Contents

Remove a VLAN from the Cisco Nexus switches .............................................................. 44
Configure a vPC .................................................................................................................. 44
Delete a vPC ...................................................................................................................... 46
Add VLANs to a vPC ......................................................................................................... 46
Remove VLANs from a vPC ............................................................................................. 46
Add vPCs to VLANs for Disjoint Layer 2 networks ......................................................... 47
View vPCs assigned to VLANs for Disjoint Layer 2 networks ........................................ 49
Remove vPCs from VLANs for Disjoint Layer 2 networks ............................................ 50
Upgrade Cisco Nexus switch software ........................................................................... 50
Downgrade Cisco Nexus switch software ........................................................................ 52

Managing Cisco MDS switches ..................................................................................... 53
Upgrade Cisco MDS switch software ............................................................................. 53
Downgrade Cisco MDS switch software .......................................................................... 55
Configure a VSAN ............................................................................................................ 55
Remove a VSAN .............................................................................................................. 55
Configure a domain ID and priority for a VSAN ............................................................ 56
Remove a domain ID and priority from a VSAN ............................................................ 56
Enable FC interfaces ....................................................................................................... 57
Disable FC interfaces ..................................................................................................... 57
Move licenses between FC interfaces ............................................................................ 58
Create FC aliases ............................................................................................................ 58
Delete an FC alias .......................................................................................................... 59
Create FC zones ............................................................................................................... 59
Delete an FC zone .......................................................................................................... 60
Create, modify, and activate zone sets ........................................................................... 60
Creating FC port channels .............................................................................................. 61
Remove an FC interface from a port channel ................................................................. 61

Managing storage resources ......................................................................................... 63
Managing XtremIO ........................................................................................................... 63
Best practices for XtremIO .............................................................................................. 63

Managing VMware vSphere ESXi 6.x ............................................................................. 66
Installing the latest VMware vSphere ESXi patch (vSphere 6.0) ..................................... 66
Installing the latest VMware vSphere ESXi patch (vSphere 6.5) ..................................... 66
Installing the latest VMware vSphere ESXi patch (VMware vSphere 6.7) ..................... 67
Configuring advanced settings for VMware vSphere ESXi (vSphere 6.0) ....................... 68
Configuring advanced settings for VMware vSphere ESXi (vSphere 6.5) ....................... 69
Configure advanced settings for VMware vSphere ESXi (VMware vSphere 6.7) .......... 70
Restoring default values for VMware vSphere ESXi advanced settings (vSphere 6.0) .. 70
Restoring default values for VMware vSphere ESXi advanced settings (vSphere 6.5) .. 71
Restoring default values for VMware vSphere ESXi advanced settings (VMware vSphere 6.7) ................................................................. 71
Hardening security on VMware vSphere ESXi hosts ..................................................... 71
Increasing the disk timeout on Microsoft Windows VMs ................................................. 71
Installing vCenter Server root certificates on web browser (vSphere 6.5) ...................... 72
Install vCenter Server root certificates on web browser (vSphere 6.7) ............................ 72
Setting up Java and Internet Explorer on the management workstation or VM (vSphere 6.x) .............................................................................................................................. 73

Manage VMware Single Sign On (VMware vSphere 6.x) .............................................. 74
VMware vCenter SSO overview .................................................................................... 74
Reset the VMware Single Sign On administrator password (VMware vSphere 6.x) .... 74
Manage the lockout status of VMware Single Sign On (VMware vSphere 6.5) ............. 74
Manage the lockout status of VMware Single Sign On account (VMware vSphere 6.7) ................................................................................................................................. 75
Manage VMware Single Sign On default password policies (VMware vSphere 6.0 or 6.5) ................................................................................................................................. 75
Manage VMware vCenter SSO default password policies (VMware vSphere 6.7) ......... 75
Manage VMware Single Sign On lockout policies (VMware vSphere 6.5) ................................................................. 76
Manage VMware Single Sign On lockout policies (VMware vSphere 6.7) ................................................................. 76
Add an AD identity source to VMware Single Sign On (IPv4) (VMware vSphere 6.7) ..................................................... 76
Add Windows AD identity source to VMware SSO (VMware vSphere 6.7) ................................................................... 77
Backing up or restoring the vCenter Server .................................................................................................................. 78
Backing up and restoring the vCenter Server and PSC (vSphere 6.5) ............................................................................ 79
Restoring the vCenter Server ........................................................................................................................................ 79
Redirect VMware vCenter Server to the secondary external VMware Platform Services Controller (VMware vSphere 6.x) ......................................................................................................................... 80
Enabling fault tolerance for the external PSC ................................................................................................................... 80

Managing virtualization.................................................................................................................................................... 81
Patch VMware vSphere ESXi hosts with the VUM (VMware vSphere 6.0) ................................................................. 81
Patch VMware vSphere ESXi hosts with the VUM (VMware vSphere 6.5) ................................................................. 83
Patch VMware vSphere ESXi hosts with the VUM (VMware vSphere 6.7) ................................................................. 85
Supported guest operating systems ............................................................................................................................... 86
Use VMware Enhanced vMotion Compatibility with Cisco UCS blade servers .......................................................... 86
Enable VMware Enhanced vMotion Compatibility within a cluster ........................................................................... 87
Manage the VMware vCenter HA Configuration (VMware vSphere 6.x) ....................................................................... 88
Manage the VMware vCenter HA Configuration (VMware vSphere 6.5) ....................................................................... 88
Convert VMware Platform Service Controllers from external to embedded (VMware vSphere 6.7) ....................... 89
Join Embedded Linked Mode domain (VMware vSphere 6.7) .................................................................................. 90
Convert external VMware Platform Service Controllers to embedded (VMware vSphere 6.x) .......................... 90
Join Embedded Linked Mode domain (VMware vSphere 6.5) .................................................................................. 91
Decommission external VMware Platform Service Controllers (VMware vSphere 6.x) ......................................... 91
Decommission external VMware Platform Service Controllers (VMware vSphere 6.5) ............................................ 92
Configure the Virtual Flash Read Cache .......................................................................................................................... 93

Manage VMware VDS (VMware vSphere 6.5) ............................................................................................................... 94
Managing licenses (VMware vSphere 6.5) .......................................................................................................................... 94
Provision a VMware VDS configuration (VMware vSphere 6.5) ................................................................................... 94
Modifying an existing distributed port group (VMware vSphere 6.5) ......................................................................... 94
Creating a distributed port group (VMware vSphere 6.5) ........................................................................................... 96
Configure a VMKernel interface (VMware vSphere 6.5) ............................................................................................... 97
Associating VMware vSphere ESXi hosts to an existing VMware VDS .......................................................................... 98
Configuring jumbo frames on VMware VDS .................................................................................................................. 99
Configuring jumbo frames on distributed port groups .................................................................................................. 99
Modifying CoS settings ............................................................................................................................................. 100
Decommissioning VMware VDS components ................................................................................................................ 101
Deleting a distributed port group ................................................................................................................................... 101
Disassociating the VMware vSphere ESXi host ............................................................................................................... 102
Removing a VMware VDS ............................................................................................................................................. 106
Using Disjoint Layer 2 configuration on VMware VDS ............................................................................................... 108
Creating a VMware VDS for Disjoint Layer 2 configuration .......................................................................................... 108
Creating distributed port groups for Disjoint Layer 2 ................................................................................................. 109
Add VMware vSphere ESXi hosts to VMware VDS .................................................................................................. 110
Backing up and restoring a VMware VDS data configuration ...................................................................................... 111
Exporting a backup of a VMware VDS configuration .................................................................................................... 111
Importing a backup of a VMware VDS configuration ................................................................................................... 112
Restoring a backup of a VMware VDS configuration ................................................................................................... 112
Managing VMware VDS (VMware vSphere 6.5) ............................................................................................................. 112
VMware VDS basic troubleshooting ............................................................................................................................... 113

Managing VMware VDS (VMware vSphere 6.7) ............................................................................................................. 114
## Configuring VMware Enhanced Linked Mode (vSphere 6.5U1)

### Introduction

- VMware ELM with VMware vSphere 6.5U1 use cases
- Back up and restoring Converged Systems with VMware ELM
- AMP design (AMP-2S only)

### VMware ELM scalability planning

- Intra Converged System VMware ELM scalability planning
- Inter Converged System VMware ELM scalability planning in Converged Systems in a single physical data center
- Inter Converged System VMware ELM scalability planning with multiple physical data centers

### VMware ELM deployment information

- VMware ELM dependencies and limitations
- VMware ELM references
- VMware ELM conclusions

### Configuring VMware Enhanced Linked Mode (vSphere 6.5U1)

- Introduction to ELM (vSphere 6.5U1)
- VMware ELM with VMware vSphere 6.5U1 use cases
- Backup and recovery for ELM 6.5
- Backup and recovery guidelines

<table>
<thead>
<tr>
<th>Task</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring VMware Enhanced Linked Mode (vSphere 6.0)</td>
<td>140</td>
</tr>
<tr>
<td>Introduction</td>
<td>140</td>
</tr>
<tr>
<td>VMware ELM with VMware vSphere 6.0 use cases</td>
<td>140</td>
</tr>
<tr>
<td>Back up and restoring Converged Systems with VMware ELM</td>
<td>141</td>
</tr>
<tr>
<td>AMP design (AMP-2S only)</td>
<td>141</td>
</tr>
<tr>
<td>VMware ELM scalability planning</td>
<td>142</td>
</tr>
<tr>
<td>Intra Converged System VMware ELM scalability planning</td>
<td>143</td>
</tr>
<tr>
<td>Inter Converged System VMware ELM scalability planning in Converged Systems in a single physical data center</td>
<td>144</td>
</tr>
<tr>
<td>Inter Converged System VMware ELM scalability planning with multiple physical data centers</td>
<td>144</td>
</tr>
<tr>
<td>VMware ELM deployment information</td>
<td>145</td>
</tr>
<tr>
<td>VMware ELM dependencies and limitations</td>
<td>146</td>
</tr>
<tr>
<td>VMware ELM references</td>
<td>147</td>
</tr>
<tr>
<td>VMware ELM conclusions</td>
<td>147</td>
</tr>
</tbody>
</table>

## Managing the Cisco Nexus 1000V Series Switch

### Managing licenses

- Adding hosts
- Creating a port profile

### Modifying the uplink port profiles
- Removing the uplink port profiles
- Modifying vEthernet data port profiles
- Modifying the QoS settings
- Upgrading the VEM software

## Managing VMware NSX with VPLEX on VxBlock Systems

### Backing up Cisco MDS switches

- Create backups of startup and running configuration files
- Scheduling backups of the startup and running configuration files
- Create a script to purge older copies of the backup files
- Schedule the task to purge older backup files

### Configuring VMware Enhanced Linked Mode (VMware vSphere 6.0)

- Introduction
- VMware ELM with VMware vSphere 6.0 use cases
- Back up and restoring Converged Systems with VMware ELM
- AMP design (AMP-2S only)

### VMware ELM scalability planning

- Intra Converged System VMware ELM scalability planning
- Inter Converged System VMware ELM scalability planning in Converged Systems in a single physical data center
- Inter Converged System VMware ELM scalability planning with multiple physical data centers

### VMware ELM deployment information

- VMware ELM dependencies and limitations
- VMware ELM references
- VMware ELM conclusions

### Configuring VMware Enhanced Linked Mode (vSphere 6.5U1)

- Introduction to ELM (vSphere 6.5U1)
- VMware ELM with VMware vSphere 6.5U1 use cases
- Backup and recovery for ELM 6.5
- Backup and recovery guidelines

<table>
<thead>
<tr>
<th>Task</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing the Cisco Nexus 1000V Series Switch</td>
<td>115</td>
</tr>
<tr>
<td>Managing licenses</td>
<td>115</td>
</tr>
<tr>
<td>Adding hosts</td>
<td>115</td>
</tr>
<tr>
<td>Creating a port profile</td>
<td>115</td>
</tr>
<tr>
<td>Modifying the uplink port profiles</td>
<td>116</td>
</tr>
<tr>
<td>Removing the uplink port profiles</td>
<td>117</td>
</tr>
<tr>
<td>Modifying vEthernet data port profiles</td>
<td>118</td>
</tr>
<tr>
<td>Modifying the QoS settings</td>
<td>119</td>
</tr>
<tr>
<td>Upgrading the VEM software</td>
<td>120</td>
</tr>
<tr>
<td>Troubleshooting the Cisco Nexus 1000V Switch</td>
<td>120</td>
</tr>
<tr>
<td>Managing VMware NSX with VPLEX on VxBlock Systems</td>
<td>121</td>
</tr>
<tr>
<td>Perform a graceful failover</td>
<td>121</td>
</tr>
<tr>
<td>Perform a graceful recovery</td>
<td>124</td>
</tr>
<tr>
<td>Guidelines for backing up configuration files</td>
<td>128</td>
</tr>
<tr>
<td>Back up configuration files</td>
<td>128</td>
</tr>
<tr>
<td>Back up network devices running Cisco NX-OS software</td>
<td>128</td>
</tr>
<tr>
<td>Back up Cisco UCS FIs</td>
<td>130</td>
</tr>
<tr>
<td>Create and run the backup using the Cisco UCS Manager</td>
<td>130</td>
</tr>
<tr>
<td>Create and run the backup using the Cisco UCS CLI</td>
<td>131</td>
</tr>
<tr>
<td>Create and run the backup using scheduled backups</td>
<td>132</td>
</tr>
<tr>
<td>Configure fault suppression</td>
<td>132</td>
</tr>
<tr>
<td>Back up the VMware vCenter SQL server database</td>
<td>133</td>
</tr>
<tr>
<td>Back up the VNXe configuration</td>
<td>136</td>
</tr>
<tr>
<td>Backing up Cisco MDS switches</td>
<td>137</td>
</tr>
<tr>
<td>Create backups of startup and running configuration files</td>
<td>137</td>
</tr>
<tr>
<td>Scheduling backups of the startup and running configuration files</td>
<td>137</td>
</tr>
<tr>
<td>Create a script to purge older copies of the backup files</td>
<td>138</td>
</tr>
<tr>
<td>Schedule the task to purge older backup files</td>
<td>139</td>
</tr>
<tr>
<td>Configuring VMware Enhanced Linked Mode (VMware vSphere 6.0)</td>
<td>140</td>
</tr>
<tr>
<td>Introduction</td>
<td>140</td>
</tr>
<tr>
<td>VMware ELM with VMware vSphere 6.0 use cases</td>
<td>140</td>
</tr>
<tr>
<td>Back up and restoring Converged Systems with VMware ELM</td>
<td>141</td>
</tr>
<tr>
<td>AMP design (AMP-2S only)</td>
<td>141</td>
</tr>
<tr>
<td>VMware ELM scalability planning</td>
<td>142</td>
</tr>
<tr>
<td>Intra Converged System VMware ELM scalability planning</td>
<td>143</td>
</tr>
<tr>
<td>Inter Converged System VMware ELM scalability planning in Converged Systems in a single physical data center</td>
<td>144</td>
</tr>
<tr>
<td>Inter Converged System VMware ELM scalability planning with multiple physical data centers</td>
<td>144</td>
</tr>
<tr>
<td>VMware ELM deployment information</td>
<td>145</td>
</tr>
<tr>
<td>VMware ELM dependencies and limitations</td>
<td>146</td>
</tr>
<tr>
<td>VMware ELM references</td>
<td>147</td>
</tr>
<tr>
<td>VMware ELM conclusions</td>
<td>147</td>
</tr>
<tr>
<td>Configuring VMware Enhanced Linked Mode (vSphere 6.5U1)</td>
<td>148</td>
</tr>
<tr>
<td>Introduction to ELM (vSphere 6.5U1)</td>
<td>148</td>
</tr>
<tr>
<td>VMware ELM with VMware vSphere 6.5U1 use cases</td>
<td>148</td>
</tr>
<tr>
<td>Backup and recovery for ELM 6.5</td>
<td>149</td>
</tr>
<tr>
<td>Backup and recovery guidelines</td>
<td>149</td>
</tr>
<tr>
<td>Converged System AMP design (ELM/VMware vSphere 6.5U1)</td>
<td>149</td>
</tr>
<tr>
<td>VMware ELM scalability planning (vSphere 6.5U1)</td>
<td>152</td>
</tr>
<tr>
<td>Intra Converged System VMware ELM scalability planning (VMware vSphere 6.5U1)</td>
<td>153</td>
</tr>
</tbody>
</table>
Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inter Converged System VMware ELM scalability planning in a single physical data center (VMware vSphere 6.5U1)</td>
<td>154</td>
</tr>
<tr>
<td>Inter Converged System VMware ELM scalability planning with multiple physical data centers (VMware vSphere 6.5U1)</td>
<td>154</td>
</tr>
<tr>
<td>VMware ELM deployment information (VMware vSphere 6.5U1)</td>
<td>154</td>
</tr>
<tr>
<td>Verify PSC and PSC Partner Status</td>
<td>156</td>
</tr>
<tr>
<td>Determining the VMware vCenter server within a vSphere Domain</td>
<td>156</td>
</tr>
<tr>
<td>Reconfiguring the ring topology</td>
<td>157</td>
</tr>
<tr>
<td>VMware ELM references (vSphere 6.5U1)</td>
<td>157</td>
</tr>
<tr>
<td>VMware ELM conclusions (VMware vSphere 6.5U1)</td>
<td>158</td>
</tr>
</tbody>
</table>

Manage VMware Embedded Linked Mode (VMware vSphere 6.7) .......................... 159
Configure VMware Embedded Linked Mode (VMware vSphere 6.7) .......................... 159

Manage VMware Embedded Linked Mode (VMware vSphere 6.5) .......................... 162
Configure VMware Embedded Linked Mode (VMware vSphere 6.5) .......................... 162

Manage VMware Enhanced Linked Mode (VMware vSphere 6.x) .......................... 165
Back up and restore VxBlock Systems with VMware Embedded Linked Mode (VMware vSphere 6.7) .................. 166
VMware Enhanced Linked Mode scalability planning (VMware vSphere 6.7) .......................... 166
Intra Converged System VMware Enhanced Linked Mode scalability planning .................. 167
VMware Enhanced Linked Mode deployment information .......................................... 167
VMware Enhanced Linked Mode references ............................................................ 168
VMware Enhanced Linked Mode conclusions (VMware vSphere 6.7) .................. 168

Setting up VxBlock Systems to use VxBlock Central ............................ 170
Access the VxBlock Central dashboard ............................................................ 170
Set up a VxBlock System ..................................................................................... 170
  Accept the end user license agreement ......................................................... 170
  Reset and reaccept end user license agreement ............................................. 171
  Start VxBlock System discovery ..................................................................... 171
  Update the Windows Registry ......................................................................... 172
  Update the IP address tables on the Core VM (optional) .......................... 173
Plan a multisystem clustered environment ......................................................... 173
  Associate a Core VM with an existing MSM VM ............................................ 175
  Form a cluster of MSM VMs ........................................................................... 176
  Remove a Core VM from an MSM VM ............................................................ 178
  Shut down and take a snapshot of the MSM cluster .................................... 179
  Recover the MSM cluster .............................................................................. 179
  Verify ElasticSearch if the MSM VM is changed ......................................... 180
Discover, decommission, or modify a component .............................................. 181
  Add Isilon Technology Extension on a VxBlock System ................................ 181
  Add a component with the configuration editor ............................................ 182
  Add eNAS to VMAX3 storage ........................................................................ 183
  Edit component credentials in the system.cfg file ........................................ 184
  Edit component properties with the configuration editor ................................ 184
  Delete a component with the configuration editor ........................................ 185
Configure VxBlock Systems and components ..................................................... 185
  Access the VxBlock Central Shell session ................................................... 185
  Run VxBlock Central Shell from a remote host ............................................ 186
  VxBlock Central Shell commands ................................................................ 186
  Components in VxBlock Central Shell .......................................................... 187
  View VxBlock Central Shell logs .................................................................. 190
  View VxBlock Central Shell jobs .................................................................. 190
Configure Secure Remote Services for VxBlock Central 2.0 and later ................. 191
Configure Secure Remote Services for VxBlock Central 1.5 and earlier ................. 191
Contents

Register VxBlock Central with a Secure Remote Services gateway .............................................................. 191
Add a software identifier for an MSM VM ........................................................................................................ 192
Retrieve the software ID from the licensing system ....................................................................................... 193
Update a Secure Remote Services gateway configuration or software identifier ........................................... 193
Deregister VxBlock Central with Secure Remote Services ........................................................................... 194
Send information to Secure Remote Services ............................................................................................... 194
Secure the connection between VxBlock Central and Secure Remote Services .......................................... 195
Verify Secure Remote Services configuration ............................................................................................... 195
Troubleshoot Secure Remote Services connectivity issues ........................................................................ 196
Integrate with SNMP ..................................................................................................................................... 197
  Provision the SNMP name, location, and contact information fields .......................................................... 197
  SNMP traps, events, and CIM indications ...................................................................................................... 198
  Communicate with the network management system .................................................................................. 199
  Send SNMP traps in readable format ........................................................................................................... 199
  Enable northbound communication through SNMP .................................................................................. 200
Integrate with AD ............................................................................................................................................ 201
  Configure AD ................................................................................................................................................ 203
  Map roles to AD groups ............................................................................................................................... 203
Configure components to send traps.................................................................................................................. 205
  Configure Cisco UCSM to forward traps ....................................................................................................... 205
  Configure iDRAC to forward traps ................................................................................................................ 205
  Configure Unisphere to forward traps .......................................................................................................... 206
  Configure XtremIO to forward traps ............................................................................................................ 206
  Configure VMAX or PowerMax to forward traps .......................................................................................... 206
  Configure Cisco MDS and Cisco Nexus switches to forward traps ............................................................... 207
  Configure alert profiles and templates to receive notification .................................................................... 207
  Configure port flapping for switches ........................................................................................................... 208
Configure the VMs to use the NTP server ....................................................................................................... 208
Verify the ElasticSearch configuration .......................................................................................................... 208
Manage credentials ........................................................................................................................................ 209
  Change the default password for root and VxBlock Central accounts ....................................................... 209
  Use the nonadministrator account ............................................................................................................. 210
  Change the default CAS password for Core VM ......................................................................................... 210
  Change the default CAS password for MSM VM ....................................................................................... 211
  Synchronize the CAS password for the admin user ................................................................................... 211
  Change the default CAS password for the MSP VM to match the MSM VM .......................................... 212
  Create users with access rights to storage components ............................................................................ 212
  Change access credentials for a VxBlock System component ................................................................... 213
  Bulk credential script ................................................................................................................................ 213
  Manage third party certificates .................................................................................................................... 214
  Configure connection and download settings ............................................................................................ 218
  Manage credentials for RCM content prepositioning ................................................................................ 221
VxBlock Central Advanced Analytics ............................................................................................................ 222
  Change VxBlock Central Operations Adapter real-time alerts collection cycle interval .......................... 222
  Change the VxBlock Central Adapter Collection cycle interval ................................................................ 223

Manage VxBlock Systems with VxBlock Central ........................................................................................... 224
  Change discovery and health polling intervals ......................................................................................... 224
  Monitor events and log messages ............................................................................................................. 224
  Change syslog rotation parameters ......................................................................................................... 225
  Forward syslog messages to remote servers .............................................................................................. 225
  Customize login banners .......................................................................................................................... 228
  Back up and restore Core VM ..................................................................................................................... 228
  Management backup .................................................................................................................................. 229
  Change the backup schedule and frequency .............................................................................................. 230
  Back up cron tasks ....................................................................................................................................... 230
Back up configuration files on demand.................................................................................................................... 231
Back up databases on demand......................................................................................................................................... 231
Restore the software configuration................................................................................................................................. 231
Restore databases.......................................................................................................................................................... 232
Back up the Core VM......................................................................................................................................................233
Back up and restore the MSM VM and MSP VM............................................................................................................ 233
Back up component configuration files.............................................................................................................................233
Ports and protocols...........................................................................................................................................................237
   Open port assignments.................................................................................................................................................. 237
   Northbound ports and protocols .................................................................................................................................237
   Southbound ports and protocols ................................................................................................................................238
Reference........................................................................................................................................................................ 239
   Core VM commands.................................................................................................................................................... 239
   MSM VM commands................................................................................................................................................... 241
   MSP VM commands................................................................................................................................................... 242
   Configuration editor component reference........................................................................................................... 243
   Components, APIs, and services for VMs.................................................................................................................... 248

Manage the AMPs............................................................................................................................................................... 251
   Upgrade the Cisco UCS C2x0 Server (CIMC 2.x firmware).......................................................................................... 251
   Upgrade the Cisco UCS C2x0 Server (CIMC 3.x and 4.x firmware)............................................................................. 252
   Upgrading VNIXe3200 software.................................................................................................................................... 252
   Create a VMware data store........................................................................................................................................ 253
   Change VMware datastore capacity ..............................................................................................................................254
   Add a VMware vSphere ESXi host for IPv4 ...................................................................................................................254
   Add data store access to a VMware vSphere ESXi Host ................................................................................................255
   Configure the VMware vSphere ESXi persistent scratch location (VMware vSphere 6.5)...........................................255
   Expand an AMP-2S cluster.......................................................................................................................................... 256
   Enable VMware Enhanced vMotion Compatibility.................................................................................................... 257
   Backing up AMP-2....................................................................................................................................................... 258
      Create an instance of the configuration repository.................................................................................................. 258
      Create a backup of a configuration repository ........................................................................................................ 259
      Restore a configuration file .................................................................................................................................... 259
      Back up targets ........................................................................................................................................................... 260
# Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Document revision</th>
<th>Description of changes</th>
</tr>
</thead>
</table>
| October 2019 | 1.23              | - Added a new topic titled *Configure Secure Remote Services for VxBlock Central 2.0 and later*
|              |                   | - Reworded the existing topic title to *Configure Secure Remote Services for VxBlock Central 1.5 and earlier* and added verification information |
| September 2019 | 1.22              | - Added support for VMware vSphere 6.5 Update 2d and VMware vSphere 6.7 Update 2.  
|              |                   | - Added note about Workflow Automation to *Configuring service profile templates*.  
|              |                   | - Added the topic *Reset and re-accept end user license agreement* to the section *Set up VxBlock Systems to use VxBlock Central*. |
| July 2019    | 1.21              | - Updated for VxBlock Central Version 2.0.  
|              |                   | - SRS configuration feature in the VxBlock Central user interface.  
|              |                   | - Component discovery feature in the VxBlock Central user interface.  
|              |                   | - New VxBlock Central alerts. |
| June 2019    | 1.20              | - Added support for expanding an AMP-2S cluster with Cisco UCS C220 M5 servers. |
| April 2019   | 1.19              | - Fixed JIRA EH-741 in *Managing storage resources > Best practices for XtremIO*. |
| March 2019   | 1.18              | - Added support for VMware vSphere 6.7.  
|              |                   | - Added support for Cisco UCS Virtual Interface Cards 1440 and 1480. |
| December 2018 | 1.16              | - Added support for VxBlock Central. |
| July 2018    | 1.15              | - Updated the following sections to include Cisco B480 M5 blade server:  
|              |                   |   - Configuring service profile templates  
|              |                   |   - Adding vNICs to the service profiles  
|              |                   |   - Configuring service profile templates for Disjoint Layer 2 |
| May 2018     | 1.14              | - Updated *Best practices for XtremIO* |
| February 2018 | 1.13              | - Updated VMware ELM 6.5 content.  
|              |                   |   *Adding a VLAN to a service template* - updated steps.  
<p>|              |                   |   Removed VMware vSphere 5.5 content. |
| October 2017 | 1.12              | - Added a section for configuring VMware Enhanced Linked Mode (vSphere 6.5U1) <em>ELM dependencies and limitations</em> - updated statement regarding Vision Intelligent Operations. |</p>
<table>
<thead>
<tr>
<th>Date</th>
<th>Document revision</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2017</td>
<td>1.11</td>
<td>Added and updated topics for VMware vSphere 6.5. Updated the following topics:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Starting Cisco UCS Manager - added UCS Manager 3.x changes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Upgrading the Cisco UCS C2x0 Server - split into two topics CIMC 2.x firmware and CIMC 3.x.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deleted the topic <em>Backing up network devices running Cisco IOS software</em> - Nexus switches do not run IOS so this topic was not required. Refer to the topic <em>Backing up network devices running Cisco NX-OS software</em>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Adding a VLAN to a service profile template</em> - removed step 4.</td>
</tr>
<tr>
<td>September 2017</td>
<td>1.10</td>
<td>Added a section containing guidance for configuring VMware Enhanced Linked Mode.</td>
</tr>
<tr>
<td>August 2017</td>
<td>1.9</td>
<td>Added support for IPv6 on VxBlock Systems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added support for the 40 GB option on VxBlock System 540.</td>
</tr>
<tr>
<td>June 2017</td>
<td>1.8</td>
<td>Updated the value for Net.TcpipHeapSize in the section Configuring Advanced Settings for VMware vSphere ESXi.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added the following section to the document:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Managing VMware NSX with VPLEX on VxBlock Systems</td>
</tr>
<tr>
<td>February 2017</td>
<td>1.7</td>
<td>Added a note about how to determine whether an NX-OS upgrade might need to be done in two stages rather than the usual one.</td>
</tr>
<tr>
<td>December 2016</td>
<td>1.6</td>
<td>- Added support for AMP-2 with Cisco UCS M4 blades and VMware vSphere 5.5.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Removed VLAN 118.</td>
</tr>
<tr>
<td>September 2016</td>
<td>1.5</td>
<td>- Added support for the Cisco MDS 9396S 16G Multilayer Fabric Switch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added support for AMP-2S and AMP enhancements</td>
</tr>
<tr>
<td>August 2016</td>
<td>1.4</td>
<td>Added information about the Cisco MDS 9706 Multilayer Director.</td>
</tr>
<tr>
<td>April 2016</td>
<td>1.3</td>
<td>Added a topic for creating vNIC templates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added information about the following Cisco switches:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Nexus 3172TQ</td>
</tr>
<tr>
<td>October 2015</td>
<td>1.2</td>
<td>Updated to include support for VMware vSphere 6.0 with Cisco Nexus 1000V Switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Removed support for VMware vSphere 5.0.</td>
</tr>
<tr>
<td>August 2015</td>
<td>1.1</td>
<td>Updated to include VxBlock System 540. Added support for VMware vSphere 6.0 with VMware VDS on the VxBlock System and for existing Vblock Systems.</td>
</tr>
<tr>
<td>February 2015</td>
<td>1.0</td>
<td>Initial version</td>
</tr>
</tbody>
</table>
Introduction

This guide contains instructions for managing the Converged Systems after installation at the customer site. In this document, the Vblock System and the VxBlock System are seen as the Converged System.

The target audience for this document includes those responsible for managing the Converged System, including the system administrator and Dell EMC personnel responsible for remote management. The document assumes that the administrator:

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

See the Glossary for definitions of terms specific to Dell EMC.
IPI Appliance

The IPI Appliance provides an intelligent gateway to gather information about power, thermals, security, alerts, and all components in the physical infrastructure of each cabinet.

VxBlock Central or Vision Intelligent Operations uses SNMP to poll the status of the IPI Appliance and then passes the results to VMware vCenter.

For cabinet-related operations such as adding users or cabinet access cards, see the Dell EMC Intelligent Physical Infrastructure Appliance User Manual.

See the release certification matrix (RCM) to identify the recommended firmware version for your IPI Appliance. Contact Support with any questions.

Access the IPI Appliance

Connect a laptop to the appropriate subnet and use a browser to access the IPI Appliance.

The following default settings apply:

- **IP address**: 192.168.0.253
- **Mask**: 255.255.255.0
- **Gateway**: 192.168.0.1
Manage compute resources

Start Cisco UCS Manager

Cisco UCS Manager, Version 3.2.1 and later releases provides an HTML5 based web interface that can be used in place of the traditional Java-based Cisco UCSM applet.

About this task

These instructions apply for Java-based interfaces on current versions of Cisco UCS Manager. Settings, policies, and pools apply regardless of the interface used.

Before you begin

For more information about using the HTML5 web interface, see the Cisco UCS Manager GUI Configuration Guide for versions 3.2.1 and higher.

Procedure

1. From a web browser, open the web link for Cisco UCS Manager GUI at: http(s)://UCSManager_IP.
2. Type the virtual cluster IP address of the management port on the fabric interconnect.
3. If a Security Alert dialog box is displayed, click Yes to accept the security certificate and continue.
4. In the Cisco UCS Manager window, click Launch UCS Manager.
5. For Cisco UCS Manager versions 3.2.1 and higher, click Launch UCS Manager to launch the HTML page.
6. If a banner window is displayed, review the message and click OK.
7. If a Security dialog box is displayed, check the box to accept all content from Cisco, and click Yes.
8. In the Login dialog box, type your username and password.
9. If your Cisco UCS implementation includes multiple domains, select the appropriate domain from the Domain drop-down list, and then click Login.

After you finish

Directly upgrading firmware at endpoints

Directly upgrade firmware at endpoints

Some Converged Systems components require a reboot after being updated. Upgrading Cisco UCS software impacts the Cisco UCS Manager, FIs, I/O modules, chassis, chassis blades, and mezzanine adapters.

Before you begin

- Coordinate firmware upgrades during maintenance windows, and see Cisco documentation for proper upgrade procedures.
- Download the latest Cisco UCS B-Series GUI Firmware Management Guide.
- Run a full state and all configuration backup.
- For a cluster configuration, verify the high availability status of both FIs shows up and running.
- Verify servers, I/O modules, and adapters are fully functional. An inoperable server cannot be upgraded.
- Verify that servers have been discovered. Discovery does not require that you power on the servers or associate them with a service profile.
- Verify that the time, date, and time zone of FIs are identical for a cluster using a time source such as NTP.
Cisco documents recommended practices for managing firmware in the Cisco UCS Manager. Ensure that the firmware versions are compatible with the *Release Certification Matrix*.

**Procedure**

1. Perform the Cisco UCS upgrade as described in the *Cisco UCS B-Series GUI Firmware Management Guide* for the release being installed.

2. To verify the upgrade, from the **Navigation** window, select the **Equipment** tab and **Equipment** node.

3. From the **Work** window, select the **Firmware Management** tab.

4. From the **Installed Firmware** tab, click **Update Firmware**.

   This step may take a few minutes, based on the number of chassis and servers.

5. From the **Update Firmware** dialog, perform the following:
   a. From the **Filter** menu, select **ALL**.
   b. Select the endpoint firmware to update, and click **OK**.

**After you finish**

Verify the following:

- All components are running the correct version of firmware.
- No new Cisco UCS faults were introduced because of the upgrade.
- All hosts have booted successfully.

*Cisco UCS Manager GUI Configuration Guide*

*Cisco UCS B-Series GUI Firmware Management Guide*

**Upgrade Cisco UCS software with Cisco UCS Firmware Auto Install**

Upgrade Cisco UCS software using Cisco UCS Firmware Auto Install on Cisco UCS B-Series chassis and blade servers.

**About this task**

The Cisco UCS Firmware Auto Install feature is performed in two stages that include upgrading the Cisco UCS infrastructure and server firmware.

Upgrading the Cisco UCS infrastructure firmware includes:

- FI kernel and system
- I/O module
- Cisco UCS Manager

Upgrading the Cisco UCS server firmware includes:

- Adapter
- BIOS
- CIMC
- RAID controller
- Disk firmware

These stages can be manually run or scheduled to run at different times, but never simultaneously. Cisco UCS infrastructure firmware upgrades must be updated first. Different versions of Cisco UCS infrastructure firmware and Cisco UCS server firmware are not supported. Cisco UCS infrastructure firmware upgrades do not support a partial upgrade to some infrastructure components in a Cisco UCS domain. Cisco UCSM does not support managing firmware on fusion I/O or LSI flash cards.

The Cisco UCS firmware auto install feature has the following scheduling options:
### Upgrade stage

<table>
<thead>
<tr>
<th>Scheduling options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infrastructure firmware</strong></td>
</tr>
<tr>
<td>- Configure an immediate upgrade, or specify a start time.</td>
</tr>
<tr>
<td>- If a start time is not specified, the upgrade begins when the transaction is committed.</td>
</tr>
<tr>
<td>- You cannot cancel a Cisco UCS infrastructure firmware upgrade after it has begun but can cancel upgrades that are scheduled to occur in the future.</td>
</tr>
<tr>
<td>- Cisco UCS infrastructure firmware upgrades require an acknowledgment for an administrator user before the primary fabric interconnect is rebooted. The subordinate fabric interconnect reboots automatically.</td>
</tr>
<tr>
<td><strong>Server firmware</strong></td>
</tr>
<tr>
<td>- The Dell EMC Host Firmware Policy must be used for Cisco UCS server firmware upgrades and can be configured for an immediate or scheduled upgrade.</td>
</tr>
<tr>
<td>- The server reboot is based on the maintenance policy that has been configured for each service profile. The default is for an immediate server reboot.</td>
</tr>
<tr>
<td>- Create and deploy a maintenance policy called VCE_UserAck with the user acknowledgment option selected. This option requires an administrator level user to acknowledge the reboot request for each server.</td>
</tr>
<tr>
<td>- You cannot cancel Cisco UCS server firmware upgrades after you complete the configuration in the Cisco UCS Install Server Firmware wizard.</td>
</tr>
<tr>
<td>- A change in the firmware version is required every time that you perform the Cisco UCS firmware auto install.</td>
</tr>
<tr>
<td>- The Cisco UCS server firmware auto install feature can only be run once per firmware version.</td>
</tr>
<tr>
<td>- You cannot run the Cisco UCS server firmware auto install feature when new servers are added.</td>
</tr>
</tbody>
</table>

### Before you begin

Reboot as needed when updating Converged System components. Coordinate firmware upgrades during maintenance windows, and see Cisco documentation for proper upgrade procedures.

- Download the latest *Cisco UCS B-Series GUI Firmware Management Guide*.
- Back up the configuration file into an all configuration backup file and perform a full state backup.
- The time, date, and time zone of the fabric interconnects must be identical for a cluster using a centralized time source such as NTP.
- Verify the following:
  - Both fabric interconnects are up and running for a cluster configuration.
  - All servers, I/O modules, and adapters are fully functional. An inoperable server cannot be upgraded.
  - All servers are discovered. Do not power on servers or associated with a service profile.
  - The software version for the UCS firmware auto install feature is 2.1(1) or later.
  - All endpoints are at Cisco UCS release 1.4 or later to run the Cisco UCS auto install.
  - All endpoints are running the latest firmware release or patch for that release.
- For the Cisco UCS Server Firmware Auto Install Feature, perform the following prerequisites:
  - Remove management firmware packages from all service profile templates and service profiles.
Configure and deploy the VCE_UserAck maintenance policy in all new and existing associated service profiles. Complete this task before configuring host firmware policies to support the Cisco UCS server firmware auto install feature.

- Create a host firmware policy for the version of code being deployed. During creation of the policy, do not set the package version or define specific firmware versions. The Cisco UCS Server Firmware Auto Install wizard updates the embedded firmware package version of the policy. Assign this host firmware policy to the service profile templates that are associated with the blade to update using Auto Install. If the service profile does not set the host firmware policy for the blade, the host firmware policy is set to the default.

- Do not update the Cisco UCS default host firmware package with server firmware upgrades or reference the package with the server Cisco UCS Auto Install wizard. This action may result in unexpected server reboots. If the default host firmware policy is updated, the blade could reboot if the default maintenance policy (immediate reboot) is configured. Updating the default host firmware package for a new firmware version can trigger an update and immediate reboot of all unassociated servers.

Setting a firmware package version during the initial creation of the host firmware policy could trigger an immediate upgrade of the blade. Depending on the maintenance policy for the service profile, an unexpected server reboot could occur. Cisco has documented practices for managing firmware in the Cisco UCS Manager. Ensure that the firmware versions are compatible with the RCM.

To perform a Cisco UCS upgrade, see the Cisco UCS B-Series GUI Firmware Management Guide for the specific release being installed.

**Procedure**

1. To upgrade the Cisco UCS Infrastructure Firmware, perform the following:
   a. Select the **Equipment** tab and then select the **Firmware Management** tab.
   b. From the **Firmware Management** tab, select the **Firmware Auto Install** tab.
   c. Select **Install Infrastructure Firmware Upgrade**.
   d. On the **Prerequisites** page, do not check any boxes.
   
      1. **Note:** If no backup was performed or the Management Interfaces Monitoring Policy has not been enabled, do not perform the upgrade. Do not bypass any of the checks, or ignore faults.
   
      1. **Note:** Scheduled upgrades are the recommended methodology for Infrastructure upgrades. The secondary FI is upgraded automatically, but the primary FI is not upgraded without a user acknowledgment.

   e. Click Finish.

2. To upgrade Cisco UCS Server Firmware, perform the following:
   a. Select the **Equipment** tab, and the **Firmware Management** tab.
   b. From the **Firmware Management** tab, select the **Firmware Auto Install** tab.
   c. Select **Install Server Firmware**.
   d. On the **Prerequisites** page, do not check any boxes.
   
      1. **Note:** If no system backup was performed or the Management Interfaces Monitoring Policy has not been enabled, do not go to the upgrade. Do not bypass any of the checks.

   e. On the **Select Package Versions** page, select the firmware version for the Cisco B-Series Blade software field and click **Next**.
   f. On the **Select Host Firmware Packages** page, select the **VCE-HostFirmware** package and click **Next**.
   g. On the **Host Firmware Package Dependencies** page, click **Next**.
h. On the **Impacted Endpoints Summary** page, click Install.

i. When appropriate, assign the new host firmware package to the blade servers that require the code upgrade. Reboot the server.

**After you finish**

If required, follow the Cisco recommended procedures for firmware downgrades. After a downgrade of a Cisco UCS domain to a previous release, delete all features that the downgraded firmware does not support.

**Note:** If your VxBlock System uses Cisco UCS 14xx VICs, and then upgrade the server and the FI to Cisco UCS firmware version 4.0.1 or higher.

---

### Activate a Cisco UCS Manager Capability Catalog

Cisco UCS Manager uses Cisco UCS Manager Capability Catalog to update the display and configure components.

**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 entry includes the vendor, model (PID), and revision. For each provider, you can view details of the equipment manufacturer and the form factor.

Each Cisco UCS Manager update includes Cisco UCS Manager Capability Catalog updates. Unless Cisco Technical Support instructs you otherwise, activate the Capability Catalog update only 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. In the Cisco UCS instance, you do not need to perform any tasks, reboot components 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**

Download, update, and activate a Cisco UCS infrastructure software bundle before activating a capability catalog.

**Procedure**

1. See the appropriate *Cisco UCS B-Series GUI Firmware Management Guide* for your release.

---

### Activate a port license

Port licenses for each Cisco UCS FI are factory-installed and shipped with the hardware.

**About this task**

The Cisco UCS 6296UP Fabric Interconnect has pre-installed licenses for the first 18 unified ports that are enabled in Cisco UCSM.

Expansion modules come with eight licenses that can be used on the expansion module or the base module. 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. If you uninstall the expansion module, the licenses are also uninstalled. Any default expansion...
module licenses that the base module is using are uninstalled from the ports on the base module, resulting in unlicensed ports.

The Cisco UCS 6332-16UP Fabric Interconnects have eight pre-installed unified port licenses, and four 40 GB QSFP port licenses. This FI is a fixed switch and does not include any expansion modules.

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. Install licenses to use more fixed ports. If you use an unlicensed port, the Cisco UCSM initiates a 120-day grace period that is measured from the first use of the unlicensed port. Installing a valid license file negates the grace period. The system records the amount of time that was used in the grace period. 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, FIs in the cluster should have the same number of licensed ports. If a failover occurs while asymmetry exists, Cisco UCS enables the missing licenses and initiates the grace period for each port used on the failover node.

Converged Systems ship with the appropriate number of FI licenses installed. If more licenses are needed, request a chassis activation kit.

**Procedure**

1. To view, obtain, download, install, and uninstall an FI license, see the [Cisco UCS Manager Configuration Guide](#) for your release.

---

**Set the time zone**

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

**About this task**

Set all devices in the Converged System to the same time.

See the *Logical Configuration Survey* for the correct time zone setting.

See the [Cisco UCS Manager Configuration Guide](#) for steps.

---

**Add the syslog server**

Logs are sent to the system log server to facilitate reporting alerts and troubleshooting.

**About this task**

VxBlock Central or Vision Intelligent Operations is configured to receive system log information from the Cisco UCS environment. For more information, see *Monitor Cisco UCS Manager using Syslog*.

**Before you begin**

Deploy a syslog server to be 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.
5. In the Server 1 section, for Admin State, click Enabled.
6. In the Level menu, click Critical.
7. In the Hostname field, type the primary syslog server IP address or hostname.
8. In the Facility field, select the appropriate facility.
9. Verify that logs have been received on the syslog server.
   See Monitor Cisco UCS Manager using syslog.

Delete a syslog server

Delete a syslog server from the Cisco UCS domain using the Cisco UCS Manager.

Procedure
   1. Log in to the Cisco UCS Manager.
   2. From the Admin tab, select Faults, Events, and Audit Log > Syslog.
   3. In the appropriate server section, for Admin State, click disabled.

Add an SNMP server

An SNMP server enables report alerting, monitoring, and troubleshooting of Cisco UCS Manager and the ability to receive SNMP traps.

About this task
SNMP v3 is the most secure protocol option.
VxBlock Central or Vision Intelligent Operations is configured to receive SNMP information from the Cisco UCS environment.

Before you begin
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 Protocol field, set Type to All.
      Note: You cannot change the default port of 161.
   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. 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.
   11. Verify that the SNMP server can poll the Cisco UCS Manager and receive traps.
Delete an SNMP server

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.
4. Select the Communication Services tab.
5. In the Admin State field, click Disabled.
6. Click Save Changes.

Create an IP address block in the management pool

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.

About this task

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Before you begin

Configure service profiles and service profile templates to use IP addresses from the management IP pool. Servers cannot be configured to use the management IP pool. All OOB IPv4 addresses in the management IP pool must be in the same subnet as the IP address of the fabric interconnect. IPv6 addresses should be in the configured in-band KVM VLAN. Do not assign static IP addresses to the management pool for a server or service profile.

Procedure

1. Log in to the Cisco UCS Manager.
2. In the Navigation window, select the LAN tab.
3. In the LAN tab, expand Pools > IP Pools.
4. Right-click the VCE-KVM-POOL IP Pool, and select Create Block of IPv4 Addresses or Create Block of IPv6 Addresses.
5. 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 or Prefix field, type the subnet mask or prefix that is 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 that is associated with the IP addresses in the block.
After you finish
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

Create a UUID range
Create a UUID pool using the Cisco UCS Manager.

Before you begin
Verify that the new UUID range does not exist on any preexisting Cisco UCS compute environment.

Procedure
1. Log in to the Cisco UCS Manager.
2. In the Navigation window, select the Servers tab.
4. Expand the node for the organization where you want to create the pool. If the system does not include multitenancy, 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, select Derived (the system creates the suffix) or Other (allows you to specify the suffix).
   d. In the Assignment Order field, select Default for the system to create the order, or Sequential to assign the UUIDs in sequence.
   e. Click Next.
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.

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

Related information
Cisco UCS Manager GUI Configuration Guide
Delete a UUID pool

If you delete a UUID pool, addresses are not reallocated from the pool been assigned to vNICs or vHBAs.

About this task

All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until:

- Associated service profiles are deleted.
- The 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

Cisco UCS Manager GUI Configuration Guide

Add a WWNN range

Add a range to the WWNN pool using the Cisco UCS Manager. A WWNN pool is a WWN pool that contains only WW node names.

About this task

A WWN pool only includes WWNNs or WWPNs in the following ranges:

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

All other WWN ranges are reserved. To ensure that Cisco UCS WWNNs and WWPNs are unique in the SAN fabric, use the 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 multitenancy, 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. In the Assignment Order field, select Default or Sequential (for Cisco UCS 2.2(2c) or higher, select Sequential), and 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.

After you finish
Include the WWNN pool in a vHBA template.

Related information
Cisco UCS Manager GUI Configuration Guide

Delete a WWNN range
Delete a range from the WWNN pool using the Cisco UCS Manager. If you delete a pool, the addresses are not reallocated from the pool that is assigned to vNICs or vHBAs.

About this task
All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until:
   • Associated service profiles are deleted.
   • The 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, select SAN > Pools > Organization_Name.
4. Expand the WWNN Pools node.
5. Right-click the WWNN pool to delete and select Delete.
6. If a confirmation dialog box appears, click Yes.

Related information
Cisco UCS Manager GUI Configuration Guide

Add a WWPN range
Add a range to the World Wide Port Names (WWPN) pool using the Cisco UCS Manager.

About this task
A WWN pool only includes WWNNs or WWPNs in the following ranges:
   • 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF
   • 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF

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

Create separate WWPN pools for SAN Fabric A and SAN Fabric B.

Before you begin
Obtain the WWPN information.
Procedure

1. Log in to the Cisco UCS Manager.
2. In the Navigation window, select the SAN tab.
3. 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 multitenancy, expand the root node.
5. Right-click WWPN Pools, and select Create WWNN Pool.
6. From the WWNN Pool window, perform the following:
   a. In the Define Name and Description window, type a unique name and description for the WWNN pool.
   b. In the Assignment Order field, select Default or Sequential (for Cisco UCS 2.2(2c) or higher, select Sequential), and click Next.
7. In the Add WWN Blocks window, click Add.
8. In the Create WWN Block window, perform the following:
   a. In the From field, type the first WWPN in the pool.
   b. In the Size field, type the number of WWPNs to include in the pool.
   c. Click OK.
9. Click Finish.

After you finish
Include the WWPN pool in a vHBA template.

Related information
Cisco UCS Manager GUI Configuration Guide

Delete a WWPN range

Delete a WWPN range from the WWPN pool using the Cisco UCS Manager. If you delete a pool, the addresses are not reallocated from the pool that is assigned to vNICs or vHBAs.

About this task
All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until:

- Associated service profiles are deleted.
- The vNIC or vHBA of the address 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 that you want to delete and select Delete.
6. If a confirmation dialog box appears, click Yes.
Add a MAC address range

Create a block of addresses to expand an existing MAC address pool.

Before you begin

Verify that the range of values does not conflict with existing MAC address values.

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 multitenancy, 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. In the Assignment Order field, select Default or Sequential (for Cisco UCS 2.2(2c) or higher, select Sequential), and 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.

Delete a MAC pool

If you delete a pool, the addresses are not reallocated from the pool that have been assigned to vNICs or vHBAs.

Before you begin

All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until:

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

For more information, see the Cisco UCS Manager GUI Configuration Guide.

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 that you want to delete and select Delete.
6. If a confirmation dialog box is displayed, click Yes.
Create a vNIC template

vNIC templates are used to create uniform virtual network adapters for service profiles and service profile templates.

**About this task**

Create a minimum of four vNIC templates for the service profiles. You can create vNIC templates for Disjoint Layer 2 configurations. As a best practice, evenly distribute vNICs between Fabric A and Fabric B.

**Procedure**

1. Log in to Cisco UCS Manager.
2. From the Navigation window, select the LAN tab, and expand Policies.
3. Under root, right-click vNIC templates and select Create vNIC Template.
4. Type a name for the template up to 16 characters. For example, vNIC-0-Fabric-A.
5. Select Fabric A.
6. Ensure Enable Failover is not selected.
7. Verify Adapter is selected for the target.
8. For Template Type, select Updating Template.
9. For MTU, type 9000.
10. Select all appropriate VLANs. If required, create VLANs.
    For a standard Cisco UCS - VDS 6.0 build, map all VLANs to each vNIC template or vNIC unless the environment dictates differently.
11. Select a preconfigured MAC Pool, or create one.
12. Select a QoS policy. VMware Virtual Standard Switch does not support QoS marking. For those adapters, the absence of QoS marking forces traffic back to a best effort QoS policy.
13. For Network Control Policy, select a policy with CDP enabled and Action on Uplink Fail set to Link Down.
    The CDP-Link-Loss policy exists.

Cisco UCS Manager GUI Configuration Guide

Create boot policies

A boot policy determines the configuration of the boot device, the location from which the server boots, and the order boot devices are invoked.

Create an SD boot policy

Add virtual media with the read-only option as the first boot order option, and local SD as the second boot option.

**Procedure**

1. Log in to Cisco UCS Manager.
2. From the Navigation window, select the Servers tab, and expand Policies.
3. Right-click Boot Policies, and select Create Boot Policy.
4. Type a name for the boot policy.
5. Leave all defaults selected.
6. Expand **Local Devices**, and select **Add Local CD/DVD** and **Add SD Card**.
7. Click **OK**.

**Create a SAN boot policy**
Add virtual media with the read-only option as the first boot order option, and local SD as the second boot option.

**Procedure**
1. Log in to Cisco UCS Manager.
2. From the **Navigation** window, select the **Servers** tab, and expand **Policies**.
3. Right-click **Boot Policies** and select **Create Boot Policy**.
4. Type a name for the boot policy.
5. Leave all defaults selected.
6. Expand **Local Devices**, and select **Add Local CD/DVD**.
7. Expand vHBAs, select **Add SAN Boot** and in the name field, type **vHBA-0**.
8. Select **Primary**, and click **OK**.
9. Click **Add SAN Boot** and in the name field, type: **vHBA-1**.
10. Select **Secondary**, and click **OK**.
11. Click **Add SAN Boot Target** and **Add SAN Boot Target to SAN Primary**.
12. Leave the Boot Target LUN set to 0.
13. In the **Boot Target WWPN** field, type the WWPN from your storage array.
14. Verify that **Type** is set to **Primary**, and click **OK**.
15. Click the **Add SAN Boot Target** and **Add SAN Boot Target to SAN Primary**.
16. Leave the Boot Target LUN set to 0.
17. In the **Boot Target WWPN** field, type the WWPN from your storage array.
18. Verify **Type** is set to **Secondary** click **OK**.
19. Click **Add SAN Boot Target** and **Add SAN Boot Target to SAN Secondary**.
20. Repeat steps 19-22.
21. Leave the **Boot Target LUN** set to 0.
22. In the **Boot Target WWPN** field, type the WWPN from your storage array.
23. Verify **Type** is set to **Secondary** click **OK**.

**Create a LAN boot policy for VxBlock Central deployments**
Add virtual media with the read-only option as the first boot order option, and local SD as the second boot option.

**Procedure**
1. Log in to Cisco UCS Manager.
2. From the **Navigation** window, select the **Servers** tab, and expand **Policies**.
3. Right-click **Boot Policies** and select **Create Boot Policy**.
4. Type a name for the boot policy.
5. Leave all defaults selected.
6. Expand **Local Devices**, and select **Add Local CD/DVD**.
7. Expand vHBAs, select **Add LAN Boot** and in the name field, type **vHNIC-0**.
8. For the IP address, type IPv4 or IPv6.
9. Click OK.
10. Repeat these steps for vNIC-1 as secondary.

Cisco Trusted Platform Module

Cisco Trusted Platform Module (TPM) provides authentication and attestation services that provide safer computing in all environments.

Cisco TPM is a computer chip that securely stores passwords, certificates, or encryption keys that are used to authenticate remote and local server sessions. Cisco TPM is available by default as a component in the Cisco UCS B- and C-Series blade servers, and is shipped disabled.

Only the Cisco TPM hardware is supported, Cisco TPM functionality is not supported. Making effective use of the Cisco TPM means using a software stack from a vendor with significant experience in trusted computing. Defer to the software stack vendor for configuration and operational considerations relating to the Cisco TPM.

VMware vSphere 6.7 supports TPM version 2.0.

Related information
www.cisco.com

BIOS policy (VMware vSphere 6.7)

Complete this task to set the BIOS policy for service profiles.

Procedure

1. Create a BIOS policy named VCE-Default.
2. Set the following options:
   - **Quiet Boot**: Disabled
   - **Intel Turbo Technology**: Enabled
   - **Intel SpeedStep Technology**: Enabled
   - **Intel Hyper-Threading Technology**: Enabled
   - **Intel Virtualization Technology**: Enabled
   - **Intel VT for Directed I/O**: Enabled
   - **CPU Performance**: Enterprise
   - **Direct Cache Access**: Enabled
   - **Power Technology**: Performance
   - **Processor C-state**: Disabled
   - **Processor C1E**: Disabled
   - **Processor C3 Report**: Disabled
   - **Processor C6 Report**: Disabled
   - **Processor C7 Report**: Disabled
   - **Energy Performance**: Performance
   - **Frequency-floor Override**: Enabled
   - **DRAM Clock Throttling**: Performance
   - **Package C-state Limit**: Platform Default
- **CPU Hardware Power Management**: Platform Default
- **Memory RAS Configuration**: Maximum Performance
- **Low-voltage Double-data-rate Mode**: Performance Mode
- **DRAM Refresh Rate**: Platform Default
- **Intel QuickPath Interconnect Snoop Mode**: Platform Default
- **CDN**: Enabled (VMware vSphere 6.7)

**Example:**

```
UCS-FI-A # scope org /
UCS-FI-A /org # create bios-policy VCE-Default
UCS-FI-A /org/bios-policy* # set quiet-boot-config quiet-boot disabled
UCS-FI-A /org/bios-policy* # set lv-dimm-support-config lv-ddr-mode performance-mode
UCS-FI-A /org/bios-policy* # set intel-turbo-boost-config turbo-boost enabled
UCS-FI-A /org/bios-policy* # set enhanced-intel-speedstep-config speed-step enabled
UCS-FI-A /org/bios-policy* # set hyper-threading-config hyper-threading enabled
UCS-FI-A /org/bios-policy* # set intel-vt-config vt enabled
UCS-FI-A /org/bios-policy* # set intel-vt-directed-io-config vtd enabled
UCS-FI-A /org/bios-policy* # set cpu-performance-config cpu-performance enterprise
UCS-FI-A /org/bios-policy* # set direct-cache-access-config access enabled
UCS-FI-A /org/bios-policy* # set processor-energy-config cpu-power-management performance
UCS-FI-A /org/bios-policy* # set processor-c-state-config c-state disabled
UCS-FI-A /org/bios-policy* # set processor-c1e-config c1e disabled
UCS-FI-A /org/bios-policy* # set processor-c3-report-config processor-c3-report disabled
UCS-FI-A /org/bios-policy* # set processor-c6-report-config processor-c6-report disabled
UCS-FI-A /org/bios-policy* # set processor-c7-report-config processor-c7-report disabled
UCS-FI-A /org/bios-policy* # set processor-energy-config energy-performance performance
UCS-FI-A /org/bios-policy* # set frequency-floor-override-config cpu-frequency enabled
UCS-FI-A /org/bios-policy* # set dram-clock-throttling-config dram-clock-throttling performance
UCS-FI-A /org/bios-policy* # set package-c-state-limit-config package-c-state-limit platform-default
UCS-FI-A /org/bios-policy* # set cpu-hardware-power-management cpu-hardware-power-management platform-default
UCS-FI-A /org/bios-policy* # set memory-ras-config ras-config maximum-performance
UCS-FI-A /org/bios-policy* # set lv-dimm-support-config lv-ddr-mode performance-mode
UCS-FI-A /org/bios-policy* # set dram-refresh-rate-config dram-refresh platform-default
UCS-FI-A /org/bios-policy* # set qpi-snoop-mode vpqpsnoopmode platform-default
```
Perform the following commands on vSphere 6.7 deployments only:

UCS-FI-A /org/bios-policy # scope token-feature "Consistent Device Name Control"
UCS-FI-A /org/bios-policy/token-feature # scope token-param cdnEnable
UCS-FI-A /org/bios-policy/token-feature/token-param # scope token-settings Enabled
UCS-FI-A /org/bios-policy/token-feature/token-param/token-settings # set is-selected yes
UCS-FI-A /org/bios-policy* # commit-buffer

Managing service profile templates

Cisco UCS service profiles are used to streamline the configuration and management of Cisco UCS servers. They provide a mechanism for rapidly provisioning servers and their associated network connections with consistency in all details of the environment. They can be set up in advance before physically installing the servers.

Service profiles override identity values on the server at the time of association. Resource pools and policies set up in the Cisco UCS Manager are used to automate administration tasks. Disassociate the service profile from one server and manually associate it with another through an automated server pool policy. Burned-in settings for the UUID and MAC address on the new server are overwritten with the configuration in the service profile. The server change is transparent to the network so there is no required reconfiguration of any component or application to use the new server.

The following system resources are used and managed through resource pools and policies:

- Virtualized identity information (including pools of MAC addresses, WWN addresses, management IP addresses, and UUIDs)
- Ethernet and FC adapter profile policies
- Firmware package policies
- Operating system boot order policies

Configure service profile templates

Before VMware vSphere ESXi is installed, add vNIC-0 and vNIC-1 only for blade servers with multiple network adapters.

About this task

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Before you begin

- Before creating service profile templates, verify that vNIC templates exist.
- Configure a minimum of four vNIC templates and two vHBA templates.

1. **Note**: Template names are provided as examples. Template names vary based on the vNIC templates that exist on the system.

2. **Note**: Use the Create New Service Profile workflow, available with VxBlock Central Workflow Automation, to automate the following process:

Procedure

1. Log in to the Cisco UCS Manager.
2. From the Navigation window, select the Servers tab and go to Service Profile Templates.
3. Right-click Service Profile Templates > 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>_<Converged System_ID>
   b. In the Type field, click Updating Template.
      
      CAUTION Updating Templates requires a UserAck Maintenance Policy. Failure to apply a UserAck Maintenance Policy may result in unexpected service profile reboots when modifying the Updating Service Profile Template.
   c. Create the policy if it does not exist and apply it to the Service Profile Updating Template. If the UserAck Maintenance Policy is not created or used, create a Service Profile Initial Template.
   d. In the UUID Assignment field, select created policy, and click Next.

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

6. On the Create vNIC window, configure vNIC-0.
   a. In the Name field, type vNIC-0.
   b. Select Use LAN Connectivity Template.
   c. In the vNIC Template field, select vNIC-0-Fabric-A.
   d. In the Adapter Policy field, select VMQ-Default > OK > Add.

   Note: Templates that are created for blade servers with multiple physical network adapters should only contain vNIC-0 and vNIC-1.

7. On the Create vNIC window, configure vNIC-1.
   a. In the Name field, type vNIC-1.
   b. Select Use LAN Connectivity Template.
   c. In the vNIC Template field, select vNIC-1-Fabric-B.
   d. In the Adapter Policy field, select VMQ-Default > OK > Add.

   Note: Templates that are created for blade servers with multiple physical network adapters should only contain vNIC-0 and vNIC-1.

8. For blade servers with a single network adapter, follow the preceding steps to create the following adapters:
   - vNIC-2 from the vNIC2-Fabric-A template
   - vNIC-3 from the vNIC-3-Fabric-B template

   Note: Servers with 1340 or 1380 single network adapter may show a mismatch in the order between vNIC in the UCS and VMNIC in the ESXi. To resolve the issue, follow the steps in How VMware ESXi determines the order in which names are assigned to devices (2091560).

9. In the Local Storage field, select UserAck Maintenance Policy, and perform the following:
   a. In the SAN Connectivity field, select Expert.
   b. In the WWNN Assignment field, select Global-WWNN-Pool, and click Add.

10. On the Create vHBA window, configure vHBA-0.
a. In the **Name** field, type **vHBA-0**.
b. Select **Use SAN Connectivity Template**.
c. In the **vHBA Template** field, select **vHBA-0-Fabric-A**.
d. In the **Adapter Policy** field, select **VMware > OK > Add**.

11. On the **Create vHBA** window, configure vHBA-1.

a. In the **Name** field, type **vHBA-1**.
b. Select **Use SAN Connectivity Template**.
c. In the **vHBA Template** field, select **vHBA-1-Fabric-B**.
d. In the **Adapter Policy** field, select **VMware > OK > Add**.

12. Retain the default **Zoning** settings.

13. For **vNIC/vHBA** placement, select **Specify Manually**, and perform the following:

<table>
<thead>
<tr>
<th>Value or field</th>
<th>Servers with a single mezzanine card</th>
<th>B200M4 blades with 1240/1280 or 1340/1380 VIC</th>
<th>B420M3 blades with 1240/1280 VIC</th>
<th>B460 blades with VMware vSphere 6.x</th>
<th>B480M5 blades with 1340/1380 or 1440/1480 VIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 vNIC-0</td>
<td>vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
</tr>
<tr>
<td>3 vNIC-1</td>
<td>vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
</tr>
<tr>
<td>4 vNIC-2</td>
<td>vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>5 vNIC-3</td>
<td>vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>6 Select the vHBAs tab.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 7 vHBA-0      | vCon 1 and click >>assign>>.          | vCon 1 and click >>assign>>.      | vCon 1 and click >>assign>>.      | vCon 1 and click >>assign>>.          | vCon 1 and click >>assign>>.      |
| 8 vHBA-1      | vCon 1 and click >>assign>>.          | vCon 2 and click >>assign>>.      | vCon 3 and click >>assign>>.      | vCon 2 and click >>assign>>.          | vCon 3 and click >>assign>>.      |

14. On the **vMedia Policy** window, retain the default settings.

15. On the **Server Boot Order** window, select the appropriate boot policy or create a one, and click **Next**.

16. From the **Maintenance Policy** field, select **Default** or **User Acknowledgement**, and click **Next**.

17. On the **Server Assignment** window, perform the following:

a. Select **Up** for the power state.

b. In the **Host Firmware** field, select the new firmware package and click **Next**.

18. On the **Operational Policies** window, select the following:

a. For **Bios Policy**, select **VCE_Default**.

b. Select **External IPMI Management Configuration**.

c. For **IPMI Access Profile**, select **IPMI**.

d. Select the **Management IP Address**.

19. In the **Scrub Policy** field, select **default**, and click **Finish**.
After you finish

For servers with more than one network adapter, add vNIC2, vNIC3, and other vNICs individually after installing VMware vSphere ESXi. Adding vNICs individually forces the vNIC and VMNIC ID numbers to match each host.

Related information

Configuring service profile templates for Disjoint Layer 2 on page 37

Cloning the service profile templates

Clone and modify the service profile templates after they have been configured.

About this task

The following table provides sample values that can be used for cloned service profile templates:

<table>
<thead>
<tr>
<th>Template type</th>
<th>Sample name</th>
<th>Sample boot policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service profile template</td>
<td>2_B200-01</td>
<td>&lt;correct boot policy&gt;</td>
</tr>
<tr>
<td>Cloned service profile template</td>
<td>3_B200-01</td>
<td>3_storagesystem_serialnumber</td>
</tr>
<tr>
<td>FC bandwidth only: service profile template</td>
<td>4_B200-01</td>
<td>4_storagesystem_serialnumber</td>
</tr>
<tr>
<td>FC bandwidth only: cloned service profile template</td>
<td>5_B200-01</td>
<td>5_storagesystem_serialnumber</td>
</tr>
</tbody>
</table>

Procedure

1. To clone a service profile template, perform the following:
   a. Right-click the service profile template that was configured, and click Create a Clone.
   b. For Clone Name, type a name for the service profile template.
   c. For Org, select the appropriate organization, and click OK.
2. To modify the cloned service profile template, perform the following:
   a. Select the service profile template, and go to the Boot Order tab.
   b. Select Modify Boot Policy.
   c. Select the correct boot policy, and click OK.
3. Repeat steps 1 and 2 for each service template you want to clone and modify.

After you finish

Repeat these steps to clone more templates.

Adding vNICs to the service profiles

vNICs can be added to any service profile template or unbound service profile.

About this task

Adding new vNICs to a service profile that is already assigned to a Cisco UCS blade server may trigger a PCIe reprovisioning of vNICs/vHBAs devices. As a result PCIe addresses or adapter placement may change after reboot.

Service templates that are created for blade servers with multiple network adapters should only contain two network adapters. A minimum of two vNICs must be added to each service profile created from a two vNIC template after VMware vSphere ESXi has been installed.
Before you begin

Verify VMware vSphere ESXi has been installed on the hosts. If adding vNICs to a service profile, verify that the service profile is unbound from the service profile template.

Procedure

1. From the Network tab, click Add.

2. On the Create vNIC window, configure vNIC-2.
   a. In the Name field, type vNIC-2.
   b. Select Use LAN Connectivity Template.
   c. In the vNIC Template field, select vNIC-2-Fabric-A.
   d. In the Adapter Policy field, select VMQ-Default > OK > Add.

3. From the Network tab, select Modify vNIC/vHBA Placement, and depending on the blade type, perform the following:

   **vNIC-2**

<table>
<thead>
<tr>
<th>Half-width blades (B200/B230/B220) with a single mezzanine card</th>
<th>B200M4 or B460M4 blades with 1240/1280 or 1340/1380 VIC</th>
<th>B420M3 blades with 1240/1280 VIC</th>
<th>B460 blades with four adapters</th>
<th>B480M5 blades with 1340/1380 or 1440/1480 VIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 2 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 3 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 4 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 3 and click &gt;&gt;assign&gt;&gt;.</td>
</tr>
</tbody>
</table>

   Note: Servers with 1340 or 1380 single network adapter may show a mismatch in the order between vNIC in the UCS and VMNIC in the ESXi. To resolve the issue, follow the steps in How VMware ESXi determines the order in which names are assigned to devices (2091560).

4. Reboot the host.

5. On the Create vNIC window, configure vNIC-3.
   a. In the Name field, type vNIC-3.
   b. Select Use LAN Connectivity Template.
   c. In the vNIC Template field, select vNIC-3-Fabric-B.
   d. In the Adapter Policy field, select VMQ-Default > OK > Add.

6. From the Network tab, select Modify vNIC/vHBA Placement and perform the following:

   **vNIC-3**

<table>
<thead>
<tr>
<th>Half-width blades (B200, B230, B220) with a single mezzanine card</th>
<th>B200M4 or B460M4 blades with 1240/1280 or 1340/1380 VIC</th>
<th>B420M3 blades with 1240/1280 VIC</th>
<th>B460 blades with four adapters</th>
<th>B480M5 blades with 1340/1380 vNIC-3 or 1440/1480 VIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 2 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 3 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 4 and click &gt;&gt;assign&gt;&gt;.</td>
<td>vCon 3 and click &gt;&gt;assign&gt;&gt;.</td>
</tr>
</tbody>
</table>

   Note: Servers with 1340 or 1380 single network adapter, you may show a mismatch in the order between vNIC in the UCS and VMNIC in the ESXi. To resolve the issue, follow the steps in How VMware ESXi determines the order in which names are assigned to devices (2091560).

7. Reboot the host.
Configuring service profile templates for Disjoint Layer 2

Configure service profile templates on half-width, full-width, or quad blades with multiple network physical ports and onboard mLOM ports.

About this task

Add vNIC-4 and vNIC-5 individually to the service profile between reboots after installing VMware ESXi with vNICs 0 through 3. VMware vSphere ESXi interprets the PCI bus enumeration of the vNICs during installation.

CAUTION Adding new vNICs to a service profile that is already assigned to a Cisco UCS blade server may trigger a PCIe reprovisioning of vNICs/vHBAs devices. As a result PCIe addresses or adapter placement may change after reboot.

VMware vSphere 5.5 and later releases do not support remapping the VMNICs after the hypervisor is installed without a support ticket due to recent driver changes.

Use vNIC templates to create a template for vNIC-4-Fabric-A and for vNIC-5-Fabric-B.

Procedure

1. From the **Network** tab of the service profile template, click **Add**.

2. On the **Create vNIC** window, configure vNIC-4.
   a. In the **Name** field, type vNIC-4.
   b. Select **Use LAN Connectivity Template**.
   c. In the **vNIC Template** field, select vNIC-4-Fabric-A.
   d. In the **Adapter Policy** field, select VMQ-Default > OK > Add.

3. From the **Network** tab, select **Modify vNIC/vHBA Placement**, and depending on the blade type, perform the following:

   **vNIC-4**

<table>
<thead>
<tr>
<th>Half-width blades (B200, B230, B220) with a single mezzanine card</th>
<th>B200M4 or B460M4 blades with 1240/1280 or 1340/1380 VIC</th>
<th>B420M3 blades with 1240/1280 VIC</th>
<th>B460 blades with four adapters</th>
<th>B480M5 blades with 1340/1380 or 1440/1480 VIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select vCon 1, and click &gt;&gt;assign&gt;&gt;.</td>
<td>Select vCon 1, and click &gt;&gt;assign&gt;&gt;.</td>
<td>Select vCon 1, and click &gt;&gt;assign&gt;&gt;.</td>
<td>Select vCon 1, and click &gt;&gt;assign&gt;&gt;.</td>
<td>Select vCon 1, and click &gt;&gt;assign&gt;&gt;.</td>
</tr>
</tbody>
</table>

   **Note:** Servers with 1340 or 1380 single network adapter may show a mismatch in the order between vNIC in the UCS and VMNIC in the ESXi. To resolve the issue, follow the steps in *How VMware ESXi determines the order in which names are assigned to devices (2091560)*.

4. Reboot the host.

5. On the **Create vNIC** window, configure vNIC-5.
   a. In the **Name** field, type vNIC-5.
   b. Select **Use LAN Connectivity Template**.
   c. In the **vNIC Template** field, select vNIC-5-Fabric-B.
   d. In the **Adapter Policy** field, select VMQ-Default > OK > Add.

6. From the **Network** tab, select **Modify vNIC/vHBA Placement**, and depending on the blade type, perform the following:

   **vNIC-5**
Half-width blades (B200, B230, B220) with a single mezzanine card

<table>
<thead>
<tr>
<th>Blade Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B200M4 or B460M4 blades with 1240/1280 or 1340/1380 VIC</td>
<td>B200M4 or B460M4 blades with 1240/1280 or 1340/1380 VIC</td>
</tr>
<tr>
<td>B420M3 blades with 1240/1280 VIC</td>
<td>B420M3 blades with 1240/1280 VIC</td>
</tr>
<tr>
<td>B460 blades with four adapters</td>
<td>B460 blades with four adapters</td>
</tr>
<tr>
<td>B480M5 blades with 1340/1380 or 1440/1480 VIC</td>
<td>B480M5 blades with 1340/1380 or 1440/1480 VIC</td>
</tr>
</tbody>
</table>

Note: Servers with 1340 or 1380 single network adapter may show a mismatch in the order between vNIC in the UCS and VMNIC in the ESXi. To resolve the issue, follow the steps in How VMware ESXi determines the order in which names are assigned to devices (2091560).

7. Reboot the host.

Related information
Configure service profile templates on page 32

Assigning or modifying a management IPv4 address

Assign or modify a management IPv4 address to the service profile or service profile template for Converged Systems using Cisco UCS Manager.

About this task
The IP address is assigned to the service profile or service profile template. Assign the IP address to the service profile instead of the blade. If the service profile moves to another blade, the IP address follows the service profile to the new blade.

With Cisco UCS management software, you can connect to the Cisco UCS Manager, or obtain access to a Cisco KVM Manager. If the Cisco KVM Manager option is used, set the management IP addresses on each service profile or service profile template. A static IP address can only be assigned to a service profile that is not associated with a service profile template. An IP pool must be used to assign management IP addresses to service profiles associated with a service profile template.

Procedure
1. From the Servers tab of the Cisco UCS Manager, select Servers > Service Profiles > Root.
2. Select the first service profile or service profile template.
3. From the General tab, select Change Management IP Address.
4. Select Static or the required IP pool from the Management IP Address Policy drop-down menu.
5. Type the IP Address, Subnet Mask, and Gateway for the static address.
6. Repeat this process for all service profiles or service profile templates.

Create a network profile for the IPv6 management address

Create an in-band network profile in the Cisco UCS Manager before assigning an IP address to a service profile or service profile template for VxBlock Systems.

About this task
IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Before you begin
- Verify that the VLAN is configured on the LAN uplink switches and exists in Cisco UCS Manager.
- Verify that the VLAN group exists in Cisco UCS Manager.
- Do not select an IP address pool in the in-band network profile.
Procedure

1. From the Navigation window of the Cisco UCS Manager, select the LAN tab.
2. Select LAN and the Global Policies tab.
3. From Inband Profile, select Inband VLAN Group and the VLAN from the Network list, and click Save Changes.

Assign or modify a management IPv6 address

Change the management IP address on a service profile or service profile template for VxBlock Systems.

About this task

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Before you begin

See Create an in-band network profile for the IPv6 management address assignment to create the IPv6 KVM VLAN, VLAN group, and in-band network profile.

Cisco only supports IPv6 KVM, or CIMC addresses using an in-band profile.

Procedure

1. On the Servers tab, select Servers > Service Profiles > Root.
2. Select the service profile or service profile template that you want.
4. From the Inband tab, select the KVM VLAN in the Network drop-down list.
5. From the Inband IPv6 tab, select Static or the IPv6 IP pool from the Management IP Address Policy drop-down list.
6. If Static is selected, type the IPv6 IP address, prefix, default gateway address, and DNS server addresses, and click OK.

Assigning service profiles to Cisco UCS blade servers

Assign service profiles to the Cisco UCS blade servers using the Cisco UCS Manager.

Procedure

1. From the Navigation window, select the Servers tab.
2. Select Service Profile Host-01-1 and click Change Service Profile Association.
3. Under Server Assignment, click Select Existing Server.
4. Select the appropriate blade for this profile.
5. Distribute service profiles evenly within a VMware cluster across available chassis. The arrangement depends on the number of installed chassis and blades 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.
6. Select **Restrict Migration** and click **OK**.
7. Repeat this procedure for all service profiles.

**Renaming service profiles**

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 service profile name, and click **OK**.
Managing networking resources

Manage VMware NSX

For information about managing VMware NSX, see the *VMware NSX for vSphere Administration Guide.*

Related information

VMware NSX for vSphere Administration Guide

Create a named VLAN on both FIs

Add a named VLAN to both FIs in the Cisco UCS instance to connect to a specific external LAN.

About this task

The VLAN isolates traffic, including broadcast traffic to that external LAN. To ensure proper failover and load-balancing, add VLANs to both FIs.

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 Do not use the same ID for a VLAN and an FCoE VLAN in a VSAN. The result is 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 in to Cisco UCS Manager and select the **LAN** tab.
2. Expand **LAN > LAN CLOUD**, right-click **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**.

Related tasks

Add a VLAN to a service profile template on page 42

Related information

Cisco UCS Manager GUI Configuration Guide
Create a VLAN group on VxBlock Systems

Create a VLAN group on VxBlock Systems to use IPv6 features such as an in-band profile within the Cisco UCS Manager.

About this task

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Before you begin

Verify that the selected VLAN is configured on the LAN uplink switches and exists in Cisco UCS Manager.

Procedure

1. Log in to the Cisco UCS Manager.
2. In the Navigation, select the LAN tab.
3. Select LAN > VLAN Groups.
4. Right-click VLAN Groups, and select Create VLAN Group.
5. Type the VLAN group name.
6. Select the VLAN from the list, and click Next.
7. In a Disjoint Layer 2 environment, select the required uplink ports or uplink port channels. In a non-Disjoint Layer 2 environment, do not select a specific uplink port or port channel.
8. Click Finish after populating required fields.

Add a VLAN to a service profile template

Add a 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, then select an Ethernet interface and click Modify. If Modify is disabled, check the name of the vNIC template which the service profile is attached to, then go to Step 6.
4. Select the VLAN you created, and click OK.
5. Repeat these steps for the other Ethernet interface.
7. Select the vNIC template, and click Modify VLANs.
8. Select the VLAN you created, and click OK.
9. Repeat these steps for any other applicable vNIC templates on your service profile template.

After you finish

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

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.

Note: Obtain approval before changing management settings.

Procedure

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

Related information
Cisco Nexus 1000V Port Profile Configuration Guide

Add a VLAN to the Cisco Nexus switches

Add a VLAN to the Cisco Nexus switches using Cisco NX-OS commands.

About this task
IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Before you begin

Name VLANs to identify usage. For example, `NFS-VLAN-109`.

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

Verify connectivity information for the Cisco Nexus switches, such as:
- Console information
- Login credentials
- IPv4/IPv6 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`
Remove a VLAN from the Cisco Nexus switches

Remove a VLAN from the Cisco Nexus switches using Cisco NX-OS commands.

About this task
IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Before you begin
Verify that the Cisco Nexus switches are up and reachable through the console or the management connection. Verify connectivity information for the Cisco Nexus switches, such as:

- Console information
- Credentials for logging on
- IPv4/IPv6 address
- Access method (SSH/TELNET)
- VLAN names

Procedure
1. To view all VLANs, type: `show vlan`
2. To enter configuration mode, type: `configure terminal`
3. To enter VLAN configuration mode, type: `vlan vlan_id`
4. To delete the specified VLAN, type: `no vlan vlan_id`

Configure a vPC

Use any available Ethernet port to form a Cisco vPC enabled port channel on Cisco Nexus switches.

About this task
Configure the spanning tree mode on the port channels appropriately. For example, spanning tree mode on port channels towards the aggregation switches can be configured as normal. Spanning tree mode on port channels towards servers and other non-network devices can be configured as edge.

Default port channels are:

- PO1 for the network uplink
- PO50 between the switches
- PO101 and PO102 from the switch to the FIs
- PO37 and PO38 for the AMP
- PO201 and PO202 for the X-Blades (if applicable)

To view ports that are reserved for VLANs, type: `show vlan brief`

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Before you begin
- Using the console or the management connection, verify that you can reach the Cisco Nexus switches.
- Verify that the Cisco Nexus switches have the vPC and LACP features enabled.
- Verify that the peering device doing port channeling with the Cisco Nexus switches has the LACP enabled.
- Verify the appropriate member Ethernet ports are physically cabled.
- Verify the Ethernet ports that are designated to become members of this port channel.
- Create a VLAN.
- Obtain required vPCs, IDs, and the VLANs required for each vPC.
- Obtain Cisco Nexus switches IPv4/IPv6 address/console information, log in credentials and access method (SSH/TELNET).

**Procedure**

1. Log in to the primary Cisco Nexus switch.
2. To start the configuration, type: `Switch-A# config terminal`
3. To specify the vPC, type: `Switch-A(config)# interface port-channel port_channel_number`
4. To add a description, type: `Switch-A(config-if)# description description`
   - **Note:** The description should include to, from, and a purpose.
5. To specify switchport mode, type: `Switch-A(config-if)# switchport mode mode`
   - where `mode` is Trunk or Access.
6. To specify the Cisco vPC ID, type: `Switch-A(config-if)# vpc vPC_ID`
7. To enable trunking on the access VLAN or the VLANs, type one of the following:
   - `Switch-A(config-if)# switchport access vlan_id`
   - `Switch-A(config-if)# switchport trunk allowed vlan vlan_id`
8. To set the spanning tree port, type: `Switch-A(config-if)# spanning-tree port type type`
   - Where `type` specifies the type: normal/network/edge trunk/etc.
9. To set the state, type: `Switch-A(config-if)# no shut`
10. To add the appropriate Ethernet ports as members of the vPC:
    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 vPC).
    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 tasks**

- Add a VLAN to the Cisco Nexus switches on page 43
- Delete a vPC on page 46
- Cisco Nexus 5000 Series Software Configuration Guide
Delete a vPC

Delete a vPC from the Cisco Nexus switch.

Procedure
1. Log in to the Cisco Nexus series switch.
2. To start the configuration, type: `Switch-A# config terminal`
3. To delete the appropriate Ethernet port as a member of the vPC, type: `Switch-A# interface ethernet port_number`
4. Type: `Switch-A(config-if)# no channel group channel_number mode active`
5. To delete the vPC, type: `Switch-A(config)# no interface port-channel port_channel_number`

Related tasks
Configure a vPC on page 44
Cisco Nexus 5000 Series Software Configuration Guide

Add VLANs to a vPC

VLANs can be added to the trunk of an existing Cisco vPC on the Cisco Nexus series switch.

About this task
Extra VLANs are added to the trunk of an existing vPC 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 must be modified is up.
- Obtain the required Cisco vPC ID and VLANs that must be added to the Cisco vPC.
- Cisco Nexus series switch connectivity information (IP address/console information), log in credentials and access method (SSH/TELNET).

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

Related tasks
Remove VLANs from a vPC on page 46

Remove VLANs from a vPC

VLANs can be deleted from the trunk of a Cisco vPC.

Procedure
1. Log in to the 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 delete the VLAN ID, type: `Switch-A(config-if)# switchport trunk allowed vlan remove VLAN_IDs`

Related tasks
Add VLANs to a vPC on page 46
Cisco Nexus 5000 Series Software Configuration Guide

Add vPCs to VLANs for Disjoint Layer 2 networks

Add vPCs to VLANs for Disjoint Layer 2 networks to define the VLANs that pass over specific uplinks using the Cisco UCS Manager.

About this task
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 vPCs 101 and 102 are production uplinks that connect to Cisco Nexus switch. Cisco vPCs 105 and 106 are customer uplinks that connect to external switches. If you use Ethernet performance port channels (103 and 104 by default), vPCs 101 through 104 should have the same VLANs assigned.
Before you begin

The procedure provides an example scenario for adding port channels to VLANs for Disjoint Layer 2 networks. Obtain the vPCs, VLANs, and VLAN-to-port channel assignments.

Procedure

1. Log in to the Cisco UCS Manager.
2. To assign VLANs to vPCs 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 vPCs 101 and 105 (Fabric B) appear under all required VLANs. See Viewing vPC assigned to VLANs for Disjoint Layer 2 networks.

3. To assign VLANs to vPCs 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 Fabric B.
e. Select Add to VLAN, and click OK.
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 vPC 106.
k. Select Add to VLAN, and click OK.
l. Verify that vPCs 102 and 106 (Fabric B) appear under all required VLANs.

Related tasks
View vPCs assigned to VLANs for Disjoint Layer 2 networks on page 49
Remove vPCs from VLANs for Disjoint Layer 2 networks on page 50

Related information
Configure upstream disjoint layer 2 network

View vPCs assigned to VLANs for Disjoint Layer 2 networks

Verify that vPCs 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 vPCs 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 vPCs.

Related tasks
Add vPCs to VLANs for Disjoint Layer 2 networks on page 47
Remove vPCs from VLANs for Disjoint Layer 2 networks on page 50

Related information
Configuring upstream disjoint layer 2 networks

Remove vPCs from VLANs for Disjoint Layer 2 networks

Remove vPCs from VLANs in a Disjoint Layer 2 network.

About this task
If you delete all port or vPC interfaces from a VLAN, the VLAN returns to the default behavior. Data traffic on that VLAN flows on all uplink ports and vPCs. 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 dropping traffic, 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 vPCs and VLANs on that fabric interconnect.
7. In the VLANs table, expand the appropriate node and the VLAN from which you want to delete the assigned ports or vPCs.
8. Select the port or vPC that you want to delete from the VLAN. 
   - Note: Hold down the Ctrl key to click multiple ports or vPCs.
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 tasks
View vPCs assigned to VLANs for Disjoint Layer 2 networks on page 49
Add vPCs to VLANs for Disjoint Layer 2 networks on page 47

Related information
Configuring upstream disjoint layer 2 networks

Upgrade Cisco Nexus switch software

Upgrade the system image on the Cisco Nexus 9000 Series Switches.

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

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

**Before you begin**

See the Cisco website to access the software upgrade code and review release notes.

Depending on the running release, a multistep upgrade may be required. To verify whether multiple upgrade steps are required, see the section in the release notes titled *Upgrading or Downgrading to a new release*.

- Obtain console (terminal) access and management IPv4/IPv6 access.
- Obtain a Cisco account to download images.
- Verify that there is an SCP, TFTP, FTP, or SFTP server to upload the Cisco NX-OS image to the switch.

**Procedure**

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

      The system copies the images to the switch, and the following message opens:

      ```
      ***** Transfer of file Completed Successfully *****
      ```
7. To view the impact of the upgrade, type: `Switch-A(config)# show install all impact kickstart bootflash:n9000-dk9.6.1.2.I2.2(1).bin`
8. If you are performing a disruptive upgrade, following warning opens:

```
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.
```

9. Type `Y` to continue the installation.

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

11. From the returned version information, verify that the system image file is the correct version.

After you finish

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

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

Related information

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/upgrade/7_x/Cisco_n3k_Upgrade_Downgrade_7x.html
Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x

Downgrade Cisco Nexus switch software

Downgrade Cisco Nexus switch software to restore the original version after a failed upgrade.

Procedure

1. To reverse a Cisco Nexus series switch software upgrade, perform the upgrade steps using the earlier version of the software.

Related information

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/upgrade/7_x/Cisco_n3k_Upgrade_Downgrade_7x.html
Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide
Managing Cisco MDS switches

Upgrade Cisco MDS switch software

Upgrade or downgrade the firmware on the Cisco MDS series switches.

About this task
IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Before you begin
- 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) and management IPv4/IPv6 access.
- Obtain a Cisco account to download any images.
- Obtain an SCP, TFTP, FTP, or SFTP server to upload the Cisco NX-OS image to the switch.
- Obtain 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.

Sample kickstart filenames are as follows:
- m9300-s1ek9-kickstart-mz-npe.6.2.13b.bin
- m9100-s5ek9-kickstart-mz.6.2.9a.bin

Sample NX-OS file names are as follows:
- m9300-s1ek9-mz.6.2.13.bin
- m9100-s5ek9-mz.6.2.9a.bin
- m9700-sf3ek9-mz.6.2.9a.bin

6. Download Kickstart and system software with the copy server.
7. To copy the Kickstart and the system files from the FTP copy server to the fabric switch, from the MDS# prompt perform the following:
   a. To access the bootflash directory, type: `cd bootflash:
   b. To verify free space, type: `dir`
   c. To copy the files, type:
8. To verify storage space on the standby supervisor, from the MDS# prompt, type:

```
cd bootflash:
dir
```

9. While in configure mode, depending on the Converged System, from the VSJ3X2M9148SB# prompt, type:

```
configure terminal
```

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

VSJ3X2M9148SB(config)# no logging level all

10. To verify the impact of the firmware upgrade, depending on the switch, perform the following:

For VBxx-9396S-A#, type:

```
show install all impact kickstart m9300-slek9-kickstart-mz-npe.6.2.13b.bin system m9300-slek9-mz.6.2.13b.bin
```

For VBxx-9706-A#, type:

```
show install all impact kickstart m9700-sf3ek9-kickstart-mz.6.2.9a.bin system m9700-sf3ek9-mz.6.2.9a.bin
```

For VSJ3X2M9148B#, type:

```
show install all impact kickstart m9100-s5ek9-kickstart-mz.6.2.9a.bin system m9100-s5ek9-mz.6.2.9a.bin
```

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

12. To install the system and kickstart software, type: install all kickstart <kickstart file> system <system file>

For example:

- MDS9396S-A# install all m9300-slek9-kickstart-mz-npe.6.2.13b.bin system m9300-slek9-mz.6.2.13b.bin
- MDS9706-A# install all kickstart m9700-sf3ek9-kickstart-mz.6.2.9a.bin system m9700-sf3ek9-mz.6.2.9a.bin
- VSJ3X2M9148B# install all kickstart m9100-s5ek9-kickstart-mz.6.2.9a.bin system m9100-s5ek9-mz.6.2.9a.bin

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

Related information
Downgrade Cisco MDS switch software

Downgrade Cisco MDS switch software to restore the original version after a failed upgrade.

**Procedure**

1. See the Cisco MDS 9000 NX-OS Software Upgrade and Downgrade Guide for your release, and follow the guidelines for downgrading the software.

Configure a VSAN

Configure a VSAN, and assign FC interfaces.

**About this task**

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

**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 must be assigned to the VSANs.
- Obtain Cisco MDS switch IPv4/IPv6 address/console information, login credentials, and access method (SSH/TELNET).
- Name VSANs to identify usage. For example, for VSAN 10: SAN_A.

**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**

Configuring and Managing VSANs

Remove a VSAN

Remove a VSAN and associated FC interfaces.

**About this task**

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

**Before you begin**

- Verify that the Cisco MDS switch is reachable through the console or management connection.
Obtain required VSANs, names, and FC interfaces.
Obtain Cisco MDS switch IPv4/IPv6 address/console information, log in to 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 delete a VSAN, type: `no vsan vsan_id`

**Related information**

Configure and Manage VSANs

### Configure a domain ID and priority for a VSAN

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

**About this task**

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

**Before you begin**

- A unique domain ID must be assigned to the new VSAN added to the switch. When a 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 or joins a new fabric, the switch can request a specific domain ID or take any available domain ID.
- Verify that the Cisco MDS switch is up and reachable through the console or management connection.
- Obtain required VSANs, names, and FC interfaces that must 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 IPv4/IPv6 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`

### Remove a domain ID and priority from a VSAN

Remove the domain ID and priority to ensure that the switch is no longer a principal switch in that VSAN. You can then change the domain ID in that VSAN during a fabric merge.

**Procedure**

1. To enter the global configuration mode and start the configuration, type: `switch# configure terminal`
2. To view the VSAN database, type: `switch(config)# vsan database`

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

## Enable FC interfaces

Enable FC interfaces on the Cisco MDS switch.

### About this task

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

### 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 IPv4/IPv6 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`

## Disable FC interfaces

Disable FC interfaces on the Cisco MDS switch.

### About this task

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

### Before you begin

- Verify that the Cisco MDS switch is up and reachable through the console or management connection.
- Obtain the FC interface IDs.
- Obtain Cisco MDS Switch IPv4/IPv6 address/console information, login credentials, and access method (SSH/TELNET).

### Procedure

1. Log in to the Cisco MDS switch.
2. To enter configuration mode, type: `switch-A# config terminal`
3. To specify the interface, type: `switch-A(config)# interface fc interface_id`
4. To disable the interface, type: `switch-A(config-if)# shutdown`
Move licenses between FC interfaces

Move licenses between FC interfaces on Cisco MDS switches.

About this task
IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

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 IPv4/IPv6 address/console information, login credentials, and access method (SSH/TELNET).

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

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

Create FC aliases

Create FC aliases.

About this task
IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Before you begin
- Verify that the Cisco MDS switch is up and reachable through the console or management connection
- Obtain:
  - Required PWWN of the device
  - VSAN ID of the device
  - Cisco MDS Switch IPv4/IPv6 address/console information, log on credentials and access method (SSH/TELNET)
Procedure

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

Delete an FC alias

Delete an FC alias.

About this task

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Procedure

1. Log in to the Cisco MDS switch.
2. Type: `switch-A# config terminal`
3. To disable the FC alias, type: `switch-A(config)# no fcalias name alias_name vsan vsan_id`

Create FC zones

Create an FC zone.

About this task

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Before you begin

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

- FC alias for members of the zone
- VSAN ID of the device
- Cisco MDS Switch IPv4/IPv6 address/console information, log on credentials and access method (SSH/TELNET)

Procedure

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

Delete an FC zone.

About this task

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Procedure

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

Create, modify, and activate zone sets

Create and activate zone sets.

About this task

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Before you begin

- Verify that the Cisco MDS switch is up and reachable through the console or management connection
- Obtain:
  - Names of the zones to be added or removed
  - Name of the zone set to be modified or created
  - VSAN ID of the zone set
  - Cisco MDS Switch IPv4/IPv6 address/console information, log on credentials and access method (SSH/TELNET)

Procedure

1. Log on to the Cisco MDS switch.
2. To start the configuration, type: `switch-A# config terminal`
3. To create or modify the zone set, type: `switch-A(config)# zoneset name zoneset_name vsan vsan_id`
4. To add members to the zone set, type: `switch-A(config-zone)# member zone_name`
5. To remove members from the zone set, type: `switch-A(config-zone)# no member zone_name`
   
   **Note:** When running zone mode enhanced, you must issue the `zone commit` command for zoning changes to take effect.

6. To activate the zone set: `switch-A(config)# zoneset activate name zoneset_name vsan vsan_id`
7. To exit: `switch-A(config-zone)# end`
8. To verify that the zone is configured, type: `show zoneset name zoneset_name vsan vsan_id`
9. To verify the active zone set, type: `show zoneset active vsan vsan_id`
Creating FC port channels

Create a FC port channel.

About this task
IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Before you begin
- Verify that the Cisco MDS switch is up and reachable through the console or management connection
- Obtain:
  - Required FC interface IDs of port channel members
  - The VSAN IDs of the interfaces
  - Cisco MDS Switch IPv4/IPv6 address/console information, log on credentials and access method (SSH/TELNET)

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

Remove an FC interface from a port channel

Remove an FC interface from a port channel.

About this task
IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Procedure
1. To start the configuration, type: switch-A# config terminal
2. To remove an FC interface from the port channel, type: `switch-A(config)# interface fc interface_id`
3. Type: `switch-A(config-if)# no channel-group`
4. To remove a port channel, type: `switch-A(config)# no interface port-channel port-channel_id`
Managing storage resources

Managing XtremIO

The XtremIO storage array provides the storage component for the Converged System. XtremIO is an all-flash system that uses building blocks known as X-Bricks that can be clustered together.

System operation of the XtremIO storage array is controlled by a standalone, dedicated, Linux-based server called XtremIO Management Server (XMS). The XMS host which can be either a physical or virtual server. XtremIO can continue operation when disconnected from the XMS, but cannot be managed.

Refer to the XtremIO Storage Array User Guide for information about managing XtremIO. Refer to the XtremIO Host Configuration Guide for guidance on recommended VMware vSphere server settings.

Best practices for XtremIO

There are recommendations for creating LUNs on XtremIO storage arrays.

When creating LUNs or adding new servers, use fewer, larger LUNs on XtremIO storage arrays. For applications requiring the most optimal performance, do not use more than 32 server initiators per XtremIO front-end port.

The following table provides the maximum blade server count for the 10 GB connectivity option:

<table>
<thead>
<tr>
<th>XtremIO storage array X-Brick count</th>
<th>FC ports per fabric</th>
<th>Maximum compute chassis (w/ 6296UP FIs)</th>
<th>Maximum blade server counts (w/ 6296UP FIs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>64</td>
<td>32 half width, 32 full-width, or 32 double-height, full-width blades</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>64</td>
<td>64 half width, 64 full-width, or 64 double-height, full-width blades</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>64</td>
<td>128 half width, 128 full-width, or 128 double-height, full-width blades</td>
</tr>
<tr>
<td>6</td>
<td>12</td>
<td>64</td>
<td>192 half width, 192 full-width, or 128 double-height, full-width blades</td>
</tr>
<tr>
<td>8</td>
<td>16</td>
<td>64</td>
<td>256 half width, 256 full-width, or 128 double-height, full-width blades</td>
</tr>
</tbody>
</table>

The following table provides the maximum blade server count for the 40 GB connectivity option:

<table>
<thead>
<tr>
<th>XtremIO storage array X-Brick count</th>
<th>FC ports per fabric</th>
<th>Maximum compute chassis (w/ 6296UP FIs)</th>
<th>Maximum blade server counts (w/ 6296UP FIs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>8</td>
<td>32 half width, 32 full-width, or 16 double-height, full-width blades</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>16</td>
<td>64 half width, 64 full-width, or 32 double-height, full-width blades</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>32</td>
<td>128 half width, 128 full-width, or 64 double-height, full-width blades</td>
</tr>
</tbody>
</table>
To balance host clusters, zone four array front-end ports to a single server or spread the VMware vSphere ESXi cluster across several X-Brick building blocks.

If host clusters are heavily imbalanced in the number of hosts, zone the clusters differently. Ensure that all X-Brick building blocks have similar I/O loads. For larger host clusters, consider configuring eight paths depending on I/O requirement.

For servers with two vHBAs, zone each vHBA to both XtremIO Storage Controllers on a single X-Brick building block. If the XtremIO array has multiple X-Brick building blocks, zone the vHBAs to different X-Brick building blocks.

- vHBA 0 -> X1-SC1-FC1 and X1-SC2-FC1
- vHBA 1 -> X2-SC1-FC2 and X2-SC2-FC2

An example of four X-Brick building blocks and four clusters:

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster 1</td>
<td>X1-SC1-P1</td>
</tr>
<tr>
<td></td>
<td>X1-SC2-P1</td>
</tr>
<tr>
<td></td>
<td>X3-SC1-P2</td>
</tr>
<tr>
<td></td>
<td>X3-SC2-P2</td>
</tr>
<tr>
<td>Cluster 2</td>
<td>X2-SC1-P1</td>
</tr>
<tr>
<td></td>
<td>X2-SC2-P1</td>
</tr>
<tr>
<td></td>
<td>X4-SC1-P2</td>
</tr>
<tr>
<td></td>
<td>X4-SC2-P2</td>
</tr>
<tr>
<td>Cluster 3</td>
<td>X1-SC1-P2</td>
</tr>
<tr>
<td></td>
<td>X1-SC2-P2</td>
</tr>
<tr>
<td></td>
<td>X3-SC1-P1</td>
</tr>
<tr>
<td></td>
<td>X3-SC2-P1</td>
</tr>
<tr>
<td>Cluster 4</td>
<td>X2-SC1-P2</td>
</tr>
<tr>
<td></td>
<td>X2-SC2-P2</td>
</tr>
<tr>
<td></td>
<td>X4-SC1-P1</td>
</tr>
<tr>
<td></td>
<td>X4-SC2-P1</td>
</tr>
</tbody>
</table>

For servers with four vHBAs, zone each vHBA to one XtremIO storage controller for four paths as follows:

<table>
<thead>
<tr>
<th>vHBA</th>
<th>XtremIO storage controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>vHBA 0</td>
<td>X1-SC1-FC1</td>
</tr>
<tr>
<td>vHBA</td>
<td>XtremIO storage controller</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>vHBA 1</td>
<td>X1-SC2-FC2</td>
</tr>
<tr>
<td>vHBA 2</td>
<td>X2-SC1-FC1</td>
</tr>
<tr>
<td>vHBA 3</td>
<td>X2-SC2-FC2</td>
</tr>
</tbody>
</table>

- If there is only one VMware vSphere ESXi cluster that is connected to the XtremIO cluster, zone the vHBAs to every XtremIO front-end port in the fabric for hosts with 2 vHBAs.
- If there are four vHBAs, zone each vHBA to half the ports in the fabric.
- For ESXi clusters on Converged Systems, zone four paths per server. Increase up to eight paths depending on application requirements.
- VMware vSphere has a limit of 1024 device paths per server. Consider this limit when configuring more than two vHBAs.
- XtremIO has a limit of 16,000 paths and 1024 initiators per XtremIO cluster.
- Configure new volumes with a block size of 512 bytes.
- Format VMware vSphere ESXi VMs as **Thick Provision Eager Zeroed**.
Installing the latest VMware vSphere ESXi patch (vSphere 6.0)

Install the latest supported VMware vSphere ESXi patch.

**About this task**

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.

Use the VUM if upgrading to a newer supported build, however, you can use the CLI to install the patch.

Do not use this procedure for major upgrades.

**Before you begin**

- Verify that the host is in **Maintenance** mode and all the VMs are evacuated.
- Verify the software compatibility for the Cisco Nexus 1000V Series Switch or VMware VDS, PowerPath VE, and the build to which you are upgrading. You might need to upgrade third-party software before upgrading VMware vSphere ESXi.
- Obtain the *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 *Release Certification Matrix*.

**Procedure**

1. Download the latest VMware vSphere ESXi patch supported for this release.
2. Using a browser, navigate to the VMware patch portal.
3. In the **Search by Product** menu, select **ESXi (Embedded and Installable) | 6.x**.
4. Click **Search**.
5. Select and download the latest supported VMware vSphere ESXi patch.
   
   For example, ESXi6X0-2017XXXXX.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.

Installing the latest VMware vSphere ESXi patch (vSphere 6.5)

Install the latest supported VMware vSphere ESXi patch.

**About this task**

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.
Dell EMC 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 VMware VDS, 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 ESXi.
- Obtain the Release Certification Matrix and Release Notes 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. Refer to the appropriate Release Certification Matrix and Release Notes.

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) 6.5.
4. Click Search.
5. Select and download the latest supported VMware vSphere ESXi patch.
6. Install the patch as described in VMware knowledge base article 2008939.
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.

Installing the latest VMware vSphere ESXi patch (VMware vSphere 6.7)

Install the latest supported VMware vSphere ESXi patch.

About this task

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.

Use the VUM if upgrading to a newer supported build, however, you can use the CLI to install the patch.

Do not use this procedure for major upgrades.

Before you begin

- Verify that the host is in Maintenance mode and all the VMs are evacuated.
- Verify the software compatibility for the Cisco Nexus 1000V Series Switch or VMware VDS, PowerPath VE, and the build to which you are upgrading. You might need to upgrade third-party software before upgrading VMware vSphere ESXi.
- Obtain the 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 Release Certification Matrix.

Procedure

1. Download the latest VMware vSphere ESXi patch supported for this release.
2. Using a browser, navigate to the VMware patch portal.
3. In the Search by Product menu, select ESXi (Embedded and Installable) | 6.x.
4. Click Search.
5. Select and download the latest supported VMware vSphere ESXi patch.
   For example, ESXi6X0-2017XXXXX.zip
6. Install the patch as described in VMware knowledge base article 2008939.
7. To verify the installation, on the VMware vSphere ESXi host Splash Screen (through Cisco UCS vKVM), confirm that the build number matches the update just applied.
8. Reboot the VMware vSphere ESXi host.

### Configuring advanced settings for VMware vSphere ESXi (vSphere 6.0)

Configure advanced VMware vSphere ESXi settings.

#### About this task

NFS performance is enhanced when advanced configuration options are set. Apply 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 to configure the settings on all VMware vSphere ESXi hosts.

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>32</td>
</tr>
<tr>
<td>Net.TcpipHeapMax</td>
<td>512</td>
</tr>
</tbody>
</table>

#### 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. In the VMware vSphere client, select the host.
2. Select the Configuration tab.
4. Set the parameters in the window.
5. To configure the settings on each VMware vSphere ESXi host in the VMware vCenter using the script:
   a. Verify that VMware vSphere PowerCLI is installed on a Microsoft Windows machine.
   b. Verify that you have network access to the VMware vCenter server.
c. Copy the script to a .ps1 file on your hard drive.

   d. Modify the $vcenter variable.

   6. Execute the script in the VMware vSphere PowerCLI environment.

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

   7. 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.

After you finish
Reboot the VMware vSphere ESXi host.

Configuring advanced settings for VMware vSphere ESXi (vSphere 6.5)

Configure advanced VMware vSphere ESXi settings.

About this task
NFS performance is enhanced when advanced configuration options are set. Apply 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 Host client.

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>32</td>
</tr>
<tr>
<td>Net.TcpipHeapMax</td>
<td>512</td>
</tr>
</tbody>
</table>

Before you begin
- Obtain the IP address and local root user credentials for the VMware vSphere ESXi host.

Procedure
1. Log in to VMware Host Client using browser.
2. Click Advanced Settings under the System tab. Search for the parameters that are displayed in the table and update the value.
3. Review the updated value in the Advanced Settings section under the System tab using the VMware Host Client on each VMware vSphere ESXi host.

After you finish
Reboot the VMware vSphere ESXi host.
Configure advanced settings for VMware vSphere ESXi (VMware vSphere 6.7)

Configure advanced VMware vSphere ESXi settings.

About this task
NFS performance is enhanced when advanced configuration options are set. Apply 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 Host client.

The following advanced settings are available.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/Net/TcpipHeapSize</td>
<td>32</td>
</tr>
<tr>
<td>/Net/TcpipHeapMax</td>
<td>512</td>
</tr>
<tr>
<td>/NFS/MaxVolumes</td>
<td>256</td>
</tr>
<tr>
<td>/NFS/HeartbeatFrequency</td>
<td>12</td>
</tr>
<tr>
<td>/NFS/HeartbeatTimeout</td>
<td>5</td>
</tr>
<tr>
<td>/NFS/HeartbeatDelta</td>
<td>5</td>
</tr>
<tr>
<td>/NFS/HeartbeatMaxFailures</td>
<td>10</td>
</tr>
</tbody>
</table>

Before you begin
Obtain the IP address and local root user credentials for the VMware vSphere ESXi host.

Procedure
1. Log in to the VMware Host Client using a browser.
2. Click Advanced Settings under the System tab. Search for the parameters displayed in the table and update the value.
3. Review the updated value in the Advanced Settings section under the System tab using the VMware Host Client on each VMware vSphere ESXi host.
4. Restart the VMware vSphere ESXi host.

Restoring default values for VMware vSphere ESXi advanced settings (vSphere 6.0)

Use this procedure to restore the advanced settings for VMware vSphere ESXi to their default values.

Procedure
1. In the VMware vSphere client, select the host.
2. Select the Configuration tab.
4. Restore the parameters in the window to their default settings.

Note: For parameters that have numerical values, the default setting is most often the minimum value.
Restoring default values for VMware vSphere ESXi advanced settings (vSphere 6.5)

Use this procedure to restore the advanced settings for VMware vSphere ESXi to their default values.

Procedure

1. In the VMware Host Client, select Manage in navigator pane.
2. Click Advanced Settings under the System tab. Search for the appropriate parameters.
3. Restore the parameters in the window to their default settings.

   Note: For parameters that have numerical values, the default setting is most often the minimum value.

Restoring default values for VMware vSphere ESXi advanced settings (VMware vSphere 6.7)

Use this procedure to restore the advanced settings for VMware vSphere ESXi to their default values.

Procedure

1. In the VMware Host Client, select Manage in navigator pane.
2. Click Advanced Settings under the System tab. Search for the appropriate parameters.
3. Restore the parameters in the window to their default settings.

   Note: For parameters that have numerical values, the default setting is most often the minimum value.

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.

Increasing the disk timeout on Microsoft Windows VMs

Increase the amount of time for a Microsoft Windows VM to wait for unresponsive disk I/O operations.

About this task

- Increase the disk timeout value to 190 seconds. VMware tools, version 3.0.2 and later sets the value to 60 seconds.
- Include 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 VM.

Installing vCenter Server root certificates on web browser (vSphere 6.5)

Install the trusted root certificate authority (CA) certificates.

About this task

Install trusted root certificate authority (CA) certificates. This procedure is applicable for Internet Explorer only. For browsers other than Internet Explorer, refer to respective browser documentation.

Procedure

1. Open the Internet Explorer web browser and go to https://vcsa_fqdn.
2. In the vCenter getting started page, select Download trusted root CA certificates and save the file locally.
3. Unzip the downloaded files.
4. Right click on each .crt file and click Open. In the pop up dialog click Install Certificate. Select Local Machine and click Next, Next, and Finish.

Note: For more information, refer the VMware Knowledge Base article 2108294.

Install vCenter Server root certificates on web browser (vSphere 6.7)

Install trusted root certificates on Internet Explorer only. For browsers other than Internet Explorer, refer to respective browser documentation.

Procedure

1. Open Internet Explorer and enter the following URL: https://vcenter_fqdn.
2. From the VMware vCenter Server getting started page, select Download trusted root CA certificates and save one or more files locally.
3. Unzip the downloaded files.
4. Right-click each .crt file and click Open. In the window that appears, click Install Certificate.
5. Select Local Machine and click Next > Next > Finish.

Exact steps may differ depending on the version of the browser. For additional information, see VMware Knowledge Base article 2108294.
Setting up Java and Internet Explorer on the management workstation or VM (vSphere 6.x)

Set up Java and Internet Explorer version 11 on the management workstation or VM (element manager) if Unisphere or other web-based applications fail to launch. Configure the Java security setting to support web-based applications.

Before you begin
- vSphere 6.0: Ensure Java version 7 Update 51 or later is installed on the management workstation or VM.
- vSphere 6.5: Ensure Java version 8 Update 131 or later is installed on the management workstation or VM.
- Ensure the Java security level complies with your corporate security policy.

Procedure
1. Using administrative privileges, log on to Microsoft Windows on the management workstation or virtual machine.
2. Navigate to the Java Windows Control Panel.
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.
Manage VMware Single Sign On (VMware vSphere 6.x)

VMware vCenter Single Sign On (SSO) is an authentication mechanism used to configure security policies and lock out or disable an account for VMware vSphere 6.5. Default policies do not require modification. You may have to modify policies or accounts if regulations require different policies or when troubleshooting a problem.

VMware vCenter SSO overview

VMware vCenter SSO is an authentication mechanism used to configure security policies and lock out or disable an account for VMware vSphere. Default policies do not require modification. However, you might have to modify policies or accounts if regulations require different policies or if you are troubleshooting a problem.

Reset the VMware Single Sign On administrator password (VMware vSphere 6.x)

The VMware vSphere knowledge base article KB 2034608 contains instructions to unlock a VMware Single Sign On (SSO) administrator account.

Procedure

1. Follow the procedure in the VMware knowledge base article Resetting the vCenter SSO Administrator Password.

   Note: For security purposes, the VMware vCenter administrator account is locked after three failed attempts to log in.

Manage the lockout status of VMware Single Sign On (VMware vSphere 6.5)

View the lockout status of a VMware Single Sign On (SSO) account for VMware vSphere.

Procedure

1. Log in to the VMware vSphere Web Client as a VMware SSO administrator. By default, the VMware SSO administrator username 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 on the system. Select the Users tab.

4. The Locked or Disabled columns show the status of each configured VMware SSO account. Right-click the appropriate account and select Enable/Disable or Unlock.

   Note: The Locked Users and Disabled Users tabs provide information for the identity sources only.

5. Click Yes to confirm.
Manage the lockout status of VMware Single Sign On account (VMware vSphere 6.7)

View the lockout status of a VMware Single Sign On (SSO) account for VMware vSphere.

About this task

By default, the VMware SSO administrator username is administrator@vsphere.local.

Procedure

1. Log in to the VMware vSphere Client (HTML5) as a VMware SSO administrator.
3. Each tab shows information from the identity sources about configured accounts on the system. Select the Users tab.
4. Select vSphere.local as the domain.
5. The Locked or Disabled columns show the status of each configured VMware SSO account. Click the ellipsis vertical bar to Enable/Disable or Unlock.
6. Click Yes to confirm.

Manage VMware Single Sign On default password policies (VMware vSphere 6.0 or 6.5)

Manage the VMware Single Sign On (SSO) default password policies for VMware vSphere.

About this task

By default, the VMware SSO passwords expire after 365 days, including the VMware SSO administrator password. You can modify the expiration policy.

Procedure

1. Log in to the VMware vSphere Web Client as a VMware SSO administrator. By default, this user is administrator@vsphere.local.
2. From the home page, select Administration > Single Sign-On > Configuration.
4. To modify the password policy, click Edit.
5. Make the required changes and click OK.

Manage VMware vCenter SSO default password policies (VMware vSphere 6.7)

Modify the strict lockout policy of VMware vCenter SSO for VMware vSphere 6.7.

Procedure

1. Log in to the VMware vCenter Client (HTML5) as an SSO administrator. By default, this user is administrator@vsphere.local.
Manage VMware Single Sign On lockout policies (VMware vSphere 6.5)

Modify the strict lockout policy of VMware Single Sign On (SSO) for VMware vSphere 6.5.

Procedure
1. Log in to the VMware vSphere Web Client as a VMware SSO administrator. 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 required changes and click OK.

Manage VMware Single Sign On lockout policies (VMware vSphere 6.7)

Modify the strict lockout policy of VMware Single Sign On (SSO) for VMware vSphere 6.7.

Procedure
1. Log in to the VMware vSphere (HTML5) Client as a VMware SSO administrator (default account is administrator@vsphere.local).
3. Select the Policies tab and select Lockout Policy.
4. Click Edit.
5. Make any changes and click OK.

Add an AD identity source to VMware Single Sign On (IPv4) (VMware vSphere 6.7)

Use this procedure to associate a Windows AD to the VMware SSO service embedded on the VMware vCenter Server. This procedure applies to Embedded PSC Deployments and to separate VMware PSCs for external deployments.

Before you begin
Obtain network access to the VMware vSphere vCenter Web Client and use AD domain admin privileges.

Embedded deployments
1. Log in to the VMware vSphere Client (HTML5) on the element manager VM using the administrator@vsphere.local account at: https://<vcenter_fqdn_or_ip_address>/ui/
2. Go to Menu > Administration.
4. For Embedded PSC deployment, select vCenter server with Embedded PSC and click Join AD.
5. Enter the AD domain, username, and password (with appropriate AD domain administrative rights).
6. Leave Organizational unit blank and click OK.
7. Restart the node.

External deployments

1. Log in to the VMware vSphere Client (HTML5) on the element manager VM using the administrator@vsphere.local account at: https://<VCENTER_FQDN OR IP>/ui/
2. Go to Menu > Administration.
4. For each PSC:
   - Select the PSC to join to the AD domain and click JOIN AD.
   - Leave Organizational unit blank and click OK.
   - Restart the appliance.
5. Select the Identity Sources tab and click ADD IDENTITY SOURCE to enter details for the Active Directory domain being added.
7. Verify that the domain name that was previously registered to the PSC is assigned to this AD domain registration.
8. Click Use machine account > OK.
9. Select the added AD domain and click SET AS DEFAULT.
10. Log in to VMware vCenter Server through the VMware vSphere Client (HTML5) as the administrator@vsphere.local administrative user.
11. Assign administrator roles and permissions for domain user accounts or groups that require access to VMware vCenter 6.5.
   By default, only the administrator@vsphere.local account can access VMware vCenter Server until similar permissions are explicitly assigned to domain users.

Add Windows AD identity source to VMware SSO (VMware vSphere 6.7)

Associate a Windows AD to the VMware SSO service embedded on the VMware vCenter Server in Embedded PSC Deployments and on separate VMware PSCs for external deployments.

Before you begin
Obtain network access to the VMware vCenter Client (HTML5) and use AD domain admin privileges.

Procedure for Embedded deployments

1. Log in to the VMware vSphere Client (HTML5) on the element manager VM using the administrator@vsphere.local account at: https://<VCENTER_FQDN OR IP>/ui/
2. Navigate to Menu > Administration.
4. For Embedded PSC deployment, select vCenter server with Embedded PSC and click Join AD.
5. Enter the AD domain, username and password (with appropriate AD domain administrative rights).
6. Leave Organizational unit blank and click OK.
7. Restart the node.
Procedure for External deployments

1. Log in to the VMware vSphere Client (HTML5) on the element manager VM using the using the administrator@vsphere.local account at: https://<VCENTER_FQDN OR IP>/ui/
2. Navigate to Menu > Administration.
4. Perform the following for each PSC:
   - Select the PSC to join to the AD domain and click JOIN AD.
   - Leave Organizational unit blank and click OK.
   - Restart the appliance.
5. Select the Identity Sources tab and click ADD IDENTITY SOURCE to enter details for the Active Directory domain being added.
7. Verify that the domain name that was previously registered to the PSC is assigned to this AD domain registration.
8. Click Use machine account > OK.
9. Select the added AD domain and click SET AS DEFAULT.

While logged in to VMware vCenter Server through the VMware vSphere Client (HTML5) as the administrator@vsphere.local administrative user, assign administrator roles and permissions for domain user accounts or groups that require access to VMware vCenter 6.7.

By default, only the administrator@vsphere.local account can access VMware vCenter Server until additional permissions are explicitly assigned to domain users.

Backing up or restoring the vCenter Server

Back up or restore the VMware vCenter PSC for VMware vSphere 6.x. It is recommended to use VCSA Native backup to backup and restore the VMware vCenter server.

About this task

Maintaining a back-up of the PSC configuration ensures continued VMware vSphere access for VMware vCenter Server components. For backup and restore guidelines, see the following:


Procedure

1. Follow the back-up and restore procedure in the VMware knowledge base article KB 2149237.
2. Refer to the Backing Up and Restoring vCenter Server section in the VMware vSphere 6.x Documentation Center, which you can find here:

   ESXi and vCenter Server 6.x Documentation > vSphere Installation and Setup > Backing Up and Restoring vCenter Server.
Backing up and restoring the vCenter Server and PSC (vSphere 6.5)

The VMware vCenter Server 6.5 supports file-based and image-based backups. You can initiate backup and restore jobs using the GUI or API interfaces. Dell EMC recommends using VCSA native file-based backup to backup/restore PSC/vCenter Server. Dell EMC also recommends following the procedure to recover failed PSC’s. All PSCs/VCs in a SSO domain must be backed-up.

A recent backup must be available locally in the recovery site. VCSA Installer of same version/build should be available for recovery operation. The failed PSC must be powered off and removed from vCenter inventory.

Backing up the PSC and vCenter Server

Refer to the File-Based Backup and Restore of vCenter Server Appliance section in the VMware vSphere 6.5 Documentation Center.


Restoring the vCenter Server

Refer to the following VMware procedure for file-based restoring to restore the vCenter server.


Restoring the PSC

Complete this task to restore the PSC.

About this task

You must repoint a VMware vCenter server connected to a failed PSC to a surviving PSC to restore vCenter services.

Procedure

1. Run the installer of same version/build.
2. Select the restore option.
3. Enter the backup details such as location of the backup files, protocol used with port number, and credentials.
4. Review the backup information and provide the appliance deployment target ESXi.
5. Provide the hostname of the failed PSC and select the deployment size.
6. Select data store and review network settings.
7. Select Finish to start the restoration.
Redirect VMware vCenter Server to the secondary external VMware Platform Services Controller (VMware vSphere 6.x)

For VMware vSphere 6.x, repoint the VMware vCenter Server for authentication under the following conditions: the primary external VMware Platform Services Controller (PSC) fails, there are multiple VMware PSCs replicating, and the PSCs are configured without fault tolerance.

Note: VMware vSphere 6.7 and VMware vSphere 6.5 are the last VMware vSphere releases that support the deployment of external PSCs. Updates to both of these VMware vSphere versions support Enhanced Linked Mode in embedded PSCs, making external PSCs no longer necessary. Upgrading to VMware vSphere 6.7 update 1 or VMware vSphere 6.5 update 2d enables you to migrate external PSCs to embedded PSCs. For more information about changing to embedded PSCs from external PSCs, consult with your account team.

See the Repointing the Connections Between vCenter Server and PSC section of the VMware vSphere Installation and Setup Guide.

Related information
- VMware docs

Enabling fault tolerance for the external PSC

Enable fault tolerance on the external PSC for VMware vSphere 6.x.

About this task
For multiple PSCs, you can create fault tolerant pairing to provide continuous availability for VMware vCenter Server instance authentication.

Before you begin

1. Read the Providing Fault Tolerance for Virtual Machines section in the VMware vSphere Availability Guide from the VMware vSphere 6.x Documentation Center.
2. Review and resolve all validation and compliance checks needed to ensure fault tolerance is operational.
3. Confirm the PSC VM 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

1. Follow the Turn On Fault Tolerance procedure in the VMware vSphere Availability Guide of the VMware vSphere 6.x Documentation Center.
Managing virtualization

Patch VMware vSphere ESXi hosts with the VUM (VMware vSphere 6.0)

Patch the VMware vSphere ESXi hosts with 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 Converged 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 baseline.
10. From the New Baseline wizard, in the Name field, type the package name. For example, PowerPath.
11. For Host Baselines, click Host Extension.
12. Click Next.
13. Find the package extension and click the down arrow to add it to the Extensions to Add field.
15. You can attach the package baseline to individually selected VMware vSphere ESXi hosts or to multiple hosts at a time by selecting the cluster.

To attach the package baseline to several VMware vSphere ESXi hosts:

   a. Go to the Compliance view and select the host that you want from the list to the left of the vSphere client window. Select a folder, cluster, or data center.
   b. In the right window, select Update Manager and then click Attach.
   c. From the Attach Baseline or Group window, under Name, select the package baseline that you created.
   d. Click Attach.
16. Select **Scan**, and check the circle in the **Compliance** box on the upper 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>You have attached the baseline to the VMware vSphere ESXi host for the first time.</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>Stage and remediate the baseline (as described in Step 17) to achieve compliance. To verify the remediation, review the information in the <strong>Recent Tasks</strong> window, or click the <strong>Tasks/Event</strong> tab.</td>
</tr>
</tbody>
</table>

17. Staging is the process of pushing the package onto individual VMware vSphere ESXi hosts from the VUM server. To stage the baseline:

a. In the **Update Manager** tab, in the **Attached Baselines** list in the middle of the screen, select 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.

   ① **Note**: Do not change the default **Name** selection. In the **Host** column, all the VMware vSphere ESXi hosts to which you attached the package baseline are selected by default.

c. Optionally, 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**.

18. To remediate the package baseline, perform the following:

a. Select the VMware vSphere ESXi host to remediate.

   ① **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, select 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.

   ① **Note**: Do not alter default selections. Under **Host**, all the VMware vSphere ESXi hosts to which you staged the package baseline are selected by default.

c. Optionally, 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 to suit your environment.

h. Click **Next**.
The Ready to Complete window appears with your remediation selections.

i. Verify the information, and click Finish.

**Patch VMware vSphere ESXi hosts with the VUM (VMware vSphere 6.5)**

Patch the VMware vSphere ESXi hosts with 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 *Converged Systems Release Certification Matrix*.

**Procedure**

1. Log in to VMware vSphere Web client.
2. Select the VMware vSphere ESXi host, right-click, and select **Maintenance mode > Enter Maintenance Mode**.
3. In the vSphere Web Client, select the host and select the **Update Manager** tab.
4. Click **Go to Admin View** tab.
5. Click **Settings**.
6. Select **Download Settings**.
7. In the **Download Sources** pane, select **Import Patches**.
8. On the **Select Patches File** page of the **Import Patches** wizard, browse to the location where you saved the patch or package software bundle, select the file and click **Open**.
9. Click **Next** and wait until the file upload completes successfully. If the upload fails, the .zip file may have been corrupted during the download process or an incorrect .zip file may have been imported. Try downloading the .zip file again and then import.
10. Click **Next**.
11. On the **Ready to complete** page of the **Import Patches** wizard, verify the package that you imported into the VUM repository, and click **Finish**.
12. Select the **Patch Repository** tab.
13. Verify that the patch appears in the list.
14. Click the **Host Baselines** tab.
15. Click **Create** to create a baseline.
16. In the **New Baseline** wizard:
   a. In the **Name and type** field, type the package name. For example, **PowerPath**.
   b. For baseline type, click **Host Extension**.
   c. Click **Next**.
   d. In the **Patch Options** page, leave defaults selected and click **Next**.
   e. In the **Criteria** page, select **Next**.
   f. In the **Patches to Exclude** page, exclude all patches except PowerPath.
   g. In the **Additional Patches** page, click **Next**.
   h. Click **Finish**.
17. Attach the package baseline to the appropriate VMware vSphere ESXi hosts. You can attach the package baseline to individually selected VMware vSphere ESXi hosts or to multiple hosts. Select the cluster in the Inventory > Hosts and Clusters view. To attach the package baseline to an individual VMware vSphere ESXi host, go to the Compliance view. Select the host that you want from the list to the left of the vSphere Web Client pane. To attach the package baseline to several VMware vSphere ESXi hosts:
   a. In the list to the left of the vSphere Web client pane, select a folder, cluster, or data center.
   b. In the right pane, select Update Manager tab and then click Attach Baseline. The Attach Baseline or Baseline Group window opens.
   c. Under Individual Baselines page, select the package baseline that was created in Step 16 under Extension Baselines.
   d. Click OK.
18. Click Scan for Updates, and click OK. Check for the Compliance Status for the attached baseline.
19. Stage the baseline. 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 Independent Baselines list, select the package baseline that was created.
   b. Click Stage Patches.
   c. When the Stage Patches Wizard appears, under the Baselines Name column in the Baselines list, the package baseline that was created is selected by default. Do not alter the default Name selection.
   d. Click Next.
   e. In the Hosts window all the VMware vSphere ESXi hosts to which the package baseline is attached are selected by default.
   f. If required, alter the default Host selection to stage the baseline to only one or some of the VMware vSphere ESXi hosts.
   g. Click Next.
   h. In the Patch and Extension Exclusion window, verify the Package information and click Next.
   i. When the Ready to Complete window appears, verify the information and click Finish.
20. Remediate the package baseline. During this stage, packages are installed on hosts that do not have the package. The package is updated on hosts that have an outdated package. To remediate the baseline:
   a. Select the VMware vSphere ESXi host to remediate and click Update Manager tab.
   b. In the Independent Baselines section, select the package baseline that was created and click Remediate.
   c. From the Remediate page, in the Baseline Groups and Types section, Extension Baselines is selected by default. In the Baselines list, the package baseline that was created is selected by default. Do not alter the selections for default Baseline Groups and Types and Extension Baselines default selections.
   d. Click Next.
   e. In the Select target objects page, all the VMware vSphere ESXi hosts to which the package baseline is staged are selected by default. Optionally, alter the default Host selection to remediate the baseline to only one or some of the VMware vSphere ESXi hosts.
   f. Click Next.
   g. When the Patches and Extensions window appears, verify the information and click Next.
   h. In the Advanced options page, click Next.
   i. Click Next.
   j. When the Ready to Complete window appears, verify the information and click Finish.
Patch VMware vSphere ESXi hosts with the VUM (VMware vSphere 6.7)

Patch the VMware vSphere ESXi hosts with VUM from the VMware vCenter Client (HTML5). Starting with VMware vSphere 6.7, the VMware vCenter Client (HTML5) has full feature parity with the traditional flex web client.

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 Converged Systems Release Certification Matrix.

Procedure

1. Log in to VMware vCenter Client (HTML5) using the administrator@vsphere.local SSO account.
2. Select Home > Hosts and Clusters.
3. Right-click the VMware vSphere ESXi host, and select Maintenance Mode > Enter Maintenance Mode.
4. In the VMware vCenter Client (HTML5), select the host and select the Updates tab.
5. In the Updates page, click the Update Manager Home button.
6. From the Update Manager Home page, select Updates > UPLOAD FROM FILE.
7. In the Import Patches window, click Browse.
8. Browse to the location where you saved the patch or package software bundle, select the file, and click Open.
9. Select the Baselines tab, and click New baseline.
10. In the Baseline Definition wizard:
   a. In the Name field, type the package name (example: PowerPath).
   b. For the Content, select Patch and click Next.
   c. Click the Matched tab.
   d. In the patches list, clear all patches and select the patch for the baseline. Find the patch by applying column header filters. Click NEXT.
   e. In the Add Patches manually window, select Next > Finish.
11. Attach the package baseline to the wanted VMware vSphere ESXi hosts.

    You can attach the package baseline to individually selected VMware vSphere ESXi hosts or to multiple hosts by selecting the cluster in the Inventory > Hosts and Clusters view.

    Option A: To attach the package baseline to an individual VMware vSphere ESXi host, select the host from the left of the VMware vCenter Client (HTML5). Select the Updates tab.

    Option B: To attach the package baseline to several VMware vSphere ESXi hosts, perform the following:
   
    a. In the left-side inventory list, select a folder, cluster, or data center.
   
    b. In the right window, select the Updates tab and then select Host Updates.

    c. On the Attached Baselines window, select the package baseline that was previously created and click ATTACH.

    d. From the Attach list, select the baseline and click ATTACH.
12. Click Overview and under Hosts' Compliance, click CHECK COMPLIANCE.
13. Go to Host Updates, and verify the Compliance Status for the attached baseline. If the status is non-compliant, remediate (patch) the host using the patches in the baseline.

14. To stage the baseline, perform the following:
   a. In the Host Updates section, select the package baseline that was created in the Baselines list under Attached Baselines.
   b. Click STAGE.
   c. From the Stage Patches Wizard, under Install in the Baselines list, verify that the package baseline that was created is selected.
   d. In the Hosts pane, all the VMware vSphere ESXi hosts to which the package baseline is attached are selected by default. If required, alter the default host selection to stage the baseline to only one or some of the VMware vSphere ESXi hosts and click OK.

15. During remediation, packages are installed on hosts that do not have the package and/or the package is updated on hosts that have an outdated package.
   To remediate the baseline, perform the following steps:
   a. Select the VMware vSphere ESXi host to remediate and select the Updates tab.
   b. In Host Updates, under Attached Baselines, select the package baseline that was created and click REMEDIATE.
   c. In the Remediate window, review the remediation precheck report and address any issues.
      All the VMware vSphere ESXi hosts to which the package baseline is staged are selected by default.
   d. Click REMEDIATE.

Supported guest operating systems

For information about installing supported guest operating systems in VMware VMs, see the VMware Guest Operating System Installation Guide.

If VMware VMs are being configured with IPv6 for VxBlock Systems, a vmxnet driver must be deployed. The deployment should occur automatically when VMware Tools are installed.

Note: IPv6 is not supported on VMware vSphere 6.5.

Related information
Guest Operating System Installation Guide

Use VMware Enhanced vMotion Compatibility with Cisco UCS blade servers

Ensure Enhanced vMotion Compatibility (EVC) when upgrading Cisco UCS blade servers in a Converged System.

Do not mix 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, consider the following guidelines:

- Cisco B200 M1, M2, and B200 M3 UCS Blade Servers support 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, power off all VMs in the cluster. Then, enable or modify the EVC mode.
• Cisco UCS Blade Servers B200 M1 and M2 support some additional CPU features such as those features provided in 32-nanometer EVC mode. However, some 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. Selecting this mode enables vMotion compatibility between Cisco UCS Blade Servers B200 M1 and other hosts. Enable EVC mode only 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. Setting the EVC mode first eliminates the need to power off 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 the goal.

**Related information**

Enable EVC on an Existing Cluster

---

**Enable VMware Enhanced vMotion Compatibility within a cluster**

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 features 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 requirements. See EVC Requirements in the VMware vSphere ESXi and vCenter Server Documentation.

**Procedure**

1. You can optionally create an empty cluster. If you have already created a cluster, skip this step.

   Creating an empty cluster 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. Then enable EVC and migrate the VMs 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 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 VMs 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 Documentation
Manage the VMware vCenter HA Configuration (VMware vSphere 6.x)

VMware vCenter High Availability (HA) protects a VMware vCenter Server Appliance (vCSA) against host and hardware failures. The active-passive architecture of the solution can also help reduce downtime when patching a VMware vCSA.

After you configure your VMware vCenter HA cluster, you can perform management tasks. These tasks include certificate replacement, replacement of SSH keys, and SNMP setup. You can also edit the cluster configuration to disable or enable vCenter HA, enter maintenance mode, and delete the cluster configuration.

If your cluster contains fewer than four hosts, you can enable a witness/vCenter or vCenter/vCenter to migrate to the same host. Adjust the DRS rules during maintenance activities to enable this same-host migration. After maintenance activity is complete, reenable the DRS rules as soon as possible. Place all vCenter HA-related VMs back on separate hosts.

For more information, see the following references:

VMware vSphere 6.7
- Manage vCenter HA Configuration
- vCenter High Availability

VMware vSphere 6.5
- Manage the vCenter HA Configuration
- vCenter High Availability

Manage the VMware vCenter HA Configuration (VMware vSphere 6.5)

VMware vCenter High Availability (HA) protects a VMware vCenter Server Appliance (vCSA) against host and hardware failures. The active-passive architecture of the solution can also help reduce downtime when patching a VMware vCSA.

After you configure your VMware vCenter HA cluster, you can perform management tasks. These tasks include certificate replacement, replacement of SSH keys, and SNMP setup. You can also edit the cluster configuration to disable or enable vCenter HA, enter maintenance mode, and remove the cluster configuration.

If your cluster contains fewer than four hosts, you can enable a witness/vCenter or vCenter/vCenter to migrate to the same host. Adjust the DRS rules during maintenance activities to enable this same-host migration. After maintenance activity is complete, re-enable the DRS rules as soon as possible. Place all vCenter HA-related VMs back on separate hosts.

For more information, see the following references:
- Manage vCenter HA Configuration
- vCenter High Availability
Convert VMware Platform Service Controllers from external to embedded (VMware vSphere 6.7)

Convert external VMware Platform Service Controllers (PSCs) to embedded VMware PSCs. Use the convergence tool provided in VMware vSphere Server Appliance (vCSA) 6.7 update 1 or later installer ISO.

About this task

Internalize VMware PSCs to simplify your topology.

Before you begin

- Validate that all the VMware vSphere PSCs and VMware vSphere ESXi hosts are upgraded to VMware vSphere 6.7 Update 1 or later.
- Back up the external VMware PSC and the VMware vCenter Server.

For the VMware documentation related to this procedure, see Converging to an Embedded Platform Services Controller Node Using the Command-Line Utility.

Procedure

1. From the HTML5 Web client, log in to the VMware vCenter Server as administrator@vsphere.local and select Hosts and Clusters.
2. Right-click AMP Cluster Edit DRS, and change the DRS setting from Fully Automated to Manual on the AMP cluster.
3. Mount the VMware vCSA 6.7 update 1 or later Installer ISO on the Element Manager VM. Connect to the Element Manager using RDP and copy the DVD:/vcsa-converge-cli folder to desktop.
4. Browse to Desktop\vcsa-converge-cli\templates\converge, and open the converge.json file in Windows WordPad.
5. Edit converge.json, and update the VMware vSphere ESXi and VMware vSphere vCenter credentials.
   a. Replace text inside <> with the appropriate values.
   
   ![Note: Password fields left blank result in a prompt.](image)
   
   b. If the VMware PSC is joined to an AD domain, update the ad_domain_info. If not, delete the section from the file.
   
   c. Save the file.
6. From the command prompts, type: cd C:\Users\Administrator\Desktop\vcsa-converge-cli\win32.
7. To run vcsa-installer.exe, type: \vcsa-util.exe converge --verify-template-only C:\Users \Administrator\Desktop\vcsa-converge-cli\templates\converge\converge.json.
8. If validation is successful, run the same command again without the verify-template-only option. If the validation is unsuccessful, fix the errors in the .json file and run verify-template-only until it comes back successful.
9. When prompted with Did you back up the participating PSC and VC nodes?, type y and press Enter.
10. When prompted with Do you accept the thumbprint?, type 1 and press Enter.

   ![Note: VMware vCenter Server is inaccessible for 10 minutes after successful completion of the migration.](image)
11. To verify that the VMware vCenter Server has an embedded PSC, to log in to the management interface, type: https://<vCenter_FQDN_or_IP_address>:5480/.
12. Log in to the VMware vCenter Server using the HTML5 client.

13. Select Hosts and Clusters. Select the AMP cluster. Right click, and change the DRS setting back to Fully Automated.

Join Embedded Linked Mode domain (VMware vSphere 6.7)

To obtain additional information about Enhanced Linked Mode, see Joining a vCenter Embedded Linked Mode Domain.

Convert external VMware Platform Service Controllers to embedded (VMware vSphere 6.x)

Convert external VMware Platform Service Controllers (PSC) to embedded VMware PSCs.

About this task

Internalize VMware PSCs to simplify the topology.

Before you begin

- For VMware vSphere 6.7, use the convergence tool provided in VMware vSphere Server Appliance (vCSA) 6.7 update 1 or later installer ISO.
- For VMware vSphere 6.5, validate that all the VMware vSphere PSCs and VMware vSphere ESXi hosts are upgraded to VMware vSphere 6.5u2d or later.
- Back up the external VMware PSC and the VMware vCenter Server.

For the VMware documentation related to this procedure, see Converging to an Embedded Platform Services Controller Node Using the Command-Line Utility.

Procedure

1. If using VMware vSphere 6.7, perform the following:
   a. Log in to the VMware vCenter Server using the HTML5 Web Client as administrator@vsphere.local and select Hosts and Clusters.
   b. Right-click AMP Cluster Edit DRS and change the DRS setting from Fully Automated to Manual on the AMP cluster and click OK.
   c. Mount the VMware vCSA 6.7 update 1 or later Installer ISO on the Element Manager VM.
   d. Continue to step 3.

2. If using VMware vSphere 6.5, perform the following:
   a. Log in to the VMware vSphere Web Client as administrator@vsphere.local and select Hosts and Clusters.
   b. Right-click AMP Cluster > Settings, and click Edit under vSphere DRS.
   c. Change the DRS setting from Fully Automated to Manual on the AMP cluster and click OK.
   d. Mount the VMware vCSA 6.5 update 2d or later Installer ISO on the Element Manager VM.

3. Connect to the Element Manager using RDP and copy the DVD:/vcsa-converge-cli folder to the desktop.

4. Browse to Desktop\vcsa-converge-cli\templates\converge and open the converge.json file in WordPad.

5. Edit converge.json and update the VMware vSphere ESXi and VMware vSphere vCenter credentials.
   a. Replace text inside < > with the appropriate values.
      Password fields left blank result in a prompt.
b. If the VMware PSC is joined to an AD domain, update the ad_domain_info. If not, delete the section from the file.

c. Save the file.

6. From the command prompts to change the directory, type:

   \c:\users\administrator\desktop\vcsa- converge-cli\win32

7. To run vcsa-installer.exe, type:

   \vcsa-util.exe converge --verify-template-only C:\Users\Administrator\Desktop\vcsa-
   converge-cli\templates\converge\converge.json

8. If validation is successful, run the command again without the verify-template-only option. If the validation is unsuccessful, fix the errors in the json file and run the command with verify-template-only until the result is successful.

9. When prompted with Did you back up the participating PSC and VC nodes?, type y and press Enter.

10. When prompted with Do you accept the thumbprint?, type 1 and press Enter.

VMware vCenter Server is inaccessible for 10 minutes after successful completion of the migration.

11. To verify that the VMware vCenter Server has an embedded PSC, log in to the management interface:

    https://<vCenterFQDN_or_IPaddress>:5480/

12. Log in to the VMware vCenter Server using the Web client for VMware vSphere 6.5 or the HTML5 client for VMware vSphere 6.7.

13. Select Hosts and Clusters. Right-click the AMP cluster, and change the DRS setting back to Fully Automated.

Join Embedded Linked Mode domain (VMware vSphere 6.5)
To obtain additional information about Enhanced Linked Mode, see Joining a vCenter Embedded Linked Mode Domain.

Decommission external VMware Platform Service Controllers (VMware vSphere 6.x)
Decommission the external VMware Platform Service Controllers (PSCs) manually.

About this task
Decommission external VMware PSCs after internalizing the VMware PSC function into VMware vCHA.

Before you begin
- Validate that the external VMware PSC has converted to an embedded VMware PSC.
- Validate the VMware vCenter lookup service is using the internal VMware PSC.
  2. Select Access Enable SSH and BASH shell.
  3. Type: shell and press Enter.
  4. Log in to the VMware vCenter Server using the SSH client as root.
  5. Type: /usr/lib/vmware-vmafd/bin/vmafd-cli get-1s-location --server-name localhost
  6. To validate that the VMware vCenter Server uses an internal lookup service, type: https://<vCenter_FQDN>/lookupservice/sdk
Procedure
1. To power off the VMware PCSs and unregister the PSC, type: cmsso-util
2. Log in to the VMware vCenter Server using the SSH client with VMware vCenter management credentials.
3. To unregister the external VMware PSC, type:

   cmsso-util unregister --node-pnid <External_PSC_FQDN_or_IP_address> --username administrator@domain

4. To ensure that replication partners no longer exist, type: /usr/lib/vmware-vmdir/bin/vdcrepadmin -f showpartners -h <vcenter_FDQN_or_IP_address> -u administrator
5. Repeat steps 3 and 4 to delete the remaining external VMware PSCs.

Decommission external VMware Platform Service Controllers (VMware vSphere 6.5)
Decommission the external VMware Platform Service Controllers (PSCs) manually.

About this task
Decommission external VMware PSCs after internalizing the VMware PSC function into VMware vCHA.

Before you begin
- Validate that the external VMware PSC was converted to an embedded VMware PSC.
- Validate that the VMware vCenter lookup service is using the embedded VMware PSC.
  - Log in to VMware vCSA management interface:
  - Select Access Enable SSH and BASH shell.
  - Enter the following command:
    shell
  - Press Enter.
  - Log in to the VMware vCenter Server using the SSH client with root credentials.
  - Enter the following command:
    /usr/lib/vmware-vmafd/bin/vmafd-cli get-1s-location --server-name localhost
  - Validate that the VMware vCenter Server uses an internal lookup service by entering the following URL:
    https://<vCenter_FQDN>/lookupservice/sdk

Procedure
1. Turn off the VMware PCSs, and unregister the PSC.
2. Enter the following command:
   cmsso-util
3. Log in to the VMware vCenter Server using the SSH client with VMware vCenter management credentials.
4. To unregister the external VMware PSC, enter the following command: cmsso-util unregister --node-pnid <External_psc_FQDN_or_IP> --username administrator@domain
5. To ensure that replication partners no longer exist, enter the following command:

   /usr/lib/vmware-vmdir/bin/vdcrepadmin -f showpartners -h <vcenter FDQN or IP> -u administrator

6. Repeat steps 3 and 4 to delete the remaining external VMware PSCs.

**Configure the Virtual Flash Read Cache**

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 VM, and select **Edit Settings**.
3. In the **Virtual Hardware** tab, expand the VMDK that you want to configure with the VFRC.
4. In the **Virtual Flash Read Cache** field, type 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 VM and associated VMDK that requires VFRC.

   VMware vSphere does NOT prevent over provisioning. Consider the total available VFRC capacity when configuring the cache size.
Manage VMware VDS (VMware vSphere 6.5)

The section provides the most common procedures for managing an existing VMware vSphere Distributed Switch (VDS).

Managing licenses (VMware vSphere 6.5)

Use this procedure for an overview of how to manage VMware vSphere Distributed Switch (VDS) licenses.

About this task

The VMware VDS is an enterprise feature of VMware vSphere vCenter Server and requires that the VMware vSphere ESXi hosts are licensed with the VMware vSphere Enterprise Plus edition. A non-Enterprise Plus edition will not support VMware VDS functionality. No additional license is required to be installed or managed for the VMware VDS.

Provision a VMware VDS configuration (VMware vSphere 6.5)

Provision an existing VMware VDS configuration requires changes to the port group, VMKernel interface, VMware vSphere ESXi hosts, jumbo frames, and class of service settings.

Modifying an existing distributed port group (VMware vSphere 6.5)

From the VMware vSphere Web Client, modify distributed port group settings such as the name, VLAN ID, teaming and failover policy, traffic filtering, and marking policies. To ensure proper Converged System operation, do not change the standard configuration settings.

About this task

Using the VMware vSphere Web Client, only one distributed port group can be edited at a time. If several port groups require modification, use the VMware PowerCLI or vSphere vCLI command line/script tools.

Before you begin

Identify the VMware VDS containing the distributed ports. The default switch name that is used is DVSwitch01-A.

Procedure

1. To launch the VMware vSphere Web Client from VMware vCenter Server, open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client

   You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

   The alternative launch method does not apply to vSphere 6.5.

2. Log in to the VMware vSphere Web Client with the administrator@vsphere.local user account (Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Expand DVSwitch01-A and right-click the distributed port group to modify and click Edit Settings.

5. The following table shows recommended settings:
<table>
<thead>
<tr>
<th>Edit option</th>
<th>Field: recommended setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td>• Name: The name that is chosen for the distributed port group</td>
</tr>
<tr>
<td></td>
<td>• Port binding: Static Binding</td>
</tr>
<tr>
<td></td>
<td>• Port allocation: Elastic</td>
</tr>
<tr>
<td></td>
<td>• <strong>Number of ports:</strong> 8 (increases automatically when Elastic is selected for port allocation)</td>
</tr>
<tr>
<td></td>
<td>• Network resource pool: Use the default setting.</td>
</tr>
<tr>
<td></td>
<td>• Description: Add details about distributed port groups.</td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td>• Configure reset at disconnect: Enabled</td>
</tr>
<tr>
<td></td>
<td>• Override port policies: Use default setting.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>• Promiscuous mode: Reject</td>
</tr>
<tr>
<td></td>
<td>• MAC address changes: Reject</td>
</tr>
<tr>
<td></td>
<td>• Forged transmit: Reject</td>
</tr>
<tr>
<td><strong>Traffic shaping</strong></td>
<td>• Ingress traffic shaping: Disabled</td>
</tr>
<tr>
<td></td>
<td>• Egress traffic shaping: Disabled</td>
</tr>
<tr>
<td><strong>VLAN</strong></td>
<td>• VLAN type: VLAN</td>
</tr>
<tr>
<td></td>
<td>• VLAN ID: See the Logical Configuration Survey.</td>
</tr>
<tr>
<td><strong>Teaming and failover</strong></td>
<td>• Load balancing: Route based on physical NIC load The vMotion port group only has one active uplink (associated with vNIC2 fabric A). The other uplink should be in standby mode.</td>
</tr>
<tr>
<td></td>
<td>• Network failure detection: Link status only</td>
</tr>
<tr>
<td></td>
<td>• Notify switches: Yes</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td>• Failback: Yes</td>
</tr>
<tr>
<td></td>
<td>• Netflow: default</td>
</tr>
<tr>
<td>Edit option</td>
<td>Field: recommended setting</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Traffic filtering and marking</td>
<td>• Status: Enable this option for vMotion NFS distributed port groups. All other port groups should be disabled.</td>
</tr>
<tr>
<td></td>
<td>• vMotion Traffic Rule Enabled - use the + sign to make edits</td>
</tr>
<tr>
<td></td>
<td>▪ Action tag</td>
</tr>
<tr>
<td></td>
<td>▪ COS value checkbox is selected.</td>
</tr>
<tr>
<td></td>
<td>▪ Set CoS to 4</td>
</tr>
<tr>
<td></td>
<td>▪ Set traffic direction to <strong>Ingress</strong> for VMware vSphere 6.x.</td>
</tr>
<tr>
<td></td>
<td>© <strong>Note:</strong> See the VMware vSphere 6.x Release Notes for information about ingress and egress parameters.</td>
</tr>
<tr>
<td></td>
<td>▪ Type <strong>System Traffic</strong> and set Protocol/Traffic Type to <strong>vMotion</strong>.</td>
</tr>
<tr>
<td></td>
<td>• NFS Traffic Rule Enabled - use the + sign to make edits</td>
</tr>
<tr>
<td></td>
<td>▪ Action tag</td>
</tr>
<tr>
<td></td>
<td>▪ COS value checkbox is selected.</td>
</tr>
<tr>
<td></td>
<td>▪ Set CoS to 2</td>
</tr>
<tr>
<td></td>
<td>▪ Set traffic direction to <strong>Ingress</strong> for VMware vSphere 6.x.</td>
</tr>
<tr>
<td></td>
<td>© <strong>Note:</strong> Refer to the VMware vSphere 6.x Release Notes for information about ingress and egress parameters.</td>
</tr>
<tr>
<td></td>
<td>▪ Type <strong>IP</strong> and set Protocol/Traffic Type to <strong>Any</strong>.</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Block all ports: No</td>
</tr>
</tbody>
</table>

**Creating a distributed port group (VMware vSphere 6.5)**

You can use the VMware vSphere Web Client to create and add virtual and VMKernel distributed port groups to an existing VMware VDS. After you create a distributed port group, you must configure the port group.

**Procedure**

1. To launch the VMware vSphere Web Client from the VMware vCenter Server, open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client.
   © **Note:** You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.
   The alternative launch method does not apply to vSphere 6.5.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Right-click DVSswitch01-A and select New Distribution Port Group.

5. From the New Distributed Port Group wizard, to create the distributed port group, perform the following:
   a. Type the name of the distributed port group and click Next.
   b. Leave Port binding and Port allocation to the default settings Static binding and Elastic.
   c. Leave the Number of Ports to the default setting of eight.
   d. Set the VLAN type to VLAN and change the VLAN ID.
e. Verify that **Customize default policies configuration** is cleared.

f. Click **Next**.

g. Review and verify the settings for the new distributed port group and click **Finish**.

Virtual distributed port groups can be assigned to the VMs. VMKernel distributed port groups require configuration.

**After you finish**

As an option, assign VMKernel distributed port groups to the VMware vSphere ESXi hosts.

### Configure a VMKernel interface (VMware vSphere 6.5)

Configure a VMKernel (vMotion or NFS) interface using the **Add and Manage Host** wizard.

**About this task**

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

**Before you begin**

Create a VMkernel distributed port group.

**Note**: IPv6 is not supported on vSphere 6.5.

**Procedure**

1. From the **VMware vSphere Web Client Home** tab, under **Inventories**, select **Networking**.

2. Right-click **DVSwitch01-A** and select **Add and Manage Hosts**.

3. From the **Add and Manage Hosts** wizard, perform the following:

   a. Select **Manage host networking** and select **Next**.

   b. Select **Attach hosts**.

   c. From the **Select member hosts** window, select the VMware vSphere ESXi host, and click **OK**.

   d. Verify that the selected host(s) have been added to the list and click **Next**.

   e. From the **Select network adapter tasks** window, deselect **Manage physical adapters** and verify that **Manage VMKernel adapters** is selected.

   f. Click **Next**.

   g. Select the VMware vSphere ESXi host and click **New adapter**.

   h. From the **Add Networking** window, verify that **Select an existing Distributed Port Group** is selected and click **Browse**.

   i. Select VMKernel (vMotion or NFS) distributed port group and click **OK**.

   j. Click **Next**.

   k. For the vMotion distributed port group only, select **vMotion traffic** and click **Next**.

   l. For the NFS distributed port group only, verify that **Enable services** is unchecked and click **Next**.

   m. Select **Use static IPv4/IPv6 settings**, apply IPv4 or IPv6 address/Subnet Mask, and click **Next**.

   **Note**: Dual IP stack is not supported.

   n. When the **Analyze impact** window appears, click **Next**.

   o. From the **Ready to complete** window, validate the settings and click **Finish**.
p. Select the new VMkernel.
q. Select Edit adapter.
r. Select NIC settings.
s. Verify that the MTU setting is set to 1500 (NFS MTU=9000).
t. Click OK and Finish.
u. Repeat steps g through s for each additional VMware vSphere ESXi host to create a new network adapter.
v. Click Next.
w. Verify that the No Impact message appears and click Next.
x. Review and verify the Summary results and click Finish.

Associating VMware vSphere ESXi hosts to an existing VMware VDS

Associating a new VMware vSphere ESXi host to an existing VMware VDS requires adding the VMNICs to the VMware VDS uplinks. From the Add and Manage Hosts wizard, you can associate the VMware vSphere ESXi hosts to the VMware VDS.

Before you begin

Verify which VMware VDS the VMware vSphere ESXi host will add.

Procedure

1. To launch the VMware vSphere Web Client from VMware vCenter Server, open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client

   ![Note:](image) You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

   The alternative launch method above does not apply to vSphere 6.5.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (SSO account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Right-click DVSwitch01-A and select Add and Manage Hosts.

5. From the Add and Manage Hosts wizard, perform the following:
   a. Select Add Hosts and click Next.
   b. Select New Hosts.
   c. From the Select new hosts window, select the VMware vSphere ESXi host to be added and click OK.

   ![Note:](image) You can modify multiple VMware vSphere ESXi hosts at a time using the Add and Manage Hosts wizard.

   The alternative launch method above does not apply to vSphere 6.5.

d. Validate the selected host appears in the list and click Next.

e. From the Select network adapter tasks window, deselect Manage VMKernel adapters.

f. Verify that Manage physical adapters is selected and click Next.

g. Select vmnic2 and click Assign uplink.
h. Select Uplink 1 and click OK.

i. Select vmnic3 and click Assign uplink.

j. Select Uplink 2 and click OK.

k. Click Next.

l. Verify that the status message displays no impact and click Next.

6. Review the Summary results and click Finish.

Configuring jumbo frames on VMware VDS

Use this procedure to configure jumbo frames on an existing VMware vSphere Distributed Switch (VDS).

Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client

   Note: You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

   The alternative launch method above does not apply to vSphere 6.5.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Right-click DVSwitch01-A and select Edit Settings.

5. On the Properties tab, select Advanced.

6. Change the MTU value from 1500 to 9000.

7. Click OK.

Configuring jumbo frames on distributed port groups

Use this procedure to configure jumbo frames on the NFS distributed port group.

Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client

   Note: You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

   The alternative launch method above does not apply to vSphere 6.5.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere Single Sign-On (SSO) account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, select Hosts and Clusters.

4. Select the first host.

   Note: Each NFS distributed port group must be modified for each VMware vSphere ESXi host.

5. Under Manage, select Networking, and then select VMKernel adapters.

6. From the table, select the adapter with the vcesys_esx_nfs listed under the network label.

7. Click the edit icon to select NIC settings and change the MTU value from 1500 to 9000.

8. Click OK.
9. Repeat this procedure for each VMware vSphere ESXi host as needed.

Modifying CoS settings

The CoS marking is leveraged as part of the standard configuration and configured with the Traffic Filtering and marking policy on VMware VDS.

Procedure

1. Launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client or open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client. (The Start Menu method does not apply to vSphere 6.5.)
2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware SSO account) or other administrative account with appropriate permissions.
3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.
4. Expand the DVswitch01-A to view all port groups.
5. Right-click vcesys_esx_vmotion distributed port group and click Edit settings.
7. From the Status drop-down box, select Enable.
8. Select the green plus (+) icon to open the New Network Traffic Rule wizard, and perform the following:
   a. For the Name, type: vMotionCOS.
   b. For Action, select Tag.
   c. Change the CoS value to 4.
   d. For VMware vSphere 6.x, change the Traffic direction to Ingress. The VMware vSphere 6.x Release Notes contain information about ingress and egress parameters.
   e. Select the green plus (+) and select New System Traffic Qualifier.
   f. Verify that the type is set System traffic and the Protocol/Traffic type is set to vMotion.
   g. Click OK.
9. Right-click the vcesys_esx_nfs distributed port group, click Edit settings.
10. From the wizard, perform the following:
    a. For the Name, type: NFSCOS
    b. For Action, select Tag.
    c. Check Update CoS tag, and change value to 2.
    d. For VMware vSphere 6.x, change the Traffic direction to Ingress. The VMware vSphere 6.x Release Notes contain information about ingress and egress parameters.
    e. Select the green plus (+) and select New IP Qualifier.
    f. From the Protocol drop-down, select Any.
    g. Leave the Type as IP and click OK.
Decommissioning VMware VDS components

Decommissioning VMware VDS components requires deleting distributed port groups, disassociating the VMware vSphere ESXi hosts, and remove the VMware VDS.

Deleting a distributed port group

Delete a distributed port group from an existing VMware VDS.

- Before deleting a distributed port group, reassign all powered-on VMs to a different distributed port group. If the VMs are powered off, delete the distributed port group.
  
  **Note:** If you delete a distributed port group with powered-on VMs and network adapter numbers assigned to the distributed port group, the system returns an error.

- Migrate the VMKernel ports from the VMware vSphere ESXi host attached to the VMware VDS.

Migrating VM distributed port group assignments to a different switch

If there are powered-on VMs on the distributed port group, migrate VM distributed port group assignments to a different distributed or standard switch.

About this task

This procedure is not required if there are no powered-on VMs on the distributed port group. VMs connected to the distributed port group can be powered-off to remove the distributed port group.

Use the VM migration wizard to migrate any port group types. However, use caution when migrating the VMware vCenter Server VMs, because a disconnect can cause the loss of the VMware vCenter Server, which could prevent the VM port group from migrating.

Use the VM migration wizard to migrate from a VMware vSphere Standard Switch to a VMware VDS, a VMware VDS to a VMware vSphere Standard Switch, or a VMware VDS to a VMware VDS seamlessly.

Before you begin

Verify the powered-on VMs on all VMware vSphere ESXi hosts attached to an existing VMware VDS are not assigned to any distributed port groups.

Verify there is an available distributed port group to which to migrate the powered-on VMs.

Create another switch with the following criteria:

- If migrating to a different VMware VDS:
  
  - Attach at least one VMNIC as an uplink for a new distributed or standard switch.
  
  - Create the distributed port groups with the same name and VLAN ID as the existing switch.

- If migrating to a standard switch:
  
  - Create a new standard switch and attach at least one VMNIC as an uplink for the standard switch.
  
  - vNIC0 and vNIC1 connect to a different set of physical switches than vNIC2 and vNIC3. Do not add vNIC2 and/or vNIC3 to vSwitch0, because it could cause the VMware vSphere ESXi host to lose network connectivity if management traffic gets switched.
  
  - If no VMNICs are available, migrate one VMNIC from the VMware VDS. Keep the second VMNIC on the Distributed Switch for VM traffic to continue to communicate
  
  - Create the VM port group with correct VLAN ID to the new standard switch.

Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client
You can also launch the VMware vSphere Web Client by selecting **Start Menu > All Programs > VMware > VMware vSphere Web Client**.

The alternative launch method above does not apply to vSphere 6.5.

2. Log on to the VMware vSphere Web Client with the **administrator@vsphere.local** user account (VMware vSphere SSO account) or other administrative account with appropriate permissions.

3. On the **VMware vSphere Web Client Home** tab, under **Inventories**, click **Networking**.

4. Right-click **DVswitch01-A** and select **Migrate VM to Another Network**.

5. From the **Migrate Virtual Machine Networking** wizard, perform the following:
   a. Verify that **Specific network** is selected and click **Browse**.
   b. Select the **Source network** distributed port group or standard port group and click **OK**.
   c. Select **Browse** for the destination network.
   d. Select the distributed port group or port group where the VMs will be reassigned and click **Ok**.
   e. Click **Next**.
   f. When the list of VMs appear, select the checkbox on each VM, and click **Next**.
   g. Validate that the source and destination is correct and click **Finish**.

   The selected VMs distributed port groups migrate to a new distributed or standard switch.

**Deleting the distributed port group from the VMware VDS**

If there are no powered on VMs on the distributed port group, delete the distributed port group from the existing VMware VDS.

**Before you begin**

Verify there is no port assignment connected to any of the distributed port group on any of the VMs.

**Procedure**

1. Launch the VMware vSphere Web Client by selecting **Start Menu > All Programs > VMware > VMware vSphere Web Client** or open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client (The **Start Menu** method does not apply to vSphere 6.5.)

2. Log on to the VMware vSphere Web Client with the **administrator@vsphere.local** user account (VMware vSphere SSO account) or other administrative account with appropriate permissions.

3. On the **VMware vSphere Web Client Home** tab, under **Inventories**, click **Networking**.

4. Select the drop-down **Array** on **DVswitch01-A** to list the distributed port groups.

5. Right-click the distributed port group and select **All vCenter Action > Remove from Inventory** and click **OK**.

**Disassociating the VMware vSphere ESXi host**

Disassociate the VMware vSphere ESXi host from an existing VMware VDS.

**Before you begin**

- Reassign all the VMs to a port group on a different distributed switch or standard switch. Otherwise, an error occurs when you attempt to delete the VMware vSphere ESXi host from the VMware VDS.
- Migrate all VMKernel ports to a different distributed switch or standard switch.
- Distributed port groups and uplink adapters do not need to be removed.

VMs network adapters assigned to a distributed port group will force an error when attempted to delete the ESXi host from the VMware VDS. All the VMs are assigned to the distributed port group need to be reassigned to a port group on
a different distributed or standard switch. The VMware VDS that is being removed must have all the VMKernel ports either migrated to a different standard Switch or VMware VDS or be removed.

After reviewing the prerequisites, perform the following procedures:

1. vMotion/evacuate all powered on VMs from the VMware vSphere ESXi host
2. Migrate VM distributed port group assignments
3. Migrate the VMkernel ports to a different switch

vMotion/evacuating all powered-on VMs from the VMware vSphere ESXi host

Evacuate/vMotion all powered-on VMs to a different VMware vSphere ESXi host to free up the ports on the VMware VDS. VMs can still point to the same distributed port groups from a different VMware vSphere ESXi host, because there are no assigned VMs on the host.

About this task

This procedure requires using the migration VM network wizard that migrates all the VMs port assignments to a different switch with no downtime. If this option is not possible due to the number of VMs or a shortage of system resource capacity, see Migrating powered-on VMs distributed port group assignments to a different switch.

Before you begin

Ensure sufficient system capacity exists on other VMware vSphere ESXi hosts to migrate all the powered-on VMs.

Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client
   
   You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.
   
   The alternative launch method above does not apply to vSphere 6.5.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere SSO account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, select Hosts and Clusters.

4. From the left window, select the appropriate VMware vSphere ESXi host and select the Related Objects tab.

5. From the right window, click Virtual Machines. Using the CTRL key, select all of the VMs.

6. Select Actions > Migrate to open the migration wizard.

7. Verify that Change host is selected and click Next.

8. Select the destination resource (cluster or VMware vSphere ESXi host) to migrate the VMs and click Next.

9. Verify that Resource CPU for optimal vMotion performance (Recommended) is selected and click Next.

10. Review the summary window and click Finish.

   The VMs migrate to a different VMware vSphere ESXi host. If the cluster was chosen as the destination with DRS enabled, VMware vCenter automatically places the VMs with a different VMware vSphere ESXi host.

11. Put the host in maintenance mode to prevent DRS from vMotioning the VMs back to the host.

Migrating VM distributed port group assignments to a different switch

If there are powered-on VMs on the distributed port group, migrate VM distributed port group assignments to a different distributed or standard switch.

About this task

This procedure is not required if there are no powered-on VMs on the distributed port group. VMs connected to the distributed port group can be powered-off to remove the distributed port group.
Use the VM migration wizard to migrate any port group types. However, use caution when migrating the VMware vCenter Server VMs, because a disconnect can cause the loss of the VMware vCenter Server, which could prevent the VM port group from migrating.

Use the VM migration wizard to migrate from a VMware vSphere Standard Switch to a VMware VDS, a VMware VDS to a VMware vSphere Standard Switch, or a VMware VDS to a VMware VDS seamlessly.

**Before you begin**

Verify the powered-on VMs on all VMware vSphere ESXi hosts attached to an existing VMware VDS are not assigned to any distributed port groups.

Verify there is an available distributed port group to which to migrate the powered-on VMs.

Create another switch with the following criteria:

- If migrating to a different VMware VDS:
  - Attach at least one VMNIC as an uplink for a new distributed or standard switch.
  - Create the distributed port groups with the same name and VLAN ID as the existing switch.

- If migrating to a standard switch:
  - Create a new standard switch and attach at least one VMNIC as an uplink for the standard switch.
  - vNIC0 and vNIC1 connect to a different set of physical switches than vNIC2 and vNIC3. Do not add vNIC2 and/or vNIC3 to vSwitch0, because it could cause the VMware vSphere ESXi host to lose network connectivity if management traffic gets switched.
  - If no VMNICs are available, migrate one VMNIC from the VMware VDS. Keep the second VMNIC on the Distributed Switch for VM traffic to continue to communicate
  - Create the VM port group with correct VLAN ID to the new standard switch.

**Procedure**

1. Open a browser and type the following URL: `https://<vCenterIP>:9443/vsphere-client`

   You can also launch the VMware vSphere Web Client by selecting **Start Menu > All Programs > VMware > VMware vSphere Web Client**.

   The alternative launch method above does not apply to vSphere 6.5.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere SSO account) or other administrative account with appropriate permissions.

3. On the **VMware vSphere Web Client Home** tab, under **Inventories**, click **Networking**.

4. Right-click **DVswitch01-A** and select **Migrate VM to Another Network**.

5. From the **Migrate Virtual Machine Networking** wizard, perform the following:
   - Verify that **Specific network** is selected and click **Browse**.
   - Select the **Source network** distributed port group or standard port group and click **OK**.
   - Select **Browse** for the destination network.
   - Select the distributed port group or port group where the VMs will be reassigned and click **Ok**.
   - Click **Next**.
   - When the list of VMs appear, select the checkbox on each VM, and click **Next**.
   - Validate that the source and destination is correct and click **Finish**.

The selected VMs distributed port groups migrate to a new distributed or standard switch.
Migrating the VMKernel ports to a different switch

Migrate the VMKernel ports to a different distributed or standard switch.

Before you begin

Do not associate the VMware vSphere ESXi host with VMKernel ports to the VMware VDS. Create another distributed or standard switch to migrate the VMKernel ports.

The standard or distributed switch must have the minimum support criteria:

- Attach at least one VMNIC to an uplink port for a new distributed or standard switch
- Create the distributed port group with the same name and VLAN ID of what is created in the existing distributed or standard switch
- If a VMware VDS is created, add the VMware vSphere ESXi host to it so that the VMKernel port can be migrated between the two distributed switches. This does not apply for a standard switch

Note: VMKernel ports can be deleted from the VMware vSphere ESXi host if a VMNIC is not available to use for an uplink on the new distributed or standard switch.

Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client
   - You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.
   - The alternative launch method does not apply to vSphere 6.5.
2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere SSO account) or other administrative account with appropriate permissions.
3. On the VMware vSphere Web Client Home tab, under Inventories, select Hosts and Clusters.
4. Left-click ESXi host and select the Manage or Configure tab.
5. Left-click Networking and select Virtual switches.
6. Left-click the distributed or standard switch to which the VMKernel adaptor will be migrated.
7. Left-click Migrate a VMKernel network adaptor to selected switch.
8. From the Migrate VMKernel Network Adapter wizard, perform the following:
   a. Select vcesys_esx_vmotion and click Next.
   b. Change the Network label to vcesys_esx_vmotion.
   c. Change the VLAN ID to 117 and click Next.
   d. Verify that the No Impact status appears and then click Next.
   e. Verify Ready to complete pages for correct results and click Finish.
   f. Wait 60 seconds and then select the VMKernel adapter link under Networking to ensure that the vcesys_esx_vmotion adapter is on the new switch.
   g. Repeat this step for each VMKernel network adapter.

Disassociate the VMware vSphere ESXi host from a VMware VDS

Disassociate the VMware vSphere ESXi host from an existing VMware VDS.

Before you begin

Verify that there are no VMs, vNIC uplinks, and VMKernel ports attached to the existing VMware VDS coming from each VMware vSphere ESXi host.
Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client.
   You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.
   The alternative launch method does not apply to vSphere 6.5.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (SSO account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Right-click DVSwitch01-A and select Add and Manage Hosts.

5. From the Add and Manage Hosts wizard, perform the following:
   a. Select Remove hosts and click Next.
   b. Select Attached hosts.
   c. From the Select member hosts window, select the VMware vSphere ESXi host that you want to delete and click OK.

   **Note:** You can modify multiple VMware vSphere ESXi hosts at a time using the Add and Manage Hosts wizard.

d. Verify that the selected host is in the list and click Next.

e. Review the summary results window and click Finish.

Removing a VMware VDS

Required procedures are provided for removing a VMware VDS.

**Before you begin**

- Uplink adapters and VMware vSphere ESXi hosts do not need to be removed to delete the VMware VDS.
- Powered on VMs cannot be attached to any distributed port groups. No VMs are permitted on any VMware vSphere ESXi host connect to the VMware VDS and attached to the distributed port groups.

Perform the following procedures:

1. Migrate VM distributed port group assignments to a different switch.
2. Migrate VMKernel ports to a different switch.

**Migrating VM distributed port group assignments to a different switch**

If there are powered-on VMs on the distributed port group, migrate VM distributed port group assignments to a different distributed or standard switch.

**About this task**

This procedure is not required if there are no powered-on VMs on the distributed port group. VMs connected to the distributed port group can be powered-off to remove the distributed port group.

Use the VM migration wizard to migrate any port group types. However, use caution when migrating the VMware vCenter Server VMs, because a disconnect can cause the loss of the VMware vCenter Server, which could prevent the VM port group from migrating.

Use the VM migration wizard to migrate from a VMware vSphere Standard Switch to a VMware VDS, a VMware VDS to a VMware vSphere Standard Switch, or a VMware VDS to a VMware VDS seamlessly.
Before you begin
Verify the powered-on VMs on all VMware vSphere ESXi hosts attached to an existing VMware VDS are not assigned to any distributed port groups.
Verify there is an available distributed port group to which to migrate the powered-on VMs.
Create another switch with the following criteria:
- If migrating to a different VMware VDS:
  - Attach at least one VMNIC as an uplink for a new distributed or standard switch.
  - Create the distributed port groups with the same name and VLAN ID as the existing switch.
- If migrating to a standard switch:
  - Create a new standard switch and attach at least one VMNIC as an uplink for the standard switch.
  - vNIC0 and vNIC1 connect to a different set of physical switches than vNIC2 and vNIC3. Do not add vNIC2 and/or vNIC3 to vSwitch0, because it could cause the VMware vSphere ESXi host to lose network connectivity if management traffic gets switched.
  - If no VMNICs are available, migrate one VMNIC from the VMware VDS. Keep the second VMNIC on the Distributed Switch for VM traffic to continue to communicate
  - Create the VM port group with correct VLAN ID to the new standard switch.

Procedure
1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client
   You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.
   The alternative launch method above does not apply to vSphere 6.5.
2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere SSO account) or other administrative account with appropriate permissions.
3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.
4. Right-click DVSwitch01-A and select Migrate VM to Another Network.
5. From the Migrate Virtual Machine Networking wizard, perform the following:
   a. Verify that Specific network is selected and click Browse.
   b. Select the Source network distributed port group or standard port group and click OK.
   c. Select Browse for the destination network.
   d. Select the distributed port group or port group where the VMs will be reassigned and click Ok.
   e. Click Next.
   f. When the list of VMs appear, select the checkbox on each VM, and click Next.
   g. Validate that the source and destination is correct and click Finish.
   - The selected VMs distributed port groups migrate to a new distributed or standard switch.

Removing VMKernel ports
Remove VMKernel ports after the VMs have been migrated from the VMware VDS.

Before you begin
Verify that all VMs have been migrated off the VMware VDS.
Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client
   You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.
   The alternative launch method above does not apply to vSphere 6.5.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere SSO account) or another administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Right-click DVswitch01-A and select Add and Manage Hosts.

5. From the Add and Manage Hosts wizard, perform the following:
   a. Select Manage host networking and click Next.
   b. Click Attach hosts.
   c. From the Select member hosts window, select the VMware vSphere ESXi hosts and click OK.
   d. Verify that the selected host has been added and click Next.
   e. From the Select network adapter tasks window, deselect Manage physical adapters so that only Manage VMKernel adapters is selected and click Next.
   f. Under On this switch, select the VMKernel port by selecting the VMKernel adapter and click Assign port group.
   g. If you need to delete VMKernel ports, under the VMKernel adapter list, select the VMKernel port and click Remove.
   h. Select the port group that belongs to a different vSwitch and click OK.
   i. Validate the VMKernel port destination and click Next.
   j. Verify that a No impact message appears and click Next.
   k. Review the summary results and click Finish.

Using Disjoint Layer 2 configuration on VMware VDS

Configure Disjoint Layer 2 on VMware VDS. Disjoint Layer 2 is not mandatory for VMware VDS.

About this task
Assign the following to the VMware VDS:

- Cisco UCS vNIC 4 (10 GB or more depending on VIC hardware)
- Cisco UCS vNIC 5 (10 GB or more depending on VIC hardware)

A separate VMware VDS is created with two dedicated uplinks to isolate Disjoint Layer 2 traffic from all other primary VDS traffic. There must be a single VMware VDS created for each data center, but not for each cluster.

Creating a VMware VDS for Disjoint Layer 2 configuration

Create a VMware VDS for Disjoint Layer 2 configuration.

About this task
On full-width blades with additional network physical ports to the onboard mLOM ports, add vNICs 4 and 5 to the service profile. This must be done individually between reboots, after installing VMware vSphere ESXi with vNIC 0-3. This is required because of the way VMware vSphere ESXi interprets the Cisco PCI bus enumeration of the vNICs.
during installation. VMware does not support remapping the vNICs after the hypervisor is installed without a support ticket.

Procedure

1. From the VMware vSphere Web Client Home tab, under Inventories, select Networking.

2. Right-click Datacenter01 (Logical Configuration Survey (LCS) default name) and select New Distributed Switch.

   ✷ Note: The disjoint layer 2 Cisco DVswitch naming scheme is as follows: DVswitch<Converged System ID>-DJL2

3. From the New Distributed Switch wizard, perform the following:
   a. Change the name of the distributed switch to DVswitch01-DJL2 unless a different cluster name is used in the LCS.
   b. Validate that the cluster location is Cluster01.
   c. Click Next.
   d. Select the appropriate Distributed switch.
   e. Click Next.
   f. From the Edit Settings window, change Number of uplinks to 2.
   g. Leave Network I/O Control enabled.
   h. Uncheck Default port group
      i. Click Next to view the Ready to complete window.
      j. Review the settings and click Finish if everything is correct. Otherwise, click Back to edit changes.

4. Repeat this procedure to create a new VMware VDS for each additional workload type.

After you finish

Creating distributed port groups for Disjoint Layer 2 configuration

Creating distributed port groups for Disjoint Layer 2

Create distributed port groups for Disjoint Layer 2.

About this task

Change the load balancing policy from Route based on originating virtual port to Route based on physical NIC load for all the VMKernel distributed port groups. Disjoint Layer 2 traffic is commonly used for virtual distributed port groups only, so it would typically be configured with the default settings.

If vcesys_esx_vmotion is configured as Disjoint Layer 2, configure teaming and failover with VMNIC4 in active state and VMNIC5 in standby state.

Procedure

1. From the VMware vSphere Web Client Home tab, under Inventories, select Networking.

2. Right-click DVswitch01-DJL2 (LCS default name) and select New Distribution Port Group.

3. From the New Distributed Port Group wizard, perform the following:
   a. Change the name of the distributed port group as provided in the Logical Configuration Survey (LCS).
   b. Click Next to configure port group settings.
   c. Under Configure Settings, leave Port binding and Port allocation as default.
d. Leave Number of Ports at 8.

e. For VLAN type, select VLAN and change the VLAN ID to what was specified in the LCS.

f. Click Next to view the Ready to complete window.

g. Review the settings and click Finish if everything is correct. Otherwise, click Back to edit changes.

4. Repeat this procedure for each distributed port group that belongs to the Disjoint Layer 2 configuration for the VMware VDS.

After you finish

Adding the VMware vSphere ESXi hosts to the VMware VDS

Add VMware vSphere ESXi hosts to VMware VDS

Add VMware vSphere ESXi hosts and attach a pair of VMNICs as uplinks to the Disjoint Layer 2 VMware VDS.

About this task

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Before you begin

IPv6 is not supported in VMware vSphere 6.5.

Procedure

1. From the VMware vSphere Web Client Home tab, under Inventories, select Networking.

2. Right-click DVswitch01-DJL2 and select Add and Manage Hosts.

3. From the Add and Manage Hosts wizard, perform the following:

a. Select Add Hosts and click Next.

b. Click (+) New Hosts.

c. Select the VMware vSphere ESXi host for VMware VDS and click OK.

d. Validate that the selected host appears and then click Next.

e. From the Select network adapter tasks window, verify that Manage physical adapters and Manage VMKernel adapters are checked and click Next.

f. Select vmnic4 and click Assign uplink.

g. Select Uplink 3 and click OK.

h. Select vmnic5 and click Assign uplink.

i. Select Uplink 4 and click OK.

j. Click Next.

k. Click Next to view the Ready to complete window.

l. Review the settings and click Finish if everything is correct. Otherwise, click Back to edit changes.

4. Add the VMkernel distributed port groups (vMotion, NFS) only if they belong to the Disjoint Layer 2 traffic. Otherwise, click Next and go to step 5.

a. From the Manage VMKernel network adapters window, verify that the host is selected and click (+) New adapter.

b. From the Add Networking wizard, select a distributed port group and click Browse.

c. Select vcesys_esx_vmotion and click OK.
d. Click Next.

e. Check vMotion traffic and click Next.

f. Select Use static IPv4 or IPv6 settings and apply IP address/Subnet Mask as specified in the LCS.

g. Click Next to view the Ready to complete window.

h. Review the settings and click Finish if everything is correct. Otherwise, click Back to edit changes.

i. Repeat this step to create the vcesys_esx_nfs port group. Do not select any checkboxes. The vcesys_esx_nfs port group has a default MTU of 1500. The MTU must be set to 9000.

j. Click Next.

5. Verify that the status displays as: No Impact and click Next. If there is a problem with the output, click Back to return to the previous window.

6. Review the summary results and click Finish.

7. Repeat this procedure for the remaining VMware vSphere ESXi hosts.

Backing up and restoring a VMware VDS data configuration

When you export a backup of the DVswitch configurations, a zip file is created. The import feature will not overwrite the existing dvSwitch(s) and instead create a separate one. The restore feature will overwrite the existing dvSwitch currently in use. Each feature is broken out by administrative procedures.

Exporting a backup of a VMware VDS configuration

Export the configuration of the VMware VDS configuration into a zip file.

About this task
The VMware dvSwitch configuration includes all the VMware VDS and distributed port group's configuration settings.

Before you begin
Verify that the VMware VDS is configured.

Procedure
1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client

   You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.

   The alternative launch method above does not apply to vSphere 6.5.

2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere SSO account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.

4. Right-click DVSwitch01-A and select All vCenter Action > Export Configuration.

5. Choose one of the following:
   - Distributed switch configuration and all port groups
   - Distributed switch only

6. In the Descriptions field, type DVSwitch01-A and click OK.

7. Click Yes to save the configuration file.
Importing a backup of a VMware VDS configuration

Create a VMware VDS from an exported configuration file using the same switch and distributed port group configuration. This does not override the existing VMware VDS.

Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client
   You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.
   The alternative launch method does not apply to vSphere 6.5.
2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware SSO account) or another administrative account with appropriate permissions.
3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.
4. Right-click Datacenter and select All vCenter Actions > Import Distributed Switch.
5. Click Browse to select Select a distributed switch backup file.
6. Select Preserve original distributed switch and port group identifiers.
7. Click Next.
8. Review the import settings and click Finish.

Restoring a backup of a VMware VDS configuration

Reset the configuration of an existing VMware VDS to the settings in the configuration file.

About this task

Restoring a VMware VDS changes the settings on the selected switch back to the settings saved in the configuration file. Restoring a backup of the VMware VDS configuration resets the existing VMware VDS configuration to the settings in the configuration file and destroy the existing VMware VDS.

Procedure

1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client
   You can also launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client.
   The alternative launch method above does not apply to vSphere 6.5.
2. Log on to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere SSO account) or other administrative account with appropriate permissions.
3. On the VMware vSphere Web Client Home tab, under Inventories, click Networking.
4. Right-click the VMware VDS to be restored and select All vCenter Actions > Restore Configuration.
5. Select Restore distributed switch or port groups or Restore distributed switch only.
6. Click Browse to select Select a distributed switch backup file and click Next.
7. Review the import settings and click Finish.

Managing VMware VDS (VMware vSphere 6.5)

The VMware VDS is an enterprise feature of VMware vSphere vCenter Server and requires that the VMware vSphere ESXi hosts are licensed with the VMware vSphere Enterprise Plus edition. A non-Enterprise Plus edition does not
support VMware vSphere Distributed Switch (VDS) functionality. No additional license is required to be installed or managed for the VMware VDS.

**VMware VDS basic troubleshooting**

The *VMware vSphere Networking Guide* contains procedures that can be used to troubleshoot a VMware VDS. For network health check, refer to *View vSphere Distributed Switch Health Check.*

For managing network rollback, refer to the following procedures:

- **vSphere Networking Rollback**
- **Disable Rollback**

For managing network recovery, refer to *Resolve Errors in the Management Network Configuration on a vSphere Distributed Switch.*

*VMware vSphere Networking guide*
Managing VMware VDS (VMware vSphere 6.7)

The VMware VDS is an enterprise feature of VMware vSphere vCenter Server and requires that the VMware vSphere ESXi hosts are licensed with the VMware vSphere Enterprise Plus edition. A non-Enterprise Plus edition does not support VMware vSphere Distributed Switch (VDS) functionality. No additional license is required to be installed or managed for the VMware VDS.
Managing the Cisco Nexus 1000V Series Switch

Managing licenses

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

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

Management settings should not be changed without Dell EMC 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`
7. 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.
8. To save the configuration: `n1000v(config)# copy run start`

**Related information**
Cisco Nexus 1000V Port Profile Configuration Guide
Modifying the uplink port profiles

Modify the trunks that carry VSM to VEM traffic, service console and VMKernel, and VM data traffic and run northbound from the Cisco Nexus 1000V Switch. Recommended VLAN numbers and IP addresses are referenced in this procedure.

About this task

If a naming convention is used that differs from what is recommended, refer to the *Logical Configuration Guide*. When modifying the uplink port profile, northbound traffic from the Cisco Nexus 1000V Switch through the Cisco UCS fabric interconnect is affected.

Before you begin

- Verify that VLANs on uplinks exist in Cisco 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 CLI.
2. To modify the UPLINK port profiles for VMware VM traffic, L3 VMotion, NFS, and VSM Layer 3 Control, type the following:

```plaintext
port-profile type ethernet PRODUCTION-UPLINK
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 300
  channel-group auto mode on mac-pinning
  no shutdown
  state enabled

/* For vSphere 6.0 and later */
port-profile type ethernet VMOTION-UPLINK
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan <106 or 117>
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan <106 or 117>
  state enabled

port-profile type ethernet N1K_L3_CONTROL-UPLINK
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 116
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 116
  state enabled

/* For unified only */
port-profile type ethernet NFS-UPLINK
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 109
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 109
  state enabled
```
3. To view the uplinks created under the Cisco Nexus 1000V Switch in the production VMware vCenter, select Inventory > Networking.

   v6vc01.mpe.lab.vce.com
   MPE-V6DC
   vb240n1kv
   N1K_L3_CONTROL-UPLINK
   NFS-UPLINK
   PRODUCTION-UPLINK
   Unused_or_Quarantine_Uplink
   VMOTION-UPLINK

**Removing the uplink port profiles**

Remove the uplink port profiles from the trunks that run northbound from the Cisco Nexus 1000V Switch. Northbound traffic from the Cisco Nexus 1000V Switch is affected.

**Before you begin**

- Verify that VLANs on uplinks exist in Cisco 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 the following commands:

   ```
   configure terminal
   no port-profile type ethernet PRODUCTION-UPLINK
   copy run start
   end
   ```
Modifying vEthernet data port profiles

Modify data port profiles for VMware VM traffic, L3 VMotion, NFS, and VSM Layer 3 Control.

Procedure

1. To modify the data port profiles for VMware VM traffic, L3 VMotion, NFS, and VSM Layer 3 Control, type the following commands:

```bash
port-profile type vethernet VM-DATA-300
vmware port-group
switchport mode access
switchport access vlan 300 or <Customer Data VLAN number>
no shutdown
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 4
system vlan 117 or <L3 vMotion vlan number>
service-policy type qos input SET_COS_4
state enabled
copy run start

/* For Unified Systems */

port-profile type vethernet VCESYS_ESX_NFS
vmware port-group
switchport mode access
switchport access vlan 109 or <ESX NFS vlan number>
no shutdown
pinning id 10
system vlan 109 or <ESX NFS vlan number>
service-policy type qos input SET_COS_2
state enabled

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

port-profile type vethernet VCESYS_N1K_L3CONTROL
vmware port-group
switchport mode access
switchport access vlan 116 or <N1K_L3_Control vlan number>
no shutdown
pinning id 8
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

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.

<table>
<thead>
<tr>
<th>For this Converged System:</th>
<th>Type:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified</td>
<td></td>
</tr>
<tr>
<td>policy-map type qos SET_COS_2</td>
<td></td>
</tr>
<tr>
<td>class class-default</td>
<td></td>
</tr>
<tr>
<td>set cos 2</td>
<td></td>
</tr>
<tr>
<td>policy-map type qos SET_COS_4</td>
<td></td>
</tr>
<tr>
<td>class class-default</td>
<td></td>
</tr>
<tr>
<td>set cos 4</td>
<td></td>
</tr>
<tr>
<td>policy-map type qos SET_COS_6</td>
<td></td>
</tr>
<tr>
<td>class class-default</td>
<td></td>
</tr>
<tr>
<td>set cos 6</td>
<td></td>
</tr>
</tbody>
</table>
For this Converged System:

<table>
<thead>
<tr>
<th>Type:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>policy-map type qos SET_COS_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>class class-default</td>
</tr>
<tr>
<td>set cos 4</td>
</tr>
<tr>
<td>policy-map type qos SET_COS_6</td>
</tr>
<tr>
<td>class class-default</td>
</tr>
<tr>
<td>set cos 6</td>
</tr>
</tbody>
</table>

### Upgrading the 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

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 VMware NSX with VPLEX on VxBlock Systems

This section provides the procedures for failover and recovery of VMware NSX with VPLEX on VxBlock Systems. This section is not applicable for vSphere 6.5.

The VxBlock System where all the VMware vSphere core VMs (PSCs, VC, and VUM) and VMware NSX VMs (NSX Manager and controllers) reside is the primary site. The other VxBlock System is the secondary site.

All the VMware vSphere core VMs (PSCs, VC, and VUM) and VMware NSX VMs (NSX Manager and controllers) reside on a shared stretched LUN provided by VPLEX in the same stretched VMware vSphere management cluster. The VMs are hosted by VMware vSphere ESXi hosts on Cisco UCS B-Series blades and connected to a separate Layer 3 management port group.

All the customer VMs reside on a shared stretched LUN provided by VPLEX in the same stretched VMware vSphere compute cluster. The VMs are hosted by VMware vSphere ESXi hosts on Cisco UCS B-Series blades and connected to a VXLAN port group. These VMs can reside on any VMware vSphere ESXi host in the primary site or the secondary site.

Perform a graceful failover

This procedure explains how to gracefully fail over management components from the primary site to the secondary site.

Procedure

1. Disable DRS on the stretched VMware vSphere management cluster.

   - **Note:** After migrating VMs to the secondary site, disabling DRS prevents VMs from automatically migrating back to the primary site. Expect a loss of network connectivity to all the VMs until the SVI is switched over.

   a. On the VMware vSphere Web Client Home tab, under Inventories, click Hosts and Clusters.
   b. Expand Datacenter to view all the vSphere clusters.
   c. Left-click the Management VPLEX vSphere cluster and select the Manage tab.
   d. Click vSphere DRS and select Edit.
   e. Uncheck the box Turn ON vSphere DRS. This stops the VM from migrating back to the hosts in the primary site after they have been migrated to the secondary site.

2. Manually power off the NSX Manager and controllers.

   - **Note:** To reduce the risk of errors, manually power off the NSX Manager and controllers before migrating. This process prevents errors after connectivity is restored in the secondary site.

   a. On the VMware vSphere Web Client Home tab, under Inventories, click Hosts and Clusters.
   b. Expand the Management VPLEX vSphere cluster to view the VMs.
   c. Right-click NSX Manager VM and select Power > Shutdown guest OS.
   d. Repeat the steps for all the NSX Controllers in the following order:
      a. NSX Controller 3
b. NSX Controller 2
c. NSX Controller 1

3. Perform a cold migration of the NSX Manager and controllers from the primary site to the secondary site.

   **Note:** After the migration, expect a loss of network communication to all the VMs until the SVI is switched over from the primary site to the secondary site.

   a. Right-click **NSX Manager VM** and select **Migrate**.
   b. The **Migrate** wizard opens. Enter the data values as requested, accept the default settings presented, and use the following configuration information:

<table>
<thead>
<tr>
<th>Wizard page</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the migration type</td>
<td>Change compute resource</td>
</tr>
<tr>
<td>Select a compute resource</td>
<td>vcesysmgmt04</td>
</tr>
<tr>
<td>Select network</td>
<td>vcesys_management</td>
</tr>
</tbody>
</table>

c. Click **Finish**.

d. Repeat the steps for all three NSX controller VMs, using the following information:

<table>
<thead>
<tr>
<th>Wizard page</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX controller 1</td>
<td>vcesysmgmt04</td>
</tr>
<tr>
<td>NSX controller 2</td>
<td>vcesysmgmt05</td>
</tr>
<tr>
<td>NSX controller 3</td>
<td>vcesysmgmt06</td>
</tr>
</tbody>
</table>

e. Verify that each VM successfully migrated to correct ESXi host.

4. Migrate the remaining management components on hosts from the primary site to the secondary site.

   **Note:** The DHCP server resides in its local site and should not be migrated to the opposite site.

   a. Right-click **PSC02 VM** and select **Migrate**.
   b. The **Migrate** wizard opens. Enter the data values as requested, accept the default settings presented, and use the following configuration information:

<table>
<thead>
<tr>
<th>Wizard page</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the migration type</td>
<td>Change compute resource</td>
</tr>
<tr>
<td>Select a compute resource</td>
<td>vcesysmgmt05</td>
</tr>
<tr>
<td>Select network</td>
<td>vcesys_management</td>
</tr>
</tbody>
</table>

c. Click **Finish**.

d. Repeat the steps for the **PSC01 VM** using the following information:

<table>
<thead>
<tr>
<th>VM</th>
<th>Wizard page</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSC01</td>
<td>Select a compute resource</td>
<td>vcesysmgmt04</td>
</tr>
</tbody>
</table>
e. Repeat the migration steps for the remaining management SQL, VC, and VUM VMs, except migrate all the VMs at the same time.

**Note:** It is important to migrate these last three VMs at the same time, because after the VMware vSphere vCenter Server is migrated, it loses connectivity and migration cannot continue. At this point you are forced to manually import the VMs from the datastore.

Use the following information:

<table>
<thead>
<tr>
<th>VMs</th>
<th>Wizard page</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL, VC, and VUM</td>
<td>Select a compute resource</td>
<td>vcesysmgmt05</td>
</tr>
</tbody>
</table>

f. Verify that each VM successfully migrated to correct ESXi host.

5. Within the primary site, manually disable the Management SVI (VLAN 136) on the Cisco 9396 switches.
   a. Use PuTTY to log in to Cisco 9396-A.
   b. Disable the Management SVI by entering the following commands:

   ```
   configure terminal
   interface vlan136 (Use the VLAN ID provided in LCS)
   shutdown
   exit
   copy running-config startup-config
   ```

   c. Repeat the steps to manually disable the Management SVI on Cisco 9396-B.

6. In the secondary site, manually enable the Management SVI (VLAN 136) on the Cisco 9396 switches.
   a. Use PuTTY to log in to Cisco 9396-A.
   b. Enable the Management SVI by entering the following commands:

   ```
   configure terminal
   interface vlan136 (Use the VLAN ID provided in LCS)
   no shutdown
   exit
   copy running-config startup-config
   ```

   c. Repeat the steps to manually enable the Management SVI on Cisco 9396-B.

7. Validate VM connectivity by performing the following steps:
   a. Open command prompt and ping each VM to validate network connectivity.
   b. Log in to the VMware Web Client to validate that VMware vSphere vCenter Server is running properly.
   c. Validate that all the VMware vSphere ESXi hosts and VMs are connected and online.

8. Manually power on NSX Manager and NSX Controllers within the secondary site by performing the following steps:
   a. On the VMware vSphere Web Client Home tab, under Inventories, click Hosts and Clusters.
   b. Expand the Management VPLEX vSphere cluster to view the VMs.
   c. Right-click NSX Manager VM and select Power > Power On.
   d. Repeat the steps for all the NSX Controllers in the following order:
Perform a graceful recovery

This procedure explains how to gracefully recover management components from the secondary site to the primary site.

Procedure

1. Manually power off the NSX Manager and controllers.

   (1) **Note:** To reduce the risk of errors, manually power off the NSX Manager and controllers before migrating. This process prevents errors after connectivity is restored in the secondary site.

   a. On the VMware vSphere Web Client **Home** tab, under **Inventories**, click **Hosts and Clusters**.
   b. Expand the **Management VPLEX vSphere cluster** to view the VMs.
   c. Right-click **NSX Manager VM**, and select **Power > Shutdown guest OS**.
   d. Repeat the steps for all the NSX Controllers in the following order:
      a. NSX Controller 3
      b. NSX Controller 2
      c. NSX Controller 1

2. Perform a cold migration of the NSX Manager and controllers from the secondary site to the primary site.

   (1) **Note:** After the migration, expect a loss of network communication to all VMs until the SVI is switched over from the secondary site to the primary site.

   a. Right-click **NSX Manager VM**, and select **Migrate**.
   b. The **Migrate** wizard opens. Enter the data values as requested, accept the default settings that are presented, and use the following configuration information:

<table>
<thead>
<tr>
<th>Wizard page</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the migration type</td>
<td>Change compute resource</td>
</tr>
</tbody>
</table>
c. Click Finish.
d. Repeat the steps for all three NSX controller VMs, using the following information:

<table>
<thead>
<tr>
<th>Wizard page</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the migration type</td>
<td>Change compute resource</td>
</tr>
<tr>
<td>Select a compute resource</td>
<td>vcesysmgmt02</td>
</tr>
<tr>
<td>Select network</td>
<td>vcesys_management</td>
</tr>
</tbody>
</table>

e. Verify that each VM successfully migrated to correct ESXi host.

3. Migrate the remaining management components on hosts from the secondary site to the primary site.

   a. Right-click PSC02 VM, and select Migrate.
   b. The Migrate wizard opens. Enter the data values as requested, accept the default settings that are presented, and use the following configuration information:

<table>
<thead>
<tr>
<th>Wizard page</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select compute</td>
<td>vcesysmgmt02</td>
</tr>
<tr>
<td>Select network</td>
<td>vcesys_management</td>
</tr>
</tbody>
</table>

   c. Click Finish.
   d. Repeat the steps for the PSC01 VM using the following information:

<table>
<thead>
<tr>
<th>VM</th>
<th>Wizard page</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSC01</td>
<td>Select compute</td>
<td>vcesysmgmt01</td>
</tr>
</tbody>
</table>

   e. Repeat the migration steps for the remaining management SQL, VC, and VUM VMs, except migrate the VMs simultaneously.

   - **Note:** After the VMware vSphere vCenter Server is migrated, it loses connectivity. Unless you migrate the last three VMs, migration cannot continue. Manually import the VMs from the datastore.

   Use the following information:

<table>
<thead>
<tr>
<th>VMs</th>
<th>Wizard page</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL, VC, and VUM</td>
<td>Select compute</td>
<td>vcesysmgmt02</td>
</tr>
</tbody>
</table>

   f. Verify that each VM successfully migrated to correct ESXi host.

4. In the secondary site, manually disable the Management SVI (VLAN 136) on the Cisco 9396 switches.
a. Use PuTTY to log in to Cisco 9396-A.

b. Disable the Management SVI by entering the following commands:

```bash
configure terminal
  interface vlan136 (Use the VLAN ID provided in LCS)
  shutdown
  exit
  copy running-config startup-config
```

c. Repeat the steps to manually disable the Management SVI on Cisco 9396 switch B.

5. In the primary site, manually enable the Management SVI (VLAN 136) on the Cisco 9396 switches.

a. Use PuTTY to log in to Cisco 9396-A.

b. Enable the Management SVI by entering the following commands:

```bash
configure terminal
  interface vlan136 (Use the VLAN ID provided in LCS)
  no shutdown
  exit
  copy running-config startup-config
```

c. Repeat the steps to manually enable the Management SVI on Cisco 9396 switch B.

6. Validate VM connectivity by performing the following steps:

a. Open command prompt and ping each VM to validate network connectivity.

b. Log in to the VMware Web Client to validate that VMware vSphere vCenter Server is running properly.

c. Validate that all the VMware vSphere ESXi hosts and VMs are connected and online.

7. Manually power on NSX Manager and NSX controllers within the secondary site by performing the following steps:

a. On the VMware vSphere Web Client Home tab, under Inventories, click Hosts and Clusters.

b. Expand the Management VPLEX vSphere cluster to view the VMs.

c. Right-click NSX Manager VM, and select Power > Power On.

d. Repeat the steps for all the NSX Controllers in the following order:

   a. NSX Controller 1
   b. NSX Controller 2
   c. NSX Controller 3

8. Validate that all NSX Controllers are connected and no warnings or errors exist.


b. Click Dashboard in the left pane, and verify the following:

   - Ensure that in System Overview that the NSX Manager and all three NSX Controllers show a green square.
   - Ensure that there are no errors or warnings within the Host Preparation Status, Firewall Publish Status, and Logical Switch Status.

   c. To resolve any errors under the Host Preparation Status, select Resolve All to fix.
9. Enable DRS on the stretched VMware vSphere management cluster.

**Note:**
This step forces all the VMs to recover back from the secondary site to the primary site. Expect a loss of network communication to all the VMs until the SVI is switched over.

a. On the VMware vSphere Web Client Home tab, under Inventories, click Hosts and Clusters.
b. Expand Datacenter to view all the vSphere clusters.
c. Click Management VPLEX vSphere cluster, and select the Manage tab.
d. Click vSphere DRS, and select Edit.
e. To force each management VM to vMotion to an assigned host, enable Turn ON vSphere DRS.

10. Click Finish. All the VMware vSphere core and NSX Manager and controller components are now running in the primary site.
Guidelines for backing up configuration files

The following section is applicable to AMP-2 only.

Back up configuration files

Back up and restore VxBlock System configuration files with VxBlock Central.
For information about performing these tasks, see VxBlock Central online help.

Back up network devices running Cisco NX-OS software

Create a configuration file to back up network devices using Cisco NX-OS operating systems.

About this task

IPv4 addresses are supported on Vblock Systems and VxBlock Systems. IPv6 addresses are supported on VxBlock Systems.

Before you begin

- TFTP service must be installed, configured, and active, on the AMP server where the configuration repository exists.
- Verify that an instance of the configuration repository exists.
- Obtain login credentials for the device configuration backup.
- Obtain the network IP address of the configuration backup repository.
- Obtain the device name and type that matches the model abbreviation that was used to create the repository subdirectory structure.

Procedure

1. Log in to the device account using administrator privileges.
2. To confirm that the scheduler feature is enabled, type:
   ```
   SWITCH# show feature | include scheduler
   scheduler             1         enabled
   ```
3. Routing requirements may require you to add VRF management to the end of each copy command. The variable \$(TIMESTAMP)\ in the file name inserts the date/time into the file name when the tasks are run. From the network device, to create the backup task, enter the following command:
   ```
   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/name_startup_$ (TIMESTAMP).cfg
   SWITCH(config-job)# copy running-config tftp://IP/device/config/name_running_$ (TIMESTAMP).cfg
   SWITCH(config-job)# end
   ```
4. To schedule the backup task, type:

```
SWITCH# conf t
SWITCH(config)# scheduler schedule name Daily0600
SWITCH(config-schedule)# time daily 06:00
SWITCH(config-schedule)# job name cfgBackup
SWITCH(config-schedule)# end
SWITCH# 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
```

5. 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://<IP_Address>/9500/config/D01-9500-01_startup_$(TIMESTAMP).cfg
copy running-config tftp://<IP_Address>/9500/config/D01-9500-01_running_$(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
```

6. Verify that the copy statements work by running each individually:

```
V00101MD9502# copy running-config tftp://<IP_Address>/9500/config/V00101MD9502_running_$(TIMESTAMP).cfg
```

```
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
TFTP put operation was successful
```

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

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

8. To verify the procedure, run each statement individually: V00101MD9502# copy running-config tftp://<IP_Address>/9500/config/V00101MD9502_running_$(TIMESTAMP).cfg
Back up Cisco UCS FIs

Restore a system configuration from any full state backup file exported from Cisco UCS Manager.

About this task

Back up using Cisco UCS Manager and take a snapshot of all or part of the system. Configure and export the file to a location on your network. You cannot use Cisco UCS Manager to back up data on the servers.

You can perform a backup while the system is up and running. The backup operation saves information from the management plane and does impact the server or network traffic.

Before you begin

- The TFTP service must be installed, configured, and active, on the AMP server where the configuration repository exists.
- Obtain login credentials for the device configuration backup.
- Obtain the network IP address of the configuration backup repository.
- Obtain the device name and type that matches the model abbreviation that was used to create the repository subdirectory structure. For example:

```
\6100\config\filename
```

Procedure

1. Create and run the backup using either the Cisco UCS Manager GUI or CLI.

Related tasks

Create and run the backup using the Cisco UCS Manager on page 130
Create and run the backup using the Cisco UCS CLI on page 131

Create and run the backup using the Cisco UCS Manager

Back up the Cisco UCS fabric interconnects configuration using the Cisco UCS Manager GUI.

About this task

Creating a backup is a one-time only task.

Procedure

1. Log in to the Cisco UCS Manager using administrator privileges.
2. To create the backup, perform the following steps:
   a. From the Navigation window, select the Admin tab.
   b. Click the All node.
   c. From the Work window, select the General tab.
   d. In the Actions area, select Backup (for UCSM 2.x).
   e. In the Actions area, select Backup Configuration. (for UCS 3.x)
   f. In the Backup Configuration window, select Create Backup Operation.
   g. Set Admin State to Disabled.
   h. Set Type to Full State.
   i. Select the Preserve Identifies checkbox.
   j. Click OK.
   k. If a confirmation window appears, click OK.
3. To run the backup, perform the following:
   
a. From the **Navigation** window, select the **Admin** tab.
   
b. Select the **All** node.
   
c. From the **Work** window, select the **General** tab.
   
d. In the **Actions** area, select **Backup**.
   
e. From the **Backup Operations** table of the **Backup Configuration** window, select the backup operation that you want to run.
   
f. In the **Admin State** field, select **Enabled**.
   
g. For all protocols except TFTP, type the password in the **Password** field.
   
h. You can optionally change the content of the other available fields.
   
i. 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.
   
j. View the progress of the backup operation by clicking the down arrows on the **FSM Details** bar.
   
k. To close the **Backup Configuration** window, click **OK**.
   
l. The backup operation continues to run until it is completed. To view the progress, reopen the **Backup Configuration** window.

**Related tasks**

Create and run the backup using the Cisco UCS Manager on page 130

Create and run the backup using the Cisco UCS CLI on page 131

### Create and run the backup using the Cisco UCS CLI

Creating a backup is a one-time only task.

**Procedure**

1. Log in to the Cisco UCS Manager using SSH administrator privileges.
   
2. To create the backup, 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 #
   ```

3. To run the backup, type:

   ```
   UCS-A# scope system
   UCS-A /system* # scope backup v00001vmfm01
   UCS-A /system* # enable
   Password:
   UCS-A /system* # commit-buffer
   ```
Guidelines for backing up configuration files

--

UCS-A /system #

Related tasks
Create and run the backup using the Cisco UCS Manager on page 130
Create and run the backup using the Cisco UCS CLI on page 131

Create and run the backup using scheduled backups
Create and run the FI backup using scheduled backups.

About this task
The following conditions apply for scheduled backups:

- Scheduled backups can be configured for full state.
- You cannot set the exact time of day that the scheduled backup occurs.
- The full state backup is a binary file that includes a snapshot of the entire system.
  - Use the binary file to restore the system during disaster recovery.
  - Use the binary file to restore or rebuild the configuration on the original FI or recreate the configuration on a different FI.
  - You cannot use the binary file for an import.
- Full state backups are encrypted.
- The full state backup policy can be configured as daily, weekly, or biweekly.
- You cannot modify the maximum number of backup files that the Cisco UCS Manager creates.
- The option to configure scheduled backups can be found on the Admin tab and on the right side of the screen on the Policy Backup & Export tab.

Procedure
1. To use the Cisco UCS Manager GUI to configure scheduled backups, see the following document:
2. To use the Cisco UCS Manager CLI to configure scheduled backups, see the following document:

Configure fault suppression
Fault suppression allows you to suppress SNMP trap and Call Home notifications during planned maintenance time.

About this task
A fault suppression task prevents notifications from being sent whenever a transient fault is raised or cleared. Faults remain suppressed until the time duration has expired or the fault suppression tasks have been manually stopped. After the fault suppression has ended, Cisco UCS Manager sends notifications for uncleared, outstanding, suppressed faults.

Fault suppression uses fixed time intervals or schedules.

You can specify the maintenance window to suppress faults using fixed time intervals or schedules. Fixed time intervals allow you to create a start time and a duration when fault suppression is active. Fixed time intervals cannot be reused. Schedules are used for one time occurrences or recurring time periods and can be saved and reused.

Fault suppression policies define the causes and fault types to suppress. Only one policy can be assigned to a task. The following table provides the Cisco UCS Manager policies:
### Policy Description

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-chassis-all-maint</td>
<td>This policy suppresses faults for the Cisco UCS 5108 Blade Server Chassis and components, including all blade servers, power supplies, fan modules, and IOMs. This policy applies only to chassis.</td>
</tr>
<tr>
<td>default-chassis-phys-maint</td>
<td>This policy suppresses faults for the chassis and all fan modules and power supplies that are installed into the chassis. This policy applies only to chassis.</td>
</tr>
<tr>
<td>default-fex-all-maint</td>
<td>This policy suppresses faults for the FEX and all power supplies, fan modules, and IOMs in the FEX. This policy applies only to the FEX.</td>
</tr>
<tr>
<td>default-fex-phys-maint</td>
<td>This policy suppresses faults for the FEX and all fan modules and power supplies in the FEX. This policy applies only to the FEX.</td>
</tr>
<tr>
<td>default-server-maint</td>
<td>This policy suppresses faults for blade servers and/or rack servers. This policy applies to chassis, organizations, and service profile. When applied to a chassis, only blade servers are affected.</td>
</tr>
<tr>
<td>default-iom-maint</td>
<td>This policy suppresses faults for IOMs in a chassis or FEX. This policy applies only to chassis, the FEX, and IOMs.</td>
</tr>
</tbody>
</table>

### Procedure

1. To use the Cisco UCS Manager GUI to configure fault suppression, see: *Cisco UCS Manager GUI Configuration Guide, Release 2.x, Cisco UCS Manager GUI Configuration Guide, Release 3.x.*
2. To use the Cisco UCS Manager CLI to configure fault suppression, see: *Cisco UCS Manager CLI Configuration Guide, Release 2.x, Cisco UCS Manager CLI Configuration Guide, Release 3.x.*

### Back up the VMware vCenter SQL server database

Create backup jobs in a Microsoft SQL server configuration. Frequency depends upon the client RPO.

**About this task**

Creating backup jobs is not required for VMware vSphere 6.5.

**Before you begin**

- Confirm that the Microsoft SQL server sa login is enabled and a password is set for the account.
- Ensure that the server authentication mode is set to the SQL Server and Windows Authentication mode.
- Obtain administrator login credentials.
- Obtain AMP element manager server network address.
- Obtain VMware vCenter SQL server network address and SQL server login credentials.
- For more information, see Microsoft Developer Network article for SQL: Change Server Authentication Mode.

**Procedure**

1. Connect to the client AMP environment jump server.
2. From the jump server, use RDP to access the SQL database server, and log in as administrator.
3. To run the SQL Server Management Studio application, go to the application and select **Start > All Programs > Microsoft SQL Server > SQL Server Management Studio**.
4. To log in to the application, perform the following:
   a. In the **Server type** field, verify that **Database Engine** appears. If not, select it.
   b. If the **Server name** field is not autofilled, select **(local)**. If no matching account exists, log in with administrator privileges.
   c. In the **Authentication** field, verify that **Windows Authentication** appears. If not, select it, and click **Connect**.
5. To confirm the list of databases that require backup, from the **Object Explorer** window, expand **Databases > System Databases**.

The databases that require backup are in the **System Databases** (master, model, msdb) and the vcenter and vum databases that appear after the **Database Snapshots** folder. Depending on the naming standard that has been followed (client or Dell EMC), 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.

6. Go to, and expand **SQL Server Agent > Jobs**.

7. To create a backup job, right-click **Jobs** and select **New Job**.
   a. From the **New Job** window, in the **Name** field, enter a name for the backup.
   b. In the **Owner** field, delete the default login and enter sa.
   c. Change the **Category** field to **Database Maintenance**.
   d. Type a description in the **Description** field.
   e. Verify **Enabled** is checked.

8. To create a job-step entry, under **Select a page**, select **Procedure (Steps)**, and then click **New**.
   a. From the **New Job Step** window, in the **Step name** field, type Backup or other text.
   b. Verify that the default value is set in the **New Job Step** window.
   c. Leave the **Run as** field empty.
   d. In the **Database** field, select the database.
   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. 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 click New.
   a. From the New Job Schedule window, type a Name for the job schedule.
   b. 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>a. In the Frequency section, set the Occurs field to Daily.</td>
</tr>
<tr>
<td></td>
<td>b. Verify that the Recurs field is set to 1 day.</td>
</tr>
<tr>
<td></td>
<td>c. In the Daily Frequency section, check Occurs once at and set to 06:30 AM.</td>
</tr>
<tr>
<td></td>
<td>d. 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>a. In the Frequency section, set the Occurs field to Daily.</td>
</tr>
<tr>
<td></td>
<td>b. Verify that the Recurs field is set to 1 day.</td>
</tr>
<tr>
<td></td>
<td>c. In the Daily Frequency section, check Occurs every, type 4, and select hours.</td>
</tr>
<tr>
<td></td>
<td>d. Set Starting at to 06:30:00 AM and Ending at to 06:29:59 AM.</td>
</tr>
<tr>
<td></td>
<td>e. In the Duration section, confirm the Start date is set to the current date and No end date is selected.</td>
</tr>
</tbody>
</table>

   c. Verify that the Schedule Type is set to Recurring and confirm Enabled is checked.
   d. Click OK to accept the schedule update.
   e. Click OK to complete backup job creation.

10. Repeat the preceding steps starting with step 8 until all databases (excluding tempdb) have a backup job.
11. To create an SQL Server backup file management job, go to step 8 and perform the following:
   a. As the job description, type BAK file management.
   b. For the database field, select master.
   c. 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
--
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
```

   d. Use the same schedule as the master database.
12. To test a backup, right-click a backup job and select Start Job at Step.
After you finish
Monitor the backup location to confirm that backups are performed on schedule.

Back up the VNXe configuration

Back up the VNXe storage array used as the AMP shared storage. 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 VNXe management address.
- Obtain administrator login credentials for service accounts.

Procedure

1. To log into Unisphere, open a URL to the VNXe management address.
2. From the login screen, type the username and password for the account with advanced administrator privileges for the VNXe system. If you are using an LDAP-based account, type the domain/username for the account and click Login.
   For more information, refer to the Configure User Access to Unisphere.
   
   Note: If you cannot remember the passwords for the VNXe default administrator or service user accounts, you can set the passwords back to the default passwords that shipped with your VNXe system.
3. To initiate configuration backup task, select Settings > Service System.
4. Type the service password to access the Service System page.
5. Under System Components, select Storage System.
6. Under Service Actions, select a service action and click Execute service action.
7. If you click Save Configuration, you can save details about the configuration settings on the 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

The file only contains details about your system configuration settings. You cannot restore your system from this file. Save the configuration settings after each major configuration change to ensure you have a current copy of the file.
Back up Cisco MDS switches

Create backups of startup and running configuration files

Create a backup of the Cisco MDS switch startup and running configuration files. Backups are stored on the Cisco UCS C220 management server.

Before you begin

- Start the TFTP service on each of the management servers.
- If it does not exist, create the following folder on each management server:
  D:\Cisco\MDS\switch-model\config
- Obtain the int-mdsbackup login ID and password to log in to the Cisco MDS switches.

Procedure

1. Log in to the switch using PuTTY with the int-mdsbackup login ID on the Converged System.
2. Use the copy command to create the configuration file backups.

```plaintext
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
```

After you finish

Schedule the backup to run regularly.

Related tasks

Scheduling backups of the startup and running configuration files on page 137

Scheduling backups of the startup and running configuration files

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 and, at the end of each line, type ctrl-z:

   scheduler aaa-authentication username login password password
   scheduler job_name switchBackup

3. To create a backup for the startup-config and running-config files, for example, type:

   ```plaintext
   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: The preceding commands add the date and timestamp to the filenames.

4. Type the following commands, one per line, and 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
cfg terminal
feature scheduler
scheduler logfile size 16
end
cfg 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
cfg terminal
Scheduler schedule name Daily
Time daily 23:00
Job name switchBackup
end

After you are satisfied with the job, issue the copy running-config startup-config command to save the configuration.

Create a script to purge older copies of the backup files
Create a script that can be scheduled to run to delete old backups of the startup and configuration files.

Procedure

1. To create a script that deletes old backups of the startup and configuration files, copy the VBS script that is included here. Save it to the following file: D:\scripts\delete_old_backups.vbs
Option Explicit
On Error Resume Next
Dim oFSO, oFolder, sDirectoryPath
Dim oFileCollection, oFile, sDir
Dim iDaysOld
' Specify Directory Path for File Deletion
sDirectoryPath = "D:\Cisco\9xxx\config"
' Specify Number of Days Old File to Delete
iDaysOld = 7
Set oFSO = CreateObject("Scripting.FileSystemObject")
Set oFolder = oFSO.GetFolder(sDirectoryPath)
Set oFileCollection = oFolder.Files
For each oFile in oFileCollection
    Specify File Extension
    'Specify number with Number of characters in the file extension
    If LCase(Right(Cstr(oFile.Name), 6)) = "config" Then
        If oFile.DateLastModified < (Date() - iDaysOld) Then
            oFile.Delete(True)
        End If
    End If
Next
Set oFSO = Nothing
Set oFolder = Nothing
Set oFileCollection = Nothing
Set oFile = Nothing

Schedule the task to purge older backup files

Schedule the script called D:\scripts\delete_old_backups.vbs daily to purge older backup files.

About this task

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

Before you begin

Obtain the password for the [Domain]\svc-vmfms01 account from your VMware administrator.

Procedure

1. 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.
Configuring VMware Enhanced Linked Mode (VMware vSphere 6.0)

Introduction

One of the advantages of a Dell EMC Converged System is delivery of a preconfigured physical and logical working system. Converged Systems are physically and logically configured during the manufacturing process. If you have multiple Converged Systems, you can use Enhanced Linked Mode (ELM) with VMware vSphere 6.0 to log in to a single VMware vCenter. Then, you can operate, manage, and maintain multiple VMware vCenter servers. The installation prerequisites, require that VMware vSphere 6.0 ELM be configured on the customer premises.

If you want to configure ELM, Dell EMC recommends that you contact Dell EMC Professional Services to have them perform the site analysis, installation, and configuration.

Dell EMC supports the following ELM with VMware vSphere 6.0 configurations:

- One or two VMware vCenter Servers that are linked to two Platform Service Controllers (PSCs) in one Converged System
- Two or more VMware vCenter Servers that are linked to two or more PSCs across two or more Converged Systems in a data center
- Two or more VMware vCenter Servers that are linked to two or more PSCs across two or more Converged Systems across two data centers

The configuration of ELM with VMware vSphere 6.0 is not be addressed in this document. Deployment of ELM with VMware vSphere 6.0 cannot be reversed. ELM with VMware vSphere 6.0 is managed as a complete system and should be considered a fault, operational, and maintenance domain. Any ELM VMware vSphere 6.0 configuration must be compatible with backup and restore processes for the following in a single VMware vSphere 6.0 Single Sign-On domain:

- All VMware vSphere PSCs (PSC)
- All VMware vCenter servers

Use the following links to obtain additional information about Enhanced Linked Mode:

**VMware vSphere 6.0 link:**


**VMware ELM with VMware vSphere 6.0 use cases**

ELM with VMware vSphere 6.0 can be used several situations.

The following use cases are focused on single pane of glass management:

- ELM with VMware vSphere provides a single interface to manage multiple VMware vCenter servers using two shared VMware vSphere PSCs in the same Converged System.
- ELM with VMware vSphere is used to integrate VMware vCenter Management for two Converged Systems in the same data center. ELM with VMware vSphere 6.0 with two Converged Systems is an operational, fault and management domain. Exceeding this approach results in an increase in the complexity of the operational, fault and management domain. Each Converged System has multiple VMware vCenter servers. In this scenario, compute, network, and storage resources are not shared between the two or more discrete VMware vCenter servers that are located in each Converged System.
• ELM with VMware vSphere is used to integrate VMware vCenter Management for two Converged Systems in separate data centers. Exceeding this approach results in an increase in the complexity of the operational, fault, and management domain. Compute, network, and storage resources are not shared between the two or more discrete VMware vCenter servers that are located in separate data centers. This configuration is similar to a configuration for two Converged Systems in the same data center, but introduces network latency.

Simplify VMware vSphere 6.0 management with more than two Converged Systems or VMware vCenter servers by using an AMP-2S with an SMP/VMP configuration.

**Back up and restoring Converged Systems with VMware ELM**

Use this information to review backup and recovery capabilities.

1. Deploy and test a Data Protection and Recovery solution for the backup and recovery of the management VMware vSphere environment. Testing is especially important with ELM configurations with multiple PSCs that maintain replication synchronization using sequence numbers. See the following links for important backup information:
   - VMware vSphere 6.0 Backing up and Restoring a VMware vCenter server environment: https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html
   - VMware vSphere 6.0 Backing up and restoring VMware vCenter server 6.0 external deployment models (KB 2110294)
   - Possible VMware vSphere.local domain inconsistencies after restoring a Platform Services Controller 6.0 Node (2086001):

2. See the *VMware vSphere 6 Data Protection Administration Guide*. The document describes how to use the VMware Data Protection appliance for a direct-to-host emergency restore when VMware vCenter server is not available. The following document describes recommendations, limitations, and unsupported features:

3. You need a tested backup and recovery solution for the VMware vSphere 6.0 PSCs and VMware vCenter servers. Do not proceed with a VMware vSphere 6.0 ELM configuration without it. ELM adds complexity to the backup and recovery solution. The number of PSCs, VMware vSphere 6.0 PSCs, and VMware vCenter servers require different backup strategies.

**AMP design (AMP-2S only)**

Dell EMC manufacturing configures the AMP with VMware vSphere 6.0 (AMP-2S only) using only VMware recommended topologies. Deployment of the PSC and VMware vCenter using a nonrecommended topology may prevent backing up and restoring a VMware vCenter server environment with a PSC.

Review the following link for recommend topologies:

- VMware vSphere 6.0 Recommended Topologies

Each Converged System participating in ELM must continue to maintain a functioning AMP. Each Converged System VMware vSphere environment must not rely on the VMware vSphere infrastructure of another Converged System to operate correctly. All VMware vSphere 6.0 management VMs in a Converged System must use local storage for the AMP-2P M4, or shared VNXe storage for the AMP-2S M4.

External PSCs are required for VMware vSphere 6.0 ELM. Dell EMC does not recommend embedded VMware PSCs.
Dell EMC does not recommend the deployment of a PSC SSO domain with multiple SSO sites. The deployment of multiple sites impacts the VMware vSphere 6.0 backup and recovery procedure. See the following link for backup limitations with multisite SSO:

- VMware vSphere 6.0 Backing up and restoring a VMware vCenter server environment: https://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html
  
  With VMware vSphere 6.0, you cannot use PSC snapshots with multisite or HA configurations. See the following link: FAQ: VMware PSC in VMware vSphere 6.0 (2113115)

Dell EMC recommends the deployment of the vCSA. However both the vCSA and VMware vCenter for Windows are supported with ELM.

After delivery and implementation, ensure that the AMP servers have network connectivity and sufficient resources to meet any additional workload. A redundant AMP is recommended.

VMware vSphere 6.0 PSC High Availability requires a load balancer. Load Balancers are not used with the Converged System. During deployment, a VMware vCenter must be associated with a local PSC. If a PSC fails, the VMware vCenter must be manually repointed to a secondary PSC.

Standard VMware vSphere 6.0 design for a Converged System includes one VMware vCenter server and a minimum of two PSCs.

For best performance, split multiple VMware vCenter servers between PSCs in the same physical Converged System or physical data center.

At minimum, ELM requires IP connectivity for the ESXI management VLANs between the Converged Systems joined in an ELM configuration. Validate IP connectivity between the two VMware vSphere 6.0 vcesys_esx_mgmt VLANs. Verify that all required protocols and ports are allowed on any firewalls between the two vcesys_esx_mgmt VLANs.

- See the following VMware KB article for additional information for VMware vSphere 6.0: https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2106283

For VMware vSphere 6.0 management traffic, extend the QoS marking across any metro or WAN links connecting separate physical data centers.

VMware vSphere 6.0 ELM configurations must use consistent IP MTU sizes with physical and logical network switches and VMkernel ports.

### VMware ELM scalability planning

Determine the number of PSCs and VMware vCenter servers that are needed for an ELM configuration with VMware vSphere 6.0 in an SSO Domain and site.

Determine if the requested number of PSCs and VMware vCenter servers is compatible with VMware vSphere 6.0 configuration maximum limits. Use the following link to see the latest VMware vSphere 6.0 ELM configuration maximums:


The following table provides the ELM with VMware vSphere 6.0 SSO configuration maximum limitations:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of linked VMware vCenter servers per SSO Domain</td>
<td>10</td>
</tr>
<tr>
<td>Maximum number of PSCs per VMware vSphere domain</td>
<td>8</td>
</tr>
<tr>
<td>Maximum number of PSCs per site, behind a load balancer</td>
<td>4</td>
</tr>
<tr>
<td>PSC management limits</td>
<td>One PSC</td>
</tr>
<tr>
<td></td>
<td>4 VMware vCenter Servers</td>
</tr>
</tbody>
</table>
### Intra Converged System VMware ELM scalability planning

Determine the maximum number of VMware vCenter servers that can be configured in a Converged System that includes two PSCs.

- A standard Converged System configuration with two PSCs can have a maximum of eight VMware vCenter servers. Half of the VMware vCenter servers point to the first PSC, while the second half point to the second PSC. Supporting ten VMware vCenter servers in a single Converged System requires three PSCs. Three PSCs in a single Converged System SSO Domain, while viable, is not a standard Converged System design.  

  **Note:** There is no available capacity to repoint a VMware vCenter server to a different PSC under the following conditions:
  - Two PSCs are deployed in a Converged System.
  - Each PSC has four VMware vCenter servers.

  Repointing one of the VMware vCenter servers requires a non-standard three-PSC configuration.

Dell EMC recommends two PSCs which can support two VMware vSphere 6.0 VMware vCenter servers. Minimizing the number of PSCs and VMware vCenter servers in an ELM configuration reduces the size of the fault, operation, management domain, and RCM upgrade complexity. Two VMware vCenter servers can support the number of compute servers in the Converged System. The following table defines the maximum number of compute hosts per Converged System:

<table>
<thead>
<tr>
<th>VxBlock or Vblock System Type</th>
<th>Number of Compute Servers (half-width)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VxBlock or Vblock 350</td>
<td>256</td>
</tr>
<tr>
<td>VxBlock or Vblock 540</td>
<td>256</td>
</tr>
<tr>
<td>VxBlock or Vblock 740</td>
<td>512</td>
</tr>
</tbody>
</table>

- Deployment of more than one VMware vCenter server per Converged System requires the deployment of a redundant AMP server with an external VNXe. Each AMP server must be appropriately scaled to support multiple VMware vCenter servers.
• Scale the entire Converged System AMP, network, storage, and compute environment resources appropriately when deploying multiple VMware vCenter servers and the associated resources in a Converged System.

Inter Converged System VMware ELM scalability planning in Converged Systems in a single physical data center

Determine the maximum number of which can be configured with ELM and VMware vSphere 6.0.

Scenario 1: Each Converged System is deployed with two PSCs.

• A standard Converged System configuration with two PSCs can have a maximum of four Converged Systems. A minimum of one VMware vCenter server is required for each Converged System. The maximum number of VMware vCenter servers with ELM is limited to ten. Each of the four Converged Systems can support more than one VMware vCenter servers. In this configuration, you must maintain the Dell EMC VMware vSphere software Release Certification Matrix (RCM) consistently across all four Converged Systems. Periodically, monitor PSC replication sequence numbers to verify PSC synchronization.
  Dell EMC recommends a maximum of two Converged Systems. Minimizing the number of PSCs and VMware vCenter servers in an ELM configuration reduces the size of the fault, operation, management domain, and RCM upgrade complexity. Each Converged System has two PSCs and a maximum of two VMware vCenter servers per Converged System. AMP-2S is recommended to maintain and operate and provide single pane of glass management for more than two Converged Systems.

• Deployment of more than one VMware vCenter server per Converged System requires a redundant AMP with an external VNXe. Scale each AMP Server to support multiple VMware vCenter servers.

• Scale the entire Converged System AMP, network, storage, and compute environment resources when deploying multiple VMware vCenter servers and the associated resources.

Determine the maximum number of Converged Systems that can be configured with ELM with VMware vSphere 6.0 in a single physical data center.

Inter Converged System ELM scalability planning with multiple physical data centers

Determine the maximum number of Converged System which can be configured with ELM with VMware vSphere 6.0 in multiple physical data centers.

• Each ELM with VMware vSphere 6.0 configuration requires a minimum of two PSC servers per physical data center. If a primary PSC outage occurs, each VMware vCenter can be repointed to the secondary PSC in the same physical data center. This approach maintains a consistent level of performance, which may not be achievable when SSO authentication must traverse a WAN. A maximum of four physical data centers are supported with an ELM configuration with VMware vSphere 6.0.

• A standard Converged System configuration with two PSCs supports a maximum of four Converged Systems with multiple physical data centers. Each Converged System requires a minimum of one VMware vCenter server. ELM has an upper limit of ten VMware vCenter servers. In this configuration, each of the four Converged Systems can support more than one VMware vCenter servers. In this configuration, you must maintain the Dell EMC VMware vSphere software Release Code Matrix (RCM) consistently across all four Converged Systems distributed across two physical data centers. Periodically, you must monitor PSC replication sequence numbers to verify PSC synchronization.

• Dell EMC recommends a maximum of two Converged Systems in an ELM configuration with VMware vSphere 6.0 and multiple physical data centers. Dell EMC does not recommend such a large fault tolerant and data protection and recovery domain when:
  - The ELM configuration includes VMware vSphere 6.0.
  - Four Converged Systems are located in two physical data centers.
Each physical data center supports one Converged System with two PSCs and a maximum of two VMware vCenter servers.

- Deployment of more than one VMware vCenter server per Converged System requires the deployment of a redundant AMP with an external VNXe. Each AMP Server must be appropriately scaled to support multiple VMware vCenter servers.
- Scale the entire Converged System, AMP, network, storage, and compute environment resources when deploying multiple VMware vCenter servers and the associated resources.

## VMware ELM deployment information

When deploying VMware ELM, replicate roles, permission, licenses, tags, and policies across linked VMware vCenter servers.

⚠️ **CAUTION** For VMware vSphere 6.0, Dell EMC recommends the following:

- A maximum RTT of 100 milliseconds between VMware PSCs at physically separate data centers
- A maximum RTT of 10 milliseconds between VMware PSCs in a site

The legacy VMware vSphere Client does not support Enhanced Linked Mode.

With VMware vSphere 6.0, you cannot consolidate multiple SSO domains in each product line.

VMware vSphere 6.0 supports both VMware vCenter Windows and vCSA in Enhanced Linked Mode.

See the following link for VMware vSphere 6.0:


For VMware vSphere 6.0, Dell EMC does not recommend and does not support mixing embedded and external PSCs. A VMware vCenter server with an embedded VMware PSC is appropriate for small environments. You cannot join other VMware vCenter servers or VMware PSCs to this VMware vCenter Single Sign-On domain.

VMware vSphere 6.0 Recommended Topologies link:


The recommended topology for VMware vSphere 6.0 is to use external PSCs. If you have deployed an extra VMware vCenter in a Converged System using an embedded PSC, you must migrate the installed VMware vCenter to an external PSC. This migration is a one-way irreversible configuration. VMware does not have any supported tools or processes to reverse an ELM configuration. The required topology for ELM with VMware vSphere 6.0 is to use external PSCs. As of 6.0U1 you can repoint a VMware vCenter server to an external PSC. See the following links:

https://blogs.vmware.com/consulting/2015/03/vsphere-datacenter-design-vcenter-architecture-changes-vsphere-6-0-part-1.html


Migrating to an ELM configuration with VMware vSphere 6.0 is an irreversible configuration. To split an ELM configuration, build a new discrete VMware vSphere 6.0 domain with PSCs, VC, and VUM. Migrate the VMware vSphere hosts and VM guests that you want to split off to the newly built VMware vSphere domain. Although workarounds have been developed to split a VMware vSphere domain, VMware does not support them.

Dell EMC has made no assumptions regarding VMware vSphere vMotion support between VMware vCenter servers. Cold migration between VMware vCenter servers using a recommended L3 Provision network is possible.

Migration between VMware vCenter servers must meet the VMware requirements.

See the following link for VMware vSphere 6.0:


After you deploy ELM with VMware vSphere 6.0, verify PSC associations and replication status for all deployed PSC servers. See the following link for VMware vSphere 6.0:
Update PSCs sequentially. Each software upgrade of a PSC takes approximately 30 minutes.

If a PSC is decommissioned, do not reuse the original PSC name in the same SSO domain.

If Microsoft Active Directory is deployed as an authentication source, it must be configured consistently for all PSCs in the SSO domain.

Repointing a VMware vCenter to a PSC is possible only under the following conditions:

- Two separate VMware vSphere 6.0 environments have been configured using the same SSO domain name and site name.
- The VMware vCenter that you want to repoint is a replication partner of the existing PSC in the first VMware vSphere environment.

Deploy inter Converged System PSCs in a ring topology, whether they are located in the same physical data centers or across multiple physical data centers.

- See the following link for configuring a ring topology with VMware vSphere 6.0:
  - https://virtualdatacave.com/2017/02/vsphere-6-0-psc-replication-ring-topology/
  - https://communities.vmware.com/thread/543306
  - http://blog.jgriffiths.org/?p=1423

Repointing VC to a different PSC is limited to the same domain or between sites with VMware vSphere 6.0. See the following links for repointing with VMware vSphere 6.0:

- How to repoint VMware vCenter server 6.0 between External PSC in a site (2113917)
- Repointing VMware vCenter server 6.0 between sites in a VMware vSphere Domain (2131191)

**VMware ELM dependencies and limitations**

All VMware PSCs and VMware vCenter Servers participating in an ELM configuration must run the same software build number.

Ensure that your configuration meets the following requirements:

- RCMs must be compatible between Converged Systems. VMware vSphere 6.0 PSCs and VMware vCenter servers must run the same build version.
- Redundant AMP must be scaled out to support multiple VCs per Converged System.
- IP MTU sizes must be consistent between Converged Systems.
- Each Converged System requires a pair of PSCs.

Although ELM enables the use of PSC, Vision Intelligent Operations and VxBlock Central do not support it. They continue to collect data directly from VMware vCenter Servers.

When configuring IP connectivity between Converged Systems, validate IP connectivity between the two VMware vSphere 6.0 vcesys_esx_mgmt VLANs. Verify that all required protocols and ports are allowed on any firewalls between the two vcesys_esx_mgmt VLANs.

- See the following VMware KB article for additional information with VMware vSphere 6.0:
All local and remote ELM with VMware vSphere 6.0 components require DNS and NTP support.

**VMware ELM references**

These references provide additional information about VMware ELM.

<table>
<thead>
<tr>
<th>Link</th>
<th>Topic title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2113917</td>
<td>How to repoint a VMware vCenter server 6.0 between External PSCs in a site</td>
</tr>
<tr>
<td>2131191</td>
<td>Repointing VMware vCenter server 6.0 between sites in a VMware vSphere Domain</td>
</tr>
<tr>
<td>2106736</td>
<td>Using the cmsso command to unregister VMware vCenter server 6.0 from Single Sign-On</td>
</tr>
<tr>
<td>2108548</td>
<td>List of recommended topologies for VMware vSphere 6.0</td>
</tr>
<tr>
<td>2127057</td>
<td>Determining replication agreements and status with the VMware Platform Services Controller 6.0</td>
</tr>
</tbody>
</table>

**VMware ELM conclusions**

ELM with VMware vSphere 6.0 provides single pane of glass management for up to eight PSCs and ten VMware vCenter servers in a Single Sign-On Domain. It also provides simultaneous single pane of glass management for up to ten VMware vCenter servers. This configuration provides an operational improvement in managing multiple VMware vCenter servers. However, as the number of PSCs and VMware vCenter servers increases, the size of the VMware vSphere 6.0 fault domain becomes larger.

Processes to back up and restore any VMware vSphere component participating in ELM must be reliable and supportable across Converged Systems and data centers. To maintain synchronization of PSC replication, ensure 100% network availability between PSCs in different Converged Systems or data centers. After a PSC outage, synchronization may take some time to occur.

As the size of the SSO Sign-On domain increased, maintenance updates require more planning and coordination. VMware Build Numbers must be consistent in an ELM with VMware vSphere 6.0 configuration. Upgrading any Converged System in an ELM with VMware vSphere 6.0 configuration requires upgrading any other Converged Systems joined to the same VMware vSphere 6.0 Single Sign-On domain. Upgrades are performed in a maintenance window with enough time to install, verify and, if necessary, back out the upgrade. A VMware vSphere 6.0 Single Sign-On domain can be large. The Dell EMC approach for ELM with VMware vSphere 6.0 deployments considers the increased complexity for backup, recovery, and RCM upgrades. Deployment of AMP-2S is recommended for large SSO domains. The following table summarizes ELM with VMware vSphere 6.0 scalability with AMP-2S:

<table>
<thead>
<tr>
<th>Maximum number of PSCs</th>
<th>Maximum number of VMware vCenter servers</th>
<th>Maximum number of VxBlock or Vblock systems</th>
<th>Maximum number of Data Centers</th>
<th>Deploy ELM</th>
<th>Deploy AMP-2S in an SMP/VMP configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>&gt; 4</td>
<td>&gt; 4</td>
<td>&gt; 2</td>
<td>&gt; 2</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>
Configuring VMware Enhanced Linked Mode (vSphere 6.5U1)

Introduction to ELM (vSphere 6.5U1)

One of the advantages of a Dell EMC Converged System is delivery of a preconfigured physical and logical working system.

Converged Systems are physically and logically configured during the manufacturing process. If you have multiple Converged Systems, you can use Enhanced Linked Mode (ELM) with VMware vSphere 6.5U1 to log in to a single VMware vCenter server. You can then operate, manage, and maintain multiple VMware vCenter servers. Due to the installation prerequisites, VMware vSphere 6.5U1 ELM must be configured on the customer premises. If you want to configure ELM, contact Dell EMC Professional Services to have them perform the site analysis, installation, and configuration.

Scenarios include the following:

- Two or more VMware vCenter Servers that are linked to two Platform Service Controllers (PSCs) in one Converged System
- Two or more VMware vCenter Servers that are linked to two or more PSCs across two or more Converged Systems in a data center
- Two or more VMware vCenter Servers that are linked to two or more PSCs across two or more Converged Systems across two data centers

Deployment of ELM with VMware vSphere 6.5U1 cannot be reversed. ELM with VMware vSphere 6.5U1 is managed as a complete system and should be considered a fault, operational, and maintenance domain. Any ELM with VMware vSphere 6.5U1 configuration must use the same backup and restore processes as the PSCs and VMware vCenter servers in the SSO domain.

Using Enhanced Linked Mode 6.5

Use this link to obtain additional information about Enhanced Linked Mode:


VMware ELM with VMware vSphere 6.5U1 use cases

VMware ELM with VMware vSphere 6.5U1 can be used in several situations.

The following use cases are focused on a single pane of glass management:

- ELM with VMware vSphere provides a single interface to manage multiple VMware vCenter Servers using two shared VMware vSphere PSCs in the same Converged System.
- ELM with VMware vSphere is used to integrate VMware vCenter Management for five Converged Systems in the same data center. ELM with VMware vSphere 6.5U1 with five Converged Systems is an operational, fault, and management domain. Exceeding this limit is not supported. Each Converged System may have multiple VMware vCenter servers. Compute, network, and storage resources are not shared between the two or more discrete VMware vCenter servers that are located in each Converged System.
- ELM with VMware vSphere is used to integrate VMware vCenter Management for five Converged Systems in separate data centers. Exceeding this limit is not supported. Compute, network, and storage resources are not shared between the two or more discrete VMware vCenter servers that are located in separate data centers.
This configuration is similar to a configuration for two Converged Systems in the same data center, but introduces network latency.

Use AMP-2S with an SMP/VMP configuration to simplify VMware vSphere 6.5U1 management with more than two Converged Systems or VMware vCenter Servers.

Backup and recovery for ELM 6.5

See Backing up and restoring the vCenter Server and PSC (vSphere 6.5U1) in this guide.

Backup and recovery guidelines

Review the backup and recovery guidelines.

You can use the VMware Data Protection appliance for a direct-to-host emergency restore when VMware vCenter server is not available. See the VMware vSphere 6.5 Data Protection Administration Guide document for recommendations, limitations, and unsupported features:


With VMware vSphere 6.5U1, you cannot use PSC snapshots with multisite or HA configurations.

Use a tested backup and recovery solution for the VMware vSphere 6.5U1 PSCs and VMware vCenter servers. Without this configuration, do not proceed with a VMware vSphere 6.5U1 ELM configuration. ELM adds complexity to the backup and recovery solution. Factors include the number of PSCs, VMware vSphere 6.5U1 PSCs, and VMware vCenter servers, each of which have differences in their respective backup strategies.

Converged System AMP design (ELM/VMware vSphere 6.5U1)

This applies to AMP-2. Dell EMC manufacturing configures the AMP with VMware vSphere 6.5U1 using only VMware recommended topologies.

Deployment of the PSC and VMware vCenter server using a nonrecommended topology may prevent backing up and restoring a VMware vCenter server environment with a PSC.

VMware vSphere 6.5U1 Recommended Topologies


The following figure includes the following topology:

- One SSO domain
- One SSO site
- Two or more vCenter Servers with two external PSC in a single Converged System
The following figure includes the following topology:

- One SSO domain
- One SSO site
- One or more VMware vCenter Servers with two external PSC in two or more Converged Systems
The following figure includes the following topology:

- One SSO domain
- One or more SSO sites
- One or more VMware vCenter Servers with two external PSC in two or more Converged Systems across multiple sites

Each Converged System participating in ELM must continue to maintain a functioning AMP. To maintain the original Converged System premise of independence, each VMware vSphere environment must not rely on the VMware vSphere infrastructure of another Converged System to operate correctly. All VMware vSphere 6.5U1 management VMs in a Converged System must use the following:

<table>
<thead>
<tr>
<th>AMP type</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMP-2P M4</td>
<td>Local storage array</td>
</tr>
<tr>
<td>AMP-2S M4</td>
<td>Shared storage array</td>
</tr>
<tr>
<td>AMP-2S M4</td>
<td>Shared VNX-e storage array</td>
</tr>
</tbody>
</table>

External PSCs are required for VMware vSphere 6.5U1 ELM. Dell EMC does not recommend embedded VMware PSCs. Dell EMC recommends the deployment of the vCSA. However both the vCSA and VMware vCenter for Windows are supported with ELM. VMware vCenter 6.5 for Windows is not supported on Converged Systems.

After delivery and implementation, ensure that the AMP servers have network connectivity and sufficient resources to meet any additional workload.

Load balancers are not supported with the Converged System. During deployment, a VMware vCenter server must be associated with a local PSC. If a PSC fails, manually repoint the VMware vCenter server to a secondary PSC.
Standard VMware vSphere 6.5U1 design for a Converged System includes one VMware vCenter server and a minimum of two PSCs.

At minimum, ELM requires IP connectivity for the ESXi management VLANs between the Converged Systems joined in an ELM configuration. Verify the IP connectivity between the two VMware vSphere 6.5U1 vcesys_esx_mgmt VLANs. Also verify that all required protocols and ports are allowed on any firewalls between the two vcesys_esx_mgmt VLANs.

The following table provides the ports that are required between Converged Systems for ELM functionality:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
<th>Required For</th>
<th>Node to Node Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>389</td>
<td>TCP/UDP</td>
<td>Port 389 must be open on the local and all remote instances of VMware vCenter server. Port 389 is the LDAP port for the Directory Services for the VMware vCenter server group. If another service is running on this port, it might be preferable to delete it or change its port to a different port. You can run the LDAP service on ports from 1025–65535.</td>
<td>Windows installations and appliance deployments of PSC vCenter Server to PSC</td>
<td>VMware vCenter Server to PSC Platform Services Controller to PSC</td>
</tr>
<tr>
<td>2012</td>
<td>TCP</td>
<td>Control Interface RPC for vCenter Single sign-on</td>
<td>Windows installations and appliance deployments of PSC</td>
<td>PSC to PSC</td>
</tr>
<tr>
<td>2015</td>
<td>TCP</td>
<td>DNS Management</td>
<td>Windows installations and appliance deployments of PSC</td>
<td>PSC to PSC</td>
</tr>
</tbody>
</table>

See the following VMware KB article for additional information for VMware vSphere 6.5U1 communication port requirements:


Extend the QoS marking for the VMware vSphere 6.5U1 management traffic across any metro or WAN links connecting separate physical data centers.

VMware vSphere 6.5U1 ELM configurations must use consistent IP MTU sizes with physical and logical network switches and VMkernel ports.

**VMware ELM scalability planning (vSphere 6.5U1)**

Determine the number of PSCs and VMware vCenter servers that are needed for an ELM configuration with VMware vSphere 6.5U1 in an SSO Domain and site.

Complete an ELM scalability assessment to determine if the requested number of PSCs and VMware vCenter servers is compatible with VMware vSphere 6.5U1 configuration maximum limits. See the following link for the latest VMware vSphere 6.5U1 ELM configuration maximums:

https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.configmax.doc/GUID-BBD10A8B-7BDC-45F3-9CA4-C44EE77749BA.html

The following table provides the ELM with VMware vSphere 6.5U1 SSO configuration maximum limitations:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of linked VMware vCenter Servers per SSO domain</td>
<td>15</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Maximum number of PSCs per VMware vSphere domain</td>
<td>10</td>
</tr>
<tr>
<td>Maximum number of PSCs per site, behind a load balancer</td>
<td>4</td>
</tr>
<tr>
<td>PSC management Limits</td>
<td></td>
</tr>
<tr>
<td>One PSC</td>
<td>8 VMware vCenter Servers</td>
</tr>
<tr>
<td>Two PSCs</td>
<td>15 VMware vCenter Servers</td>
</tr>
<tr>
<td>Maximum number of VMware solutions that are connected to a single PSC</td>
<td>8</td>
</tr>
<tr>
<td>Each VMware vCenter server is considered a VMware solution.</td>
<td></td>
</tr>
<tr>
<td>Maximum number of VMware solutions in a VMware vSphere domain</td>
<td>15 (This number includes VMware vCenter Servers).</td>
</tr>
<tr>
<td>Each VMware vCenter Server is considered a VMware solution.</td>
<td></td>
</tr>
<tr>
<td>Maximum number of Converged Systems</td>
<td>5 (with 2 PSCs each)</td>
</tr>
</tbody>
</table>

Use the following guidelines when determining the maximum number of VMware vCenter Servers per SSO domain configuration:

- The number of linked VMware vCenter Servers defines the maximum number of VMware vCenter Servers that can be supported in an Enhanced Linked Mode (ELM) configuration. By definition, an ELM consists of a single SSO domain. You can have a maximum of 15 VMware vCenter Servers per SSO domain.
- Determine the maximum number of PSCs per VMware vSphere domain, which defines the maximum number of PSCs that can be part of a single SSO domain. You can have a maximum of 10 PSCs per SSO domain.

**Intra Converged System VMware ELM scalability planning (VMware vSphere 6.5U1)**

Determine the maximum number of VMware vCenter servers with ELM that can be configured in a Converged System configured with two PSCs.

- A standard Converged System configuration with two PSCs can have a maximum of 15 VMware vCenter servers. Half of the VMware vCenter servers point to the first PSC, while the second half point to the second PSC.

The following table defines the maximum number of compute hosts per Converged System:

<table>
<thead>
<tr>
<th>VxBlock System</th>
<th>Number of compute servers (half-width)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VxBlock 350</td>
<td>256</td>
</tr>
<tr>
<td>VxBlock 540</td>
<td>256</td>
</tr>
<tr>
<td>VxBlock 740</td>
<td>512</td>
</tr>
</tbody>
</table>

- AMP-2: Deployment of more than one VMware vCenter server per Converged System requires the deployment of a redundant AMP server with an external storage array. Each AMP server must be appropriately scaled to support multiple VMware vCenter servers.
- Scale all Converged System AMP, network, storage, and compute environment resources appropriately when deploying multiple VMware vCenter servers with their associated resources in a Converged System.
Inter Converged System VMware ELM scalability planning in a single physical data center (VMware vSphere 6.5U1)

Determine the maximum number of Converged Systems configured with VMware ELM and VMware vSphere 6.5U1.

Scenario 1: Each Converged System is deployed with two PSCs.

- A standard Converged System configuration with two PSCs can have a maximum of five Converged Systems. A minimum of one VMware vCenter server is required for each Converged System. The maximum number of VMware vCenter servers with ELM is limited to 15. Each of the five Converged Systems can support more than one VMware vCenter servers. In this configuration, you must maintain the Dell EMC VMware vSphere software Release Certification Matrix (RCM) consistently across all five Converged Systems. Periodically, monitor PSC replication sequence numbers to verify PSC synchronization.

- AMP-2S: Deployment of more than one VMware vCenter server per Converged System requires a redundant AMP server with an external storage array. Scale each AMP Server to support multiple VMware vCenter servers.

- Scale the entire Converged System AMP, network, storage, and compute environment resources when deploying multiple VMware vCenter servers with its associated resources in a Converged System.

Inter Converged System VMware ELM scalability planning with multiple physical data centers (VMware vSphere 6.5U1)

Determine the maximum number of Converged System that can be configured with ELM with VMware vSphere 6.5U1 in multiple physical data centers.

- Each VMware ELM with VMware vSphere 6.5U1 configuration requires a minimum of two PSCs per physical data center. If a primary PSC outage occurs, each VMware vCenter server can be repointed to the secondary PSC in the same physical data center. This approach maintains a consistent level of performance. A maximum of five physical data centers are supported with an VMware ELM configuration with VMware vSphere 6.5U1.

- A standard Converged System configuration with two PSCs supports a maximum of five Converged Systems with multiple physical data centers. Each Converged System requires a minimum of one VMware vCenter server. ELM has an upper limit of 15 VMware vCenter servers. In this configuration, each of the four Converged Systems can support more than one VMware vCenter servers. Maintain the Dell EMC VMware vSphere software Release Certification Matrix (RCM) consistently across all five Converged Systems that are distributed across physical data centers. Periodically, monitor PSC replication sequence numbers to verify PSC synchronization.

- Deployment of more than one VMware vCenter server per Converged System requires the deployment of a redundant AMP system. Each AMP system must be appropriately scaled to support multiple VMware vCenter servers.

- Scale all Converged System, AMP, network, storage, and compute environment resources when deploying multiple VMware vCenter servers and the associated resources in a Converged System.

VMware ELM deployment information (VMware vSphere 6.5U1)

When deploying VMware ELM, replicate roles, permission, licenses, tags, and policies across linked VMware vCenter servers.

⚠️ CAUTION For VMware vSphere 6.5U1, Dell EMC recommends the following:
- No higher than 150 milliseconds RTT between VMware PSCs at physically separate data centers
- No higher than 10 milliseconds RTT between VMware PSCs in a site

The legacy VMware vSphere Client does not support Enhanced Linked Mode.

With VMware vSphere 6.5U1, you cannot consolidate multiple SSO domains in each product line.

For VMware vSphere 6.5U1, Dell EMC does not recommend and does not support mixing embedded and external PSCs. A VMware vCenter server with an embedded VMware PSC is appropriate for small environments. You cannot join other VMware vCenter servers or VMware PSCs to this VMware vCenter Single Sign-On domain.

Dell EMC has made no assumptions regarding VMware vSphere vMotion support between VMware vCenter servers. Cold migration between VMware vCenter servers using a recommended L3 Provision network is possible.

Migration between VMware vCenter servers must meet the VMware requirements.

After you deploy ELM with VMware vSphere 6.5U1, verify PSC associations and replication status for all deployed PSC servers. See the following link for VMware vSphere 6.x:

Update PSCs sequentially. Each software upgrade of a PSC may take 30 minutes approximately.

If a PSC is decommissioned, do not reuse the original PSC name in the same SSO domain.

If Microsoft Active Directory is deployed as an authentication source, it must be configured consistently for all PSCs in the SSO domain.

Repointing a VMware vCenter server to a PSC is possible only under the following conditions:
- Two separate VMware vSphere 6.5U1 environments have been configured using the same SSO domain name and site name.
- The VMware vCenter server that you want to repoint is a replication partner of the existing PSC in the first VMware vSphere environment.

Deploy inter Converged System PSCs in a ring topology, whether they are located in the same physical data center or across multiple physical data centers.

See the following link for configuring a ring topology with VMware vSphere 6.5U1:

Repointing a vCenter server to a different PSC is limited to the same domain with VMware vSphere 6.5U1. See the following link for repointing with VMware vSphere 6.5U1 between External PSCs in a site (2113917):

**VMware ELM dependencies and limitations**

All PSCs and VMware vCenter servers participating in an ELM configuration must run the same software build number.

Although ELM enables the use of PSC, Vision Intelligent Operations or VxBlock Central does not support it. Vision Intelligent Operations or VxBlock Central continues to collect data from the vCenter servers directly.

Ensure that your configuration meets the following requirements:
- RCMs must be compatible between Converged Systems. VMware vSphere 6.5U1 PSCs and VMware vCenter servers must run the same build version.
- IP MTU sizes must be consistent between Converged Systems.
- Each Converged System requires a pair of PSCs.

When configuring IP connectivity between Converged Systems, you must verify IP connectivity between the two VMware vSphere 6.5U1 vcesys_esx_mgmt VLANs. Also verify that all required protocols and ports are allowed on any firewalls between the two vcesys_esx_mgmt VLANs.

See the following VMware KB article for additional information with VMware vSphere 6.5U1:

Dell EMC VxBlock™ and Vblock™ Systems 540 Administration Guide 155
All local and remote ELM with VMware vSphere 6.5U1 components require DNS and NTP support.

### Verify PSC and PSC Partner Status

Dell EMC recommends that each PSC have two partners in a ring topology and a single peer in a dual PSC deployment.

**About this task**

This task includes the following:

- Listing the PSC partners
- Displaying the PSC replication status

**Procedure**

1. Use SSH to connect to the PSC CLI and run the following commands to view and verify PSC partner servers:

   ```
   shell.set -enabled True
   shell
   cd /usr/lib/vmware-vmdir/bin
   ./vdcrepadmin -f showpartners -h localhost -u administrator
   ```

2. Use the following command to display replication status:

   ```
   ./vdcrepadmin -f showpartnerstatus -h localhost -u administrator
   ```

**Note:** Change numbers are used to maintain replication between adjacent PSCs. Each PSC uses a unique change number. Each PSC partner should be 0 changes behind.

### Determining the VMware vCenter server within a vSphere Domain

Complete this task to determine ownership of each vCenter server participating in the same VMware vSphere SSO domain.

**About this task**

This task shows how to determine ownership in the following ways:

- Using the GUI on VCSA
- Using VCSA CLI commands
- Using a Windows-based vCenter server

**Procedure**

1. Find ownership using the GUI on the VCSA as follows: Log in to the vCenter server. Under the **advanced settings**, review the property `config.vpxd.sso.admin.uri` which specifies the configured PSC.

2. Find ownership using VCSA CLI commands as follows:
   a. Use SSH to connect to the VCSA.
   b. Enter `shell.set -enabled True`.
   c. Enter `cd /usr/lib/vmware-vmafd/bin`.
d. Enter 

```
./vmafd-cli get-1s-location --server-name localhost
```

The command returns the PSC vCenter server used.

3. Find ownership on a Windows-based VMware vCenter server as follows: Enter

```
C:\Program Files\VMware \vCenter Server\vmafd\vmafd-cli get-1s-location --server-name localhost
```

The command returns the PSC vCenter server used.

**Reconfiguring the ring topology**

Complete this task to reconfigure the ring topology.

**Procedure**

1. Use SSH to connect to the PSC.
2. Enter `shell.set –enabled True`.
3. Enter `cd /usr/lib/vmware-vmdir/bin`.
4. Break the old partnership as follows:

   a. Use SSH to connect to the PSC CLI that you want to decommission and run the following commands to determine the `node-pnid` information: Stop all services.

   ```
   shell.set –enabled True
   shell
   cd /usr/lib/vmware-vmafd/bin
   ./vmafd-cli get-pnid --server-name localhost
   ```

   b. Run the following commands to determine the partner PSC servers:

   ```
   cd /usr/lib/vmware-vmdir/bin
   ./vdcrepadmin –f showpartners -h localhost –u administrator
   service-control --stop --all
   ```

   c. On one of the partner PSCs of the PSC that you want to decommission, run the following command to decommission the node:

   ```
   cmsso-util unregister --node-pnid <pscFQDN> --hostId <pscFQDN> --username administrator@vsphere.local
   ```

5. Use SSH to connect to one of the PSCs which you want to establish a partnership. Provide the FQDN of the peer PSC with which you want to establish partnership. Type

   ```
   ./vdcrepadmin -f createagreement -2 -h –server-name <Localhost> -u Administrator -H <PSC Name with which you want to create Partnership> -u Administrator
   ```

**VMware ELM references (vSphere 6.5U1)**

These references provide additional information about VMware ELM.

<table>
<thead>
<tr>
<th>Link</th>
<th>Topic title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2113917</td>
<td>How to repoint a VMware vCenter server 6.5 between External PSCs in a site.</td>
</tr>
<tr>
<td>2127057</td>
<td>Determining replication agreements and status with the VMware Platform Services Controller 6.5.</td>
</tr>
</tbody>
</table>
VMware ELM conclusions (VMware vSphere 6.5U1)

Conclusions for VMware ELM with vSphere 6.5U1 are provided.

VMware ELM with VMware vSphere 6.5U1 provides a single pane of glass management for the following in a Single Sign-On domain:

- Up to 10 VMware Platform Service Controllers (PSC)
- Up to 15 VMware vCenter servers

This single pane of management provides an operational improvement in managing multiple VMware vCenter Servers. As the number of VMware PSCs and vCenter servers increases, the size of the VMware vSphere 6.5U1 fault domain becomes larger.

Processes to back up and restore any VMware vSphere component participating in ELM must be reliable and supportable across Converged Systems and data centers. Maintaining synchronization of VMware PSC replication requires 100 percent network availability between PSCs in different Converged Systems or data centers. After a PSC outage, synchronization may take some time to occur.

As the size of the SSO domain increases, maintenance updates require more planning and coordination. VMware build numbers must be consistent in an ELM with VMware vSphere 6.5U1 configuration. Upgrading any Converged System in an ELM with VMware vSphere 6.5U1 configuration requires a corresponding upgrade for any other Converged Systems joined to the same VMware vSphere 6.5U1 SSO domain.

Perform upgrades in a maintenance window with time allocated to install, verify and, if necessary, back out the upgrade. A VMware vSphere 6.5U1 SSO domain may be large. The Dell EMC approach for ELM with VMware vSphere 6.5U1 deployments assesses the increased complexity for backup and recovery and RCM upgrades. The following table summarizes how ELM with VMware vSphere 6.5U1 scales with AMP:

<table>
<thead>
<tr>
<th>Maximum number of PSCs</th>
<th>Maximum number of VMware vCenter servers</th>
<th>Maximum number of VxBlock Systems</th>
<th>Maximum number of data centers</th>
<th>Deploy ELM</th>
<th>Deploy AMP-2S in an SMP/VMP configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>&gt;10</td>
<td>&gt;15</td>
<td>&gt;5</td>
<td>&gt;5</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>
Manage VMware Embedded Linked Mode (VMware vSphere 6.7)

One advantage of a Converged System is delivery of a preconfigured physical and logical working system. Converged Systems are physically and logically configured during the manufacturing process.

If you have multiple Converged Systems, you can use Embedded Linked Mode (ELM) with VMware vSphere 6.7 to log in to a single VMware vCenter. You can then operate, manage, and maintain multiple VMware vCenter servers. Due to the installation prerequisites, VMware ELM must be configured on the customer premises. If you want to configure ELM, contact Dell EMC Professional Services to have them perform the site analysis, installation, and configuration.

vCenter Embedded Linked Mode is enhanced linked mode support for vCenter Server Appliance with an embedded Platform Services Controller.

With vCenter Embedded Linked Mode, you can connect a vCenter Server Appliance with an embedded Platform Services Controller together to form a domain. vCenter Embedded Linked Mode is not supported for Windows vCenter Server installations.

Scenarios include the following:

- Two or more VMware vCenter Servers with Embedded Platform Service Controller in one Converged System
- Two or more VMware vCenter Servers with Embedded Platform Service Controller across two or more Converged Systems in a data center

Embedded Linked Mode is not supported across sites.

Deployment of ELM with VMware vSphere 6.7 cannot be reversed. ELM with VMware vSphere 6.7 is managed as a complete system and should be considered a fault, operational, and maintenance domain. Any ELM with VMware vSphere 6.7 configuration must use backup and restore processes compatible with the associated VMware vCenter servers in the Single Sign-On domain.

Configure VMware Embedded Linked Mode (VMware vSphere 6.7)

VMware vCenter Embedded Linked Mode (ELM) is enhanced linked mode support for vCenter Server Appliance with an embedded Platform Services Controller.

About this task

Use Embedded Linked mode with VMware vSphere 6.7 to log in to a single VMware vCenter server. You can then operate, manage, and maintain multiple VMware vCenter servers on multiple Converged Systems.

Converged Systems are physically and logically configured during the manufacturing process. Due to the installation prerequisites, VMware vSphere 6.7 ELM must be configured on the customer premises.

However, if multiple Converged Systems are ordered and the systems are not expected to join the existing customer domain, ELM can be configured during manufacturing. If you want to configure ELM, Dell EMC recommends that you have Dell EMC Professional Services perform the site analysis, installation, and configuration.

The following list outlines some of the guidelines for ELM in a VxBlock System:

- Linked VMware vCenter servers must be in the same SSO domain. If different SSO domains are required, linked mode is not possible.
- A single SSO domain must have no more than 8 linked VMware vCenter servers.

Note: Embedded Linked Mode is not supported across physical sites.
The following figure shows a topology with:

- A single SSO domain
- A single SSO site
- VMware vCenter servers with embedded PSC and two converged systems

![Diagram of Two VxBlock Systems – Single Site / SSO Domain](image)

The following figure shows a topology with:

- A single SSO domain
- A single SSO site
- VMware vCenter servers with embedded PSC and three converged systems

![Diagram of Three VxBlock Systems – Single Site / SSO Domain](image)

**Procedure**

1. Log in to the vCenter Server appliance and perform the following steps to create the replication agreement:
a. Log in to the vCenter management interface using root user: https://<vcenter_fqdn>:5480/. Select Access, then enable SSH and BASH shell.

b. SSH into vCenter as root. To log in to shell mode, type shell.

c. To verify the current replication partner, enter the following command:

   /usr/lib/vmware-vmdir/bin/vdcrepadmin -f showpartners -h <vCenter_IP_Address> -u administrator

d. To create a replication partner for the PSC, enter the following command:

   /usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement -2 -h <vCenter_IP_Address> -H <New Replication Partner IP Address> -u administrator

Deployment of ELM cannot be reversed. ELM is managed as a complete system and should be considered a fault, operational, and maintenance domain. Any ELM configuration must be compatible with backup and restore processes for the associated VMware vCenter servers in a single VMware vSphere SSO domain.
Manage VMware Embedded Linked Mode (VMware vSphere 6.5)

One advantage of a Converged System is delivery of a preconfigured physical and logical working system. Converged Systems are physically and logically configured during the manufacturing process.

If you have multiple Converged Systems, you can use Embedded Linked Mode (ELM) with VMware vSphere 6.5 to log in to a single VMware vCenter. You can then operate, manage, and maintain multiple VMware vCenter servers. Due to the installation prerequisites, VMware ELM must be configured on the customer premises. If you want to configure ELM, contact Dell EMC Professional Services to have them perform the site analysis, installation, and configuration.

vCenter Embedded Linked Mode is enhanced linked mode support for vCenter Server Appliance with an embedded Platform Services Controller.

With vCenter Embedded Linked Mode, you can connect a vCenter Server Appliance with an embedded Platform Services Controller together to form a domain. vCenter Embedded Linked Mode is not supported for Windows vCenter Server installations.

Scenarios include the following:

- Two or more VMware vCenters with Embedded Platform Service Controller in one Converged System
- Two or more VMware vCenters with Embedded Platform Service Controller across two or more Converged Systems in a data center
- Two or more VMware vCenters with Embedded Platform Service Controller across two or more Converged Systems across two data centers

Embedded Linked Mode is not supported across sites.

Deployment of ELM with VMware vSphere 6.5 cannot be reversed. ELM with VMware vSphere 6.5 is managed as a complete system and should be considered a fault, operational, and maintenance domain. Any ELM with VMware vSphere 6.5 configuration must use backup and restore processes compatible with the associated VMware vCenter servers in the Single Sign-On domain.

Configure VMware Embedded Linked Mode (VMware vSphere 6.5)

vCenter Embedded Linked Mode (ELM) is enhanced linked mode support for vCenter Server Appliance with an embedded Platform Services Controller.

About this task

Use Embedded Linked mode with VMware vSphere 6.5 to log in to a single VMware vCenter server. You can then operate, manage, and maintain multiple VMware vCenter servers on multiple Converged Systems.

Converged Systems are physically and logically configured during the manufacturing process. Due to the installation prerequisites, VMware vSphere 6.5 ELM must be configured on the customer premises.

However, if multiple Converged Systems are ordered and the systems are not expected to join the existing customer domain, ELM can be configured during manufacturing. If you want to configure ELM, Dell EMC recommends that you have Dell EMC Professional Services perform the site analysis, installation, and configuration.

The following list outlines some of the guidelines for ELM in a VxBlock System:

- Linked VMware vCenter servers must be in the same SSO domain. If different SSO domains are required, linked mode is not possible.
A single SSO domain must have no more than 8 linked VMware vCenter servers. 

Note: Embedded Linked Mode is not supported across physical sites.

The following figure shows a topology with:

- A single SSO domain
- A single SSO site
- VMware vCenter servers with embedded PSC and two converged systems

![Diagram](image_url)

- A single SSO domain
- A single SSO site
- VMware vCenter servers with embedded PSC and three converged systems

![Diagram](image_url)
**Procedure**

1. Log in to the vCenter Server appliance and perform the following steps to create the replication agreement:
   
   a. Log in to the vCenter management interface using root user: https://<vcenter_fqdn>:5480/. Select **Access**, then enable SSH and BASH shell.
   
   b. SSH into vCenter as root. To log in to shell mode, type `shell`.
   
   c. To verify the current replication partner, enter the following command:
      
      ```
      type: /usr/lib/vmware-vmdir/bin/vdcrepadmin -f showpartners -h <vCenter_IP_Address> -u administrator
      ```
   
   d. To create a replication partner for the PSC, enter the following command:
      
      ```
      /usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement -2 -h <vCenter IP Address> -H <New Replication Partner IP Address> -u administrator
      ```

Deployment of ELM cannot be reversed. ELM is managed as a complete system and should be considered a fault, operational, and maintenance domain. Any ELM configuration must be compatible with backup and restore processes for the associated VMware vCenter servers in a single VMware vSphere SSO domain.
Manage VMware Enhanced Linked Mode (VMware vSphere 6.x)

VxBlock Systems are physically and logically configured during the manufacturing process.

Due to the installation prerequisites, VMware ELM must be configured on site. To configure VMware ELM, contact Dell EMC Professional Services to have them perform the site analysis, installation, and configuration.

For multiple VxBlock Systems, use VMware Enhanced Linked Mode (ELM) with VMware vSphere to log in and manage a single VMware vCenter with VMware vCenter Servers.

The following VMware ELM scenarios are provided:

- Two or more VMware vCenter Servers that are linked to two VMware Platform Service Controllers (PSCs) in one Converged System.
- Two or more VMware vCenter Servers that are linked to two or more VMware PSCs across two or more VxBlock Systems in a data center.
- For VMware vSphere 6.7, two or more VMware vCenter Servers linked to two or more VMware PSCs across two or more Converged Systems across two data centers.

The following list outlines the requirements for VMware ELM in a VxBlock System 1000:

- A maximum of two Production VMware vCenter Servers in the default AMP-VX (four nodes)
- Up to eight linked VMware vCenter Servers are allowed in a single VxBlock System 1000 or across multiple VxBlock Systems 1000.
- A maximum of 625 hosts per linked VMware vCenter Server
- Linked VMware vCenter Servers must be in the same VMware SSO domain. If different VMware SSO domains are required, linked mode is not possible.
- If different SSO domains are required, you can have more than the maximum of eight VMware vCenter Servers.

Note: Linking the AMP-VX VMware vCenter Server and the VxBlock System VMware vCenter Server is not recommended.

You cannot reverse deployment of VMware ELM with VMware vSphere 6.7. VMware ELM with VMware vSphere 6.7 is managed as a complete system and should be considered a fault, operational, and maintenance domain.
must use the same backup and restore processes as the VMware vSphere PSCs and VMware vCenter servers in the SSO domain.

Deployment of ELM with VMware vSphere 6.5U1 cannot be reversed. ELM with VMware vSphere 6.5U1 is managed as a complete system and should be considered a fault, operational, and maintenance domain. Any ELM with VMware vSphere 6.5U1 configuration must be compatible with all associated VMware vSphere PSCs and VMware vCenter servers in a single VMware vSphere 6.5U1 Single Sign-On domain.

Related information
Use Enhanced Linked Mode

**Back up and restore VxBlock Systems with VMware Embedded Linked Mode (VMware vSphere 6.7)**

Use VMware vCenter server appliance (vCSA) native backup to back up and restore the VMware vCSA.

For backup and restore guidelines, see the following:

- File-based backup and restore of VMware vCenter Server Appliance
- Image-based backup and restore of a VMware vCenter Server environment

**VMware Enhanced Linked Mode scalability planning (VMware vSphere 6.7)**

Determine the number of PSCs and VMware vCenter servers that are needed for an ELM configuration with VMware vSphere in an SSO domain and SSO site.

The following table provides the ELM with VMware vSphere 6.7 SSO configuration for a VxBlock System. Dell EMC recommends these configuration limits to achieve eight linked VMware vCenter servers while maintaining N+1 redundancy for the PSCs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of linked VMware vCenter servers per SSO domain</td>
<td>8</td>
</tr>
<tr>
<td>Number of PSCs per VMware vSphere domain</td>
<td>5</td>
</tr>
<tr>
<td>Number of VMware vCenter servers pointing to a single PSC</td>
<td>2</td>
</tr>
<tr>
<td>Number of Converged Systems</td>
<td>8</td>
</tr>
<tr>
<td>Number of VMware vCenter servers per PSC: First – fourth VMware vCenter server</td>
<td>1</td>
</tr>
<tr>
<td>Number of VMware vCenter servers per PSC: Fifth – eighth VMware vCenter server</td>
<td>2</td>
</tr>
</tbody>
</table>
Intra Converged System VMware Enhanced Linked Mode scalability planning

Determine the number of VMware vCenter servers with ELM to configure in a Converged System.

- Based on a standard Converged System configuration with two PSCs, it is recommended to have a single VMware vCenter server in a standard Converged System.
- As more VMware vCenter servers are deployed into an ELM configuration, an extra PSC is deployed up to the sixth VMware vCenter server.
- The first four VMware vCenter servers are associated with the first four PSCs.
- The fifth through eighth VMware vCenter servers are associated with the first four PSCs as well.
- The fifth VMware PSC remains unassociated with a VMware vCenter server for quick repointing during failure and maintaining N+1 redundancy.
- Deployment of more than two VMware vCenter servers may require the deployment of more AMP servers.

VMware Enhanced Linked Mode deployment information

When deploying VMware ELM, replicate roles, permission, licenses, tags, and policies across linked VMware vCenter servers.

⚠️ CAUTION For VMware vSphere 6.7, Dell EMC recommends no higher than 10-ms RTT between VMware PSCs in a site.

With VMware vSphere, you cannot consolidate multiple SSO domains in each product line.

For VMware vSphere, Dell EMC does not support embedded and external PSCs. If VMware vCenter servers or VMware PSCs are deployed to their own SSO domain, you cannot join them to existing VMware vCenter SSO domains.

Dell EMC has made no assumptions regarding VMware vSphere vMotion support between VMware vCenter servers. Cold migration between VMware vCenter servers using a recommended Layer 3 provisioned network is possible.

Migration between VMware vCenter servers must meet the VMware requirements.

After you deploy ELM with VMware vSphere 6.7, verify PSC associations and replication status for all deployed PSC servers. See Determining replication agreements and status with the Platform Services Controller 6.X (2127057):
https://kb.vmware.com/s/article/2127057

Update PSCs sequentially. Each software upgrade of a PSC may take approximately 30 minutes.

If a PSC is decommissioned, do not reuse the original PSC name in the same SSO domain.

If Microsoft AD is deployed as an authentication source, configure it consistently for all PSCs in the SSO domain.

You can repoint a VMware vCenter server to a VMware PSC only when it is a replication partner of the existing VMware PSC.

Deploy inter-Converged System PSCs in a ring topology.

See Deployment Topologies with External Platform Services Controller Instances and High Availability for configuring a ring topology with VMware vSphere:

Repointing VC to a different PSC is limited to the same domain with VMware vSphere 6.7. See How to repoint VMware vCenter server 6.7 between External PSC in a site (2113917) for repointing with VMware vSphere 6.7:
VMware ELM dependencies and limitations

All PSCs and VMware vCenter servers participating in an ELM configuration must run software that has the same build number.

Ensure that your configuration meets the following requirements:

- RCMs must be compatible between Converged Systems. VMware PSCs and VMware vCenter servers must run the same build version.
- IP MTU sizes must be consistent between Converged Systems.

Although VMware ELM enables the use of VMware PSC, VxBlock Central or Vision software does not support it. VxBlock Central or Vision software continues to collect data from the VMware vCenter servers directly.

When configuring IP connectivity between Converged Systems, you must validate IP connectivity between the two VMware vSphere 6.7 vcesys_esx_mgmt VLANs. Also verify that all required protocols and ports are enabled on any firewalls between the two vcesys_esx_mgmt VLANs.

See Required Ports for vCenter Server and Platform Services Controller for additional information:

All local and remote ELM components require DNS and NTP support.

The following references provide additional information about VMware ELM:

- How to repoint a VMware vCenter server between External PSCs in a site
- Determining replication agreements and status with the VMware Platform Services Controller

VMware Enhanced Linked Mode references

References provide additional information about VMware ELM.

- How to repoint a VMware vCenter server between External PSCs in a site
- Determining replication agreements and status with the VMware Platform Services Controller

VMware Enhanced Linked Mode conclusions (VMware vSphere 6.7)

Conclusions for VMware ELM are provided.

Enhanced Linked Mode provides single pane of glass management for up to five PSCs and eight VMware vCenter servers in an SSO domain. It also provides simultaneous single pane of glass management for up to eight VMware vCenter servers. This single pane of glass management provides an operational improvement in managing multiple VMware vCenter servers. As the number of PSCs and VMware vCenter servers increase, the size of the VMware vSphere 6.7 fault domain becomes larger.

Processes to back up and restore any VMware vSphere component participating in ELM must be reliable and supportable across Converged Systems and data centers. Synchronization of PSC replication requires 100% network availability between PSCs in different Converged Systems or data centers. After a PSC outage, synchronization may take some time to occur.

As the size of the SSO domain increases, maintenance updates require more planning and coordination. VMware build numbers must be consistent in an ELM with VMware vSphere 6.7 configuration. Upgrading any Converged System in an ELM with VMware vSphere 6.7 also requires a corresponding upgrade for any other Converged Systems in the same VMware vSphere 6.7 SSO domain. Perform upgrades in a maintenance window with time that is allocated to install, verify, and, if necessary, back out of the upgrade. In a large VMware vSphere 6.7 SSO domain, the Dell EMC approach
for ELM with VMware vSphere 6.7 deployments assesses the increased complexity for backup, recovery, and upgrades.
Setting up VxBlock Systems to use VxBlock Central

Access the VxBlock Central dashboard

The VxBlock Central dashboard allows monitoring the health and compliance of systems, components, and specific elements of components.

**About this task**

Use a browser to access VxBlock Central. For more information about monitoring the health and compliance, click the Dashboard menu in VxBlock Central.

The dashboard supports a minimum screen resolution of 1280 x 1024.

**Procedure**

   
   **Note:** The MSM VM must be able to ping the FQDN of the Core VM. If it cannot, a host file entry for the Core VM must exist on the MSM VM.

2. Log in with the following default credentials:
   - Username: `admin`
   - Password: `D@ngerous1`

Set up a VxBlock System

The procedures in this section need to be performed only once.

**Accept the end user license agreement**

After the VxBlock System is delivered, accept the end user license agreement (EULA) on each VxBlock System in your environment to enable discovery and health polling.

**About this task**

VxBlock Central does not discover VxBlock System components or poll for health status until you accept the EULA.

To accept the EULA, you must run a command on the Core VM. You must specify EULA acceptance information such as a name, job title, licensee company, and accepting company.

Fields cannot exceed 500 characters or contain angle brackets, `< or >`.

**Before you begin**

Connect to the Core VM.

**Procedure**

1. Type: `startEulaAcceptance`

2. Scroll through the EULA until you are prompted to type a name.
3. Enter a name for EULA acceptance, and then press Enter.
4. Enter a job title, and then press Enter.
5. Enter the name of the licensee company, and then press Enter.
6. (Optional) Enter the name of the accepting company, and then press Enter.
   If you do not specify an accepting company, the value defaults to the licensee company.
7. Enter yes to accept the EULA.

**Reset and reaccept end user license agreement**
Reset the End User License Agreement (EULA) for administrative changes. Reaccept the EULA after reset.

**About this task**
Reaccept the EULA after reset to enable the discovery and health polling.

**Procedure**
1. To reset EULA, perform the following:
   a. Enter: `/opt/vce/fm/bin/resetEulaAcceptance`
   b. When prompted, enter yes.
2. To reaccept EULA, perform the following:
   a. Enter: `startEulaAcceptance`
   b. Scroll through the EULA until you are prompted to enter a name.
   c. Enter a name for EULA acceptance, and then press Enter.
   d. Enter a job title, and then press Enter.
   e. Enter the name of the licensee company, and then press Enter.
   f. Enter the name of the accepting company, and then press Enter.
      If you do not specify an accepting company, the value defaults to the licensee company.
   g. Enter yes to accept the EULA.

**Start VxBlock System discovery**
After you configure the VxBlock System configuration file, start the discovery process to connect the Core VM to VxBlock System components.

**Note:** For VxBlock Central Version 2.0 and later, add, configure, and discover Converged Systems using the VxBlock Central user interface. See *Discover Converged Systems* online help for more information.

Follow the *Simplified VxBlock Central configuration* procedure.

**Before you begin**
- Accept the end user license agreement (EULA).
- Configure the `vblock.xml` file or the VxBlock System configuration.
- Enable northbound communication using SNMP.
- Connect to the Core VM.

**Procedure**
1. Type: `startFMagent`
2. After 15 minutes, check FMAgent.log to determine if discovery is complete.
3. To confirm, type:
   ```
   cd /opt/vce/fm/logs/
   grep -i 'current status' FMA* | grep 100 | grep discoverAll
   ```
4. Open a web browser and go to https://fqdn:8443/fm/systems where FQDN is the fully qualified domain name of the Core VM.
5. Authenticate to the Central Authentication Service (CAS) service.

### Update the Windows Registry

Before configuring application hosts on the Core VM, update the Element Manager with new registry keys to enable Windows Management Instrumentation (WMI) support.

**About this task**

Each application host is a Windows-based VM on an AMP with one or more of the following management software applications:

- Navisphere CLI
- PowerPath/ Electronic License Management Server
- Unisphere Client
- Unisphere Server
- Unisphere Service Manager
- SMI-S Provider

**Note:** If you previously updated the registry keys to configure applications hosts, you do not need to update them again.

**Procedure**

1. As a local administrator, connect to the Element Manager VM.
2. To start the Registry Editor, type: `regedit`
3. Search for HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}.
4. Right-click the key, and select Permissions.
5. On the Permissions window, click Advanced.
7. In the Select User or Group window, from the From this location field, ensure that the location is your local computer.
8. From the Select User or Group window, enter Administrator in the Enter the object name to select field to change the owner. Click OK > OK.
9. From the Permissions window, select the Administrators group and select Full Control and click OK.
10. Right-click key HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}.
    **Note:** Ensure that brackets are included.
11. Select New > String value and type AppID for the name. Right-click and modify the AppID. Set the value to {76A64158-CB41-11D1-8B02-00600806D9B6}.
Set the Owner and Permissions back to the original settings:

a. Right-click HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}, and select Permissions.

b. Remove the Full Control permissions for the Administrators group.

c. Click Advanced, and select Change.

d. In the Select User or Group window, from the From this location field, ensure that the location is your local computer.

e. From the Select User or Group window, type NT Service\TrustedInstaller in the Enter the object name to select field. Click OK > OK > OK.

13. Search for key HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\AppID.

14. Right-click the key, and select New > Key, and type {76A64158-CB41-11D1-8B02-00600806D9B6}.

15. Right-click the new key, and select New > String value. Type DllSurrogate for the name and leave the value empty.

Update the IP address tables on the Core VM (optional)

Run a script to parse the vblock.xml file and update the IP address tables so that VxBlock Central does not block traffic from Converged System components. The vblock.xml file is available in /opt/vce/fm/conf.

Procedure

1. To parse the vblock.xml and update IP address table rules to include the IP addresses of Converged System components, type: /opt/vce/fm/bin/runConfigCollector -iptablesOnly

2. To confirm the IP addresses for Converged System components are in the IP address table rules, type: iptables -L

Plan a multisystem clustered environment

Sizing guidelines are provided to plan a multisystem clustered environment.

If your deployment configuration exceeds these guidelines, the system performance degrades and the MSM VM cluster may be unsupported.

When planning an MSM VM cluster deployment, ensure that the topology (including the data centers and VxBlock System involved) is well defined.

VMs are used to provide features and functionality for VxBlock Central. The following table provides an overview of VxBlock Central VMs:

<table>
<thead>
<tr>
<th>VM</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core</td>
<td>Discovers and gathers information about the inventory, location, and health of the VxBlock System</td>
</tr>
<tr>
<td>MSM</td>
<td>Provides functions to manage multiple VxBlock Systems</td>
</tr>
<tr>
<td>MSP (optional)</td>
<td>In a data center environment, one MSM VM can be associated with up to 8 Core VMs.</td>
</tr>
<tr>
<td>MSP (optional)</td>
<td>Provides functions for RCM content prepositioning</td>
</tr>
</tbody>
</table>

VxBlock Central includes the Core VM and the multisystem management (MSM) VM as a minimum configuration. For prepositioning, deploy and configure the multisystem prepositioning (MSP) VM as part of the installation process.
### Single-site and multisite environments

If the VxBlock System has AMP resources to support the Core VM and MSM VMs, cluster multiple MSM VMs together, instead of mapping multiple Core VMs to a single MSM VM.

In single-site cluster deployments, where three MSM VM nodes are supported, the failure of a single MSM VM node does not negatively impact read/write operations in the environment. A minimum of two MSM VM nodes should be operational to prevent data consistency problems.

In multisite cluster deployments, where two MSM nodes are supported, the failure of a single MSM node can impact read/write operations in that particular site only. There is no fault tolerance. If there is a network connectivity failure between the sites, this failure could negatively impact operations on all sites.

The following sizing restrictions apply to single-site and multisite configurations:

- **In a single-site environment:**
  - Associate an MSM VM with up to two Core VMs.
  - You can run up to three MSM VMs in a data center.
  - You can associate up to two Core VMs with an MSM VM.

- **In a multisite environment,** each data center may have no more than two MSM VMs running. Each MSM VM is associated with up to two Core VMs.
  - You can configure a cluster that includes a maximum of three data centers.
  - You can have up to two MSM VMs in each data center.
  - You can associate each MSM VM with up to two Core VMs.

### Latency

WAN latency is defined as the latency between data centers in multiple data center deployments. LAN latency is defined as the latency between MSM VM nodes within a data center.

The following latency restrictions apply:

- In a three data center deployment, do not exceed 100 milliseconds of WAN latency between data centers.
- In a two data center deployment with two MSM VM nodes, and four Core VMs, you can have up to 300 milliseconds of WAN latency.
- In a single-site environment, do not exceed 25 milliseconds of LAN latency between two MSM VM nodes in a data center.

### VxBlock Systems

The following sizing guidelines apply to VxBlock Systems in a clustered environment:

- If you configure an MSM VM cluster in a three data center deployment, you can have up to 12 VxBlock Systems in the cluster.
- You can have up to two VxBlock Systems in a node with a maximum of one VMAX per MSM VM node. You can attach one Fabric Technology Extension in the two system node. A VMAX Storage Technology Extension or Fabric Technology Extension is not recommended on a VxBlock System with VMAX storage.
- The reference deployment contains a VMAX system with 5000 storage volumes and 390 disks. If your VMAX exceeds 5000 storage volumes and 390 disks, MSM VM cluster performance may be degraded. Reduce the total number of Core VMs in the deployment.

### Simultaneous users

Dell EMC recommends a maximum of three simultaneous users per MSM node.

### LDAP configuration

In a large data center environment that spans multiple geographical locations, the AD configuration is replicated to all locations. To prevent MSM VMs from crossing geographical lines to perform AD look ups, use local DNS practices. Doing so ensures that each node can access the local AD server for look ups.
The total number of groups an LDAP user belongs to impacts system response time.

**CPU**

If performance degrades, increase the number of CPU cores. The default number of cores on the MSM VM is four.

### Associate a Core VM with an existing MSM VM

Associate a Core VM with an existing MSM VM after initial deployment. You can also add a Core VM after an MSM VM cluster is created.

**About this task**

**Note:** For VxBlock Central Version 2.0 and later, add, configure, and discover Converged Systems using the VxBlock Central user interface. See Discover Converged Systems online help for more information.

MSM VM provides the `addSlibHost.sh` wrapper script to add the IP address of a Core VM to an MSM VM. In a single system environment where one Core VM is mapped to a single MSM VM, only run the `addSlibHost.sh` script under the following conditions:

- The Optional Initial System Library IP(s) OVF property is not configured.
- The property is configured, and there are failures when adding the Core VM on MSM VM first boot.

To ensure that your environment can successfully add a Core VM to an existing MSM VM, run precheck by typing:

```
/opt/vce/multivbmgmt/install/addSlibHost.sh -p IP_address
```

The `-p` option runs the precheck but does not add the Core VM to the MSM VM.

When you associate a Core VM to an MSM VM, do not perform any operations on that Core VM from any other MSM VMs, until the association is complete.

The script verifies that the IP address has a valid format. If the IP address is valid, the script imports the `vblock.xml` file and then imports the credentials.

If your Core VM is already associated with your MSM VM, ensure the Core VM is configured to use NTP. To configure the Core VM to use NTP, type:

```
/opt/vce/multivbmgmt/install/addSlibHost.sh -n IP_address
```

Where the IP address is the server for which you want to set the time. The `-n` option sets up the NTP on the Core VM, but does not add it to the MSM VM.

**Before you begin**

- You can associate up four VxBlock Systems with an MSM VM.
- Take a snapshot of each MSM VM within the cluster.
- Ensure the firstboot script has completed successfully on the MSM VM where you are adding the Core VM. The subsequent boot script must not be in progress. To access the logs, go to `/opt/vmware/var/log/firstboot` and `/opt/vmware/var/log/subsequentboot`.

**Note:** The `addSlibHost` script performs checks on the previous criteria. If your environment does not meet the criteria, the `addSlibHost` script displays the failure and does not allow the Core VM to be added.

To ensure that discovery is complete, open a web browser and go to: `https://{FQDN}:8443/fm/vblocks`, where `FQDN` is the fully qualified domain name of the Core VM.

**Procedure**

1. To add the Core VM to an existing MSM VM, type:

   ```
   /opt/vce/multivbmgmt/install/addSlibHost.sh IP_address
   ```
2. Check the /opt/vce/logs/multivbmgmt/addSlibHost.log file if you encounter any problems adding hosts. It may take up to 30 minutes before the data is available.

Form a cluster of MSM VMs

The initial MSM VM deployment configures a single VM. After deploying multiple MSM VMs, you can form a cluster of several nodes where each node is a separate MSM VM. The seed node is the first MSM VM in the cluster.

About this task

Configure a cluster for a single site or multisite environment. If configuring a cluster for a single site environment, MSM VMs are in the same data center. For a multisite environment, the MSM VMs are in different data centers. You can mix various types of VxBlock Systems in a single site or multisite clustered environment.

Add MSM VMs to a cluster one at a time, each time joining the same seed node. You cannot join existing clusters together. After an MSM VM has been added to a cluster, it cannot be deleted from the cluster.

Before you begin

- Ensure all MSM VMs for the cluster you want to join are deployed, powered on, and configured.
  - Take a snapshot of each node before clustering, and after each node is successfully added to the cluster.
  - The FQDN for each Core VM, MSM VM, and MSP VM must not contain underscores or other special characters. Only hyphens and periods are accepted as special characters.
  - The data center names and cluster name in an MSM VM must begin with an alphanumeric character, and can contain numbers, letters, and underscores. Use up to 255 characters.
- If configuring a cluster for a single-site environment, ensure that the data center name is the same for all nodes in the cluster. Verify the capitalization.
  
  Note: Data centers with the same name but different capitalization, for example, Cork_DC on MSM VM 1 and Cork_Dc on MSM VM 2, initiate multiple data center clustering.

- If configuring a cluster for a multisite environment, ensure that each site has a unique data center name. In each site, ensure all MSM VMs use the same data center name.
- Ensure that the cluster name is the same across all MSM VMs in the cluster and across all sites.
  
  Note: The data center names and cluster name cannot be changed after you power on the VMs. To change the data center names or the cluster name, redeploy all the VMs in the cluster.
- In a multisite clustered environment, change your firewall rule to open ports 7000, 7001, and 7199, as these ports are used for Cassandra node-to-node communication.
- Ensure that the MSM VMs that join to the cluster have the same MSM VM CAS password.

Procedure

1. To add a node to the cluster:
   a. Use DNS recommended practices to ensure the FQDNs for all MSM VMs and Core VMs are resolvable across all data centers.
      
      Note: From each MSM VM, be able to resolve the FQDN of any of Core VMs that have been added, regardless of which MSM VM it was added to.

   b. For all nodes in the cluster, including the node that is being added, type:

   /opt/vce/multivbmgmt/install/docompact_schemas.sh 1000 30
The first parameter of 1000 specifies the threshold of open files that are allowed in Cassandra before compaction begins. If the total number of files open in Cassandra is greater than the value of this parameter, compaction begins.

To check the total number of open files, type:

```
lsoc -n | grep 'cassandra' | wc -l
```

**Note:** The value for the first parameter must not exceed the `Max open files` limit set for Cassandra. The value of 1000 work for most environments, since the standard configuration for Cassandra sets the `Max open files` limit to 4096.

The second parameter of 30 for the script specifies the waiting time in seconds before compaction starts.

c. On any node that is being clustered to disable the repair cron jobs, enter the following command:

```
/opt/vce/multivbmgmt/install/cassandra_cluster_maintenance.sh --cron-enable-repair SEED_IP,JOINING_IP
```

Where:
- `SEED_IP` is the IP address for the seed node in the cluster. All joining nodes must specify the same seed node.
- `JOINING_IP` is the IP address for the node that is joining the cluster.

**Note:** If you have multiple `JOINING_IP` addresses, include them all and separate them by commas.

d. On the seed node in the cluster, type:

```
cat /opt/vce/credential-management/deploy/conf/AOtRN.dat
```

e. For the next MSM VM to add to the cluster, type:

```
/opt/vce/multivbmgmt/install/joinMSMCluster.sh -k KEY -s SEED_IP -v
```

Where:
- `KEY` is the Credential Manager key for the seed node in the cluster you want to join. You can copy and paste the key value that was retrieved earlier.
- `SEED_IP` is the IP address for the seed node in the cluster. All joining nodes must specify the same seed node.

**Note:** Before clustering, some MSM VMs may be configured to use different Active Directory servers. However, after these nodes are added to a cluster, they must use a single AD server instance. When you add an MSM VM to an existing cluster, the join script replicates the configuration data from the seed node to each joining node. The script discards the configuration data from the joining node. If you want to preserve a particular Active Directory user configuration, use an MSM VM node with that configuration as the seed node.

- `-v` runs the script in verbose mode, which sends extra messages on the console terminal.

If you omit any required parameter, the script prompts for the parameter value.

f. Respond to the command prompts for any required parameters that are not specified when the `joinMSMCluster.sh` script was initiated.

g. Type the root and passwords to set up the SSH keys for the machine.

If you have not connected to that host before, you are prompted for the root password for the seed node.
h. Verify configuration settings. If all settings look correct, type y to continue. If not, type n and run the script again with the correct settings.

Ignore any warnings that may be displayed. The join process may take several hours, depending on the amount of data you have and how many nodes are being clustered.

i. Wait for successful completion of the clustering configuration before joining more nodes to the cluster.

If the clustering configuration does not complete successfully, revert each of the MSM VMs and address the issues that caused the errors. This reversion may be necessary if a VM goes down in the middle of the clustering process, since the cluster is left in an inoperable state. After errors have been corrected and verified, recover the MSM VMs and retry clustering. You do not need to revert the Core VMs for a clustering error.

**Note:** If you encounter any problems during the join process, see the `/opt/vce/logs/multivbmgmt/joinMSMCluster.log` file.

j. To confirm that the cluster is configured correctly, on the seed node, type:

```
/opt/cassandra/bin/nodetool status
```

The Cassandra node tool checks that all clustered MSM VMs are in UN (up and normal) state.

k. To add the repair cron jobs back to the seed node, type:

```
/opt/vce/multivbmgmt/install/cassandra_cluster_maintenance.sh --cron-enable-repair SEED_IP
```

Where:

- `SEED_IP` is the IP address for the seed node in the cluster.

l. To clean up all nodes in the cluster, type:

```
/opt/cassandra/bin/nodetool cleanup
```

**After you finish**

After adding an MSM VM to an existing cluster, log in to the VxBlock Central for each VM. Verify that the data is the same on each VM in the cluster.

After clustering, if you change the MSM VM CAS password on one of the MSM VMs in the cluster, to change the password on other nodes in the cluster. Update the CAS password on the MSP VM to match the CAS password on the MSM VM.

### Remove a Core VM from an MSM VM

Remove a Core VM from an MSM VM. The MSM VMs can be either clustered or not clustered.

**About this task**

**Note:** For VxBlock Central Version 2.0 and later, add, configure, and discover Converged Systems using the VxBlock Central user interface. See `Discover Converged Systems` online help for more information.

The `removeSlibHost` script deletes the following information about the Core VM from the MSM VM:

- MSM Collector configuration files
- Cassandra database
- Titan database
- Elasticsearch database

---

Dell EMC VxBlock™ and Vblock™ Systems 540 Administration Guide

178
VxBlock System credentials

Remove each Core VM from an MSM VM one at a time. No operations can be performed on that Core VM from any other MSM VMs until the removal is complete.

You can delete one Core VM from an MSM VM after a cluster with one or more MSM VMs has been formed. Remove the Core VM from the MSM VM to which it was originally added.

If a Core VM was deleted from an MSM VM, you can add the Core VM back to the same MSM VM. The data from the original Core VM is not restored, but new data is collected.

Procedure

1. To delete the Core VM from the MSM VM, type:

   ```
   /opt/vce/multivbmgmt/install/removeSlibHost.sh IP address
   ```

   Where `IP address` is the IP address of the Core VM that you want to delete.

2. To verify the Core VM was deleted from the MSM VM, on the MSM VM from which you deleted the Core VM, type:

   ```
   /opt/vce/multivbmgmt/install/listSlibNodes.sh
   ```

Shut down and take a snapshot of the MSM cluster

Locate the seed MSM VM node, shut down the MSM VM cluster, and recover a system.

Before you begin

Record the order that you shut down the MSM VM nodes.

Procedure

1. To find the seed node, start an SSH session to any MSM VM in the cluster and type:

   ```
   grep seeds: /opt/cassandra/conf/cassandra.yaml
   ```

   The IP address in the output is the IP address of the seed node.

2. Power off each MSM VM in the cluster, ensuring to power off the seed node last:

   a. Using VMware vCenter, individually shut down the nodes in the MSM VM cluster. Use five minute intervals to allow time for RabbitMQ to react to the MSM nodes being shut down.

      ```
      Note: If the seed node is powered off last, the order in which you shut down the nodes does not matter. Be sure to record the order.
      ```

   b. Take a snapshot of all the nodes in the MSM cluster.

After you finish

Recover your clustered environment. To recover your system after you take a snapshot, see Recover the MSM cluster.

Related tasks

Recover the MSM cluster on page 179

Recover the MSM cluster

Restore an MSM cluster using the VMware vSphere Client. Restore when an error occurs when joining nodes to the cluster or when the connectivity for one of the MSM nodes in the cluster is down.

About this task

Perform this task only during the upgrade process.
Power on MSM nodes in the reverse order that they were powered off, starting with the seed node.

Before you begin
Verify the order that the MSM nodes were powered off. If the order is unknown, begin with the MSM nodes in the seed node of VMware vCenter.

Procedure
1. Power on the MSM seed node using the VMware vCenter vSphere Client. Open a console connection to the VM, and wait for the login prompt.
2. Perform the following steps for each MSM node in the same data center in the reverse order from shutdown:
   a. Power on the next MSM node using the VMware vCenter vSphere Client. Continue powering on each MSM node in the cluster in five minute increments.
      Repeat the recovery process for every MSM node in each data center of your clustered environment.
   b. After all the MSM nodes in all data centers are powered back on, on each of the MSM nodes in the clustered environment, type:
      
      service tomcat restart
   c. To check the services, type:
      
      vision start
   d. To monitor the status of the cluster, type:
      
      /opt/cassandra/bin/nodetool status
   e. After all MSM nodes are up and running in the same data center, verify that the IP address of each data center MSM node is displayed. Type:
      
      rabbitmqctl cluster_status
3. After all the nodes in all data centers are powered on, perform the following:
   a. Check the VxBlock Central dashboard to ensure you can view your Converged Systems. If not, to restart the Tomcat service, type:
      
      service tomcat restart
   b. Check the Compliance and Remediation of the VxBlock Central dashboard to ensure that the compliance status is displayed. If not, type:
      
      service vision-mvb-compliance restart

Verify ElasticSearch if the MSM VM is changed

After the OVA for MSM VM is deployed, ElasticSearch is installed and configured. ElasticSearch is a distributed search server that provides a full-text search engine and is included with MSM VM.

About this task
Verify the ElasticSearch configuration if you modify the MSM VM environment by including more VMs in the cluster. The elasticsearch.yml configuration file is configured automatically during OVA deployment. No additional changes to the configuration should be needed. However, you should verify the configuration by looking at the contents of the /etc/elasticsearch/elasticsearch.yml file.

Verify the following properties within the elasticsearch.yml file:
- The cluster.name property is set to the value of the Cluster Name OVA property.
- The node.name property is a short hostname that is based on the configured FQDN.
- The discovery.zen.ping.multicast.enabled property is set to false.

**Procedure**

1. Display the contents of the /etc/elasticsearch/elasticsearch.yml file, and review the properties.
2. If you want to restart the Elasticsearch service, enter the following command:
   ```bash
   sudo service elasticsearch restart
   ```

**Discover, decommission, or modify a component**

**Add Isilon Technology Extension on a VxBlock System**

Add a Cisco Nexus switch to support the Isilon array.

**About this task**

**Note**: For VxBlock Central Version 2.0 and later, add, configure, and discover Converged Systems using the VxBlock Central user interface. See Discover Converged Systems online help for more information.

**Before you begin**

Deploy the Core VM and MSM VM.

**Procedure**

1. Start an SSH session to the Core VM.
   **Note**: Use PuTTY to access the configuration editor for Windows-based systems as non-VSCII supported terminals display incorrectly.

2. Log in to the Core VM.
3. If configuring an existing VxBlock System in /opt/vce/fm/conf, type `configTool.sh --multiple-switch` to load the existing configuration file.
4. Follow the prompts and change attribute information for the VxBlock System.
5. When the script prompts you to add switches, type 0 to include more switches in the configuration.
6. Type the number of switches that you want to add.
7. When the script prompts you to change the IP address to the switch IP address and configure properties for the switch, type one of the following:
   - 0 to continue to the next step.
   - 1 to change the community.
   - 2 to set the password. You must set the password.
   - 3 to change the username.
   - v to validate the information.

8. Complete the prompts as necessary.
After you finish

1. View the VxBlock System configuration file.
2. To restart the FM Agent services from the Core VM, type:
   ```
   stopFMAgent
   startFMAgent
   ```
3. Log in to the VxBlock Central and search for `switch`. `n<x>k` is displayed under the **Model Name**.

Related reference

Configuration editor component reference on page 243

Add a component with the configuration editor

Use the configuration editor to add new components to the VxBlock System configuration.

About this task

**Note:** For VxBlock Central Version 2.0 and later, add, configure, and discover Converged Systems using the VxBlock Central user interface. See Discover Converged Systems online help for more information.

VxBlock Systems are template-based. Components can only be added if they are supported in the template.

Add the following component types to the system configuration:

<table>
<thead>
<tr>
<th>Component types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rack</td>
<td>Panduit Rack</td>
</tr>
<tr>
<td>Storage</td>
<td>The storage array component is supported on a VxBlock System. VxBlock Central does not support the use of a single ECOM server (Element Manager) IP address for multiple storage arrays. Specify a different ECOM server IP for each additional storage array you want to add.</td>
</tr>
<tr>
<td>Switch</td>
<td>Available for VxBlock Systems</td>
</tr>
<tr>
<td>Cisco DCNM</td>
<td>Available for VxBlock Systems</td>
</tr>
<tr>
<td>VMware vCenter</td>
<td>The <code>&lt;url&gt;</code> attribute of VMware vCenter, specified in the configuration file, must be in the form of an IP address. VxBlock Central discovers the IP address.</td>
</tr>
<tr>
<td>Storage virtualizer</td>
<td>Available for VxBlock Systems.</td>
</tr>
<tr>
<td>Application host</td>
<td>The application host component is supported on a VxBlock System.</td>
</tr>
</tbody>
</table>

Before you begin

Configure the VxBlock System. See Configuration editor component reference for component information.

Procedure

1. To open the configuration editor, type:
   ```
   configSystem edit
   ```
2. Select **Add** in the **Configuration Editor** dialog.
3. Select the component type that you want to add and click **Enter**.
4. Select **Add**.
   a. In the configuration editor dialog, use the **Next** and **Back** options to go to the component you want to edit.
   b. Click **Tab** or use the arrow keys to go to the specific component property you want to edit.
c. Select the Backspace key or the Delete key to edit the property fields.

5. Select Save or Cancel to exit the configuration editor without saving your changes.

After you finish

To restart the FM Agent services from the Core VM, type:

stopFMagent

startFMagent

Add eNAS to VMAX3 storage

Add embedded Network Attached Storage (eNAS) to VMAX3 to deploy one infrastructure to manage block and file resources. Add eNAS properties to an existing VMAX3 storage array on a VxBlock System using the configuration editor.

About this task

Note: For VxBlock Central Version 2.0 and later, add, configure, and discover Converged Systems using the VxBlock Central user interface. See Discover Converged Systems online help for more information.

Before you begin

Deploy the Core VM and MSM VM.

Procedure

1. Start an SSH session to the Core VM.

   Note: Use PuTTY to access the configuration editor for Windows-based systems as non-VSCI supported terminals display styling incorrectly.

2. Log in to the Core VM.

3. To launch the configuration editor, type:

   configSystem edit

4. Use Next to go to the VMAX storage array and select Add.

5. Select Extra properties for selected component > Add.

6. In the Which field, type eNAS. The value for the Which field is case-sensitive.

7. In the Method field, type the IP address of eNAS.

8. In the Username field, type the username.

9. In the Password field, type the password.

   You do not need to enter a community string.

10. Select Save or Cancel to exit the configuration editor without saving your changes.

After you finish

1. View the vblock.xml file and verify that eNAS is contained under storage.

2. To restart the FM Agent services from the Core VM, type:

   stopFMagent

   startFMagent

3. Log in to VxBlock Central and search for eNAS.
Edit component credentials in the system.cfg file

Using an input file, you can change the credentials for VMware vCenter, compute server, network switch, and the storage component in the system.cfg file.

About this task

**Note:** For VxBlock Central Version 2.0 and later, add, configure, and discover Converged Systems using the VxBlock Central user interface. See Discover Converged Systems online help for more information.

Procedure

1. Use vi editor to open the input file.
2. For example, to change the IP address of VMware vCenter and the community, copy and paste the following lines to the input file:

   ```
   vcenters.vcenter[2].url=192.192.179.00
   compute.server[1].credentials.community=L0KI@123
   ```
3. To run the script, type: `./componentcredentialmanager.sh`

Edit component properties with the configuration editor

Modify various component properties on a VxBlock System.

About this task

**Note:** For VxBlock Central Version 2.0 and later, add, configure, and discover Converged Systems using the VxBlock Central user interface. See Discover Converged Systems online help for more information.

Edit the following component properties:

- IP address
- Username
- Password
- Community string
- Method

**Note:** Depending on the method and component type, this value can be lower case or mixed case. Most fields have case-sensitive values.

Sensitive information such as passwords and community strings are masked in the configuration editor and encrypted in the configuration file.

Before you begin

Configure the VxBlock System.

Procedure

1. To open the configuration editor, type: `configSystem edit`.
2. Follow these steps to edit the component properties:
   a. In the configuration editor dialog, use the **Next** and **Back** options to go to the component you want to edit.
   b. Click **Tab** or use the arrow keys to go to the specific property you want to edit.
   c. Click **Backspace** or **Delete** to edit the properties.
3. Select **Save** or **Cancel** to exit the configuration editor without saving your changes.
The configuration editor uses the `system.cfg` to create (or update) an `vblock.xml` file.

**After you finish**
To restart FM Agent Services from the Core VM, type:

```
stopFMagent
startFMagent
```

**Related reference**

- [Configuration editor component reference on page 243](#)

---

### Delete a component with the configuration editor

Use the configuration editor to delete components from the VxBlock System configuration.

**About this task**

**Note:** For VxBlock Central Version 2.0 and later, add, configure, and discover Converged Systems using the VxBlock Central user interface. See *Discover Converged Systems* online help for more information.

**Before you begin**

Ensure that you have configured the VxBlock System.

**Procedure**

1. To open the configuration editor, type:
   ```
   configSystem edit
   ```

2. Use **Next** and **Back** to go to the component type to delete in the VxBlock System.

3. Select **Delete**.
   Type **Yes** and press **Enter** to delete the component.

4. Select **Save** to save changes, and exit the configuration editor.

**After you finish**

To restart the FM Agent services from the Core VM, type:

```
stopFMagent
startFMagent
```

**Related reference**

- [Configuration editor component reference on page 243](#)

---

### Configure VxBlock Systems and components

VxBlock Central uses VxBlock Central Shell which provides a single interface to manage and configure VxBlock Systems and components.

**Access the VxBlock Central Shell session**

Access a VxBlock Central Shell session to manage and configure your VxBlock System.

**About this task**

To change default passwords, see *Manage credentials.*
**Procedure**

1. Establish an SSH connection to the MSM VM and log in with default credentials.
   Change the password to protect the system from unauthorized access.

2. Type: `vshell` or to skip the prompts, type:
   `vshell -l conf/ipython.conf`

3. Type the MSM VM hostname that you want to connect to or press **Enter** for the local host.

4. When prompted, log in with default credentials.
   Change the password to protect the system from unauthorized access.

**Related information**

*Manage credentials on page 209*

**Run VxBlock Central Shell from a remote host**

Install VxBlock Central Shell to connect to the MSM VM from a remote VM.

**Before you begin**

- The VM must be running CentOS release 6.3 or Red Hat Enterprise Linux 6.5.
- Obtain the hostname for the MSM node you want to connect to.

**Procedure**

1. Download the RPM to the host where you want to install VxBlock Central Shell.

2. From the same directory where the RPM is located, type:
   `rpm -Uvh vision-shell-remote-x.x.x.x-build_number.x86_64.rpm`

   Where:
   - `x.x.x.x` is the VxBlock Central release number.
   - `build_number` is the unique identifier of the VxBlock Central Shell build.

3. After installation is complete, type: `vshell`

4. When prompted, type the FQDN for the MSM node.

5. When prompted, type your username and password to log in to the shell.

**VxBlock Central Shell commands**

The VxBlock Central Shell provides commands to work independently in the shell environment.

**Show command**

Shell commands are grouped into extension packs. Each extension pack contains a related set of commands. Use the show command to find information about commands and their extension packs.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show extension_packs</code></td>
<td>Lists all available extension packs on the MSM VM</td>
</tr>
<tr>
<td><code>show extension_pack_name</code></td>
<td>Lists the commands for a specific extension pack</td>
</tr>
<tr>
<td></td>
<td>For example, <code>show default</code> lists the commands in the default extension pack</td>
</tr>
</tbody>
</table>

**Command** | **Description**
---|---
`show component_type` | Lists the commands for a specific component

For example, `show storagearray` lists the commands that can be performed with storage arrays.

In `show` command output, all commands are listed with a preceding percent (%) character. The commands can be issued with or without the percent character. This character is required only when assigning the output of a command to a variable.

Output from the `show` command can include the following commands. These commands are intended for shell extension developers and not useful for any other purpose.

- `%cs_template`
- `%hello_world`
- `%check_max_config`

**Access help**

From the shell command line, type `help` to get some general information about using the shell.

To get help for a shell command, append the command name with a question mark. For example: `connect?`

**Components in VxBlock Central Shell**

Commands in the VxBlock Central Shell enable you to gather information and make configuration changes to components across one or more VxBlock Systems.

**Gather information about switches**

Use VxBlock Central Shell to gather information about switches across all VxBlock Systems and to make configuration changes.

**Get a list of switches**

Run the `switch` command to list all switches in the network. You can address each switch individually in subsequent commands as follows:

- **By index position**
  
  Each switch in the `switch` command output is assigned an index number, starting with 0, for reference.

- **By alias**
  
  The alias for the switch is found in the first string on each line of the `switch` command output. Examples from the previous output include 'N5B' and 'M9A'.

- **By IP address**
  
  You can reference any switch by the IP address that is provided in the `switch` command output.

**Retrieving detailed information about a switch**

Use the Python `print` command to get detailed information about the attributes of a switch. Identify the switch by its index number. Python commands like `print` are not available using the MSM VM REST API for VxBlock Central Shell.

**Finding switches by attributes**

You can search to find switches by attribute value, using the same search syntax in the VxBlock Central. For example, you can find all switches with operating status that is not `operable`.

**Note:** Search syntax in VxBlock Central Shell is case-sensitive.
VxBlock Central Shell commands

To view a list of all commands that are available when working with switches, type: `show switch`

The following shell commands are for working with switches:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%connect</code></td>
<td>Opens an interactive connection with the target component command-line interface. Only one device can be connected at a time.</td>
</tr>
<tr>
<td><code>%diff</code></td>
<td>Shows the difference between the attributes of two components.</td>
</tr>
<tr>
<td><code>%run_commands</code></td>
<td>Runs a list of commands through the target command-line interface and returns the output as a string</td>
</tr>
</tbody>
</table>

Gather information about storage

Use these commands for getting information about storage arrays for the VxBlock Systems.

Get a list of storage arrays

Run the `storagearray` command in VxBlock Central Shell to list all storage arrays in the network. You can also use `sa` as a shortcut.

You can address each storage array individually in subsequent commands as follows:

- **By index position**
  Each storage array in the `storagearray` command output is assigned an index number, starting with 0, for reference.

- **By alias**
  The alias for the storage array is found in the first string on each line of the `storagearray` command output.

- **By IP address**
  You can reference any storage array by the IP address that is provided in the `storagearray` command output, for example, `10.1.139.50`.

Retrieve detailed information about a storage array

Use the Python `print` command to get detailed information about the attributes of a storage array.

**Note:** Python commands like `print` are not available using the MSM VM REST API for VxBlock Central Shell.

Find storage arrays by attributes

You can search to find storage arrays by attribute value, using the same search syntax in the VxBlock Central.

**Note:** Search syntax in VxBlock Central Shell is case-sensitive.

For more information about search syntax, see *Search within VxBlock Central Shell*.

Gather information about compute systems

Use these commands to view information about the compute systems for the VxBlock Systems.

Get a list of compute systems

Type `computesystem` in VxBlock Central Shell to list all compute systems in the network.

You can address each compute system individually in subsequent commands as follows:

- **By index position**
  Each system in the `computesystem` output is assigned an index number, starting with 0, for reference.
By componentTag
The componentTag for the compute system is displayed in the first string of each line in the computesystem output. Examples from the previous output include VMABO-UCS-1 and SERVER-B.

By IP address
You can reference any compute system by the IP address in the computesystem output, for example, 10.1.139.30.

Retrieve detailed information about compute systems
Use the Python print command to view detailed information about the attributes of a compute system.

Note: Python commands like print are not available using the MSM VM REST API for VxBlock Central Shell.

Find compute systems by attributes
You can search for compute systems by attribute value, using the same search syntax in the VxBlock Central.

Note: Search syntax in VxBlock Central Shell is case-sensitive.

For more information about search syntax, see Search within VxBlock Central shell.

VxBlock Central Shell commands
The following commands are for working with compute systems within the VxBlock Central Shell:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%connect</td>
<td>Opens an interactive connection with the target component command-line interface Only one device can be connected at a time.</td>
</tr>
<tr>
<td>%diff</td>
<td>Shows the difference between the attributes of 2 components</td>
</tr>
</tbody>
</table>

Gather information about VMware vSphere ESXi hosts
Use these commands to view information about the VMware vSphere ESXi hosts for the VxBlock Systems.

Get a list of VMware vSphere ESXi hosts
Run the esxi command in VxBlock Central Shell to list all ESXi hosts in the network.

You can address each VMware vSphere ESXi host individually in subsequent commands by index position. Each host in the esxi command output is assigned an index number, starting with 0, for reference.

Retrieve detailed information about an ESXi host
Use the Python print command to get detailed information about the attributes of an ESXi host.

Note: Python commands like print are not available using the MSM VM REST API for VxBlock Central Shell.

Find ESXi hosts by attribute
You can search to find ESXi hosts by attribute value, using the same search syntax in the VxBlock Central. Use the os keyword to represent the ESXi hosts.

Note: Search syntax in VxBlock Central Shell is case-sensitive.

For more information about search syntax, see Search within VxBlock Central Shell.

VxBlock Central Shell commands
To view available commands when with working with VMware ESXi hosts, type the show esxi command. The output lists the commands along with a brief description.
View VxBlock Central Shell logs

VxBlock Central Shell keeps activity logs in the `/opt/vce/shell/log` directory on the MSM VM.

The following log files are available:

<table>
<thead>
<tr>
<th>File name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cs_framework.log</td>
<td>Keeps a record of every command that is entered and the messages that are returned. The log rotates when it reaches the maximum file size of 10 MB. Logs rotate up to five times. When a log is rotated, a numerical suffix is appended to indicate the order in which that log was rotated. For example, <code>cs_framework.log.1</code> would be the name of the first log after it has reached its maximum file size and is no longer being used.</td>
</tr>
<tr>
<td>extension.log</td>
<td>The VxBlock Central Shell extensions record activity to the extensions log file.</td>
</tr>
</tbody>
</table>
| audit.log | The audit log records the following events in VxBlock Central Shell:  
- Event  
- User  
- Date  
- Client hostname  
- Command issued |

View VxBlock Central Shell jobs

Use `show_jobs` to view a log of submitted requests. The log results include the unique identifier, job timestamp information, username that issued the request, the submitted command and details, and the command status.

The `show_jobs` command tracks the following requests:

- `software_modules list states`
- `software_modules list modules`
- `software_modules create events`

To view a list of submitted requests, type: `show_jobs status`

1: Running
2: Partially completed
3: Completed
4: Failed
5: Interrupted

To return a list of all completed jobs, type: `show_jobs status=2`

If a job status is **RUNNING**, and needs to be canceled, quit the shell session and restart the VxBlock Central Shell.
Configure Secure Remote Services for VxBlock Central 2.0 and later

Secure Remote Services (SRS) must be configured in the field during deployment. Secure Remote Services automatically sends system inventory, RCM fitness, and alerts information through the Secure Remote Services connection to the Business Data Lake (BDL).

About this task
Dell EMC Support uses the collected data for analysis and remote troubleshooting. For more information about configuring Secure Remote Services, click the Settings icon > Configure SRS Gateway in VxBlock Central.

Configure Secure Remote Services for VxBlock Central 1.5 and earlier

VxBlock Central can connect to Secure Remote Services (SRS) and automatically send system inventory, RCM fitness, and alerts information through the Secure Remote Services connection to the Dell EMC Data Lake. Dell EMC Support uses the collected data for analysis and remote troubleshooting.


Register VxBlock Central with a Secure Remote Services gateway

Use the VxBlock Central Shell to register VxBlock Central with Secure Remote Services.

Before you begin
To register VxBlock Central with Secure Remote Services, ensure that you have received an email message from Dell EMC with a license activation code (LAC). Use the LAC you received with the VxBlock Central to obtain a Common Licensing Platform (CLP) file from the Electronic Licensing Management System (ELMS). This CLP contains the unique software identifier (SWID) required to register a VxBlock Central instance with Secure Remote Services. See Retrieving the software ID from the Licensing system if you need information about how to obtain the SWID.

Procedure
1. Establish an SSH connection to the MSM VM and log in with default credentials. Change this password to protect the system from unauthorized access.

2. Run the following script:
   `/opt/vce/shell/bin/ESRSScript/esrs_setup.sh`

3. When prompted with the following message:
   ```
   Are you a Dell EMC employee using a RSA token (FOB)? (yes/[no]):
   ```
   
   - If yes, go to Step 4.
   - If no, go to Step 5.

4. Type `yes` at the prompt.
   
   a. When prompted to enter the SWID, type `yes`.
b. Type the SWID.

c. Type the Secure Remote Services gateway IPv4 address.

d. Type your Dell EMC network/Windows ID.

e. Type your RSA pin and token. It takes a moment to authenticate.

f. Go to Step 6.

5. Type **no** at the prompt.

   a. When prompted, type **yes** to create a Secure Remote Services gateway configuration.

   b. Type the Secure Remote Services gateway hostname or IPv4 address. Then provide your username and password for Support at the prompt for each.

   c. Type **yes** to enter the SWID.

   d. At the SWID prompt, type the unique SWID from the CLP file.

6. Verify the registration status by performing the following steps:

   a. Type: **vshell** or to skip prompts, type: **vshell -l /opt/vce/shell/conf/ipython.conf**

   b. Type the MSM hostname to which you want to connect or press **Enter** for the local host.

   c. When prompted, log in with credentials

   d. Wait until you see the following parameter values:

      • deviceState = Managed

      • deviceStatus = Online

**Add a software identifier for an MSM VM**

Use the VxBlock Central Shell to add a software ID for an MSM VM to an already configured Secure Remote Services gateway. You are prompted to type the Secure Remote Services gateway to use from a known list of Secure Remote Services gateway IPv4 addresses.

**Before you begin**

When adding a software ID to a Secure Remote Services gateway that has not been configured, see *Register VxBlock Central with a Secure Remote Services gateway* for directions.

**Procedure**

1. Establish an SSH connection to the MSM VM and log in with default credentials. Change this password to protect the system from unauthorized access.

2. Type: **vshell** or to skip prompts, type: **vshell -l /opt/vce/shell/conf/ipython.conf**

3. Type the MSM VM hostname to which you want to connect, or press **Enter** for the local host.

4. When prompted, log in with default credentials. Change this password to protect the system from unauthorized access.

5. To view existing Secure Remote Services gateways, type: **esrs_register add swid=software identifier**

6. Type the number (0, 1, 2...) of the Secure Remote Services gateway to register the VM.
Retrieve the software ID from the licensing system

Retrieve the software ID (SWID) from the Dell EMC Licensing system. You need this software ID when configuring Secure Remote Services.

Before you begin

Ensure that you have received an email message from Dell EMC with a license activation code. You can also enter the sales order number during this procedure.

For more information about software activation, see the product documentation that is at Dell EMC Software Licensing Central.

Procedure

1. Connect to Dell EMC Software Licensing Central.
2. Select Activate My Software.
3. In the License Authorization Code field, type (or copy and paste) the code. You can enter the sales order number in the Sales Order # field. Click Search.
4. Select the product to activate, and click Start the Activation Process.
5. Confirm the company registered for the activation. Click Select a Machine.
6. In the Add a New Machine field, type a unique identifier for the machine name such as the VxBlock System serial number. Click Save Machine & Continue to Next Step.
7. In the Quantity to Activate field, enter the quantity of entitlements to activate for the machine. Click Next: Review.
8. Review the information. Click Activate to generate the software identifier.
9. Obtain a copy of the software identifier used to configure Secure Remote Services for Vision software or VxBlock Central by performing either:
   - Copy to the clipboard the SOFTWARE ID displayed after Your new key files are listed below:
   - Email the information:
     - Click View Certificate.
     - On the next page, click Email Certificate.
     - Under Choose what will be emailed, select Email and license key files.
     - In the Email Addresses box, provide at least one email address.
     - Click Send Email.
     - Open the email message, and copy the software identifier to the clipboard.

Update a Secure Remote Services gateway configuration or software identifier

Update either an existing Secure Remote Services gateway configuration or software identifier (SWID) for a host.

Before you begin

- Verify that the Secure Remote Services host and user exist in VxBlock Central Credential Manager.
- You have an email message from Dell EMC with a License Activation Code (LAC). Use the LAC you received with the VxBlock Central to obtain a Common Licensing Platform (CLP) file from the Dell EMC Electronic Licensing Management System (ELMS). This CLP contains the SWID required to register a VxBlock Central instance with Secure Remote Services.

Procedure

1. Establish an SSH connection to the MSM VM and log in with the default credentials. Change the password to protect the system from unauthorized access.
2. To run the script, type: `/opt/vce/shell/bin/ESRSScript/esrs_setup.sh`

3. When the following message opens:

   Are you a Dell EMC employee using a RSA token (FOB)? (yes/[no]):

   Type no.

4. Perform one of the following actions:
   - To update the Secure Remote Services gateway configuration, type yes at the prompt. Then type the Secure Remote Services gateway hostname or IPv4 address and the username and password for Support at the prompt for each.
   - If you do not want to update the Secure Remote Services gateway configuration, type no or press Enter.

5. If you want to update the SWID, type yes.

6. Type the unique software identifier from the CLP file when prompted.

---

**Deregister VxBlock Central with Secure Remote Services**

Use the VxBlock Central Shell to deregister a VxBlock System with Secure Remote Services.

**About this task**

⚠️ **CAUTION** The `esrs_register delete` command uninstalls an MSM VM instance from the Secure Remote Services gateway. It also deletes the credential manager credential for the same MSM VM to authenticate with the Secure Remote Services gateway. If the MSM VM has already been uninstalled from the Secure Remote Services gateway (such as through the Secure Remote Services gateway user interface), the command might fail. You may have to manually clean up the MSM VM credential manager entry.

**Procedure**

1. Establish an SSH connection to the MSM VM and log in with default credentials. Change the password to protect the system from unauthorized access.

2. Type: `vshell` or to skip the login prompts, type: `vshell -l /opt/vce/shell/conf/ipython.conf`

3. Type the MSM VM hostname to which you want to connect or press Enter for the localhost.

4. When prompted, and log in with credentials.

5. Type: `srs_register delete`

---

**Send information to Secure Remote Services**

Send VxBlock System inventory and RCM compliance information to Secure Remote Services automatically at regularly scheduled intervals or on-demand through a manual upload.

By default, VxBlock Central is set to automatically upload an inventory and compliance file one time per week on a randomly selected day. Use VxBlock Central Shell to view or modify this schedule at any time.

Send the real-time critical alerts of all components to Secure Remote Services if the option is checked in **General Settings** page of VxBlock Central.

To view the current automatic upload schedule, see *View the current Secure Remote Services upload schedule.*

To modify the upload schedule, see *Modify the schedule that is used to send information to Secure Remote Services.*

To perform an on-demand upload to Secure Remote Services, see *Manually upload information to Secure Remote Services.*
Secure the connection between VxBlock Central and Secure Remote Services

Secure Remote Services provides a two-way remote connection between Dell EMC Support and VxBlock Central. There are steps that you can take to make this connection more secure.

Change the default password

Dell EMC Support uses the VxBlock Central user account to remotely connect to VxBlock Central through Secure Remote Services. You are advised to change the default password for this account. See Change the default password for the root and VxBlock Central accounts for more information.

Restrict the remote connection

To prevent remote access into VxBlock Central, you can configure the Secure Remote Services Policy Manager to deny incoming connections to VxBlock Central. For more information, see the Secure Remote Services Installation and Operations Guide.

View VxBlock Central login history

If a two-way remote connection occurs, you can use the CentOS Linux VxBlock Central user account to view the VxBlock Central login history to determine who logged in. You can also see the following:

- The IP address associated with the remote user login
- The time that the login occurred
- The time that the session ended.

To view login history, use the last command.

Verify Secure Remote Services configuration

After configuring Secure Remote Services, verify the connection and the datafile transfer.

About this task

There are multiple ways to verify if the Secure Remote Services gateway is connected and the datafiles are transferred.

Procedure

1. Ensure that you receive a successful message in VxBlock Central, after Secure Remote Services is configured.
   The configuration issues are wrong software ID or wrong credentials. For wrong credentials, contact Dell EMC Support. For wrong software ID, see Retrieve the software ID for Secure Remote Services configuration.

2. Check the Secure Remote Services connectivity in the Secure Remote Services gateway UI by performing the following:
   a. Log in to Secure Remote Services gateway <IP address:9443> with administrator credentials.
   b. Go to Devices > Manage Devices.
   c. Ensure that the Device Status is Online.
   
   **Note:** If Device Status is Offline, then check the gateway connectivity. For more information, see Check the Secure Remote Services gateway connectivity.

3. Check the Secure Remote Services connectivity in Service Link UI by performing the following:
   a. Log in to Service Link: http://servicelink.emc.com/ URL.
   b. Go to Manage Clusters and search for the configured Secure Remote Services gateway serial number.
      If you do not have the gateway serial number, log in to Secure Remote Services gateway <IP address:9443> to obtain it.
c. Ensure that the **GW Connection** status is a *green* icon.

![Note: GW Connection status is a *red* icon when the Secure Remote Services gateway is not configured. (1)

Go to VxBlock Central to configure. If you are unable to configure the gateway, then see **Check the Secure Remote Services gateway connectivity.**](image)

4. Check that the datafiles are transferred in Service Link UI by performing the following:
   a. Log in to Secure Remote Services gateway `<IP address:9443>` with administrator credentials.
   b. Go to **Audit > MFT Audit.**
   c. Ensure that the percentage for the transfer of files is **100%**.

![Note: If the files are not available, wait for a day and recheck, as the files are transferred on a daily basis. After a day, if the files are still not available, contact Dell EMC Support.](image)

**Troubleshoot Secure Remote Services connectivity issues**

If you encounter issues that are related to Secure Remote Services connectivity, you need to know what to do to resolve the problem.

Common potential issues related to Secure Remote Services connectivity and tips on how to troubleshoot these issues are provided.

A Secure Remote Services shell extension causes the following exception: `Exception('ERROR: No SRS configuration found on CVM Host X.X.X.X.')`

<table>
<thead>
<tr>
<th>Cause</th>
<th>This exception occurs if the Secure Remote Services extension is not configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution</td>
<td>To configure Secure Remote Services, type: <code>/opt/vce/shell/bin/ESRSScript/esrs_setup.sh</code></td>
</tr>
</tbody>
</table>

When attempting to run the `esrs_setup.sh` script, the following error displays: `ERROR: Registration failed for host X.X.X.X due to urlopen error`

<table>
<thead>
<tr>
<th>Cause</th>
<th>The provided gateway hostname or IP address is not for a Secure Remote Services server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution</td>
<td>Use the correct address for your Secure Remote Services server.</td>
</tr>
</tbody>
</table>

When running a Secure Remote Services shell extension command, the following error displays: `urllib2.URLError(socket.error(111, 'Connection refused'))`

<table>
<thead>
<tr>
<th>Cause</th>
<th>The Secure Remote Services gateway is not running, or it is unreachable.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution</td>
<td>Check the Secure Remote Services gateway status to verify whether it is running. Verify network connectivity to the Secure Remote Services gateway by pinging or using <code>traceroute</code> from the same VM on which VxBlock Central Shell is running.</td>
</tr>
</tbody>
</table>

When running a Secure Remote Services shell extension command, the following error displays: `urllib2.URLError(socket.gaierror(-2, 'Name or service not known'))`

<table>
<thead>
<tr>
<th>Cause</th>
<th>The Secure Remote Services gateway hostname is not resolvable.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution</td>
<td>Use the gateway IP address, or add the hostname to the local host file or DNS server.</td>
</tr>
</tbody>
</table>
Integrate with SNMP

Integrate VxBlock Central with your network management system (NMS) to monitor and maintain your VxBlock System using SNMP.

VxBlock Central supports different SNMP versions, depending on the communication path and function. Determine the SNMP versions that you can use to establish communication between the Core VM and your NMS.

The following table describes the communication paths, functions, and supported SNMP versions:

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Function</th>
<th>SNMP version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core VM</td>
<td>NMS</td>
<td>• Forwarding traps to the NMS.</td>
<td>SNMPv1, SNMPv2c, SNMPv3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Making MIB information available to the NMS.</td>
<td></td>
</tr>
<tr>
<td>Components</td>
<td>VxBlock Central</td>
<td>• Receiving traps</td>
<td>SNMPv1, SNMPv2c</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VxBlock Central augments incoming traps with additional information.</td>
<td></td>
</tr>
</tbody>
</table>

Provision the SNMP name, location, and contact information fields

Modify the name, location, and contact information fields used for SNMP MIB identification and the generated traps on your VxBlock System. This updates SNMP Information only and does not affect the restful API data.

Before you begin

For the VxBlock System, obtain:

- Name
- (Optional) location
- (Optional) contact person

Procedure

1. Start an SSH session to the Core VM and log in as root.
2. Type:

   `setSNMPParams [-n sysName system_name] [-l sysLocation system_location] [-c sysContact system_contact] [-h] [-v] [-f]`

   When using the `setSNMPParams` command, surround a value with double quotes if the value includes spaces. For example, `setSNMPParams -n sysName "Vxblock System 1000-23" -f`.

   Where:
   - `-n sysName system_name` Specifies the name of the VxBlock System. The default is the hostname.
   - `-l sysLocation system_location` Specifies the location of the VxBlock System. The default is an empty string.
   - `-c sysContact system_contact` Specifies the contact name in your organization for VxBlock System related matters. The default is an empty string.
   - `-h` Displays the usage help.
- Displays the version.
- Forces the Core VM to reload the changes immediately.

If you do not specify the `-f` option, the changes take effect on the corresponding SNMP MIB objects when you restart the Core VM FM Agent. To do so, type: `service vce-fm-master restart`

**SNMP traps, events, and CIM indications**

Traps, events, and CIM indications are sent from a device to the Core VM.

To enable the forwarding of traps, events, and CIM indications, enable SNMP on the device. Also, the IP address for the Core VM must be set as the trap target on the device.

**Access traps, events, and CIM indications**

Messages are accessed on the Network Management System in two methods.

- **AMQP messaging:** SNMP traps, events, and CIM indications are translated into FMEvents, in .xml format, using the AMQP messaging service. If the required MIB is supported in the Core VM and it has been successfully compiled, augmentation is provided for the FMEvents.

- **SNMP traps:** To forward raw SNMP traps to an NMS, use the configureSNMP script to set the NMS IP address as the target for the trap forwarding. VxBlock Central forwards the raw SNMP traps to the NMS. To translate the traps, ensure that your NMS has the MIB files that VxBlock Central supports.
Communicate with the network management system

SNMP enables communication between VxBlock Central and the network management system (NMS). VxBlock Central sends SNMP traps and events to NMS to facilitate discovery polling and report health status changes or issues with physical and logical components or real-time alerts.

Send SNMP traps in readable format

VxBlock Central transforms SMI-compliant MIB files to send SNMP traps from AMQP queues in a readable format instead of as object identifiers.

About this task

VxBlock Central provides a base set of MIB files only. To receive other SNMP traps in a readable format, add the MIB files for those components on the Core VM.

The following table describes the Dell EMC MIB file:

<table>
<thead>
<tr>
<th>MIB module</th>
<th>Description</th>
<th>RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCE-SMI-MIB</td>
<td>Provides top-level organization of the Dell EMC private enterprise namespace</td>
<td>vce-smi-mib.txt</td>
</tr>
<tr>
<td>VCE-VBLOCK-HEALTH-MIB</td>
<td>Contains two tables that are both populated They share common indexes with the corresponding tables in the Entity MIB.</td>
<td>vce-vblock-health-mib.txt</td>
</tr>
</tbody>
</table>
### MIB module

<table>
<thead>
<tr>
<th>MIB module</th>
<th>Description</th>
<th>RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCE-VBLOCK-LOCATION-MIB</td>
<td>Describes the VxBlock System location and where all the chassis are located in the various cabinets. This MIB ties together with the Entity MIB module.</td>
<td>vce-vblock_location-mib.txt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VCE-FM-AGENT-MIB</td>
<td>Generates event notifications that System Library forwards to the NMS.</td>
<td>vce-fm-agent-mib.txt</td>
</tr>
<tr>
<td>VCE-AGENT-CAPS-MIB</td>
<td>Defines the agent capabilities and identities for the VxBlock System.</td>
<td>vce-agent-caps-mib.txt</td>
</tr>
<tr>
<td></td>
<td>The sysObjectID value identifies the System Library, and the sysORTable contains the capabilities of System Library.</td>
<td></td>
</tr>
<tr>
<td>VCE-VLAN-MIB</td>
<td>Defines information about VLANs in a VxBlock System</td>
<td>vce-vlan-mib.txt</td>
</tr>
<tr>
<td>VCE-ALERT-MIB</td>
<td>Defines the alerts that VxBlock Central generates for components</td>
<td>vce-alert-mib.txt</td>
</tr>
</tbody>
</table>

### Before you begin

- Ensure that the MIB files are SMI-compliant.
  If MIB files are not SMI-compliant, VxBlock Central sends SNMP traps from AMQP as object identifiers and an error message is written to the `/opt/vce/fm/logs/FMagent.log` file.
- Connect to the Core VM.

### Procedure

1. To stop the FM agent, type:
   ```
   stopFMagent
   ```
2. Transfer the MIB files to the following directory on the Core VM: `/opt/vce/fm/mibs/mibRepository`
3. To start the FM agent, type:
   ```
   startFMagent
   ```

### Enable northbound communication through SNMP

Complete these steps to configure SNMP communication between VxBlock Central and your NMS to send traps. Obtain the IP address of the trap target and the SNMPv1 or SNMPv2c community string.

### Procedure

1. Type:
   ```
   configureSNMP
   ```
The script prompts the following list of actions:

```
[root@hostname ~]# configureSNMP
Select your action
1) Add v1/v2c community with read only permissions
2) Add v1/v2c community with read/write permissions
3) Add v1/v2c trap target
4) Add v3 user with minimal security (no auth, no priv)
5) Add v3 user with moderate security (auth, no priv)
6) Add v3 user with maximum security (auth, priv)
7) Add v3 trap target
8) List community/user and trap targets
9) Delete v1/v2c community
10) Delete v3 user
11) Delete trap target
12) Done
#?
```

2. Perform one of the following:
   - Type 1 to create a read-only community string.
   - Type 2 to create a read/write community string.

The script prompts you to enter the following information:

- SNMP version
- Community string

After you specify the SNMP version and community string, the script returns to the list of actions.

3. Type 3 to create a trap target.

The script prompts you to enter the following information:

- SNMP version
- Community string
- IP address of the trap target

After you specify the trap target, the script returns to the list of actions. Repeat this step to enter another trap target.

4. Type 12 when you are done configuring SNMP.

The script prompts you to update the following file: `/etc/srconf/agt/snmpd.cnf`

5. Type one of the following values:
   - Type 1 to commit your changes.
   - Type 2 to discard your changes.

---

**Integrate with AD**

Control access to VxBlock Central across one or more VxBlock Systems in a data center environment. Configure VxBlock Central to work with AD for authentication and authorization.

**Management security**

VxBlock Central configures multisystem AD integration and maps AD groups to VxBlock Central roles (for authorized VxBlock Central administrators).

The following user security management capabilities are included:

- Credential management which enables you to:
Create users with the appropriate access rights.
- Update default passwords.
- Update access credentials for a component.
- Update Central Authentication Services (CAS) credential information.
- Import third-party SSL certificates for VxBlock Central.

Integrate VxBlock Central with AD which enables you to:
- Use role-based access control (RBAC) to perform security authorization checks for any client applications making an API call.
- Map roles to AD groups.
- Set up VMware SSO for VxBlock Central.

Integrate with AD

When VxBlock Central is integrated with AD, VxBlock Central authenticates AD users and supports a mapping between AD groups and roles.

VxBlock Central enables you to define an AD configuration that hovers over an AD server and map AD groups to roles. Defined roles in the MSP VM are independent from roles that are defined in the Core VM. Because the two VMs support different application functions, the roles that are defined in the MSM VM do not apply to the Core VM.

When VxBlock Central is integrated with AD, AD users can authenticate to VxBlock Central. Role mappings control the actions that the user is authorized to perform. By mapping an AD group to a role, you can control which permissions the user is given. When an AD user logs in to VxBlock Central, the software checks the role mappings for the AD groups to which the user is assigned. The set of available permissions depends on which roles have been mapped to groups in which the user is a member.

To use AD with VxBlock Central, set up the VMware vSphere Web Client to use an AD identity source. After setup complete, configure VxBlock Central to use the same AD server to control the users access to VxBlock Central. See VMware vSphere help for more information.

When VxBlock Central is integrated with AD, you do not need to create users and passwords within the VxBlock Central REST APIs. However, both methods of authentication and authorization are used, with the AD implementation taking precedence. If an AD user cannot be authenticated, the system attempts to authenticate with a VxBlock Central user created with REST API.

Note: You can create a VxBlock Central user with the REST API with the same name as an AD user. That user has roles that are granted through AD integration and VxBlock Central.

VxBlock Central supports the use of a single AD configuration for a single AD server. You can modify an existing AD configuration, but only one configuration can be used at any point in time. VxBlock Central enforces this restriction.

Remove groups from AD

Remove roles that are mapped to a group before deleting the group from AD. If a group is deleted without deleting the mappings first, the role mappings are saved on the MSM VM. The following problems can occur:

- Mappings between the nonexistent group and the roles are displayed in the REST API.
- If the group is ever re-created, members in new group are granted all permissions that role mappings of the previous group define. Users in the re-created group might be granted permissions that they are not intended to have.

If a group is re-created and inherits the former role mappings, use the dashboard to make corrections to the group roles. The LDAP administrator needs to communicate configuration changes with the VxBlock Central administrator.
Configure AD

Active Directory (AD) enables VxBlock Central to authenticate AD users and support mapping between AD groups and roles.

Before you begin

Set up AD.

For the AD configuration, obtain the following:

- IP address or hostname
- Port
- SSL configuration
- Credentials required to connect to AD with read-access to the base distinguished name (DN) for users
- Base DN for users (for example, OU=Users,DC=Example,DC=com)
- Base DN for user groups (for example, OU=Users,DC=Example,DC=com)
- User filter (for example, userPrincipalName=username)

The user filter supports a simple or compound search filter. The default setting (userPrincipalName=%u) is a simple filter that handles LDAP authentication. The filter uses user principal names (UPN), which are the email addresses of system users. In most AD environments, (userPrincipalName=%u) is the correct user filter.

You can change the user filter for your AD configuration. For example, you might specify a compound filter to check multiple attributes during LDAP authentication to authenticate service accounts that do not have email addresses. For example, specify a compound user filter to ensure that the sAMAccountName (User Logon Name in Windows systems older than Windows 2000) is also supported: (|(userPrincipalName=%u)(sAMAccountName=%u))

For the DN of service accounts for users, you can change the base DN to a common parent. For example, rather than specifying OU=Users as the AD location within the Base DN, specify a higher-level DN, such as OU=Accounts that includes both the OU=Users and OU=Service locations: OU=Accounts,OU=vbadtest,DC=adtest,DC=vcemo,DC=lab

Procedure

1. Log in to VxBlock Central.
2. From the main toolbar, select Roles > Connect to Active Directory.
3. Complete the fields with the AD information.
4. Click Save.

Map roles to AD groups

VxBlock Central can be configured to use AD to manage users and groups and assign roles to the groups in AD. The roles include the permissions that define what tasks the users in that role can perform after logging on to VxBlock Central.

Before you begin

Configure AD.

Procedure

1. Log in to VxBlock Central and click the menu icon.
2. Under the Administration, select Manage > Roles.
3. For each group, select one or more roles in the appropriate column.
4. When you are finished, click Save.
Default roles

The AD configuration must be connected to the multisystem management (MSM) node before you can assign roles. VxBlock Central ships with following default.

**VxBlock Central administrator**

Administrator with full access to the VxBlock Central and REST APIs.

**VxBlock Central shell administrator**

Administrator with full access to VxBlock Central Shell. Users with this role can run commands that make configuration changes to components in Converged Systems.

**VxBlock Central user**

User with read access to the VxBlock Central, REST APIs, and VxBlock Central Shell. The VxBlock Central user role can sign in to the dashboard but does not have access to any data or functionality unless one or more of the following secondary roles are included.

<table>
<thead>
<tr>
<th>Secondary Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System: vceSystemDescription</td>
<td>Dynamic role created to filter search results to the system identified by vceSystemDescription. Users with the VxBlock Central user role can have system roles to search and view status information for these systems in the dashboard.</td>
</tr>
<tr>
<td>Location: vceSystemGeo</td>
<td>Dynamic role created to filter search results to the systems located in vceSystemGeo. Users with the VxBlock Central user role can have location roles to search and view status information for systems by vceSystemGeo attribute.</td>
</tr>
<tr>
<td>LDAP configuration administrator</td>
<td>Users with this role can create, edit, delete, and connect LDAP configurations for MSM using the Connect to Active Directory configuration page in the dashboard.</td>
</tr>
<tr>
<td>Log administrator</td>
<td>Users with this role can download AA logs from the Central Authentication Service using the /securityweb/security/aalogs REST API.</td>
</tr>
<tr>
<td>RCM content prepositioning administrator</td>
<td>Users with this role can:</td>
</tr>
<tr>
<td></td>
<td>* Access the RCM content prepositioning features in the dashboard</td>
</tr>
<tr>
<td></td>
<td>* Download RCM content</td>
</tr>
<tr>
<td></td>
<td>* Delete RCM content</td>
</tr>
<tr>
<td></td>
<td>* Cancel downloads</td>
</tr>
<tr>
<td>RCM content prepositioning user</td>
<td>Users with this role can view RCM content prepositioning features in the dashboard.</td>
</tr>
</tbody>
</table>

**Note:** In addition to the roles provided by Dell EMC, some installations can have custom roles created using the MSM Rest API for Security Web. It is important that any custom roles must also be given permissions using the Rest API. Users who are assigned a custom role that does not include permissions cannot log into the dashboard, regardless of any other roles to which they are assigned.
Configure components to send traps

Configure every component in VxBlock Central to send traps to the Core VM. When a hardware event occurs, an SNMP trap is expected for most of the components that is sent out as a trap to the configured receivers. The trap receiver on the Core listens and receives these traps that are sent out.

About this task

When a fault repeatedly occurs in a specific time interval from the same system or component, only a single alert is displayed on VxBlock Central for the fault. Multiple notifications are sent to the user during the interval and this interval is configurable.

Configure Cisco UCSM to forward traps

To receive faults from Cisco UCS servers, enable the trap configuration on Cisco UCSM.

About this task

Cisco UCSM reports equipment and logical faults through SNMP. When Cisco UCSM detects an abnormal condition or defect at the component, equipment, or subsystem level, it reports faults through SNMP traps.

Procedure

1. Log in to UCS user interface.
2. Go to Admin > Communication Management > Communication Services > SNMP.
3. For Admin State, select Enabled.
4. Select All for Protocol.
5. In SNMP Traps click Add.
6. In Create SNMP Trap add the SLIB(Core) Host IP with community, port, and version details and click Save.

Configure iDRAC to forward traps

To receive the failures on Dell servers, configure trap forwarding on the iDRAC.

About this task

iDRAC generates events in response to changes in the status of sensors and other monitored parameters. When an event with predefined characteristics occurs on the system, the SNMP subagent sends information about the event with trap variables to the management console.

Procedure

1. Open iDRAC for the Dell server.
2. Select Configuration > System Settings.
3. Under Alert Configurations, from the Alerts drop-down menu, select Enabled and then click Apply.
4. From SNMP Traps Configuration, for the Alert Destination, enter the Core IP address and then click Apply.
5. Under SNMP Settings, enter details for Community String, SNMP Alert Port Number and SNMP Trap Format, and then click Apply.
6. From SNMP Traps Configuration, under Test SNMP Trap, click Send.
Configure Unisphere to forward traps

To receive traps from Dell EMC Unity, configure the trap receiver on the Unisphere that monitors the Dell EMC Unity storage array.

About this task

Unisphere 4.2.1 and later supports the reception of alerts by the Core VM. SNMPv2 and SNMPv3 are supported.

Procedure

1. Open Unisphere and log in to the Dell EMC Unity storage array.
2. Select Update System Settings > Alerts > SNMP.
3. On the Manage SNMP Alerts window, click Add to add the SNMP trap destination target.
4. From the SNMP target window, type the VxBlock Central software VM IP address.
5. Enter the username to authenticate.
6. Select the following:
   - Trap authentication protocol, the password, and privacy protocol
   - Severity level of alerts
7. Click Apply.

Configure XtremIO to forward traps

The XtremIO storage array supports sending SNMP notifications to predefined recipients.

Procedure

1. Open XMS of the XtremIO storage array.
2. From the top menu, select System Settings > Notifications.
3. From the XMS Notifications window menu, select SNMP Notifications to display the Email Notifications.
4. Click Add (+) to add recipients address, and enter the details.
5. Provide SNMP version-related details.
6. Select Send SNMP Notifications.
7. Click Apply to save the changes.
8. From the top menu bar, select System Settings > Cluster Settings.
9. From the Cluster Settings window, select SNMP Heartbeat.
10. From the SNMP Heartbeat window, select ON. Provide a time interval of approximately five minutes.

Configure VMAX or PowerMax to forward traps

The event daemon on VMAX or PowerMax provides the necessary SNMP MIB support and trap generation services. These services are required to monitor the status of VMAX or PowerMax storage environments.

About this task

The event daemon has a loadable SNMP library that acts as an SNMP agent when enabled and configured in the daemon_options file.

Procedure

1. Log in to VMAX or PowerMax vAPP Manager: https://<vmax_ip>:5480/
2. Go to Configuration > Solutions Enabler Service Configuration.

3. For Log Event Targets, enter: snmp

4. For Log Symmetrix Events, enter: sid=<Symmetrix_ID>,categories
   For example, sid=00019700235, status, events, array subsystem, checksum, diagnostic, environmental, device pool, service processor, srdf system, srdf link, srdf session, srdf consistency group, director, device, disk

5. For SNMP Trap Client Registration, enter: <Core_IP>,<port>,<filter>,<state>
   For example, 172.16.23.32,162,10,ACTION.

6. Select RUN COMMANDS.

7. On SYMCLI command, select "stordaemon" and on command arguments, enter: "action storevntd -cmd setflt 000197700087:SYMEVT38"

8. Click Run.

9. Close the vAPP Manager.

**Configure Cisco MDS and Cisco Nexus switches to forward traps**

Complete this task to configure Cisco MDS and Cisco Nexus switches to forward traps.

**About this task**

To configure switch alerts, log in to the switches and configure VxBlock Central as the SNMP trap host.

**Procedure**

1. Use SSH to access the switch as root.

2. Enter the following:

   ```
   snmp-server host <Core_IP> traps version 2c public
   ```

**Configure alert profiles and templates to receive notification**

To receive alerts as email messages or SNMP traps, create profiles from the templates that VxBlock Central provides.

See Profiles and Templates in the Online help.

Alerts are not generated for components in maintenance mode. To see if a component is in maintenance mode, see the VxBlock Central Inventory tab.

When a fault repeatedly appears within a specific time interval from the same system or component, only a single alert is visible on VxBlock Central for the fault. Multiple notifications are not sent during the interval.

This interval is configurable and can be configured as follows:

1. On the Core VM, open `/opt/vce/fm/conf/events/event.properties` file.

2. Edit `eventFloodControlInterval = 300` to the required time interval in seconds. The default interval is set to 300 seconds.

Any modification to the `/opt/vce/fm/conf/events/event.properties` file requires restart of the FM Agent service for the changes to take effect.

To restart the FM Agent services from the Core VM, type:

```stopFMagent```
Configure port flapping for switches

Configure port flapping in the switch configuration file.

About this task

To enable the port flapping for the switches, set the flag to true in the `/opt/vce/multivbmgmt/conf/general-configuration.properties` configuration file.

In the configuration file, type: `portFlapping.event = true`

Configure the VMs to use the NTP server

Configure each MSM VM and Core VM to use an NTP server. If redeploying an MSM VM, specify an NTP server IP address when configuring the server.

Before you begin

Determine the NTP server to use for the data center. Use the VLAN gateway or the gateway of the Converged System.

For each MSM VM and Core VM, perform the following steps:

Procedure

1. Use SSH to access the VM as the root user.
2. To verify access to the NTP server, type:
   ```
   ntpdate -u <IP_address>
   ```
   Where `IP_address` is the NTP server IP address.
3. Edit `/etc/ntp.conf`.
4. Comment out the default CentOS server entries, and add the following entry:
   ```
   server <IP_address>
   ```
   If the lines are already commented out, skip this step and run `service ntpd status` to check if the NTP daemon is running. If the daemon is running, skip the remaining steps and move to the next VM.
5. To save the changes and start the NTPD service, type:
   ```
   service ntpd restart
   ```
6. To start ntpd service on reboot, type:
   ```
   chkconfig ntpd on
   ```

Verify the ElasticSearch configuration

ElasticSearch is a distributed search server that provides a full-text search engine that is included with MSM VM. After deploying the OVA for MSM VM, verify ElasticSearch is properly installed and configured.

About this task

If you modify the MSM VM environment by including more VMs in the cluster, you may need to verify the ElasticSearch configuration again. The `elasticsearch.yml` file is configured automatically during OVA deployment. Do not change the configuration. However, you should verify the configuration by viewing the contents of `/etc/elasticsearch/elasticsearch.yml`. 
Verify the following properties within the `elasticsearch.yml` file:

- The `cluster.name` property is set to the value of the Cluster Name OVA property.
- The `node.name` property is a short hostname that is based on the configured FQDN.
- The `discovery.zen.ping.multicast.enabled` property is set to false.

**Procedure**

1. Display the contents of the `/etc/elasticsearch/elasticsearch.yml` file, and review the preceding properties.
2. If necessary, to restart the Elasticsearch service, type:
   ```
   sudo service elasticsearch restart
   ```

**Manage credentials**

Dell EMC recommends that you change all default passwords that are associated with the VxBlock Central, and the access credentials for VxBlock System components.

If any default passwords for VxBlock Central are still in use, administrators are notified when logging in to the dashboard and are prompted to change them.

Any changes made to component credentials are propagated automatically to the MSM VM. It may take up to five minutes for the MSM VM to update with credential changes.

**Change the default password for root and VxBlock Central accounts**

Core VM and the MSM VM run on CentOS Linux and have a `root` user. Change the default password for the `root` user on both VMs when you start VxBlock Central.

**About this task**

Follow these steps to change the password for the VxBlock System user on the MSM VM.

**Procedure**

1. Start an SSH session to log in to the VM.
2. Type: `passwd`
3. Type and confirm the new password when prompted. Update the MSM VM credential manager service with the new password.
4. Use one of the following steps for Core VM or MSM VM:
   a. To change the MSM password for credential manager to match the changed password, type:
      ```
      /opt/vce/credential-management/bin/credential-manager-cli create -credential-protocol SSH -credential-right ADMINISTRATOR -credential-type MSM -host-address MSM-IP -username <username>
      ```
      
      Where:
      - `MSM-IP` is the IP address for the MSM VM.
      - `newpassword` is the new password. This password must be the same as the new password provided on the `passwd` command.
      - `username` is either `root` or the VxBlock Central user, depending on the account that you are changing.
Note: In a clustered environment, if you change the password for the MSM VM admin user account, you must synchronize the password with the other MSM VM nodes in the cluster. Otherwise, the command fails.

b. Type the new password.
   - a. Log in to the MSM VM as the root user.
   - b. To change the Core VM root user password for MSM VM, type:

```
/opt/vce/multivbmgmt/install/addSlibHost.sh <core_IPaddress>
```

where `core_IPaddress` is the IP address for the Core VM where the password was changed.
   - c. Type yes.
   - d. Type root (or press Enter) for the username.
   - e. Type the new password for the Core VM.

After you finish
To optionally specify a password aging policy, type:

```
chage
```

```
chage -h
```

Use the nonadministrator account

VxBlock Central provides a nonadministrator account that enables you to delegate authority to run administrative commands.

About this task

The nonadministrator account allows the person using the account to run any administrative command using `sudo`, as if they were user root.

Note: The nonadministrator account is valid on the MSM VM only.

Before you begin

Connect to the MSM VM.

Procedure

1. To use the VxBlock Central account, log in using credentials.
2. To switch to the user root account while logged on, type: `su - root`

Change the default CAS password for Core VM

VxBlock Central uses a Central Authentication Service (CAS) for authentication to web services.

About this task

After the CAS password is changed, any client applications that are configured must also need be updated.

Before you begin

Connect to the Core VM.

Consider the following for the new CAS password:

- Is case-sensitive
- Must be 8 to 20 characters in length
- Must include one uppercase letter, one digit, and one special character
**Procedure**

1. Type: `/opt/vce/fm/bin/slibCasChangepw.sh`
2. When prompted, type `y` to continue.
3. Type the current default password for the `admin`.
4. Type the new password, and confirm it when prompted.

**Change the default CAS password for MSM VM**

MSM VM uses a Central Authentication Service (CAS) for authentication to its services. You can also change the default CAS password for users as appropriate.

**Before you begin**

Connect to the MSM VM.

The following password parameters apply:

- Is case-sensitive
- Must be 8 to 20 characters in length
- Must include one uppercase letter, one digit, and one special character
- Cannot contain any of the following special characters: `\ / % + ' " ( ) ; : < > |`

**Procedure**

1. Type:
   
   `/opt/vce/multivbsecurity/bin/caschangepw.sh`

   **Note:** During the processing of this script, services that are required for the operation of VxBlock Central are stopped and restarted. If the script is terminated during the process, either by issuing `Ctrl + Z` or terminating the SSH session, some VxBlock Central services are not restarted. To regain full operation, restart the MSM VM.

2. When prompted, type `y` to continue.
3. Type the password for the admin.
4. Type the new password for the admin user and then confirm it.

**After you finish**

Update the CAS password on the MSP VM to match the updated password on the MSM VM.

In a clustered environment containing multiple MSM VM nodes, synchronize the passwords on each MSM VM node with this new password.

**Synchronize the CAS password for the admin user**

In a clustered environment containing multiple MSM VM nodes, the CAS password for the MSM VM admin must be the same on all MSM VM nodes.

**Before you begin**

Obtain the new password that was changed on the first MSM VM node and use this password for these steps.
Dell EMC VxBlock™ and Vblock™ Systems 540 Administration Guide

Setting up VxBlock Systems to use VxBlock Central

**Procedure**

1. Connect to the MSM VM.
2. Type:
   
   `/opt/vce/multivbsecurity/bin/caschangepw.sh`

   **Note:**
   
   During the processing of this script, services that are required for the operation of VxBlock Central are stopped and restarted. If the script is terminated during the process, some VxBlock Central services are not restarted. Restart the MSM VM to regain full operation.

3. Type `y` to continue.
4. Type the new admin password that was changed on the first MSM VM node.

   **Note:** Do not type the previous admin user password for this MSM.

5. When prompted, type the same password that is used in the previous step and then confirm it when prompted.

**After you finish**

Repeat these steps for each additional MSM VM node in the cluster.

**Change the default CAS password for the MSP VM to match the MSM VM**

Change the Central Authentication Service (CAS) password for the MSP VM to match the password on the MSM VM.

**About this task**

RCM content prepositioning uses CAS authentication to services running on the MSP VM. The MSP VM shares the same CAS password used on the MSM VM. If the CAS password is updated on the MSM VM, update the CAS password on the MSP VM to match.

**Before you begin**

Connect to the MSP VM.

**Procedure**

1. Type: `/opt/vce/msp/install/update-cas-password.sh`
2. Type `y` to continue.
3. Type and confirm the MSM CAS password for the admin user.

   **Note:** This password must match the password that is used for CAS authentication on the MSM VM.

**Create users with access rights to storage components**

VxBlock Central Shell enables you to retrieve and update information about VxBlock System components. You cannot make updates to storage components until you create a user with administrative access to storage. The shell uses this credential to access storage components and make updates.

**Before you begin**

Establish an SSH connection to a MSM VM to perform this task.

**Procedure**

1. Establish an SSH connection to the MSM VM and log in.
2. To change directory, type: `/opt/vce/credential-management/bin/`
3. Type:

```
./credential-manager-cli create -credential-protocol SSH -credential-right ADMINISTRATOR -
credential-type STORAGE -host-address storage-ip -username SSHadminuser -password
SSHadminpassword
```

Where:

- `storage-ip` is the IP address of the storage component. To give the same user access to other storage
  components, reissue this command for each IP address.
- `SSHadminuser` is the username for logging on.
- `SSHadminpassword` is the password for logging on.

---

### Change access credentials for a VxBlock System component

Create, edit, or delete the configuration files necessary for discovery on a VxBlock System.

#### Before you begin

Ensure `system.cfg` is in the `/opt/vce/fm/conf` directory on the Core VM. If `system.cfg` is not present, contact Dell EMC Support.

#### Procedure

1. Start an SSH session to the Core VM.
   
   **Note:** Use PuTTY to access the configuration editor for Windows-based systems as non-VSCII supported
   terminals display styling incorrectly.

2. Log in using `root/V1rtu@1c3!`.

3. To launch the configuration editor and edit a configuration, type: `configSystem edit`

---

### Bulk credential script

The bulk credential script is used to change the password for multiple components.

#### About this task

**Note:** For VxBlock Central Version 2.0 and later, add, configure, and discover Converged Systems using the
VxBlock Central user interface. See *Discover Converged Systems* online help for more information.

The script can change the password for the following components:

- Compute
- Network
- Virtualization
- Application host
- AMP
- Storage (VMAX, ISILON, VNXe pending)

Copy the components that you want to change the password for from `system.cfg` file to an `inputfile` file. The
script automatically changes the password for the listed components. The script also checks if the password parameter
is empty in the `inputfile` and if IP address parameter is entered. If this parameter is listed, an error message is
generated and request to key in the parameter. The script validates the `system.cfg` file and creates
`vblock.xml`. After this task is complete, the discovery process starts.
configSystem edit -u runs to start validation
startFMAgent runs after validation to start discovery

The system.cfg must be in the /opt/vce/fm/conf directory. If this configuration file is missing, an error message opens. Copy and paste the system.cfg into inputfile. After the component details are entered, type the following command:

./bulkcredentialchg.sh

Manage third party certificates

Use a third-party signed certificate on the Core VM

Generate a new certificate with a Certificate Signing Request (CSR) and then import this certificate into JBoss for use with the VxBlock Central.

About this task

This section describes the procedure for importing a third-party SSL certificate into the application server that is provided with VxBlock Central.

The procedure begins with the generation of a CSR. Specific requirements for a CSR may vary among vendors. Depending on the Certificate Authority (CA) vendor or internal Private Key Infrastructure (PKI), you may receive a root CA or Intermediate CA and Signing CA Certificates. If so, install the CAs with the new server certificate. Your CA vendor or PKI administrators can provide details on retrieving all the certificates that are used in the certificate signing chain.

Before you begin

- The following tools are required:
  - Keytool
  - OpenSSL (available in your Linux distribution)
- Replace the password with the password you intend to use.
- All passwords that are supplied in steps 1–6 must be the same.
- Filenames in the procedure are provided as examples.

Note: Encrypted passwords from two .dat files in /etc/vce must be decrypted for Step 7. Contact Dell EMC Support to get the passwords decrypted.

Procedure

1. Back up copies of your cryptography material in a secure location. Back up the following files on the Core VM:
   - /opt/jboss/standalone/configuration/server.crt
   - /opt/jboss/standalone/configuration/server.keystore
   - /usr/java/default/lib/security/cacerts

2. Create a local certificate.
   This certificate is for generating the CSR and does not have to be performed on the target server. These steps include exporting the private key for later combinations with the generated certificate for import on the target server. The DN name parameters may be adjusted to fit your environment and CSR requirements. The following example shows creating a local certificate with the alias jbosskey for the keystore entry:

3. Export the private key for this self-signed certificate and convert it to PEM format for later use. Store the private key in a secure location. The RSA encryption is deleted from the file for flexibility with existing and future VxBlock Central certificate management tools. Type:

```
/usr/java/default/bin/keytool -importkeystore -srckeystore my.keystore
-destkeystore privatekey-rsa.p12 -deststoretype PKCS12 -srcalias jbosskey
-storepass customer-supplied-password -keypass customer-supplied-password
```

Type the **customer-supplied-password** at the **Enter source keyword password** prompt.

a. To parse the PKCS12 private key and convert it to PEM format, type:

```
/usr/bin/openssl pkcs12 -in private-key-rsa.p12 -out private-key-rsa.pem -nocerts
```

b. To convert the private key to PKCS8 format, type:

```
/usr/bin/openssl pkcs8 -topk8 -nocrypt -in private-key-rsa.pem -inform PEM
-out private-key.pem -outform PEM
```

Type the **customer-supplied-password** at the **Enter pass phrase for ./private-key-rsa.pem** prompt.

4. To generate a CSR, type:

```
/usr/java/default/bin/keytool -certreq -keyalg RSA -alias jbosskey -file certreq.csr
-keystore my.keystore
```

Type the **customer-supplied-password** at the **Enter keystore password** prompt.

5. Send the resulting certreq.csr to your selected CA.

Your returned certificate (.der or .cer) should be in PEM format. If the file is a .cer, change the extension to .pem. If the file is not a Base64 PEM encoded .cer file, to convert it to PEM format, type:

```
/usr/bin/openssl x509 -inform der -in <certificate>.der -out <certificate>.pem
```

If you have a .cer certificate, type:

```
cp <certificate>.cer <certificate>.pem
```

6. To assemble the certificate and the private key, type:

```
/usr/bin/openssl pkcs12 -export -in <certificate>.pem -inkey private-key.pem
-out cert-andkey.p12 -name jbosskey
```

Type the **customer-supplied-password** at the **Enter export password** prompt. 
Type the **customer-supplied-password** at the **Verifying - Enter keystore password** prompt.

7. Import the issuing certificate chain in to the cacerts keystore (root and intermediate certificates PEM files). Rename the root and intermediate certificates as .pem (if required).

a. For root certificate, type:

```
/usr/java/default/bin/keytool -import -file <rootCert.pem> -alias jbosskey1
-keystore /usr/java/default/lib/security/cacerts
```

b. For intermediate certificate, type:

```
/usr/java/default/bin/keytool -import -file <IntermediateCert.pem>
-alias jbosskey2 -keystore /usr/java/default/lib/security/cacerts
```
### Use a third party signed certificate on the MSM VM

You can generate a new certificate with a Certificate Signing Request (CSR) and then import this certificate into Tomcat for use with VxBlock Central.

#### About this task

This section describes the procedure for importing a third-party SSL certificate into the application server that is provided with the VxBlock Central.

Specific requirements for a CSR may vary among vendors.

Depending on the Certificate Authority (CA) vendor or internal Private Key Infrastructure (PKI), you may receive a root CA or Intermediate CA and Signing CA Certificates. If so, install the CAs with the new server certificate. Your CA vendor or PKI administrators can provide details on retrieving all the certificates that are used in the certificate signing chain.

| Note: | If you change the MSM VM hostname after performing this procedure, you must repeat this procedure to import the third-party SSL certificate again. |

#### Before you begin

- The following tools are required:
  - Keytool
  - OpenSSL (available in your Linux distribution)
- Replace the password with the password you intend to use.
- All passwords that are supplied in steps 1–5 must be the same.
- All filenames in the procedure are examples.

| Note: | Encrypted passwords from two .dat files in /etc/vce must be decrypted for Step 6. Contact Dell EMC Support to get the passwords decrypted. |

#### Procedure

1. Back up copies of your cryptography material in a secure location. The following files should be backed up on an MSM VM:
   - `/usr/java/default/lib/security/cacerts`
   - `/opt/vce/tomcat/conf/*`

2. Create a local certificate.

   This certificate is for generating the CSR and does not have to be performed on the target server. These steps include exporting the private key for later combinations with the generated certificate for import on the target server. The DN name parameters may be adjusted to fit your environment and CSR requirements.
   The following is an example creating a local certificate using the alias `<your keyAlias>` for the keystore entry:

   ```shell
   ```
3. Export the private key for this self-signed certificate and convert it to PEM format for later use.

Store the private key in a secure location. The RSA encryption will also be deleted from the file for flexibility with existing and future VxBlock Central certificate management tools.

   a. Type:

   `/usr/java/default/bin/keytool -importkeystore -srckeystore my.keystore
   -destkeystore privatekey-rsa.p12 -deststoretype PKCS12 -srcalias <your keyAlias>
   -storepass <customer-supplied-password>

   Type the `customer-supplied-password` at the Enter source keystore password prompt.

   b. To parse the PKCS12 private key and convert it to PEM format, type:

   `/usr/bin/openssl pkcs12 -in private-key-rsa.p12 -out private-key-rsa.pem -nocerts`

   c. To convert the private key to PKCS8 format, type:

   `/usr/bin/openssl pkcs8 -topk8 -nocrypt -in private-key-rsa.pem -inform PEM
   -out private-key.pem -outform PEM`

   Type the `customer-supplied-password` at the Enter pass phrase for ./private-key-rsa.pem prompt.

4. To generate a CSR, type:

   `/usr/java/default/bin/keytool -certreq -keyalg RSA -alias <your keyAlias>
   -file certreq.csr -keystore my.keystore`

   Type the `customer-supplied-password` at the Enter keystore password prompt.

5. Send the resulting certreq.csr to your selected CA or PKI administrator.

   Your returned certificate (.der or .cer) should be in PEM format. If the file is a .cer, change the extension to .pem. If the file is not a Base64 PEM encoded .cer file, to convert to PEM format, type:

   `/usr/bin/openssl x509 -inform der -in <certificate>.der -out <certificate>.pem`

   If you have a .cer certificate, type:

   `cp <certificate>.cer <certificate>.pem`

6. To convert the primary key to an RSA key, type:

   `openssl rsa -in <private-key.pem> -out <rsa-key.pem>

7. Import the issuing certificate chain into the cacerts keystore (root and intermediate certificates PEM files).

   Rename the root and intermediate certificates as .pem (if required).

   a. For root certificate, type:

   `/usr/java/default/bin/keytool -import -file <rootCert.pem> -alias visionkey
   -keystore /usr/java/default/lib/security/cacerts`

   b. For intermediate certificate, type:

   `/usr/java/default/bin/keytool -import -file <IntermediateCert.pem>
   -alias visionkey2 -keystore/usr/java/default/lib/security/cacerts`

**Note:** When prompted for a password, type the one that you requested from Dell EMC Support.
8. To import the new certificate, this time specifying the certificate and private key filenames, type:

```
```

### Configure connection and download settings

Configure settings for VxBlock Central to connect to the RCM content distribution network and manage RCM content that is downloaded. These settings include the proxy server information, connection timeout, the download rate, and retry attempts and intervals.

**About this task**

VxBlock Central retrieves property settings from the following property files on the MSP VM:

- `/opt/vce/msp/conf/msp-common.properties`
- `/opt/vce/msp/downloader/conf/msp-downloader.properties`
- `/opt/vce/msp/contentsource/conf/msp-contentsource.properties`
- `/opt/vce/msp/contentshare/conf/msp-contentshare.properties`
- `/opt/vce/msp/assetmanager/conf/msp-assetmanager.properties`

To configure settings, specify the property values in the property files.

### Configure VxBlock Central to access a proxy server

Configure VxBlock Central to use a proxy server to access the RCM content distribution network.

**About this task**

To configure the VxBlock Central to use a proxy server, in `/opt/vce/msp/conf/msp-common.properties` on the MSP VM, set values for the following properties:

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxy.hostname</td>
<td>Sets the hostname of the proxy server</td>
</tr>
<tr>
<td>proxy.port</td>
<td>Sets the port number that the MSP VM uses to connect to the proxy server</td>
</tr>
<tr>
<td>proxy.username</td>
<td>Sets the username to authenticate to the proxy server</td>
</tr>
<tr>
<td>proxy.password</td>
<td><strong>WARNING</strong> Do not modify this property manually. Use the <code>opt/vce/msp/install/update-proxy-password.sh</code> script to set the proxy.password property. See the related topic for information about running this script.</td>
</tr>
</tbody>
</table>

**Before you begin**

- Connect to the MSP VM.
- Back up the `/opt/vce/msp/conf/msp-common.properties` file.

**Procedure**

1. Open `/opt/vce/msp/conf/msp-common.properties` to edit.
2. Locate **Proxy Server Configuration settings**.
3. Specify values for each property to allow VxBlock Central access to the proxy server.
   
   **Note:** Use the `opt/vce/msp/install/update-proxy-password.sh` script to set the `proxy.password` property. See the related topic for information about running this script.
4. Save and close the `msp-common.properties` file.
5. To restart the Downloader service, type:

   service vision-downloader restart

6. To restart the Content Source service, type:

   service vision-contentsource restart

Configure the connection timeout

Configure the time that VxBlock Central can maintain an inactive connection.

About this task

To configure the connection timeout, set values for the following properties in msp-contentsource.properties on the MSP VM:

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connection.timeout.millis</td>
<td>Sets the maximum amount of time, in milliseconds, that VxBlock Central can maintain an inactive connection to the RCM content distribution network. Specify a value of 0 to disable the timeout. The default value is 18000.</td>
</tr>
</tbody>
</table>

Before you begin

- Connect to the MSP VM.
- Back up the /opt/vce/msp/contentsource/conf/msp-contentsource.properties file.

Procedure

1. Open /opt/vce/msp/contentsource/conf/msp-contentsource.properties for editing.
2. Locate the Connection settings section.
3. Remove comments from properties as appropriate.
   - To delete the comment from the property, delete the hash (#) at the start of the line.
4. Specify values for the property as appropriate.
5. Save and close the msp-contentsource.properties file.
6. To restart the Content Source service, type:

   service vision-contentsource restart

Configure the download rate

Configure the download rate at VxBlock Central uses when downloading RCM content and as a result, minimize the impact of RCM content downloads on your bandwidth.

About this task

To configure the download rate, set the value for the following property in msp-downloader.properties on the MSP VM:
Before you begin

- Connect to the MSP VM.
- Back up the `/opt/vce/msp/downloader/conf/msp-downloader.properties` file.

Procedure

1. Open `/opt/vce/msp/downloader/conf/msp-downloader.properties` for editing.
2. Locate the Downloader settings section and specify the download rate that VxBlock Central uses to download RCM content.

   ![Note:](image)

   - The download rate can be specified in B, K, or M, for example:
     - 1024 B - value in bytes
     - 1 K - value in kilobytes
     - 1 M - value in megabytes
   - A value of 0 is interpreted as unlimited.
   - The minimum value that can be specified is 1024 bytes for the download rate.

3. Save and close the `msp-downloader.properties` file.
4. To restart the downloader service, type:
   ```bash
   service vision-downloader restart
   ```

Configure retry attempts and intervals

Configure the retry attempts and intervals that VxBlock Central uses when downloading RCM content.

About this task

To configure the retry settings, set values for the following properties in `msp-downloader.properties` on the MSP VM:

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>retry.max.attempts</td>
<td>Sets the maximum number of attempts that VxBlock Central makes to connect to the RCM content distribution network before displaying a downloading error. The default value is 10.</td>
</tr>
<tr>
<td>retry.initial.interval</td>
<td>Sets the maximum number of milliseconds, that VxBlock Central will wait to attempt to reconnect after failing on first attempt to connect to the RCM content distribution network. The default value is 100.</td>
</tr>
</tbody>
</table>
### Before you begin

- Connect to the MSP VM.
- Back up the `/opt/vce/msp/downloader/conf/msp-downloader.properties` file.

### Procedure

1. Open `/opt/vce/msp/downloader/conf/msp-downloader.properties` for editing.

2. Locate the **Retry settings** and specify values for each property to change the default retry attempts and interval settings.

3. Save and close the `msp-downloader.properties` file.

4. To restart the Downloader service, type:

   ```bash
   service vision-downloader restart
   ```

### Manage credentials for RCM content prepositioning

#### Change the PostgreSQL database password

To change the default password for the Content Share PostgreSQL database and the Asset Manager, you run a script on each service on the MSP VM. The script updates the password, encrypts it, and then saves it to an internal database.

### About this task

VxBlock Central uses a PostgreSQL database to store downloaded RCM content in the MSP VM. These databases are independent of each other, but if required, you can update the default credentials on both to be the same or different if appropriate. The steps in this procedure explain how to run the update scripts for both the Asset Manager and the Content Share services.

The following password criteria apply:

- Is case-sensitive
- Must be 8 to 20 characters in length
- Must include one uppercase letter, one digit, and one special character
- Cannot contain any of the following special characters: `\ / % + ' " ( ) ; : < > |`

### Before you begin

Connect to the MSP VM.
**Procedure**

1. Type:
   
   `/opt/vce/msp/install/update-assetmanager-db-password.sh`

2. When prompted to continue, type `y`.
3. Type the new password for the admin user and confirm.
4. When a message opens confirming that the password has been changed, type the following command:
   
   `/opt/vce/msp/install/update-contentshare-db-password.sh`

5. When the prompt appears to continue, type `y`.
6. Type the new password for the admin user and confirm.

**Change the password for the proxy server**

Configure VxBlock Central to use a proxy server to access the RCM content distribution network.

**About this task**

To change the proxy password for the specified username, run the `/opt/vce/msp/install/update-proxy-password.sh` script on the MSP VM. This script updates the password, encrypts it, and then saves it to an internal database.

**Before you begin**

Connect to the MSP VM.

**Procedure**

1. Type:
   
   `/opt/vce/msp/install/update-proxy-password.sh`

2. When prompted to continue, type `y`.
3. Type the new password for the user, and confirm it when prompted.

**VxBlock Central Advanced Analytics**

The VxBlock Central Advanced Analytics is installed in the field and provides VxBlock Central Operations functionality. See the *Dell EMC VxBlock Central Installation Guide* for the procedures necessary to install VxBlock Central Operations, including the VMware vRealize Operations (vROps) Adapter.

**Change VxBlock Central Operations Adapter real-time alerts collection cycle interval**

Change the default collection cycle for real-time alerts for the VxBlock Central Operations Adapter for VMware vRealize Operations 6.6 and earlier. The default collection cycle for real-time alerts is three minutes.

**About this task**

Managed objects and associated metrics from VxBlock Central are collected once in five cycles, which is every 15 minutes.
Procedure

1. Select Administration > Configuration > Inventory Explorer.
2. Expand Adapter Instances and click Dell EMC Converged System Adapter Instance to view the list of configured MSMs.
3. Click Edit Object, and select Advanced Settings.
4. Change the Collection Interval (Minutes) to 3.
5. Repeat steps 3 and 4 for all configured MSM VM instances.

Change the VxBlock Central Adapter Collection cycle interval

Increase the collection interval for larger environments.

About this task

By default, the adapter collection cycle is set to 15 minutes. The default collection cycle is adequate for most environments. In larger environments, you may need to increase the collection interval.

Procedure

1. Expand Adapter Instances and click VxBlock Central Operations Management Pack to view the list of MSM VMs.
2. Click Edit Object, and go to Advanced Settings.
3. Change the Collection Interval (Minutes).
4. Repeat the preceding steps for all configured MSM instances.
Manage VxBlock Systems with VxBlock Central

Change discovery and health polling intervals

Change the interval at which VxBlock Central discovers VxBlock System components and the interval at which VxBlock Central polls components for operating status.

About this task

VxBlock Central runs the discovery process every 15 minutes. You can set the discovery interval between five and 1440 minutes. VxBlock Central polls VxBlock System components every five minutes to gather the operating status of each component to update health scores. You can set the health polling interval between two and 15 minutes.

Note: Health for Data Domain 3300 displays as Unknown.

Before you begin

Connect to the Core VM.

Procedure

1. To stop the agent and go to agent directory, type:

```
stopFMagent
```

```
   cd /opt/vce/fm/conf directory
```

2. Open fmagent.xml to edit.

3. Locate the SchedulerConfig section.

   The following example shows the SchedulerConfig section with the default values:

   ```xml
   <FMAgentConfig>
     <SchedulerConfig>
       <DiscoveryCycle>15</DiscoveryCycle>
       <HealthPollCycle>5</HealthPollCycle>
     </SchedulerConfig>
   </FMAgentConfig>
   ```

   DiscoveryCycle sets the interval for VxBlock System component discovery.
   HealthPollCycle sets the interval for which VxBlock Central polls VxBlock System for operating status.

4. Change the intervals for the discovery cycle and health polling as appropriate.

5. Save and close the fmagent.xml file.

6. To start the FM agent, type: `startFMagent`

Monitor events and log messages

VxBlock Central monitors the physical and logical components of a VxBlock System, such as switches, compute systems, and storage arrays, for alerts and notifications.

VxBlock Central Version 2.0 and later, also monitors for component discovery failure, and for issues with Secure Remote Services.
VxBlock Central uses standard mechanisms, such as SNMP traps and SMI indications to monitor the events. These events are protocol-dependent and come in different types and formats. You can view these events with your network management software.

**Syslog messages**

The following syslog files are located in the `/etc/logrotate.d/syslog` directory:

<table>
<thead>
<tr>
<th>Syslog</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/var/log/cron</code></td>
<td>Information about cron jobs when the cron daemon starts a cron job</td>
</tr>
<tr>
<td><code>/var/log/maillog</code></td>
<td>Log information from the mail server that is running on the VxBlock System</td>
</tr>
<tr>
<td><code>/var/log/messages</code></td>
<td>Global system messages</td>
</tr>
<tr>
<td><code>/var/log/secure</code></td>
<td>Information that is related to authentication and authorization privileges</td>
</tr>
<tr>
<td><code>/var/log/spooler</code></td>
<td>Information for news and the UNIX-to-UNIX Copy Program (UUCP) system</td>
</tr>
</tbody>
</table>

**Change syslog rotation parameters**

VxBlock Central uses a log rotation tool for syslog messages. You can modify the rotation parameters to suit your needs.

**Before you begin**

Connect to the Core VM.

**Procedure**

1. Open the `/etc/logrotate.d/syslog` file for editing.
2. Modify rotation parameters, as needed.
3. To save your changes, type:
   
   ```bash
   logrotate -f /etc/logrotate.d/syslog
   ```

**Forward syslog messages to remote servers**

VxBlock Central uses syslog protocol to store syslog messages on the VxBlock System. Since local storage on the VxBlock Systems is limited, forward syslog messages to a remote server for backup and archiving.

**About this task**

You can configure VxBlock Central with multiple forwarding entries; however, you can set only one forwarding entry per remote server. You can also apply forwarding filters that are based on facility type and severity level. For example, you can configure VxBlock Central to forward syslog messages as follows:

- All syslog message go to one remote server
- Syslog messages of a given severity to a different remote server

To configure custom filters, use `MessagePattern=\[(facility.severity)\]`. The default is `*.*` which forwards log messages of all facilities and severity levels to the remote syslog server. Use a comma to separate multiple values for a filter.

The following table provides facility and severity values:
<table>
<thead>
<tr>
<th>Filter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>auth</td>
</tr>
<tr>
<td></td>
<td>authpriv</td>
</tr>
<tr>
<td></td>
<td>daemon</td>
</tr>
<tr>
<td></td>
<td>cron</td>
</tr>
<tr>
<td></td>
<td>ftp</td>
</tr>
<tr>
<td></td>
<td>lpr</td>
</tr>
<tr>
<td></td>
<td>kern</td>
</tr>
<tr>
<td></td>
<td>mail</td>
</tr>
<tr>
<td></td>
<td>news</td>
</tr>
<tr>
<td></td>
<td>syslog</td>
</tr>
<tr>
<td></td>
<td>ser</td>
</tr>
<tr>
<td></td>
<td>uucp</td>
</tr>
<tr>
<td></td>
<td>local0</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>local7</td>
</tr>
<tr>
<td></td>
<td>*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Facility</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>emerg</td>
</tr>
<tr>
<td></td>
<td>alert</td>
</tr>
<tr>
<td></td>
<td>crit</td>
</tr>
<tr>
<td></td>
<td>err</td>
</tr>
<tr>
<td></td>
<td>warn</td>
</tr>
<tr>
<td></td>
<td>notice</td>
</tr>
<tr>
<td></td>
<td>info</td>
</tr>
<tr>
<td></td>
<td>debug</td>
</tr>
<tr>
<td></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>*</td>
</tr>
</tbody>
</table>

**Before you begin**

- Obtain the IP address of the remote syslog server hostname and the port where the server is accepting syslog messages.
- If you are only sending a portion of the syslog messages to a remote server, obtain the facility and severity of the log messages to forward.
- Connect to the Core VM.

**Procedure**

1. Type:

Where:
- [-h|-help|--help]: Displays the usage help
- [-l host-ip [port]]: Lists the specified or all syslog forward entries using the IP address of the hostname for the remote server and the port where the server is accepting syslog messages
- [-d host-ip [port]]: Deletes a syslog forward entry using the IP address of the hostname for the remote server and the port where the server is accepting syslog messages
- [-a host-ip [port] [options]]: Adds a syslog forward entry using the IP address of the hostname for the remote server and the port where the server is accepting syslog messages
- The [options] are as follows:
  - WorkDirectory=<location>: The location for spool files
    The default is /var/rsyslog/work.
  - ActionQueueFileName=<name>: A unique name prefix for spool files
    The default is the IP address of the hostname and port for the remote syslog server.
  - ActionQueueType= [FixedArray | LinkedList | Direct | Disk]:
    - FixedArray – Uses a fixed, preallocated array that holds pointers to queue elements
    - LinkedList – Uses asynchronous processing
      This value is the default.
    - Direct – A nonqueuing queue
    - Disk - Uses disk drives for buffering
  - ActionQueueMaxDiskSpace=<number>: Specifies the maximum amount of disk space a queue can use
    The default is 1g.
  - ActionResumeRetryCount=<n>: The number of infinite retries on an insert failure
    The default is -1 which means eternal.
  - ActionQueueSaveOnShutdown=[on|off]: Saves in-memory data if the remote syslog server shuts down
    The default is on.
  - Protocol=[UDP|TCP]: The network protocol used to transfer the log messages
    The default is TCP.
  - MessagePattern= [(facility).(severity)]: The filters for select messages
    The default is *. *
  - [-u host-ip [port] [options]]: Update a syslog forward entry using the IP address of the hostname for the remote server and the port where the server is accepting syslog messages.
    Specific [options] values are provided in the preceding list.

Example 1 Examples

To forward all syslog messages to a remote server with an IP address of 12.3.45.678 at port 10514, type:

configureSyslogForward -a 12.3.45.678 10514

To forward syslog messages that match a facility type of auth and any severity level, type:
Example 1  Examples (continued)

configureSyslogForward -a 12.3.45.678 10514 --MessagePattern=auth.*

To forward syslog messages that match a facility type of auth and a severity level of emerg, type:

configureSyslogForward -a 12.3.45.678 10514 --
MessagePattern=auth.emerg

To forward syslog messages over UPD, if the syslog message matches any facility type and a severity level of debug, type:

configureSyslogForward -a 12.3.45.678 10514 --Protocol=UDP --
MessagePattern=*.debug

Customize login banners

Add login banners to display customized information when users log in to VxBlock Central.

Before you begin

Connect to the Core VM.

Procedure

1. Open the following files for editing:
   - /etc/motd
     *Note:* Do not overwrite existing content in /etc/motd.
   - /etc/issue
   - /etc/issue.net

2. Update each file with the login banner as appropriate.

3. Save and close the files.

Back up and restore Core VM

Core VM backs up configuration and environment data so that you can restore the Core VM to a working state. Files and data that Core VM backs up are described and the format and location of backup files.

Core VM backs up the following:

- Core VM configuration files in the /opt/vce/fm/conf directory and:
  - /etc/snmp/snmpd.conf
  - /etc/logrotate.d/syslog
  - /etc/srconf/agt/snmpd.cnf
- JBoss configuration files, including keystore files
- Core VM administrative, configuration, and model database schemas and datafiles
- PostgreSQL database schema and data
During manufacturing, Dell EMC creates backups on the Core VM so that they are available when the VxBlock System is delivered to your site. After the VxBlock System is up and running at your site, VxBlock Central automatically runs backup tasks according to the default schedules.

Backup file format and location
Core VM software creates backups in **tar.gz** file format on the Core VM, as follows:

- Core VM and JBoss configuration files are saved to a single **tar.gz** file in the `/opt/vce/fm/backup/snapshots` directory.
- PostgreSQL database schema and data are saved to multiple **tar.gz** files in the `/opt/vce/fm/backup/postgres` directory.

By default, Core VM software stores:

- A maximum of seven Core VMs and JBoss configuration backups
- PostgreSQL database backups for the current day and the previous two days

The following example describes how VxBlock Central stores PostgreSQL database backup files:

- At 11:59 PM on Tuesday, Core VM stores backup files for Tuesday, Monday, and Sunday.
- At 12:00 AM on Wednesday, Core VM stores backup files for Wednesday, Tuesday, and Monday. Core VM deletes the backup files for Sunday.

Default backup schedule
By default, backup tasks occur:

- Daily at 12:00 AM for the Core VM configuration files
- Every 10 minutes for the PostgreSQL database schema and data

You can change the schedule and frequency of the backup tasks. You can run backups on demand outside of the scheduled tasks.

Management backup
VxBlock Central automatically backs up Core VM configuration files.

When the backup task runs, it creates a `.TAR` file that contains:

- Core VM configuration files from:
  - `/opt/vce/fm/conf`
  - `/etc/snmp/snmpd.conf`
  - `/etc/logrotate.d/syslog`
  - `/etc/srconf/agt/snmpd.cnf`
- JBoss configuration files
- Core VM administrative, configuration, and model database schemas and datafile

By default, the backup is performed daily at 12:00 AM. A maximum of seven backups are saved on the system. Core VM configuration files are backed up to: `/opt/vce/fm/backup/`

PostgreSQL database backup
Besides Core VM configuration files, VxBlock Central automatically backs up PostgreSQL database schema and data to restore VxBlock Central to a working state, if required.

VxBlock Central creates backups of the database in **tar.gz** file format to the `/opt/vce/fm/backup/postgres` directory. By default, VxBlock Central stores the PostgreSQL database backups for the current day and the previous two days.
The following example describes how VxBlock Central stores PostgreSQL database backup files:

- At 11:59 PM on Tuesday, VxBlock Central stores backup files for Tuesday, Monday, and Sunday.
- At 12:00 AM on Wednesday, VxBlock Central stores backup files for Wednesday, Tuesday, and Monday. VxBlock Central deletes the backup files for Sunday.

VxBlock Central backs up the database schema and data every 10 minutes. You can change the schedule and frequency of the backup tasks and run backups at any time, outside of scheduled tasks.

### Change the backup schedule and frequency

VxBlock Central uses a crontab file to specify the schedule and frequency of the configuration file and database backup tasks to the cron daemon. To change the schedule or frequency of any backup tasks, edit the crontab file.

#### Before you begin

Connect to the Core VM.

#### Procedure

1. To view the current cron tasks, type: `crontab -l`
   
   For example, the following cron tasks display:

   ```
   # HEADER: This file was autogenerated at <time_stamp> by puppet.
   # HEADER: While it can still be managed manually, it is definitely not recommended.
   # HEADER: Note particularly that the comments starting with 'Puppet Name' should
   # HEADER: not be deleted, as doing so could cause duplicate cron jobs.
   00 00 * * * /opt/vce/fm/install/backupConfig.sh > /dev/null 2>&1
   30 1,13 * * * /opt/vce/fm/bin/collectConfig.sh > /dev/null 2>&1
   # Puppet Name: vce-puppet
   */1 * * * * /usr/bin/puppet apply $(puppet config print manifest) > /dev/null 2>&1
   */10 * * * * /opt/vce/fm/install/backupDatabase.sh > /dev/null 2>&1
   
   # Puppet Name: vce-puppet
   */1 * * * * /usr/bin/puppet apply $(puppet config print manifest) > /dev/null 2>&1
   
   # Puppet Name: vce-puppet
   ```

2. To change a cron task, type: `crontab -e`

3. Make the required changes to the cron tasks and save the file.

   Ensure that you do not edit or delete the Puppet apply line:

   ```
   # Puppet Name: vce-puppet
   */1 * * * * /usr/bin/puppet apply $(puppet config print manifest) > /dev/null 2>&1
   ```

### Back up cron tasks

VxBlock Central uses cron tasks to run scripts at set intervals to back up configuration files.

VxBlock Central runs the following backup scripts with cron tasks:

<table>
<thead>
<tr>
<th>Script</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backupConfig.sh</td>
<td>Backs up VxBlock Central configuration files</td>
</tr>
<tr>
<td>collectConfig.sh</td>
<td>Backs up VxBlock System configuration files</td>
</tr>
<tr>
<td>backupDatabase.sh</td>
<td>Backs up PostgreSQL database schema and data</td>
</tr>
</tbody>
</table>

The following fields set the schedule and frequency of the cron tasks:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minute of the hour</td>
<td>A number, 0–59 for the corresponding minute of the hour or * for every minute</td>
</tr>
</tbody>
</table>
### Back up configuration files on demand

Back up configuration files for VxBlock Central outside of the automatically scheduled backup task.

**Before you begin**

Connect to the Core VM.

**Procedure**

1. Type: `cd /opt/vce/fm/install`

2. Type with the appropriate parameters: `sh backupConfig.sh`
   
   To view help usage, type: `sh backupConfig.sh -h`

**After you finish**

Change to the backup directory and verify that the backup files are successfully created.

### Back up databases on demand

Back up the PostgreSQL database schema and data outside of the automatically scheduled backup task.

**Before you begin**

Connect to the Core VM.

**Procedure**

1. Type: `cd /opt/vce/fm/install`

2. Type: `sh ./backupDatabase.sh`

**After you finish**

Change to the backup directory and verify that the backup files are successfully created.

### Restore the software configuration

Restore the VxBlock Central configuration from a backup file to overwrite the current configuration.

**Before you begin**

- Back up your configuration files.
- Connect to the Core VM.

**Procedure**

1. Type:
Manage VxBlock Systems with VxBlock Central

```bash
cd /opt/vce/fm/install
```

2. To view help usage, type: `sh restoreConfig.sh -h`

3. When prompted to confirm restoration:
   - Type 1 to continue restoring the VxBlock Central configuration.
   - Type 2 to quit.

**After you finish**

Check the following logfile to ensure that the restoration was successful: `opt/vce/fm/backup/restore_logs/restore_file_name.log`

**Restore databases**

Restore PostgreSQL database schema and data from backup files if the database becomes corrupted or you need to restore for some other reason.

**Before you begin**

Connect to the Core VM.

**Procedure**


2. Change to the subdirectory that contains the specific database backup that you want to restore.
   VxBlock Central stores database backups as **tar.gz** files in directories with the following format: `YYYY-DD-MM`.

3. To extract the **tar.gz** file, type:
   ```bash
tar -zxvf ./file_name -C /tmp
   ```

4. To confirm that the file is extracted, perform the following:
   a. Change to the `/tmp` directory.
   b. Type:
      ```bash
      ls -l
      ```
      The backed-up .sql file displays in the terminal window as follows: `database_name_DB.sql`

5. To switch to the Postgres user, type:
   ```bash
   sudo su - postgres
   ```

6. Before you restore the database, drop the schema and delete all existing data. If you do not drop the schema, you cannot successfully restore the database.

    The following table lists the schema in the databases that VxBlock Central backs up:

    | Database name | Schema |
    |---------------|--------|
    | model         | • admin
                   • model
                   • rbac |

    Dell EMC VxBlock™ and Vblock™ Systems 540 Administration Guide
a. Log in to the database: `psql database_name`

b. List all schema in the database: `select schema_name from information_schema.schemata where schema_owner='admin';`

c. Drop the schema: `drop schema if exists schema_name cascade;`

d. Confirm that the drop was successful: `select schema_name from information_schema.schemata where schema_owner='admin';`

e. Exit: `

7. To restore the database, type:

`psql -d database_name -U postgres -f path_to_backed_up_sql_file`

Where:

- `-d` specifies the name of the database to which you are restoring the schema and data.
- `-f` specifies the path of the backed-up .sql file.

⚠️ **Note:** The name of the database to which you are restoring must match the name of the database from the backed-up .sql file.

For more information about the command to restore the database, see the appropriate PostgreSQL documentation.

---

**After you finish**

Repeat the preceding steps for each backed-up .sql file to restore.

---

**Back up the Core VM**

To maintain a low recovery time objective (RTO), it is critical that you back up the VxBlock Central at the VM level. If you do not back up the Core VM, you can slow recovery and limit visibility into the management of your VxBlock System.

**Procedure**

1. Perform daily backups of the Core VM at 7 AM and PM.
2. Perform daily backups of the VMware vCenter SQL Server database every four hours.
   - This schedule coincides with daily server backups at 3, 7, and 11 AM and PM.
3. Set your backup retention period to 35 days.

---

**Back up and restore the MSM VM and MSP VM**

Perform an agent-less VM backup using your backup software.

---

**Back up component configuration files**

Every VxBlock System is deployed with backups of the VxBlock System component configuration files. To ensure you can recover from the loss of a VxBlock System or a single component, back up configuration files daily.

VxBlock Central automatically gathers every configuration file in a VxBlock System component and stores the configuration files on the Core VM. For disaster recovery, you only need to:

- Save VxBlock System configuration files to a remote system.
- Back up the VMware vCenter SQL server.

Each Converged System is deployed with configuration backups for each component, as follows:
<table>
<thead>
<tr>
<th>Converged System</th>
<th>Component</th>
</tr>
</thead>
</table>
| Vblock System 200 series | Cisco Nexus 5000 Switch  
Cisco Nexus 1000V Switch  
Cisco Nexus 3000  
Cisco C-Series servers  
VNX  
Vblock compute servers (CIMC)  
Management servers (CIMC) |
| Vblock System 300 series | Cisco MDS 9000  
Cisco Nexus 5000  
Cisco Nexus 1000V  
Cisco Nexus 3000  
Cisco UCS fabric interconnects (UCS Manager)  
VNX  
Management servers (CIMC)  
Technology Extension for Storage  
Converged Technology Extension for Cisco UCS compute |
| VxBlock System 340      | Cisco MDS 9000  
Cisco Nexus 5000  
Cisco Nexus 1000V  
Cisco Nexus 3000  
Cisco UCS fabric interconnects (UCS Manager)  
VNX  
Management servers (CIMC)  
Technology Extension for Storage |
| VxBlock System 350      | Cisco MDS 9000  
Cisco Nexus 5000  
Cisco Nexus 1000V  
Cisco Nexus 3000  
Cisco UCS fabric interconnects (UCS Manager)  
Management servers (CIMC)  
Technology Extension for Storage  
Converged Technology Extension for Cisco UCS compute |
<table>
<thead>
<tr>
<th>Converged System</th>
<th>Component</th>
</tr>
</thead>
</table>
| Vblock System 540        | Cisco MDS 9000  
|                          | Cisco Nexus 5000  
|                          | Cisco Nexus 3000  
|                          | Cisco Nexus 7000 and/or Cisco Nexus 9000  
|                          | Cisco Nexus 1000V  
|                          | Cisco UCS fabric interconnects (UCS Manager)  
|                          | XtremIO  
|                          | Management servers (CIMC)  
|                          | Technology Extension for Storage  
|                          | Converged Technology Extension for Cisco UCS compute  |
| VxBlock System 540       | Cisco MDS 9000  
|                          | Cisco Nexus 5000  
|                          | Cisco Nexus 3000  
|                          | Cisco Nexus 7000 and/or Cisco Nexus 9000  
|                          | Cisco Nexus 1000V  
|                          | Cisco UCS fabric interconnects (UCS Manager)  
|                          | XtremIO  
|                          | Management servers (CIMC)  
|                          | Technology Extension for Storage  |
| Vblock System 700 series | Cisco MDS 9000  
|                          | Cisco Nexus 5000  
|                          | Cisco Nexus 3000  
|                          | Cisco Nexus 7000 and/or Cisco Nexus 9000  
|                          | Cisco Nexus 1000V  
|                          | Cisco UCS fabric interconnects (UCS Manager)  
|                          | Management servers (CIMC)  
|                          | Technology Extension for Storage  
|                          | Converged Technology Extension for Cisco UCS compute  |
| VxBlock System 740       | Cisco MDS 9000  
|                          | Cisco Nexus 5000  
|                          | Cisco Nexus 3000  
|                          | Cisco Nexus 7000, and/or Cisco Nexus 9000  
|                          | Cisco Nexus 1000V  
|                          | Cisco UCS fabric interconnects (UCS Manager)  
|                          | Management servers (CIMC)  
<p>|                          | Technology Extension for Storage  |</p>
<table>
<thead>
<tr>
<th>Converged System</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>VxBlock System 1000</td>
<td>Cisco MDS 9000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 3000</td>
</tr>
<tr>
<td></td>
<td>Cisco UCS fabric interconnects (UCS Manager)</td>
</tr>
<tr>
<td></td>
<td>Management servers (CIMC)</td>
</tr>
<tr>
<td></td>
<td>Technology Extension for Storage</td>
</tr>
<tr>
<td></td>
<td>Converged Technology Extension for Cisco UCS compute</td>
</tr>
<tr>
<td></td>
<td>XtremIO</td>
</tr>
<tr>
<td>AMP-3S</td>
<td>Management servers (CIMC)</td>
</tr>
<tr>
<td>Vblock Specialized Systems for Extreme</td>
<td>Cisco UCS fabric interconnects (UCS Manager)</td>
</tr>
<tr>
<td>Applications</td>
<td>Cisco Nexus 3000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 5000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 1000V</td>
</tr>
<tr>
<td></td>
<td>XtremIO</td>
</tr>
<tr>
<td></td>
<td>Management servers (CIMC)</td>
</tr>
</tbody>
</table>

**Manual backup**

Due to component limitations or known issues, the following configuration files are not backed up:

- Dell EMC Unity storage on VxBlock Systems
- Cisco Nexus operating system switches
  
  See the relevant *Backing up Cisco Nexus operating system switches* in the *Administration Guide*.
- VMware vCenter Server
  
  See the *Backup the VMware vCenter SQL server database* section of the *Administration Guide* that is relevant to your VxBlock System.

**Backup schedule, location, and retention period**

By default, the VxBlock Central backs up twice a day at 1:30 AM and 1:30 PM to the following directories:

- /opt/vce/backup/amp2
- /opt/vce/backup/storage
- /opt/vce/backup/network
- /opt/vce/backup/compute

VxBlock Central retains backed up configuration files for seven days by default. However, you can configure the retention period within a range of 3 days to 30 days. Use the `collectConfig.sh` script in the `/opt/vce/fm/bin` directory on the Core VM specify the retention period. To view help usage, run `sh collectConfig.sh -h`.

**Saving VxBlock System configuration files**

Use the following VxBlock Central REST resource to export an archive of the VxBlock System configuration files:

```
https://FQDN:8443/fm/configcollector
```

Where *FQDN* is the fully qualified domain name of the Core VM:

This REST resource exports an archive of all configuration files under the `/opt/vce/backup` directory.
Ports and protocols

Review ports and protocols for communicating with VxBlock Central.

Communication with VxBlock Central occurs through northbound traffic over an external network and through southbound traffic to Converged System components.

Review the ports and protocols to help troubleshoot issues after installation.

Open port assignments

MSM VM runs several small services on various ports. Not all ports on the MSM VM are opened through the firewall.

The following ports are available from outside of the MSM VM for VxBlock Central:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Linux Application</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>SSH</td>
<td>SSH</td>
</tr>
<tr>
<td>80</td>
<td>UDP</td>
<td>Apache HTTP</td>
<td>Web server providing access to the VxBlock Central and all REST APIs. Requests are redirected to Port 443.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Apache HTTP</td>
<td>HTTPS access to VxBlock Central and all REST APIs</td>
</tr>
<tr>
<td>5672</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>Message service that VxBlock Central uses</td>
</tr>
<tr>
<td>7000</td>
<td>TCP</td>
<td>SSL</td>
<td>Cassandra SSL internode communication</td>
</tr>
<tr>
<td>9042</td>
<td>TCP, UDP</td>
<td>Cassandra</td>
<td>Cassandra native client port</td>
</tr>
<tr>
<td>9160</td>
<td>TCP</td>
<td>Cassandra</td>
<td>Cassandra thrift client port</td>
</tr>
<tr>
<td>9301</td>
<td>TCP</td>
<td>Elasticsearch</td>
<td>Elasticsearch node-to-node communication</td>
</tr>
</tbody>
</table>

If the port 9301 is not open:

1. Type `vi /etc/sysconfig/iptables`.
2. Add the following line: `-A INPUT -p tcp -m state --state NEW,ESTABLISHED -m tcp --dport 9301 -j ACCEPT`.
3. Type `service iptables save`.
4. Type `service iptables restart`.
5. Type `netstat -l | grep 9301` to check the status of the port.

Note: LISTEN indicates that the port is open.

Northbound ports and protocols

The third-party applications and network management systems (NMS) can use northbound ports and protocols to communicate with VxBlock Central.

The following ports are available for VxBlock Central:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Usage</th>
<th>Destination</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>HTTP</td>
<td>RCM content distribution network (CDN) destination addresses that include the</td>
<td>Outbound</td>
</tr>
</tbody>
</table>
### Southbound ports and protocols

VxBlock Central uses specific ports and protocols for southbound communication with VxBlock System components. The following ports are available for VxBlock Central:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Usage</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>69</td>
<td>UDP</td>
<td>TFTP traffic from the Configuration Collector to back up VxBlock System component configuration</td>
<td>VxBlock Central</td>
</tr>
<tr>
<td>162</td>
<td>UDP</td>
<td>SNMP trap messages</td>
<td></td>
</tr>
<tr>
<td>514</td>
<td>UDP</td>
<td>syslog messages</td>
<td></td>
</tr>
</tbody>
</table>

### Compute components

Review the ports and protocols that VxBlock Central uses for communication with compute components. The following Dell iDRAC ports are available for VxBlock Central:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Usage</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>iDRAC accesses this port using the RedFish API.</td>
<td>iDRAC</td>
</tr>
</tbody>
</table>
Network components
Review the ports and protocols that VxBlock Central uses for communication with network switches, including physical and virtual switches.

The following ports are available for VxBlock Central:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Usage</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>Secure shell (SSH)</td>
<td>Network switches</td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>General SNMP messages</td>
<td></td>
</tr>
</tbody>
</table>

Storage components
Review the ports and protocols that VxBlock Central uses for communication with various storage components.

The following ScaleIO ports are available for VxBlock Central:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Usage</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>REST API</td>
<td>ScaleIO</td>
</tr>
</tbody>
</table>

Management components
VxBlock Central communicates with management components using certain ports and protocols.

The following ports are available for VxBlock Central:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Usage</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>161</td>
<td>TCP</td>
<td>SNMP</td>
<td>IPI appliance</td>
</tr>
</tbody>
</table>

Virtualization components
Review the ports and protocols that VxBlock Central uses for communication with virtualization components.

The following ports are available for VxBlock Central:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Usage</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>XML API</td>
<td>VMware vCenter Server</td>
</tr>
</tbody>
</table>

Reference
Use these commands and scripts to configure, monitor, and maintain VxBlock Central VMs.

Core VM commands

<table>
<thead>
<tr>
<th>Command or script</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backupConfig.sh</td>
<td>Backs up VxBlock Central configuration files</td>
</tr>
<tr>
<td></td>
<td>Run this script from the /opt/vce/fm/install directory.</td>
</tr>
<tr>
<td>backupDatabase.sh</td>
<td>Backs up PostgreSQL database schema and data</td>
</tr>
<tr>
<td></td>
<td>Run this script from the /opt/vce/fm/install directory.</td>
</tr>
<tr>
<td>Command or script</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>collectConfig.sh</td>
<td>Collects and backs up VxBlock System configuration files. Run this script from the /opt/vce/fm/bin directory. <strong>Note:</strong> The <code>collectConfig.sh</code> command is supported on a VxBlock System only.</td>
</tr>
<tr>
<td>configureSyslogForward</td>
<td>Configures syslog forwarding. <strong>Note:</strong> The <code>configureSyslogForward</code> command is supported on a VxBlock System only.</td>
</tr>
<tr>
<td>configureNTP</td>
<td>Manages network time protocol (NTP) synchronization settings on the Core VM</td>
</tr>
<tr>
<td>configureSNMP</td>
<td>Configures northbound SNMP communication between VxBlock Central and a network management system (NMS) or trap target. <strong>Note:</strong> The <code>configureSNMP</code> command is supported on a VxBlock System only.</td>
</tr>
<tr>
<td>createEULASoftCopy</td>
<td>Creates a soft copy of the end user license agreement (EULA) in the following directory: /opt/vce/fm/eula</td>
</tr>
<tr>
<td>displayEula</td>
<td>Displays the end user license agreement (EULA). Run this command from the /opt/vce/fm/bin directory.</td>
</tr>
<tr>
<td>export-fm-config.sh</td>
<td>Exports VxBlock Central configuration to the following directory: /opt/vce/fm/back. Run this script from the /opt/vce/fm/bin directory.</td>
</tr>
<tr>
<td>getFMagentInfo</td>
<td>Displays version and build information about VxBlock Central</td>
</tr>
<tr>
<td>install_content.sh</td>
<td>Installs compliance content. Run this script from the /opt/vce/compliance/content directory.</td>
</tr>
<tr>
<td>restoreConfig.sh</td>
<td>Restores VxBlock Central configuration from a backup file. Run this script from the /opt/vce/fm/install directory.</td>
</tr>
</tbody>
</table>
| setSNMPParams           | Modifies the following SNMP parameters for a VxBlock System:  
  - sysName  
  - sysContact  
  - sysLocation  
  Use double quotes for values that contain space characters. |
<p>| shutdown -h now         | Stops the Core VM |
| shutdown -r now         | Restarts the Core VM |
| slibCasChangepw.sh      | Changes the Central Authentication Service (CAS) password. Run this script from the /opt/vce/fm/bin directory. |
| startEulaAcceptance     | Starts the end user license agreement (EULA) |
| startFMagent            | Starts the Core VM FM Agent services. Running this command starts the discovery process. |
| stopFMagent             | Stops the Core VM FM Agent services. Running this command stops the discovery process. |</p>
<table>
<thead>
<tr>
<th>Command or script</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vce-puppet-disable.pp</td>
<td>Enables the Puppet service management utility to monitor VxBlock Central</td>
</tr>
<tr>
<td></td>
<td>services. Run this script from the /etc/puppet/manifests directory using the</td>
</tr>
<tr>
<td></td>
<td>puppet apply command.</td>
</tr>
<tr>
<td>vce-puppet-enable.pp</td>
<td>Enables the Puppet service management utility to monitor VxBlock Central</td>
</tr>
<tr>
<td></td>
<td>services. Run this script from the /etc/puppet/manifests directory using the</td>
</tr>
<tr>
<td></td>
<td>puppet apply command.</td>
</tr>
<tr>
<td>vce-puppet-start.pp</td>
<td>Start all VxBlock Central services. Run this script from the /etc/puppet/</td>
</tr>
<tr>
<td></td>
<td>manifests directory using the puppet apply command. This script uses the</td>
</tr>
<tr>
<td></td>
<td>Puppet service management utility to start services.</td>
</tr>
<tr>
<td>vce-puppet-stop.pp</td>
<td>Stop all VxBlock Central services. Run this script from the /etc/puppet/</td>
</tr>
<tr>
<td></td>
<td>manifests directory using the puppet apply command. This script uses the</td>
</tr>
<tr>
<td></td>
<td>Puppet service management utility to gracefully stop services and prevent</td>
</tr>
<tr>
<td></td>
<td>issues that can occur when stopping services individually.</td>
</tr>
<tr>
<td>vision start</td>
<td>Checks if each service is running. If not, starts the service.</td>
</tr>
</tbody>
</table>

### MSM VM commands

<table>
<thead>
<tr>
<th>Command or script</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>addSlibHost.sh</td>
<td>Adds a Core VM to an existing MSM VM Run this script from the /opt/vce/multivbmgmt/install directory.</td>
</tr>
<tr>
<td>caschangepw.sh</td>
<td>Changes the CAS password for MSM VM Run this script from the /opt/vce/multivbsecurity/bin directory.</td>
</tr>
<tr>
<td>credential-manager-cli</td>
<td>Lets you manage credentials within the MSM VM environment. Run this script</td>
</tr>
<tr>
<td></td>
<td>from the /opt/vce/credential-management/bin directory.</td>
</tr>
<tr>
<td>joinMSMCluster.sh</td>
<td>Adds an MSM VM to that node in the cluster Run this script from the /opt/vce/multivbmgmt/install directory.</td>
</tr>
<tr>
<td>nodetool status</td>
<td>Verifies that Cassandra is installed and configured correctly Run this</td>
</tr>
<tr>
<td></td>
<td>command from the /opt/cassandra/bin directory.</td>
</tr>
<tr>
<td>service multivbmgmt status</td>
<td>Verifies that the multivbmgmt service is running</td>
</tr>
<tr>
<td>service multivbmgmt start</td>
<td>Starts the multivbmgmt service</td>
</tr>
<tr>
<td>service tomcat status</td>
<td>Verifies that the tomcat service is running</td>
</tr>
<tr>
<td>service tomcat start</td>
<td>Starts the tomcat service</td>
</tr>
<tr>
<td>service vision-credential-manager status</td>
<td>Verifies that the Credential Manager service is running</td>
</tr>
</tbody>
</table>
## Command or script

<table>
<thead>
<tr>
<th>Command or script</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>service vision-credential-manager start</code></td>
<td>Starts the Credential Manager service</td>
</tr>
<tr>
<td><code>service vision-mvb-compliance status</code></td>
<td>Verifies that the compliance service is running</td>
</tr>
<tr>
<td><code>service vision-mvb-compliance start</code></td>
<td>Starts the compliance service</td>
</tr>
<tr>
<td><code>service vision-shell status</code></td>
<td>Verifies that the VxBlock Central Shell service is running</td>
</tr>
<tr>
<td><code>service vision-shell start</code></td>
<td>Starts the VxBlock Central Shell service</td>
</tr>
<tr>
<td><code>start_cassandra.sh</code></td>
<td>Starts Cassandra</td>
</tr>
<tr>
<td></td>
<td>Run this script from the <code>/opt/cassandra/install</code> directory.</td>
</tr>
<tr>
<td><code>stop_cassandra.sh</code></td>
<td>Stops Cassandra</td>
</tr>
<tr>
<td></td>
<td>Run this script from the <code>/opt/cassandra/install</code> directory.</td>
</tr>
<tr>
<td><code>vision start</code></td>
<td>Checks if each service is running. If not, starts the service.</td>
</tr>
<tr>
<td><code>service vision-web-ui restart</code></td>
<td>Restarts the VxBlock Central Web UI service</td>
</tr>
</tbody>
</table>

## MSP VM commands

<table>
<thead>
<tr>
<th>Command or script</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/opt/vce/msp/install/update-cas-password.sh</code></td>
<td>Enables you to update the Central Authentication Service (CAS) password for the admin user in a clustered environment</td>
</tr>
<tr>
<td><code>/opt/vce/msp/install/update-proxy-password.sh</code></td>
<td>Enables you to set a password for a proxy server to access the RCM content distribution network This script can also be used to change the proxy password if required.</td>
</tr>
<tr>
<td><code>/opt/vce/msp/install/update-assetmanager-db-password.sh</code></td>
<td>Enables you to change the default password for the Asset Manager</td>
</tr>
<tr>
<td><code>/opt/vce/msp/install/update-contentshare-db-password.sh</code></td>
<td>Enables you to change the default password for the Content Share PostgreSQL database</td>
</tr>
<tr>
<td><code>vision status</code></td>
<td>Provides a status on all MSP services</td>
</tr>
<tr>
<td><code>vision stop</code></td>
<td>Stops all MSP services</td>
</tr>
<tr>
<td><code>vision start</code></td>
<td>Starts all MSP services</td>
</tr>
<tr>
<td><code>service vision-contentsource restart</code></td>
<td>Restarts the contentsource service</td>
</tr>
<tr>
<td><code>service vision-contentsource stop</code></td>
<td>Stops the contentsource service</td>
</tr>
<tr>
<td><code>service vision-contentsource start</code></td>
<td>Starts the contentsource service</td>
</tr>
<tr>
<td><code>service vision-contentshare restart</code></td>
<td>Restarts the contentshare service</td>
</tr>
<tr>
<td><code>service vision-contentshare stop</code></td>
<td>Stops the contentshare service</td>
</tr>
<tr>
<td><code>service vision-contentshare start</code></td>
<td>Starts the contentshare service</td>
</tr>
<tr>
<td><code>service vision-downloader restart</code></td>
<td>Restarts the downloader service</td>
</tr>
<tr>
<td><code>service vision-downloader stop</code></td>
<td>Stops the downloader service</td>
</tr>
<tr>
<td>Command or script</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>service vision-downloader start</code></td>
<td>Starts the downloader service</td>
</tr>
<tr>
<td><code>service vision-assetmanager restart</code></td>
<td>Restarts the assetmanager service</td>
</tr>
<tr>
<td><code>service vision-assetmanager stop</code></td>
<td>Stops the assetmanager service</td>
</tr>
<tr>
<td><code>service vision-assetmanager start</code></td>
<td>Starts the assetmanager service</td>
</tr>
</tbody>
</table>

### Configuration editor component reference

Use the tables to configure VxBlock Systems with the configuration editor. All values, including location information, are mandatory.

#### System configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Rules</th>
<th>Field value example</th>
</tr>
</thead>
<tbody>
<tr>
<td>System type</td>
<td>Indicates the VxBlock System product</td>
<td>VXBLOCK</td>
</tr>
<tr>
<td></td>
<td>The mandatory value is VXBLOCK.</td>
<td></td>
</tr>
<tr>
<td>Product</td>
<td>Indicates the VxBlock System product</td>
<td>VxBlock</td>
</tr>
<tr>
<td></td>
<td>The mandatory value is VxBlock.</td>
<td></td>
</tr>
<tr>
<td>Product type</td>
<td>The first three digits determine the VxBlock System type.</td>
<td>1000XXXX</td>
</tr>
<tr>
<td>Serial number</td>
<td>Any value</td>
<td>VB1000-975-318-642</td>
</tr>
<tr>
<td>Component tag</td>
<td>Any value</td>
<td>VX-1000</td>
</tr>
<tr>
<td>Geo</td>
<td>Data center location</td>
<td>Anytown, MA</td>
</tr>
<tr>
<td>Building</td>
<td>Building name</td>
<td>Building 4</td>
</tr>
<tr>
<td>Floor</td>
<td>Floor number</td>
<td>1</td>
</tr>
<tr>
<td>Room</td>
<td>Room number</td>
<td>1</td>
</tr>
<tr>
<td>Row</td>
<td>Row number</td>
<td>1</td>
</tr>
<tr>
<td>Tile</td>
<td>Tile number</td>
<td>1</td>
</tr>
<tr>
<td>Component tag</td>
<td>Any value</td>
<td>VMAX3-Storage</td>
</tr>
<tr>
<td>Serial number</td>
<td>Any value</td>
<td>VxBlock-abc-123</td>
</tr>
</tbody>
</table>

#### Component configuration settings

VxBlock Central does not support the use of a single ECOM server IP address for multiple storage arrays. Specify a different ECOM server IP address for each additional storage array that you want to add.

<table>
<thead>
<tr>
<th>Component type</th>
<th>Field</th>
<th>Rules</th>
<th>Field value example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute server</td>
<td>In AMP</td>
<td>Specifies if the component is a part of the AMP configuration</td>
<td>x</td>
</tr>
<tr>
<td>Compute server</td>
<td>Name</td>
<td>First server: sys (default); Additional servers: sys###, where sys is lowercase, and ### is a unique number (for example sys2)</td>
<td>sys</td>
</tr>
<tr>
<td>Component type</td>
<td>Field</td>
<td>Rules</td>
<td>Field value example</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Compute server</td>
<td>Type</td>
<td>Must be one of the following: UCS, C200M1, C200M2, C220M3, C220M4, C220M5, C240M3, C240M4</td>
<td>UCS</td>
</tr>
<tr>
<td>Compute server</td>
<td>Component tag</td>
<td>Any meaningful value</td>
<td>VMABO-UCS-1</td>
</tr>
<tr>
<td>Compute server</td>
<td>Server IPv4/IPv6 Address</td>
<td>Dotted IP address</td>
<td>10.1.139.30 / 2010:201::279</td>
</tr>
<tr>
<td>Compute server</td>
<td>Username</td>
<td>SSH username</td>
<td>admin</td>
</tr>
<tr>
<td>Compute server</td>
<td>Method</td>
<td>Must be one of the following: REDFISH, SNMPV2C, IMPIV2, WEBSERVICE, SSH</td>
<td>REDFISH</td>
</tr>
<tr>
<td>Compute server</td>
<td>Password</td>
<td>SSH password</td>
<td>password</td>
</tr>
<tr>
<td>Compute server</td>
<td>Community</td>
<td>The SNMP community string The community string is necessary only for the SNMP method.</td>
<td>public</td>
</tr>
<tr>
<td>AMP</td>
<td>Amp type</td>
<td>VxBlock System: AMP-type, where type is the AMP model in your environment</td>
<td>AMP-2S</td>
</tr>
<tr>
<td>AMP</td>
<td>Component tag</td>
<td>Any meaningful value</td>
<td>Management</td>
</tr>
<tr>
<td>AMP</td>
<td>Serial number</td>
<td>Any meaningful value</td>
<td>AMP-KYL-123</td>
</tr>
<tr>
<td>Component credentials</td>
<td>Community</td>
<td>SNMP community string</td>
<td>public</td>
</tr>
<tr>
<td>Component credentials</td>
<td>Username</td>
<td>Username</td>
<td>root</td>
</tr>
<tr>
<td>Component credentials</td>
<td>Method</td>
<td>Must be one of the following: IPMIV2, SNMPV2C, WEBSERVICE, SSH, REDFISH</td>
<td>SSH</td>
</tr>
<tr>
<td>Component credentials</td>
<td>Password</td>
<td>Password</td>
<td>password</td>
</tr>
<tr>
<td>Switch</td>
<td>In AMP</td>
<td>Specifies if the component is a part of the AMP configuration</td>
<td>x</td>
</tr>
<tr>
<td>Switch</td>
<td>Type</td>
<td>Must be one of the following: CA3750, MDS9000, Nexus3000, Nexus5000, Nexus7000, Nexus9000, Nexus1000V, or NSX</td>
<td>Nexus5000</td>
</tr>
<tr>
<td>Switch</td>
<td>Method</td>
<td>Must be one of the following: IPMIV2, SNMPV2C, WEBSERVICE, SSH</td>
<td>snmpv2c</td>
</tr>
<tr>
<td>Switch</td>
<td>IP Address</td>
<td>Dotted IP address</td>
<td>10.1.139.22</td>
</tr>
<tr>
<td>Component type</td>
<td>Field</td>
<td>Rules</td>
<td>Field value example</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------</td>
<td>------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Switch</td>
<td>Username</td>
<td>SSH username</td>
<td>admin</td>
</tr>
<tr>
<td>Switch</td>
<td>Password</td>
<td>Password</td>
<td>password</td>
</tr>
<tr>
<td>Switch</td>
<td>Community</td>
<td>SNMP community string</td>
<td>public</td>
</tr>
<tr>
<td>DCNM</td>
<td>IPv4 Address</td>
<td>Dotted IP address</td>
<td>10.1.33.232</td>
</tr>
<tr>
<td>Storage array VMAX/PowerMax</td>
<td>In AMP</td>
<td>Specifies if the component is a part of the AMP configuration</td>
<td>x</td>
</tr>
<tr>
<td>Storage array VMAX/PowerMax</td>
<td>Type</td>
<td>Must be one of the following: VMAX, VMAX10K, VMAX20K, VMAX40K, VMAX100K, VMAX200K, VMAX400K, VMAX3, VMAXe, VMAX450F, VMAX450FX, VMAX850F, VMAX850FX</td>
<td>VMAX10K</td>
</tr>
<tr>
<td>Storage array VMAX/PowerMax</td>
<td>Component tag</td>
<td>Must be one of the following: VMAX10K-ARRAY, VMAX20K-ARRAY, VMAX40K-ARRAY, VMAX3-ARRAY, VMAX100K-ARRAY, VMAX200K-ARRAY, VMAX250F-ARRAY, VMAX250FX-ARRAY, VMAX400K-ARRAY, VMAX-ARRAY, VMAXe-ARRAY, VMAX450F-ARRAY, VMAX450FX-ARRAY, VMAX850F-ARRAY, VMAX850FX-ARRAY</td>
<td>VMAX10K-ARRAY</td>
</tr>
<tr>
<td>Storage array VMAX/PowerMax</td>
<td>IP Address</td>
<td>Dotted IP address</td>
<td>10.1.139.52</td>
</tr>
<tr>
<td>Storage array VMAX/PowerMax</td>
<td>Which</td>
<td>Must be VMAX.</td>
<td>VMAX</td>
</tr>
<tr>
<td>Storage array VMAX/PowerMax</td>
<td>Method</td>
<td>Dotted IP address; CIM entry point when Which is an ECOM server or Control Station.</td>
<td>10.1.139.42</td>
</tr>
<tr>
<td>Storage array VMAX/PowerMax</td>
<td>Username</td>
<td>Username</td>
<td>fmuser</td>
</tr>
<tr>
<td>Storage array VMAX/PowerMax</td>
<td>Password</td>
<td>Password</td>
<td>password</td>
</tr>
<tr>
<td>Storage array VMAX w/ gateway</td>
<td>In AMP</td>
<td>Specifies if the component is a part of the AMP configuration</td>
<td>x</td>
</tr>
<tr>
<td>Storage array VMAX w/ gateway</td>
<td>Type</td>
<td>Must be one of the following: VMAX, VMAX10K, VMAX20K, VMAX40K, VMAX100K, VMAX200K, VMAX400K, VMAX3, VMAXe, VMAX450F, VMAX450FX, VMAX850F, VMAX850FX</td>
<td>VMAX10K</td>
</tr>
<tr>
<td>Component type</td>
<td>Field</td>
<td>Rules</td>
<td>Field value example</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Storage array VMAX w/</td>
<td>Component tag</td>
<td>Must be one of the following:</td>
<td>VMAX10K-ARRAY</td>
</tr>
<tr>
<td>gateway</td>
<td></td>
<td>VMAX10K-ARRAY, VMAX20K-ARRAY, VMAX40K-ARRAY, VMAX3-ARRAY, VMAX100K-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ARRAY, VMAX200K-ARRAY, VMAX400K-ARRAY, VMAXARRAY, VMAXe-ARRAY, VMAX-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>450F-ARRAY, VMAX450FX-ARRAY, VMAX850F-ARRAY, VMAX850FX-ARRAY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Address</td>
<td>Dotted IP address</td>
<td>10.1.139.52</td>
</tr>
<tr>
<td></td>
<td>Which</td>
<td>Must be VMAX</td>
<td>VMAX</td>
</tr>
<tr>
<td></td>
<td>Method</td>
<td>Dotted IP address</td>
<td>10.1.139.42</td>
</tr>
<tr>
<td></td>
<td>Username</td>
<td>VMAX username</td>
<td>fmuser</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>VMAX password</td>
<td>password</td>
</tr>
<tr>
<td></td>
<td>Which</td>
<td>The second Which field must be gateway.</td>
<td>gateway</td>
</tr>
<tr>
<td></td>
<td>Method</td>
<td>The second Method is a dotted IP address.</td>
<td>10.1.139.42</td>
</tr>
<tr>
<td></td>
<td>Username</td>
<td>NAS administrator username</td>
<td>nasadmin</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>NAS administrator password</td>
<td>password</td>
</tr>
<tr>
<td></td>
<td>In AMP</td>
<td>Specifies if the component is a part of the AMP configuration</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Must be XTREMIO</td>
<td>XTREMIO</td>
</tr>
<tr>
<td></td>
<td>Component tag</td>
<td>Must be XIO-ARRAY-1</td>
<td>XIO-ARRAY-1</td>
</tr>
<tr>
<td></td>
<td>IP Address</td>
<td>Dotted IP address</td>
<td>10.1.139.52</td>
</tr>
<tr>
<td></td>
<td>Which</td>
<td>Must be XTREMIO</td>
<td>XTREMIO</td>
</tr>
<tr>
<td></td>
<td>Method</td>
<td>Must be xml</td>
<td>xml</td>
</tr>
<tr>
<td></td>
<td>Username</td>
<td>XtremIO username</td>
<td>admin</td>
</tr>
<tr>
<td>Component type</td>
<td>Field</td>
<td>Rules</td>
<td>Field value example</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------</td>
<td>--------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Storage array</td>
<td>Password</td>
<td>XtremIO password</td>
<td>password</td>
</tr>
<tr>
<td>XtremIO</td>
<td>In AMP</td>
<td>Specifies if the component is a part of the AMP configuration</td>
<td>x</td>
</tr>
<tr>
<td>Isilon</td>
<td>Type</td>
<td>Must be ISILON.</td>
<td>ISILON</td>
</tr>
<tr>
<td></td>
<td>Component tag</td>
<td>Must be ISILON-ARRAY-CLUSTER-1</td>
<td>ISILON-ARRAY-CLUSTER-1</td>
</tr>
<tr>
<td></td>
<td>IP Address</td>
<td>Dotted IP address</td>
<td>10.1.139.52</td>
</tr>
<tr>
<td></td>
<td>Method</td>
<td>Must be one of the following: IPMIv2, SNMPv2C, WEBSERVICE, SSH</td>
<td>snmpv2c</td>
</tr>
<tr>
<td></td>
<td>Username</td>
<td>Isilon username</td>
<td>admin</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>Isilon password</td>
<td>password</td>
</tr>
<tr>
<td></td>
<td>In AMP</td>
<td>Specifies if the component is a part of the AMP configuration</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Must be UNITY</td>
<td>UNITY</td>
</tr>
<tr>
<td></td>
<td>Component tag</td>
<td>Must be UNITY-ARRAY-x, where x is the number of the array</td>
<td>UNITY-ARRAY-1</td>
</tr>
<tr>
<td></td>
<td>IPv4/IPv6 Address</td>
<td>Dotted IP address</td>
<td>10.1.139.52/ 201::XX</td>
</tr>
<tr>
<td></td>
<td>Method</td>
<td>Must be restApi</td>
<td>restApi</td>
</tr>
<tr>
<td></td>
<td>Username</td>
<td>Dell EMC Unity username</td>
<td>admin</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>Dell EMC Unity password</td>
<td>password</td>
</tr>
<tr>
<td>Component type</td>
<td>Field</td>
<td>Rules</td>
<td>Field value example</td>
</tr>
<tr>
<td>----------------</td>
<td>-------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| vCenter        | In AMP| Specifies if the component is a part of the AMP configuration  
If configuring a shared vCenter with MSM VM, include the shared vCenter server information in the configuration file on each Core VM associated with an MSM VM node. | x                   |
| vCenter        | Name  | vCenter1, vCenter2, … vCenterN, and so forth:  
If configuring a shared vCenter with MSM VM, include the shared vCenter server information in the configuration file on each Core VM associated with an MSM VM node.  
When a shared vCenter resides on an SMP, that SMP is not discovered. However, the fact that multiple VxBlock Systems share the vCenter is apparent in the results that are returned for a find VIDManager query. | vcenter1            |
| vCenter        | URL   | A dotted IP address to the vCenter server:  
If configuring a shared vCenter with MSM VM, include the shared vCenter server information in the configuration file on each Core VM associated with an MSM VM node. | 10.1.139.39        |

<table>
<thead>
<tr>
<th>Application host</th>
<th>Name</th>
<th>Application hostname</th>
<th>app-host-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application host</td>
<td>IP Address</td>
<td>Dotted IP address</td>
<td>10.1.139.42</td>
</tr>
<tr>
<td>Application host</td>
<td>Username</td>
<td>Username</td>
<td>admin</td>
</tr>
<tr>
<td>Application host</td>
<td>Password</td>
<td>Password</td>
<td>password</td>
</tr>
<tr>
<td>DCNM</td>
<td>address</td>
<td>Dotted IP address</td>
<td>10.3.xx.xx</td>
</tr>
</tbody>
</table>

### Components, APIs, and services for VMs

Components, APIs, and services for VMs are described.

The following table provides components, APIs, and services running on each Core VM:

<table>
<thead>
<tr>
<th>Components, APIs, services</th>
<th>Description</th>
</tr>
</thead>
</table>
| FMAgent                     | On a scheduled basis, retrieves information from VxBlock System components  
The information is used to update the system information in PostgreSQL.     |
| VxBlock Central Repository  | Provides an API to manage VxBlock Central on the Core VM that RCM content  
prepositioning uses to store RCM content                                       |
| VxBlock Central API for VxBlock Central Security | Provides REST resources for controlling access to system resources through role-based access control |
RabbitMQ

Provides the Core VM services and applications with a common platform to send and receive messages asynchronously and ensures that messages are delivered.

PostgreSQL

Stores collected data, credentials, and records for Core VM services.

The following table provides components, APIs, and services running on each MSM VM:

<table>
<thead>
<tr>
<th>Components, APIs, and services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RabbitMQ</td>
<td>Provides MSM VM services and applications with a common platform to send and receive messages asynchronously</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>Stores collected data, credentials, and records for Core VM services.</td>
</tr>
</tbody>
</table>

The following table shows the components and services running on each MSP VM:

<table>
<thead>
<tr>
<th>Components, APIs, and services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache HTTP Proxy</td>
<td>Used as a proxy server for all HTTP-based communication to ensure VxBlock Central is accessible through the proxy server</td>
</tr>
<tr>
<td>VxBlock Central</td>
<td>Provides information about all VxBlock Systems and components.</td>
</tr>
<tr>
<td>MSM VM</td>
<td>Provides REST resources.</td>
</tr>
<tr>
<td>MSM VM Compliance service</td>
<td>Validates VxBlock Systems are compliant when compared to different criteria. A compliance scan can be performed for the following:</td>
</tr>
<tr>
<td></td>
<td>• Release Certification Matrix (RCM) compliance</td>
</tr>
<tr>
<td></td>
<td>• Dell EMC Security and Technical Advisory compliance</td>
</tr>
<tr>
<td>MSM VM API for multisystem services</td>
<td>Queries and filters data that is collected from VxBlock Systems in an MSM VM environment</td>
</tr>
<tr>
<td>Collection Manager service</td>
<td>Runs the MSM VM collection manager that runs in the Vert.x instance and performs data collection</td>
</tr>
<tr>
<td>MSM VM API for Security Web</td>
<td>Provides REST resources for to control access to system resources within an MSM VM environment through role-based access control (RBAC)</td>
</tr>
<tr>
<td>MSP API for RCM content prepositioning</td>
<td>Provides REST resources that are used to run the RCM content prepositioning functions, such as downloading RCM content, deleting content, and canceling RCM download</td>
</tr>
<tr>
<td>VxBlock Central Shell</td>
<td>Uses the services from the MSM VM to manage multiple VxBlock Systems VxBlock Central Shell provides a REST API using CherryPy, which is a lightweight Python web server that is used to expose VxBlock Central Shell functionality through REST APIs.</td>
</tr>
<tr>
<td>RabbitMQ</td>
<td>Provides MSM VM services and applications with a common platform to send and receive messages asynchronously</td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>Provides a full-text search engine by using a REST API. The documents or records in ElasticSearch are JSON objects that are stored and made searchable by indexing collected data.</td>
</tr>
<tr>
<td>Vert.x</td>
<td>A lightweight event-driven application platform for web applications The Vert.x instance contains the MSM VM collection manager.</td>
</tr>
<tr>
<td>Cassandra</td>
<td>A distributed database management system designed to handle large amounts of data across a clustered server environment In MSM VM, Cassandra stores collected data, credentials, metadata and element associations for the MSM VM services.</td>
</tr>
<tr>
<td>Components and services</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Content Share service</td>
<td>Manages the inventory of RCM content local to the running instance of the assetmanager service</td>
</tr>
<tr>
<td>Download service</td>
<td>Manages the following tasks:</td>
</tr>
<tr>
<td></td>
<td>• Acknowledges a download request</td>
</tr>
<tr>
<td></td>
<td>• Downloads each required file from the Content Distribution Network (CDN)</td>
</tr>
<tr>
<td></td>
<td>• Provides status updates during the download process</td>
</tr>
<tr>
<td>Content source service</td>
<td>Manages entitlements and request notifications from the CDN, and ensures that all downloaded RCM content matches the download requests</td>
</tr>
<tr>
<td>Asset manager service</td>
<td>Coordinates the content share, content source, and the downloader services for working with RCM content on the MSP VM</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>Stores the downloaded RCM content on the MSP VM</td>
</tr>
</tbody>
</table>
Manage the AMPs

Upgrade the Cisco UCS C2x0 Server (CIMC 2.x firmware)

Perform a remote upgrade using KVM with CIMC for the Cisco UCS C2x0 Server firmware.

Before you begin

Migrate the VMs off the host that is being upgraded. Find the ISO file download for your server online and download it to a temporary location accessible from the Cisco UCS C2x0 Server being upgraded.

For additional information, see the Cisco Host Upgrade Utility User Guide.

Procedure

1. Use a browser to go 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, select 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, in the Mapped column, select the ISO file that you added and then wait for mapping to complete.
   g. Verify the ISO file displays as a mapped remote device.
   h. Boot the server and press F6 to open the Boot Menu screen.

2. On the Boot Menu screen, select Cisco vKVM-Mapped vDVD1.22 and press Enter.

3. When the server BIOS and CIMC firmware versions display, at the Have you read the Cisco EULA? prompt, select I agree.

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

5. At the Confirmation screen, select Yes.

6. From the Confirmation screen for the BIOS update, select Yes.

7. After reboot is complete, verify that the VMware vSphere ESXi host is accessible to the AMP-2 vCenter Server instance.

Related information

Cisco.com
Upgrade the Cisco UCS C2x0 Server (CIMC 3.x and 4.x firmware)

Perform a remote upgrade using KVM with CIMC for Cisco UCS C2x0 Server firmware for servers running CIMC 3.x and 4.x firmware.

Before you begin

Migrate the VMs off the host that is being upgraded. Find the ISO file download for your server online and download it to a temporary location accessible from the Cisco UCS C2x0 Server being upgraded.

For additional information, see the Cisco Host Upgrade Utility User Guide.

Procedure

1. Use a browser to go to the CIMC Manager software on the server that you are upgrading.
   a. Type the CIMC IPv4/IPv6 address for the server in the address field of the browser.
   b. Type your username and password.
   c. From the toolbar, click Launch KVM.
   d. From drop-down options, select HTML Version.
   e. From the Virtual Media tab, select Activate Virtual Devices.
   f. From Virtual Media tab, select Map CD/DVD.
   g. Click Browse, and select the downloaded ISO file.
   h. Click Map Drive to complete Mapping.
   i. Verify that the ISO file is displayed as a mapped remote device.
   j. Boot the server and press F6 to open the Boot Menu.
2. On the Boot Menu, select the KVM DVD matching entry and press Enter.
3. When the server BIOS and CIMC firmware versions displays, at the Have you read the Cisco EULA? prompt, select I agree.
4. From the Host Upgrade menu, select Update and Activate All.
5. At the Confirmation screen, select Yes.
6. From the BIOS Update Confirmation screen, select Yes.
7. After reboot, verify that the VMware vSphere ESXi host is accessible to the AMP VMware vCenter Server instance.

Upgrading VNXe3200 software

Upgrade the software of an VNXe3200 storage array using the VNXe Unisphere GUI.

Before you begin

The VNXe3200 management interface does not support an IPv4 and IPv6 dual stack network configuration. The management interface of the VNXe3200 can only be configured with IPv4.

- A week before upgrading, perform a system health check and resolve any underlying problems that would prevent a successful upgrade.
• See the VNXe Unisphere GUI for the latest upgrade process. Click the question mark on the right side of the Update Software page.

• For detailed instructions, see the online help topic Updating system software, firmware, and language packs.

• Obtain the IP address and login credentials for the VNXe3200 storage array.

Procedure

1. Check for software updates on the Support website. If your system includes hot fixes, ensure that those hot fixes are in the upgrade software to which you are upgrading. Otherwise, you may encounter a regression in system functionality after the software upgrade. Contact your service provider to ensure that the upgrade software includes your hot fixes.

2. Download the new software to a local machine on your network.

3. Upload the new software from your local machine to your storage array.

4. Install the file on your storage array.

   The installation checks the health of the system to determine if any issues would prevent a successful upgrade. If the health check finds issues, the upgrade stops. Resolve any issues before resuming the upgrade.

Create a VMware data store

Create a VMware data store by adding data stores on pair at a time for the storage array.

Before you begin

Use the Unisphere GUI online help for the latest process.

• Obtain the IPv4/IPv6 address and the login credentials for the storage array.

• Confirm that the planned data store size does not exceed the recommended 2 TB maximum.

• Confirm that new data stores do not exceed the total array capacity.

Procedure

1. Select Storage > VMware data stores.

2. Select + to start the VMware Storage Wizard.

3. Specify the following settings:

   a. For the type of data store, select Block or VMFS6, depending on your system.

   b. For the NAS server, specify SPA for the first data store and SPB for the second data store.

   c. Specify a new data store name using the following convention: MGMT-DS-A03 or MGMT-DS-B03.

   d. Confirm that Storage Pool is the default.

   e. Set the Tiering Policy to Auto-Tier.

   f. Ensure that the data store size is not greater than 2 TB.

   g. Clear Thin.

   h. Select Do not configure a snapshot schedule.

   i. Set the host access for all entries to Read/Write, allow Root.

   j. Confirm the settings on the Summary page and click Back to modify settings or Finish to confirm the settings.

The wizard creates a data store, and the steps appear on the screen. The setup runs as a background task, allowing you to close the wizard window. You can find the status of the data store by clicking the Jobs link at the
bottom of the screen. After the data store is created, the wizard displays a notification message. The new data store appears in the list of VMware data stores.

Change VMware datastore capacity

The datastore must be rescanned and expanded from host after Dell EMC Unity expansion. Change the capacity of a VMware datastore using the Unisphere GUI online help for the latest process.

About this task

To access the online help, click the question mark on the VMware Data stores page.

Before you begin

- Obtain the IPv4/IPv6 address and the login credentials for the storage array.
- Confirm that the planned datastore size does not exceed the recommended 2 TB maximum.
- Confirm that adding new datastores does not exceed the total array capacity.

Procedure

1. Select Storage > VMware > Data stores.
2. Select a datastore, and click Edit.
3. Under Storage Details, select General > Size, type the total amount of space the datastore can use for data.
   
   **Note:** For thin-provisioned VMFS datastores, you can increase the storage space, but not decrease it.

4. Click Apply.

The status of the operation and works in the background are displayed in the Applying Changes window. Check the status of the operation by clicking Jobs at the bottom of the screen. After the operation has been completed, a notification message is displayed.

Add a VMware vSphere ESXi host for IPv4

Add a VMware vSphere ESXi host to the VNXe array configuration for IPv4.

Before you begin

- Use the VNXe Unisphere GUI online help for the latest process. You can access the online help by clicking the question mark on the right side of the VMware Hosts page.
- Obtain the IP address and login credentials for the VNXe array.
- Obtain the VMware ESXi host IP address on the vcesys_oob_mgmt VLAN or client equivalent.

Procedure

1. Select Hosts > VMware Hosts.
2. Click Find ESX hosts to start the Add ESX Hosts wizard.
   
   **Note:** VNXe automatically discovers the initiators for VMware vSphere ESXi hosts with block access.

3. Select vCenter or ESX Server Address.
4. Select IP Address.
5. Type the value for the VMware vSphere ESXi server and click Find.
6. Select the discovered nodes, and click Next.
7. Verify the host settings in the Summary page.
8. Click **Finish** to accept the settings and add the VMware host configuration or click **Back** and modify a setting.

   The **Add ESX Hosts** wizard creates the VMware host configuration and adds it to the Unisphere list of VMware hosts.

**After you finish**

After you add a VMware host configuration, you can specify its access to a specific storage resource. You can also configure access for VMware vCenter servers and VMware vSphere ESXi nodes to storage resources from the **Host Access** tab for individual VMware data stores.

---

**Add data store access to a VMware vSphere ESXi Host**

Enable data store access for a new VMware vSphere ESXi host on the VNXe array configuration.

**About this task**

Use the VNXe Unisphere GUI online help for the latest process. Access the online help by clicking the question mark on the right side of the **VMware Datastores** page.

**Before you begin**

- Obtain the IP address and login credentials for the VNXe array.
- Confirm the list of existing data stores to which the new host needs access.

**Procedure**

1. Select **Storage > VMware Datastores**.
2. Select a data store, and click **Details**.
3. Under **Storage Details**, select the **Host Access** tab.
4. Click **Modify Access**.
5. Set the new host access to **Read/Write, allow Root**.
6. Click **OK**.
7. Repeat this process for the list of required data stores.

---

**Configure the VMware vSphere ESXi persistent scratch location (VMware vSphere 6.5)**

Configure all management VMware vSphere ESXi hosts.

**Before you begin**

- Obtain administrative privileges to the VMware vSphere ESXi hosts.
- Assign datastores to VMware vSphere ESXi hosts.

**Procedure**

1. Connect to VMware vCenter Server or the VMware vSphere ESXi host from the VMware vSphere Web Client.
2. Select the VMware vSphere ESXi host in the inventory.
3. Select the **Configuration** tab, and select **Storage**.
4. Right-click the datastore, click **Browse**, and select MGMT-SCRATCH-01.
5. Create a unique directory name for this VMware vSphere ESXi host. For example, `.locker_ESXHostname`.
6. Close the **Datastore** browser.
7. From the Software window, click Advanced Settings.
8. Select the ScratchConfig section.
9. (AMP-2HA/2S only) Update the ScratchConfig.ConfiguredScratchLocation parameter. Type the full path to directory. For example: /vmfs/volumes/MGMT-SCRATCH-01/.locker_ESXHostname

**Note:** Hosts must be assigned to respective folders. Issues may occur if two hosts use the same scratch folder location.

10. Click OK.
11. Put the VMware vSphere ESXi host into maintenance mode and reboot for the configuration change to take effect.
12. (AMP-2HA/2S only) Repeat these steps on the remaining Cisco UCS C2x0 servers.

## Expand an AMP-2S cluster

Expand an AMP-2S cluster with extra Cisco UCS C220 M5 servers.

**About this task**

While installing the ESXi image on the Cisco UCS C220 M5 servers, do not use the default Cisco UCS C220 M4 image. Instead use the VMware custom image for Cisco, which includes the updated drivers for Cisco UCS C220 M5 hardware.

You can expand an AMP setup containing Cisco UCS C220 M4 servers by using C220 M5 servers. Use VMware EVC with the baseline set to C220 M4 servers.

AMP expansion requires that you power off and then power on all VMs in the cluster after enabling VMware EVC. HA, DRS, and CPU Affinity must be disabled during AMP expansion.

Expansion for AMP-2S using Cisco UCS C220 M5 servers is supported in VMware VSS and VMware VDS environments.

The Cisco Nexus 93180YC-EX switch is the only supported production switch for AMP-2S cluster expansion with Cisco UCS C200 M5 servers.

**Procedure**

1. Install each additional AMP-2S server in the designated cabinet and rack unit using the Rail Installation Guide and the Cisco UCS C220 Service and Installation Guide.
2. Cable the CIMC port on each additional AMP-2S server using the management switch port map.
3. Cable the Intel LOM Intel I550 and Intel X550 ports on each additional AMP-2S server using the management switch port map.
4. Cable the Cisco UCS VIC 1457 adapter ports on each additional AMP-2S server using the production switch port map.
5. Configure the management switch ports (see port maps) for the additional CIMC, Intel I550, and Intel X550 for each additional AMP-2S server. See the Configure AMP-2S section of the logical build guides for your platform.
6. Power on each additional AMP-2S server and verify that there are no hardware issues on the CIMC.
7. Complete the following sections of Configure AMP-2S in the logical build guide for your platform:
   - Initialize CIMC on the Cisco UCS C2x0 M5 servers.
   - Configure CIMC BIOS and firmware on Cisco UCS c2x0 M5 servers.
   - Configure the AMP-2S CIMC Interface (VMware vSphere 6.5 and 6.7).
Enable VMware Enhanced vMotion Compatibility

Use the procedure to enable VMware Enhanced vMotion Compatibility (EVC) on an AMP cluster.

About this task

VMware EVC ensures vMotion compatibility for hosts in a cluster. It 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. VMware EVC uses 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 C220 M4 and C220 M5 servers.

VMware EVC must be enabled on an AMP cluster with a vNetwork Standard Switch (VSS) environment before networking is migrated to the VMware Virtual Distributed Switch (VDS).

Procedure

1. Log in to the VMware vCenter Server and select the AMP cluster.
2. Select Configure, and then select VMware EVC.
3. Select Enable EVC for Intel Hosts, and use one of the following based on the hosts in the cluster:
   - Intel Haswell Generation for the Intel Xeon v3 processor
   - Intel Broadwell Generation for the Intel Xeon v4 processor

   **Note**: Enabling VMware EVC may cause an error with the compatibility check failure as some CPUs may not expose all their feature sets. VMs on the cluster must be powered off before enabling VMware EVC. Follow the rest of this procedure only if you encounter this compatibility error.

   **CAUTION** These steps are not recommended for a vCenter Server VM running on a VMware VDS where the vCenter Server VM is part of the same cluster. The vCenter Server and PSC1 VM networking must be migrated to the VMware VSS before proceeding. After EVC enablement, the networking can be migrated back to VMware VDS.

4. Identify the VMware ESXi host in the cluster hosting the vCSA/PSC1 VMs and put it in maintenance mode.
5. HA automatically moves the VMware vCSA/PSC1 and other VMs to another host in the cluster using vMotion.
6. Move the VMware ESXi host that is in maintenance mode out of the cluster in the data center.
7. Take the VMware ESXi host out of maintenance mode.
8. Verify the network settings for the VMware ESXi host outside cluster are consistent with the cluster network settings.
9. Migrate the VMware vCSA/PSC1 VMs from the AMP cluster to the VMware ESXi host outside the cluster using VMware vSphere vMotion.

10. Note the details of the datastore hosting the VCSA/PSC1 VMs.

11. Disable the HA, DRS, and CPU Affinity Rules on the cluster.

12. Power off all remaining VMs in the cluster.

13. Enable VMware EVC on the cluster (see Step 1 and 2).

14. Note the hostname and IP address of one of the VMware ESXi hosts in the cluster.

15. Connect to the VMware ESXi host running the VMware vCSA/PSC1 VMs using the VMware vSphere Host Client, and power off the vCSA/PSC1 VMs.

16. Select the vCSA/PSC1 VMs, and unregister them from the host.

17. Put the VMware ESXi host running the vCSA/PSC1 VMs into maintenance mode.

18. Connect to the host noted in Step 14 using the VMware vSphere Host Client.

19. Browse to the datastore containing the VMware vCSA/PSC1 VMs.

20. Select **Register a VM**, and register the VCSA/PSC1 VMs with the host.

21. Power on the VMware vCSA/PSC1 VMs on the new host in the VMware EVC enabled cluster.

22. Wait until the VMware vCSA/PSC1 VMs are powered on completely and verify you can log in VMware vCenter.

23. Log in to VMware vCenter and move the VMware ESXi host outside the cluster back into the VMware EVC enabled cluster. Then take it out of maintenance mode.

24. Verify network settings on all hosts in the cluster.

25. Power on all remaining VMs and verify the Element Manager VMs can access their respective VxBlock System components.


**Back up AMP-2**

**Create an instance of the configuration repository**

Build the environment to support the capture of VxBlock System configuration files for change management and recovery.

**About this task**

> **Note:** This process is required to support the recovery of the Cisco network devices.

Establish a process to perform network device configuration backups to place the repository on the AMP Element Manager for the array.

**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 for the repository.
- Monitor disk storage resources to prevent overuse issues and data unavailability.

**Procedure**

1. To create the backup directory, type: `<drive>:\Cisco`. 

Use the D:\ drive, if possible. If the D:\ drive is not available, use the C:\ drive. This drive is referenced throughout these instructions.

2. Create the named devices and data subdirectories. It is recommended that you create one set of empty subdirectories and then copy them to the other device directories. The directory names are the major model numbers with 00 substituted for the last two digits of the device model.

   Note: The list of device models is provided as an example. Create only the entries required to support the Converged System being deployed.

3. Install the TFTP server.

4. To configure the TFTP server, restrict read/write access to the home directory, <drive>:\Cisco. Permit access by an IP address range that includes those devices sending configuration files.

5. To verify the procedure, monitor the config directories for entries that are copied from the network devices in the Converged System.

After you finish
Initiate network device configuration backups.

Create a backup of a configuration repository

Create a backup of one or more hosts where Cisco network device configuration files are stored.

About this task
When you back up the configuration repository, Cisco UCS fabric interconnects and Cisco switches are recovered. Establish a process to perform host backups that allow file-level restores.

Procedure

1. Verify that the configuration backup repository exists with regularly scheduled tasks to keep it up-to-date.
2. Verify the location of the host repository.
3. Monitor disk resources to prevent overuse and data unavailability.
4. See the documentation supplied by the backup vendor for this procedure.

After you finish

Establish a procedure to accomplish one of the following:

- Restore a single configuration file, the entire repository, and the process to populate it.
- Restore the complete host where the repository exists

Restore a configuration file

Restore a network or storage device configuration file after a failure, corruption, or other data loss event.

About this task

Follow the vendor recommended restore processes for the device.

Before you begin

- Verify local or remote connectivity exists to the impacted device.
- Access the configuration file that is required 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

1. To restore a configuration file, see the vendor documentation to restore the device.

Back up targets

Back up targets that are in the AMP in the Converged System.

About this task

- Back up all VMs at daily at 7 A.M. and 7 P.M.
- Back up the VMware vCenter SQL Server database every four hours to coincide with server daily backups at 3, 7, 11 A.M. and 3, 7, 11 P.M.
- Set the retention value to 35 days.

⚠️ CAUTION Disk storage resources should be monitored to prevent overuse issues and data unavailability.

If AMP-2 is lost, the AMP-2 servers backup and binaries must be stored on the backup media so that they can be installed or restored. Otherwise, you are unable, or severely limited, in the ability to manage or recover the Converged System.

AMP servers are:

- VMware vCSA
- VMware Platform Services Controllers (PSC)
- VMware vCenter Server, Web Server, and Inventory Service
- VMware vCenter SQL database
- VMware vCenter Update Manager
- VMware SSO Service and SQL Database
- Element Manager
- Other VMs identified as part of the core or optional workloads to manage the Converged System.

Perform configuration backups for these Converged System devices:

- Cisco management switches (Cisco Nexus 3000 Switch or Cisco Nexus 9000 Switch)
  See the appropriate RCM for a list of what is supported on your Converged System.
- Cisco MDS switches
- Cisco UCS fabric interconnections
- Storage platform

To back up targets in AMP-2 and the Converged Systems, see the documentation from the backup tool vendor.