Nexus 55xxUP 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`
3. To use jumbo frames, type:
   ```
   system mtu 9000
   port-profile type ethernet DATA-UPLINK
   vmware port-group
   ```
4. Type `port-profile type ethernet DATA-UPLINK`
5. 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>&lt;br&gt;OR&lt;br&gt;<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>&lt;br&gt;OR&lt;br&gt;<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;</code></td>
</tr>
</tbody>
</table>

Type:

```
channel-group auto mode on mac-pinning
no shutdown
```

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>system vlan 105-107, 109, 116-117</code>&lt;br&gt;OR&lt;br&gt;<code>&lt;ESX mgmt vlan number&gt;, &lt;vMotion vlan number&gt;, &lt;FT vlan number&gt;, &lt;ESX NFS vlan number&gt;, &lt;N1K L3 Control VLAN number&gt;, &lt;L3 vmotion VLAN number&gt;</code></td>
</tr>
<tr>
<td>Block</td>
<td><code>system vlan 105-107, 116-117</code>&lt;br&gt;OR&lt;br&gt;<code>&lt;ESX mgmt vlan number&gt;, &lt;vMotion vlan number&gt;, &lt;FT vlan number&gt;, &lt;N1K L3 Control VLAN number&gt;, &lt;L3 vmotion VLAN number&gt;</code></td>
</tr>
</tbody>
</table>

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>mtu 9000</code></td>
</tr>
<tr>
<td>Block</td>
<td><code>mtu 9000</code> (to use jumbo frames)`</td>
</tr>
</tbody>
</table>

Type:

```
state enabled
```
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
   - end

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

To modify the data port profiles for VMware VM traffic, MGMT, VMotion, Fault Tolerance, NFS, and VSM Layer 3 Control, type the following commands:

```bash
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
copy run start

/***************

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

2 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:
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></td>
</tr>
<tr>
<td></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></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>
</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
Managing service operations

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 using EMC UIM/P 3.x (see page 32)
Adding a UUID range using EMC UIM/P 3.x (see page 14)
Adding a WWNN range using EMC UIM/P 3.x (see page 20)
Adding a WWPN range using EMC UIM/P 3.x (see page 26)
Adding an IP pool and range of addresses using EMC UIM/P 3.x (see page 38)
Accessing VCE documentation (see page 10)
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.

Caution: 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.
   - Caution: EULA=end user license agreement.

4. From the Host Upgrade Menu, select Update All.

5. At the Confirmation screen, select Yes.
From the **Confirmation** screen for the BIOS Update, select **Yes**.

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:

   ```bash
   Switch# copy startup-config [tftp:|SCP|FTP|SFTP]
   ```
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#
```

If there is not enough space, delete the current image.

To save the configuration, type: **copy run start**

To copy the new image to the flash directory in router, type: **VSJ3X2C3560A# copy ftp://ftp:@X.X.X.X c3560e-universalk9-mz.150-1.SE.bin**

Address or name of remote host [10.10.1.39]?
Source filename [c3560e-universalk9-mz.150-1.SE.bin]?
Destination filename [c3560e-universalk9-mz.150-1.SE.bin]?

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`

```
Cisco IOS Software, C3560E Software (C3560E=UNIVERSALK9-M), Version 12.2 (55)SE1
Release Software (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Thu 02-Dec-10 06:44 by prodrel team
Image text-base: 0x00003000, data-base: 0x02800000
ROM: Bootstrap program is C3560E boot loader
BOOTLDR: C3560E Boot Loader (C3560X-HBOOT-M) Version 12.2(53r)SE2,RELEASE SOFTWARE (fc1)

VSJ3X2C3560A uptime is 28 weeks, 2 days, 29 minutes System returned to ROM by power-on
System image file is "flash:/c3560e-universalk9-mz.122-55.SE1/c3560e-universalk9-mz.122-55.SE1.bin"

This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic
products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

License Level: ipbase
License Type: Permanent
Next reload license Level: ipbase
cisco WS-C3560X-24 (PowerPC405) processor (revision A0) with 262144K bytes of memory.
Processor board ID FD01511217Y
Last reset from power-on
12 Virtual Ethernet interfaces
2 FastEthernet interfaces
28 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address : 40:55:39:A0:4F:80
Motherboard assembly number : 73-12554-05
Motherboard serial number : XXXXXXXXXX
Model revision number : A0
Motherboard revision number : A0
Model number : WS-C3560X-24T-S
Daughterboard assembly number : 800-32786-01
Daughterboard serial number : XXXXXXXXXX
System serial number : XXXXXXXXXX Top Assembly
Part Number : 800-31331-02
Top Assembly Revision Number : A0
Version ID : V02
CLEI Code Number : COMJU00ARB
Hardware Board Revision Number : 0x03

```
Switch Ports Model   SW Version    SW Image
------ -------------- ---------------
*  1 30  WS-C3560X-24  12.2(55)SE1  C3560E-UNIVERSALK9-M

Configuration register is 0xF
```
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: `drive :\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.
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 `drive:\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.

### 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.

⚠️ CAUTION: 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
• Other VMs identified as part of the Core or VCE Optional workloads to manage the Vblock System.

To back up targets in AMP and the Vblock System, refer to the documentation provided with the backup tool vendor.
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 10)

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.
To confirm that the scheduler feature is enabled, type: `SWITCH# show feature | include scheduler`

```
scheduler             1         enabled
```

From the network device, to create the backup task, type:

```
SWITCH# conf t

SWITCH(config)# scheduler aaa-authentication username login password 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.

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#
```
To confirm the scheduler update, type: `SWITCH# show scheduler config`

```
config terminal
feature scheduler
scheduler logfile size 16
end
config 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
config terminal
scheduler schedule name Daily0600
time daily 06:00
job name cfgBackup
end
config terminal
scheduler schedule name Daily1800
time daily 18:00
job name cfgBackup
end
```

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

To save the configuration updates, type: `SWITCH# copy running-config startup-config`

```
[################################################] 100%
```

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 174)
Creating and running the fabric interconnect backup using the Cisco UCS Manager CLI (see page 175)

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.
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 174)
- Creating and running the fabric interconnect backup using the Cisco UCS Manager CLI (see page 175)

**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 174)
Creating and running the fabric interconnect backup using the Cisco UCS Manager CLI (see page 175)

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/device/config/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
   ```
To save the configuration updates, type: SWITCH# copy running-config startup-config

---

**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:
   - In the **Server type** field, verify that **Database Engine** appears. If not, select it.
   - If the **Server name** field is not auto-filled, select **(local)**. If no matching account exists, log in with administrator privileges.
   - In the **Authentication** field, verify that **Windows Authentication** appears. If not, select it, and click **Connect**.
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 xmgmtvcenter and xmgmtvum, where x is a unique identifier. The tempdb database should be excluded from the backup process creation tasks.

Navigate to and expand **SQL Server Agent > Jobs**.

To create a backup job, right-click **Jobs** and select **New Job**.

- From the **New Job** window, in the **Name** field, type a value to correspond with the backup to be performed.
- In the **Owner** field, remove the default login and type sa.
- Change the **Category** field to **Database Maintenance**.
- Type a description in the **Description** field.
- 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.
e  Copy and paste this text into the Command area, and modify the @DIRNAME and @DBNAME variables accordingly:

```sql
-- SQL Server Transact SQL script to perform database backup
-- Use this script for each of the databases in the (AMP or AMP-2). Modify the following variable
-- for the shared location of the backup files -
--
--     DIRNAME = Set location of the backup files
--
-- Modify the following variable for the name unique to each database:
--
--     DBNAME  = Set database name
--
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;
```

f  Under Select a page, select the Advanced tab.

g  For the On success action field, select Quit the job reporting success.

h  Under Select a page, select the Advanced tab.

<i>Note: </i>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

i  Click OK.

9  To create the job schedule, under Select a page, select Schedules, and then click New.

a  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>
<tbody>
<tr>
<td>master, model, msdb</td>
<td>1 In the Frequency section, set the Occurs field to Daily.</td>
</tr>
<tr>
<td></td>
<td>2 Verify that the Recurs field is set to 1 day(s).</td>
</tr>
<tr>
<td></td>
<td>3 In the Daily Frequency section, check Occurs once at 06:30 AM.</td>
</tr>
<tr>
<td></td>
<td>4 In the Duration section, confirm that the Start date is set to the current date and No end date is selected.</td>
</tr>
<tr>
<td>vcenter, vum</td>
<td>1 In the Frequency section, set the Occurs field to Daily.</td>
</tr>
<tr>
<td></td>
<td>2 Verify that the Recurs field is set to 1 day(s).</td>
</tr>
<tr>
<td></td>
<td>3 In the Daily Frequency section, check Occurs every, type 4, and select hours.</td>
</tr>
<tr>
<td></td>
<td>4 Set Starting at 06:30:00 AM and Ending at 06:29:59 AM.</td>
</tr>
<tr>
<td></td>
<td>5 In the Duration section, confirm that the Start date is set to the current date and No end date is selected.</td>
</tr>
</tbody>
</table>

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
```

You can optionally type a directory location and file name into the Output file field to capture script log messages. For example, Filemgmt.log
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](#)

**Backing up the EMC VNX configuration**

Use this procedure to back up EMC VNX configurations.

**About this task**

When the script is initiated, it queries the EMC VNX Service Processors, A and B, to capture the array configuration that supports the Vblock System deployment.

VCE recommends that you perform this task on a daily basis using Windows Task Scheduler with an account that does not expire.

**Before you begin**

- Verify that an array name exists in DNS
- Put the security file in place to allow the script to run without a userid or password in the script. Refer to naviseccli -AddUserSecurity command syntax
- Determine the number of days to retain backups and the location for the configuration backups

**Procedure**

1. In the EMC VNX platform configuration script, update the following line in the script: `set arrayname=\array_name`  
2. To set the number of days you would like the archive to contain, update the following line: `set archivedays=-90`  
3. To set the location for the backup, include the full path of the directory enclosed with quotes. For example, to set the location for a specific path, type: `set location="d:\VNX\backup"`
To execute the configuration platform backup task, create a .bat file and place it in a common scripts directory. Type (or copy) the following script, updating the runtime variables as described above:

```bash
set arrayname=v00018c19601
set archivedays=-90
set location="d:\VNX\backup"
::
navisecccli.exe -h 10.236.10.11 arrayconfig -capture -output %location% \SPA_conf_backup.xml -format xml -o ::
ren %location%\SPA_conf_backup.xml %arrayname%_SPA_conf_backup_%date:~-4,4% %date:~-10,2%\%date:~-7,2%.xml ::
navisecccli.exe -h 10.236.10.12 arrayconfig -capture -output %location% \SPB_conf_backup.xml -format xml -o ::
ren %location%\SPB_conf_backup.xml %arrayname%_SPB_conf_backup_%date:~-4,4% %date:~-10,2%\%date:~-7,2%.xml ::
forfiles -p %location% -m *.xml -d %archivedays% -c "cmd /c del @file" 2>NUL ::
exit 0
```

To verify that the procedure was completed successfully, from the backup directory location, check for the current day’s *.xml file after task execution.

### Reversing the procedure

**Procedure**

To reverse this procedure, remove or disable the entry in Task Scheduler.

### Backing 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.
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*.

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.
Back 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 185)

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
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
conf t
```

**NOTE:** This adds the date and timestamp to filenames.

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
```
5 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

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.

⚠️ **CAUTION:** This script deletes any file in the D:\Cisco\9xxx\config directory that has a .config file extension and is older than seven days.

```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
    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.

⚠️ **CAUTION:** This script deletes any file in the D:\Cisco\9xxx\config directory with a .config file extension older than seven days.

**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.