Contents

Revision History........................................................................................................................................9

Introduction...............................................................................................................................................11

IPI Appliance...........................................................................................................................................12

Manage compute resources.......................................................................................................................13
Start Cisco UCS Manager..........................................................................................................................13
Upgrade Cisco UCS firmware.....................................................................................................................13
Create a host firmware package................................................................................................................14
Activate the Cisco UCS Manager Capability Catalog................................................................................14
Activate the port license............................................................................................................................15
Set the time zone......................................................................................................................................15
Add the NTP server....................................................................................................................................16
Add the syslog server...............................................................................................................................16
Delete a syslog server...............................................................................................................................17
Add an SNMP server...............................................................................................................................17
Delete an SNMP server............................................................................................................................18
Create an IP address pool.........................................................................................................................18
Expand an IP address pool.......................................................................................................................18
Create a UUID pool...............................................................................................................................19
Add a UUID range.....................................................................................................................................20
Delete a UUID pool..................................................................................................................................20
Create a WWNN pool...............................................................................................................................21
Add a WWNN range..................................................................................................................................21
Delete a WWNN range...............................................................................................................................22
Create a WWPN pool...............................................................................................................................22
Add a WWPN range..................................................................................................................................23
Delete a WWPN range...............................................................................................................................24
Create a MAC address pool.....................................................................................................................24
Add a MAC address range.......................................................................................................................25
Delete a MAC pool..................................................................................................................................25
Create a vNIC template............................................................................................................................26
Create boot policies...............................................................................................................................26
  Create an SD boot policy......................................................................................................................26
  Create a SAN boot policy.....................................................................................................................27
  Create a LAN boot policy for VxFlex Central deployments...............................................................27
Cisco Trusted Platform Module...............................................................................................................28
Manage service profile templates.........................................................................................................28
  Configure service profile templates .................................................................................................28
  Clone service profile templates ........................................................................................................31
  Add vNICs to the service profiles.......................................................................................................32
  Configure service profile templates for Disjoint Layer 2...............................................................33
  Create a network profile for the IPv6 management address............................................................35
  Assign or modify a management IPv6 address................................................................................35
  Assign service profiles to Cisco UCS blade servers........................................................................35
  Rename service profiles....................................................................................................................36
  Assign or modify a management IP address....................................................................................36
Remove LDAP..........................................................................................................................................37

Manage network resources....................................................................................................................38
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify ElasticSearch if the MSM VM is changed</td>
<td>140</td>
</tr>
<tr>
<td>Discover, decommission, or modify a component</td>
<td>140</td>
</tr>
<tr>
<td>Add Isilon Technology Extension on a VxBlock System</td>
<td>140</td>
</tr>
<tr>
<td>Add a component with the configuration editor</td>
<td>141</td>
</tr>
<tr>
<td>Add eNAS to VMAX3 storage</td>
<td>142</td>
</tr>
<tr>
<td>Edit component credentials in the system.cfg file</td>
<td>143</td>
</tr>
<tr>
<td>Edit component properties with the configuration editor</td>
<td>143</td>
</tr>
<tr>
<td>Delete a component with the configuration editor</td>
<td>144</td>
</tr>
<tr>
<td>Configure VxBlock Systems and components</td>
<td>145</td>
</tr>
<tr>
<td>Access the VxBlock Central Shell session</td>
<td>145</td>
</tr>
<tr>
<td>Run VxBlock Central Shell from a remote host</td>
<td>145</td>
</tr>
<tr>
<td>VxBlock Central Shell commands</td>
<td>146</td>
</tr>
<tr>
<td>Components in VxBlock Central Shell</td>
<td>146</td>
</tr>
<tr>
<td>View VxBlock Central Shell logs</td>
<td>149</td>
</tr>
<tr>
<td>View VxBlock Central Shell jobs</td>
<td>149</td>
</tr>
<tr>
<td>Configure Secure Remote Services for VxBlock Central 2.0 and earlier</td>
<td>150</td>
</tr>
<tr>
<td>Configure Secure Remote Services for VxBlock Central 1.5 and earlier</td>
<td>150</td>
</tr>
<tr>
<td>Register VxBlock Central with a Secure Remote Services gateway</td>
<td>150</td>
</tr>
<tr>
<td>Add a software identifier for an MSM VM</td>
<td>151</td>
</tr>
<tr>
<td>Retrieve the software ID from the licensing system</td>
<td>152</td>
</tr>
<tr>
<td>Update a Secure Remote Services gateway configuration or software identifier</td>
<td>153</td>
</tr>
<tr>
<td>Deregister VxBlock Central with Secure Remote Services</td>
<td>153</td>
</tr>
<tr>
<td>Send information to Secure Remote Services</td>
<td>154</td>
</tr>
<tr>
<td>Secure the connection between VxBlock Central and Secure Remote Services</td>
<td>154</td>
</tr>
<tr>
<td>Verify Secure Remote Services configuration</td>
<td>154</td>
</tr>
<tr>
<td>Troubleshoot Secure Remote Services connectivity issues</td>
<td>155</td>
</tr>
<tr>
<td>Integrate with SNMP</td>
<td>156</td>
</tr>
<tr>
<td>Provision the SNMP name, location, and contact information fields</td>
<td>156</td>
</tr>
<tr>
<td>SNMP traps, events, and CIM indications</td>
<td>157</td>
</tr>
<tr>
<td>Communicate with the network management system</td>
<td>159</td>
</tr>
<tr>
<td>Send SNMP traps in readable format</td>
<td>159</td>
</tr>
<tr>
<td>Enable northbound communication through SNMP</td>
<td>160</td>
</tr>
<tr>
<td>Integrate with AD</td>
<td>161</td>
</tr>
<tr>
<td>Configure AD</td>
<td>163</td>
</tr>
<tr>
<td>Map roles to AD groups</td>
<td>163</td>
</tr>
<tr>
<td>Integrate components to send traps</td>
<td>165</td>
</tr>
<tr>
<td>Configure Cisco UCSM to forward traps</td>
<td>165</td>
</tr>
<tr>
<td>Configure iDRAC to forward traps</td>
<td>165</td>
</tr>
<tr>
<td>Configure Unisphere to forward traps</td>
<td>166</td>
</tr>
<tr>
<td>Configure XtremiO to forward traps</td>
<td>166</td>
</tr>
<tr>
<td>Configure VMAX or PowerMax to forward traps</td>
<td>166</td>
</tr>
<tr>
<td>Configure Cisco MDS and Cisco Nexus switches to forward traps</td>
<td>167</td>
</tr>
<tr>
<td>Configure alert profiles and templates to receive notification</td>
<td>167</td>
</tr>
<tr>
<td>Configure port flapping for switches</td>
<td>168</td>
</tr>
<tr>
<td>Configure the VMs to use the NTP server</td>
<td>168</td>
</tr>
<tr>
<td>Verify the ElasticSearch configuration</td>
<td>168</td>
</tr>
<tr>
<td>Manage credentials</td>
<td>169</td>
</tr>
<tr>
<td>Change the default password for root and VxBlock Central accounts</td>
<td>169</td>
</tr>
<tr>
<td>Use the nonadministrator account</td>
<td>170</td>
</tr>
<tr>
<td>Change the default CAS password for Core VM</td>
<td>170</td>
</tr>
<tr>
<td>Change the default CAS password for MSM VM</td>
<td>171</td>
</tr>
<tr>
<td>Synchronize the CAS password for the admin user</td>
<td>171</td>
</tr>
<tr>
<td>Change the default CAS password for the MSP VM to match the MSM VM</td>
<td>172</td>
</tr>
<tr>
<td>Create users with access rights to storage components</td>
<td>172</td>
</tr>
<tr>
<td>Change access credentials for a VxBlock System component</td>
<td>173</td>
</tr>
<tr>
<td>Bulk credential script</td>
<td>173</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Manage third party certificates</td>
<td></td>
</tr>
<tr>
<td>Configure connection and download settings</td>
<td></td>
</tr>
<tr>
<td>Manage credentials for RCM content prepositioning</td>
<td></td>
</tr>
<tr>
<td>Manage VxBlock Central Orchestration Services and VxBlock Central Orchestration Workflows</td>
<td></td>
</tr>
<tr>
<td>VxBlock Central Advanced Analytics</td>
<td></td>
</tr>
<tr>
<td>Change VxBlock Central Operations Adapter real-time alerts collection cycle interval</td>
<td></td>
</tr>
<tr>
<td>Change the VxBlock Central Adapter Collection cycle interval</td>
<td></td>
</tr>
<tr>
<td>Back up Core VM</td>
<td></td>
</tr>
<tr>
<td>Management backup</td>
<td></td>
</tr>
<tr>
<td>Change the backup schedule and frequency</td>
<td></td>
</tr>
<tr>
<td>Back up cron tasks</td>
<td></td>
</tr>
<tr>
<td>Back up configuration files on demand</td>
<td></td>
</tr>
<tr>
<td>Back up databases on demand</td>
<td></td>
</tr>
<tr>
<td>Restore the software configuration</td>
<td></td>
</tr>
<tr>
<td>Restore databases</td>
<td></td>
</tr>
<tr>
<td>Back up the Core VM</td>
<td></td>
</tr>
<tr>
<td>Back up and restore the MSP VM and MSP VM</td>
<td></td>
</tr>
<tr>
<td>Back up component configuration files</td>
<td></td>
</tr>
<tr>
<td>Ports and protocols</td>
<td></td>
</tr>
<tr>
<td>Open port assignments</td>
<td></td>
</tr>
<tr>
<td>Northbound ports and protocols</td>
<td></td>
</tr>
<tr>
<td>Southbound ports and protocols</td>
<td></td>
</tr>
<tr>
<td>Reference</td>
<td></td>
</tr>
<tr>
<td>Core VM commands</td>
<td></td>
</tr>
<tr>
<td>MSM VM commands</td>
<td></td>
</tr>
<tr>
<td>MSP VM commands</td>
<td></td>
</tr>
<tr>
<td>Configuration editor component reference</td>
<td></td>
</tr>
<tr>
<td>Components, APIs, and services for VMs</td>
<td></td>
</tr>
<tr>
<td>Upgrade the Cisco UCS C2x0 Server (CIMC 3.x and 4.x firmware)</td>
<td></td>
</tr>
<tr>
<td>Upgrade Dell EMC Unity software</td>
<td></td>
</tr>
<tr>
<td>Create a VMware data store</td>
<td></td>
</tr>
<tr>
<td>Change VMware datastore capacity</td>
<td></td>
</tr>
<tr>
<td>Add a VMware vSphere ESXi host</td>
<td></td>
</tr>
<tr>
<td>Configure VMware vSphere ESXi persistent scratch location (VMware vSphere 6.7)</td>
<td></td>
</tr>
<tr>
<td>Configure the VMware vSphere ESXi persistent scratch location (VMware vSphere 6.5)</td>
<td></td>
</tr>
<tr>
<td>Disable VAAI primitives</td>
<td></td>
</tr>
<tr>
<td>Back up AMP-3S</td>
<td></td>
</tr>
<tr>
<td>Create an instance of the configuration repository</td>
<td></td>
</tr>
<tr>
<td>Create a backup of a configuration repository</td>
<td></td>
</tr>
<tr>
<td>Restore a configuration file</td>
<td></td>
</tr>
<tr>
<td>Back up targets (VMware vSphere 6.x)</td>
<td></td>
</tr>
<tr>
<td>Back up the Dell EMC Unity configuration</td>
<td></td>
</tr>
<tr>
<td>AMP and VxBlock System Integrated Data Protection</td>
<td></td>
</tr>
<tr>
<td>Back up the AMP-3S management core workload</td>
<td></td>
</tr>
<tr>
<td>Avamar and NetWorker VMware vCenter Server user account</td>
<td></td>
</tr>
<tr>
<td>Application-specific scripted backups</td>
<td></td>
</tr>
<tr>
<td>Password security</td>
<td></td>
</tr>
</tbody>
</table>

VxBlock System 1000 Administration Guide
Contents

Update the CPSD-DP-Settings.cfg file .................................................................................................................. 224
Create the scheduled tasks for all backups............................................................................................................. 225
Backup types and scripted backup locations........................................................................................................... 226
Establish Avamar image backups for restored VMs ................................................................................................. 226
Establish NetWorker image backups for restored VMs ........................................................................................... 227
Enable the scripted backup configuration .............................................................................................................. 228
## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Document revision</th>
<th>Description of changes</th>
</tr>
</thead>
</table>
| October 2019| 1.15              | - 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| 1.14          | Added support for Dell EMC Unity XT.  
Removed sections about managing PowerMax and VMAX storage with Unisphere. For more information about creating and managing storage groups, initiator groups, port groups and masking views, see the *Unisphere for PowerMax Online Help* or *Unisphere for VMAX Online Help*.  
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    | 1.13             | 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    | 1.12             | Added support for Dell EMC Unity OS 4.5.  
Added support for the Cisco MDS 9148T and 9396T 32G Multilayer Fabric Switches.  
Updated for new VxBlock Central licensing. |
| May 2019     | 1.11             | Added IPv6 support for AMP-3S with Cisco UCS C220 M5 servers. |
| April 2019   | 1.10             | Added support for Integrated Data Protection script updates. |
| March 2019   | 1.9              | Added support for:  
- VxBlock Central updates and AMP-3S Integrated Data Protection backups  
- VMware vSphere 6.7  
- Cisco UCS Gen 4  
- Dell EMC Unity Hybrid |
<p>| January 2019 | 1.8              | Added support for Dell EMC Unity OS 4.4. |
| December 2018| 1.7              | Added support for VxBlock Central. |
| October 2018 | 1.6              | Added support for NSX 6.4. |
| September 2018| 1.5             | Added support for IPv6. |</p>
<table>
<thead>
<tr>
<th>Date</th>
<th>Document revision</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2018</td>
<td>1.4</td>
<td>Added support for:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- AMP-3S</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- PowerMax 2000 and 8000 storage arrays</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added the topic <em>Removing LDAP</em> under <em>Managing compute resources</em>.</td>
</tr>
<tr>
<td>July 2018</td>
<td>1.3</td>
<td>Updated the following sections to include Cisco B480 M5 blade server:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Configuring service profile templates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Adding vNICs to the service profiles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Configuring service profile templates for Disjoint Layer 2</td>
</tr>
<tr>
<td>May 2018</td>
<td>1.2</td>
<td>Updated the section <em>Managing storage - Dell EMC Unity storage</em> with information about data reduction.</td>
</tr>
<tr>
<td>May 2018</td>
<td>1.1</td>
<td>Adding XtremIO X2 information.</td>
</tr>
<tr>
<td>February 2018</td>
<td>1.0</td>
<td>Initial version</td>
</tr>
</tbody>
</table>
Introduction

This guide contains instructions for managing the VxBlock System 1000 with Cisco UCS Gen 3 and 4 after installation at the customer site.

The target audience for this document includes those people responsible for managing the VxBlock System 1000, 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 VxBlock System 1000 concepts and terminology
- Has VxBlock System 1000 troubleshooting skills
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

Use Cisco UCS Manager to provision and manage the Cisco UCS servers.

About this task

These instructions apply to the HTML5 web interface on Cisco UCS Manager version 3.2.1 and higher.

Note: Cisco UCS Manager for a Cisco UCS Gen 4 environment must be version 4.0(2b) or higher.

For more information about using the HTML5 web interface, see the Cisco UCS Manager GUI Configuration Guide for versions 3.2.1 and higher and for Cisco UCS Gen 4 and 4.0(2b).

Procedure

1. From a web browser, open the web link for Cisco UCS Manager GUI at:
   http(s)://UCSManager_VIP_IP

2. Type the virtual cluster IP address of the management port on the fabric interconnect.

3. If a Security Alert dialog box displays, click Yes or Proceed to accept the security certificate and continue.

4. If a banner window displays, review the message and click OK.

5. In the Login dialog box, type your username and password.

6. If your Cisco UCS implementation includes multiple domains, select the appropriate domain from the Domain list and click Login.

Upgrade Cisco UCS firmware

Cisco UCS components can be upgraded individually based on the fix for an issue or compatibility requirements.

About this task

Cisco UCS Manager Firmware Auto Install feature is recommended to ensure that infrastructure, and server components are updated in the required order. It also ensures that proper system checks are performed in advance.

Before you begin

- Coordinate firmware upgrades during maintenance windows, and see the Cisco documentation for proper upgrade procedures.
- Download the latest Cisco UCS Manager GUI Firmware Management Guide.
- Run a full state and all configuration backup.
- For a cluster configuration, verify the high availability status of both FIs is up and running.
- Verify all servers, I/O modules, and adapters are fully functional. An inoperable server cannot be upgraded.
- Verify that all servers have been discovered. The discovery process does not require that servers are powered on or are associated with a service profile.
- Verify the time, date, and time zone of FIs are identical for a cluster using a central time source such as NTP.
- Verify that the VCE-UserAck maintenance policy is assigned to the service profiles/service profile templates with the user-ack option selected.
- Download the required firmware images from the Cisco UCS software download website.
- Download the firmware images to the FI.
- Create a host firmware policy that with the new firmware versions assigned. This policy can be used to update the servers after the infrastructure firmware has been installed.

Cisco documents recommended practices for managing firmware in the Cisco UCS Manager. Ensure that the firmware versions are compatible with the Release Certification Matrix.

See the Cisco UCS Firmware Management Guide for instructions.

**Create a host firmware package**

Host Firmware Packages ensures each service profile template or service profile is running the same server firmware bundle, and that upgrading the default firmware package has no effect on the assigned service profiles.

**Before you begin**

- Download the required blade and rack mount server firmware bundles.
- Verify the installed infrastructure firmware is the same version, or a newer version than the server firmware desired for the new Host Firmware Package.
- Consult the firmware release notes for hardware compatibility.

**Procedure**

1. Log in to the Cisco UCS Manager.
2. In the Navigation window, click the Servers tab.
4. Expand the node for the organization that contains the pool. If the system does not include multi-tenancy, expand the root node.
5. Right-click Host Firmware Packages and select Create Host Firmware Package.
6. In the Create Host Firmware Package window, type the name `VCE-HFirm-<firmware version>` (for example `VCE-HFirm-3.2.2b`).
   
   **Note:** The host firmware package for a Cisco UCS Gen 4 environment must be 4.0(2b) or higher.

7. Ensure Simple is selected.
8. Select the appropriate blade package, rack package, and if necessary, a service pack.
9. Click OK to finish.

**Activate the Cisco UCS Manager Capability Catalog**

Cisco UCS Manager uses the 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 is identified by the vendor, model (PID), and revision. For each provider, you can view details of the equipment manufacturer and the form factor.

Cisco UCS Manager Capability Catalog updates are included in each Cisco UCS Manager update. Unless otherwise instructed by Cisco Technical Support, 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. You do not need to perform any further tasks or reboot any component in the Cisco UCS instance or reinstall the Cisco UCS Manager when you perform an update.

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

The catalog is compatible with Cisco UCS Manager, Release 3.2.1, and later.

**Before you begin**

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

See the [Cisco UCS Firmware Management Guide](#) for your release to update the Cisco UCS Manager Capability Catalog.

**Activate the port license**

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

**About this task**

- Cisco UCS Generation 3: The Cisco UCS 6332-16UP Fabric Interconnects have eight pre-installed unified port licenses and four 40 GB QSFP port licenses. Cisco UCS 6332-16UP Fabric Interconnects are fixed and do not include any expansion modules.
- Cisco UCS Generation 4: The Cisco UCS 6454 Fabric Interconnects have eight pre-installed unified ports along, 10 more host server ports (total of 18), and two 100 GB QSFP port licenses. Cisco UCS 6454 Fabric Interconnects are fixed and do 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 additional fixed ports. If you use an unlicensed port, Cisco UCSM initiates a 120-day grace period measured from the first use is paused when a valid license file is installed. The amount of time used in the grace period is retained by the system. 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 symmetry is not maintained and failover occurs, Cisco UCS enables the missing licenses and initiates the grace period for each port used on the failover node.

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

To view, obtain, download, install, and uninstall a 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.
Procedure

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

Add the NTP server

Cisco UCS requires both an instance-specific time zone setting and an NTP server to ensure the correct time appears in the Cisco UCS Manager.

About this task

To add an NTP server, see the Cisco UCS Manager Configuration Guide.

When you add an NTP server, devices receive time from the same source. Set all devices in a VxBlock Systems to the same time.

Before you begin

Set up the NTP server to be reachable from the Cisco UCS Manager.

After you finish

To delete an NTP server, see the Cisco UCS Manager Configuration Guide.

Related information

Cisco UCS Manager Configuration Guide

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.

**Related information**

Cisco UCS Manager Configuration Guide
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.
3. Expand **All > Communication Management > Communication Services**.
4. Select the **Communication Services** tab.
5. In the **Admin State** field, click **Disabled**.
6. Click **Save Changes**.

**Related information**

Cisco UCS Manager Configuration Guide

Create an IP address pool

IP pools are used to assign management IP addresses to the service profiles. By selecting the management IP address pool in the service profile template, each new service profile generated from the template automatically gets an assigned IP address.

**Before you begin**

- Verify IP addresses in the new pool do not conflict with addresses in an existing IP pool.
- Note the required IP subnet mask, IP gateway, and DNS server addresses.

**Procedure**

1. Log in to the Cisco UCS Manager.
2. In the **Navigation** window, select the **LAN** tab.
3. In the **LAN** tab, expand **LAN > Pools**.
4. Expand the node for the organization that contains the pool. If the system does not include multitenancy, expand the root node.
5. Right-click the **IP Pools** and select **Create IP Pool**.
6. In the **Create IP Pool** window, perform the following:
   a. In the **Name** field, type the name of the IP pool.
   b. In the **Description** field, type a description of the pool.
   c. Set the **assignment order** to **Sequential**.
   d. In **Add IPv4/IPv6 Blocks**, click **Add**.
   e. Type the IP information, DNS server addresses, and wanted size of the pool and click **OK**.
7. Click **Finish**.

Expand an IP address pool

Increase available IP addresses to assign to service profiles.

**Before you begin**

Verify the starting IP address to add to the block and quantity of new addresses needed.
Procedure
1. Log in to the Cisco UCS Manager.
2. In the Navigation window, select the LAN tab.
3. In the LAN tab, expand LAN > Pools.
4. Expand the node for the organization that contains the pool. If the system does not include multitenancy, expand the root node.
5. Right-click the IP Pool and select Create Block of IPv4/IPv6 Addresses.
6. Perform the following steps:
   a. Type the starting address in the From field.
   b. Type the remaining IP information and size of the new block.
7. Click Finish.

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

Before you begin
Verify the new UUID range does not exist on any pre-existing 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 Other (specify the suffix). The standard Converged System UUID prefix is 000025B5-XXXX-0000 with XXXX representing which Converged System is being installed. For example, the first Converged System has the UUID prefix 000025B5-0001-0000, and the second has 000025B5-0002-0000.
   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, Type the first UUID suffix in the pool and the number of UUID suffixes to include in the pool. Click OK.
9. Click Finish.

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

Add a range to 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 the UUID pool and select Create a block of UUID Suffixes.
6. From the Create a Block of UUID Suffixes window:
   a. Type the first UUID suffix in the pool in the From box and the number of UUID suffixes to include in the pool.
   b. Click OK.
7. Click Finish.

After you finish

Create a WWNN pool using Cisco UCS Manager.

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
Create a WWNN pool

Create a WWNN pool using the Cisco UCS Manager.

About this task

To ensure the uniqueness of the Cisco UCS WWNNs in the SAN fabric, use the WWN prefix 20:00:00:25:B5:XX:XX:XX for all blocks in a pool. By default, the Converged System includes a WWNN pool with these guidelines:

- After B5, a value is set representing the Converged System number or Cisco UCS Domain ID (01 represents the first Converged System/Cisco UCS Domain, 02 represents the second Converged System/Cisco UCS Domain), and 11 to indicate WWNN rather than WWPN.
- Create a block beginning at 20:00:00:25:B5:XX:11:01 to 20:00:00:25:B5:XX:11:A0.

Before you begin

Verify that the pools wanted values do not conflict with the configured WWNN 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.
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 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 the service profile or service profile template.

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 includes only 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 uniqueness of the Cisco UCS WWNNs and WWPNs 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 the WWNN pool and select **Create WWN Block**.
6. 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**.
7. Click **Finish**.

**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

**Create a WWPN pool**

Create a WWPN pool using the Cisco UCS Manager.

**About this task**

To ensure uniqueness of the Cisco UCS WWPNs in the SAN fabric, use the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX.
Before you begin
Verify the new pools wanted values do not conflict with the currently configured WWPN Pools.

Procedure
1. Log in to the Cisco UCS Manager.
2. In the Navigation window, select the SAN tab.
3. Expand SAN > Pools.
4. Expand the node for the organization where you want to create the pool. If the system does not include multi-tenancy, expand the root node.
5. Right-click WWPN Pools and select Create WWPN Pool.
6. From the Create WWPN Pool window, perform the following:
   a. In the Define Name and Description window, type a unique name and description for the WWPN pool.
   b. In the Assignment Order field, 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.

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

Add a WWPN range

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

Before you begin
Verify the range of desired values does not conflict with the currently configured WWPN values.

Procedure
1. Log in to Cisco UCS Manager.
2. In the Navigation window, click 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 the WWPN Pool and select Create WWN Block.
6. In the Create WWN Block window:
   a. In the From field, enter the first WWPN in the pool. Enter 20:00:00:25:B5:XX:XX:XX with the first XX being the Converged System number or Cisco UCS Domain ID (01 represents the first Converged System/UCS Domain. 02 would represent the second Converged System/UCS Domain, and so on). The second XX represents the fabric and vHBA number. The last XX indicates the first WWN value in the block.
   b. In the Size field, type the number of WWPNs to include in the pool.
c. Click OK.
7. Click Finish.

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.

Create a MAC address pool

Create a MAC address pool using the Cisco UCS Manager. In a Converged System, a MAC address pool should be created for every vNIC.

Before you begin

Record the Converged System ID or Cisco UCS domain ID used as part of the MAC address to identify the location of the assigned interface.

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 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. The first three bytes of the MAC address cannot be changed. Leave them as 00:25:B5.
9. Click Finish.
Add a MAC address range

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

**Before you begin**

Verify the range of wanted values does not conflict with configured MAC address values.

**Procedure**

1. Log in to the Cisco UCS Manager.
2. In the Navigation window, select the LAN tab.
3. In the LAN tab, expand LAN > Pools.
4. Expand the node for the organization that contains the pool. If the system does not include multitenancy, expand the root node.
5. Right-click the MAC address pool and select Create a Block of MAC Addresses.
6. In the Create a Block of MAC Addresses window, perform the following:
   a. In the From MAC Address field, enter 20:00:00:25:B5:XX:XX:XX with the first XX being the Converged System number or Cisco UCS Domain ID (01 represents the first Converged System/UCS Domain. 02 represents the second Converged System/UCS Domain, and so on). The second XX represents the fabric and vNIC number. The last XX indicates the first MAC address value in the block.
   b. In the Size field, type the number of MAC addresses to include in the pool.
   c. Click OK.
7. 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 additional vNIC templates for Disjoint Layer 2 configurations. As a best practice, evenly distribute vNICs between Fabric A and Fabric B.

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

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 within the menu.
4. Type a name for the template that is less than or equal to 16 characters and can be identified during service profile creation. 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 the MTU setting, type 9000.
10. Select all appropriate VLANs. If required, create additional VLANs.
   For a standard Cisco UCS - VDS 6.5 configuration, map all VLANs to each vNIC template or vNIC unless the environment dictates differently.
11. For CDN Source, select vNIC Name.
12. For MTU setting, type 9000.
13. Select a preconfigured MAC pool or create a new one.
15. For Network Control Policy, select CDP-Link-Loss.
16. For Connection Policy, select VMQ.
17. For VMQ Connection Policy, select VMQ-Default.

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

## Manage 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 in the service profiles are used to automate administration tasks. 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 for blade servers with multiple network adapters. vNICs can be added one at a time after VMware vSphere ESXi has been installed to prevent PCIe enumeration issues in the hypervisor.

**Before you begin**

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

**Note:** Template names are provided as examples. Template names vary based on the vNIC templates that exist on the system.
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>_<VxBlock_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 a created pool, and click Next.
5. On the Storage Provisioning tab, select the Local Disk Configuration Policy tab. Choose the Local Storage drop-down menu and choose Local-SD. If Local-SD is not an option, click Create Local Disk Configuration Policy. Perform the following:
   a. In the Name field, type Local-SD.
   b. In the Description field, type Local-SD Boot.
   c. In the Mode field, leave to Any Configuration.
   d. For Protect Configuration, leave the checkbox checked.
   e. Set FlexFlash to Enable.
   f. Set FlexFlash State to Enable.
   g. For Cisco UCS 3.2(2) firmware versions and higher, you are prompted to choose a FlexFlash Removable State. Leave as No Change.
6. On the Networking tab, under How would you like to configure LAN Connectivity? field, select Expert and click Add.
7. On the Create vNIC window, click + Add to configure vNIC-0.
   a. In the Name field, type vNIC-0.
   b. Click Use vNIC 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 contain only vNIC-0 and vNIC-1.
8. On the Create vNIC window, configure vNIC-1.
   a. In the Name field, type vNIC-1.
   b. Click Use vNIC Template.
c. In the vNIC Template field, click vNIC-1-Fabric-B.
d. In the Adapter Policy field, select VMQ-Default > OK > Add.

9. 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:** Verify the order of vNICs on servers with a 1340 or 1380 single network adapter. If the vNIC order in the Cisco UCS and VMNIC in the VMware vSphere ESXi is not the same, resolve the issue. Follow the steps in How VMware ESXi determines the order in which names are assigned to devices (2091560).

10. On the SAN Connectivity tab, under How would you like to configure SAN Connectivity, select Expert and click Add.
   a. In the WWNN Assignment field, select Global-WWNN-Pool, scroll down, and click Add.

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

12. On the Create vHBA window, configure vHBA-1.
   a. In the Name field, type vHBA-1.
   b. Click Use vHBA Template.
   c. In the vHBA Template field, select vHBA-1-Fabric-B.
   d. In the Adapter Policy field, select VMware > OK > Add.

13. Retain the default Zoning settings.

14. For vNIC/vHBA placement, under Select Placement, choose Specify Manually and perform the following:

<table>
<thead>
<tr>
<th>VNIC</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 5.5 or vSphere 6.0</th>
<th>B480M5 blades (with 1340/1380 or 1440/1480 VIC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>vNIC-0</td>
<td>vCon 1 Click &gt;&gt;assign&gt;&gt;</td>
<td>vCon 1 Click &gt;&gt;assign&gt;&gt;</td>
<td>vCon 1 Click &gt;&gt;assign&gt;&gt;</td>
<td>vCon 1 Click &gt;&gt;assign&gt;&gt;</td>
</tr>
<tr>
<td>2</td>
<td>vNIC-1</td>
<td>vCon 1 Click &gt;&gt;assign&gt;&gt;</td>
<td>vCon 1 Click &gt;&gt;assign&gt;&gt;</td>
<td>vCon 1 Click &gt;&gt;assign&gt;&gt;</td>
<td>vCon 1 Click &gt;&gt;assign&gt;&gt;</td>
</tr>
<tr>
<td>3</td>
<td>vNIC-2</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>4</td>
<td>vNIC-3</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>5</td>
<td>Select the vHBAs tab.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VxBlock System 1000 Administration Guide
15. On the vMedia Policy window, retain the default settings.
16. On the Server Boot Order window, select the appropriate boot policy or create one, and click Next.
17. From the Maintenance Policy field, select Default or User Acknowledgement, and click Next.
18. On the Server Assignment window, perform the following:
   a. Select Up for the power state.
   b. Expand the Firmware Management (BIOS, Disk Controller, Adapter) field and click Host Firmware Package to select the new firmware package. Click Next.
19. 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 and choose KVM-IP-POOL.
20. 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. Add the vNICs after installing VMware vSphere ESXi to force the vNIC and VMNIC ID numbers to match each host.

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

About this task
The following table provides sample values 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>
</tbody>
</table>

Procedure
1. To clone a service profile template, perform the following:
   a. Right-click the service profile template that was just 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 navigate 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 as needed to clone more templates.

### Add vNICs to the service profiles

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

**About this task**

**CAUTION** Adding new vNICs to a service profile 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 created for blade servers with multiple network adapters should contain only two network adapters. A minimum of two additional 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. Click **Use vNIC Template**.
   c. In the **vNIC Template** field, click **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 for **vNIC-2**:

<table>
<thead>
<tr>
<th>For this blade type</th>
<th>Do the following</th>
</tr>
</thead>
<tbody>
<tr>
<td>Half-width blades (B200/B230/B22) with a single mezzanine card</td>
<td>Select vCon 1 and click &gt;&gt;&gt;assign&gt;&gt;&gt;.</td>
</tr>
<tr>
<td>B200M4 or B460M4 blades (with 1240/1280 or 1340/1380 VIC)</td>
<td>Select vCon 2 and click &gt;&gt;&gt;assign&gt;&gt;&gt;.</td>
</tr>
<tr>
<td>B420M3 blades (with 1240/1280 VIC)</td>
<td>Select vCon 3 and click &gt;&gt;&gt;assign&gt;&gt;&gt;.</td>
</tr>
<tr>
<td>B460 blades with four adapters</td>
<td>Select vCon 2 and click &gt;&gt;&gt;assign&gt;&gt;&gt;.</td>
</tr>
<tr>
<td>B480M5 blades (with 1340/1380 or 1440/1480 VIC)</td>
<td>Select vCon 3 and click &gt;&gt;&gt;assign&gt;&gt;&gt;.</td>
</tr>
</tbody>
</table>

For servers with 1340 or 1380 single network adapter, you may experience 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. Click Use vNIC Template.
   c. In the vNIC Template field, click 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 depending on the blade type perform one of the following for vNIC-3:

<table>
<thead>
<tr>
<th>For this blade type</th>
<th>Do the following</th>
</tr>
</thead>
<tbody>
<tr>
<td>Half-width blades (B200/B230/B22) with a single mezzanine card</td>
<td>Select vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
</tr>
<tr>
<td>B200M4 or B460M4 blades (with 1240/1280 or 1340/1380 VIC)</td>
<td>Select vCon 2 and click &gt;&gt;assign&gt;&gt;.</td>
</tr>
<tr>
<td>B420M3 blades (with 1240/1280 VIC)</td>
<td>Select vCon 3 and click &gt;&gt;assign&gt;&gt;.</td>
</tr>
<tr>
<td>B460 blades with four adapters</td>
<td>Select vCon 4 and click &gt;&gt;assign&gt;&gt;.</td>
</tr>
<tr>
<td>B480M5 blades (with 1340/1380 or 1440/1480 VIC)</td>
<td>Select vCon 3 and click &gt;&gt;assign&gt;&gt;.</td>
</tr>
</tbody>
</table>

For servers with 1340 or 1380 single network adaptor, you may experience 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.

**Configure 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 0–3. VMware vSphere ESXi interprets the PCI bus enumeration of the vNICs during installation.

**CAUTION** Adding new vNICs to a service profile 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.

Beginning with VMware vSphere 5.5, VMware does 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. Click Use vNIC Template.
   c. In the vNIC Template field, select vNIC-4-Fabric-A.
   d. In the Adapter Policy field, select VMQ-Default > OK > Add.
Note: Templates created for blade servers with multiple physical network adapters should contain only vNIC-0 and vNIC-1.

3. From the Network tab, select Modify vNIC/vHBA Placement, and select vCon 1 and click >>assign>> for vNIC-4. This applies to the following blade types:
   - Half-width blades (B200/B230/B22) with a single mezzanine card
   - B200M4 or B460M4 blades (with 1240/1280 or 1340/1380 VIC)
   - B420M3 blades (with 1240/1280 VIC)
   - B460 blades with four adapters
   - B480M5 blades (with 1340/1380 or 1440/1480 VIC)

   For servers with 1340 or 1380 single network adaptor, you may experience a mismatch in the order between vNIC in the UCS and VMNIC in the VMware vSphere 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. Click Use vNIC Template.
   c. In the vNIC Template field, select vNIC-5-Fabric-B.
   d. In the Adapter Policy field, select VMQ-Default > OK > Add.

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

6. From the Network tab, select Modify vNIC/vHBA Placement, and depending on the blade type, perform the following for vNIC-5:

<table>
<thead>
<tr>
<th>For this blade type</th>
<th>Do the following</th>
</tr>
</thead>
<tbody>
<tr>
<td>half-width blades (B200/B230/B22) with a single mezzanine card</td>
<td>Select vCon 1 and click &gt;&gt;assign&gt;&gt;.</td>
</tr>
<tr>
<td>B200M4 or B460M4 blades (with 1240/1280 or 1340/1380 VIC)</td>
<td>Select vCon 2 and click &gt;&gt;assign&gt;&gt;.</td>
</tr>
<tr>
<td>B420M3 blades (with 1240/1280 VIC)</td>
<td>Select vCon 3 and click &gt;&gt;assign&gt;&gt;.</td>
</tr>
<tr>
<td>B460 blades with four adapters</td>
<td>Select vCon 3 and click &gt;&gt;assign&gt;&gt;.</td>
</tr>
<tr>
<td>B480M5 blades (with 1340/1380 or 1440/1480 VIC)</td>
<td>Select vCon 3 and click &gt;&gt;assign&gt;&gt;.</td>
</tr>
</tbody>
</table>

   For servers with 1340 or 1380 single network adaptor, you may experience 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.
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.

Before you begin
- Verify the VLAN is configured on the LAN uplink switches and exists in the Cisco UCS Manager.
- Verify the VLAN group exists in the 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 the Global Policies tab.
3. On the In-band Profile window, select the in-band 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 using the Cisco UCS Manager.

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

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

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

Procedure
1. On the Servers tab, select Servers > Service Profiles > Root.
2. Select the desired service profile or service profile template.
4. From the In-band tab, select the KVM VLAN in the Network menu.
5. From the In-band window, select the IPv6 tab.
6. In the Management IP Address Policy menu, select either Static or IPv6 IP pool.
7. If Static is selected, type the IPv6 IP address, prefix, default gateway address, and DNS server addresses, and click OK.

Assign 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 in a VMware cluster evenly 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 equal 32 blades. Four 8-node VMware clusters equal 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.

**Rename 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 a service profile name and click OK.

**Assign or modify a management IP address**

Assign or modify a management IP 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. For a static address, type the IP Address, Subnet Mask, and Gateway.
6. Repeat this process for all service profiles or service profile templates.
Remove LDAP

Remove LDAP from the Cisco UCS.

Procedure

1. Delete the authentication domain.
2. Delete the LDAP Group Maps.
3. Delete all LDAP provider (authentication server) groups.
4. Delete the Provider Servers.
Manage network resources

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 through 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 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 information
Cisco UCS Manager Configuration Guide

Set VLAN on vNIC templates to native

Set VLAN 110 (vcesys_esx_build) on vNIC templates to native.

Procedure
1. Log in to the Cisco UCS Manager and select the Servers tab.
2. Select the LAN tab.
3. From the drop-down menu, select LAN Cloud.
4. At the bottom of the list click VLANs.
5. From the VLAN list, locate and right-click vce_esx_build (VLAN 110).
6. Select Set as Native VLAN and click OK.
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.
4. Select an Ethernet interface and click Modify.
5. If Use vNIC Template is selected, clear it to modify this single service profile.
6. Select the VLAN you created and click OK.
7. Repeat these steps for the other Ethernet interface.

Add a VLAN to the Cisco Nexus switches

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

Before you begin

Name VLANs to identify usage. For example, NFS-VLAN-109.
Verify the Cisco Nexus switches are up and reachable through the console or the management connection.
Verify the following connectivity information for the Cisco Nexus switches:

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

Procedure

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

Remove a VLAN from the Cisco Nexus series switches

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

Before you begin

Verify the Cisco Nexus switches are up and reachable through the console or the management connection.
Verify the following connectivity information for the Cisco Nexus switches:

- Console information
Configure an AMP trunk port

Configure all the default and Logical Configuration Survey (LCS) defined VLAN IDs on the trunk ports for AMP-3S.

**About this task**

See *Default VLANs and parameters (Cisco Nexus management and management aggregation switches)* for the VLAN list.

**Procedure**

1. Set the default or LCS defined description.
2. Set switchport mode to **TRUNK**.
3. Set allowed VLANs to default or LCS defined values.
4. Set spanning-tree port type to **EDGE TRUNK**.
5. Set the MTU value to **9216**.
6. Enable the interfaces.
7. Set the speed for management switch trunk ports to **10000**.
8. Set the speed for the ToR switch for AMP-3S to **10000**.
9. Set the duplex to **full**.

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. For more information, see the *Cisco Nexus 9000 Series Software Configuration Guide*.

Default port channels are:

- POs 3 and 4 for L2 uplinks between optional data switch pairs
- PO 50 for vPC peer links between the data switches
- POs 101 and 102 from the switch to the FIs
- POs 201 and 202 for the X-Blades (if applicable)

To view reserved ports, type: `show vlan brief`
Before you begin

- Verify that the Cisco Nexus switches are reachable through the console or the management connection.
- Verify the vPC and LACP features are enabled on the Cisco Nexus switches.
- Verify that the LACP is enabled on the peering device doing port channeling with the Cisco Nexus switches.
- Verify the appropriate member Ethernet ports are physically cabled.
- Verify the Ethernet ports that become members of this port channel.
- Create a VLAN.
- Obtain required vPCs, IDs, and the VLANs required for each vPC.
- Obtain Cisco Nexus switches IP 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:
   ```
   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:
   ```
   switchport mode <mode>
   ```
   Where *mode*: Trunk | Access
6. To specify the Cisco vPC ID, type:
   ```
   vpc <vPC_ID>
   ```
7. To specify the access VLAN or the VLANs to be trunked, type one of the following:
   ```
   switchport access <vlan_id>
   switchport trunk allowed vlan <vlan_id>
   ```
8. To set the spanning tree port, type:
   ```
   spanning-tree port type <type>
   ```
   Where *type*: normal | network | edge trunk
9. To set the state, type:
   ```
   no shut
   ```
10. To add the appropriate Ethernet ports as members of the vPC:
a. At the Switch-A(config)# prompt, type:
   ```
   interface ethernet <port_number>
   ```

b. At the Switch-A(config-if)# prompt, type:
   ```
   switchport mode <mode>
   ```
   Where mode: Trunk or Access (same as the vPC).

c. Type:
   ```
   channel group <channel_number> mode active
   ```

11. To set the state, at the Switch-A(config-if)# prompt, type: no shut
12. To save the configuration, at the Switch-A# prompt, type: copy run start
13. Repeat this procedure on the peer switch.

### 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, from the Switch-A# prompt, type:
   ```
   config terminal
   ```
3. To remove the appropriate Ethernet port as members of the vPC, type:
   ```
   interface ethernet <port_number>
   ```
4. From the Switch-A(config-if)# prompt, type:
   ```
   no channel group <channel_number> mode active
   ```
5. To delete the vPC, from the Switch-A(config)# prompt, type:
   ```
   no interface port-channel <port_channel_number>
   ```

### Add VLANs to a vPC

VLANs can be added to the trunk of an existing Cisco vPC when it is modified on the Cisco Nexus switch.

**Before you begin**

- Verify that the Cisco Nexus switch is reachable through the console or the management connection.
- Verify that the Cisco vPC that you want to modify is up.
- Obtain the required Cisco vPC ID and VLANs to add to the Cisco vPC.
- Cisco Nexus switch connectivity information (IP address/console information), login credentials, and access method (SSH/TELNET)
Procedure

1. Log in to the primary Cisco Nexus switch.

2. To run the configuration, from the Switch-A# prompt, type:

   config terminal

3. To specify the port channel, from the Switch-A(config)# prompt, type:

   interface port-channel <port_channel_number>

4. To add the VLANs, type:

   switchport trunk allowed vlan add <VLAN_IDs>

5. Repeat this procedure on the peer Cisco Nexus series switch.

Delete 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, from the Switch-A# prompt, type: config terminal

3. From the Switch-A(config)# prompt, type:

   interface port-channel <port_channel_number>

4. To delete the VLAN ID, from the Switch-A(config-if)# prompt, type:

   switchport trunk allowed vlan remove <VLAN_IDs>

Add VLANs to vPCs for Disjoint Layer 2 networks

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

About this task

All VLANs must be explicitly assigned to an uplink, including VLANs added after initial deployment. Otherwise, a VLAN is enabled 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 switches. 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), assign the same VLAN for vPCs 101 to 104.
Before you begin

The procedure provides an example scenario for adding VLANs to port channels 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 vPCs 101 and 105 (Fabric B) are displayed under all required VLANs. See View VLANs assigned to VPCs 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 VLAN Manager.

   e. Select Fabric B.

   f. In the Port Channels and Uplinks tab, select Port-Channel 102.

   g. In the VLANs table, select the VLANs to assign to port channel 102.
      Use the CTRL key to select more than one VLAN.

   h. Select Add to VLAN and click OK.

   i. In the Port Channels and Uplinks tab, select Port-Channel 106.

   j. In the VLANs table, select the VLANs to assign to vPC 106.

   k. Select Add to VLAN and click OK.

   l. Verify vPCs 102 and 106 (Fabric B) are displayed under all required VLANs.

**Related information**

**Configure upstream disjoint layer 2 network**

**View VLANs assigned to vPCs for Disjoint Layer 2 networks**

Verify VLANs have been assigned to vPCs.

**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 the FI.
7. In the VLANs table, expand the appropriate node and the VLAN to view the assigned ports or vPCs.
Upgrade Cisco Nexus switch software

Upgrade the system image on the Cisco Nexus switches.

About this task

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

Before you begin

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 *Upgrading or Downgrading to a new release* in Release Notes.

- Obtain console (terminal) access and management IP access.
- Obtain a Cisco account to download images.
- Verify 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 switch.
2. Upload the file to the switch with the copy server (TFTP, SCP, FTP, or SFTP) being used.
3. To back up the switch running the configuration, type:
   
   ```
   copy running-config startup-config
   ```
4. To verify the switch has enough space for the new image, from the `Switch-A#` prompt, type:
   
   ```
   dir bootflash:
   ```
5. If there is not enough space, type:
   
   ```
   delete bootflash:<file_name>
   ```
6. To copy the updated images to the switch, from the `Switch (config)#` prompt, type:
   
   ```
   copy <ftp | scp>: bootflash:
   ```
   ```
   copy ftp: bootflash:
   ```
   a. Type the filename of the kickstart bin file from the Cisco download site.
      
      For example, `n9000-dk9.6.1.2.I2.2(1).bin`
   b. For VRF, type: `management`.
   c. Type the hostname of the SCP or FTP server.
   d. Type the username and password.
7. To view the impact of the upgrade, from the `Switch-A(config)#` prompt, type:
show install all impact kickstart bootflash:n9000-xx.xx.bin

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

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.
Switch(config)# 2011 Sep  8 18:16:43 Switch Sep  8 18:16:43 %KERN-0-SYSTEM_MSG: Shutdown Ports.. - kernel
2011 Sep  8 18:16:43 Switch Sep  8 18:16:43 %KERN-0-SYSTEM_MSG: writing reset reason 49, - kernel
Broadcast message from root (Thu Sep  8 18:16:43 2011):
The system is going down for reboot NOW!

9. Type Y to go to the installation.
10. When the switch reboots, to verify that the updated version of the software is running, type: show version
11. Verify the system image file that displays 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
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.
To reverse a Cisco Nexus series switch software upgrade, perform the upgrade steps using the earlier version of the software.

For more information, see the following:
- Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide
- Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide
Use Cisco DCNM

Cisco DCNM is installed as part of the AMP-VX management suite. See the Cisco DCNM online help system for more information.

1. Point your web browser to https://<FQDN of DCNM server>
2. Log in with the default username and password.
3. To access help, click admin or the user ID on the top-right corner of the window.
4. Select Help Content.

Discover LAN devices with Cisco DCNM

Discover the LAN devices with the Cisco DCNM application.

About this task
For Cisco DCNM to manage the LAN switches, they must be discovered.

Procedure
1. Log in to Cisco DCNM by opening a browser to the Cisco DCNM VM management IP address.
2. Select Inventory from the menu.
4. Click the plus sign (+) to add LAN switches.
5. Set the Discovery Type to Switch List.
6. In the Switch List field, type a comma-separated list containing all LAN devices that you would like to add.
7. Type the username and password for the switches.
8. Leave all remaining fields at their default values.
9. Click Next.
10. Verify that all switches were found.
11. Select the checkbox next to each switch and click Add.

Configure switch groups with Cisco DCNM

Because a single Cisco DCNM instance can manage multiple VxBlock Systems, sort switches into groups for ease of identification.

About this task

Procedure
1. Go to the Cisco DCNM VM management IP address to log in to Cisco DCNM.
2. Select Administration > Switch Groups, and click Add.
3. Type the name of the VxBlock Systems from the LCS. Click Add.
4. Click and drag each LAN switch into the newly created folder. Click Add.
5. Type the name of the VxBlock Systems from the LCS, and append -SAN to the name.
6. Click Add.
7. Click and drag each SAN switch into the new folder.
View network topology and SAN components

The topology view gives a customizable, graphical view of the network and SAN components of the VxBlock System 1000 for Cisco DCNM.

Procedure

1. On the Menu bar, click Topology.
2. Click elements to select them or drag elements to move them.
3. Click Save to save the layout.

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
Manage storage - Cisco MDS switches

Follow best practices to configure, zone and manage Cisco MDS switches.

Best practices to configure

The Cisco MDS 9148S Multilayer Fabric Switch uses a three-forwarding engine architecture which has the following capacities:

- Each forwarding engine has 2,852 TCAM entries, which limits the number of hosts that are supported per forwarding engine.
- Each forwarding engine supports a maximum of 64 servers.
- If the servers are spread across the three forwarding engines (e0-e2) on the switch, each switch supports a maximum of 192 servers.

The following switches use dynamic port mapping for device connectivity:

- Cisco MDS 9706 Multilayer Director Switch
- Cisco MDS 9710 Multilayer Director Switch
- Cisco MDS 9148S Multilayer Fabric Switch
- Cisco MDS 9148T 32G Multilayer Fabric Switch
- Cisco MDS 9396S 16G Multilayer Fabric Switch
- Cisco MDS 9396T 32G Multilayer Fabric Switch

The following switches do not have the TCAM exhaustion issue:

- Cisco MDS 9706 Multilayer Director Switch
- Cisco MDS 9710 Multilayer Director Switch
- Cisco MDS 9148T 32G Multilayer Fabric Switch
- Cisco MDS 9396S 16G Multilayer Fabric Switch
- Cisco MDS 9396T 32G Multilayer Fabric Switch

The following switches are built on the same ASICs as the Cisco MDS 9700 32 G Line Card:

- Cisco MDS 9148T 32G Multilayer Fabric Switch
- Cisco MDS 9396T 32G Multilayer Fabric Switch

Each ASIC contains 16 32 G ports. The switches and line card have the following capacities:

- The Cisco MDS 9148T and the Cisco MDS 9700 48 port 32 G Line Card contain three ASICs (forwarding engines).
- The Cisco MDS 9396T contains six ASICs.
- Each forwarding engine supports 49,136 Region 3 (zoning) TCAM entries.

The Cisco MDS 9148S 16G Multilayer Fabric Switch has three forwarding engines with four port groups of four ports each (total 16 ports per engine). Each forwarding engine is limited to 2,852 Region 3 (Zoning) TCAM entries. This limit restricts the number of hosts that can be zoned behind each UCS FC port channel.

The Cisco MDS 9396S 16G Multilayer Fabric Switch has 12 forwarding engines with two port groups of four ports each (total eight ports per engine). Each forwarding engine is limited to 49,136 Region 3 (Zoning) TCAM entries. To distinguish servers on the compute side, create multiple pools or blocks of 64 WWNs instead of one large pool/block of 128 identifiers. Essentially, each WWPN should have a distinguishing value relative to its corresponding N-Port-channel. The vHBA templates should ensure that servers are pinned to the appropriate N-Port-channels.
See Cisco issue CSCuz11494 when bringing up an FC port-channel-trunk between a Cisco MDS Switch and a Cisco UCS switch.

**Best practices to zone Cisco MDS switches**

- Use smart zoning on the Cisco MDS switches (unless restricted by the HBA device vendor).
- Use enhanced zoning.
- Use the device alias and FC alias.
- Specify the zone member types as FC alias.
- FC alias member types = device alias. Identify the device alias member as the target or initiator.

**Note:** There is a fabric-wide limit of 8000 device aliases and 2000 FC aliases.

**Upgrade or downgrade Cisco MDS switch software**

Upgrade or downgrade Cisco MDS switch software for RCM compliance.

Use the upgrade or downgrade procedures in the Cisco MDS 9000 NX-OS Software Upgrade and Downgrade Guide for your release.

**Configure a VSAN**

Configure a VSAN and assign FC interfaces.

**Before you begin**

- Verify that the Cisco MDS switch is up and reachable through the console or management connection.
- Obtain required VSAN names and FC interfaces to assign to the VSANs.
- Obtain Cisco MDS switch IP address/console information, login credentials, and access method (SSH/TELNET).
- Name the VSANs to identify usage. For example, for VSAN 10: vsan-A-10

**Procedure**

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

   vsan <vsan_id> interface fc <interface_id>

Related information
Configure and Manage VSANs

Remove a VSAN

Remove a VSAN and associated FC interfaces.

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

Procedure

1. Log in to the Cisco MDS switch.
2. To view VSANs, type:
   
   show vsan

3. To enter the global configuration mode and start the configuration, type:
   
   configure terminal

4. To configure the database for VSAN, from the switch(config)# prompt, type:
   
   vsan database

5. To delete a VSAN, from the switch(config-vsan-db)# prompt, type:
   
   no vsan <vsan_id>

Related information
Configure and Managing VSANs

Configure a VSAN domain ID and priority

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.

Before you begin

A unique domain ID must be assigned to the new VSAN added to the switch. When a new VSAN is added to a switch in a fabric, use the domain manager 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 you want to assign 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 IP address/console information, login credentials, and access method (SSH/TELNET).

**Procedure**

1. Log in to the Cisco MDS switch.
2. To view VSANs, type:
   ```
   show vsan
   ```
3. To view the domain ID of the existing VSAN on the switch, type:
   ```
   show fcdomain domain-list
   ```
4. To enter the global configuration mode and start the configuration, type:
   ```
   configure terminal
   ```
5. To assign a domain ID, at the `switch(config)#` prompt, type:
   ```
   fcdomain domain <domain_id> static vsan <vsan_id>
   ```
6. To assign a priority, type:
   ```
   fcdomain priority 2 vsan <vsan_id>
   ```
7. To restart the VSAN with these changes, type:
   ```
   fcdomain restart vsan <vsan_id>
   ```

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

Remove the domain ID and priority to ensure the switch is no longer a principal switch in that VSAN. This enables the domain ID in that VSAN to be changed during a fabric merge.

**Procedure**

1. To enter the global configuration mode and start the configuration, type:
   ```
   configure terminal
   ```
2. To remove the domain ID, at the `switch(config)#` prompt, type:
   ```
   no fcdomain domain <domain_id> static vsan <vsan_id>
   ```
3. To remove priority, type:
   ```
   no fcdomain priority 2 vsan <vsan_id>
   ```

**Enable FC interfaces**

Enable FC interfaces on the Cisco MDS switch.

**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 IP address/console information, login credentials, and access method (SSH/TELNET).

Procedure
1. Log in to the Cisco MDS switch.
2. To start the configuration, type:
   ```
   config terminal
   ```
3. To configure the interface, at the `switch(config)#` prompt, type:
   ```
   interface fc <interface_id>
   ```
4. For switches with port licenses, at the `switch(config-if)#` prompt, type:
   ```
   port-license acquire
   ```
5. To enable the interface, type:
   ```
   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.

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 IP 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:
   ```
   config terminal
   ```
3. To specify the interface, at the `switch(config)#` prompt, type:
   ```
   interface fc <interface_id>
   ```
4. To disable the interface, at the `switch(config-if)#` prompt, type:
   ```
   shutdown
   ```
Move licenses between FC interfaces

Move licenses between FC interfaces on Cisco MDS switches.

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

Procedure

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

Port licenses can be disabled and moved to other interfaces.

About this task

To configure the switch for other SAN features, see the Cisco MDS 9000 NX-OS Fabric Configuration Guide.

Procedure

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

2. To configure the interface where license is being moved, type:
   
   ```
   switch(config)# interface fc <interface_id>
   ```

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

4. To exit, type:
   
   ```
   switch(config-if)# end
   ```

Create backups of Cisco MDS switch startup and configuration files

Create a backup of the Cisco MDS switch startup and running configuration files.

About this task

Backups are stored on the VxBlock Systems 1000 management server.

Before you begin

- Start the TFTP service on each management server.
- Create the following folder on each management server (if it does not yet exist):
  
  ```
  D:\Cisco\MDS\switch-model\config
  ```
- Obtain the int-mdsbackup login and password to log in to the Cisco MDS switches.

Procedure

1. Log in to the switch with PuTTY using your int-mdsbackup login.
2. Use the copy command to create the configuration file backups.

After you finish

Schedule the backup to run on a regular basis.
Schedule backups of startup and configuration files for Cisco MDS switches

Create and schedule a job to back up the Cisco MDS switch startup and configuration files.

Procedure

1. From the host, at the switch# prompt, type:
   ```
   config t
   ```

2. At the switch(config)# prompt, type the following commands, one per line. At the end of each line, type Ctrl-Z:
   ```
   scheduler aaa-authentication username <username> password <password>
   scheduler job-name <job_name>
   ```

3. To create a backup for the startup-config and running-config files, at the switch(config-job)# prompt, type commands similar to the following:
   ```
   copy startup-config tftp://192.168.101.93/9502/config/V00101MDxxxx_startup_$ (TIMESTAMP).config
   copy running-config tftp://192.168.101.93/9502/config/V00101MDxxxx_running_$ (TIMESTAMP).config
   end
   ```

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

4. Type the following commands, one per line. At the end of each line, type Ctrl+Z.
   ```
   switch# conf t
   switch(config)# scheduler schedule name <name>
   switch(config-schedule)# job name <name>
   switch(config-schedule)# time daily 23:00
   switch(config-schedule)# show scheduler schedule
   switch(config-schedule)# end
   ```

5. To verify the action, type:
   ```
   switch# show schedule config
   ```
Create a script to purge copies of the backup files

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 and save it as D:\scripts\delete_old_backups.vbs. This script deletes any file in the D:\Cisco\9xxx\config directory with a .config file extension older than 7 days.

```
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

Create a task to purge older backup files.

About this task

The D:\scripts\delete_old_backups.vbs that deletes older backups. Complete the following steps to schedule that script to run on a daily basis. This script deletes any file in the D:\Cisco\9xxx\config directory with a .config file extension older than seven days.

Before you begin

Obtain the password for the [Domain]\svc-vmfms01 account from your VMware administrator.

Procedure

1. To create a task within the VMFMS01 server to run the .vbs script daily at 01:00, select Start > Programs > Accessories > System Tools > Scheduled Tasks.
2. Browse to D:\scripts\delete_old_backups.vbs.
3. Use the credentials for the [Domain]\svc-vmfms01 account to run the task.

4. On the Schedule tab, schedule the task to run daily at 1:00 AM.
Manage storage - Dell EMC Unity or Unity XT storage

Create storage pools

The Dell EMC Unity or Dell EMC Unity XT storage array consists entirely of virtual drive pools.

**About this task**

Configure fewer, larger pools to enable the array to place the data where it is most appropriate. A single pool can accommodate both Block and File data. For VMware, both boot LUNs and data LUNs can reside in the same pool. Use multiple when there are drives of different sizes.

For Hybrid arrays, use multiple pools only when different drive types/sizes are used or when different types of data have different performance requirements. For instance, data may require a multiple tier pool. Place data that is more static in a pool that contains only capacity tier drives. Whenever possible, use at least 5% of a multiple tier disk pool for the Extreme Performance (flash drive) Tier.

Separate pools should be created for any bare metal server to reduce the effect of bare metal servers on the system.

**Note:**

A Dynamic Pool is created by default when creating a pool in Unisphere in Dell EMC Unity OE version 4.2 and later for All-Flash arrays.

**Procedure**

1. From the Unisphere GUI, log in to the Dell EMC Unity or Dell EMC Unity XT storage array to create the storage pool.
2. Select **Storage > Pools**.
3. Click + to create the storage pool.
4. Enter information into the **Pool Name** and **Description** fields.
5. Click **Next**.
6. In the **Select Storage Tiers** page, choose the preferred tier and RAID configuration.
7. Click **Next**.
8. Select the amount from the **Storage** menu and click **Next**.
9. Leave the default settings for **VMware Capability Profile**.
10. Click **Next**.
11. In the **Summary** page, review the selections.
12. When satisfied with the selections, click **Finish**.

**Notes:**

- Hybrid models display the default RAID configuration for your Tier selection.
- For Hybrid models, Fast Cache is enabled by default. Disable Fast Cache if you have Extreme Performance Tier in your pool.
Expand a storage pool

Expand a storage pool on the Dell EMC Unity or Dell EMC Unity XT storage array to increase capacity to grow existing LUNs or create new ones.

About this task

By default, pools created on All-Flash arrays are dynamic and can be expanded by one or more drives. Dynamic pools are comprised of Drive Partnership Groups (DPG), which are a grouping of up to 64 drives. To expand beyond 64 drives in a pool, the system must create an additional DPG. Each additional DPG requires a minimum number of drives based on the RAID stripe width. For example, a RAID 5 dynamic pool created with 6 drives has a RAID width of 4+1. To expand this pool beyond 64 drives, you need an additional 6 drives (spare capacity equal to one drive) to create the additional DPG. A pool with a RAID 5 stripe width of 12+1 requires 14 drives to create the additional DPG.

For more information on dynamic pools, see Dell EMC Unity Dynamic Pools.

Traditional pools can be expanded by the RAID stripe width. For example, RAID 5 4+1 requires 5 drives. The system does not allow a traditional pool to be expanded beyond the available hot spare coverage. If you have a RAID 5 4+1 configuration and try to expand the pool using the last five un-configured drives, the system will prevent the action.

Before you begin

Verify that storage pools exist and disk drives are available to expand the storage pool.

Procedure

1. From the Unisphere GUI, log in to the Dell EMC Unity or Dell EMC Unity XT storage array to expand the storage pool.
2. Select Storage > Pools.
3. Select the check box for the pool you want to expand and click Expand Pool.
4. In the Select Storage Tiers page, select the tier that has available drives.
5. Click Next.
6. Select the amount from the Storage menu and click Next.
7. In the Summary page, review the selections.
8. When satisfied with the selections, click Finish.

Related information

Dell EMC Unity Dynamic Pools

Allocate block storage

On all Dell EMC Unity or Dell EMC Unity XT storage arrays, you can allocate storage to one or more hosts.

About this task

You can allocate additional storage to one or more hosts in the following ways:

- Create a new LUN from the same or a different pool
- Extend an existing LUN.
- Add additional hosts to existing LUNs.

The following topics explain how to allocate storage using each of these methods.
Create a LUN from the same or different pool

Create a LUN from the same or different pool.

About this task

With Dell EMC Unity or Dell EMC Unity XT OS 4.5 and later, you can create multiple LUNs. When you create multiple LUNs or when the LUN names are not unique, the storage system appends a number to the LUN name.

Procedure

1. From the Unisphere GUI, log in to the Dell EMC Unity or Dell EMC Unity XT storage array to allocate storage.
2. Select Storage > Block > LUNs.
3. To create a LUN, click +.
   
   Note: If you are creating more than one LUN, enter the number of LUNs you want to create.

4. Using the wizard, perform the following steps:
   a. Type the name and description.
   b. Select the storage pool, tiering policy, capacity, wanted host I/O limit and, if necessary, data reduction.
   c. Click Next.

   Notes:
   • Enable data reduction on data LUNs only if you have determined that the application is suited to handle compression.
   • Data reduction is supported only on All-Flash pools.
   • Advanced deduplication is available on the following Dell EMC Unity and Unity XT storage arrays:
     - Dell EMC Unity OE 4.5 and later:
       - Unity All-Flash 450F
       - Unity All-Flash 550F
       - Unity All-Flash 650F
     - Dell EMC Unity OE 5.0 and later:
       - Unity XT All-Flash 380F
       - Unity XT All-Flash 480F
       - Unity XT All-Flash 680F
       - Unity XT All-Flash 880F arrays
   d. Click + to configure host access and select the designated hosts.
   e. Click OK.
   f. Set the host LUN ID by clicking the pencil icon. Alternatively, you can enable the system to automatically assign the ID by omitting a value.
   g. Click Next.
   h. Set the defined snapshot and replication options.
   i. In the Summary page, review the selections.
   j. When satisfied with the selections, click Finish.
Modify LUN settings

Modify existing LUN settings and enable advanced deduplication and data reduction.

About this task

You can enable advanced deduplication on the following Dell EMC Unity and Unity XT storage arrays:

- Dell EMC Unity OE 4.5 and later:
  - Unity All-Flash 450F
  - Unity All-Flash 550F
  - Unity All-Flash 650F
- Dell EMC Unity OE 5.0 and later:
  - Unity XT All-Flash 380F
  - Unity XT All-Flash 480F
  - Unity XT All-Flash 680F
  - Unity XT All-Flash 880F arrays

To enable advanced deduplication, you must enable data reduction first.

Procedure

1. From the Unisphere GUI, log in to the Dell EMC Unity or Dell EMC Unity XT storage array to allocate storage.
2. Select **Storage > Block > LUNs**.
3. Check the LUN and perform the following steps:
   a. Click the pencil icon.
   b. From the **General** tab, modify the name, description, size, or SP owner, and enable or disable data reduction.
      
      **Note:**
      - Enable data reduction on data LUNs only if the application can handle compression.
      - Data reduction is supported only on All-Flash pools.

4. To enable data reduction and advanced deduplication on an existing LUN, perform the following steps:
   a. Select **Data Reduction**.

      All previously written data is left in its original state. Data reduction applies only new writes or overwrites. To apply data reduction savings on existing storage data, use the **Local LUN Move** option.

      Pool performance may be impacted during the move operation.

      **Note:** Data reduction is supported only on All-Flash pools.
   b. (Optional) Select the **Advanced Deduplication** check box.
5. Click **Next**.
6. In the **Summary** page, review the selections.
7. When satisfied with the selections, click **Finish**.
Add hosts to existing LUNs

Add hosts to existing LUNs.

Procedure

1. From the Unisphere GUI, log in to the Dell EMC Unity or Dell EMC Unity XT storage array to allocate storage.
2. Select Storage > Block > LUNs.
3. Select the LUN.
4. Click the pencil icon.
5. In the LUN Properties window, select the Host Access tab.
6. Click + to add or modify the host access.
7. Follow the wizard to create new hosts, grant access to existing hosts, or modify the type of access to the LUN and its snapshots.

Modify the host LUN ID

Modify the host LUN ID.

Procedure

1. From the Unisphere GUI, log in to the Dell EMC Unity or Dell EMC Unity XT storage array to allocate storage.
2. Select Storage > Block > LUNs.
3. Select the LUN.
4. Click the pencil icon.
5. From the Host Access tab, select hosts to modify their Host LUN IDs.
6. Click Modify Host LUN IDs.
7. Click the pencil icon to modify the host LUN ID.
8. Click OK.

Manage NFS

Create the NAS server

NAS servers can share file storage using various protocols including CIFS/SMB, NFS, and FTP.

About this task

To allocate file storage, first create a NAS server on the Dell EMC Unity or Dell EMC Unity XT storage array. The NAS server is a stand-alone service with dedicated network interfaces to share file through single or multiple NAS protocols. The network interfaces can share a common physical connection to the LAN with other NAS servers.

Separate, dedicated physical links are required for internal or external NAS servers. Internal servers provide file shares to hosts and VMs inside the VxBlock System. External servers connect to LAN devices outside of the VxBlock System.

A NAS server must be assigned to run primarily on one SP. If an SP outage occurs, the NAS server automatically fails over to the other SP. To balance workload across SPs, allocate NAS servers in pairs, one on SP-A and the other on SP-B. Each server shares different file systems. IP multitenancy is optional and can be configured depending on the use case.

Procedure

1. Log in to the Dell EMC Unity or Dell EMC Unity XT storage array where you want to create a NAS server.
2. Select **Storage > File > NAS Servers**.

3. Click + to create a server.

4. Using the wizard, perform the following:
   a. Type the name, tenant, storage pool, and SP.
   b. Click Next.
   c. Select the Ethernet port (physical link), IPv4/IPv6 information, and VLAN.
   d. Click Next.
   e. Select the protocol (NFS, SMP, or Multiprotocol).
   f. Click Next.
   g. Configure the **Unix Directory Service**.
   h. Click Next.
   i. Enable DNS and specify domain servers.
   j. Click Next.
   k. (Optional) Configure replication settings.
   l. Click Next.
   m. In the Summary page, review the selections.
   n. When satisfied with the selections, click Finish.

5. Create a second NAS server with similar characteristics on the other SP.

**Create the file system**

Specify the file system size, storage type, the NAS server, and other characteristics, such as snapshots and replication.

**Procedure**

1. From the Unisphere GUI, log in to the Dell EMC Unity or Dell EMC Unity XT where you want to create a file system.

2. Select **Storage > File > File Systems**.

3. Click + to create a file system.

4. Using the wizard, perform the following:
   a. Set the NAS protocol and server.
   b. Click Next.
   c. Type the name and description of the file system.
   d. Click Next.
   e. (Optional) Configure the **File-level Retention**.
   f. Click Next.
   g. Select the pool and tiering policy.
   h. Select the file system options as defined in the LCS: (Thin, Data Reduction, and Advanced Deduplication)

   **Note:**
   - Enable Data Reduction on data LUNs only if the application can handle the increased latency.
   - Data Reduction is supported only on All Flash pools.
Advanced Deduplication is available only on Dell EMC Unity All-Flash 450F, 550F, or 650F arrays (Dell EMC Unity OE 4.5 and later) or Dell EMC Unity XT 380F, 480F, 680F, and 880F arrays (Dell EMC Unity OE 5.0 and later). You can enable Advanced deduplication only if you have enabled Data Reduction first.

i. (Optional) Configure the initial NFS share and access.

j. Click Next.

k. Set the snapshot and replication options.

l. In the Summary page, review the selections.

m. When satisfied with the selections, click Finish.

**Create the tenant**

Create a tenant by specifying the name, optional UUID, and adding VLANs.

**Procedure**

1. Using the Unisphere GUI, log in to the Dell EMC Unity or Dell EMC Unity XT storage array where you want to create a tenant.
2. Select Storage > File > Tenants.
3. Click + to create a new tenant.
4. Using the wizard, perform the following:
   a. Type the name of the tenant.
   b. Optionally, specify a manual UUID by enabling the check box and typing a UUID.
   c. Select Add to enter a VLAN.
   d. Repeat step c for each additional VLAN.
   e. Click OK.

**Create an NFS share**

An NFS share defines the access of a file system on the array, including the share name and authorization access to the file system.

**About this task**

An NFS share can have a defined default access type such as No Access.

**Procedure**

1. From the Unisphere GUI, log in to the Dell EMC Unity or Dell EMC Unity XT storage array where you want to create the NFS share.
2. Select Storage > File > NFS Shares.
3. Click + to create an NFS share.
4. Using the wizard, perform the following:
   a. From the File System menu, select the file system to be shared.
   b. Click Next.
   c. Type the share name, description, and local path of the NAS server.
   d. Click Next.
e. Set the default access and defined host access rights.

f. Click **Next**.

g. In the **Summary** page, review the selections.

h. When satisfied with the selections, click **Finish**.
Manage storage - Isilon

Use the OneFS interface to manage SMB shares, NFS exports, and SmartQuotas.

1. Download the *Isilon OneFS Web Administration Guide*. Search support.emc.com for the following string: Isilon OneFS Web Administration Guide

2. Find the following procedures in the Isilon OneFS Web Administration Guide:
   - Create an SMB share
   - Modify an SMB share
   - Delete an SMB share
   - Add a user or group to an SMB share
   - Create an NFS export
   - Modify an NFS export
   - Delete an NFS export
   - Create SmartQuotas
   - Manage SmartQuotas
Manage storage - PowerMax and VMAX arrays

Unisphere for PowerMax and VMAX is an intuitive management interface that provides simpler configuration of the array by reducing the number of required steps.

The services for Unisphere for PowerMax and VMAX, Solutions Enabler, and SMI-S are embedded with Embedded Management (eMGMT).

For more information about creating and managing storage groups, initiator groups, port groups and masking views, see the Unisphere for PowerMax Online Help or Unisphere for VMAX Online Help.

Log in to a PowerMax or VMAX storage array

Log in to the storage array using Unisphere for PowerMax or VMAX.

Before you begin

Verify that you have the proper IP addresses of the PowerMax or VMAX eMGMT servers.

Obtain the username and password for Unisphere for PowerMax or VMAX.

Procedure

1. To launch Unisphere for the storage array, type the following URL:
   
   `https://emgmt IP:8443`

2. Log in with user credentials.

eNAS for PowerMax or VMAX configuration guidelines

Data LUN and file system configuration guidelines to manage embedded NAS (eNAS) for PowerMax or VMAX.

Data LUN configuration guidelines

Use the following default values unless otherwise specified:

- Use the Provision Storage for File option to create storage groups. This option creates a masking view for each storage group using the EMBEDDED_NAS_DM_IG initiator group and the EMBEDDED_NAS_DM_PG port group.
- Create the storage groups for each application with the following options:
  - Storage Resource Pool (SRP): SRP_1
  - Service Level Objective (SLO): Diamond (or the LCS value)
  - Compression: Clear if the customer has not selected this option.
  - Enable Compliance Alerts: Check if the customer has selected this option.
  - Create configured volumes in multiples of eight.
  - From the total pool size (total capacity/number of volumes), determine the size of the device.
  - Target and LUN addressing for all eNAS data LUNs should be 10 or higher (hexadecimal) and should use the next available address.
  - eNAS target LUN assignments 00 through 0F are reserved and cannot be used for eNAS data LUNs.
File system guidelines

For best performance, create sliced devices that enable the control station to allocate space across available LUNs in the pool.

The following replication requirements may restrict slicing:

- TF/SRDF require full volumes so slicing is not permitted.
- Slicing is permitted for VNX Replicator because it replicates the file system regardless of the underlying storage volume configuration.
- Select Thin Enabled for the file system even though all underlying LUNs are thin.
- Optionally, select Deduplication Enabled.
- Optionally, select VMware VAAI nested clone support.
- Do not use of the autoextend feature unless requested. The autoextend feature reduces the possibility of a file system full event, but requires monitoring and space management.
- The maximum recommended file system size is 16 TB. File systems larger than 16 TB cannot be backed up and restored while maintaining SLAs.
- Enable uncached write on NFS file systems to be used as VMware datastores.
- You can increase performance by caching writes in the X-Blade and not requiring downstream acknowledgments from the array before acknowledging the write to the host. If an extended power outage occurs, X-Blades are not designed to preserve cached writes.

**Note:** If the X-Blade cache is not bypassed to increase performance, you may experience data loss or corruption during an extended power outage.
System operation of the XtremIO storage array is controlled by a standalone Linux-based server called XtremIO Management Server (XMS). The XMS host is deployed as a virtual server (VM) on the VxBlock 1000 Management infrastructure. XtremIO can continue operation when disconnected from the XMS, but cannot be managed.

Access the Dell EMC XtremIO User Guide.

In Managing Tags, locate the following tasks:
- Creating and Assigning a New Tag
- Assigning Tags to Storage Elements
- Modifying Tags
- Untagging an Object
- Removing a Tag

In Managing Volumes and Copies, locate the following tasks:
- Creating a Volume
- Modifying Volume Properties
  -Renaming a Volume
  -Resizing a Volume
- Removing a Volume
- Managing Initiator Groups
- Managing Initiators
- Mapping
- Cluster Operations

In Managing Initiator Groups, locate the following tasks:
- Creating an Initiator Group
- Renaming an Initiator Group
- Removing an Initiator Group
- Modifying the Initiators List in an Initiator Group

In Managing Initiators, locate the following task:
- Renaming an Initiator

In Mapping, locate the following tasks:
- Generating LUN Mappings for Volumes and Initiator Groups
- Deleting LUN Mapping for Selected Volumes and Initiator Groups
- Changing LUN Mapping for Selected Volumes and Initiator Groups

In Cluster Operations, locate the following tasks:
- Managing the Virtual XMS
  - Expanding the Virtual XMS Configuration
Manage virtualization (VMware vSphere 6.x)

This section contains virtualization procedures that are applicable for VMware vSphere 6.5 and 6.7. In cases where procedures are different, separate procedures are provided.

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.

---

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

Patch the VMware vSphere ESXi hosts with VUM (Flex 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 the VMware vSphere Web client.

2. Select the VMware vSphere ESXi host, right-click and select Maintenance mode > Enter Maintenance Mode.

3. In the VMware vSphere Web Client, select the host and select the Update Manager tab.

4. Click Go to Admin View tab.

5. Click the Manage tab.
6. Select Download Settings.
7. In the Download Sources window, select Import Patches.
8. On the Upload Patches 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, then it is possible that the .zip file was corrupted during the download process or the incorrect zip file has 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 new baseline.
16. In the New Baseline wizard:
   a. In the Name field, type the package name. For example, PowerPath.
   b. For baseline type, click Host Patch.
   c. Click Next.
   d. In the Patch Options page, leave defaults selected and click Next.
   e. In the Patches page, include all desired patches.
   f. Click Next.
   g. Click Finish.
17. Attach the package baseline to the desired VMware vSphere ESXi hosts.
   You can attach the package baseline to individually selected VMware vSphere ESXi hosts or to multiple hosts at a time by selecting 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 and highlight the desired host in the list to the left of the VMware vSphere Web Client pane. To attach the package baseline to several VMware vSphere ESXi hosts, perform the following:
   a. In the list to the left of the VMware vSphere Web Client pane, select a folder, cluster, or datacenter.
   b. In the right pane, select Update Manager tab and then click Attach Baseline.
      The Attach Baseline or Baseline Group window appears.
   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, highlight the package baseline that was created.
b. Click **Stage Patches**.

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.

c. Click **Next**.

In the **Hosts** window, all the VMware vSphere ESXi hosts to which the package baseline is attached are selected by default.

d. If required, change the default Host selection to stage the baseline to only one or some of the VMware vSphere ESXi hosts.

e. Click **Next**.

f. In the **Patch and Extension Exclusion** window, verify the **Package** information and click **Next**.

g. 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. Highlight the VMware vSphere ESXi host to remediate and click the **Update Manager** tab

b. In the **Independent Baselines** section, highlight the package baseline that was created and click **Remediate**.

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.

The default **Baseline Groups and Types** and **Extension Baselines** default selections should not be altered.

c. Click **Next**.

d. In the **Select target objects** page, all the VMware vSphere ESXi hosts to which the package baseline is staged are selected by default. If desired, change the default Host selection to remediate the baseline to only one or some of the VMware vSphere ESXi hosts.

e. Click **Next**.

f. When the **Patches and Extensions** window appears, verify the information and click **Next**.

g. In the **Advanced options** page, click **Next**.

h. Click **Next**.

i. When the **Ready to Complete** window appears, verify the information and click **Finish**.

---

**Supported guest operating systems (VMware vSphere 6.x)**

To install 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 is automatically deployed when VMware tools are installed.

*VMware Guest Operating System Installation Guide*
VMware para virtual SCSI controllers (VMware vSphere 6.x)

VMware vSphere selects the recommended virtual SCSI controller that is based on the operating system installed to the new VM. Dell EMC recommends maintaining the automatically selected virtual SCSI controller.

Changing to the VMware para virtual SCSI controller may result in better I/O performance and reduced CPU utilization on the VM. Additional information and limitations of the VMware para virtual adapter can be found in the *vSphere Virtual Machine Administration Guide* in the section titled *About VMware Para virtual SCSI Controllers*.

For optimal resource utilization of VMs with XtremIO, Dell EMC recommends configuring VMs with VMware para virtual SCSI controllers.

*VMware vSphere Virtual Machine Administration Guide*

Use VMware Enhanced vMotion Compatibility with Cisco UCS blade servers (VMware vSphere 6.x)

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

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:

- If the CPU feature sets are greater than the EVC mode you are enabling, power down all VMs in the cluster and enable or modify the EVC mode.
- To ensure complete and reliable vMotion compatibility when mixing blade types in a single cluster, use Intel "Nehalem" Gen. (formerly Intel Xeon Core™ i7) EVC mode.
- EVC mode should be enabled 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. This eliminates the need to power down the VMs running on the blade servers. Setting a lower EVC mode than the CPU can support may hide some CPU features, which may impact performance. Proper planning is needed if performance or future compatibility within the cluster is desired.
- For EVC mode compatibility support see VMware KB article 1003212.

Enable VMware Enhanced vMotion Compatibility in a cluster (VMware vSphere 6.x)

Enable VMware Enhanced vMotion Compatibility (EVC) within a cluster.

About this task

The VMware EVC ensures vMotion compatibility for hosts in a cluster. VMware EVC verifies that all hosts in a cluster present the same CPU feature set to the VMs, even if the CPUs on the hosts are different. The EVC feature uses the Intel FlexMigration technology to mask processor features so that hosts can present the feature set of an earlier generation of processors. This feature is required if hosts in a cluster use different CPU types.

Before you begin

Before enabling VMware EVC on an existing cluster, ensure that the hosts in the cluster meet the requirements listed in EVC Requirements in the VMware vSphere ESXi and vCenter Server Documentation.
Procedure

1. You can optionally create an empty cluster.
   If you have already created a cluster, skip this step. This is the least disruptive method of creating and enabling a VMware EVC cluster.
2. Select the cluster for which you want to enable VMware EVC.
3. Power off all the VMs on the hosts with feature sets greater than the VMware EVC mode.
4. Migrate the cluster's VMs to another host outside of the cluster.
5. Edit the cluster settings and enable EVC.
6. Select the CPU vendor and feature set appropriate for the hosts in the cluster.
7. 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.

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

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:
   ```
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 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**.

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.

1. Log in to VMware vCSA management interface: https://<vcenter_FQDN>:5480 as **root**.
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_FQDN_or_IP_address> -u administrator`
5. Repeat steps 3 and 4 to delete the remaining external VMware PSCs.

Manage VMware vSphere ESXi

Install the latest VMware vSphere ESXi patch (VMware vSphere 6.x)

Install the latest supported VMware vSphere ESXi patch.

**About this task**

After the latest patch is installed, when a VMware vSphere ESXi host is updated to a newer build, the host no longer shares the same build.
Use the VMware vCenter 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.

The VMware vSphere ESXi image file can be reused multiple times in workflows. If the version of the VMware vSphere ESXi image file changes, the image file must be uploaded again in the VxBlock Central Orchestration Services user interface.

**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. Upgrade third-party software before 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. See 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)**.
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 that is applied.
8. Reboot the VMware vSphere ESXi host.

**Configure advanced settings for VMware vSphere ESXi (VMware vSphere 6.x)**

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 or CLI.

The following table describes the advanced settings that are available:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<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**

- For CLI - Obtain the IP address and local root user credentials for the VMware vSphere ESXi host.
- For VMware Host Client - Obtain the IP address and root user credentials for the vSphere ESXi host.
VMware vSphere Web Client

1. Log in to the VMware Host Client using a 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.

Procedure – ESXCLI

1. Log in to each host using SSH or the DCUI.
2. Set Net.TcpipHeapSize to Value of 32.
   
   Example:
   ```
   esxcli system settings advanced set --int-value=32 -o /Net/TcpipHeapSize
   ```
   
   Example:
   ```
   esxcli system settings advanced set --int-value=512 -o /Net/TcpipHeapMax
   ```
4. Set NFS.MaxVolumes to Value of 256.
   
   Example:
   ```
   esxcli system settings advanced set --int-value=256 -o /NFS/MaxVolumes
   ```
5. Set NFS.HeartbeatFrequency to Value of 12
   
   Example:
   ```
   esxcli system settings advanced set --int-value=12 -o /NFS/HeartbeatFrequency
   ```
6. Set NFS.HeartbeatTimeout to Value of 5
   
   Example:
   ```
   esxcli system settings advanced set --int-value=5 -o /NFS/HeartbeatTimeout
   ```
7. Set NFS.HeartbeatDelta to Value of 5.
   
   Example:
   ```
   esxcli system settings advanced set --int-value=5 -o /NFS/HeartbeatDelta
   ```
8. Set NFS.HeartbeatMaxFailures to Value of 10
   
   Example:
   ```
   esxcli system settings advanced set --int-value=10 -o /NFS/HeartbeatMaxFailures
   ```

After you finish

Reboot the VMware vSphere ESXi host.

Restore default values for VMware vSphere ESXi advanced settings (VMware vSphere 6.x)

Restore the advanced settings for VMware vSphere ESXi to their default values.

Procedure

1. In the VMware Host Client, select Manage.
2. Click Advanced Settings under the System tab.
3. Search for the appropriate parameters.
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.

Harden security on VMware vSphere ESXi hosts (VMware vSphere 6.x)
The VMware vSphere client is used to access each VMware vSphere ESXi host.

Procedure
1. Under Advanced Settings, review the settings that have been modified.

Increase 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, see the VMware Knowledge Base entry 1014.

Procedure
1. Using the Microsoft regedit application, go 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 datatype to REG_DWORD.
5. For the data value, type 190 (decimal).
6. Reboot the VM.

Install VxBlock vCenter Server root certificates on web browser (VMware vSphere 6.x)
Install the trusted root certificate authority certificates.

About this task
This procedure is applicable for Internet Explorer only. For any browser other than Internet Explorer, see the documentation for that browser.

Procedure
1. Open Internet Explorer and type the URL https://<vcsa_fqdn>.
2. Select Download trusted root CA certificates and save the file locally.
3. Unzip the downloaded file.
4. Right-click on each .crt file, click Open and Install Certificate.
5. Select Local Machine > Next > Next > Finish.

Note: For more information, see VMware Knowledge Base article 2108294.
Set up Java and Internet Explorer on the management workstation or VM (VMware vSphere 6.x)

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

**Before you begin**

- Ensure Java version 8 Update 131 or later is installed on the management workstation or VM.
- Ensure that the Java security level complies with your corporate security policy.

**Procedure**

1. Using administrative privileges, log in to Microsoft Windows on the management workstation or VM.
2. Go to **Java Windows Control**.
3. Select the **Security** tab.
4. Set the security level to the lowest setting (least secure).
5. Click **Edit Site List...**
6. Add the URLs of web-based applications. For example: `https://<ip_address_of_web_based_application>`
7. Click **OK**.
8. Click **OK**.

Manage VMware vCenter SSO (VMware vSphere 6.x)

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 may have to modify policies or accounts if regulations require different policies or if you are troubleshooting a problem.

Unlock and reset the VMware vCenter SSO administrator password (VMware vSphere 6.x)

Unlock and reset the VMware vCenter SSO administrator account.

**About this task**

For security purposes, the VMware vCenter administrator account is locked after three failed login attempts. Follow the instructions outlined in VMware Knowledge Base Article 2146224 to unlock and reset a password.

Manage the lockout status of VMware vCenter SSO (VMware vSphere 6.x)

View the lockout status of a VMware vCenter SSO account for VMware vSphere.

**Procedure**

1. Log in as an SSO administrator to the VMware vCenter Client (HTML5) for VMware vSphere 6.7 or the VMware vSphere Web Client for VMware vSphere 6.5. By default, the user is `administrator@vsphere.local`.
2. From the home page, select **Administration > Single Sign-On > Users and Groups**.
3. Each tab shows information from the identity sources about configured accounts that are on the system. Select the **Users** tab.
4. For VMware vSphere 6.7, select the `vSphere.local` domain.

5. The `Locked` or `Disabled` columns show the status of each configured SSO account. Depending on which version of VMware vSphere you are running, perform one of the following:
   - VMware vSphere 6.7: Click the ellipsis vertical bar to `Enable/Disable` or `Unlock`.
   - VMware vSphere 6.5: Right-click the appropriate account and select `Enable/Disable` or `Unlock`.

6. Click `Yes` to confirm.

**Manage VMware vCenter SSO default password policies (VMware vSphere 6.x)**

Modify the strict lockout policy of VMware vCenter SSO for VMware vSphere 6.x.

**Procedure**

1. Log in as an SSO administrator to the VMware vCenter Client (HTML5) for VMware vSphere 6.7 or the VMware vSphere Web Client for VMware vSphere 6.5. By default, this user is `administrator@vsphere.local`.

2. From the home page, select `Administration > Single Sign-On > Configuration`.

3. Select the `Policies` tab and then select `Lockout Policy` to view the current lockout policies.

4. To modify the lockout policy, select `Edit`.

5. Make the required changes and click `OK`.

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

Associate a Windows AD to the VMware SSO service in embedded VMware Platform Service Controller (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.

**Embedded deployments**

1. Log in to the VMware vSphere Client (HTML5) on the element manager VM as `administrator@vsphere.local` account at: `https://<VCENTER_FQDN OR IP>/ui/

2. Go to `Menu > Administration`.


4. For embedded PSC deployment, select `vCenter server with Embedded PSC` and click `Join AD`.

5. Type 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 as `administrator@vsphere.local` account at: `https://<VCENTER_FQDN OR IP>/ui/`

2. Go to `Menu > Administration`.


4. Perform the following for each VMware PSC:
   - Select the PSC to join to the AD domain and click `JOIN AD`.
   - Leave `Organizational unit` blank and click `OK`. 

• Log in to https://<psc_fqdn>:5480/ as root.
• Restart the appliance.

5. Select the Identity Sources tab and click ADD IDENTITY SOURCE to type details for the AD domain.

6. Select the AD (Integrated Windows Authentication) under Identity source type.

7. Verify that the domain name that was previously registered to the VMware PSC is assigned to this AD domain registration.

8. Select Use machine account > OK.

9. Select the added AD domain, and click SET AS DEFAULT.

Log in to VMware vCenter Server through the VMware vSphere Client (HTML5) as the administrator@vsphere.local and 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.

Add a Windows AD identity source to VMware vCenter SSO (VMware vSphere 6.5)

Associate Windows AD to the VMware vCenter SSO service for VMware vSphere on the VMware PSCs.

About this task

Obtain network access to the VMware vCenter Web Client and AD domain admin privileges.

Procedure

1. Log in to the VMware vSphere Web Client on the Element Manager VM.

   Use the administrator@vsphere.local account and the following URL:

   https://<VCENTER_FQDN OR IP>:9443/vsphere-client/

2. Select Administration > Deployment > System Configuration > Nodes.

3. Select hostname for PSC 2, select the Manage tab and click Settings.

4. Under Advanced, select AD, and click Join....

5. Type the AD domain, username, and password (with appropriate AD domain administrative rights). Leave Organizational unit blank, and click OK.

6. Reboot the PSC Node under the Actions menu.

7. Repeat Steps 2-5 but select the hostname for PSC 1.

8. Reboot the PSC Node under the Actions menu.

   Note: Rebooting the (primary) PSC Node 1 affects the following:

   • All running tasks on the node are cancelled or interrupted.
   • All users currently accessing this node temporarily lose connectivity.
   • If this node is a VMware vCenter Server, features such as DRS and vMotion will temporarily become unavailable.
   • If this node is a PSC, services such as SSO, licensing and certificate, running on this node will temporarily go down.


10. Select the Identity Sources tab, and then click the green + icon to type the details for the AD domain.
11. Select **AD** (Integrated Windows Authentication) under **Identity source type**.

12. Verify that the domain name that was previously registered to the PSC is assigned to this AD domain registration.

13. Select **Use machine account** and click **Next**.

14. The AD registration is complete. While logged in to VMware vCenter through the Web Client or VMware vSphere Client as the administrator@vsphere.local user, assign Administrator roles/permissions for domain user accounts or groups that require access to VMware vCenter. By default, only the administrator@vsphere.local account can access VMware vCenter until more permissions are explicitly assigned to domain users.

### Back up or restore the external VMware Platform Service Controller (VMware vSphere 6.x)

Back up or restore the VMware Platform Service Controller (PSC) for VMware vSphere 6.x.

**About this task**

To back up or restore the external VMware PSC configuration, see *Application-specific scripted backups* in the AMP product guide.

### Restore and back up VMware vCenter Server Appliance (VMware vSphere 6.x)

Back up or restore the VMware vCenter Server Appliance (vCSA) for VMware vSphere using a file-based backup.

**About this task**

Maintaining a backup of the VMware Platform Service Controller (PSC) configuration ensures continued VMware vSphere access for VMware vCenter Server components.

For information about backing up or restoring the VMware external PSC configuration, see *Application-specific scripted backups* in the AMP product guide.

For AMP-3S, see the following VMware documents for guidelines:

- File-Based Backup and Restore of vCenter Server Appliance
- Image-Based Backup and Restore of a vCenter Server Environment

### Redirect VMware vCenter Server to the secondary external VMware Platform Services controller (VMware vSphere 6.x)

If the primary external VMware Platform Services Controller (PSC) fails and there are multiple VMware PSCs that are replicating without fault tolerance configured, repoint the VMware vCenter Server for authentication.

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

For more information, see the VMware Platform Services Controller FAQ.

### Manage VMware VDS (VMware vSphere 6.x)

The VMware vSphere Distributed Switch (VDS) is an enterprise feature of VMware vSphere vCenter Server. VMware VDS requires the VMware vSphere ESXi hosts are licensed with the VMware vSphere Enterprise Plus edition. A non-Enterprise Plus edition does 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.x)

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.

Modify an existing distributed port group (VMware vSphere 6.7)

From the VMware vCenter Client (HTML5), modify distributed port group settings such as the name, VLAN ID, teaming and failover policy, traffic filtering and marking policies. Standard configuration settings must not be changed to ensure proper operation.

About this task

Using the VMware vCenter Client (HTML5), 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 used is DVSwitch01-A.

Procedure

1. To launch the VMware vCenter Client (HTML5), open a browser and type the following URL: https://<VCENTER_FQDN OR IP>/ui/.
2. Log in to the VMware vCenter Client (HTML5) with the administrator@vsphere.local user account (Single Sign-On (SSO) account) or other administrative account with appropriate permissions.
3. On the VMware vCenter Client (HTML5) Home tab, click Networking.
4. Expand the distributed switch containing the distributed port group for example, DVSwitch01-A, 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>General</td>
<td>• Name: the name chosen for the distributed port group</td>
</tr>
<tr>
<td></td>
<td>• Port binding: Static Binding</td>
</tr>
<tr>
<td></td>
<td>• Port allocation: Elastic</td>
</tr>
<tr>
<td></td>
<td>• Number of ports: 8 (increases automatically as long as Elastic is selected for port allocation)</td>
</tr>
<tr>
<td></td>
<td>• Network resource pool: use default setting</td>
</tr>
<tr>
<td></td>
<td>• Description: Add details about distributed port groups</td>
</tr>
<tr>
<td>Advanced</td>
<td>• Configure reset at disconnect: Enabled</td>
</tr>
<tr>
<td></td>
<td>• Override port policies: use default setting</td>
</tr>
<tr>
<td>Security</td>
<td>• Promiscuous mode: Reject</td>
</tr>
<tr>
<td></td>
<td>• MAC address changes: Reject</td>
</tr>
<tr>
<td></td>
<td>• Forged transmit: Reject</td>
</tr>
<tr>
<td>Traffic shaping</td>
<td>• Ingress traffic shaping: Disabled</td>
</tr>
<tr>
<td></td>
<td>• Egress traffic shaping: Disabled</td>
</tr>
<tr>
<td>Edit option</td>
<td>Field: recommended setting</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| VLAN                 | • **VLAN type:** VLAN  
 • **VLAN ID:** See the *Logical Configuration Survey*                                                                                               |
| Teaming and failover | • **Load balancing:** Route based on originating virtual port. The vMotion port group has only one active uplink (associated with vNIC2 fabric A) and is set to use explicit failover order. The other uplink should be in standby mode.  
 • **Network failure detection:** Link status only  
 • **Notify switches:** Yes  
 • **Failback:** Yes                                                                                                           |
| Monitoring           | **Netflow:** Disabled (default)                                                                                                                                |
| Miscellaneous        | **Block all ports:** No                                                                                                                                          |

6. Edit the Traffic filtering and Marking using the following steps.
   a. Select the port group and navigate to the **Configure** tab.
   b. Under **Settings**, select **Traffic Filtering and Marking**.
   c. Click **ENABLE AND REORDER**.
   d. In the **Enable and Reorder Traffic Rules** window, turn on **Enable all traffic rules**.
   e. Click **OK**.
   f. Click the **+Add** button to add traffic rules.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Field: recommended setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic filtering and marking</td>
<td>- Status: Enable this option for Management, vMotion, and NFS distributed port groups. All other port groups should be disabled</td>
</tr>
<tr>
<td></td>
<td>- Name: Management Traffic Rule</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 6</td>
</tr>
<tr>
<td></td>
<td>- DSCP value checkbox is selected</td>
</tr>
<tr>
<td></td>
<td>- Set DSCP to 48</td>
</tr>
<tr>
<td></td>
<td>- Set traffic direction to Ingress.</td>
</tr>
<tr>
<td></td>
<td>- Note: See the <em>VMware vSphere Release Notes</em> for information about ingress and egress parameters.</td>
</tr>
<tr>
<td></td>
<td>- Traffic qualifier: System Traffic</td>
</tr>
<tr>
<td></td>
<td>- Enable Qualifier: Enabled</td>
</tr>
<tr>
<td></td>
<td>- System Traffic: Management</td>
</tr>
<tr>
<td></td>
<td>- Name: NFS Traffic Rule</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>- DSCP value checkbox is selected</td>
</tr>
<tr>
<td></td>
<td>- Set DSCP to 16</td>
</tr>
<tr>
<td></td>
<td>- Set traffic direction to Ingress.</td>
</tr>
<tr>
<td></td>
<td>- Note: See the <em>VMware vSphere Release Notes</em> for information about ingress and egress parameters.</td>
</tr>
<tr>
<td></td>
<td>- Traffic qualifier: IP</td>
</tr>
<tr>
<td></td>
<td>- Enable Qualifier: Enabled</td>
</tr>
<tr>
<td></td>
<td>- Protocol number: Any</td>
</tr>
<tr>
<td></td>
<td>- Name: vMotion Traffic Rule</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>- DSCP value checkbox is selected</td>
</tr>
<tr>
<td></td>
<td>- Set DSCP to 26</td>
</tr>
<tr>
<td></td>
<td>- Set traffic direction to Ingress.</td>
</tr>
<tr>
<td></td>
<td>- Note: See the <em>VMware vSphere Release Notes</em> for information about ingress and egress parameters.</td>
</tr>
<tr>
<td></td>
<td>- Traffic qualifier: System Traffic</td>
</tr>
<tr>
<td></td>
<td>- Enable Qualifier: Enabled</td>
</tr>
<tr>
<td></td>
<td>- System Traffic: vMotion</td>
</tr>
</tbody>
</table>
Create a distributed port group (VMware vSphere 6.7)

Use the VMware vSphere Client (HTML5) to create and add virtual and VMKernel distributed port groups to an existing VMware VDS.

About this task

After you create a distributed port group, you must configure the port group.

Procedure

1. To launch the VMware vSphere Client (HTML5), open a browser and type the following URL: https://<VCENTER_FQDN OR IP>/ui/.
2. Log in to the VMware vSphere Client (HTML5) with the administrator@vsphere.local VMware SSO user account or other administrative account with appropriate permissions.
4. Right-click DVSwitch01-A and select New Distribution Port Group.
5. From the New Distributed Port Group wizard, to create the distributed port group, perform the following:
   a. Type the name of the distributed port group and click Next.
   b. Leave Port binding and Port allocation to the default settings Static binding and Elastic.
   c. Leave the Number of Ports to the default setting of eight.
   d. Set the VLAN type to VLAN and change the VLAN ID.
   e. Enable Customize default policies configuration.
   f. Leave Security to the default.
   g. Leave Traffic shaping to the default.
   h. In the Teaming and failover section, use the settings from the following table for load balancing and uplinks as a guide:

<table>
<thead>
<tr>
<th>Port Group</th>
<th>Active uplinks</th>
<th>Standby uplinks</th>
<th>Unused uplinks</th>
<th>Load Balancing</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcesys_esx_mgmt</td>
<td>Uplink1</td>
<td>Uplink2</td>
<td>N/A</td>
<td>Originating virtual port</td>
</tr>
<tr>
<td></td>
<td>Uplink3</td>
<td>Uplink4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vcesys_esx_vmotion</td>
<td>Uplink1</td>
<td>Uplink2</td>
<td>N/A</td>
<td>Explicit Failover</td>
</tr>
<tr>
<td></td>
<td>Uplink3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vcesys_esx_ft</td>
<td>Uplink2</td>
<td>Uplink1</td>
<td>N/A</td>
<td>Originating virtual port</td>
</tr>
<tr>
<td></td>
<td>Uplink4</td>
<td>Uplink3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vcesys_esx_nfs</td>
<td>Uplink1</td>
<td>Uplink2</td>
<td>N/A</td>
<td>Originating virtual port</td>
</tr>
<tr>
<td></td>
<td>Uplink3</td>
<td>Uplink4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Port Group | Active uplinks | Standby uplinks | Unused uplinks | Load Balancing
---|---|---|---|---
customer data | Uplink1, Uplink2, Uplink3, Uplink4 | N/A | N/A | Originating virtual port

i. Leave Monitoring to the default.

j. Leave Miscellaneous to the default.

k. Do not edit any other settings.

l. Click NEXT to view the Ready to complete dialog.

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.

**Add a new VMKernel interface (VMware vSphere 6.7)**

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

**Before you begin**

Create a VMKernel distributed port group.

**Procedure**

1. From the VMware vSphere Client (HTML5) Home tab, click Hosts and Clusters.
2. Select the ESXi host and click the Configure tab.
4. In the VMkernel adapters pane, click Add host networking.
   a. Select the VMkernel Network Adapter connection type and click Next.
   b. Under Select an existing network, click Browse.
   c. Select the port group to be changed, click OK, and click Next.
   d. Select the desired TCP/IP stack from the menu and click Next.
      * For vMotion, choose vMotion TCP/IP stack
      * For NFS, choose Default TCP/IP stack
      * For FT, ensure that Default TCP/IP, Fault Tolerance Logging service is enabled.
   e. Choose IPv4 or IPv6 for IP Settings, type the IPv4 or IPv6 address and subnet mask, and click Next. Dual IP stack is not supported.
   f. At Ready to Complete, verify the settings and click Finish.
Associate VMware vSphere ESXi hosts to an existing VMware VDS (VMware vSphere 6.7)

Associating a new VMware vSphere ESXi host to an existing VMware VDS requires the addition of 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 to associate with the VMware vSphere ESXi host.

**Procedure**

1. To launch the VMware vSphere Client (HTML5), open a browser and enter the following URL: https://<VCENTER_FQDN OR IP>/ui/
2. Log in to the VMware vSphere HTML5 Client (HTML5) with the administrator@vsphere.local user account (SSO account) or other administrative account with appropriate permissions.
3. On the VMware vSphere Client (HTML5) Home tab, click Networking.
4. Right-click DVSwitch01-A and select Add and Manage Hosts.
5. From the Add Hosts wizard, perform the following:
   a. Select Add Hosts and click Next.
   b. Select New Hosts.
   c. In the Select new hosts window, select the VMware vSphere ESXi host to be added and click OK.
      You can modify multiple VMware vSphere ESXi hosts at a time using the Add and Manage Hosts wizard.
   d. Verify that the selected host appears in the list and click Next.
   e. In the Manage physical adapters page.
      a. Select Uplink 2 for vmnic1 and click OK.
      b. Select Uplink 3 for vmnic2 and click OK.
      c. Select Uplink 4 for vmnic3 and click OK
      Disjoint Layer 2 configurations use vmnic4/5 respectively.
   f. Click Next for Manage VMkernel Adapters and Migrate VM networking page.
6. Review the Summary results and click Finish.
   After adding the host to the VDS, the Management VMKernel port and vmnic0 must be migrated to Uplink1 on the VDS.

Configure jumbo frames on VMware VDS components (VMware vSphere 6.7)

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://<VCENTER_FQDN OR IP>/ui/
2. Log in to the VMware vSphere Client (HTML5) 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 Client (HTML5) Home tab, 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.
Modify CoS settings (VMware vSphere 6.7)

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 Client (HTML5) from browser by typing the following URL:
   
   ```
   https://<VCENTER_FQDN OR IP>/ui/
   ```

2. Log in to the VMware vSphere Client (HTML5) with the administrator@vsphere.local user account (VMware SSO account) or other administrative account with appropriate permissions.


4. Expand the DVswitch01-A to view all port groups.

5. Select vcesys_esx_mgmt distributed port group and select the Configure tab.


7. Click the ENABLE AND REORDER button.

8. In the Enable and Reorder Traffic Rules window, turn on Enable all traffic rules. Click OK.

9. Click the +ADD button to add traffic rules.

10. In the New Traffic Rule wizard, and perform the following:
   a. For the Name, type: MgmtCOS.
   b. For Action, select Tag.
   c. Enable Update CoS tag and change value to 6.
   d. Enable Update DSCP tag and change value to 48.
   e. Change the Traffic direction to Ingress.
   
   The VMware vSphere Release Notes contain information about ingress and egress parameters.

   f. Select System Traffic under Traffic Qualifiers and enable Enable Qualifier.
   g. Set System traffic to Management.
   h. Click OK.

11. Select vcesys_esx_vmotion distributed port group and click the Configure tab.


13. Click the +ADD button to add traffic rules.

14. In the Network Traffic Rule wizard, perform the following:
   a. For the Name, type: vMotionCOS.
   b. For Action, select Tag.
   c. Enable Update CoS tag and change the value to 4.
   d. Enable Update DSCP tag and change value to 26.
   e. Change the Traffic direction to Ingress.
   
   The VMware vSphere Release Notes contain information about ingress and egress parameters.

   f. Select System Traffic under Traffic Qualifiers and enable Enable Qualifier.
g. Set System traffic to vMotion.

h. Click OK.

15. Select vcesys_esx_nfs distributed port group and click the Configure tab.

16. In the Network Traffic Rule wizard, perform the following:
   
a. For the Name, type: NFSCOS
   
b. For Action, select Tag.
   
c. Enable Update CoS tag and change value to 2.
   
d. Enable Update DSCP tag and change value to 16.
   
e. Change the Traffic direction to Ingress.
      
The VMware vSphere Release Notes contain information about ingress and egress parameters.
   
f. Select IP under Traffic Qualifiers and enable Enable qualifier.
   
g. From the Protocol number menu, select Any.
   
h. Click OK.

Modify 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. Do not change standard configuration settings to ensure proper operation.

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.

2. Log in 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 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>General</td>
<td></td>
</tr>
<tr>
<td></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>• Number of ports: 8 (increases automatically if Elastic is selected for port allocation)</td>
</tr>
<tr>
<td></td>
<td>• Network resource pool: use default setting</td>
</tr>
<tr>
<td></td>
<td>• Description: Add details about distributed port groups.</td>
</tr>
<tr>
<td>Advanced</td>
<td>• Configure reset at disconnect: Enabled</td>
</tr>
<tr>
<td></td>
<td>• Override port policies: use default setting</td>
</tr>
<tr>
<td>Security</td>
<td>• Promiscuous mode: Reject</td>
</tr>
<tr>
<td></td>
<td>• MAC address changes: Reject</td>
</tr>
<tr>
<td></td>
<td>• Forged transmit: Reject</td>
</tr>
<tr>
<td>Traffic shaping</td>
<td>• Ingress traffic shaping: Disabled</td>
</tr>
<tr>
<td></td>
<td>• Egress traffic shaping: Disabled</td>
</tr>
<tr>
<td>VLAN</td>
<td>• VLAN type: VLAN</td>
</tr>
<tr>
<td></td>
<td>• VLAN ID: Refer to the Logical Configuration Survey.</td>
</tr>
<tr>
<td>Teaming and failover</td>
<td>• Load balancing: Route based on originating virtual port. The vMotion port group only has one active uplink (associated with vNIC2 fabric A) and is set to use explicit failover order. The other uplink should be in standby mode.</td>
</tr>
<tr>
<td></td>
<td>• Network failure detection: Link status only</td>
</tr>
<tr>
<td></td>
<td>• Notify switches: Yes</td>
</tr>
<tr>
<td></td>
<td>• Failback: Yes</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Netflow: default</td>
</tr>
</tbody>
</table>
### Traffic filtering and marking

<table>
<thead>
<tr>
<th>Edit option</th>
<th>Field: recommended setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status:</strong> enable this option for Management, vMotion, and NFS distributed port groups. All other port groups should be disabled.</td>
<td></td>
</tr>
<tr>
<td><strong>Management Traffic Rule Enabled</strong> - use the + sign to make edits</td>
<td></td>
</tr>
<tr>
<td>• Action tag</td>
<td></td>
</tr>
<tr>
<td>• COS value checkbox is selected.</td>
<td></td>
</tr>
<tr>
<td>• Set CoS to 6</td>
<td></td>
</tr>
<tr>
<td>• DSCP value checkbox is selected.</td>
<td></td>
</tr>
<tr>
<td>• Set DSCP to 48</td>
<td></td>
</tr>
<tr>
<td>• Set traffic direction to Ingress.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> See the VMware vSphere Release Notes for information about ingress and egress parameters.</td>
<td></td>
</tr>
<tr>
<td>• Type System Traffic and set Protocol/Traffic Type to Management</td>
<td></td>
</tr>
<tr>
<td><strong>vMotion Traffic Rule Enabled</strong> - use the + sign to make edits</td>
<td></td>
</tr>
<tr>
<td>• Action tag</td>
<td></td>
</tr>
<tr>
<td>• COS value checkbox is selected.</td>
<td></td>
</tr>
<tr>
<td>• Set CoS to 4</td>
<td></td>
</tr>
<tr>
<td>• DSCP value checkbox is selected.</td>
<td></td>
</tr>
<tr>
<td>• Set DSCP to 26</td>
<td></td>
</tr>
<tr>
<td>• Set traffic direction to Ingress.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> See the VMware vSphere Release Notes for information about ingress and egress parameters.</td>
<td></td>
</tr>
<tr>
<td>• Type System Traffic and set Protocol/Traffic Type to vMotion.</td>
<td></td>
</tr>
<tr>
<td><strong>NFS Traffic Rule Enabled</strong> - use the + sign to make edits</td>
<td></td>
</tr>
<tr>
<td>• Action tag</td>
<td></td>
</tr>
<tr>
<td>• COS value checkbox is selected.</td>
<td></td>
</tr>
<tr>
<td>• Set CoS to 2</td>
<td></td>
</tr>
<tr>
<td>• DSCP value checkbox is selected.</td>
<td></td>
</tr>
<tr>
<td>• Set DSCP to 16</td>
<td></td>
</tr>
<tr>
<td>• Set traffic direction to Ingress.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> See the VMware vSphere Release Notes for information about ingress and egress parameters.</td>
<td></td>
</tr>
<tr>
<td>• Type IP and set Protocol/Traffic Type to Any.</td>
<td></td>
</tr>
</tbody>
</table>

### Miscellaneous

<table>
<thead>
<tr>
<th>Field</th>
<th>recommended setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Block all ports:</strong></td>
<td>No</td>
</tr>
</tbody>
</table>
Create a distributed port group (VMware vSphere 6.5)

Use the VMware vSphere Web Client to create and add virtual and VMKernel distributed port groups to an existing VMware VDS.

About this task

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.
2. Log in 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 Home tab, under Inventories, click Networking.
4. Right-click DVSwitch01-A and select New Distribution Port Group.
5. From the New Distributed Port Group wizard, to create the distributed port group, perform the following:
   a. Type the name of the distributed port group and click Next.
   b. Leave Port binding and Port allocation to the default settings Static binding and Elastic.
   c. Leave the Number of Ports to the default setting of eight.
   d. Set the VLAN type to VLAN and change the VLAN ID.
   e. Enable Customize default policies configuration.
   f. Leave Security to the default.
   g. Leave Traffic shaping to the default.
   h. In the Teaming and failover section, use the settings from the chart below for load balancing and uplinks as a guide. Uplink1 and Uplink2 are only used for Management and FT traffic.

<table>
<thead>
<tr>
<th>Port Group</th>
<th>Active uplinks</th>
<th>Standby uplinks</th>
<th>Unused uplinks</th>
<th>Load Balancing</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcesys_esx_vmotion</td>
<td>Uplink3</td>
<td>Uplink4</td>
<td>Uplink1, Uplink 2</td>
<td>Explicit Failover</td>
</tr>
<tr>
<td>vcesys_esx_nfs</td>
<td>Uplink3, Uplink 4</td>
<td>N/A</td>
<td>Uplink1, Uplink 2</td>
<td>Originating virtual port</td>
</tr>
<tr>
<td>customer data</td>
<td>Uplink3, Uplink 4</td>
<td>N/A</td>
<td>Uplink1, Uplink 2</td>
<td>Originating virtual port</td>
</tr>
</tbody>
</table>

   i. Leave Monitoring to the default.
   j. Leave Miscellaneous to the default.
   k. Do not edit additional settings.
   l. Click NEXT to view the Ready to complete dialog.

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 (Management, vMotion, NFS, or FT) interface using the Add and Manage Host wizard.

**Before you begin**

Create a VMkernel distributed port group.

**Procedure**

1. From the VMware vSphere Web Client Home tab, under Inventories, select Networking.
2. Right-click DVSswitch01-A and select Add and Manage Hosts.
3. From the Add and Manage Hosts wizard, perform the following:
   a. Select Manage host networking and click Next.
   b. Select Attached 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 network is enabled and click Browse.
   i. Select VMKernel (Management, vMotion, NFS, or FT) distributed port group and click OK.
   j. Click Next.
   k. For the vMotion distributed port group only, select TCP/IP stack vMotion and click Next.
   l. For the NFS distributed port group only, verify that Enable services is unchecked and click Next.
   m. For the FT distributed port group only, select Fault Tolerance Logging and click Next.
   n. Select Use static IPv4/IPv6 Settings, type the IPv4/IPv6 address and subnet mask, and click Next.
      
      (Note: Dual IP stack is not supported.)
   o. When the Analyze impact window appears, click Next.
   p. From the Ready to complete window, validate the settings and click Finish.
   q. Select the new VMKernel.
   r. Select Edit adapter.
   s. Select NIC settings.
   t. Verify that the MTU setting is set to 9000. (Only Management uses MTU 1500)
   u. Click OK and Finish.
   v. Repeat steps g through s for each additional VMware vSphere ESXi host to create a new network adapter.
   w. Click Next.
   x. Verify that the No Impact message appears and click Next.
   y. Review and verify the Summary results and click Finish.
Associate VMware vSphere ESXi hosts to an existing VMware VDS

Associating a new VMware vSphere ESXi host to an existing VMware VDS requires the addition of 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 to associate with the VMware vSphere ESXi host.

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
2. Log in 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 Home tab, under Inventories, click Networking.
4. Right-click DVSwitch01-A and select Add and Manage Hosts.
5. From the Add and Manage Hosts wizard, perform the following:
   a. Select Add Hosts and click Next.
   b. Select New Hosts.
   c. From the Select new hosts window, select the VMware vSphere ESXi host to be added and click OK.
      
      Note: You can modify multiple VMware vSphere ESXi hosts at a time using the Add and Manage Hosts wizard.

   d. Validate the selected host appears in the list and click Next.
   e. From the Select network adapter tasks window, deselect Manage VMKernel adapters.
   f. Verify that Manage physical adapters is selected and click Next.
   g. Select Uplink 2 for vmnic1 and click OK.
   h. Select Uplink 3 for vmnic2 and click OK.
   i. Select Uplink 4 for vmnic3 and click OK.
      
      Note: Disjoint Layer 2 configurations use vmnic4/5 respectively.
   j. Click Next.
   k. Verify that the status message displays no impact and click Next.
6. Review the Summary results and click Finish.

   Note: After adding the host to the VDS, the Management VMKernel port and vmnic0 need to be migrated to Uplink1 on the VDS.

Configure jumbo frames on VMware VDS

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
2. Log in 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 **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**.

**Modify 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`
2. Log in 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 **Home** tab, under **Inventories**, click **Networking**.
4. Expand the DVswitch01-A to view all port groups.
5. Right-click **vcesys_esx_mgmt** distributed port group and click **Edit settings**.
6. Select **Traffic filtering and marking**.
7. From the Status drop-down box, select **Enable**.
8. Select the green plus (+) icon to open the New Network Traffic Rule wizard, and perform the following:
   a. For the Name, type: `MgmtCOS`.
   b. For Action, select **Tag**.
   c. Check Update CoS tag and change value to 6.
   d. Check Update DSCP tag and change value to 48.
   e. Change the Traffic direction to **Ingress**.
      The VMware vSphere Release Notes contain information about ingress and egress parameters.
   f. Select the green plus (+) and select **New System Traffic Qualifier**.
   g. Verify that the type is set System traffic and the Protocol/Traffic type is set to **Management**.
   h. Click **OK**.
9. Right-click **vcesys_esx_vmotion** distributed port group and click **Edit settings**.
10. Select **Traffic filtering and marking**.
11. From the Status drop-down box, select **Enable**.
12. Select the green plus (+) icon to open the New Network Traffic Rule wizard, and perform the following:
   a. For the Name, type: `vMotionCOS`.
   b. For Action, select **Tag**.
   c. Check Update CoS tag and change value to 4.
   d. Check Update DSCP tag and change value to 26.
   e. Change the Traffic direction to **Ingress**.
      The VMware vSphere Release Notes contain information about ingress and egress parameters.
f. Select the green plus (+) and select **New System Traffic Qualifier**.
g. Verify that the type is set to **System traffic** and the Protocol/Traffic type is set to **vMotion**.
h. Click **OK**.

13. Right-click the `vcesys_esx_nfs` distributed port group, click **Edit settings**.

14. 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. Check Update DSCP tag and change value to 16.
   e. Change the Traffic direction to **Ingress**.
      The VMware vSphere Release Notes contain information about ingress and egress parameters.
   f. Select the green plus (+) and select **New IP Qualifier**.
   g. From the Protocol drop-down, select **Any**.
   h. Leave the Type as IP and click **OK**.

**Decommission VMware VDS components (VMware vSphere 6.x)**

To decommission VMware VDS components, you must perform tasks on the port groups and hosts prior to removing the VMware VDS.

The following actions are required to decommission VMware VDS components:
- Delete distributed port groups
- Dissociate VMware vSphere ESXi hosts
- Remove VMware VDS

**Delete a distributed port group (VMware vSphere 6.x)**

Reassign all VMs for the distributed port group to a different distributed port group.

Before you delete the port group, ensure that there are no VMs or network adapter numbers assigned. If you delete a distributed port group with VMs and network adapter numbers assigned, an error is returned.

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

**Migrate VM distributed port group assignments to a different switch (VMware vSphere 6.x)**

This procedure is required if there are VMs on the distributed port group.

**About this task**

Use the VM migration wizard to migrate port group types.

⚠️ **CAUTION** Use caution when migrating the VMware vCenter Server VMs. A disconnection may cause the loss of the VMware vCenter Server, which could prevent the VM port group from migrating.

Use the VM migration wizard to migrate seamlessly as described in the following table:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSphere Standard Switch</td>
<td>VMware vSphere Distributed Switch</td>
</tr>
<tr>
<td>VMware vSphere Distributed Switch</td>
<td>VMware vSphere Standard Switch</td>
</tr>
</tbody>
</table>
Before you begin

VMware vSphere ESXi hosts attached to an existing VMware vSphere Distributed Switch (VDS) contain VMs that are powered on. Verify that these VMs are not assigned to any distributed port groups on the new VMware VDS.

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

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 VMware vSphere 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 VMware VDS for VM traffic to continue to communicate.
- Create the VM port group with correct VLAN ID to the new standard switch.

Procedure

1. For VMware vSphere 6.7, open a browser and type the following URL: `https://<VCENTER_FQDN_OR_IP_address>/ui/`
   For VMware vSphere 6.5, open a browser and type the following URL: `https://<vCenterIP>:9443/vsphere-client`
2. Log in to the VMware vSphere Client (HTML5 for VMware vSphere 6.7) with the administrator@vsphere.local user account (VMware SSO account) or other administrative account with appropriate permissions.
3. On the VMware vSphere Client (HTML5), select the Home tab, click Networking. For VMware vSphere 6.5, select the Home tab, and click Inventories > Networking.
4. Right-click DVswitch01-A and select Migrate VM to Another Network.
5. From the Migrate VMs to another Network wizard, perform the following:
   a. Verify that Source network is selected and click Browse.
   b. Select the distributed port group or port group to reassign the VMs and click OK.
   c. Click Next.
   d. When the list of VMs is displayed, check each VM, and click Next.
   e. Verify that the source and destination networks are correct and click Finish.

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

Delete the distributed port group from the VMware VDS (VMware vSphere 6.x)

Verify that there is no port assignment that is connected to any distributed port group on any of the VMs and delete the port group from the VMware VDS.

Procedure

1. Depending on the version of VMware vSphere 6.x, perform one of the following:
   - For VMware vSphere 6.7, launch the VMware vSphere Client (HTML5) from a browser and type: `https://<VCENTER_FQDN_OR_IP>/ui/`
For VMware vSphere 6.5, launch the VMware vSphere Web Client by selecting Start Menu > All Programs > VMware > VMware vSphere Web Client or open a browser and type: https://<vCenterIP>:9443/vsphere-client

2. Log in 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 Home tab, select Inventories (Inventories only applies for HTML5 interface) and click Networking.

4. Select the arrow on DVswitch01-A to list the distributed port groups.

5. Depending on the version of VMware vSphere 6.x, perform one of the following:
   - Right-click the distributed port group, click Delete, and click YES to delete the port group.
   - Right-click the distributed port group and select All vCenter Action > Remove from Inventory and click OK.

Dissociate the VMware vSphere ESXi host (VMware vSphere 6.x)

Dissociate 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.
- You do not need to remove distributed port groups and uplink adapters.

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

Procedure

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

VMotion and evacuate all powered-on VMs from the VMware vSphere ESXi host (VMware vSphere 6.7)

Evacuate and 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 VM distributed port group assignments to a different switch section

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://<VCENTER_FQDN OR IP>/ui/
2. Log in to the VMware vSphere Client (HTML5) with the administrator@vsphere.local user account (VMware vSphere SSO account) or other administrative account with appropriate permissions.
3. On the VMware vSphere Client (HTML5) Home tab, select Hosts and Clusters.
4. From the left window, select the appropriate VMware vSphere ESXi host and select the VMs tab.
5. From the right window, click Virtual Machines. Press the CTRL key and select all of the VMs.
6. With the VMs selected, right-click and select Migrate to open the migration wizard.
7. Verify that Change compute resource only is selected and click Next.
8. Select the destination resource (cluster or VMware vSphere ESXi host) to migrate the VMs and click Next.
9. In the Select networks page, verify that the destination networks are correct, and click Next.
10. Verify that Schedule vMotion with high priority (Recommended) is selected and click Next.
11. Review the Ready to complete 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.

12. Put the host in maintenance mode to prevent DRS from vmotioning the VMs back to the host.

**Migrate VM distributed port group assignments to a different switch (VMware vSphere 6.7)**

If there are powered-on VMs on the distributed port group, migrate VM distributed port group assignments to a different VMware VDS 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://<VCENTER_FQDN OR IP>/ui/
2. Log in to the VMware vSphere Client (HTML5) with the administrator@vsphere.local user account (VMware vSphere SSO account) or other administrative account with appropriate permissions.


4. Expand DVswitch01-A and select the port group where the VMs are connected.

5. Right-click the port group and select Migrate VMs to another Network.

6. From the Migrate VMs to another Network wizard, perform the following:
   a. Verify that Source network is selected.
   b. Select Browse for the destination network.
   c. Select the distributed port group or port group to which the VMs are to be reassigned and click OK.
   d. Click Next.
   e. When the list of VMs appears, enable the checkbox on each VM, and click Next.
   f. Verify that the source and destination networks are correct and click Finish.

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

---

Migrate the VMKernel ports to a different switch (VMware vSphere 6.7)

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. Ensure that the uplink used has the appropriate VLANs before migrating.
- 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

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://<VCENTER_FQDN OR IP>/ui/

2. Log in to the VMware vSphere Client (HTML5) with the administrator@vsphere.local user account (VMware vSphere SSO account) or other administrative account with appropriate permissions.

3. On the Home tab, select Hosts and Clusters.

4. Select the ESXi host and select Configure tab.

5. Under Networking select Virtual switches.

6. Select the distributed or standard switch to which the VMKernel adapter is to be migrated.

7. Click Migrate VMKernel network adaptor to the selected switch.

8. From the Migrate VMKernel Network Adapter wizard, perform the following:
   a. Select the VMKernel corresponding to 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 Ready to complete pages contain the correct results and click Finish.

e. 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.

f. Repeat this step for each VMKernel network adapter.

### Dissociate the VMware vSphere ESXi host from a VMware VDS (VMware vSphere 6.7)

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

#### Before you begin

Verify that there are no VMs, vNIC uplinks, or 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://<VCENTER_FQDN OR IP>/ui/

2. Log in to the VMware vSphere Client (HTML5) with the administrator@vsphere.local user account (SSO account) or other administrative account with appropriate permissions.

3. On the VMware vSphere Client (HTML5) Home tab, click Networking.

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

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

a. Select Remove hosts and click Next.

b. Select Attached hosts.

c. From the Select member hosts window, select the VMware vSphere ESXi host to be deleted and click OK. To modify multiple VMware vSphere ESXi hosts at the same time, use the Add and Manage Hosts wizard.

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

e. Review the summary in the Ready to complete window and click Finish.

### Dissociate the VMware vSphere ESXi host (VMware vSphere 6.5)

Dissociate 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.
- Migrate all VMKernel ports to a different distributed switch or standard switch.
- You do not need to remove distributed port groups and uplink adapters.

The VM network adapters assigned to a distributed port group force an error when deleting the ESXi host from the VMware VDS. All the VMs assigned to the distributed port group must be reassigned to a port group on a different distributed or standard switch. The VMware VDS must have all the VMKernel ports that are migrated to a different standard switch or VMware VDS, or be removed.

#### Procedure

1. VMware vSphere 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/evacuate all powered-on VMs from the VMware vSphere ESXi host (VMware vSphere 6.5)

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 use 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 port assignments for the VMs 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 Migrate powered-on VMs distributed port group assignments to a different switch.

Before you begin

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

Procedure

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

2. Log in 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 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 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.

Migrate VM distributed port group assignments to a different switch (VMware vSphere 6.5)

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. Use caution when migrating the VMware vCenter Server VMs. 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 seamlessly as described in the following table:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSphere Standard Switch</td>
<td>VMware VDS</td>
</tr>
</tbody>
</table>
Before you begin

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

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

Create another switch with the following criteria:

- If migrating to a different VMware 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 does not apply to vSphere 6.5.

2. Log in 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 you want to reassign the VMs and click OK.

   e. Click Next.

   f. When the list of VMs opens, 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.
Migrate the VMKernel ports to a different switch (VMware vSphere 6.5)

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. Ensure that the uplink used has the appropriate VLANs before migrating.
- 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 the VMKernel port can be migrated between the two distributed switches. You cannot add a VMware vSphere ESXi host to a standard switch.

Note: If a VMNIC is not available as an uplink, delete VMKernel ports from the VMware vSphere ESXi host 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 in 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 you want to migrate the VMKernel adapter.
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 opens and then click Next.
   e. Verify Ready to complete pages for correct results and click Finish.
   f. Wait one minute 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.

Dissociate the VMware vSphere ESXi host from a VMware VDS (VMware vSphere 6.5)

Dissociate 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.

2. Log in 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 DVSswitch01-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.

Remove a VMware VDS (VMware vSphere 6.7)

Remove 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.

**Procedure**

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

Migrate VM distributed port group assignments to a different switch (VMware vSphere 6.7)

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

**About this task**

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 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 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 the correct VLAN ID to the new standard switch.

**Procedure**

1. Open a browser and type the following URL: https://<VCENTER_FQDN OR IP>/ui/
2. Log in to the VMware vSphere Client (HTML5) with the administrator@vsphere.local user account (VMware vSphere SSO account) or other administrative account with appropriate permissions.
3. On the VMware vSphere Client (HTML5) Home tab, click Networking.
4. Expand DVswitch01-A and select the port group where the VMs are connected.
5. Right-click the port group and select Migrate VMs to another Network.
6. From the Migrate VMs to another Network wizard, perform the following:
   a. Verify that Source network is selected.
   b. Select Browse for the destination network.
   c. Select the distributed port group or port group to which the VMs are to be reassigned and click OK.
   d. Click Next.
   e. When the list of VMs appears, enable the checkbox for each VM, and click Next.
   f. Verify that the source and destination networks are correct and click Finish.

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

**Remove VMKernel ports (Flex client) (VMware vSphere 6.7)**

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. Use vSphere Web Client (Flex) to perform this procedure.

This procedure requires the FLEX client, because the required functionality is not yet available in HTML5.

**Procedure**

1. Open a browser and type the following URL: https://<VCENTER_FQDN OR IP>/vsphere-client
2. Log in to the VMware vSphere Web Client with the administrator@vsphere.local user account (VMware vSphere SSO account) or another administrative account with appropriate permissions.
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 clicking 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.

Remove a VMware VDS (VMware vSphere 6.5)
Migrate VM distributed port group assignments and VMKernel ports to a different switch.

Before you begin
- You do not need to remove uplink adapters and VMware vSphere ESXi hosts 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.

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

Migrate VM distributed port group assignments to a different switch (VMware vSphere 6.5)
If there are VMs on the distributed port group, migrate VM distributed port group assignments to a different distributed or standard switch.

About this task
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. Use caution when migrating the VMware vCenter Server VMs. 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 the following switches:
- VMware vSphere Standard Switch to a VMware VDS
- VMware VDS to a VMware vSphere Standard Switch
- VMware VDS to a VMware VDS seamlessly

Before you begin
Verify that VMs on all VMware vSphere ESXi hosts that are attached to an existing VMware VDS are not assigned to any distributed port groups.
Verify that there is an available distributed port group to which to migrate the 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 the 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 does not apply to VMware vSphere 6.5.

2. Log in 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 are reassigned and click OK.
   e. Click Next.
   f. When the list of VMs open, 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.

**Remove VMKernel ports (VMware vSphere 6.5)**

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.
2. Log in 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, clear 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. 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 opens and click Next.
   k. Review the summary results and click Finish.

Use Disjoint Layer 2 configuration on VMware VDS (VMware vSphere 6.x)

Configure Disjoint Layer 2 on VMware VDS. Disjoint Layer 2 is not mandatory for VMware VDS.
To use a Disjoint Layer 2 configuration, assign the following to the VMware VDS:
- Cisco UCS vNIC 4 (10 Gb/s or more depending on VIC hardware)
- Cisco UCS vNIC 5 (10 Gb/s 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.

Create a VMware VDS for Disjoint Layer 2 configuration (VMware vSphere 6.7)

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. vSphere 6.7 supports Consistent Device Naming(CDN) and doesn’t require reboots while adding additional vNICs. Please make sure CDN is enabled in the BIOS Policy and mapped to appropriate vNIC name in Service Profile.

Procedure

1. From the VMware vSphere Client (HTML5) Home tab, select Networking.
2. Right-click Datacenter01 (the default name from the Logical Configuration Survey) and select Distributed Switch > New Distributed Switch.
   The disjoint layer 2 Cisco DVswitch naming scheme is as follows: DVswitch<Converged System ID>.
3. From the New Distributed Switch wizard, perform the following:
a. Validate that the cluster location is Datacenter01.

b. Click Next.

c. Select the appropriate distributed switch version.

d. Click Next.

e. From the Edit Settings window, change the number of uplinks to 2.

f. Leave Network I/O Control enabled.

g. Disable Create a Default port group.

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

i. 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.

   Be sure to edit settings after completion and set MTU to 9000.

After you finish

Create distributed port groups for Disjoint Layer 2 (VMware vSphere 6.7)

Create distributed port groups for Disjoint Layer 2 (VMware vSphere 6.7)
Create distributed port groups for Disjoint Layer 2 configuration.

About this task

Set the load balancing policy for all the VMKernel distributed port groups to Route based on originating virtual port. Disjoint Layer 2 traffic is commonly associated with 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 the active state and VMNIC5 in the standby state.

Procedure

1. From the VMware vSphere Client (HTML5) Home tab, select Networking.

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

3. From the New Distributed Port Group wizard, perform the following:

   a. Change the name of the distributed port group to the one provided in the Logical Configuration Survey (LCS).

   b. Click Next to configure port group settings.

   c. Under Configure Settings, leave the default values for Port binding and Port allocation.

   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. Enable Customize default policies configuration.

   g. Leave the default value for Security.

   h. Leave the default value for Traffic shaping.

   i. In the Teaming and failover section, use the settings for load balancing and uplinks as a guide from the chart below.
Port group | Active uplinks | Standby uplinks | Unused uplinks | Load balancing
--- | --- | --- | --- | ---
New port group example | Uplink1 | Uplink2 | N/A | N/A | Originating virtual port
vMotion example | Uplink1 | Uplink2 | N/A | N/A | Explicit failover

j. Leave the default value for Monitoring.
k. Leave the default value for Miscellaneous.
l. Do not edit additional settings.
m. Click Next to view the Ready to complete dialog.
n. Review the settings and click Finish if everything is correct. 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**

**Add VMware vSphere ESXi hosts to VMware VDS (VMware vSphere 6.7)**

**Add VMware vSphere ESXi hosts to VMware VDS (VMware vSphere 6.7) (Flex client)**

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

**About this task**

Use the Flex client to perform this task. No option to create a VMkernel port group is available in the HTML5 GUI in the VMware VDS Add and Manage hosts wizard.

**Procedure**

1. From the VMware vSphere Client (HTML5) Home tab, 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. Verify that the selected host appears and click Next.
   e. From the Select network adapter tasks window, verify that Manage physical adapters and Manage VMKernel adapters are enabled and click Next.
   f. Select vmnic4 and click Assign uplink.
   g. Select Uplink 1 and click OK.
   h. Select vmnic5 and click Assign uplink.
   i. Select Uplink 2 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. Click Back to edit changes.
4. Add the VMkernel distributed port groups (vMotion, NFS, FT) only if they belong to the Disjoint Layer 2 traffic. If not, 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. Enable vMotion traffic and click Next.

f. Select Use static IPv4/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. Click Back to edit changes.

i. Repeat this step to create the new port groups. Do not enable any check boxes. The MTU must be set to 9000.

j. Click Next.

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

6. Review the summary results and click Finish.

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

Create a VMware VDS for Disjoint Layer 2 configuration (VMware vSphere 6.5)

On full-width blades with more network physical ports to the onboard mLOM ports, add vNICs 4 and 5 to the service profile individually between reboots.

About this task
First install VMware vSphere ESXi with vNIC 0 to 3 because 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 beginning with VMware vSphere 5.5 without a support ticket.

Procedure

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

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

   \*Note: The Disjoint Layer 2 Cisco VMware VDS naming scheme is as follows: DVswitch<Converged System ID>

3. From the New Distributed Switch wizard, perform the following:

   a. Validate that the cluster location is Cluster01.

   b. Click Next.

   c. Select the appropriate distributed switch.

   d. Click Next.

   e. From the Edit Settings window, change the number of uplinks to 2.

   f. Leave Network I/O Control enabled.

   g. Uncheck Default port group.

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

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

4. Repeat this procedure to create a VMware VDS for each additional workload type.
After you finish

Creating distributed port groups for Disjoint Layer 2

Create distributed port groups for Disjoint Layer 2 (VMware vSphere 6.5)

Create a VMware VDS for Disjoint Layer 2 configuration.

About this task

Set the load-balancing policy for all the VMKernel distributed port groups to Route based on originating virtual port. Disjoint Layer 2 traffic is commonly associated with 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 the active state and VMNIC5 in the standby state.

Procedure

1. From the VMware vSphere Web Client Home tab, under Inventories, select Networking.
2. Right-click DVswitch01-DJL2 (Logical Configuration Survey (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 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. Check Customize default policies configuration.
   g. Leave Security to the default.
   h. Leave Traffic shaping to the default.
   i. In the Teaming and failover section, use the settings for load balancing and uplinks as a guide from the following chart:

<table>
<thead>
<tr>
<th>Port Group</th>
<th>Active uplinks</th>
<th>Standby uplinks</th>
<th>Unused uplinks</th>
<th>Load Balancing</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Port Group</td>
<td>Uplink1, Uplink2</td>
<td>N/A</td>
<td>N/A</td>
<td>Originating virtual port</td>
</tr>
<tr>
<td>Example</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vMotion Example</td>
<td>Uplink1</td>
<td>Uplink2</td>
<td>N/A</td>
<td>Explicit Failover</td>
</tr>
</tbody>
</table>

j. Leave Monitoring to the default.

k. Leave Miscellaneous to the default.

l. Do not edit more settings.

m. Click NEXT to view the Ready to complete dialog.

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

o. 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 (VMware vSphere 6.5)

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

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 the host displays and 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 1 and click OK.
   h. Select vmnic5 and click Assign uplink.
   i. Select Uplink 2 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, FT) 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/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 port groups. Do not select any checkboxes. 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.
Back up and restore a VMware VDS data configuration (VMware vSphere 6.x)

A zip file is created when you export the backup of a VMware VDS data configuration. The existing VMware VDS data configuration is not overwritten when you import the backup, instead a new version is created. When you perform a restore, the active VMware VDS data configuration is overwritten. Each feature is broken out by administrative procedures.

Export a backup of a VMware VDS configuration (VMware vSphere 6.7)

Export the VMware VDS configuration into a .zip file.

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

Before you begin
Verify that the VMware VDS is configured.

Procedure

1. Open a browser and type the following URL:
   https://<VCENTER_FQDN OR IP>/ui/
2. Log in to the VMware vSphere Client (HTML5) with the administrator@vsphere.local user account (VMware SSO account) or another administrative account with the appropriate permissions.
4. Right-click DVSwitch01-A and select Settings > Export Configuration.
5. Choose one of the following:
   - Distributed switch 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.

Import a backup of a VMware VDS configuration (VMware vSphere 6.7)

Create a VMware VDS from an exported configuration file using the same switch and distributed port group configuration.

About this task
Importing a backup does not override the existing VMware VDS.

Procedure

1. Open a browser and type the following URL: https://<VCENTER_FQDN OR IP>/ui/
2. Log in to the VMware vSphere Client (HTML5) with the administrator@vsphere.local user account (VMware SSO account) or another administrative account with appropriate permissions.
4. Right-click Datacenter and select Distributed Switch > Import Distributed Switch.
5. Click Browse > 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**.

### Restore a backup of a VMware VDS configuration (VMware vSphere 6.7)

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 destroys the existing VMware VDS.

#### Procedure

1. Open a browser and type the following URL: `https://<VCENTER_FQDN OR IP>/ui/`
2. Log in to the VMware vSphere Client (HTML5) with the `administrator@vsphere.local` user account (VMware vSphere SSO account) or other administrative account with appropriate permissions.
3. On the **Home** tab, click **Networking**.
4. Right-click the VMware VDS to be restored and select **Settings > Restore Configuration**.
5. Select one of the following:
   - Restore distributed switch and all port groups
   - Restore distributed switch only
6. Click **Browse**.
7. Select a distributed switch backup file and click **Next**.
8. Review the import settings and click **Finish**.

### Export a backup of a VMware VDS configuration (VMware vSphere 6.5)

Export the VMware VDS configuration into a .zip file.

#### About this task

The VMware VDS configuration includes all the VMware VDS and distributed port group 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`
2. Log in 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.
Import a backup of a VMware VDS configuration (VMware vSphere 6.5)
Create a VMware VDS from an exported configuration file using the same switch and distributed port group configuration.

About this task
Importing a backup does not override the existing VMware VDS.

Procedure
1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client
2. Log in 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 tab, under Inventories, click Networking.
4. Right-click the data center and select All vCenter Actions > Import Distributed Switch.
5. Click Browse > 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.

Restore a backup of a VMware VDS configuration (VMware vSphere 6.5)
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 to the settings in the configuration file and destroys the existing VMware VDS.

Procedure
1. Open a browser and type the following URL: https://<vCenterIP>:9443/vsphere-client
2. Log in 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 tab, under Inventories, click Networking.
4. Right-click the VMware VDS that you want to restore and select All vCenter Actions > Restore Configuration.
5. Select Restore distributed switch or port groups or Restore distributed switch only.
6. Click Browse > Select a distributed switch backup file and click Next.
7. Review the import settings and click Finish.

VMware VDS basic troubleshooting (VMware vSphere 6.x)
VMware documentation contains procedures to troubleshoot a VMware VDS.

To manage network health and rollback, see the following procedures:

- View vSphere Distributed Switch Health Check
- vSphere Networking Rollback
- Disable Rollback
- Resolve Errors in the Management Network Configuration on a vSphere Distributed Switch

VMware vSphere documentation
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. VMware ELM 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

Configure VMware Embedded Linked Mode (VMware vSphere 6.x)

VMware Embedded Link Mode provides VMware Enhanced Linked Mode (ELM) support for VMware vCenter Server Appliance (vCSA) with an embedded VMware Platform Services Controller (PSC). VMware Embedded Link Mode is provided for AMP-VX or AMP-3S.

About this task
Use VMware Embedded Link Mode with VMware vSphere 6.x to log in to a single VMware vCenter Server to manage multiple VMware vCenter Servers on multiple VxBlock Systems 1000.

VxBlock 1000 is physically and logically configured during manufacturing. Due to the installation prerequisites, VMware Embedded Link Mode must be configured on site. If multiple VxBlock 1000 Systems are ordered and are not part of the existing external domain, VMware Embedded Link Mode can be configured during manufacturing. To configure VMware Embedded Link Mode, contact Dell EMC Professional Services perform the site analysis, installation, and configuration.

AMP-VX

The following requirements apply for VMware Embedded Link Mode in a VxBlock 1000:

- A maximum of two production VMware vCenter servers in the default AMP-VX (four node)
- Up to eight linked VMware vCenter servers are enabled in a single VxBlock 1000 or across multiple VxBlock Systems 1000.
- A maximum of 625 hosts are enabled per linked VMware vCenter Server.
- Linked VMware vCenter Servers must be in the same VMware SSO domain. If different VMware Single Sign-On (SSO) domains are required, linked mode is not possible.

Note: VMware ELM is not supported across sites.

The eighth production VMware vCenter (VCprod08) creates a replication agreement with VCprod07 during deployment to join the existing VMware SSO. A manual replication agreement is created between VCprod08 and VCprod01 to complete the recommended ring topology.

AMP-3S

The following list outlines some of the guidelines for VMware Embedded Link Mode in a VxBlock 1000 with AMP-3S:

- Linked VMware vCenter Servers must be in the same VMware SSO domain. If different VMware SSO domains are required, linked mode is not possible.
- A maximum of eight linked VMware vCenter Servers is supported in a single VMware SSO domain.

Note: VMware Embedded Link Mode is not supported across sites.

The following figure shows two VxBlock Systems with a single VMware SSO site and domain:
The VMware vCenter Servers contain embedded VMware PSC and two VxBlock Systems.

**Procedure**

1. Log in to the VMware vCSA and perform the following steps to create the replication agreement:
   b. To enable SSH login and the bash shell, select Access and click Edit.
   c. To connect to `<vcenter_fqdn>` as root and log in to shell mode, type: `shell`
   d. To verify the current replication partner, type:
      ```
      /usr/lib/vmware-vmdir/bin/vdcrepadmin -f showpartners -h <vCenter_IP_Address> -u administrator
      ```
   e. To create a replication partner for the VMware PSC, type:
      ```
      /usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement -2 -h <vCenter_IP_Address> -H <New_Replication_Partner_IP_Address> -u administrator
      ```

   Do not link the AMP-VX VMware vCenter server and the VxBlock System VMware vCenter server.

   You cannot reverse deployment of VMware Embedded Link Mode. VMware Embedded Link Mode is managed as a complete system and should be considered a fault, operational, and maintenance domain. VMware Embedded Link Mode configurations must be compatible with backup and restore processes for all VMware vCenter servers in a single VMware SSO domain.

**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 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 the VxBlock System 1000. 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: 1st – 4th VMware vCenter server</td>
<td>1</td>
</tr>
<tr>
<td>Number of VMware vCenter servers per PSC: 5th – 8th VMware vCenter server</td>
<td>2</td>
</tr>
</tbody>
</table>

Intra VxBlock 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, Dell EMC recommends having a single VMware vCenter server in a standard Converged System.
- As extra 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):
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: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.psc.doc/GUID-62CC201A-01ED-4116-8604-FF123481DAFC.html

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: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.install.doc/GUID-E7DFB362-1875-4BCF-AB84-4F21408F87A6.html

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: https://docs.vmware.com/en/vCenter Server and Platform Services Controller/6.7/com.vmware.vsphere.upgrade.doc/GUID-925370DD-E3D1-455B-81C7-CB28AAF20617.html

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 conclusions (VMware vSphere 6.7)**

The following are the conclusions for VMware ELM.

Enhanced Linked Mode provides single pane of glass management for up to five PSCs and eight VMware vCenter servers in an SSO domain and provides simultaneous single pane of glass management for up to eight VMware vCenter servers. This provides an operational improvement in managing multiple VMware vCenter servers. However, as the number of PSCs and VMware vCenter servers increase, the size of the VMware vSphere 6.7 fault domain becomes larger.

Processes to backup and restore any VMware vSphere component participating in ELM must be absolutely 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.

In addition, as the size of the SSO domain increases, maintenance updates require more planning and coordination, because 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. Upgrades are usually performed in a maintenance window with time allocated to install, verify, and, if necessary, back out of the upgrade. Although a VMware vSphere 6.7 SSO domain can be large, the Dell EMC approach for ELM with VMware vSphere 6.7 deployments takes into account 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}`.
Note: Ensure that brackets are included.

12. 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:
   ```bash
   /opt/vce/fm/bin/runConfigCollector -iptablesOnly
   ```
2. To confirm the IP addresses for Converged System components are in the IP address table rules, type:
   ```bash
   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></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>
<tr>
<td>VMware vRO</td>
<td>Provides workflow engine and workflow designer capabilities</td>
</tr>
<tr>
<td>VxBlock Central Orchestration Services</td>
<td>Provides firmware repository management, credentials management, log management, PXE management VxBlock System workflows require.</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 lookups, use local DNS practices. Doing so ensures that each node can access the local AD server for lookups.

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:

```
lsotr -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-disable-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.

   \[\text{Note: If you encounter any problems during the join process, see the }\opt/vce/logs/multivbmrgmt/joinMSMCluster.log\text{ file.}\]

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/multivbmrgmt/install/cassandra_cluster_maintenance.sh --cron-enable-repair SEED_IP

   Where:
   
   * \text{SEED\_IP}\text{ 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

\[\text{Note: For VxBlock Central Version 2.0 and later, add, configure, and discover Converged Systems using the VxBlock Central user interface. See Discover Converged Systems online help for more information.}\]

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
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 139
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:
   
   ```
   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.
• ν 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 204

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 &lt;url&gt; 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.
Setting up VxBlock Systems to use VxBlock Central

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

1. **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 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 204

Delete a component with the configuration editor

Use the configuration editor to delete components from the VxBlock System configuration.

About this task

1. **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 204
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 169

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>show extension_packs</td>
<td>Lists all available extension packs on the MSM VM</td>
</tr>
<tr>
<td>show extension_pack_name</td>
<td>Lists the commands for a specific extension pack</td>
</tr>
<tr>
<td></td>
<td>For example, show default lists the commands in the default extension pack.</td>
</tr>
<tr>
<td>show component_type</td>
<td>Lists the commands for a specific component</td>
</tr>
<tr>
<td></td>
<td>For example, show storagearray lists the commands that can be</td>
</tr>
<tr>
<td></td>
<td>performed with storage arrays.</td>
</tr>
</tbody>
</table>

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'.

146   VxBlock System 1000 Administration Guide
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>%connect</td>
<td>Opens an interactive connection with the target component command-line interface</td>
</tr>
<tr>
<td></td>
<td>Only one device can be connected at a time.</td>
</tr>
<tr>
<td>%diff</td>
<td>Shows the difference between the attributes of two components</td>
</tr>
<tr>
<td>%run_commands</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.
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 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>
<tr>
<td>audit.log</td>
<td>The audit log records the following events in VxBlock Central Shell:</td>
</tr>
<tr>
<td></td>
<td>- Event</td>
</tr>
<tr>
<td></td>
<td>- User</td>
</tr>
<tr>
<td></td>
<td>- Date</td>
</tr>
<tr>
<td></td>
<td>- Client hostname</td>
</tr>
<tr>
<td></td>
<td>- Command issued</td>
</tr>
</tbody>
</table>

**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 configure Secure Remote Services for VxBlock Central, provide a software identifier (SWID). See `Retrieving the software ID from the Licensing system` for information about how to obtain the SWID.

⚠️ **CAUTION** Perform Secure Remote Services for VxBlock Central configuration only at a customer site.

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:

   ```bash
   /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.

⚠️ CAUTION Perform Secure Remote Services for VxBlock Central configuration only at a customer site.
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. Go to VxBlock Central to configure. If you are unable to configure the gateway, then see Check the Secure Remote Services gateway connectivity.

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.

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: /opt/vce/shell/bin/ESRSScript/esrs_setup.sh</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'))

| Cause | The Secure Remote Services gateway is not running, or it is unreachable. |
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 `traceroute` from the same VM on which VxBlock Central Shell is running.

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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Making MIB information available to the NMS.</td>
<td>SNMPv2c</td>
</tr>
<tr>
<td>Components</td>
<td>VxBlock Central</td>
<td>• Receiving traps</td>
<td>SNMPv1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VxBlock Central augments incoming traps with additional information.</td>
<td>SNMPv2c</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`.
-n  `sysName`  `system_name`  Specifies the name of the VxBlock System. The default is the hostname.

-1  `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.

-v  Displays the version.

-f  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>
### 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:
   ```bash
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:
   ```bash
   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:
   ```bash
   type configureSNMP
   ```

---

<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>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>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>
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:
Setting up VxBlock Systems to use VxBlock Central

- 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 enable 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.

1. 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>
</tbody>
</table>
| RCM content prepositioning administrator | Users with this role can:  
  - Access the RCM content prepositioning features in the dashboard  
  - Download RCM content  
  - Delete RCM content  
  - Cancel downloads |
| RCM content prepositioning user | Users with this role can view RCM content prepositioning features in the dashboard. |

**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 or Dell EMC Unity XT, configure the trap receiver on the Unisphere that monitors the Dell EMC Unity or Dell EMC Unity XT 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 or Dell EMC Unity XT 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, srdfa 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,ACTIVE`.

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 FMAgent 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`. 

---

**Setting up VxBlock Systems to use VxBlock Central**

$startFMagent

**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`. 

---

**VxBlock System 1000 Administration Guide**

168
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:

   ```bash
   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:

     ```bash
     /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.

**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
• Cannot contain any of the following special characters: ` / % + ' " ( ) ; : < > |

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.

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:

- \textit{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.
- \textit{SSHadminuser} is the username for logging on.
- \textit{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 \textit{system.cfg} is in the \textit{/opt/vce/fm/conf} directory on the Core VM. If \textit{system.cfg} is not present, contact Dell EMC Support.

**Procedure**

1. Start an SSH session to the Core VM.
   
   \textbf{Note}: Use PuTTY to access the configuration editor for Windows-based systems as non-VSCII supported terminals display styling incorrectly.

2. Log in using \texttt{root/V1rtu@1c3!}.

3. To launch the configuration editor and edit a configuration, type: \texttt{configSystem edit}

**Bulk credential script**

The bulk credential script is used to change the password for multiple components.

**About this task**

\textbf{Note}: For VxBlock Central Version 2.0 and later, add, configure, and discover Converged Systems using the VxBlock Central user interface. See \textit{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 \textit{system.cfg} file to an \textit{inputfile} file. The script automatically changes the password for the listed components. The script also checks if the password parameter is empty in the \textit{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 \textit{system.cfg} file and creates \textit{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:

   ```
   ```
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 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 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 <code>proxy.password</code> 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:
   ```bash
   service vision-downloader restart
   ```

6. To restart the Content Source service, type:
   ```bash
   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:
   ```bash
   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:
A minimum download rate of 1024 bytes is required. The default value is 0 which is interpreted as an unlimited download rate. Set a minimum download rate of 2 MB. Downloading a full RCM Content with less bandwidth may result in an incomplete RCM download after 8 hours. Restart any incomplete RCM download.

### 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:** When specifying the download rate, note the following:
   - 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><code>retry.max.attempts</code></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><code>retry.initial.interval</code></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>
### Property name and Description

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>retry.multiplier</td>
<td>Sets the multiplication factor that is used for attempts to connect to the RCM content distribution network.</td>
</tr>
<tr>
<td></td>
<td>This multiplier is used if VxBlock Central fails to connect a second time.</td>
</tr>
<tr>
<td></td>
<td>The default value is 2.0.</td>
</tr>
<tr>
<td></td>
<td>For example, if VxBlock Central waited for 100 milliseconds after the initial failure and the multiplier is 2.0, VxBlock Central waits for 200 milliseconds before the third attempt and 400 milliseconds before the fourth attempt.</td>
</tr>
<tr>
<td>retry.max.interval</td>
<td>Sets the maximum time interval, in milliseconds, between each retry from VxBlock Central to the RCM content distribution network.</td>
</tr>
<tr>
<td></td>
<td>The default value is 50000.</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:
   ```
   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.
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.

Manage VxBlock Central Orchestration Services and VxBlock Central Orchestration Workflows

VxBlock Central Orchestration Services and VxBlock Central Orchestration Workflows are set up during the VxBlock Central configuration.

VxBlock Central Orchestration Workflows automate and simplify component provisioning and configuring for VxBlock Central Orchestration Services to provide an overview of health and status of in-built services that are used by workflows.

Configure the following VxBlock Central Orchestration Services:

- Admin Credentials for VxBlock System Components
- DHCP Configuration
- Firmware Repository

These services must be configured before you can run compute expansion workflows.
VxBlock Central Orchestration Services

Online describes the VxBlock Central Orchestration Services dashboard which contains a high-level health status of critical back-end services that are used by VxBlock Central Orchestration Workflows. Online help is also provided to manage credentials and the firmware repository, configure the network and collect logfiles.

VxBlock Central Orchestration Services provides the following features:

- **Dashboard**: Provides health view for all VxBlock Central Orchestration Services. You can start, stop, or restart individual services.
- **Credential Store**: Displays list of VxBlock Systems and their underlying components that are pulled from VxBlock Central without credentials. To run VxBlock Central Orchestration workflows, admin credentials are required for each component.
- **DHCP Configuration**: Used to configure DHCP which is used to allocate initial IP Address for Cisco UCS servers that are used for TFTP Boot. After the PXE boot is completed the IP Address that is provided by user in workflow is configured for servers.
- **Firmware Repository Management**: Use to manage firmware images for VMware vSphere ESXi server provisionning.

**Note**: Administrators can reuse ISO images multiple times in VMware vRO workflows. If a new version of VMware vSphere ESXi is applied to a system (during RCM updates, for example), the same version must be manually uploaded to the VxBlock Central Orchestration Services firmware repository. This ensures that future workflows use the version that matches the rest of the system when provisioning VMware vSphere ESXi.

VxBlock Central Orchestration Workflows

VMware vRealize (vRO) contains service and fulfillment workflows that can be used to automate configuration and provisioning tasks.

Online help provides a description of all available workflows and how to use them in VxBlock Central Orchestration Workflows.

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:
   ```
   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>
<tr>
<td>Facility</td>
<td></td>
</tr>
<tr>
<td>Severity</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)

```bash
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:

```bash
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:

```bash
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
   # Puppet Name: vce-puppet
   */10 * * * * /opt/vce/fm/install/backupDatabase.sh > /dev/null 2>&1
   ```

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:
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**

1. Change directory to /opt/vce/fm/backup/postgres/.
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:
   ```
   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:
      ```
      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:
   ```
   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:

<table>
<thead>
<tr>
<th>Database name</th>
<th>Schema</th>
</tr>
</thead>
</table>
   | model         | • admin
                  • model
                  • rbac    |
a. Log in to the database:

```sql
psql database_name
```

b. List all schema in the database:

```sql
select schema_name from information_schema.schemata where
schema_owner = 'admin';
```

c. Drop the schema:

```sql
drop schema if exists schema_name cascade;
```

d. Confirm that the drop was successful:

```sql
select schema_name from information_schema.schemata where
schema_owner = 'admin';
```

e. Exit: `\q`

7. To restore the database, type:

```sql
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  
<p>|                           | Converged Technology Extension for Cisco UCS compute |</p>
<table>
<thead>
<tr>
<th>Converged System</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vblock System 540</td>
<td>Cisco MDS 9000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 5000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 3000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 7000 and/or Cisco Nexus 9000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 1000V</td>
</tr>
<tr>
<td></td>
<td>Cisco UCS fabric interconnects (UCS Manager)</td>
</tr>
<tr>
<td></td>
<td>XtremIO</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>VxBlock System 540</td>
<td>Cisco MDS 9000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 5000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 3000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 7000 and/or Cisco Nexus 9000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 1000V</td>
</tr>
<tr>
<td></td>
<td>Cisco UCS fabric interconnects (UCS Manager)</td>
</tr>
<tr>
<td></td>
<td>XtremIO</td>
</tr>
<tr>
<td></td>
<td>Management servers (CIMC)</td>
</tr>
<tr>
<td></td>
<td>Technology Extension for Storage</td>
</tr>
<tr>
<td>Vblock System 700 series</td>
<td>Cisco MDS 9000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 5000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 3000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 7000 and/or Cisco Nexus 9000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 1000V</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>VxBlock System 740</td>
<td>Cisco MDS 9000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 5000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 3000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 7000, and/or Cisco Nexus 9000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 1000V</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>
</tbody>
</table>
### Manual backup

Due to component limitations or known issues, the following configuration files are not backed up:

- Dell EMC Unity and Unity XT 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 to 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>Secure shell (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>
</tbody>
</table>
| collectConfig.sh       | Collects and backs up VxBlock System configuration files  
Run this script from the `/opt/vce/fm/bin` directory.  
**Note:** The `collectConfig.sh` command is supported on a VxBlock System only. |
| configureSyslogForward | Configures syslog forwarding  
**Note:** The `configureSyslogForward` command is supported on a VxBlock System only. |
| configureNTP           | Manages network time protocol (NTP) synchronization settings on the Core VM |
| configureSNMP          | Configures northbound SNMP communication between VxBlock Central and a network management system (NMS) or trap target  
**Note:** The `configureSNMP` command is supported on a VxBlock System only. |
| createEULASoftCopy     | Creates a soft copy of the end user license agreement (EULA) in the following directory: `/opt/vce/fm/eula` |
| displayEula            | Displays the end user license agreement (EULA)  
Run this command from the `/opt/vce/fm/bin` directory. |
| export-fm-config.sh    | Exports VxBlock Central configuration to the following directory: `/opt/vce/fm/back`.  
Run this script from the `/opt/vce/fm/bin` directory. |
| getFMagentInfo         | Displays version and build information about VxBlock Central |
| install_content.sh     | Installs compliance content  
Run this script from the `/opt/vce/compliance/content` directory. |
| restoreConfig.sh       | Restores VxBlock Central configuration from a backup file  
Run this script from the `/opt/vce/fm/install` directory. |
| setSNMPParams          | Modifies the following SNMP parameters for a VxBlock System:  
- sysName  
- sysContact  
- sysLocation  
Use double quotes for values that contain space characters. |
| 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. |
# Manage VxBlock Systems with VxBlock Central

<table>
<thead>
<tr>
<th>Command or script</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vce-puppet-disable.pp</td>
<td>Disables the Puppet service management utility from monitoring VxBlock Central services. Run this script from the <code>/etc/puppet/manifests</code> directory using the <code>puppet apply</code> command.</td>
</tr>
<tr>
<td>vce-puppet-enable.pp</td>
<td>Enables the Puppet service management utility to monitor VxBlock Central services. Run this script from the <code>/etc/puppet/manifests</code> directory using the <code>puppet apply</code> command.</td>
</tr>
<tr>
<td>vce-puppet-start.pp</td>
<td>Start all VxBlock Central services. Run this script from the <code>/etc/puppet/manifests</code> directory using the <code>puppet apply</code> command. This script uses the 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 <code>/etc/puppet/manifests</code> directory using the <code>puppet apply</code> command. This script uses the Puppet service management utility to gracefully stop services and prevent 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 <code>/opt/vce/multivbmgmt/install</code> directory.</td>
</tr>
<tr>
<td>caschangepw.sh</td>
<td>Changes the CAS password for MSM VM. Run this script from the <code>/opt/vce/multivbsecurity/bin</code> directory.</td>
</tr>
<tr>
<td>credential-manager-cli</td>
<td>Lets you manage credentials within the MSM VM environment. Run this script from the <code>/opt/vce/credential-management/bin</code> directory.</td>
</tr>
<tr>
<td>joinMSMCluster.sh</td>
<td>Adds an MSM VM to that node in the cluster. Run this script from the <code>/opt/vce/multivbmgmt/install</code> directory.</td>
</tr>
<tr>
<td>nodetool status</td>
<td>Verifies that Cassandra is installed and configured correctly. Run this command from the <code>/opt/cassandra/bin</code> 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>service vision-credential-manager start</td>
<td>Starts the Credential Manager service</td>
</tr>
<tr>
<td>service vision-mvb-compliance status</td>
<td>Verifies that the compliance service is running</td>
</tr>
<tr>
<td>service vision-mvb-compliance start</td>
<td>Starts the compliance service</td>
</tr>
<tr>
<td>service vision-shell status</td>
<td>Verifies that the VxBlock Central Shell service is running</td>
</tr>
<tr>
<td>service vision-shell start</td>
<td>Starts the VxBlock Central Shell service</td>
</tr>
<tr>
<td>start_cassandra.sh</td>
<td>Starts Cassandra&lt;br&gt;Run this script from the /opt/cassandra/install directory.</td>
</tr>
<tr>
<td>stop_cassandra.sh</td>
<td>Stops Cassandra&lt;br&gt;Run this script from the /opt/cassandra/install directory.</td>
</tr>
<tr>
<td>vision start</td>
<td>Checks if each service is running. If not, starts the service.</td>
</tr>
<tr>
<td>service vision-web-ui restart</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>/opt/vce/msp/install/update-cas-password.sh</td>
<td>Enables you to update the Central Authentication Service (CAS) password for the admin user in a clustered environment</td>
</tr>
<tr>
<td>/opt/vce/msp/install/update-proxy-password.sh</td>
<td>Enables you to set a password for a proxy server to access the RCM content distribution network&lt;br&gt;This script can also be used to change the proxy password if required.</td>
</tr>
<tr>
<td>/opt/vce/msp/install/update-assetmanager-db-password.sh</td>
<td>Enables you to change the default password for the Asset Manager</td>
</tr>
<tr>
<td>/opt/vce/msp/install/update-contentshare-db-password.sh</td>
<td>Enables you to change the default password for the Content Share PostgreSQL database</td>
</tr>
<tr>
<td>vision status</td>
<td>Provides a status on all MSP services</td>
</tr>
<tr>
<td>vision stop</td>
<td>Stops all MSP services</td>
</tr>
<tr>
<td>vision start</td>
<td>Starts all MSP services</td>
</tr>
<tr>
<td>service vision-contentsource restart</td>
<td>Restarts the contentsource service</td>
</tr>
<tr>
<td>service vision-contentsource stop</td>
<td>Stops the contentsource service</td>
</tr>
<tr>
<td>service vision-contentsource start</td>
<td>Starts the contentsource service</td>
</tr>
<tr>
<td>service vision-contentshare restart</td>
<td>Restarts the contentshare service</td>
</tr>
<tr>
<td>service vision-contentshare stop</td>
<td>Stops the contentshare service</td>
</tr>
<tr>
<td>service vision-contentshare start</td>
<td>Starts the contentshare service</td>
</tr>
<tr>
<td>service vision-downloader restart</td>
<td>Restarts the downloader service</td>
</tr>
<tr>
<td>service vision-downloader stop</td>
<td>Stops the downloader service</td>
</tr>
</tbody>
</table>
**Command or script**

<table>
<thead>
<tr>
<th>Command or script</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service vision-downloader start</td>
<td>Starts the downloader service</td>
</tr>
<tr>
<td>service vision-assetmanager restart</td>
<td>Restarts the assetmanager service</td>
</tr>
<tr>
<td>service vision-assetmanager stop</td>
<td>Stops the assetmanager service</td>
</tr>
<tr>
<td>service vision-assetmanager start</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</td>
<td>In AMP</td>
<td>Specifies if the component is a part of the AMP configuration</td>
<td>x</td>
</tr>
<tr>
<td>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</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</td>
<td>IP Address</td>
<td>Dotted IP address</td>
<td>10.1.139.52</td>
</tr>
<tr>
<td>VMAX/PowerMax</td>
<td>Which</td>
<td>Must be VMAX.</td>
<td>VMAX</td>
</tr>
<tr>
<td>Storage array</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</td>
<td>Username</td>
<td>Username</td>
<td>fmuser</td>
</tr>
<tr>
<td>VMAX/PowerMax</td>
<td>Password</td>
<td>Password</td>
<td>password</td>
</tr>
<tr>
<td>Storage array</td>
<td>In AMP</td>
<td>Specifies if the component is a part of the AMP configuration</td>
<td>x</td>
</tr>
<tr>
<td>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/ gateway</td>
<td>Component tag</td>
<td>Must be one of the following: VMAX10K-ARRAY, VMAX20K-ARRAY, VMAX40K-ARRAY, VMAX3ARRAY, VMAX100K-ARRAY, VMAX200K-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 w/ gateway</td>
<td>IP Address</td>
<td>Dotted IP address</td>
<td>10.1.139.52</td>
</tr>
<tr>
<td>Storage array VMAX w/ gateway</td>
<td>Which</td>
<td>Must be VMAX</td>
<td>VMAX</td>
</tr>
<tr>
<td>Storage array VMAX w/ gateway</td>
<td>Method</td>
<td>Dotted IP address</td>
<td>10.1.139.42</td>
</tr>
<tr>
<td>Storage array VMAX w/ gateway</td>
<td>Username</td>
<td>VMAX username</td>
<td>fmuser</td>
</tr>
<tr>
<td>Storage array VMAX w/ gateway</td>
<td>Password</td>
<td>VMAX password</td>
<td>password</td>
</tr>
<tr>
<td>Storage array VMAX w/ gateway</td>
<td>Which</td>
<td>The second Which field must be gateway.</td>
<td>gateway</td>
</tr>
<tr>
<td>Storage array VMAX w/ gateway</td>
<td>Method</td>
<td>The second Method is a dotted IP address.</td>
<td>10.1.139.42</td>
</tr>
<tr>
<td>Storage array VMAX w/ gateway</td>
<td>Username</td>
<td>NAS administrator username</td>
<td>nasadmin</td>
</tr>
<tr>
<td>Storage array VMAX w/ gateway</td>
<td>Password</td>
<td>NAS administrator password</td>
<td>password</td>
</tr>
<tr>
<td>Storage array 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>Storage array XtremIO</td>
<td>Type</td>
<td>Must be XTREMIO</td>
<td>XTREMIO</td>
</tr>
<tr>
<td>Storage array XtremIO</td>
<td>Component tag</td>
<td>Must be XIO-ARRAY-1</td>
<td>XIO-ARRAY-1</td>
</tr>
<tr>
<td>Storage array XtremIO</td>
<td>IP Address</td>
<td>Dotted IP address</td>
<td>10.1.139.52</td>
</tr>
<tr>
<td>Storage array XtremIO</td>
<td>Which</td>
<td>Must be XTREMIO</td>
<td>XTREMIO</td>
</tr>
<tr>
<td>Storage array XtremIO</td>
<td>Method</td>
<td>Must be xml</td>
<td>xml</td>
</tr>
<tr>
<td>Storage array XtremIO</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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Type</td>
<td>Must be ISILON</td>
<td>ISILON</td>
</tr>
<tr>
<td>Isilon</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Component tag</td>
<td>Must be ISILON-ARRAY-CLUSTER-1</td>
<td>ISILON-ARRAY-CLUSTER-1</td>
</tr>
<tr>
<td>Isilon</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>IP Address</td>
<td>Dotted IP address</td>
<td>10.1.139.52</td>
</tr>
<tr>
<td>Isilon</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Method</td>
<td>Must be one of the following: IPMIv2, SNMPv2C, WEBSERVICE, SSH</td>
<td>snmpv2c</td>
</tr>
<tr>
<td>Isilon</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Username</td>
<td>Isilon username</td>
<td>admin</td>
</tr>
<tr>
<td>Isilon</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Password</td>
<td>Isilon password</td>
<td>password</td>
</tr>
<tr>
<td>Isilon</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>In AMP</td>
<td>Specifies if the component is a part of the AMP configuration</td>
<td>x</td>
</tr>
<tr>
<td>Dell EMC Unity and Dell EMC Unity XT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Type</td>
<td>Must be UNITY</td>
<td>UNITY</td>
</tr>
<tr>
<td>Dell EMC Unity and Dell EMC Unity XT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</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>Dell EMC Unity and Dell EMC Unity XT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>IPv4/IPv6 Address</td>
<td>Dotted IP address</td>
<td>10.1.139.52/ 201::XX</td>
</tr>
<tr>
<td>Dell EMC Unity and Dell EMC Unity XT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Method</td>
<td>Must be restApi</td>
<td>restApi</td>
</tr>
<tr>
<td>Dell EMC Unity and Dell EMC Unity XT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Username</td>
<td>Dell EMC Unity username</td>
<td>admin</td>
</tr>
<tr>
<td>Dell EMC Unity and Dell EMC Unity XT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Password</td>
<td>Dell EMC Unity password</td>
<td>password</td>
</tr>
<tr>
<td>Dell EMC Unity and Dell EMC Unity XT</td>
<td></td>
<td></td>
<td></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>vCenter</td>
<td>In AMP</td>
<td>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.</td>
<td>x</td>
</tr>
<tr>
<td>vCenter</td>
<td>Name</td>
<td>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 VIManager query.</td>
<td>vcenter1</td>
</tr>
<tr>
<td>vCenter</td>
<td>URL</td>
<td>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.</td>
<td>10.1.139.39</td>
</tr>
</tbody>
</table>

<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>
<tbody>
<tr>
<td>FMAgent</td>
<td>On a scheduled basis, retrieves information from VxBlock System components. The information is used to update the system information in PostgreSQL.</td>
</tr>
<tr>
<td>VxBlock Central Repository</td>
<td>Provides an API to manage VxBlock Central on the Core VM that RCM content prepositioning uses to store RCM content</td>
</tr>
<tr>
<td>VxBlock Central API for VxBlock Central Security</td>
<td>Provides REST resources for controlling access to system resources through role-based access control</td>
</tr>
</tbody>
</table>
Components, APIs, services

<table>
<thead>
<tr>
<th>Components, APIs, services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RabbitMQ</td>
<td>Provides the Core VM services and applications with a common platform to send and receive messages asynchronously and ensures that messages are delivered</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>Stores collected data, credentials, and records for Core VM services</td>
</tr>
</tbody>
</table>

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>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>
</tbody>
</table>
| MSM VM Compliance service     | Validates VxBlock Systems are compliant when compared to different criteria. A compliance scan can be performed for the following:  
  - Release Certification Matrix (RCM) compliance  
  - Dell EMC Security and Technical Advisory compliance |
| MSM VM API for multisystem services | Queries and filters data that is collected from VxBlock Systems in an MSM VM environment |
| Collection Manager service    | Runs the MSM VM collection manager that runs in the Vert.x instance and performs data collection |
| MSM VM API for Security Web   | Provides REST resources for to control access to system resources within an MSM VM environment through role-based access control (RBAC) |
| MSP API for RCM content prepositioning | Provides REST resources that are used to run the RCM content prepositioning functions, such as downloading RCM content, deleting content, and canceling RCM download |
| VxBlock Central Shell         | 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. |
| RabbitMQ                     | Provides MSM VM services and applications with a common platform to send and receive messages asynchronously |
| Elasticsearch                | 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. |
| Vert.x                       | A lightweight event-driven application platform for web applications. The Vert.x instance contains the MSM VM collection manager. |
| Cassandra                    | 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. |

The following table shows the components and services running on each MSP VM:
### Components and services
<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manages the inventory of RCM content local to the running instance of the assetmanager service</td>
</tr>
<tr>
<td>Manages the following tasks:</td>
</tr>
<tr>
<td>- Acknowledges a download request</td>
</tr>
<tr>
<td>- Downloads each required file from the Content Distribution Network (CDN)</td>
</tr>
<tr>
<td>- Provides status updates during the download process</td>
</tr>
<tr>
<td>Manages entitlements and request notifications from the CDN, and ensures that all downloaded RCM content matches the download requests</td>
</tr>
<tr>
<td>Coordinates the content share, content source, and the downloader services for working with RCM content on the MSP VM</td>
</tr>
<tr>
<td>Stores the downloaded RCM content on the MSP VM</td>
</tr>
</tbody>
</table>

The following table shows the components and services that are running on VxBlock Central Orchestration VM:

<table>
<thead>
<tr>
<th>Components and services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP service</td>
<td>Allots the initial IP address for Cisco UCS servers that are used for TFTP boot. After PXE boot is completed, the IP address provided by user in the workflow is configured for these servers.</td>
</tr>
<tr>
<td>TFTP service</td>
<td>Loads VMware vSphere ESXi ISO images to Cisco UCS server during PXE boot</td>
</tr>
<tr>
<td>PXE</td>
<td>Installs VMware vSphere ESXi ISO images on Cisco UCS Servers. Starts PXE boot using the IP address, hostname, password provided by user in the workflow for the Cisco UCS server.</td>
</tr>
<tr>
<td>Registry service</td>
<td>Provides a single point of entry for all VxBlock Central Orchestration Services</td>
</tr>
<tr>
<td>API Gateway service</td>
<td>Stores the downloaded RCM content on the MSP VM</td>
</tr>
<tr>
<td>Credential service</td>
<td>Provides a single point to obtain credential information for all VxBlock System components</td>
</tr>
<tr>
<td>Firmware Repository service</td>
<td>Stores ESXi ISO images.</td>
</tr>
<tr>
<td>PXE Configuration service</td>
<td>Generates Kickstart and Firstboot file used during Cisco UCS server PXE boot</td>
</tr>
<tr>
<td>Storage Operation service</td>
<td>Performs operations on VMAX</td>
</tr>
<tr>
<td>MongoDB</td>
<td>Manages VxBlock System provider/components details, VMware vSphere ESXi ISO images, DHCP configuration details and collected log details</td>
</tr>
<tr>
<td>InfraOps Service</td>
<td>Performs operations on Cisco UCS servers and Cisco MDS switches</td>
</tr>
</tbody>
</table>
Manage the AMPs

VxBlock Systems are managed by AMPs that use their own resources to manage workflows. VxBlock Systems can be managed by the following AMP configurations:

- AMP-3S
- AMP-VX

Procedures to manage VxBlock Systems with AMP-3S are provided in this guide. See the Dell EMC AMP-VX Product Guide to manage AMP-VX.

VxBlock Central

The following table provides an overview of VxBlock Central support for the AMPs:

<table>
<thead>
<tr>
<th>AMP</th>
<th>VxBlock Central Base</th>
<th>VxBlock Central Workflow Automation</th>
<th>VxBlock Central Advanced Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMP-3S</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>AMP-VX</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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.

Upgrade Dell EMC Unity software

Upgrade Dell EMC Unity storage array software using the Dell EMC Unity Unisphere GUI.

About this task
Use the IPv4 address to access the Dell EMC Unity management port.

Before you begin
- Perform a system health check and resolve any underlying problems that would prevent a successful upgrade one week before the upgrade.
- See the Dell EMC Unity 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 Update system software, firmware, and language packs.
- Obtain the IPv4/IPv6 address and login credentials for the AMP Dell EMC Unity management array.

Procedure
1. Check for software updates on the Dell EMC Support website.
2. If the software 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 Dell EMC service provider to ensure that the upgrade software includes your hot fixes.
3. Download the new software to a local machine on your network.
4. Upload the new software from your local machine to your storage array.
5. Install the file on your storage array.
   The installation checks the health of the system to determine if any issues 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. Specify a new data store name using the following convention: `MGMT-DS-A03` or `MGMT-DS-B03`.
   c. Confirm that **Storage Pool** is the default.
   d. Set the **Tiering Policy** to **Auto-Tier**.
   e. Ensure that the data store size is not greater than 2 TB.
   f. Clear **Thin**.
   g. Select **Do not configure a snapshot schedule**.
   h. Set the host access for all entries to **Read/Write, allow Root**.
   i. 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 log in 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

Add a VMware vSphere ESXi host to the Dell EMC Unity storage array configuration for IPv4 and IPv6.

Before you begin

- Use the Dell EMC Unity Unisphere GUI online help for the latest process. Access the online help by clicking the question mark on the VMware Hosts page.
- Obtain the IPv4/IPv6 address and log in credentials for the Dell EMC Unity storage array.
- Obtain the VMware vSphere ESXi host IPv4/IPv6 address on the vcesys_oob-mgmt VLAN or client equivalent. VMware vSphere ESXi supports IPv4 and IPv6, but does not support dual stack.
- Ensure the VMware vSphere ESXi host is added to VMware vSphere and the iSCSI adapter installed. The Dell EMC Unity array discovers hosts when the iSCSI adapter is added and scanned from VMware vSphere.

Procedure

1. Log in to the Unisphere GUI.
2. Click the bars.
3. Select Storage > Block > LUNs.
4. On the LUNs page, select the first listed MGMT-DS-<#> LUN, and click View/Edit.
   a. Select the Host Access tab, then +.
   b. Under Select Host Access, confirm all ESXi host entries are listed. Select the checkbox for each host that should have access to the LUN, and click OK.
   c. View new entries in Host Access table and click Apply.
5. Repeat the prior step for the remaining listed MGMT-LUN-<#> LUNs.

After you finish

After you add a VMware host configuration, 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 datastores.

Configure VMware vSphere ESXi persistent scratch location (VMware vSphere 6.7)

Configure all management VMware vSphere ESXi hosts with persistent scratch location.

Before you begin

- Obtain administrative privileges to the VMware vSphere ESXi hosts.
- Assign datastores to VMware vSphere ESXi hosts.
- See VMware KB article Creating a persistent scratch location for ESXi 4.x/5.x/6.x.

Procedure

1. Log in to VMware vSphere Client (HTML5) using the administrator@vsphere.local SSO account.
2. Go to Home > Storage.
3. Right-click the MGMT-SCRATCH-01 datastore and click Browse.
4. Click New Folder and create a unique directory name for the VMware vSphere ESXi host. For example, .locker_ESXHostname.
5. Select Home > Hosts and Clusters.
6. Select the host and go to Configure tab > System > Advanced System Settings.
7. Click Edit and in the filter type ScratchConfig.
8. To update the ScratchConfig.ConfigurationScratchLocation parameter, type the full path to directory. For example: `/vmfs/volumes/MGMT-SCRATCH-01/.locker_ESXHostname`
   
   Hosts must be assigned to respective folders. Issues may occur if two hosts use the same scratch folder location.
9. Click OK.
10. Put the VMware vSphere ESXi host into maintenance mode and restart for the configuration change to take effect.
11. Repeat this procedure for each management ESXi host.

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. Update the ScratchConfig.ConfigurationScratchLocation 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. Repeat these steps on the remaining Cisco UCS C2x0 servers.
Disable VAAI primitives

When you install VMware vSphere ESXi, disable the VAAI primitive for each VMware vSphere ESXi host.

**About this task**

For more information, see VMware Knowledge Base article 103665.

**Before you begin**

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

**Procedure**

1. From the VMware vSphere ESXi host, type:
   
   ```bash
   esxcli system settings advanced set --int-value 0 --option /DataMover/
   HardwareAcceleratedMove
   
   esxcli system settings advanced set --int-value 0 --option /DataMover/
   HardwareAcceleratedInit
   
   esxcli system settings advanced set --int-value 0 --option /VMFS3/
   HardwareAcceleratedLocking
   ```

2. To confirm that the setting was made, type:
   
   ```bash
   esxcli system settings advanced list --option=/VMFS3/HardwareAcceleratedLocking
   
   esxcli system settings advanced list --option=/DataMover/HardwareAcceleratedMove
   
   esxcli system settings advanced list --option=/DataMover/HardwareAcceleratedInit
   ```

3. From the command output, verify the **Int Value** is set to 0.

**Back up AMP-3S**

**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 (VMware vSphere 6.x)**

Back up targets in the AMP for the Converged System.

- Back up all VMs daily at 7 A.M. and 7 P.M.
- Set the retention value to 35 days.

⚠️ **CAUTION** Disk storage resources should be monitored to prevent overuse issues and data unavailability.

Store AMP servers backup and binaries on backup media so that they can be installed or restored. Otherwise, managing or recovering the Converged System might not be possible.

AMP servers are:

- VMware vCenter Server with Embedded PSC
- VMware vCenter Server Appliance (vCSA)
- VMware Platform Services Controllers (PSC)
- Element Manager
- Other VMs identified as part of the core or optional workloads to manage the Converged System.

You configure backups for Cisco management switches (Cisco Nexus 3000/9000 Switch). See the appropriate RCM for a list of what is supported on your Converged System.

To back up targets in AMP and the Converged Systems, see the documentation from the backup tool vendor.

**Back up the Dell EMC Unity configuration**

Back up the Dell EMC Unity storage array that is 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 IPv4/IPv6 address and/or URL of the Dell EMC Unity management address.
- Obtain administrator login credentials for service accounts.

**Procedure**

1. Open a URL to the Dell EMC Unity management address to log in to Unisphere.
2. From the login screen, type the username and password for the account with advanced administrator privileges for the Dell EMC Unity system. If using an LDAP-based account, type the domain/username and click Login.
3. To initiate a configuration backup task, select System > Service > Service Tasks.
4. Select Save Configuration.
5. Select More Information... on the right side of the page for details instructions on performing this procedure.

If you click Save Configuration, you can save details about the configuration settings on the Dell EMC Unity system to a local file. Service personnel can use this file to assist with reconfiguring your system after a major system failure or a system reinitialization.

The configuration details include information about:

- System specifications
AMP and VxBlock System Integrated Data Protection

Back up the AMP-3S management core workload

For VxBlock Systems with integrated data protection managed by the AMP-3S, the backup software is preconfigured to perform proxy-based image backups of the core management workload VMs.

Image backups are also performed for the management and production VMware vCenter Server Appliances (vCSAs) and VMware Platform Service Controllers (PSCs). A backup client is installed on the Windows Server-based element manager VMs to start file system backups of the VMs.

The following table shows the specific AMP management workload VMs that Integrated Data Protection backup protects:

<table>
<thead>
<tr>
<th>VM</th>
<th>Backup type</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vCSAs</td>
<td>Proxy-based image</td>
</tr>
<tr>
<td>VMware PSCs</td>
<td>Proxy-based image</td>
</tr>
<tr>
<td>Element manager for data protection</td>
<td>Proxy-based Image</td>
</tr>
<tr>
<td></td>
<td>Client-based file system</td>
</tr>
<tr>
<td>Element manager for storage arrays</td>
<td>Proxy-based Image</td>
</tr>
<tr>
<td></td>
<td>Client-based file system</td>
</tr>
<tr>
<td>PowerPath Management Appliance</td>
<td>Proxy-based image</td>
</tr>
<tr>
<td>VxBlock Central</td>
<td>Proxy-based image</td>
</tr>
</tbody>
</table>

The following table lists the Avamar configuration for AMP backup:

<table>
<thead>
<tr>
<th>Avamar System</th>
<th>VMs</th>
<th>Dataset</th>
<th>Plug-In</th>
<th>Options</th>
<th>Stored backup</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avamar Virtual Edition, Avamar Single Node, Avamar Multi-Node with Data Domain</td>
<td>Management VMware vCSA Management VMware PSCs</td>
<td>AMP VMware Image Dataset AMP-3S VMware Image Dataset</td>
<td>Linux VMware Image</td>
<td>Changed Block Tracking enabled</td>
<td>Data Domain</td>
<td>AMP vCenter Image AMP-3 vCenter Image</td>
</tr>
<tr>
<td>Avamar Multi-Node</td>
<td>Management VMware vCSA Management VMware PSCs</td>
<td>AMP VMware Image Dataset AMP-3S VMware Image Dataset</td>
<td>Linux VMware Image</td>
<td>Changed Block Tracking enabled</td>
<td>Avamar Multi-Node Datastore nodes</td>
<td>AMP vCenter Image AMP-3 vCenter Image</td>
</tr>
</tbody>
</table>
The following table lists the NetWorker configuration for AMP backup:

<table>
<thead>
<tr>
<th>Avamar System</th>
<th>VMs</th>
<th>Dataset</th>
<th>Plug-In</th>
<th>Options</th>
<th>Stored backup</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avamar Virtual Edition, Avamar Single Node,</td>
<td>EM01 EM02</td>
<td>AMP VMware Image Dataset</td>
<td>Linux VMware Image</td>
<td>Changed Block Tracking enabled</td>
<td>Data Domain</td>
<td>AMP Mgmt VM Image</td>
</tr>
<tr>
<td>Avamar Multi-Node with Data Domain</td>
<td>PPMA</td>
<td>AMP-3S VMware Image Dataset</td>
<td>Windows VMware Image</td>
<td></td>
<td></td>
<td>AMP-3 Mgmt VM Image</td>
</tr>
<tr>
<td>PPMA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EM01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EM02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avamar Virtual Edition, Avamar Single Node,</td>
<td>VxBlock Central Core</td>
<td>AMP VMware Image Dataset</td>
<td>Linux VMware Image</td>
<td>Changed Block Tracking enabled</td>
<td>Data Domain</td>
<td>AMP VxBlock Central VM Image</td>
</tr>
<tr>
<td>Avamar Multi-Node with Data Domain</td>
<td>VxBlock Central MSM</td>
<td>AMP-3S VMware Image Dataset</td>
<td>Windows VMware Image</td>
<td></td>
<td></td>
<td>AMP-3 VxBlock Central Image</td>
</tr>
<tr>
<td>Avamar Multi-Node</td>
<td>VxBlock Central MSM</td>
<td>AMP-3S VMware Image Dataset</td>
<td>Windows VMware Image</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VxBlock Central MSM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VxBlock Central MSP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMware vRO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VxBlock Central Orchestration Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avamar Multi-Node</td>
<td>VxBlock Central Core</td>
<td>AMP VMware Image Dataset</td>
<td>Linux VMware Image</td>
<td>Changed Block Tracking enabled</td>
<td>Avamar Multi-Node Datastore</td>
<td>AMP Mgmt VM Image</td>
</tr>
<tr>
<td>VxBlock Central MSM</td>
<td></td>
<td>AMP-3S VMware Image Dataset</td>
<td>Windows VMware Image</td>
<td></td>
<td>nodes</td>
<td>AMP-3 Mgmt VM Image</td>
</tr>
<tr>
<td>Avamar Multi-Node</td>
<td>VxBlock Central MSM</td>
<td>AMP-3S VMware Image Dataset</td>
<td>Windows VMware Image</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VxBlock Central MSM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VxBlock Central Orchestration Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avamar Multi-Node</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PPMA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EM01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EM02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VxBlock System 1000 Administration Guide 221
The following table shows the backup schedule and retention period configuration for Avamar and NetWorker for AMP data protection:

<table>
<thead>
<tr>
<th>Name</th>
<th>Backup Frequency</th>
<th>Days</th>
<th>Start time</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMP-3S VMware vCenter Image Backup</td>
<td>Once daily</td>
<td>Sunday through Saturday</td>
<td>12:00 am</td>
<td>14 days</td>
</tr>
<tr>
<td>AMP-3S VxBlock Central Image Backup</td>
<td>Once daily</td>
<td>Sunday through Saturday</td>
<td>01:00 am</td>
<td>14 days</td>
</tr>
<tr>
<td>AMP-3S Mgmt Image Backup</td>
<td>Once daily</td>
<td>Sunday through Saturday</td>
<td>03:00 am</td>
<td>14 days</td>
</tr>
<tr>
<td>AMP-3S Mgmt Windows File System Backup</td>
<td>Once daily</td>
<td>Sunday through Saturday</td>
<td>04:00 am</td>
<td>14 days</td>
</tr>
</tbody>
</table>

**Avamar and NetWorker VMware vCenter Server user account**

Integrate the AMP management VMware vCenter Server with the Integrated Data Protection backup application to perform proxy-based image backups and restores of the management workload VMs.

**About this task**

A VMware vCenter Server user account with the appropriate privileges for authentication is required to integrate the management VMware vCenter Server with the Integrated Data Protection backup application. Although `administrator@vsphere.local` is sufficient, create a user account with only the necessary privileges for this task.
purpose. The management VMware vCenter Server has a user account (`dp-vcadmin@vsphere.local`) created for this reason.

To manage proxy-based image backup and recovery through VMware vCenter Server, use the backup applications plug-in for VMware vSphere Web Client. The plug-in provides a simple interface through the VMware vSphere web client for backup and restoration.

**Procedure**

1. To back up or restore through the backup applications plug-in, log in the VMware vSphere Web Client using the `dp-vcadmin@vsphere.local` user account.

**Application-specific scripted backups**

Besides Avamar backups, there are customized scripts to perform application-specific backups for certain VMs. The following VMs have customized scripts:

- VMware vCenter Server Appliance (vCSA)
- VMware Platform Services Controller (PSC)
- PowerPath Management Appliance
- Backup of the VMware vCenter Server database and VMware vSphere Distributed Switches (VDS)
- VMware vRO

These scripts reside on the element manager for data protection which has preconfigured tasks within Microsoft Task Scheduler for execution. The scheduled scripts execute backups through the applications native command-line. Backup file(s) are sent through the command-line to a repository on the element manager for data protection through FTP or SCP.

The backups performed by these scripts require an administrative username and password such as `admin`, `administrator@vsphere.local`, or `root`, as well as the FQDN and display name for the VMs to be backed up. During the factory logical build of the Integrated Data Protection backup solution, an interactive PowerShell script named `Configure-Credentials.ps1` was executed to update the `CPSD-DP-Settings.cfg` file with these inputs.

You can execute the same script to update or add the username, password, FQDN and display name of a protected VM. The script is on the element manager for data protection in `D:\DataProtection\BIN`.

Execute the script:

- To add another production VMware vCenter Server.
- When you change the `administrator@vsphere.local` or VMware vCSA root password.
- When you change the `root` or `admin` password of the Cisco DCNM or PowerPath Management Appliance instances.
- When you change the FQDN of Cisco DCNM or PowerPath Management Appliance instances.

All passwords entered and stored in the `CPSD-DP-Settings.cfg` file are stored in an encrypted format. For information on how passwords are encrypted, see "Password Security".

**Password security**

Passwords that are typed during `CPSD-Configure-Credentials.ps1` script execution are placed into a nonreadable variable as a `SecureString`.

When the password is typed as a `SecureString`, the password is encrypted with a 256-bit encryption key. The password is first read from an encryption key file, and written to `CPSD-DP-Settings.cfg`.

The `CPSD-Configure-Credentials.ps1` script checks if the encryption key file is located in `D:\DataProtection\PSW` on the data protection element manager. The encryption file contains the key that is used.
for the encryption of the passwords before they are written to CPSD-DP-Settings.cfg. If the encryption file is missing, the script automatically creates an encryption key file.

**Change administrator passwords**

Change passwords every six months, every quarter, or when key personnel are no longer employed.

When the administrator@vsphere.local password for VMware vCenter or the root password changes for Cisco DCNM or PowerPath Management Appliance, encrypted passwords in CPSD-DP-Settings.cfg must also change. Otherwise, system backups may be interrupted.

Later procedures update the CPSD-DP-Settings.cfg with the new passwords in the encrypted format. It also provides for changing of the hostname/FQDN, and display name for each VM.

**Update the CPSD-DP-Settings.cfg file**

Update the CPSD-DP-Settings.cfg with usernames, passwords, FQDNs, and display names for each VM.

**About this task**

You do not need to enter information at all prompts in the script. Current information is displayed at the prompts and may be accepted as if no changes are required. If the prompt requires new information, type the appropriate information and continue through the script.

**Before you begin**

For any system requiring updates, obtain the following:

- Display names
- FQDNs
- Usernames
- New passwords

Useful notes when running this script:

- To exit the script, type **N** at the first prompt.
- From the second prompt on, type **N** at any prompt to continue to the next prompt.
- At the appropriate prompt, select 1 - AMP-3S.
- At the appropriate prompt, select either AMP-3S with External PSCs or AMP-3S without External PSCs AMP Central without External PSCs.
- At the appropriate prompt, indicate if VxBlock Central is installed.
- Type **Y** at the **Would you like to enter the AMP credentials now? (Y/N)** prompt to change the display name, FQDN, username, and/or passwords for the following items:
  - FTP server (element manager for data protection)
  - VMware vCenter Server Appliance (vCSA)
  - Encryption password for VMware vCSA
  - VMware Platform Services Controllers (PSCs)
  - Encryption password for VMware PSCs
  - PowerPath Management Appliance
  - Cisco DCNM appliance
  - VMware vRealize Orchestrator
- When **Would you like to...?** is displayed, type the required information or type **N** to continue.
- Use only the provided script to update the configuration file.
**Procedure**

1. From the VMware vSphere Web Client console, log in to the data protection element manager as local Administrator.

2. Launch PowerShell as administrator and type:

   ```sh
   D:
cd \DataProtection\BIN
   .\CPSD-Configure-Credentials.ps1
   ```

3. The script reads CPSD-DP-Settings.cfg, and then requests the following input:

<table>
<thead>
<tr>
<th>System</th>
<th>FQDN example</th>
<th>Display name examples</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>M01EM01.abc.com</td>
<td>M01EM01</td>
<td>Windows server FTP user account:</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CPSD-DP-FTP</td>
<td></td>
</tr>
<tr>
<td>VMware vCSA</td>
<td>M01VCSA01.abc.com</td>
<td>M01VCSA01</td>
<td>Root username: root</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>VMware vCSA</td>
<td>M01VCSA01.abc.com</td>
<td>M01VCSA01</td>
<td>SSO username: <a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>VMware vCSA</td>
<td>M01VCSA01.abc.com</td>
<td>M01VCSA01</td>
<td>No username</td>
<td>Backup Encryption Password</td>
</tr>
<tr>
<td>VMware vCSA</td>
<td>M01VCSA01.abc.com</td>
<td>M01VCSA01</td>
<td>No username</td>
<td>Backup Encryption Password</td>
</tr>
<tr>
<td>VMware PSCs</td>
<td>M01PSC0&lt;1-2&gt;.abc.com</td>
<td>M01PSC0&lt;1-2&gt;</td>
<td>Root username: root</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>VMware PSCs</td>
<td>M01PSC0&lt;1-2&gt;.abc.com</td>
<td>M01PSC0&lt;1-2&gt;</td>
<td>SSO username: <a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>VMware PSCs</td>
<td>M01PSC0&lt;1-2&gt;.abc.com</td>
<td>M01PSC0&lt;1-2&gt;</td>
<td>No username</td>
<td>Backup Encryption Password</td>
</tr>
<tr>
<td>PowerPath Management Appliance</td>
<td>V01PPMA01.abc.com</td>
<td>V01PPMA01</td>
<td>Root username: root</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>Cisco DCNM</td>
<td>V01DCNM01.abc.com</td>
<td>V01DCNM01</td>
<td>Root username: root</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>VMware vRealize Orchestrator</td>
<td>V01VRO01.abc.com</td>
<td>V01VRO01</td>
<td>Root username: root</td>
<td>&lt;new_password&gt;</td>
</tr>
</tbody>
</table>

**Create the scheduled tasks for all backups**

Update Microsoft scheduled tasks for backups if: changes are made to the FQDN or display name, or if production VMware vCenter Servers are added or removed during execution CPSD-Configure-Credentials.ps1.

**Procedure**

1. Log in to the element manager data protection VM as local Administrator using the console from within the VMware vSphere web client.
2. Launch PowerShell as administrator and type:

```
D:
cd \DataProtection\BIN
.CPSD-Create-Scheduled-Tasks.ps1
```

3. To verify that the scheduled tasks were created, right-click Start > Run, type `Taskschd.msc` and click OK.

4. In the left window, select Task Scheduler Library.

Each backup task is scheduled in 5 minute increments. The script checks for the existence of scheduled tasks with the text CPSD-backup in the name. If any tasks are found, the script prompts you to proceed. The script deletes the existing CPSD-backup tasks and re-creates them with the data from CPSD-DP-Settings.cfg.

**Backup types and scripted backup locations**

Scripted application file backups that are sent to the element manager for Integrated Data Protection back up to Avamar and Data Domain.

Scripted application file backups back up through the Avamar image backup and Avamar client file-level backup of the element manager for data protection.

The following table provides backup information:

<table>
<thead>
<tr>
<th>Workload VM</th>
<th>Scripted application file backup</th>
<th>Backup location</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vCenter Server Appliance</td>
<td>Yes</td>
<td>D:\DataProtection\backup\VCSA</td>
</tr>
<tr>
<td>VMware Platform Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controllers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMware vCenter Server database</td>
<td>Yes</td>
<td>D:\DataProtection\backup\VCSA-DB</td>
</tr>
<tr>
<td>VMware VDS</td>
<td>Yes</td>
<td>D:\DataProtection\backup\VCSA-VDS</td>
</tr>
<tr>
<td>PowerPath Management Appliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMware vRO</td>
<td>Yes</td>
<td>D:\DataProtection\backup\VxBC-vRO</td>
</tr>
</tbody>
</table>

**Establish Avamar image backups for restored VMs**

Establish the Avamar Image backups of restored VMs.

**Procedure**

1. From the Avamar administrator console, select Administration launch.
2. Select vCenter > Virtual Machines.
3. Right-click the restored VM name and select Retire Client with the default settings.
4. Select vCenter > Virtual Machines.
5. Right-click Virtual Machines > New Client.
6. Select the Hosts and Clusters tab and go to the AMP cluster.
7. Select the restored VM, ensure Enable Changed Block Tracking is selected and click OK.
8. From the Avamar administrator console, click Policy.
9. Select vCenter > Virtual Machines.
10. Use the following table to click the appropriate group and click **Edit**:

<table>
<thead>
<tr>
<th>VM</th>
<th>Group Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element manager for storage arrays</td>
<td>AMP-3S Mgmt VM Image</td>
</tr>
<tr>
<td>Element manager for data protection</td>
<td>AMP-3S Mgmt VM Image</td>
</tr>
<tr>
<td>Cisco DCNM</td>
<td>AMP-3S Mgmt VM Image</td>
</tr>
<tr>
<td>PowerPath Management Appliance</td>
<td>AMP-3S Mgmt VM Image</td>
</tr>
<tr>
<td>Core MSM</td>
<td>AMP-3S VxBlock Central VM Image</td>
</tr>
<tr>
<td>MSP</td>
<td>AMP-3S Mgmt VM Image</td>
</tr>
<tr>
<td>VMware vRO</td>
<td>AMP-3S Mgmt VM Image</td>
</tr>
<tr>
<td>VxBlock Central Orchestration Services</td>
<td>AMP-3S Mgmt vCenter Image</td>
</tr>
<tr>
<td>VMware vCSA for management</td>
<td>AMP-3S Mgmt vCenter Image</td>
</tr>
</tbody>
</table>

11. In the **Edit Group** console, select the **Members** tab.

12. Select the restored VM and click **Include** and **OK**.

**Establish NetWorker image backups for restored VMs**

Establish NetWorker image backups for restored VMs.

**Procedure**

1. Launch the NetWorker Management Console and then the NetWorker Administration Console.
2. Select the **Protection** tab.
3. Right-click the **VMware** view and select **Refresh** to ensure that the restored VM has been discovered.
4. Expand groups and select the appropriate group for the VM that was restored based on the following table:

<table>
<thead>
<tr>
<th>VM</th>
<th>Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element manager for storage arrays</td>
<td>AMP-3S Mgmt VM Image</td>
</tr>
<tr>
<td>Element manager for data protection</td>
<td>AMP-3S Mgmt VM Image</td>
</tr>
<tr>
<td>Cisco DCNM</td>
<td>AMP-3S Mgmt VM Image</td>
</tr>
<tr>
<td>PowerPath Management Appliance</td>
<td>AMP-3S Mgmt VM Image</td>
</tr>
<tr>
<td>VxBlock Central Core, MSM, and MSP</td>
<td>AMP-3S VxBlock Central VM Image</td>
</tr>
<tr>
<td>VMware vRO</td>
<td>AMP-3S VxBlock Central VM Image</td>
</tr>
<tr>
<td>VxBlock Central Orchestration Services</td>
<td>AMP-3S VMware vRealize Operations Manager</td>
</tr>
<tr>
<td>VxBlock Central VMware vRealize Operations Manager</td>
<td>AMP-3S VMware vRealize Operations Manager</td>
</tr>
<tr>
<td>VMware vCSA</td>
<td>AMP-3S vCenter Image</td>
</tr>
<tr>
<td>VMware PSCs</td>
<td>AMP-3S vCenter Image</td>
</tr>
</tbody>
</table>

5. Right-click the group and select **Properties**.
6. Under **VMware**, expand **VMware View**. Locate and select the restored VM, and click **OK**.
Enable the scripted backup configuration

Enable backups for the management PowerPath Management Appliance (PPMA) or any of the VMware vCenter Server Appliance (vCSA).

About this task

After updating the settings file, run the .\CPSD-Create-Scheduled-Tasks.ps1 script. This script creates scheduled tasks for the backups and creates scheduled tasks to configure the PPMA and VMware vCSA for backups.

Procedure

1. Log in to the data protection element manager VM, as local Administrator using the console within the VMware vSphere Web Client.
2. Right-click the Start > Run, type tasksched.msc and click OK.
3. Click Task Scheduler Library.
4. Scroll down the list of scheduled tasks in the middle pane and locate tasks that start with CPSD-Reconfigure.
5. From the list of CPSD-Reconfigure tasks, locate the correct application (PPMA or VMware vCSA) and environment (AMP).
6. Right-click the scheduled task and click Run.
7. When the task is complete, in the Last Run Results column, the following message should open:
   The operation completed successfully (0x0)

   If this message is not displayed, verify:
   • The appliance is powered up and has finished booting.
   • The appliance is reachable by the ping command when using the FQDN. If the FQDN has changed, see Update the CPSD-DP-Settings.cfg file with new usernames, passwords, FQDNs, and display names to run the configure credentials script.
   • The username and password is the same as they were before the restore. If the credentials were changed, see Update the CPSD-DP-Settings.cfg file with new usernames, passwords, FQDNs, and display names to run the configure credentials script.
8. After the restored appliance has been reconfigured, scheduled backups resume.