## Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Document revision</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2018</td>
<td>1.3</td>
<td>Additional features available on VxBlock Systems.</td>
</tr>
<tr>
<td>July 2018</td>
<td>1.2</td>
<td>3.6.2 release of the product.</td>
</tr>
<tr>
<td>March 2018</td>
<td>1.1</td>
<td>3.6.1 release of the product.</td>
</tr>
<tr>
<td>January 2018</td>
<td>1.0</td>
<td>New release of the product.</td>
</tr>
</tbody>
</table>
Contents

Introduction.................................................................................................................................................7

Viewing third party licenses...................................................................................................................... 8

Setting up a VCE System........................................................................................................................... 9
  Accepting the end user license agreement (EULA).............................................................................. 9
  Starting discovery.................................................................................................................................10
    Confirming discovery is complete.................................................................................................. 11
  Updating the Windows Registry........................................................................................................... 12

Managing multiple VCE Systems in a clustered environment.............................................................15
  Planning a multisystem clustered environment.............................................................................. 15
  Associating a Vision Core VM with an existing MSM VM.............................................................. 16
  Forming a cluster of MSM VMs............................................................................................................ 18
  Removing a Vision Core VM from an MSM VM................................................................................... 23
  Shutting down and taking a snapshot of the MSM cluster................................................................... 24
  Recovering the MSM cluster................................................................................................................ 25

Configuring Vision software for discovery............................................................................................ 27
  Configuring Vision software to discover Vblock System components.............................................. 27
    Adding Network Attached Storage (eNAS) to VMAX3 on a Vblock System.................................. 27
    Adding Isilon Technology Extension on a Vblock System.............................................................. 28
  Configuring Vision to discover VxBlock System and VxRack System components.............................30
    Configuration editor overview........................................................................................................ 31
    Configuring a VxBlock System or a VxRack System using the configuration editor......................33
    Editing component credentials with the configuration editor....................................................... 33
    Adding a component with the configuration editor....................................................................... 35
    Adding Network Attached Storage (eNAS) to VMAX3 on a VxBlock System................................ 36
    Deleting a component with the configuration editor...................................................................... 38
    Configuration editor component reference.................................................................................. 38
  Configuring Vision software to discover a VxRail Appliance............................................................ 49
    Configuring a VxRail Appliance using the configuration editor.................................................... 49
    Modifying the configuration file for a VxRail Appliance using the configuration editor
      (attended mode)......................................................................................................................... 52
    Modifying the configuration file for a VxRail Appliance using the configuration editor
      (unattended mode).................................................................................................................... 54

Using the Vision dashboard.................................................................................................................... 57
  Vision dashboard overview................................................................................................................... 57
  Vision dashboard layout....................................................................................................................... 57
  Accessing the Vision dashboard........................................................................................................... 59

Using the Vision Shell.............................................................................................................................. 61
  Vision shell........................................................................................................................................... 61
  Accessing the Vision shell session...................................................................................................... 61
  Running Vision shell from a remote host............................................................................................ 63
  Getting started with shell commands................................................................................................. 63
Working with components in Vision shell................................................................. 65
Working with switches............................................................................................... 65
Working with storage................................................................................................... 69
Working with compute systems.................................................................................. 71
Working with VMware ESXi hosts............................................................................. 74
Viewing Vision shell logs........................................................................................... 77
Viewing Vision shell jobs............................................................................................ 78

Command reference..................................................................................................... 79
Vision Core VM commands......................................................................................... 79
MSM VM commands.................................................................................................... 81
MSP VM commands.................................................................................................... 82

Managing security....................................................................................................... 83
Managing credentials................................................................................................. 83
  Changing the default password for the root and vision accounts............................... 83
  Using the non-administrator account......................................................................... 85
  Changing the Central Authentication Service (CAS) password for Vision Core VM........ 86
  Changing the Central Authentication Service (CAS) password for multi-system management (MSP).................................................................................................................. 87
  Synchronizing the CAS password for the admin user in a clustered environment......... 89
  Changing the CAS password for the MSP VM to match the CAS password on the MSM VM...... 90
  Creating users with access rights to storage components............................................ 91
  Changing access credentials for a component on a Vblock System............................. 92
  Changing access credentials for a component on a VxBlock system or a VxRack System .... 94
  Changing the password for the Vision shell administrator.......................................... 96
Managing third party certificates................................................................................ 97
  Using a third party signed certificate on the Vision Core VM...................................... 97
  Using a third party signed certificate on the MSM VM................................................ 100
Integrating Vision software with Active Directory..................................................... 102
  Overview of Active Directory integration.................................................................... 102
  Configuring Active Directory..................................................................................... 104
  Mapping roles to Active Directory groups................................................................. 105

Ensuring VCE System compliance........................................................................... 107
Compliance overview............................................................................................... 107
Managing compliance across all VCE Systems......................................................... 108
Assessing the results of a compliance scan............................................................. 109
Using Vision software to download RCM content..................................................... 110
  Working with the multisystem prepositioning (MSP) VM........................................... 110
  Download process..................................................................................................... 112
  Configuring connection and download settings......................................................... 113
  Managing credentials for RCM Content Pre-positioning............................................ 118
  Downloading RCM content using the Vision dashboard............................................ 121
  Accessing downloaded RCM content....................................................................... 121
  Troubleshooting....................................................................................................... 123
Remediating security issues using the Vision shell..................................................... 125
  Compute system security compliance checks............................................................ 126
  Networking security compliance checks................................................................... 127
Table of Contents

Monitoring resources ................................................................................................................................. 134
  Health monitoring ................................................................................................................................. 134
    How health is calculated ....................................................................................................................... 135
    Monitoring the health of VCE Systems and components ..................................................................... 136
    Locating the source of a health issue .................................................................................................... 136
  Monitoring events and log messages ..................................................................................................... 138
    Monitoring and filtering events ............................................................................................................ 138
    Syslog messaging ................................................................................................................................. 138
    Changing syslog rotation parameters .................................................................................................... 138
    Forwarding syslog messages to remote servers ................................................................................... 139
    Monitoring VM resources ..................................................................................................................... 142

Working with SNMP .................................................................................................................................. 145
  Overview of SNMP ................................................................................................................................ 145
  Provisioning the SNMP name, location, and contact information fields for your VCE System ............. 145
  Using SNMP traps events and CIM indications .................................................................................... 146
    Accessing traps events and CIM indications ......................................................................................... 146
  Communicating with the Network Management System ......................................................................... 148
  Sending SNMP traps in readable format ................................................................................................. 148
  List of generated traps ............................................................................................................................ 150

Changing settings on a VCE System .......................................................................................................... 151
  Changing discovery and health polling intervals .................................................................................... 151
  Customizing logon banners for the Vision Core VM .............................................................................. 152

Using the search tools ............................................................................................................................... 153
  Tools for searching ................................................................................................................................. 153
  Searching within Vision shell .................................................................................................................. 153
  Combining search with Vision shell commands ..................................................................................... 162

Working with key performance indicators (KPI) ..................................................................................... 164
  KPI overview ......................................................................................................................................... 164
  Accessing KPI information ................................................................................................................... 164

Working with Secure Remote Services (ESRS) .................................................................................... 166
  Configuring ESRS ................................................................................................................................. 166
    Registering Vision software with an ESRS gateway ........................................................................... 166
    Adding a software identifier for an MSM VM ....................................................................................... 169
    Retrieving the software ID from the Licensing system ....................................................................... 170
    Updating an ESRS gateway configuration or software identifier (SWID) ........................................... 171
    Updating a software identifier (SWID) (for Dell EMC employees only) ............................................. 172
    Deregistering Vision software with ESRS ............................................................................................ 173
  Sending information to ESRS ................................................................................................................ 174
    Manually uploading information to ESRS ........................................................................................... 175
    Viewing the current ESRS upload schedule ......................................................................................... 176

Storage security compliance checks ........................................................................................................ 131
Virtualization security compliance checks ................................................................................................ 132
VCE System security compliance checks ................................................................................................. 132
Working with compliance on Vision Core ............................................................................................... 133

Monitoring resources ................................................................................................................................. 134
Health monitoring ......................................................................................................................................... 134
How health is calculated ............................................................................................................................. 135
Monitoring the health of VCE Systems and components .......................................................................... 136
Locating the source of a health issue .......................................................................................................... 136
Monitoring events and log messages .......................................................................................................... 138
Monitoring and filtering events ................................................................................................................ 138
Syslog messaging ....................................................................................................................................... 138
Changing syslog rotation parameters ......................................................................................................... 138
Forwarding syslog messages to remote servers ........................................................................................ 139
Monitoring VM resources .......................................................................................................................... 142

Working with SNMP ..................................................................................................................................... 145
Overview of SNMP ...................................................................................................................................... 145
Provisioning the SNMP name, location, and contact information fields for your VCE System .............. 145
Using SNMP traps events and CIM indications ....................................................................................... 146
Accessing traps events and CIM indications ............................................................................................ 146
Communicating with the Network Management System .......................................................................... 148
Sending SNMP traps in readable format ................................................................................................. 148
List of generated traps ............................................................................................................................... 150

Changing settings on a VCE System .......................................................................................................... 151
Changing discovery and health polling intervals .................................................................................... 151
Customizing logon banners for the Vision Core VM ............................................................................... 152

Using the search tools ............................................................................................................................... 153
Tools for searching ...................................................................................................................................... 153
Searching within Vision shell .................................................................................................................. 153
Combining search with Vision shell commands ........................................................................................ 162

Working with key performance indicators (KPI) ....................................................................................... 164
KPI overview ............................................................................................................................................... 164
Accessing KPI information ........................................................................................................................ 164

Working with Secure Remote Services (ESRS) ....................................................................................... 166
Configuring ESRS ....................................................................................................................................... 166
Registering Vision software with an ESRS gateway .................................................................................. 166
Adding a software identifier for an MSM VM ............................................................................................ 169
Retrieving the software ID from the Licensing system ............................................................................ 170
Updating an ESRS gateway configuration or software identifier (SWID) .............................................. 171
Updating a software identifier (SWID) (for Dell EMC employees only) ................................................ 172
Deregistering Vision software with ESRS .................................................................................................. 173
Sending information to ESRS ................................................................................................................ 174
Manually uploading information to ESRS ................................................................................................ 175
Viewing the current ESRS upload schedule ............................................................................................ 176
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modifying the schedule used to send information to ESRS</td>
<td>178</td>
</tr>
<tr>
<td>Securing the connection between Vision software and ESRS</td>
<td>179</td>
</tr>
<tr>
<td>Troubleshooting ESRS connectivity issues</td>
<td>180</td>
</tr>
<tr>
<td>Managing software modules</td>
<td>181</td>
</tr>
<tr>
<td>Roles and operations for Software Module Manager</td>
<td>182</td>
</tr>
<tr>
<td>Managing software modules using the Vision dashboard</td>
<td>182</td>
</tr>
<tr>
<td>Managing software modules using the Vision shell</td>
<td>182</td>
</tr>
<tr>
<td>Vision shell commands</td>
<td>183</td>
</tr>
<tr>
<td>Log files for the Software Module Manager</td>
<td>184</td>
</tr>
<tr>
<td>Configuring audit log properties</td>
<td>184</td>
</tr>
<tr>
<td>Software Module Manager message identifiers</td>
<td>185</td>
</tr>
<tr>
<td>Collecting logs</td>
<td>185</td>
</tr>
<tr>
<td>Devices for log collection</td>
<td>185</td>
</tr>
<tr>
<td>Using the Vision dashboard</td>
<td>186</td>
</tr>
<tr>
<td>Using the REST API</td>
<td>187</td>
</tr>
<tr>
<td>Backing up and restoring</td>
<td>188</td>
</tr>
<tr>
<td>Backing up and restoring the Vision Core VM</td>
<td>188</td>
</tr>
<tr>
<td>Vision Core software backups</td>
<td>188</td>
</tr>
<tr>
<td>Backing up configuration files on demand</td>
<td>190</td>
</tr>
<tr>
<td>Backing up databases on demand</td>
<td>192</td>
</tr>
<tr>
<td>Restoring the Vision software configuration</td>
<td>192</td>
</tr>
<tr>
<td>Restoring databases</td>
<td>194</td>
</tr>
<tr>
<td>Backing up the Vision Core VM</td>
<td>195</td>
</tr>
<tr>
<td>Backing up and restoring the MSM VM</td>
<td>195</td>
</tr>
<tr>
<td>Backing up and restoring the MSP VM</td>
<td>196</td>
</tr>
<tr>
<td>Backing up component configuration files</td>
<td>196</td>
</tr>
<tr>
<td>How VCE System backups work</td>
<td>196</td>
</tr>
<tr>
<td>Appendix</td>
<td>200</td>
</tr>
<tr>
<td>System requirements</td>
<td>200</td>
</tr>
<tr>
<td>Ports and protocols</td>
<td>201</td>
</tr>
<tr>
<td>Open port assignments</td>
<td>201</td>
</tr>
<tr>
<td>Northbound ports and protocols</td>
<td>203</td>
</tr>
<tr>
<td>Southbound ports and protocols</td>
<td>204</td>
</tr>
<tr>
<td>Configuring the NTP server</td>
<td>205</td>
</tr>
<tr>
<td>Verifying the Elasticsearch configuration</td>
<td>206</td>
</tr>
</tbody>
</table>
Introduction

This document provides information needed to manage one or more VCE Systems and to perform administrative tasks with the Dell EMC Vision Intelligent Operations suite of software.

The target audience for this document is the person responsible for managing one or more VCE Systems in a data center.

The Glossary provides terms, definitions, and acronyms that are related to VCE Systems.
Viewing third party licenses

The third-party license document provides a list of the third party software used to create the Vision software and the associated licenses.

The third party licenses document for Vision software is available directly on the Vision Core VM.

Before you begin

Ensure the Vision Core VM is running.

Procedure


   Where FQDN is the fully qualified domain name of the Vision Core VM.

2. Accept the security certificate, if prompted.

Results

The third party licenses PDF document opens.
Setting up a VCE System

VCE Systems have a Vision Core, multi-system management VM (MSM VM), and a multi-system prepositioning VM (MSP VM) deployed and configured as part of the installation process.

**Vision Core VM**

The Vision Core VM provides a set of REST resources that give customers the ability to access data in System Library.

**MSM VM**

In a data center environment with one or more VCE Systems, each VCE System may contain an MSM VM.

**MSP VM**

The MSP VM is responsible for providing the functions required for the RCM content prepositioning feature.

**Important:** Only one MSP VM must be deployed and configured within a cluster. The MSP VM must be associated with the MSM VMs in its local data center for that cluster. If other MSP VMs have been deployed and configured, you must power down these VMs.

**Accepting the end user license agreement (EULA)**

After the VCE System is delivered, you must accept the EULA to enable discovery and health polling. Vision software does not discover VCE System components or poll for health status until you accept the EULA.

**About this task**

You must accept the EULA on each VCE System in your environment.

Accepting the EULA involves running a command on the Vision Core VM. You must then 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 Vision Core VM.

**Procedure**

1. Run the following command:

   ```
   startEulaAcceptance
   ```

   The EULA displays in the terminal window.

2. Scroll through the EULA until you are prompted to enter a name. The prompt to enter a name is as follows: *Enter 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 when prompted. A message such as the following displays:

   Do you accept the End User License Agreement:[yes/no]> yes
   Softcopy of End User License Agreement File created in: /opt/vce/fm/eula/
   VCE_EULA_V3_0.txt
   time_stamp EULA has been accepted.

### Starting discovery

After you accept the end user license agreement (EULA), start the discovery process so that System Library can connect to and start polling components.

**About this task**

Starting discovery involves running a script on the Vision Core VM.

**Before you begin**

- Accept the EULA.
- Connect to the Vision Core VM.

**Procedure**

Run the following command:

`startFMagent`

The FM Agent services start. The following example shows the messages that display in the console:

```bash
[user@hostname log]$ startFMagent
Enabling FMagent services to start automatically...
Waiting for the FMagent services to start.................
vce-fm-master is running (pid=19357)
vce-fm-adapter is running (pid=19871)
vce-fm-agent is running (pid=20130)
vce-fm-net-snmpd (pid=19617) is running
vce-fm-naaagent is running (pid=20409)
```

**Related information**

- [Adding a component with the configuration editor](#) (see page 35)
Confirming discovery is complete

After starting the process to discover components in your VCE System using Vision software, you should wait approximately 15 minutes and confirm the discovery process is complete.

About this task

You can check `FMAgent.log` to determine if discovery is complete. Confirm that the Vision API for System Library returns details for your VCE System.

Before you begin

Connect to the Vision Core VM.

Procedure

1. Run the following command:

   ```bash
   cd /opt/vce/fm/logs/
   ```

2. Run the following command:

   ```bash
   grep -i 'current status' FMA* | grep 100 | grep discoverAll
   ```

   The command searches `FMAgent.log` for messages that indicate discovery is complete, as follows:

   ```
   INFO time_stamp [thread_pool] : VblockDiscoveryTask -
   Current status of Vblock System discoverAll: started at time_stamp with 100% finished,
   Current finishing component:
   INFO time_stamp [thread_pool] : FMEventServiceFactory - publish event: id=Vblock
   System all
   Current status of Vblock System discoverAll: started at time_stamp with 100% finished,
   Current finishing component:
   ```

3. Open a web browser and navigate to the following URL:

   - `https://FQDN:8443/fm/vblocks` for a Vblock System, or
   - `https://fqdn:8443/fm/systems` for a VxBlock System or a VxRack System.

   Where `FQDN` is the fully qualified domain name of the Vision Core VM.
4 Authenticate to the Central Authentication Service (CAS) service.

The API for System Library returns details for the VCE System components, as in the following XML snippets:

```xml
<vblocks>
  <vblock>
    <alias>model_number</alias>
    <dbId>5188</dbId>
    <description>340w5400 (Vblock 340w5400)</description>
    <moId>serial_number</moId>
    <name/>
    <url>https://FQDN:8443/fm/vblocks/6188</url>
    <assetId/>
    <calculatedStatus>major</calculatedStatus>
    <firmwareRev/>
    <fru>false</fru>
    <hardwareRev/>
    <lastOperStatus>critical</lastOperStatus>
    <lastStatusChange>time_stamp</lastStatusChange>
  </vblock>
</vblocks>

<systems>
  <system>
    <alias>VxRack1000FLEX</alias>
    <dbId>5188</dbId>
    <description>VxRack VCE System</description>
    <moId>VX1032-975-318-642</moId>
    <name/>
    <uniqueId>VX1032-975-318-642</uniqueId>
    <url>https://fqdn:8443/fm/systems/5188</url>
    <assetId/>
    <calculatedStatus>critical</calculatedStatus>
    <firmwareRev/>
    <fru>false</fru>
    <hardwareRev/>
    <lastOperStatus>notApplicable</lastOperStatus>
    <lastStatusChange>time_stamp</lastStatusChange>
  </system>
</systems>
```

**Updating the Windows Registry**

Before configuring Application Hosts on the Vision 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 Advanced Management Platform (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 have 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. Run `regedit` to start the registry editor.

3. Search for `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID \{76A64158-CB41-11D1-8B02-00600806D9B6}`.

**NOTE:** Ensure the brackets are included.

4. Right-click the key and select **Permissions**.

5. On the **Permissions** window, click **Advanced**.

6. On the **Advanced Security Settings** window, change the Owner.

   - For Windows 2008: Select the **Owner** tab, and click **Other users or groups**.
   
   - For Windows 2012: Select **Change**.

7. In the **Select User or Group** window, from the **From this location** field, ensure the location is your local computer.

8. From the **Select User or Group** window, type **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 the checkbox for **Full Control**. Click **OK**.

10. Right-click key `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID \{76A64158-CB41-11D1-8B02-00600806D9B6}`.

**NOTE:** Ensure the brackets are included.

11. Select **New > String value** and enter **AppID** for the name. Right-click and modify the **AppID**, and set the value to `{76A64158-CB41-11D1-8B02-00600806D9B6}`.

**NOTE:** Ensure the brackets are included.
12 Set the Owner and Permissions back to the original settings:

   a Right click on the key HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}, and select Permissions.

      NOTE: Ensure the brackets are included.

   b Remove the Full Control permissions for the Administrators group.

   c Click Advanced.

      — For Windows 2008: Select the Owner tab, and click Other users or groups.

      — For Windows 2012: Select Change.

   d In the Select User or Group window, from the From this location field, ensure 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 on the key, and select New > Key, and enter {76A64158-CB41-11D1-8B02-00600806D9B6}, for the name.

   NOTE: Ensure the brackets are included.

15 Right click on the new key, and select New > String value, and type DllSurrogate for the name and leave the value empty.
Managing multiple VCE Systems in a clustered environment

You can configure a data center environment that supports multiple VCE Systems.

Planning a multisystem clustered environment

This section provides sizing guidelines you can use to plan a multisystem clustered environment. If your deployment configuration exceeds the guidelines provided below, the system performance will degrade and the MSM cluster may be unsupported.

When planning an MSM cluster deployment, you need to ensure that the topology (including the data centers and VCE Systems involved) is well defined. Some sizing guidelines from testing are listed as a reference.

Single-site and multi-site environments

In general, if your VCE System has AMP resources to support the Vision Core and MSM VMs, Dell EMC recommends a configuration with multiple MSM VMs clustered together, rather than a configuration with multiple Vision Core VMs mapped to a single MSM VM.

The following sizing restrictions apply to single-site and multi-site configurations:

- In a single-site environment, an MSM VM may be associated with up to two Vision Core VMs. In a single-site configuration, each data center may have no more than three MSM VMs running, where each MSM VM is associated with up to two Vision Core VMs.

- In a multi-site environment, you can configure a cluster that includes a maximum of three data centers. In a multi-site configuration with three data centers, each data center may have no more than two MSM VMs running, where each MSM VM is associated with up to two Vision Core VMs.

In single-site cluster deployments, where three MSM nodes are supported, the failure of a single MSM node will not negatively impact read and write operations in the environment. A minimum of two MSM nodes should be operational to prevent data consistency problems.

In multi-site cluster deployments, where two MSM nodes are supported within each site, the failure of a single MSM node will impact read and write operations in that particular site only.

In a multi-site cluster deployment, there is no fault tolerance. If there is a network connectivity failure between the sites, this failure could negatively impact operations on all sites.

Latency

WAN latency is defined as the latency between data centers in multi-data center deployments. LAN latency is defined as the latency between MSM nodes within a data center.

The following latency restrictions apply:

- In a multi-site environment, Dell EMC does not recommend exceeding 100 ms of WAN Latency between data centers in a three data center deployment.

- From our reference deployment, Dell EMC can recommend 300ms of WAN Latency in a two data center deployment, with two MSM nodes, and four Vision Core VMs.
In a single-site environment, Dell EMC does not recommend exceeding 25 ms of LAN Latency between any two MSM nodes in a data center.

**VCE Systems**

The following sizing guidelines apply to the number of VCE Systems in a clustered environment:

- Dell EMC recommends no more than 12 VCE Systems in an MSM cluster if configured in a three data center deployment.
- Dell EMC recommends no more than two VCE Systems in a node with a maximum of one VMAX per MSM node. We also recommend that no more than one Fabric Technology Extension be attached in the two system node. A VMAX Storage Technology Extension or Fabric Technology Extension is not recommended on a VMAX based VCE System.
- Our reference deployment contains a VMAX with 5000 Storage Volumes and 390 disks. If your VMAX is anticipated to exceed 5000 Storage Volumes and 390 Disks, MSM cluster performance may degrade and Dell EMC recommends reducing the total number of Vision Core VMs in the deployment. The Dell EMC test environment had up to 10,000 storage volumes and 900 disks.

**Simultaneous users**

Dell EMC recommends fewer than three simultaneous users per MSM node.

**LDAP configuration**

In a large data center environment that spans multiple geographical locations, the Active Directory configuration would typically be replicated to all locations. To prevent MSM from going across geographical lines to perform Active Directory look ups, you can use local DNS practices. This will ensure that each MSM node is able to access the local Active Directory server to perform look ups.

System response time is impacted by the total number of groups an LDAP user belongs to. Our reference testbed included 13 groups for a given LDAP user.

**CPU**

If you experience performance degradation, you should increase the number of CPU cores. The default number of cores on the MSM VM is four.

**Associating a Vision Core VM with an existing MSM VM**

You can associate a Vision Core VM (System Library host) with an existing MSM VM after the initial MSM deployment. You can also add a Vision Core VM after a cluster of MSM VMs has been formed.

ℹ️ **NOTE:** You can skip this section if you have followed the Simplified Vision Configuration procedure.

**About this task**

The MSM VM provides a wrapper script called `addSlibHost.sh` that allows you to add the IP address of a Vision Core VM to an MSM VM. In a single system environment where one Vision Core VM is mapped to a single MSM VM, you should only execute the `addSlibHost.sh` script if either the **Optional Initial System Library IP(s)** OVF property is not configured, or if the property is configured, and there were failures adding the Vision Core VM on MSM first boot.
To ensure your environment can successfully add a Vision Core VM to an existing MSM VM, you can run a pre-check option of the script by running the following command:

```
/opt/vce/multivbmgmt/install/addSlibHost.sh -p IP_address
```

The `-p` option runs the pre-check logic but does not add the Vision Core VM to the MSM VM.

When associating a Vision Core VM to an MSM VM, no other operations should be performed on that Vision 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 Vision Core VM is already associated with your MSM VM, ensure the Vision Core VM is configured to use NTP. To do that, you must set the NTP server on the Vision Core VM. To configure the Vision Core VM to use NTP, run the following command:

```
/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 Vision Core VM, it does not add it to the MSM VM.

### Before you begin

You must set up NTP in the MSM VM. Refer to the related topic for more information.

Before you associate a Vision Core VM with an MSM VM, you must take a snapshot of each MSM VM within the cluster. In addition, you must ensure that the firstboot script has completed successfully on the MSM VM where you will be adding the Vision Core VM, and the subsequentboot script must not still be in progress. To access the logs, navigate to `/opt/vmware/var/log/firstboot` and `/opt/vmware/var/log/subsequentboot`.

Before you associate a Vision Core VM with an MSM VM, ensure that the following conditions are true:

- The version of the System Library is the same version as the MSM VM.
- The number of VCE Systems to associate with an MSM VM cannot exceed four.
- The serial number of the Vblock System can be added once. Each serial number must be unique.
- You can only have one Vblock System 7xx with VMAX.

**NOTE:** The addSlibHost script performs checks on the previous criteria when you run the script. If your environment does not meet these criteria, the addSlibHost script provides you with the reason it failed and does not allow the Vision Core VM to be added.

To ensure discovery is complete, open a web browser and navigate to the following URL: `https://FQDN:8443/fm/vblocks`, where `FQDN` is the fully qualified domain name of the Vision Core VM.
Procedure

Run the following command to add the Vision Core VM to an existing MSM VM:

```
/opt/vce/multivbmgmt/install/addSlibHost.sh IP_address
```

You can 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.

Related information

[Configuring the NTP server](#) (see page 205)

**Forming a cluster of MSM VMs**

The initial MSM deployment configures a single VM. After the deployment of 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

You can configure a cluster for a single-site or a multi-site environment. If you are configuring a cluster for a single-site environment, the MSM VMs will be located in the same data center. If you are configuring a cluster for a multi-site environment, the MSM VMs will be located in different data centers. You can mix various types of VCE Systems within a single-site or multi-site clustered environment.

You must join MSM VMs to a cluster one at a time, each time joining the same seed node. You cannot join existing clusters together.

**Important:** Once an MSM VM has been added to a cluster, it cannot be removed from the cluster.

Before you begin

- Ensure that all MSM VMs for the cluster you want to join have been deployed, powered on, and configured before joining the cluster. Take a snapshot of each node before clustering, and after each node is successfully added to the cluster. For details, see the related topic on shutting down and taking a snapshot of the MSM cluster.

  **NOTE:** The value for the FQDN for each MSM VM must not contain underscores or other special characters. Only hyphens and periods are accepted as special characters.

  **NOTE:** The value for the data center name(s) and cluster name must begin with an alphanumeric character, and can only contain numbers, letters, and underscores. These values must not exceed 255 characters.

- If you are configuring a cluster for a single-site environment, ensure that the data center name is exactly the same for all nodes within the cluster. This includes capitalization.

  **NOTE:** Data centers with the same name but different capitalization, for example, ‘Cork_DC’ on MSM 1 and ‘Cork_Dc’ on MSM 2, will initiate multi-data center clustering.
• If you are configuring a cluster for a multi-site environment, ensure that each site is distinguished by its data center name. Within each site, ensure that all MSM VMs use the exact same data center name.

• Ensure that the cluster name is the same across all MSM VMs within the cluster and across all sites.

**NOTE:** The data center name(s) and cluster name cannot be changed after you power on the VMs. If you need to change the data center name(s) or the cluster name, you need to redeploy all the VMs within the cluster.

• In a multi-site 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 all of the MSM VMs that join to the cluster have the same MSM CAS password.

**Procedure**

To add a node to the cluster:

1. Use DNS best practices to ensure that the FQDNs for all MSM VMs and Vision Core VMs are resolvable across all data centers.

   **NOTE:** From each MSM VM, you must be able to resolve the FQDN of any of the Vision Core VMs that have been added, regardless of which MSM VM it was added to.

2. Run the following command on all nodes that will be part of the cluster, including the node that is being added:

   ```bash
   /opt/vce/multivbmgmt/install/docompact_schemas.sh 1000 30
   ```

   The first parameter of 1000 specifies the threshold of open files that will be allowed in Cassandra before compaction begins. If the total number of files that are currently open in Cassandra is greater than the value of this parameter, compaction will begin.

   To check the total number of files currently open, run this command:

   ```bash
   lsof -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 will 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 will start.
3 Run the following command on any node that is being clustered to disable the repair cron jobs:

```
/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 within 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, you must include them all, separated by commas.

4 Run the following command on the seed node in the cluster:

```
cat /opt/vce/credential-management/deploy/conf/AOtRN.dat
```

This will retrieve the Credential Manager key for the cluster you want to join. You need to provide this key when you join a new node to the cluster.

5 Run the following command on the next MSM VM that you want to add to the cluster:

```
/opt/vce/multivbmgmt/install/joinMSMCluster.sh -k KEY -s SEED_IP -v
```

Where:

- **KEY** is the Credential Manager key for the seed node within the cluster you want to join. You can copy and paste the key value retrieved earlier.

- **SEED_IP** is the IP address for the seed node within the cluster. All joining nodes must specify the same seed node.

**NOTE:** Before clustering, a set of MSM VMs may be configured to use different Active Directory servers. However, once these nodes are joined together in a cluster, they must use a single Active Directory server instance. When you add an MSM VM to an existing cluster, the join script replicates the configuration data from the seed node to the joining node and discards the configuration data from the joining node. If a particular Active Directory user configuration needs to be preserved after clustering, that MSM node must be used as the seed node when the clustering command is executed.

- `-v` runs the script in verbose mode, which causes additional messages to be printed to the console.

If you omit any required parameter, the script will prompt for the parameter value.

6 Respond to the command prompts for any required parameters that were not specified when the `joinMSMCluster.sh` script was initiated.
Enter the current root password and msm vision password in order to set up the SSH keys for the machine.

**NOTE:**
The default passwords are as follows:
- root password: Vlrtu@1c3!
- MSM vision password: L!NkT@T3cA

You will also be prompted for the root password for the seed node, if you have not connected to that host before.

Verify the configuration settings. If all of the settings look correct, type **y** to continue. If not, type **n** and run the script again with the correct settings.

The join process will backup the Cassandra data before the Cassandra join step is performed, and then restore the Cassandra data after the Cassandra join step is completed. During the backup and restore steps, you may see the following warnings:

```
WARN 17:55:37,670 Filtering out TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as it isn't supported by the socket

Skipping file file-name.db: column family column-family doesn't exist
```

These warnings do not indicate a problem with the backup and restore process and can be ignored.

The join process may take several hours, depending on how much data you have and how many nodes are being clustered.

Wait for successful completion of the clustering configuration before joining additional nodes to the cluster.

If the clustering configuration does not complete successfully, you need to revert each of the MSM VMs and address the issues that caused the errors. For example, this might be necessary if a VM were to go down in the middle of the clustering process, since this would leave the cluster in an inoperable state. Once the errors have been corrected and the fixes have been verified, you can recover the MSM VMs and then try the clustering procedure again. You do not need to revert the Vision Core VMs in the event of a clustering error.

For details on recovering the MSM VMs, see the related topic on recovering the MSM cluster.

**NOTE:** If you encounter any problems during the join process, you can check the `/opt/vce/logs/multivmbmgmt/joinMSMCluster.log` file.

Confirm that the cluster is configured correctly by running the following command on the seed node:

```
/opt/cassandra/bin/nodetool status
```

The Cassandra nodetool checks that all clustered MSM VMs are in UN (up and normal) state.
Run the following command to add the repair cron jobs back to the seed node:

```
/opt/vce/multivbmgmt/install/cassandra_cluster_maintenance.sh --cron-enable-repair SEED_IP
```

Where:
- **SEED_IP** is the IP address for the seed node within the cluster.

Run the following command on all nodes within the cluster for cleanup purposes.

```
/opt/cassandra/bin/nodetool cleanup
```

**Results**

When you add an MSM VM to an existing cluster, the following configuration changes occur:

- Credential Manager encryption is migrated to the common cluster key specified by the user.
- Cassandra is configured to join the cluster.
- Separate crontab jobs, running the script `/opt/vce/multivbmgmt/install/crontab_schema_compaction.sh`, are scheduled to run at the same time once a day on each MSM node. If the MSM nodes are in the same LUN for storage, the crontab jobs should be run at different times on each node. In this case, you would need to edit each crontab job for compaction. Dell EMC recommends that the jobs be run one hour apart. Contact VCE Support for assistance.
- Elasticsearch is configured to join the cluster and port 9301 is configured as open for node-to-node communication.
- The nodetool repair command is run so that data may be distributed across the cluster.
- The cluster is automatically configured to encrypt Cassandra traffic between the MSM VMs.
- The Active Directory configuration data from the seed node is replicated to the joining node. After clustering, all nodes will share a single internal admin user (`/securityweb/security/users/1`) with the password from the seed node.

**NOTE:** In a large data center environment that spans multiple geographical locations, the Active Directory configuration would typically be replicated to all locations. To prevent MSM from going across geographical lines to perform Active Directory look ups, you can use local DNS practices. This will ensure that each MSM node is able to access the local Active Directory server to perform look ups.

**What to do next**

After adding an MSM VM to an existing cluster, log on to the Vision dashboard for each VM and verify that the data is the same on each VM within the cluster.
After clustering, if you change the MSM CAS password on one of the MSM VMs within the cluster (so that all of them match), you need to change the password on all of the other nodes within the cluster, as described below:

1. Run the following command:
   
   /opt/vce/multivbsecurity/bin/caschangepw.sh

2. When prompted for the current (old) password, enter the new password.

3. When prompted for the new password, enter the new password again.

**NOTE:** You must also update the CAS password on the multisystem prepositioning (MSP) VM to match the CAS password on the MSM VM. For instructions on how to do this, refer to the related topic.

**Related information**

- Changing the CAS password for the MSP VM to match the CAS password on the MSM VM (see page 90)
- Shutting down and taking a snapshot of the MSM cluster (see page 24)
- Recovering the MSM cluster (see page 25)

**Removing a Vision Core VM from an MSM VM**

Use this procedure to remove a Vision Core VM from an MSM VM. The MSM VMs can be either clustered or not clustered.

**About this task**

The removeSlibHost script removes the following information about the Vision Core VM from the MSM VM:

- MSM Collector configuration files
- Cassandra database
- Titan database
- Elasticsearch database
- VCE System credentials managed by the Credential Manager

You must remove each Vision Core VM from an MSM VM one at a time. When removing a Vision Core VM from an MSM VM, no other operations should be performed on that Vision Core VM from any other MSM VMs, until the removal is complete.

You can remove one Vision Core VM from an MSM VM after a cluster with one or more MSM VMs has been formed. You must remove the Vision Core VM from the MSM VM to which it was originally added.
If you have previously removed a Vision Core VM from an MSM VM, you can add the Vision Core VM back to the same MSM VM at a later time. The data from the original Vision Core VM will not be restored, but new data will be collected.

Procedure

Run the following command to remove the Vision Core VM from the MSM VM:

```
/opt/vce/multivbmgmt/install/removeSlibHost.sh IP address
```

where *IP address* is the IP address of the Vision Core VM that you want to remove.

**NOTE**: To verify the Vision Core VM was removed from the MSM VM, run the following command on the MSM VM from which you removed the Vision Core VM:

```
/opt/vce/multivbmgmt/install/listSlibNodes.sh
```

The IP address/hostname of the Vision Core VM that you removed will not be listed.

### Shutting down and taking a snapshot of the MSM cluster

Use this procedure to locate the seed MSM node, shut down the MSM cluster, and recover a downed system.

**Before you begin**

Take note of the order that you will shut down the MSM nodes.

**Procedure**

1. To find the seed node, start an SSH session to any MSM VM in the cluster and run the following command:

   ```
   grep seeds: /opt/cassandra/conf/cassandra.yaml
   ```

   The IP address in the output is the IP address of the seed node.

2. Power down each MSM VM in the cluster, ensuring to power down the seed node last:

   a. Using vCenter, shut down the nodes in the MSM cluster one by one in five minute intervals allowing time for RabbitMQ to react to the MSM nodes being shut down.

      **NOTE**: The order in which you shut down the nodes does not matter as long as the seed node is powered down last, but you must record the order.

   b. Take a snapshot of all the nodes in the MSM cluster.

**What to do next**

Recover your clustered environment. To recover your system after you take a snapshot, refer to [Recovering the MSM cluster](#) (see page 25).
Recovering the MSM cluster

You must restore your MSM cluster using the VMware vSphere Client.

About this task

The MSM nodes must be powered on in the reverse order that they were powered down, starting with the seed node.

Before you begin

Ensure you know the order in which the MSM nodes were powered down. If the order is unknown, begin with the MSM nodes in the seed node's VMware vCenter, starting with the seed node.

Procedure

1. Power on the MSM seed node using the vCenter vSphere Client, open a console connection to the VM, and wait for the log on prompt.

2. Perform the following for each MSM node in the same data center in the reverse order from the shutdown order:

   a. Power on the next MSM node using the vCenter vSphere Client. Continue powering on each MSM node in the cluster in five minute increments.

   ![NOTE](image)
   Repeat the recovery process for every MSM node in each data center of your clustered environment.

   b. After all of the MSM nodes in all data centers are powered back on, type the following command on each of the MSM nodes in the clustered environment:

   ```
   service tomcat restart
   ```

   c. Check the services by typing the following command:

   ```
   vision start
   ```

   This command checks whether each service is running. If the command does not run, the service is started.

   d. Monitor the status of the cluster by typing the following command:

   ```
   /opt/cassandra/bin/nodetool status
   ```

   Ensure all MSM nodes display UN status.

   e. Type the following command after all of the MSM nodes are up and running in the same data center to ensure the IP address of each MSM node in that data center appears:

   ```
   rabbitmqctl cluster_status
   ```
3 After all of the nodes in all data centers are powered back on, do the following:

   a Check the Vision dashboard to ensure you can view your VCE Systems. If you cannot view your VCE Systems, run the following command to restart the Tomcat service:

   ```
   service tomcat restart
   ```

   b Check the **Compliance and Remediation** section of the Vision dashboard and ensure the compliance status appears. If the compliance status does not appear, type the following command:

   ```
   service vision-mvb-compliance restart
   ```
Configuring Vision software for discovery

Configuring Vision Software to discover Vblock System components

Adding Network Attached Storage (eNAS) to VMAX3 on a Vblock System

Adding Network Attached Storage (eNAS) to VMAX3 enables you to deploy one infrastructure to manage block and file resources. You can add eNAS to an existing VMAX3 storage array on a Vblock System 740 using the configuration tool after the initial deployment.

Before you begin

Ensure that the Vision Core VM and multisystem management (MSM) VMs are deployed.

Refer to Installing and configuring the multisystem management VM topic in the Dell EMC Vision Intelligent Operations Installation Guide.

Procedure

1. Start an SSH session to the Vision Core VM.

   Important: Use PuTTY to access the configuration editor for Windows-based systems as non-VSCII supported terminals display styling incorrectly.

2. Log on to the Vision Core VM using the following credentials:
   - Username: root
   - Password: V1rtu@1c3!

3. If you are configuring an existing vblock.xml file in /opt/vce/fm/conf, type configTool.sh --multiple-storage and load the existing vblock.xml file.

4. Follow the prompts and make any changes to the attribute information for the Vblock System.

   Refer to the Configuring the vblock.xml file topic in the Dell EMC Vision Intelligent Operations Installation Guide for information about each prompt and the attribute information you can enter.

5. The script prompts you to add eNAS to VMAX3, as follows:

   Do you want to add a eNAS to the VMAX with componentTag: 'VMAX-ARRAY' in this configuration? ('0' to include, 's' to skip) [s] :

   Type 0 to include eNAS in the configuration.
6 The script prompts you to configure the properties for eNAS, as follows:

```
Credentials                             StorageArray        4    ipaddress:
  'eNAS',
  (1) ipaddress, '192.168.101.46'
  (2) password, ''
  (3) username, 'admin'
Enter selection ('0' to continue to next step, or 'v' to validate ):
```

- Type one of the following values:
  - Type 0 to continue to the next step.
  - Type 1 to change the IP address of eNAS.
  - Type 2 to set the password. You must set the password.
  - Type 3 to change the username.
  - Type v to validate the information for eNAS.

7 Complete the prompts as necessary. When you finish making changes, the script starts the validation process and displays output such as the following:

```
"Validation of connection to {enas_IP}:5989 succeeded!"
```

8 Save the vblock.xml file. This overwrites the original vblock.xml file.

What to do next

1 View the vblock.xml file and verify that eNAS is contained under storage.

2 Restart the FM Agent services from the Vision Core VM.
   - Run the following command:
     ```
     stopFMagent
     ```
   - Run the following command:
     ```
     startFMagent
     ```

3 Log on to the Vision dashboard and search for eNAS.

**Adding Isilon Technology Extension on a Vblock System**

Adding an additional Nexus 5k switch enables you to support the Isilon array.

**Before you begin**

Ensure that the Vision Core VM and multisystem management (MSM) VMs are deployed.
Refer to the Installing and configuring the multisystem management VM topic in the *Dell EMC Vision Intelligent Operations Installation Guide*.

**Procedure**

1. Start an SSH session to the Vision Core VM.

   **Important:** Use PuTTY to access the configuration editor for Windows-based systems as non-VSCI1 supported terminals display styling incorrectly.

2. Log on to the Vision Core VM using the following credentials:
   - Username: `root`
   - Password: `V1rtu@1c3!`

3. If you are configuring an existing `vblock.xml` file in `/opt/vce/fm/conf`, type `configTool.sh --multiple-switch` and load the existing `vblock.xml` file.

4. Follow the prompts and make any changes to the attribute information for the Vblock System.

   Refer to the Configuring the `vblock.xml` file topic in the *Dell EMC Vision Intelligent Operations Installation Guide* for information about each prompt and the attribute information you can enter.

5. The script prompts you to add Nexus 5K switches, as follows:

   ```
   Do you want to include additional Nexus5k switches in this configuration? ('0' to include, 's' to skip) [s] :
   ```

   Type 0 to include additional 5K switches in the configuration.

6. The script prompts you for the number of Nexus 5K switches that you want to add, as follows:

   ```
   Enter the number of additional Nexus5k configurations in the system you are configuring:
   ```

7. The script prompts you to change the IP address to the Nexus 5K IP address, as follows:

   ```
   Switch                             Network        3    address: '192.16.10.103',
   componentTag: 'MGMT-N5G', type: 'Nexus5000'  
   (1) ipaddress, '192.16.10.103'
   ```

   To change an attribute enter the corresponding number from the list ('0' to continue to next step): 1

   ```
   Enter a new value for attribute 'address' [192.16.10.103] ('s' to skip): 10.3.54.5
   ```

   ```
   Switch                             Network        3    address: '10.3.54.5',
   componentTag: 'MGMT-N5G', type: 'Nexus5000'  
   (1) ipaddress, '10.3.54.5'
   ```
The script prompts you to configure the properties for the switch, as follows:

<table>
<thead>
<tr>
<th>Credentials</th>
<th>Switch</th>
<th>community: 'public', method: 'snmpv2c', username: 'admin',</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(1) community, 'public'</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2) password, ''</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(3) username, 'admin'</td>
</tr>
</tbody>
</table>

Enter selection ('0' to continue to next step, or 'v' to validate):

a  Type one of the following values:

- Type 0 to continue to the next step.
- Type 1 to change the community.
- Type 2 to set the password. You must set the password.
- Type 3 to change the username.
- Type v to validate the information.

9 Complete the prompts as necessary. When you finish making changes, the script starts the validation process and displays output such as the following:

Validating SNMP connection for ComponentTag=MGMT-N5G ipAddress=10.3.54.5 Please wait...
Validating SNMP connection succeeded!
Validating SSH connection. Please wait...
Validating SSH connection succeeded!

10 Save the vblock.xml file. This overwrites the original vblock.xml file.

What to do next

1 View the vblock.xml file and verify that N5K is contained under switch.

2 Restart the FM Agent services from the Vision Core VM.
   
a  Run the following command:

        stopFMagent

   b  Run the following command:

        startFMagent

3 Log on to the Vision dashboard and search for switch. The n5k will appear under the Model Name.

Configuring Vision software to discover VxBlock System and VxRack System components
Configuration editor overview

The configuration editor enables you to create and edit the configuration files necessary for VxBlock System and VxRack System discovery. The configuration editor prompts you for specific information about the VxBlock System or VxRack System you are configuring.

Vision software then uses the system.cfg to create an xml file that is used for initial discovery of the compute, network, storage, and management components in the VCE System. The name of this file varies depending on the system you are configuring. For VxBlock Systems, it creates a vblock.xml file. For VxRack Systems, it creates a vxrack.xml file.

The following VCE Systems can be configured using the configuration editor:

- All VxBlock Systems
- VxRack System with FLEX

**NOTE:** The same configuration applies for both VMAX and PowerMax on any VxBlock System.

See below for configuration file examples:

- **VxBlock System 1000 (Block only, no AMP)**

```xml
product=VxBlock
system=VXBLOCK
type=1000
componentTag=VXB-1000
serialNumber=V70FN4013002CM

centric.vcenter[1].name=Vcenter1
centric.vcenter[1].url=10.136.28.57
centric.vcenter[1].username=administrator@vsphere.local
centric.vcenter[1].password=@RtpCoe123

compute.server[1].name=sys1
compute.server[1].type=UCS
compute.server[1].componentTag=VMABO-UCS-1
compute.server[1].address=10.234.137.134
compute.server[1].credentials.username=svc_vision
compute.server[1].credentials.password=Password123
compute.server[1].credentials.community=public
compute.server[2].name=sys2
compute.server[2].type=UCS
compute.server[2].componentTag=VMABO-UCS-2
compute.server[2].address=10.234.137.136
compute.server[2].credentials.username=svc_vision
compute.server[2].credentials.password=Password123
compute.server[2].credentials.community=public

network.switch[1].type=Nexus3000
network.switch[1].componentTag=MGMT-N3A
network.switch[1].address=10.234.137.151
network.switch[1].credentials.username=svc_vision
network.switch[1].credentials.password=Password123
network.switch[1].credentials.community=COERTP123
network.switch[2].type=Nexus3000
network.switch[2].componentTag=MGMT-N3B
network.switch[2].address=10.234.137.152
network.switch[2].credentials.username=svc_vision
network.switch[2].credentials.password=Password123
```
<table>
<thead>
<tr>
<th>switch</th>
<th>type</th>
<th>componentTag</th>
<th>address</th>
<th>credentials.username</th>
<th>credentials.password</th>
<th>credentials.community</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch[2]</td>
<td>network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>switch[6]</td>
<td>network</td>
<td>MDS9000</td>
<td>10.234.137.133</td>
<td>svc_vision</td>
<td>Password123</td>
<td>COERTP123</td>
</tr>
<tr>
<td>switch[7]</td>
<td>network</td>
<td>NSX</td>
<td>10.239.138.210</td>
<td>admin</td>
<td>V1rtu1c3!</td>
<td></td>
</tr>
<tr>
<td>array[1]</td>
<td>storage</td>
<td>UNITY</td>
<td>10.234.137.160</td>
<td><a href="mailto:svc_vision@pde.lab.vce.com">svc_vision@pde.lab.vce.com</a></td>
<td>Password123</td>
<td></td>
</tr>
<tr>
<td>array[2]</td>
<td>storage</td>
<td>VMAX</td>
<td>10.136.43.56</td>
<td>admin</td>
<td>#1Password</td>
<td></td>
</tr>
</tbody>
</table>

**Related information**

[Configuration editor component reference](see page 38)
Configuring a VxBlock System or a VxRack System using the configuration editor

Use the configuration editor to create, edit, or delete the configuration files necessary for discovery on a VxBlock System and a VxRack System.

Before you begin

Ensure the system.cfg file is in the /opt/vce/fm/conf directory on the Vision Core VM. If the system.cfg file is not located in this directory, contact VCE Support.

Procedure

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

2. Log on using the following credentials:
   
   Username: root
   
   Password: V1rtu@1c3!

3. Run the following command to launch the configuration editor and edit a previously imported configuration:

   ```bash
   configSystem edit
   ```

   The VCE Systems configuration editor opens.

What to do next

Add components to the configuration. Refer to Adding a component with the configuration editor (see page 35) for more information.

Editing component properties with the configuration editor

Use the configuration editor to modify various component properties on a VxBlock System or a VxRack System.

About this task

You can edit the following component properties:

- IP address
- Username
- Password
- Community string
Method

**NOTE:** Depending on method and component type, this value can be lower or mixed case sensitive. Values for most fields are case sensitive, however, for a VxRack System method, the value is case insensitive.

Sensitive information such as passwords and community strings are masked in the configuration editor and encrypted in the configuration file.

Before you begin

Ensure you have configured the VxBlock System or VxRack System.

Procedure

1. Type the command `configSystem edit` to open the configuration editor.
2. Follow these steps to edit the component properties:
   a. In the configuration editor dialog, use the **Next** and **Back** options to navigate to the component you want to edit.
   b. Click **Tab** or use the arrow keys to navigate to the specific property you want to edit.
   c. Click the **Backspace** key or the **Delete** key to edit the properties.
3. Select **Save** to save the configuration changes and exit the configuration editor, or **Cancel** to exit the configuration editor without saving your changes.

   The configuration editor uses the system.cfg to create (or update) an xml file that is used for initial discovery. For VxBlock Systems, it creates a vblock.xml file. For VxRack Systems, it creates a vxrack.xml file.

What to do next

Restart the FM Agent services from the Vision Core VM.

1. Run the following command:
   ```
   stopFMagent
   ```
2. Run the following command:
   ```
   startFMagent
   ```

Related information

[Configuring a VxBlock System or a VxRack System using the configuration editor](see page 33)
Adding a component with the configuration editor

Use the configuration editor to add new components to the system configuration of your VxBlock System and VxRack System.

About this task

**NOTE:** VxBlock Systems are template based. Components can only be added if they are supported in the template. For example, Nexus 9000 switches cannot be added to a VxBlock 340.

You can add the following new component types to the system configuration:

<table>
<thead>
<tr>
<th>Component types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rack</td>
<td>This is the Panduit Rack.</td>
</tr>
<tr>
<td>Storage array</td>
<td>The storage array component is supported on a VxBlock System, VxRack System and Vscale Fabric Technology Extension. Vision software does not support the use of a single ECOM server (Element Manager) IP for multiple storage arrays. You must specify a different ECOM server IP for each additional storage array you want to add.</td>
</tr>
<tr>
<td>Switch</td>
<td>Available for VxRack Systems and VxBlock Systems.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The limitation of 6 network switches for VxBlock Systems has been removed from Vision 3.6.2 onwards.</td>
</tr>
<tr>
<td>DCNM</td>
<td>Available for VxBlock Systems.</td>
</tr>
<tr>
<td>Compute Server</td>
<td>The Product Serial Number is used to identify each chassis in a VxRack System. Ensure that the value in the Product Serial Number field for each node in a specific chassis is identical. If you move a node from one chassis to another, you must manually update the value in the Product Serial Number field to ensure that the value is identical to the value for the existing nodes for that chassis.</td>
</tr>
<tr>
<td>vCenter</td>
<td>The &lt;url&gt; attribute of the vCenter, specified in the configuration file, must be in the form of an IP address to be discovered by Vision software.</td>
</tr>
<tr>
<td>Storage virtualizer</td>
<td>Available for VxRack Systems and VxBlock Systems.</td>
</tr>
<tr>
<td>Application host</td>
<td>The application host component is supported on a VxBlock System.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Available for VxRack Systems only.</td>
</tr>
<tr>
<td>VxRack Controller</td>
<td>Available for VxRack Systems and VxBlock Systems.</td>
</tr>
<tr>
<td>Extra properties for selected component</td>
<td>Available for VxRack Systems only. This component type is only displayed when a storage array is selected.</td>
</tr>
</tbody>
</table>

Before you begin

Ensure you have configured the VxBlock System or VxRack System system.
Refer to Configuration editor component reference (see page 38) for component information.

Procedure

1. Type the command `configSystem edit` to open the configuration editor.

2. Select Add in the Configuration Editor dialog. The Add Component dialog opens.

3. Select the component type you want to add and click Enter.

4. Select Add. An empty component form is added as the last component in the sequence.
   a. In the configuration editor dialog, use the Next and Back options to navigate to the component you want to edit.
   b. Click Tab or use the arrow keys to navigate to the specific component property you want to edit.
   c. Click the Backspace key or the Delete key to edit the property fields.

5. Select Save to save the configuration changes and exit the configuration editor, or Cancel to exit the configuration editor without saving your changes.

The configuration editor uses the system.cfg to create (or update) an xml file that is used for initial discovery. For VxBlock Systems, it creates a vblock.xml file. For VxRack Systems, it creates a vxrack.xml file.

What to do next

Restart the FM Agent services from the Vision Core VM.

1. Run the following command:

   ```bash
   stopFMagent
   ```

2. Run the following command:

   ```bash
   startFMagent
   ```

Related information

- Starting discovery (see page 10)
- Configuring a VxBlock System or a VxRack System using the configuration editor (see page 33)

Adding Network Attached Storage (eNAS) to VMAX3 on a VxBlock System

Adding Network Attached Storage (eNAS) to VMAX3 enables you to deploy one infrastructure to manage block and file resources. You can add eNAS properties to an existing VMAX3 storage array on a VxBlock System using the configuration editor.
Before you begin

Ensure that the Vision Core and MSM VM are deployed.

Procedure

1. Start an SSH session to the Vision Core VM.

   **Important:** Use PuTTY to access the configuration editor for Windows-based systems as non-VSCII supported terminals display styling incorrectly.

2. Log on to the Vision Core VM using the following credentials:
   - **Username:** root
   - **Password:** V1rtu@1c3!

3. Run the following command to launch the configuration editor:

   ```
   configSystem edit
   ```

4. Use the **Next** option to navigate to the **VMAX** storage array and select **Add**.

5. Select **Extra properties for selected component > Add**.

6. In the **Which** field, enter eNAS. The value for the **Which** field is case sensitive.

7. In the **Method** field, enter the IP address of eNAS. For example, 10.4.49.22.

8. In the **Username** field, enter the username. For example, bcsadmin.

9. In the **Password** field, enter the password. For example, B2ute@2a4!!!. You do not need to enter a community string.

10. Select **Save** to save the properties and exit the configuration editor, or **Cancel** to exit the configuration editor without saving your changes.

What to do next

1. View the vblock.xml file and verify that eNAS is contained under storage.

2. Restart the FM Agent services from the Vision Core VM.
   a. Run the following command:

       ```
       stopFMagent
       ```
   b. Run the following command:

       ```
       startFMagent
       ```

3. Log on to the Vision dashboard and search for eNAS.
Deleting a component with the configuration editor

Use the configuration editor to remove components from the system configuration of your VxBlock System and VxRack System.

Before you begin

Ensure you have configured the VxBlock System or VxRack System.

Procedure

1. Use the Next and Back options to navigate to the component type you want to delete in the VCE Systems configuration editor dialog.

2. Select Delete. The Component deletion dialog opens displaying the following message:

   Are you sure you wish to delete the component?

   – Type Yes and press Enter to delete the component. The Component deletion dialog closes and the component is deleted.

   – Type No and press Enter if you do not want to delete the component. The Component deletion dialog closes and you are returned to the configuration editor dialog.

3. Select Save to save the configuration changes and exit the configuration editor, or Cancel to exit the configuration editor without saving your changes.

What to do next

Restart the FM Agent services from the Vision Core VM.

1. Run the following command:

   stopFMagent

2. Run the following command:

   startFMagent

Related information

Configuring a VxBlock System or a VxRack System using the configuration editor (see page 33)

Configuration editor component reference

Use the tables to configure VCE Systems with the configuration editor. All values, including location information, are mandatory.
### VxBlock 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>Dictates the VxBlock System product. The mandatory value is <strong>VXBLOCK</strong>.</td>
<td>VXBLOCK</td>
</tr>
<tr>
<td>Product</td>
<td>Dictates the VxBlock System product. The mandatory value is <strong>VxBlock</strong>.</td>
<td>VxBlock</td>
</tr>
<tr>
<td>Product type</td>
<td>The first three digits determine the VxBlock System type. This is a mandatory field.</td>
<td>320XXXX</td>
</tr>
<tr>
<td>Serial number</td>
<td>Should be a meaningful value.</td>
<td>VB320-975-318-642</td>
</tr>
<tr>
<td>Component tag</td>
<td>Should be a meaningful value.</td>
<td>VB-320</td>
</tr>
<tr>
<td>Geo</td>
<td>The data center location.</td>
<td>Marlborough, MA</td>
</tr>
<tr>
<td>Building</td>
<td>The building name.</td>
<td>Building 4</td>
</tr>
<tr>
<td>Floor</td>
<td>The floor number.</td>
<td>1</td>
</tr>
<tr>
<td>Room</td>
<td>The room number.</td>
<td>1</td>
</tr>
<tr>
<td>Row</td>
<td>The row number.</td>
<td>1</td>
</tr>
<tr>
<td>Tile</td>
<td>The tile number.</td>
<td>1</td>
</tr>
</tbody>
</table>

### VxRack 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>Dictates the VxRack System product. The mandatory value is <strong>VXRACK</strong>.</td>
<td>VXRACK</td>
</tr>
<tr>
<td>Product</td>
<td>The VxRack System product. The mandatory value is <strong>VxRack</strong>.</td>
<td>VxRack</td>
</tr>
<tr>
<td>Product type</td>
<td>VxRack System with FLEX is currently the only supported VxRack System product type. This is a mandatory field.</td>
<td>VxRack1000FLEX</td>
</tr>
<tr>
<td>Serial number</td>
<td>Can be any meaningful value.</td>
<td>VX1000FLEX-77 7-888-999</td>
</tr>
<tr>
<td>Component tag</td>
<td>Can be any meaningful value.</td>
<td>VX1000FLEX</td>
</tr>
<tr>
<td>Geo</td>
<td>The data center location.</td>
<td>Marlborough, MA</td>
</tr>
<tr>
<td>Building</td>
<td>The building name.</td>
<td>Building 4</td>
</tr>
<tr>
<td>Floor</td>
<td>The floor number.</td>
<td>1</td>
</tr>
<tr>
<td>Room</td>
<td>The room number.</td>
<td>1</td>
</tr>
<tr>
<td>Row</td>
<td>The row number.</td>
<td>1</td>
</tr>
<tr>
<td>Tile</td>
<td>The tile number.</td>
<td>1</td>
</tr>
</tbody>
</table>
### Component configuration settings

<table>
<thead>
<tr>
<th>Component type</th>
<th>VCE Systems</th>
<th>Field</th>
<th>Rules</th>
<th>Field value example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute server</td>
<td>VxBlock System, VxRack System</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></td>
<td>Name</td>
<td>The default name for UCS servers is <code>sys</code>. For each additional UCS server, ensure the name is in the following format: <code>sysXXXX</code> where <code>sys</code> is lowercase and <code>XXXX</code> is a unique number. For example <code>sys2</code>.</td>
<td><code>sys</code></td>
</tr>
<tr>
<td>Compute server</td>
<td></td>
<td>Type</td>
<td>Must be one of the following: UCS, C200M1, C200M2, C220M3, C220M4, C240M3, C240M4, VxRack Controller</td>
<td><code>UCS</code></td>
</tr>
<tr>
<td>Compute server</td>
<td></td>
<td>Component tag</td>
<td>Can be any meaningful value.</td>
<td><code>VMABO-UCS-1</code></td>
</tr>
<tr>
<td>Compute server</td>
<td></td>
<td>Server IP Address</td>
<td>Should be a dotted IP address. In the case of VxRack Controller, you can specify ranges by separating the first and last IP in a range with a hyphen. For example, 10.1.139.30 - 10.1.139.35.</td>
<td><code>10.1.139.30</code></td>
</tr>
<tr>
<td>Compute server</td>
<td></td>
<td>Username</td>
<td>The SSH username.</td>
<td><code>admin</code></td>
</tr>
<tr>
<td>Compute server</td>
<td></td>
<td>Method</td>
<td>Must be one of the following: REDFISH, SNMPV2C, IMPIV2, WEBSERVICE, SSH</td>
<td><code>REDFISH</code></td>
</tr>
<tr>
<td>Compute server</td>
<td></td>
<td>Password</td>
<td>The SSH password.</td>
<td><code>password</code></td>
</tr>
<tr>
<td>Compute server</td>
<td></td>
<td>Community</td>
<td>The SNMP community string. Community string is only necessary for the SNMP method. For VxRack Controller, there is no community string.</td>
<td><code>public</code></td>
</tr>
<tr>
<td>Operating system</td>
<td>VxRack System</td>
<td>Type</td>
<td>Must be: REDHAT</td>
<td><code>REDHAT</code></td>
</tr>
<tr>
<td>Operating system</td>
<td></td>
<td>Component tag</td>
<td>Can be any meaningful value.</td>
<td><code>RedHat-1</code></td>
</tr>
<tr>
<td>Component type</td>
<td>VCE Systems</td>
<td>Field</td>
<td>Rules</td>
<td>Field value example</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>-------------------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| Operating system |             | IP Address        | Can be any meaningful value. You can specify IP ranges by separating the first and last IP in a range with a hyphen. For example, 10.1.139.30 - 10.1.139.35. | XXX.XXX.XXX.XXX-XXX.XXX.XXX.XXX XXX-XXX.XXX.XXX.XXX XXX-XXX.XXX.XXX.XXX-
| Operating system |             | Username          | The SSH username                                                      | root                |
| Operating system |             | Method            | Must be: SSH                                                         | SSH                 |
| Operating system |             | PasswordMethod    | The SSH password (optional if using SSH public key authentication)    | password            |
| AMP             | VxBlock System, VxRack System | Amp type          | Can be any of the following: VxBlock System: AMP-<code type>, where <code type> is the AMP model in your environment VxRack System: AMP-KYL | AMP-2S AMP-KYL AMP-3S |
| AMP             |             | Component tag     | Can be any meaningful value.                                         | Management          |
| AMP             |             | Serial number     | Can be any meaningful value.                                         | AMP-KYL-123         |
| Component credentials | VxRack System | IP Range          | Should be a range of dotted IP addresses. You can specify ranges by separating the first and last IP in a range with a hyphen. For example, 10.1.139.30 - 10.1.139.35. | XXX.XXX.XXX.XXX-XXX.XXX.XXX.XXX XXX-XXX.XXX.XXX.XXX XXX-XXX.XXX.XXX.XXX-
<p>| Component credentials |             | Community         | The SNMP community string.                                           | public              |
| Component credentials |             | Username          | The username                                                         | root                |
| Component credentials |             | Method            | Must be one of the following: IPMIV2, SNMPV2C, WEBSERVICE, SSH, REDFISH | SSH                 |
| Component credentials |             | Password          | The password                                                         | password            |
| Rack            | VxBlock System, VxRack System | Rack ID           | The unique identifier of a rack.                                      | 1                   |</p>
<table>
<thead>
<tr>
<th>Component type</th>
<th>VCE Systems</th>
<th>Field</th>
<th>Rules</th>
<th>Field value example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rack</td>
<td>VCE Systems</td>
<td>Rack Type</td>
<td>Refers to the model of rack.</td>
<td>1</td>
</tr>
<tr>
<td>Rack</td>
<td>Rack Format</td>
<td>US</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rack</td>
<td>Gateway IP Address</td>
<td>Specifies the default gateway for a rack.</td>
<td>192.168.1.X</td>
<td></td>
</tr>
<tr>
<td>Rack</td>
<td>Method</td>
<td>Must be one of the following: IPMIv2, SNMPv2C, WEBSERVICE, SSH</td>
<td>snmpv2c</td>
<td></td>
</tr>
<tr>
<td>Rack</td>
<td>Community</td>
<td>The SNMP community string configured on the rack.</td>
<td>public</td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td>VxBlock System, VxRack System</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>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td>Method</td>
<td>Must be one of the following: IPMIv2, SNMPv2C, WEBSERVICE, SSH</td>
<td>snmpv2c</td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td>IP Address</td>
<td>Should be a dotted IP address.</td>
<td>10.1.139.22</td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td>Username</td>
<td>The SSH username.</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td>Password</td>
<td>The password</td>
<td>password</td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td>Community</td>
<td>The SNMP community string.</td>
<td>public</td>
<td></td>
</tr>
<tr>
<td>DCNM</td>
<td>VxBlock System</td>
<td>IP Address</td>
<td>Should be a dotted IP address.</td>
<td>10.1.33.232</td>
</tr>
<tr>
<td>Component type</td>
<td>VCE Systems</td>
<td>Field</td>
<td>Rules</td>
<td>Field value example</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Storage array VNX</td>
<td>VxBlock System</td>
<td><strong>In AMP</strong></td>
<td>Specifies if the component is a part of the AMP configuration.</td>
<td>x</td>
</tr>
<tr>
<td>Storage array VNX</td>
<td></td>
<td><strong>Type</strong></td>
<td>Must be one of the following: VNX, VNX5200, VNX5300, VNX5400, VNX5500, VNX5600, VNX5700, VNX5800, VNX7500, VNX7600, VNX8000, VNXe, VNXe3150, VNXe3300</td>
<td>VNX5500</td>
</tr>
<tr>
<td>Storage array VNX</td>
<td></td>
<td><strong>Component tag</strong></td>
<td>Must be one of the following: VNXe3150-ARRAY, VNXe3300-ARRAY, VNX5300-ARRAY, VNX5500-ARRAY, VNX5700-ARRAY, VNX7500-ARRAY, VNX5200-ARRAY, VNX5400-ARRAY, VNX5600-ARRAY, VNX5800-ARRAY, VNX7600-ARRAY, VNX8000-ARRAY, VNXe-ARRAY, VNX-ARRAY</td>
<td>VNX5500-ARRAY</td>
</tr>
<tr>
<td>Storage array VNX</td>
<td></td>
<td><strong>IP Address</strong></td>
<td>Should be a dotted IP address.</td>
<td>10.1.139.52</td>
</tr>
<tr>
<td>Storage array VNX</td>
<td></td>
<td><strong>Username</strong></td>
<td>The username.</td>
<td>admin</td>
</tr>
<tr>
<td>Storage array VNX</td>
<td></td>
<td><strong>Password</strong></td>
<td>The password.</td>
<td>password</td>
</tr>
<tr>
<td>Storage array VNX</td>
<td></td>
<td><strong>Which</strong></td>
<td>Should be one of the following: ECOM Server, Control Station, SPA, SPB</td>
<td>ECOM Server</td>
</tr>
<tr>
<td>Storage array VNX</td>
<td></td>
<td><strong>Method</strong></td>
<td>Must be a dotted IP address. This is the CIM entry point when <strong>Which</strong> is an ECOM server or Control Station.</td>
<td>10.1.139.42</td>
</tr>
<tr>
<td>Storage array VNX</td>
<td></td>
<td><strong>Username</strong></td>
<td>The username.</td>
<td>sysadmin</td>
</tr>
<tr>
<td>Storage array VNX</td>
<td></td>
<td><strong>Password</strong></td>
<td>The password.</td>
<td>password</td>
</tr>
<tr>
<td>Component type</td>
<td>VCE Systems</td>
<td>Field</td>
<td>Rules</td>
<td>Field value example</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Storage array</td>
<td>VNX</td>
<td>Community</td>
<td>The SNMP community string.</td>
<td>public</td>
</tr>
<tr>
<td>Storage array</td>
<td>VMAX/PowerMax</td>
<td>In AMP</td>
<td>Specifies if the component is a part of the AMP configuration.</td>
<td>x</td>
</tr>
<tr>
<td>Storage array</td>
<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>VMAX/PowerMax</td>
<td>Component tag</td>
<td>Must be one of the following: VMAX10K-ARRAY, VMAX20K-ARRAY, VMAX40K-ARRAY, VMAX3-ARRAY, VMAX100K-ARRAY, VMAX200K-ARRAY, VMAX250F-ARRAY, VMAX250FX-ARRAY, VMAX400K-ARRAY, VMAX-ARRAY, VMAXe-ARRAY, VMAX450F-ARRAY, VMAX450FX-ARRAY, VMAX850F-ARRAY, VMAX850FX-ARRAY</td>
<td>VMAX10K-ARRAY</td>
</tr>
<tr>
<td>Storage array</td>
<td>VMAX/PowerMax</td>
<td>IP Address</td>
<td>Should be a dotted IP address.</td>
<td>10.1.139.52</td>
</tr>
<tr>
<td>Storage array</td>
<td>VMAX/PowerMax</td>
<td>Which</td>
<td>Should be one of the following: VMAX</td>
<td>VMAX</td>
</tr>
<tr>
<td>Storage array</td>
<td>VMAX/PowerMax</td>
<td>Method</td>
<td>Must be a dotted IP address. This is the 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>VMAX/PowerMax</td>
<td>Username</td>
<td>The username.</td>
<td>fmuser</td>
</tr>
<tr>
<td>Storage array</td>
<td>VMAX/PowerMax</td>
<td>Password</td>
<td>The password.</td>
<td>password</td>
</tr>
<tr>
<td>Storage array</td>
<td>VMAX w/ gateway</td>
<td>In AMP</td>
<td>Specifies if the component is a part of the AMP configuration.</td>
<td>x</td>
</tr>
<tr>
<td>Component type</td>
<td>VCE Systems</td>
<td>Field</td>
<td>Rules</td>
<td>Field value example</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>-------</td>
<td>-------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</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>VCE Systems</td>
<td>Component tag</td>
<td>Must be one of the following: VMAX10K-ARRAY, VMAX20K-ARRAY, VMAX40K-ARRAY, VMAX3-ARRAY, 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</td>
<td>IP Address</td>
<td>Should be a dotted IP address.</td>
<td>10.1.139.52</td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Which</td>
<td>Should be: VMAX</td>
<td>VMAX</td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Method</td>
<td>Must be a dotted IP address.</td>
<td>10.1.139.42</td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Username</td>
<td>The VMAX username.</td>
<td>fmuser</td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Password</td>
<td>The VMAX password.</td>
<td>password</td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Which</td>
<td>The second Which field should be: gateway</td>
<td>gateway</td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Method</td>
<td>The second Method is a dotted IP address.</td>
<td>10.1.139.42</td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Username</td>
<td>The NAS administrator username.</td>
<td>nasadmin</td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>Password</td>
<td>The NAS administrator password.</td>
<td>password</td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VxBlock System</td>
<td>In AMP</td>
<td>Specifies if the component is a part of the AMP configuration.</td>
<td>x</td>
</tr>
<tr>
<td>Component type</td>
<td>VCE Systems</td>
<td>Field</td>
<td>Rules</td>
<td>Field value example</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>-------------</td>
<td>--------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</td>
<td>Type</td>
<td>Must be the following: XTREMIO</td>
<td>XTREMIO</td>
</tr>
<tr>
<td>XtremIO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</td>
<td>Component tag</td>
<td>Must be the following: XIO-ARRAY-1</td>
<td>XIO-ARRAY-1</td>
</tr>
<tr>
<td>XtremIO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</td>
<td>IP Address</td>
<td>Should be a dotted IP address.</td>
<td>10.1.139.52</td>
</tr>
<tr>
<td>XtremIO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</td>
<td>Which</td>
<td>Should be: XTREMIO</td>
<td>XTREMIO</td>
</tr>
<tr>
<td>XtremIO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</td>
<td>Method</td>
<td>Should be xml.</td>
<td>xml</td>
</tr>
<tr>
<td>XtremIO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</td>
<td>Username</td>
<td>The XtremIO username.</td>
<td>admin</td>
</tr>
<tr>
<td>XtremIO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</td>
<td>Password</td>
<td>The Xtremio password.</td>
<td>password</td>
</tr>
<tr>
<td>XtremIO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</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>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</td>
<td>Type</td>
<td>Must be the following: ISILON</td>
<td>ISILON</td>
</tr>
<tr>
<td>Isilon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</td>
<td>Component tag</td>
<td>Must be the following: ISILON-ARRAY-CLUSTER-1</td>
<td>ISILON-ARRAY-CLUSTER-1</td>
</tr>
<tr>
<td>Isilon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</td>
<td>IP Address</td>
<td>Should be a dotted IP address.</td>
<td>10.1.139.52</td>
</tr>
<tr>
<td>Isilon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</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>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</td>
<td>Username</td>
<td>The Isilon username.</td>
<td>admin</td>
</tr>
<tr>
<td>Isilon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</td>
<td>Password</td>
<td>The Isilon password.</td>
<td>password</td>
</tr>
<tr>
<td>Isilon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</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</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</td>
<td>Type</td>
<td>Must be the following: UNITY</td>
<td>UNITY</td>
</tr>
<tr>
<td>Dell EMC Unity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage array</td>
<td>VCE Systems</td>
<td>Component tag</td>
<td>Must be the following: UNITY-ARRAY-x where x is the number of the array</td>
<td>UNITY-ARRAY-1</td>
</tr>
<tr>
<td>Dell EMC Unity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Component type</td>
<td>VCE Systems</td>
<td>Field</td>
<td>Rules</td>
<td>Field value example</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------</td>
<td>----------</td>
<td>------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Storage array</td>
<td>Dell EMC Unity</td>
<td>IP Address</td>
<td>Should be a dotted IP address.</td>
<td>10.1.139.52</td>
</tr>
<tr>
<td>Storage array</td>
<td>Dell EMC Unity</td>
<td>Method</td>
<td>Must be <code>restApi</code>.</td>
<td><code>restApi</code></td>
</tr>
<tr>
<td>Storage array</td>
<td>Dell EMC Unity</td>
<td>Username</td>
<td>The Dell EMC Unity username.</td>
<td><code>admin</code></td>
</tr>
<tr>
<td>Storage array</td>
<td>Dell EMC Unity</td>
<td>Password</td>
<td>The Dell EMC Unity password.</td>
<td><code>password</code></td>
</tr>
<tr>
<td>vCenter</td>
<td>VxBlock System, VxRack System</td>
<td>In AMP</td>
<td>Specifies if the component is a part of the AMP configuration. If you are configuring a shared vCenter with MSM, be sure to include the shared vCenter server information in the configuration file on each Vision Core VM that is associated with an MSM node. Do not define a shared vCenter as a part of the AMP if the shared vCenter resides on a Shared Management Platform (SMP), rather than on a VCE System.</td>
<td><code>x</code></td>
</tr>
<tr>
<td>vCenter</td>
<td></td>
<td>Name</td>
<td>Should be vCenter1, vCenter2, ... vCenterN, and so forth. If you are configuring a shared vCenter with MSM, be sure to include the shared vCenter server information in the configuration file on each Vision Core VM that is associated with an MSM node. When a shared vCenter resides on an SMP, that SMP will not be discovered. However, the fact that the vCenter is shared by multiple VCE Systems will be apparent in the results returned for a <code>find VIManager</code> query.</td>
<td><code>vCenter1</code></td>
</tr>
<tr>
<td>Component type</td>
<td>VCE Systems</td>
<td>Field</td>
<td>Rules</td>
<td>Field value example</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>-------</td>
<td>-------</td>
<td>---------------------</td>
</tr>
<tr>
<td>vCenter</td>
<td></td>
<td>URL</td>
<td>Should be a dotted IP address to the vCenter server. If you are configuring a shared vCenter with MSM, be sure to include the shared vCenter server information in the configuration file on each Vision Core VM that is associated with an MSM node.</td>
<td>10.1.139.39</td>
</tr>
<tr>
<td>vCenter</td>
<td></td>
<td>Username</td>
<td>The vCenter server SDK username. If you are configuring a shared vCenter with MSM, be sure to include the shared vCenter server information in the configuration file on each Vision Core VM that is associated with an MSM node.</td>
<td>vb300swqa\administrator</td>
</tr>
<tr>
<td>vCenter</td>
<td></td>
<td>Password</td>
<td>The vCenter server SDK password. If you are configuring a shared vCenter with MSM, be sure to include the shared vCenter server information in the configuration file on each Vision Core VM that is associated with an MSM node.</td>
<td>password</td>
</tr>
<tr>
<td>Application host</td>
<td>VxBlock System</td>
<td>Name</td>
<td>The Application host name.</td>
<td>app-host-1</td>
</tr>
<tr>
<td>Application host</td>
<td></td>
<td>IP Address</td>
<td>Should be a dotted IP address.</td>
<td>10.1.139.42</td>
</tr>
<tr>
<td>Application host</td>
<td></td>
<td>Username</td>
<td>The username.</td>
<td>admin</td>
</tr>
<tr>
<td>Application host</td>
<td></td>
<td>Password</td>
<td>The password.</td>
<td>password</td>
</tr>
<tr>
<td>Storage virtualizer VPLEX</td>
<td>VxBlock System</td>
<td>Type</td>
<td>Must be the following: VPLEX</td>
<td>VPLEX</td>
</tr>
<tr>
<td>Storage virtualizer VPLEX</td>
<td></td>
<td>Component tag</td>
<td>Can be any meaningful value.</td>
<td>VPLEX-000-XXX</td>
</tr>
<tr>
<td>Storage virtualizer VPLEX</td>
<td></td>
<td>Address</td>
<td>Should be a dotted IP address.</td>
<td>10.1.139.5</td>
</tr>
</tbody>
</table>
### Configuring Vision software to discover a VxRail Appliance

#### Configuring a VxRail Appliance using the configuration editor

Use the configuration editor in attended mode and a user interface guides you through the process of creating a VxRail Appliance configuration file. Vision software then discovers the VxRail Appliance on an existing MSM VM. You can view the VxRail Appliance and its components through the Vision dashboard.

#### Before you begin

Ensure you have the IP address of the VxRail Manager Extension.

#### About this task

Vision software uses the IP address of a VxRail Manager Extension to discover a VxRail Appliance. VxRail Manager Extension automatically detects a new VxRail Appliance when it is added to a cluster.

---

<table>
<thead>
<tr>
<th>Component type</th>
<th>VCE Systems</th>
<th>Field</th>
<th>Rules</th>
<th>Field value example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage virtualizer</td>
<td>VPLEX</td>
<td>Method</td>
<td>Must be xml.</td>
<td>xml</td>
</tr>
<tr>
<td>Storage virtualizer</td>
<td>VPLEX</td>
<td>Username</td>
<td>The username.</td>
<td>service</td>
</tr>
<tr>
<td>Storage virtualizer</td>
<td>VPLEX</td>
<td>Password</td>
<td>The password.</td>
<td>password</td>
</tr>
<tr>
<td>Storage virtualizer</td>
<td>ScaleIO</td>
<td>VxRack System</td>
<td>Type</td>
<td>Must be the following: SCALEIO</td>
</tr>
<tr>
<td>Storage virtualizer</td>
<td>ScaleIO</td>
<td>Component tag</td>
<td>Can be any meaningful value.</td>
<td>SCALEIO-000-XXX</td>
</tr>
<tr>
<td>Storage virtualizer</td>
<td>ScaleIO</td>
<td>Address</td>
<td>Should be a dotted IP address.</td>
<td>10.3.249.240</td>
</tr>
<tr>
<td>Storage virtualizer</td>
<td>ScaleIO</td>
<td>Method</td>
<td>Must be restApi</td>
<td>restApi</td>
</tr>
<tr>
<td>Storage virtualizer</td>
<td>ScaleIO</td>
<td>Username</td>
<td>The username.</td>
<td>admin</td>
</tr>
<tr>
<td>Storage virtualizer</td>
<td>ScaleIO</td>
<td>Password</td>
<td>The password.</td>
<td>password</td>
</tr>
<tr>
<td>DCNM</td>
<td>VxBlock System</td>
<td>address</td>
<td>Should be a dotted IP address.</td>
<td>10.3.249.240</td>
</tr>
</tbody>
</table>

---

**Related information**

- [Configuration editor overview](#) (see page 31)
You can configure the following attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Editable (Y/N)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>User defined</td>
<td>Yes</td>
<td>IP address of the VxRail Manager Extension</td>
</tr>
<tr>
<td>Geo</td>
<td>User defined</td>
<td>Yes</td>
<td>Geographic location of the core data center</td>
</tr>
<tr>
<td>Building</td>
<td>User defined</td>
<td>Yes</td>
<td>Building where the core data center is located</td>
</tr>
<tr>
<td>Floor</td>
<td>User defined</td>
<td>Yes</td>
<td>Floor in the building where the core data center is located</td>
</tr>
<tr>
<td>Room</td>
<td>User defined</td>
<td>Yes</td>
<td>Room where the core data center is located</td>
</tr>
<tr>
<td>Row</td>
<td>User defined</td>
<td>Yes</td>
<td>Row where the core data center is located</td>
</tr>
<tr>
<td>Tile</td>
<td>User defined</td>
<td>Yes</td>
<td>Tile where the networking cable is accessed in the core data center</td>
</tr>
</tbody>
</table>

The following shows a sample configuration file for a single VxRail Appliance:

<table>
<thead>
<tr>
<th>Component</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>VxRail Appliance</td>
<td>product=VxRAIL</td>
</tr>
<tr>
<td></td>
<td>system=VXRAIL</td>
</tr>
<tr>
<td></td>
<td>type=VxRail</td>
</tr>
<tr>
<td></td>
<td>componentTag=VX</td>
</tr>
</tbody>
</table>
## Procedure

1. Start an SSH session to the MSM VM. Use PuTTY to access the configuration editor for Windows-based systems as non-VSCII supported terminals display styling incorrectly.

2. Enter the root credentials for accessing the MSM VM.

3. Run the following command:

   ```
   configVxRail new <name>
   ```

   The configuration editor opens.

4. Select **Add**. The **VxRail Manager Extension** dialog opens.

5. Enter a valid VxRail Manager Extension IP address in the **VxRail Manager Extension Address** field.

   **NOTE:** You must enter a unique IP address for each VxRail Manager Extension within a VCE System. If you have more than one VCE System, you can enter the same IP address for VxRail Manager Extensions.
When all the VxRail Manager Extension IP addresses are added, select **Save**. The **Save** dialog opens and displays the following message:

Are you sure want to save your changes?

- Select **Yes** to save the changes.
- Select **No** if you do not want to save the changes.

**What to do next**

Verify that Vision software discovered the VxRail Appliance by completing the following steps:

1. As the Vision administrator, log on to the Vision dashboard.

   ☑️ **NOTE:** If you have System and Location privileges, you can log on to Vision dashboard as a Vision user.

2. Select the **Details** tab.

3. Select the VxRail Appliance that you want to view.

   ☑️ **NOTE:** If you want to view multiple VCE Systems, ensure the **Location** checkbox is selected.

4. Click **Related Components** to view the VxRail Appliance and its components.

**Modifying the configuration file for a VxRail Appliance using the configuration editor (attended mode)**

Use the configuration editor in attended mode to be guided through the process of manually modifying the attributes of a VxRail Appliance through a user interface.

**About this task**

You can modify the following attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>User defined</td>
<td>IP address of the VxRail Manager Extension</td>
</tr>
<tr>
<td>Geo</td>
<td>User defined</td>
<td>Geographic location of the core data center</td>
</tr>
<tr>
<td>Building</td>
<td>User defined</td>
<td>Building where the core data center is located</td>
</tr>
<tr>
<td>Floor</td>
<td>User defined</td>
<td>Floor in the building where the core data center is located</td>
</tr>
<tr>
<td>Room</td>
<td>User defined</td>
<td>Room where the core data center is located</td>
</tr>
<tr>
<td>Row</td>
<td>User defined</td>
<td>Row where the core data center is located</td>
</tr>
<tr>
<td>Attribute</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Tile</td>
<td>User defined</td>
<td>Tile where the networking cable is accessed in the core data center</td>
</tr>
</tbody>
</table>

**NOTE:** An attribute that is grayed out cannot be modified.

**Before you begin**

- Ensure the configuration file, for example, `vxrail.cfg`, is created using the `configVxRail` configuration script. [Configuring Vision software to discover a VxRail Appliance](#) (see page 49)

**Procedure**

1. Start an SSH session to the MSM VM. Use PuTTY to access the configuration editor for Windows-based systems as non-VSCII supported terminals display styling incorrectly.

2. Enter the root credentials for accessing the MSM VM.

3. Run the following command:
   ```
   cd /opt/vce/multivbmgmt/conf/vision/UUID
   ```
   **NOTE:** The UUID is the unique ID that is created per configuration.

4. Run the following command:
   ```
   configVxRail update <cfg_name>.cfg
   ```
   **NOTE:** The `<cfg_name>` is the name of the configuration file.

   The configuration editor opens.

5. Follow these steps to edit the attributes of VxRail Manager Extension, for example, change the IP address of VxRail Manager Extension:
   a. In the configuration editor dialog, use the **Next** and **Back** options to navigate to the VxRail Manager Extension whose IP address you want to edit.
   b. Click **Tab** or use the arrow keys to navigate to the **VxRail Manager Extension Address** field.
   c. Edit the VxRail Manager Extension IP address in the **VxRail Manager Extension Address** field.
   d. Click **Save**. The **Save** dialog opens and displays the following message:
      ```
      Are you sure want to save your changes?
      ```
      - Select **Yes** to save the changes.
      - Select **No** if you do not want to save the changes.
What to do next

Verify that the changes made by completing the following steps:

1. As the Vision administrator, log on to the Vision dashboard.
   - **NOTE:** If you have System and Location privileges, you can log on to Vision dashboard as a Vision user.

2. Select the Details tab.

3. Select the VxRail Appliance that you want to view.
   - **NOTE:** If you want to view multiple VCE Systems, ensure the Location checkbox is selected.

4. Click Related Components to view the VxRail Appliance and its components.

Modifying the configuration file for a VxRail Appliance using the configuration editor (unattended mode)

Use the configuration editor in unattended mode to automatically modify the attributes of the VxRail Appliance configuration file.

About this task

You can modify the following attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>User defined</td>
<td>IP address of the VxRail Manager Extension</td>
</tr>
<tr>
<td>Geo</td>
<td>User defined</td>
<td>Geographic location of the core data center</td>
</tr>
<tr>
<td>Building</td>
<td>User defined</td>
<td>Building where the core data center is located</td>
</tr>
<tr>
<td>Floor</td>
<td>User defined</td>
<td>Floor in the building where the core data center is located</td>
</tr>
<tr>
<td>Room</td>
<td>User defined</td>
<td>Room where the core data center is located</td>
</tr>
<tr>
<td>Row</td>
<td>User defined</td>
<td>Row where the core data center is located</td>
</tr>
<tr>
<td>Tile</td>
<td>User defined</td>
<td>Tile where the networking cable is accessed in the core data center</td>
</tr>
</tbody>
</table>

The following is a list of commands and optional parameters:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-u --unattended</td>
<td>Runs in the unattended configuration tool</td>
</tr>
<tr>
<td>-v --verbose</td>
<td>Shows more detailed information</td>
</tr>
</tbody>
</table>
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h --help</td>
<td>Shows this help</td>
</tr>
<tr>
<td>--iv</td>
<td>Ignores validation results</td>
</tr>
</tbody>
</table>

## Before you begin

- Ensure the configuration file, for example, `vxrail.cfg`, is created using the `configVxRail` configuration script. *Configuring Vision software to discover a VxRail Appliance* (see page 49)

## Procedure

1. Modify the attributes in the `vxrail.cfg` file.
   - **NOTE:** If you modify the attributes of more than one VxRail Manager Extension, you must index each VxRail Manager Extension address.
   
   For example:
   ```
   VxRailManagers.VxRailManager[1].address=127.0.0.1
   VxRailManagers.VxRailManager[2].address=127.0.0.2
   VxRailManagers.VxRailManager[3].address=127.0.0.3
   ```

2. You can run either of the following commands:
   ```
   cd/opt/vce/multivbmgt/conf/vision/UUID
   configVxRail update VXRAIL.cfg -u
   ```
   ```
   configVxRail update /opt/vce/multivbmgt/conf/vision/UUID/VXRAIL.cfg -u
   ```
   - **NOTE:** The UUID is the unique ID that is created per configuration.

3. Run the following command:
   ```
   configVxRail update VXRAIL.cfg -u
   ```
   - **NOTE:** The `<cfg_name>` is the name of the configuration file.

## What to do next

1. Manually restart the Tomcat service by running:
   ```
   service tomcat restart
   ```

2. Manually restart the multivbmgmt service by running:
3. As the Vision administrator, log on to the Vision dashboard.

**NOTE:** If you have System and Location privileges, you can log on to Vision dashboard as a Vision user.

4. Select the Details tab.

5. Select the VxRail Appliance that you want to view.

**NOTE:** If you want to view multiple VCE Systems, ensure the Location checkbox is selected.

6. Click Related Components to view the VxRail Appliance and its components.
Using the Vision dashboard

Vision dashboard overview

The dashboard is an application used to manage and monitor VCE Systems in a data center.

Use the dashboard to:

• View the health/compliance of multiple VCE Systems.
• Run a compliance scan on one or more VCE Systems.
• Issue a freeform or assisted search (wizard), and display the returned list of items in a consumable format.
• View charts of key performance indicators (KPI) for one or more components or elements.
• Configure multisystem Active Directory integration and map AD Groups to Vision roles (for authorized Vision administrators).
• Enable and disable optional packages, such as the Vision Security Compliance Module.
• Download software and firmware components to maintain compliance with the current RCM.

Vision dashboard layout

The dashboard provides a browser-based interface to manage and access information about the VCE Systems in a data center.
Overview

The following figure shows the layout of the dashboard. The toolbar is available on every page. The dashboard provides all available information about the latest search results. When you first log in, the dashboard searches for all VCE Systems.

Toolbar

Provides a search field and a management menu at the top of every page of the dashboard

Overview

Displays status information about items selected in the Search Results

Details

Displays detailed information about the attributes of items in your search results

Related Components

Displays components related to an item that you select from the Search Results
Search Results

Lists the results from the latest search. When you click on an item in the search results, the dashboard is updated to highlight status information for the selection.

Actions

Lists the tasks that you can perform on your search results.

Refer to the dashboard help for more information about the features of the dashboard.

Related information

Monitoring VM resources (see page 142)

Ensuring VCE System compliance (see page 107)

Health monitoring (see page 134)

Using the search tools (see page 153)

Working with key performance indicators (KPIs) (see page 164)

Accessing the Vision dashboard

Accessing the Vision dashboard provides you with a display where you can assess the status of your VCE System.

Before you begin

You need the following information to access the dashboard:

- Fully-qualified domain name (FQDN) of the multisystem management (MSM) VM.
- A username and password with access to the Vision dashboard.
- One of the following supported browsers:
  - Google Chrome
  - Microsoft Internet Explorer, Version 11

The dashboard supports a minimum screen resolution of 1280 x 1024.
Procedure

1. Use a web browser to navigate to the MSM VM.
   The URL format is https://FQDN, where FQDN is the fully qualified domain name of the MSM VM.

   ○ NOTE: The MSM VM has to be able to ping the FQDN of the Vision Core VM. If it cannot, a host file entry for the Vision Core VM must exist on the MSM VM.

2. Log on with your username and password.
   The default credentials for the dashboard are:
   - Username: admin
   - Password: D@ngerous1

   ○ NOTE: This password should be changed to protect the system from unauthorized access.

   If this is the first time you have opened the dashboard, there is a quick tour of some of the new features.

3. When you finish the tour, click End Tour.

Results

The dashboard initially displays the list of VCE Systems.
Using the Vision shell

NOTE: In Vision software, the Vision shell is supported only on a Vblock System or a VxBlock System.

Vision shell

The Vision shell is an extensible management tool that provides a single interface to manage and configure VCE Systems and components.

The Vision shell removes the complexity of working with individual component interfaces for management and configuration tasks and provides a plug-in structure that can be extended to include additional functionality. Vision shell creates an abstraction layer that removes the burden of having to use different login credentials, IP addresses, and syntax to make configuration changes across multiple components. Vision shell can help manage multiple VCE Systems.

For example, suppose you must update the NTP server IP addresses configured for all switches on a VCE System. By issuing a single command, this change is made without having to log on to each component and perform the task one switch at a time:

```bash
Vision> ntp switch set ['10.1.139.235', '10.1.219.13']
[Switch 'N5B' at 10.1.139.23:, result: ['10.1.139.235', '10.1.219.13'],
 Switch 'N5A' at 10.1.139.22:, result: ['10.1.139.235', '10.1.219.13'],
 Switch 'MGMT-N3B' at 10.1.139.2:, result: ['10.1.139.235', '10.1.219.13'],
 Switch 'MGMT-N3A' at 10.1.139.1:; result: ['10.1.139.235', '10.1.219.13'],
 Switch 'N1A' at 10.1.140.235:, result: ['10.1.139.235', '10.1.219.13'],
 Switch 'M9A' at 10.1.139.20:, result: ['10.1.139.235', '10.1.219.13'],
 Switch 'M9B' at 10.1.139.21:, result: ['10.1.139.235', '10.1.219.13']]
```


The shell is a framework layer built on top of Python and Vision API bindings. In addition to the commands provided, any valid Python command can be run in the shell.

Developers writing extensions for the Vision shell can provide a single interface for all components and enable users to:

- Perform operations on each VCE System as a single logical entity rather than a collection of components.
- Configure and manage settings at the individual VCE System component level.

See the Dell EMC Vision Intelligent Operations Shell Developer's Guide for information about developing your own extensions. Developers working on shell extensions should register with the VCE developer forum at http://www.vce.com/developers. Use this forum for any issues or questions regarding the development of new Python extensions to the Vision shell environment.

Accessing the Vision shell session

Access a Vision shell session to manage and configure your Vblock System or VxBlock System.
Procedure

1. Establish an SSH connection to the MSM VM and log on. The default credentials are:
   - Username: root
   - Password: V1rtu@1c3!
   This password should be changed to protect the system from unauthorized access.

2. Run the following command: vshell
   
   The Vision shell initializes with the following messages.

   VCE Vision shell 3.5.0.0
   Copyright 2013-2016 VCE Company, LLC. All rights reserved.
   VCE, VCE Vision, VCE Vscale, Vblock, VxBlock, VxRail and the VCE logo are registered trademarks or trademarks of VCE Company LLC.
   All other trademarks used herein are the property of their respective owners.
   MSM Hostname (Press Enter for localhost):

   ☢️| NOTE: As an alternative, you can skip the log on prompts by starting shell with the following option:

   vshell -l conf/ipython.conf

3. Enter the MSM hostname to which you want to connect, or press Enter for the localhost.

4. When prompted, enter your username and password. The default administrative credentials for Vision shell are:
   - Username: csadmin
   - Password: D@ngerous1
   This password should be changed to protect the system from unauthorized access.

Results

The following message indicates that Vision shell has completed initialization and is ready for operation.

Initializing. . . . . . [Done]
Type "help" for an introduction to VCE Vision shell
or type "show" to see a list of available commands
Vision>

What to do next

Changing the default password for the root and vision accounts (see page 83)

Change the password for the Vision shell administrator (see page 96)
Running Vision shell from a remote host

Follow these steps to install Vision 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.
- You need the hostname for the MSM node you want to connect to.

Procedure

1. Download the RPM to the host where you want to install Vision shell.
2. Enter the following command from the same directory where the RPM is located:

```bash
rpm -Uvh vision-shell-remote-x.x.x.x-build_number.x86_64.rpm
```

where:

- `x.x.x.x` is the Vision software release number.
- `build_number` is the unique identifier of the Vision shell build.

3. After the installation completes, enter the following command from a command prompt:

```
vshell
```

4. When prompted, enter the fully-qualified domain name for the MSM node.
5. When prompted, enter your username and password to log on to the shell.

Results

The Vision shell is initialized and ready when the following messages are displayed:

```
Initializing. . . . . [Done]
Type "help" for an introduction to VCE Vision shell
or type "show" to see a list of available commands
Vision>
```

Getting started with shell commands

The shell has commands to help you learn how 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 of the 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. For example, show default lists all of the commands in the default extension pack.</td>
</tr>
<tr>
<td>show component_type</td>
<td>Lists all of the commands for a specific component. For example, show storagearray lists all of the commands that can be performed with storage arrays.</td>
</tr>
</tbody>
</table>

In the output of the show command, 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.

**NOTE:** The following commands are often listed by the show command. These commands are intended for shell extension developers and not useful for any other purpose:

- %cs_template
- %hello_world
- %check_max_config
Accessing 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:

```
Vision>connect?
Type:      Magic function
String Form:<bound method CShellExtension8.CShellExtension8 of <vshell.vision_defs.CShellExtension8 ...
Namespace: IPython internal
File:      /opt/vce/shell/vshell/vision_defs.py
Definition: connect(self, line)
Docstring:
Opens an interactive connection with the target component's command line interface. Only one device can be connected at a time. Terminate the session to return to the VCE Vision shell session.
Syntax: %connect <target>
Input:
  <target> is a VCE System component or components specified by index number.
For example:
  switch[1]: Indicates the second switch by index number (where 0 indicates the first position in a list of switches)
Examples:
  connect computesystem[0]
  Returns: The command line prompt for the specified compute system along with any related login messages
  connect switch[0]
  Returns: The command line prompt for the specified switch along with any related login messages
Compatibility:
  Nexus switches
  Storage arrays
  UCS
```

Related information

[Searching within Vision shell](#) (see page 153)

**Working with components in Vision shell**

Commands in the Vision shell allow you gather information and make configuration changes to components across one or more VCE Systems.

**Working with switches**

Use the Vision shell to gather information about switches across all VCE Systems and to make configuration changes.
Gathering information about switches

Use these commands for getting information about the switches for the VCE Systems.

Get a list of switches

Run the shell `switch` command to list all switches in the network. You can also use `sw` as a shortcut, for example:

```
Vision>sw
[Switch 'N5B' at 10.1.140.23 in Vblock 'Vb-720',
 Switch 'M9B' at 10.1.140.21 in Vblock 'Vb-720',
 Switch 'M9A' at 10.1.140.20 in Vblock 'Vb-720',
 Switch 'M9B' at 10.1.140.21 in Vblock 'Vb-720',
 Switch 'N1A' at 10.1.140.235 in Vblock 'Vb-720',
 Switch 'N5A' at 10.1.140.22 in Vblock 'Vb-720',
 Switch 'N5A' at 10.1.140.22 in Vblock 'Vb-720',
 Switch 'N5B' at 10.1.140.23 in Vblock 'Vb-720',
 Switch 'N1A' at 10.1.140.235 in Vblock 'Vb-720',
 Switch 'M9A' at 10.1.140.20 in Vblock 'Vb-720']
```

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. For example, specifying `switch[0]` refers to the first switch in the previous output:

```
Vision>switch[0]
Switch 'N5B' at 10.1.140.23 in Vblock 'Vb-720'
```

**By alias**

The alias for the switch is found in the first string on each line of the `switch` command output. Examples from the previous output include 'N5B' and 'M9A'.

**By IP address**

You can reference any switch by the IP address provided by the `switch` command output. For example, the following command displays runs the `show banner motd` command for the switch with the IP address, 10.1.140.235.

```
Vision>%run_commands 10.1.140.235 'show banner motd'
'\n**\n\n**W A R N I N G** THIS IS A PRIVATE COMPUTER SYSTEM. This computer system including all related equipment, network devices, are provided only for authorized use. \nWARNING: Unauthorized access to this system is forbidden and will be prosecuted by law. \n''
```

Retrieving detailed information about a switch

Use the Python `print` command to get detailed information about the attributes of a switch. You must refer to the switch by index number, for example:

```
Vision>print switch[4]
All current attributes:
```
aaaCommandAuthorizationIsApplicable : true
aaaCommandAuthorizationIsError : false
accountingConfigurationIsApplicable : true
accountingConfigurationIsError : false
accountingConfigurationValue : default: local
alias : N5A
authenticationConfigurationIsApplicable : true
authenticationConfigurationIsError : false
authenticationConfigurationValue : default: local;console: local
authenticationStatusEnabledIsApplicable : true
authenticationStatusEnabledIsError : false
authenticationStatusEnabledValue : false
authorizationConfigurationIsApplicable : true
authorizationConfigurationIsError : false
authorizationConfigurationValue : pki-ssh-cert: local;pki-ssh-pubkey: local
bannerIsApplicable : true
bannerIsError : false
bannerValue : ***W A R N I N G*** THIS IS A PRIVATE COMPUTER SYSTEM. This computer system including all related equipment, network devices, are provided only for authorized use. All computer systems may be monitored for all lawful purposes, including those activities that are authorized for management of the system. All information including personal information, stored or sent over this system may be monitored. Uses of this system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. WARNING: Unauthorized access to this system is forbidden and will be prosecuted by law. By accessing this system, you agree that your actions may be monitored.
calculatedStatus : minor
cdpServiceEnabledIsApplicable : true
cdpServiceEnabledIsError : false
cdpServiceEnabledValue : true
client : <vshell.convergedclient.ConvergedClient object at 0x3037850>
communicationHttpEnabled : false
communicationSshEnabled : true
communicationTelnetEnabled : false
cvmHost : vision174-15.vb300swqa.vcemo.lab
dataCenter : voltronlanddc
description : Nexus5000
firmwareRev : 5.2(1)N1(7)
hardwareRev : 0.0
hardwareRevision : 0.0
host : vision174-105.vb700swqa.vcemo.lab
hostinstance : <vshell.convergedclient.ConvergedHost instance at 0x623f3b0>
ipAddress : 10.1.139.22
ipSourceRoutingIsApplicable : true
ipSourceRoutingIsError : false
ipSourceRoutingValue : true
isFRU : false
isdeleted : False
lastOperStatus : notApplicable
lastStatusChange : 2015-04-01T23:09:10.656Z
lldpServiceEnabledIsApplicable : true
lldpServiceEnabledIsError : false
lldpServiceEnabledValue : true
locationNumber : 0
locationPosition : 0
manufacturer : Cisco Systems, Inc.
memoryUtilization : 0
modelName : N5K-C5548P
name : vb300swqa-N5548-A
ntpEnabledIsApplicable : true
ntpEnabledIsError : false
ntpEnabledValue : true
ntpPeerConfigurationIsApplicable : true
ntpPeerConfigurationIsError : false
ntpServerConfigurationIsApplicable : true
ntpServerConfigurationIsError : false
### ntpServerConfigurationValue
- `10.11.6.4;10.1.219.13`

### operStatus
- `minor`

### processorUtilization
- `0`

### properties
- `{}`

### remoteSyslogEnabledApplicable
- `true`

### remoteSyslogEnabledError
- `false`

### remoteSyslogEnabledValue
- `true`

### serialNum
- `SSI15060FVB`

### slibHost
- `vision174-105.vb700swqa.vcemo.lab`

### snmpReadOnlyConfigurationApplicable
- `true`

### snmpReadOnlyConfigurationError
- `false`

### snmpReadOnlyConfigurationValue
- `convergedtest`

### snmpReadWriteConfigurationApplicable
- `true`

### snmpReadWriteConfigurationError
- `false`

### snmpReadWriteConfigurationValue
- `nx5kpublic;public`

### snmpServiceEnabledApplicable
- `true`

### snmpServiceEnabledError
- `false`

### snmpServiceEnabledValue
- `true`

### softwareRev
- `5.2(1)N1(7)`

### sshKeySizeApplicable
- `true`

### sshKeySizeError
- `false`

### sshKeySizeValue
- `2048`

### strongPasswordEnabledApplicable
- `true`

### strongPasswordEnabledError
- `false`

### strongPasswordEnabledValue
- `true`

### switchInOctets
- `26949994008.0`

### switchOutOctets
- `25570906268.0`

### switchType
- `Nexus5k`

### time
- `1429021800000`

### uid
- `10.1.139.22`

### unusedRouterInterfaceEnabledApplicable
- `true`

### unusedRouterInterfaceEnabledError
- `false`

### unusedRouterInterfaceEnabledValue
- `Eth1/5;Eth1/26;Eth1/28`

### vblockBuilding
- `2635 Derimian Parkway`

### vblockDescription
- `VB340-976-319-643`

### vblockGeo
- `DURHAM, NC`

### vblockModelName
- `340w5400`

### vblockSerialNo
- `VB340-976-319-643`

### vblockTag
- `VB-340`

### vendor
- `Cisco Systems, Inc.`

### visionVersion
- `x.x.x.x`

### vtyConsoleExecTimeoutApplicable
- `true`

### vtyConsoleExecTimeoutError
- `false`

### vtyConsoleExecTimeoutValue
- `0`

### vtyLineExecTimeoutApplicable
- `true`

### vtyLineExecTimeoutError
- `false`

### vtyLineExecTimeoutValue
- `525599`

### vtyLineSessionLimitApplicable
- `true`

### vtyLineSessionLimitError
- `false`

### vtyLineSessionLimitValue
- `64`

---

**NOTE:** Python commands like `print` are not available using the MSM REST API for Vision shell.

### Finding switches by attributes

You can search to find switches by attribute value, using the same search syntax in the Vision dashboard. For example, to find all switches with operating status that is not 'operable', issue this command:

```
Vision>find switch where operStatus != operable
[Switch 'N5A' at 10.1.140.22 in Vblock 'Vb-720', Switch 'M9A' at 10.1.140.20 in Vblock 'Vb-720']
```

**NOTE:** Search syntax in Vision shell is case-sensitive.
For more information about search syntax, refer to Searching within Vision shell (see page 153).

Shell commands for switches

Use these commands to perform inquiries and configuration changes on switches for VCE Systems.

To see a list of all commands that are available when working with switches, issue the show switch command. The output lists the commands along with a brief description.

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. 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>

Working with storage

Use the Vision shell to gather information about storage across all VCE Systems and to make configuration changes.

Some commands will not make updates in storage until you create a user with administrative rights to the storage components. Refer to Creating users with access rights to storage components (see page 91) for more information.

Gathering information about storage

Use these commands for getting information about storage arrays for the VCE Systems.

Get a list of storage arrays

Run the storagearray command in Vision shell to list all storage arrays in the network. You can also use sa as a shortcut, for example:

```
Vision>sa
[Storage Array 'Array-3013' at 10.1.139.6 in Vblock 'VB-340',
 Storage Array '000198701339' at 10.1.140.58 in Vblock 'Vb-340',
 Storage Array 'vcemoVNX5400-CS0' at 10.1.139.50 in Vblock 'VB-340']
```

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. For example, specifying storagearray[0] refers to the first storage array in the previous output:

```
Storage Array 'Array-3013' at 10.1.139.6 in Vblock 'VB-340'
```
By alias

The alias for the storage array is found in the first string on each line of the `storagearray` command output. Examples from the previous output include 'Array-3013', '000198701339', and 'vcemoVNX5400-CS0'.

By IP address

You can reference any storage array by the IP address provided by the `storagearray` command output, for example, 10.1.139.50.

Retrieving detailed information about a storage array

Use the Python `print` command to get detailed information about the attributes of a storage array. You must refer to the storage array by index number, for example:

```python
Vision>print sa[1]
All current attributes:
****************************
alias                          : 000198701339
auditingConfigured             : false
calculatedStatus               : operable
capacityUtilization            : 100.0
client                         : <vshell.convergedclient.ConvergedClient object at 0x3ad9850>
cvmHost                        : vision174-16.vb300swqa.vcemo.lab
dataCenter                     : voltronlanddc
description                    : SYMMETRIX
host                           : vision174-106.vb700swqa.vcemo.lab
hostinstance                   : <vshell.convergedclient.ConvergedHost instance at 0x6b64f80>
hotspareCapacity               : 5271627458240
ipAddress                      : 10.1.140.58
isdeleted                      : False
kBytesRead                     : 3016602433.0
kBytesTransferred              : 7490718309.0
kBytesWritten                  : 4474115876.0
lastOperStatus                 : notApplicable
lastStatusChange               : 2015-04-08T13:41:45.435Z
ldapConfigured                 : false
modelName                      : VMAX10K
name                           : Symmetrix Array 000198701339
operStatus                     : operable
properties                     : {}
readIOs                        : 85261241.0
remainingManagedSpace          : 0.0
remainingManagedSpacePercentage : 0.0
remainingRawCapacity           : 0.0
remainingRawCapacityPercentage : 0.0
serialNum                      : 000198701339
slibHost                       : vision174-106.vb700swqa.vcemo.lab
softwareRev                    : 5876.268.174
time                           : 1429047000000
totalIOs                       : 2145271236.0
totalManagedSpace              : 188898.526521
totalRawCapacity               : 188898.526521
type                           : VMAX
uid                            : root/
emc:Symm_StorageSystem.CreationClassName="Symm_StorageSystem",Name="SYMMETRIX+000198701339"
usedManagedSpace               : 188898.526521
usedRawCapacity                : 188898.526521
vblockBuilding                 : 2635 Meridian Parkway
vblockDescription              : 720w10k VB720-976-319-643
vblockGeo                      : DURHAM, NC
vblockModelName                : 720w10k
vblockSerialNo                 : VB720-976-319-643
```
Python commands like `print` are not available using the MSM REST API for Vision shell.

### Finding storage arrays by attributes

You can search to find storage arrays by attribute value, using the same search syntax in the Vision dashboard. For example, to find all storage arrays with `remainingRawCapacity` that is less than '1000', issue this command:

```
Vision>: find storagearray where remainingRawCapacity < 1000
[Storage Array '000198701339' at 10.1.140.58 in Vblock 'Vb-340',
 Storage Array 'Array-3013' at 10.1.139.6 in Vblock 'VB-340']
```

**NOTE:** Search syntax in Vision shell is case-sensitive.

For more information about search syntax, refer to [Searching within Vision shell](#) (see page 153).

### Shell commands for storage

Use these commands to perform inquiries and configuration changes on storage arrays for VCE Systems.

To see a list of all commands that are available when with working with storage arrays, issue the `show storage` command. The output lists the commands along with a brief description.

The following commands are for working with storage within the Vision 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 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>

### Working with compute systems

Use the Vision shell to gather information about compute systems across VCE Systems and to make configuration changes.

**NOTE:** The Vision shell does not support gathering information about or making configuration changes to compute systems on VxRack Systems.

### Gathering information about compute systems

Use these commands for getting information about the compute systems for the VCE Systems.
**Get a list of compute systems**

Run the `computesystem` command in Vision shell to list all compute systems in the network. You can also use `ucs` as a shortcut, for example:

```shell
Vision> ucs
[UCS 'VMABO-UCS-1' at 10.1.139.30 in Vblock 'VB-340',
 UCS 'SERVER-B' at 10.1.144.11 in Vblock 'VB-340',
 UCS 'VMABO-UCS-1' at 10.1.140.30 in Vblock 'VB-340']
```

You can address each compute system individually in subsequent commands as follows:

**By index position**

Each system in the `computesystem` command output is assigned an index number, starting with 0, for reference. For example, specifying `computesystem[1]` refers to the second compute system in the previous output:

```shell
UCS 'SERVER-B' at 10.1.144.11 in Vblock 'VB-340'
```

**By componentTag**

The componentTag for the compute system is found in the first string on each line of the `computesystem` command 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 provided by the `computesystem` command output, for example, 10.1.139.30.

**Retrieved detailed information about a compute systems**

Use the Python `print` command to get detailed information about the attributes of a compute system. You must refer to the compute system by index number, for example:

```shell
Vision> print computesystem[0]
All current attributes:
****************************
aaaServiceEnabled              : true
alias                          : VMABO-UCS-1
async_handle                   : CShellHandle-97762640         :<bound method
ComputeSystem.banner_ucs of UCS 'VMABO-UCS-1' at 10.1.140.30 in Vblock 'Vb-720'>:Done      :
100%
calculatedStatus               : minor
client                         : <vshell.convergedclient.ConvergedClient object at 0x2869850>
communicationCimxmlEnabled     : true
communicationHttpEnabled       : false
communicationHttpsEnabled      : true
communicationSshEnabled        : true
communicationTelnetEnabled     : false
compute_type                   : UCSM
cvmHost                        : vision174-16.vb300swqa.vcemo.lab
dataCenter                     : voltronlanddc
defaultCIMCPasswordIsApplicable : false
defaultCIMCPasswordIsError     : false
description                    : Cisco UCS System
firmwareRev                     : 2.2(3b)
handle                         : <UcsSdk.UcsHandle.UcsHandle instance at 0x5cbd638>
```
Python commands like print are not available using the MSM REST API for Vision shell.

### Finding compute systems by attributes

You can search to find compute systems by attribute value, using the same search syntax in the Vision dashboard. For example, to find all servers located in 'Geneva', issue this command:

```
Vision>find computesystem where vblockGeo = Geneva
(UCS 'VMABO-UCS-1' at 10.1.140.30 in Vblock 'Vb-340',
UCS 'VMABO-UCS-1' at 10.1.139.30 in Vblock 'VB-340')
```

⚠️**NOTE:** Search syntax in Vision shell is case-sensitive.

For more information about search syntax, refer to [Searching within Vision shell](#) (see page 153).
Shell commands for compute systems

Use these commands to perform inquiries and configuration changes on compute systems for VCE Systems.

To see a list of all commands that are available when working with compute systems, issue the show computestystem command. The output lists the commands along with a brief description.

The following commands are for working with compute systems within the Vision 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 two components.</td>
</tr>
<tr>
<td>%refresh_handle</td>
<td>Refreshes the SDK connection handle for the target device.</td>
</tr>
</tbody>
</table>

Working with VMware ESXi hosts

Use the Vision shell to gather information about ESXi hosts across all VCE Systems and to make configuration changes.

Before starting these tasks, log on to the Vision shell. Refer to Accessing the Vision shell (see page 61) for more information.

Gathering information about VMware ESXi hosts

Use these commands for getting information about the ESXi hosts for the VCE Systems.

Get a list of ESXi hosts

Run the esxi command in Vision shell to list all ESXi hosts in the network, for example:

```
Vision>esxi
[ESXi Host 'pe31-esx02.example.lab' at 10.3.32.199 in vcesystem 'VB-340',
 ESXi Host 'pe31-esx03.example.lab' at 10.3.32.200 in vcesystem 'VB-340',
 ESXi Host 'pe31-esx01.example.lab' at 10.3.32.196 in vcesystem 'VB-340',
 ESXi Host 'pe31-esx04.example.lab' at 10.3.32.201 in vcesystem 'VB-340']
```

You can address each 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. For example, specifying esxi[2] refers to the third host in the previous output:

```
ESXi Host 'pe31-esx01.example.lab' at 10.3.32.196 in vcesystem 'VB-340'
```

Retrieving detailed information about an ESXi host

Use the Python print command to get detailed information about the attributes of an ESXi host, for example:
Vision>print esxi[0]
All current attributes:
******************************
VCID                           : BE78F8CE-4851-49A2-8C8F-D67800B283D4
allocatedStorageMB             : 94388651.0
blockForgedMACTxIsApplicable   : false
blockForgedMACTxIsError        : false
blockMACAddressChangesIsApplicable : false
build                          : 1746974
calculatedStatus               : critical
calculatedStatus               : critical
client : <vshell.convergedclient.ConvergedClient
object                                                      at 0x5527190>
cvmHost                        : slib-auto-test23.example.lab
dataCenter                     : florencedatacenter
description                    : VMware ESXi 5.5.0 build-1746974
directConsoleUserInterfaceEnabledValue : true
directConsoleUserInterfaceEnabledValue : true
emcpVersion                    : EMC PowerPath (c) Version 5.9 SP1 (build 11),
                                  built on: Dec 3 2013
enicVersion                    : Version 2.1.2.38, Build: 1198611, Interface:
                                  9.2 Built on: Sep 5 2013
entityObjectId                 : host-82
esxi                           : None
fnicVersion                    : Version 1.5.0.45, Build: 1198611, Interface:
                                  9.2 Built on: Jul 31 2013
freeStorageMB                  : 84387406.0
host                           : slib-auto-test34.example.lab
hostinstance                   : <vshell.convergedclient.ConvergedHost
instance                                                      at 0x6341098>
ipAddress                      : 10.3.32.199
isdeleted                      : False
lastOperStatus                 : notApplicable
lastStatusChange               : 2015-07-22T13:49:40.539Z
lockdownModeEnabledIsApplicable : true
lockdownModeEnabledIsError     : false
lockdownModeEnabledValue       : false
modelName                      : embeddedEsx
name                           : pe31-esx02.example.lab
ntpServerConfigurationIsApplicable : true
ntpServerConfigurationIsError  : false
operStatus                     : critical
osName                         : esxi
osType                         : vmnx-x86
overallCpuUsage                : 2.0
properties                     : {}
shellInteractiveTimeoutValue   : 0.0
shellStatusValue               : false
shellTimeoutValue              : 0.0
si                             : None
slibHost                       : slib-auto-test34.example.lab
sshEnabledValue                : false
time                           : 1437596385285
uid                            : BE78F8CE-4851-49A2-8C8F-D67800B283D4-host-82
uniqueId                       : BE78F8CE-4851-49A2-8C8F-D67800B283D4-host-82
vceSystemBuilding              : 350 Campus
vceSystemDescription           : 340w5600 VB340-975-318-642
vceSystemGeo                   : Marlborough, MA
vceSystemModelName             : 340w5600
vceSystemSerialNo              : VB340-975-318-642
vceSystemTag                   : VB-340
vendor                         : VMware
version                        : 5.5.0
visionVersion                  : x.x.x.x

Vision>print esxi[0]
All current attributes:
******************************
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCID</td>
<td>BE78F8CE-4851-49A2-8C8F-D67800B283D4</td>
</tr>
<tr>
<td>allocatedStorageMB</td>
<td>94388651.0</td>
</tr>
<tr>
<td>blockForgedMACTxIsApplicable</td>
<td>False</td>
</tr>
<tr>
<td>blockForgedMACTxIsError</td>
<td>False</td>
</tr>
<tr>
<td>blockMACAddressChangesIsApplicable</td>
<td>False</td>
</tr>
<tr>
<td>blockMACAddressChangesIsError</td>
<td>False</td>
</tr>
<tr>
<td>build</td>
<td>1746974</td>
</tr>
<tr>
<td>calculatedStatus</td>
<td>Critical</td>
</tr>
<tr>
<td>client</td>
<td>&lt;vshell.convergedclient.ConvergedClient object at 0x5527190&gt;</td>
</tr>
<tr>
<td>cvmHost</td>
<td>slib-auto-test23.example.lab</td>
</tr>
<tr>
<td>dataCenter</td>
<td>florencedatacenter</td>
</tr>
<tr>
<td>description</td>
<td>VMware ESXi 5.5.0 build-1746974</td>
</tr>
<tr>
<td>directConsoleUserInterfaceEnabledValue</td>
<td>True</td>
</tr>
<tr>
<td>emcpVersion</td>
<td>EMC PowerPath (c) Version 5.9 SP1 (build 11), Built on: Dec 3 2013</td>
</tr>
<tr>
<td>enicVersion</td>
<td>Version 2.1.2.38, Build: 1198611, Interface: 9.2 Built on:</td>
</tr>
<tr>
<td>entityObjectId</td>
<td>host-82</td>
</tr>
<tr>
<td>esxi</td>
<td>None</td>
</tr>
<tr>
<td>fnicVersion</td>
<td>Version 1.5.0.45, Build: 1198611, Interface: 9.2 Built on:</td>
</tr>
<tr>
<td>freeStorageMB</td>
<td>84387406.0</td>
</tr>
<tr>
<td>host instance</td>
<td>&lt;vshell.convergedclient.ConvergedHost instance at 0x6341098&gt;</td>
</tr>
<tr>
<td>ipAddress</td>
<td>10.3.32.199</td>
</tr>
<tr>
<td>isdeleted</td>
<td>False</td>
</tr>
<tr>
<td>lastOperStatus</td>
<td>notApplicable</td>
</tr>
<tr>
<td>lastStatusChange</td>
<td>2015-07-22T13:49:40.539Z</td>
</tr>
<tr>
<td>lockdownModeEnabledIsApplicable</td>
<td>True</td>
</tr>
<tr>
<td>lockdownModeEnabledIsError</td>
<td>False</td>
</tr>
<tr>
<td>lockdownModeEnabledValue</td>
<td>False</td>
</tr>
<tr>
<td>modelName</td>
<td>embeddedEsx</td>
</tr>
<tr>
<td>name</td>
<td>pe31-esx02.example.lab</td>
</tr>
<tr>
<td>ntpServerConfigurationIsApplicable</td>
<td>True</td>
</tr>
<tr>
<td>ntpServerConfigurationIsError</td>
<td>False</td>
</tr>
<tr>
<td>operStatus</td>
<td>critical</td>
</tr>
<tr>
<td>osName</td>
<td>esxi</td>
</tr>
<tr>
<td>osType</td>
<td>vmnix-x86</td>
</tr>
<tr>
<td>overallCpuUsage</td>
<td>2.0</td>
</tr>
<tr>
<td>properties</td>
<td>{}</td>
</tr>
<tr>
<td>shellInteractiveTimeoutValue</td>
<td>0.0</td>
</tr>
<tr>
<td>shellStatusValue</td>
<td>false</td>
</tr>
<tr>
<td>shellTimeoutValue</td>
<td>0.0</td>
</tr>
<tr>
<td>si</td>
<td>None</td>
</tr>
<tr>
<td>slibHost</td>
<td>slib-auto-test34.example.lab</td>
</tr>
<tr>
<td>sshEnabledValue</td>
<td>False</td>
</tr>
<tr>
<td>time</td>
<td>1437596385285</td>
</tr>
<tr>
<td>uid</td>
<td>BE78F8CE-4851-49A2-8C8F-D67800B283D4-host-82</td>
</tr>
<tr>
<td>uniqueId</td>
<td>BE78F8CE-4851-49A2-8C8F-D67800B283D4-host-82</td>
</tr>
<tr>
<td>vceSystemBuilding</td>
<td>350 Campus</td>
</tr>
<tr>
<td>vceSystemDescription</td>
<td>340w5600 VB340-975-318-642</td>
</tr>
<tr>
<td>vceSystemGeo</td>
<td>Marlborough, MA</td>
</tr>
<tr>
<td>vceSystemModelName</td>
<td>340w5600</td>
</tr>
<tr>
<td>vceSystemSerialNo</td>
<td>VB340-975-318-642</td>
</tr>
<tr>
<td>vceSystemTag</td>
<td>VB-340</td>
</tr>
<tr>
<td>vendor</td>
<td>VMware</td>
</tr>
<tr>
<td>version</td>
<td>5.5.0</td>
</tr>
<tr>
<td>visionVersion</td>
<td>x.x.x.x</td>
</tr>
</tbody>
</table>

**NOTE:** Python commands like `print` are not available using the MSM REST API for Vision shell.

**Finding ESXi hosts by attribute**

You can search to find ESXi hosts by attribute value, using the same search syntax in the Vision dashboard. You must use the `os` keyword to represent the ESXi hosts. For example, to find all hosts with more than 2999000 megabytes of free storage, issue this command:
NOTE: Search syntax in Vision shell is case-sensitive.

For more information about search syntax, refer to Searching within Vision shell (see page 153).

Shell commands for VMware ESXi hosts

Use these commands to perform inquiries and configuration changes on VMware ESXi hosts for VCE Systems.

To see a list of all commands that are available when working with VMware ESXi hosts, issue the show esxi command. The output lists the commands along with a brief description.

Use the following command to work with VMware ESXi hosts within the Vision shell.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%refresh_handle</td>
<td>Refreshes the SDK connection handle for the target device.</td>
</tr>
</tbody>
</table>

Viewing Vision shell logs

Vision shell keeps activity logs in the /opt/vce/shell/log directory on the MSM VM.

The following log files are available:

- **cs_framework.log**
  
  The framework log keeps a record of every command users enter and the messages returned. The log rotates when it reaches the maximum file size of 10MB. Logs rotate up to five times and a log that has rotated will be appended with a numerical suffix indicating the order in which that log was rotated. For example, cs_framework.log.1 would be the name of the first log after it has reached its maximum file size and is no longer actively being used.

- **extension.log**
  
  The Vision shell extensions record activity to the extensions log file.
• audit.log

The audit log records the following events in Vision shell:

- Event
- User
- Date
- Client hostname
- Command that the user issued

**Viewing Vision shell jobs**

Use the `show_jobs` command 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:

- `esrs_register add`
- `esrs_register delete`
- `esrs_devicemgmt target upload parameters`

To view a list of submitted requests, run the following command: `show_jobs status`

| status   | 1: Running  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2: Partially completed</td>
</tr>
<tr>
<td></td>
<td>3: Completed</td>
</tr>
<tr>
<td></td>
<td>4: Failed</td>
</tr>
<tr>
<td></td>
<td>5: Interrupted</td>
</tr>
</tbody>
</table>

For example: the following command returns a list of all jobs that have completed: `show_jobs status=2`

If a job appears in a **RUNNING** status and needs to be canceled, quit the shell session and restart the Vision shell.
Use these commands and scripts to configure, monitor, and maintain the Vision Core VM, MSM VM and MSP VM.

**Vision 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 Vision software configuration files. 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. Run this script from the /opt/vce/fm/install directory.</td>
</tr>
</tbody>
</table>
| collectConfig.sh            | Collects and backs up VCE System configuration files. Run this script from the /opt/vce/fm/bin directory.  

**NOTE:** The collectConfig.sh command is supported on a Vblock System or a VxBlock System only.

| configureSyslogForward      | Configures syslog forwarding.  

**NOTE:** The configureSyslogForward command is supported on a Vblock System or a VxBlock System only.

| configTool.sh               | Configures the vblock.xml file that contains the locations and access credentials for Vblock System components. Vision software uses the vblock.xml to perform the initial discovery of the Vblock System. |

| configureNTP                | Manages network time protocol (NTP) synchronization settings on the Vision Core VM. |

| configureSNMP               | Configures northbound SNMP communication between Vision software and a network management system (NMS) or trap target.  

**NOTE:** The configureSNMP command is supported on a Vblock System or 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 Vision software configuration to the following directory: /opt/vce/fm/back. Run this script from the /opt/vce/fm/bin directory. |

<p>| getFMagentInfo              | Displays version and build information about Vision software. |</p>
<table>
<thead>
<tr>
<th>Command or script</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>install_content.sh</td>
<td>Installs compliance content. Run this script from the <code>/opt/vce/compliance/content</code> directory.</td>
</tr>
<tr>
<td>restoreConfig.sh</td>
<td>Restores Vision software configuration from a backed up file. Run this script from the <code>/opt/vce/fm/install</code> directory.</td>
</tr>
</tbody>
</table>
| setSNMPParams             | Modifies the following SNMP parameters for a VCE System:  
  - sysName  
  - sysContact  
  - sysLocation  
  Use double quotes for values that contain space characters. For example, to change a Vblock System name to Vblock System 700-23, run `setSNMPParams -n sysName "Vblock System 700-23"`. |
| shutdown -h now           | Stops the Vision Core VM.                                                                                                                                                                                    |
| shutdown -r now           | Restarts the Vision 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 System Library FM Agent services. Running this command starts the discovery process.                                                                                                           |
| stopFMagent               | Stops the System Library FM Agent services. Running this command stops the discovery process.                                                                                                                |
| vce-puppet-disable.pp     | Disables the Puppet service management utility from monitoring Vision software services. Run this script from the `/etc/puppet/manifests` directory using the `puppet apply` command. |
| vce-puppet-enable.pp      | Enables the Puppet service management utility to monitor Vision software services. Run this script from the `/etc/puppet/manifests` directory using the `puppet apply` command. |
| vce-puppet-start.pp       | Start all Vision software services. Run this script from the `/etc/puppet/manifests` directory using the `puppet apply` command. This script uses the Puppet service management utility to start services. |
| vce-puppet-stop.pp        | Stop all Vision software services. Run this script from the `/etc/puppet/manifests` directory using the `puppet apply` command. This script uses the Puppet service management utility to gracefully stop services and prevent issues that can occur when stopping services individually. |
| vision start              | Checks if each service is running. If not, starts the service.                                                                                                                                              |
## 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 Vision Core VM to an existing MSM VM.</td>
</tr>
<tr>
<td></td>
<td>Run this script from the /opt/vce/multivbmgmt/ install directory.</td>
</tr>
<tr>
<td>caschangepw.sh</td>
<td>Changes the CAS password for MSM.</td>
</tr>
<tr>
<td></td>
<td>Run this script from the /opt/vce/multivbsecurity/bin directory.</td>
</tr>
<tr>
<td>credential-manager-cli</td>
<td>Lets you manage credentials within the MSM environment.</td>
</tr>
<tr>
<td></td>
<td>Run this script from the /opt/vce/credential-management/bin directory.</td>
</tr>
<tr>
<td>joinMSMCluster.sh</td>
<td>Adds an MSM VM to that node in the cluster.</td>
</tr>
<tr>
<td></td>
<td>Run this script from the /opt/vce/multivbmgmt/ install directory.</td>
</tr>
<tr>
<td>nodetool status</td>
<td>Verifies that Cassandra is installed and configured correctly.</td>
</tr>
<tr>
<td></td>
<td>Run this command from the /opt/cassandra/bin directory.</td>
</tr>
<tr>
<td>service multivbmgmt status</td>
<td>Verifies that the multivbmgmt service is running.</td>
</tr>
<tr>
<td>service multivbmgmt start</td>
<td>Starts the multivbmgmt service.</td>
</tr>
<tr>
<td>service tomcat status</td>
<td>Verifies that the tomcat service is running.</td>
</tr>
<tr>
<td>service tomcat start</td>
<td>Starts the tomcat service.</td>
</tr>
<tr>
<td>service vision-credential-manager</td>
<td>Verifies that the Credential Manager service is running.</td>
</tr>
<tr>
<td>status</td>
<td>Starts the Credential Manager service.</td>
</tr>
<tr>
<td>service vision-credential-manager</td>
<td>Verifies that the compliance service is running.</td>
</tr>
<tr>
<td>start</td>
<td>Starts the compliance 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 Vision shell service is running.</td>
</tr>
<tr>
<td>service vision-shell start</td>
<td>Starts the Vision shell service.</td>
</tr>
<tr>
<td>start_cassandra.sh</td>
<td>Starts Cassandra.</td>
</tr>
<tr>
<td></td>
<td>Run this script from the /opt/cassandra/install directory.</td>
</tr>
<tr>
<td>stop_cassandra.sh</td>
<td>Stops Cassandra.</td>
</tr>
<tr>
<td></td>
<td>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 Vision Web UI service.</td>
</tr>
</tbody>
</table>
## MSP VM commands

<table>
<thead>
<tr>
<th>Command or script</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/opt/vce/msp/install/update-cas-password.sh</code></td>
<td>Allows you update the Central Authentication Service (CAS) password for the admin user in a clustered environment.</td>
</tr>
<tr>
<td><code>/opt/vce/msp/install/update-proxy-password.sh</code></td>
<td>Allows you set a password for a proxy server to access the RCM content distribution network. This script can also be used to change the proxy password if required.</td>
</tr>
<tr>
<td><code>/opt/vce/msp/install/update-assetmanager-db-password.sh</code></td>
<td>Allows you change the default password for the Asset Manager.</td>
</tr>
<tr>
<td><code>/opt/vce/msp/install/update-contentshare-db-password.sh</code></td>
<td>Allows you change the default password for the Content Share PostgreSQL database.</td>
</tr>
<tr>
<td><code>vision status</code></td>
<td>Provides a status on all MSP services.</td>
</tr>
<tr>
<td><code>vision stop</code></td>
<td>Stops all MSP services.</td>
</tr>
<tr>
<td><code>vision start</code></td>
<td>Starts all MSP services.</td>
</tr>
<tr>
<td><code>service vision-contentsource restart</code></td>
<td>Restarts the contentsource service.</td>
</tr>
<tr>
<td><code>service vision-contentsource stop</code></td>
<td>Stops the contentsource service.</td>
</tr>
<tr>
<td><code>service vision-contentsource start</code></td>
<td>Starts the contentsource service.</td>
</tr>
<tr>
<td><code>service vision-contentshare restart</code></td>
<td>Restarts the contentshare service.</td>
</tr>
<tr>
<td><code>service vision-contentshare stop</code></td>
<td>Stops the contentshare service.</td>
</tr>
<tr>
<td><code>service vision-contentshare start</code></td>
<td>Starts the contentshare service.</td>
</tr>
<tr>
<td><code>service vision-downloader restart</code></td>
<td>Restarts the downloader service.</td>
</tr>
<tr>
<td><code>service vision-downloader stop</code></td>
<td>Stops the downloader service.</td>
</tr>
<tr>
<td><code>service vision-downloader start</code></td>
<td>Starts the downloader service.</td>
</tr>
<tr>
<td><code>service vision-assetmanager restart</code></td>
<td>Restarts the assetmanager service.</td>
</tr>
<tr>
<td><code>service vision-assetmanager stop</code></td>
<td>Stops the assetmanager service.</td>
</tr>
<tr>
<td><code>service vision-assetmanager start</code></td>
<td>Starts the assetmanager service.</td>
</tr>
</tbody>
</table>
Managing security

Managing credentials

Managing credentials involves changing the default passwords for Vision software to comply with your organization’s security policies, and also changing access credentials for VCE System components.

Dell EMC recommends that you change all default passwords associated with the Vision software, as well as the access credentials for VCE System components. When logging on to the dashboard, administrators are notified if any default passwords for Vision software are still in use and are prompted to change them.

Any changes made to component credentials will be propagated automatically to the MSM VM. It may take up to five minutes for the MSM VM to be updated with credential changes.

Changing the default password for the root and vision accounts

The Vision Core virtual machine and the MSM VM run on CentOS Linux and have a root user. You should change the default password for the root user on both VMs when you first start using Vision software.

About this task

You can also follow these steps to change the password for the vision user on the MSM VM.

Before you begin

Start an SSH session to the VM and log on.

Procedure

1. Run the following command:

   ```
   passwd
   ```

2. Enter and then confirm the new password when prompted. The following is example output for a successful password change:

   ```
   [root@hostname ~]# passwd
   Changing password for user username.
   New password: 
   Retype new password: 
   passwd: all authentication tokens updated successfully
   ```

   **NOTE:** You must also update the MSM credential manager service with the new password.
Use one of the following steps, depending on whether the password was changed on the Vision Core virtual machine or the MSM VM.

**MSM VM:**

a. Run the following command to change the MSM password for credential manager to match the password changed with the *passwd* command.

```
/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 must be the same as the new password provided on the *passwd* command.
- **username** is either *root* or *vision*, depending on the account you are changing.

**NOTE:** If the password for the MSM admin user account has been changed in a clustered environment, this command fails if the password is not synchronized with the other MSM nodes in the cluster.

The script prompts you for the new password.

b. Enter the new password.

When the password change is complete, the script returns the following message:

```
Successfully created credential for 'root' @ '10.11.12.13'
```

**Vision Core virtual machine:**

a. Log on to the MSM VM as the root user.

b. Type the following command to change the Vision Core virtual machine root user password for MSM:

```
/opt/vce/multivbmgmt/install/addSlibHost.sh <core_IPaddress>
```

where **core_IPaddress** is the IP address for the Vision Core virtual machine where the password was changed.

The script prompts you to update the configuration:

```
Would you like to update existing configuration? (yes/no) [Default = no]:
```

c. Respond by entering **yes**. The script prompts you for the root credentials:

```
Enter the SSH credentials for System Library host 10.20.30.40 (attempt 1 of 3). User name [Default: root]:
```
Enter the root (or press Enter) for the username.

Type the new password for the Vision Core virtual machine.

The script continues processing with a series of messages. When it has finished, the following message is displayed:

```
Vision System Library Host(s) at 10.20.30.40 have been added successfully!
```

The new password for the Vision Core virtual machine is picked up by the MSM VM during the next collection cycle.

**What to do next**

You can optionally specify a password aging policy with the following command:

```
chage
```

Run the following command to view help usage:

```
chage -h
```

**Using the non-administrator account**

Vision software provides a non-administrator account that enables you, as a system administrator, to delegate authority to run administrative commands.

**About this task**

The non-administrator, *vision user*, account allows the person using the account to run any administrative command using `sudo`, as if they were user root.

**NOTE:** The non-administrator account is valid on the MSM VM only.

**Before you begin**

Connect to the MSM VM.

**Procedure**

1. To use the vision user account, log on using the following credentials:
   
   - Username: *vision*
   
   - Password: `L!NkT@T3cA`

2. To switch to the user root account while logged on as the *vision user*, run the following command:

   ```
su - root
   ```
Changing the Central Authentication Service (CAS) password for Vision Core VM

Vision software uses a Central Authentication Service (CAS) for authentication to web services. You should change the default password for the admin user, which has full administrator privileges, as a best practice.

About this task

Changing the CAS password involves running a script on the Vision Core VM that updates the password, encrypts it, and then saves it internally. After this password is changed, any Client applications that are configured with it will also need to be updated.

The default CAS administrator credentials are as follows:

- Username: admin
- Password: 7j@m4Qd+1L

Before you begin

- Determine a new password, understanding that the CAS password:
  - Is case sensitive.
  - Must be between 8 and 20 characters in length.
  - Must include one uppercase letter, one digit, and one special character.
  - Cannot contain any of the following special characters: \ / % + ' " ( ) ; : < > |
- Connect to the Vision Core VM

Procedure

1. Run the following command:

```
/opt/vce/fm/bin/slibCasChangepw.sh
```

The script prompts you with the following message:

```
Warning: This script will restart JBoss, Vision FM Agent and other services. Please ensure that a maintenance window has been scheduled, and there is no active upgrade session going on.

Do you want to continue ([y/n])?
```

2. Enter y to continue. The script then prompts you with the following:

```
Please enter current user password:
```
3 Enter the current password for the admin user.

The script then prompts you with the following:

```
Please enter new password (Press Ctrl C to exit):
```

4 Enter the new password for the admin user and then confirm it when prompted.

The script restarts services and displays the following message when it is finished:

```
CAS password has been changed for admin user.
If any other client applications are using this password, please update them.
```

**Changing the Central Authentication Service (CAS) password for multisystem management (MSM)**

MSM uses a Central Authentication Service (CAS) for authentication to its services. You should change the default administrator password as a best practice. You can also change the default CAS password for users as appropriate.

**About this task**

Changing the CAS password for the default administrator involves running a script on the MSM VM that updates the password, encrypts it, and then saves it to an internal database.

The default CAS administrator credentials are as follows:

- **Username:** `admin`
- **Password:** `D@ngerous1`

**Before you begin**

Connect to the MSM VM.
Procedure

1. Run the following command:

```
/opt/vce/multivbsecurity/bin/caschangepw.sh
```

The script prompts you with the following message:

```
Warning: This script will restart Tomcat and other services.
Please ensure that a maintenance window has been scheduled,
and there is no active upgrade session going on.

Do you want to continue ([y/n])?
```

**Attention:**

During the processing of this script, the services required for the operation of Vision software are stopped and restarted. If the script is terminated during the process, either by issuing `Ctrl + Z` or terminating the SSH session, some Vision services are not restarted. The MSM VM has to be restarted to regain full operation.

2. Enter `y` to continue. The script then prompts you with the following:

```
Please enter current admin password:
```

3. Enter the current password for the admin user. The script then prompts you with the following:

```
Please enter new password(Press Ctrl C to exit):
```

4. Enter the new password for the admin user and then confirm it when prompted.

The CAS password:

- Is case sensitive.
- Must be between 8 and 20 characters in length.
- Must include one uppercase letter, one digit, and one special character.
- Cannot contain any of the following special characters: `\ / % + ' " ( ) ; : < > |`

The script restarts services and displays the following message:

```
CAS password has been changed for admin user.
Please update any other client applications using this password.
```

What to do next

**NOTE:** You must also update the CAS password on the multisystem prepositioning (MSP) VM to match the updated password on the MSM VM. Refer to the related topic for information on how to do this.
In a clustered environment containing multiple MSM nodes, you must also synchronize the passwords on each MSM node with this new password.

Related information

Changing the CAS password for the MSP VM to match the CAS password on the MSM VM (see page 90)

Synchronizing the CAS password for the admin user in a clustered environment (see page 89)

**Synchronizing the CAS password for the admin user in a clustered environment**

In a clustered environment containing multiple MSM nodes, if the CAS password for the MSM admin username is changed on one node, the password must be changed on all other MSM nodes to make them all identical.

**Before you begin**

You need the new password that was changed on the first MSM node. For example, if the password was changed to `pA55w0R#d` on the first MSM node, use this password for these steps.

**Procedure**

1. Connect to the MSM VM.
2. Run the following command:
   ```
   /opt/vce/multivbsecurity/bin/caschangepw.sh
   ```
   The script prompts you with the following message:
   
   Warning: This script will restart Tomcat and other services. Please ensure that a maintenance window has been scheduled, and there is no active upgrade session going on.

   Do you want to continue ([y/n])?

   **Attention:** During the processing of this script, the services required for the operation of Vision software are stopped and restarted. If the script is terminated during the process, either by issuing `Ctrl + Z` or terminating the SSH session, some Vision services are not restarted. The MSM VM has to be restarted to regain full operation.

3. Enter `y` to continue. The script then prompts you with the following:

   Please enter current admin password:
Enter the new admin password that was changed on the first MSM node, for example, pA55w0R#d.

**Important:** Do not enter the previous admin user password for this MSM.

The script then prompts you with the following:

```
Please enter new password (Press Ctrl C to exit):
```

Enter the same password that was used in the previous step, for example, pA55w0R#d, and then confirm it when prompted.

The script restarts services and displays the following message:

```
CAS password has been changed for admin user.
Please update any other client applications using this password.
```

**What to do next**

Repeat these steps for each additional MSM node in the cluster.

**Related information**

[Changing the Central Authentication Service (CAS) password for multisystem management (MSM)](page 87)

**Changing the CAS password for the MSP VM to match the CAS password on the MSM VM**

RCM content prepositioning uses a Central Authentication Service (CAS) for authentication to the 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, you must update the CAS password on the MSP VM to ensure the passwords match.

**About this task**

Updating the CAS password for the default administrator involves running a script on the MSP VM that updates the password, encrypts it, and saves it to an internal database.

**Before you begin**

- Ensure you know the CAS password that was updated on the MSM VM.
- Connect to the MSP VM.
Procedure

1. Run the following command:

```
/opt/vce/msp/install/update-cas-password.sh
```

The script prompts you with the following message:

```
Warning: This script will restart vision-assetmanager, vision-contentshare, vision-contentsource, and vision-downloader services. Do you want to continue ([y/n])?
```

2. Type `y` to continue. The script then prompts you with the following:

```
Please enter the MSM CAS password (Press Ctrl C to exit):
```

3. Type the MSM CAS password for the admin user and then confirm it when prompted.

   **Important:** This password must be exactly the same password used for CAS authentication on the MSM VM.

The script shows the following message and restarts the MSP services that are impacted:

```
AMQP CAS password has been updated. About to restart services that are impacted...
```

Related information

- **RCM content prepositioning services and components** (see page 112)
- **Forming a cluster of MSM VMs** (see page 18)
- **Changing the Central Authentication Service (CAS) password for multisystem management (MSM)** (see page 87)

**Creating users with access rights to storage components**

Vision shell allows you to retrieve and update information on components on each system in your network. However, you cannot make any 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**

You must establish an SSH connection to a MSM VM to perform this task.

Follow these steps to add users with administrative access to storage components.
Procedure

1. Establish an SSH connection to the MSM VM and log on.

2. Change to the following directory: `/opt/vce/credential-management/bin/`

3. Run the following command:

   ```
   ./credential-manager-cli create -credential-protocol SSH -credential-right ADMINISTRATOR -credential-type STORAGE -host-address storage-ip -username SSHadminuser -password SSHadminpassword
   ```

   where
   
   - `storage-ip` is the IP address of the storage component. To give the same user access to additional storage components, reissue this command for each IP address.
   
   - `SSHadminuser` is the username for logging on.
   
   - `SSHadminpassword` is the password for logging on.

What to do next

When you have finished, [Start a session with the Vision shell](#) (see page 61) with the new credentials and verify that you can perform configuration changes on the storage component.

**Changing access credentials for a component on a Vblock System**

Vision software retrieves credentials from the `vblock.xml` file to connect to the Vblock System components. In this way, Vision software can access the components for discovery and health polling. If the credentials to access a Vblock System component change, you must update the `vblock.xml` file to reflect that change.

Before you begin

- Verify the access credentials for the component.
- Verify the configuration file where Vision software retrieves the credentials, if not the default `vblock.xml`.
- Connect to the Vision Core VM.

Procedure

1. Run the following command to stop System Library services:

   ```
   stopFMagent
   ```

2. Run the following command to start the configuration script:

   ```
   configTool.sh
   ```
3 Type /opt/vce/fm/conf/vblock.xml to load the existing vblock.xml file.

Press Enter to display the list of available templates, or Enter the full path of an existing vblock.xml file: [/opt/vce/fm/conf/template] :/opt/vce/fm/conf/vblock.xml

Enter the number that corresponds to the system you are configuring ['0' to specify new file or directory]: 1

Loaded: /opt/vce/fm/conf/vblock.xml

4 Follow the script prompts and configure access credentials as appropriate. The following is an example of changing the access credentials for a vCenter.

VCenter VCenters ipaddress: '10.1.139.39', url: 'https://10.1.139.39/sdk', username: 'administrator@vsphere.local',
    (1) ipaddress, '10.1.139.39'
    (2) password, '**********'
    (3) username, 'administrator@vsphere.local'

a Type 1 to change the IP address.

Enter selection ('0' to continue to next step, or 'v' to validate ): 1

Enter new value for attribute 'ipaddress' [10.1.139.39] ('s' to skip):10.1.139.39

VCenter VCenters ipaddress: '10.1.139.39', url: 'https://10.1.139.39/sdk', username: 'administrator@vsphere.local',
    (1) ipaddress, '10.1.139.39'
    (2) password, '**********'
    (3) username, 'administrator@vsphere.local'

b Type 2 to change the password.

Enter selection ('0' to continue to next step, or 'v' to validate ): 2

Enter new value for attribute 'password' [**********] {Press [ENTER] to Skip} :Enter value for attribute 'password': **********

c Type 3 to change the username for vCenter.

Enter selection ('0' to continue to next step, or 'v' to validate ): 3

Enter new value for attribute 'username' [administrator] ('s' to skip):admin
d Type `v` to validate the changes.

```
Validating VCenter connection: url=https://10.1.139.39/sdk, user=administrator@vsphere.local. Please wait...
Validating VCenter connection succeeded!
```

5 Validate the `vblock.xml` file when you reach the end of the configuration. The following is an example of the validation output:

```
Validating VCenter connection: url=https://IP_address/sdk, user=Administrator, password=password. Please wait...
Validating VCenter connection succeeded!
Validating XmlApi connection. Please wait...
Validating XmlApi connection succeeded!
Validating SNMP connection. Please wait...
Validating SNMP connection succeeded!
Validating SSH connection. Please wait...
```

6 Save the `vblock.xml` file. The script will prompt you to overwrite the existing `vblock.xml` file. Type `y` to save the file with the changes.

```
Enter full path of a valid filename or Press Enter to save in [/opt/vce/fm/conf/vblock.xml] :
File exists would you like to overwrite (y/n)? y
```

7 Run the following command to start System Library services:

```
startFMagent
```

Related information

VCE Support

**Changing access credentials for a component on a VxBlock System or a VxRack System**

Configuring a VxBlock System or a VxRack System using the configuration editor

Use the configuration editor to create, edit, or delete the configuration files necessary for discovery on a VxBlock System and a VxRack System.
Before you begin

Ensure the system.cfg file is in the /opt/vce/fm/conf directory on the Vision Core VM. If the system.cfg file is not located in this directory, contact VCE Support.

Procedure

1. Start an SSH session to the Vision Core VM.
   
   **Important:** Use PuTTY to access the configuration editor for Windows-based systems as non-VSCIIC supported terminals display styling incorrectly.

2. Log on using the following credentials:
   - Username: root
   - Password: V1rtu@1c3!

3. Run the following command to launch the configuration editor and edit a previously imported configuration:

   configSystem edit

   The VCE Systems configuration editor opens.

What to do next

Add components to the configuration. Refer to Adding a component with the configuration editor (see page 35) for more information.

Editing component properties with the configuration editor

Use the configuration editor to modify various component properties on a VxBlock System or a VxRack System.

About this task

You can edit the following component properties:

- IP address
- Username
- Password
- Community string
- Method

**NOTE:** Depending on method and component type, this value can be lower or mixed case sensitive. Values for most fields are case sensitive, however, for a VxRack System method, the value is case insensitive.
Sensitive information such as passwords and community strings are masked in the configuration editor and encrypted in the configuration file.

Before you begin

Ensure you have configured the VxBlock System or VxRack System.

Procedure

1. Type the command `configSystem edit` to open the configuration editor.

2. Follow these steps to edit the component properties:
   a. In the configuration editor dialog, use the **Next** and **Back** options to navigate to the component you want to edit.
   b. Click **Tab** or use the arrow keys to navigate to the specific property you want to edit.
   c. Click the **Backspace** key or the **Delete** key to edit the properties.

3. Select **Save** to save the configuration changes and exit the configuration editor, or **Cancel** to exit the configuration editor without saving your changes.

The configuration editor uses the system.cfg to create (or update) an xml file that is used for initial discovery. For VxBlock Systems, it creates a vblock.xml file. For VxRack Systems, it creates a vxrack.xml file.

What to do next

Restart the FM Agent services from the Vision Core VM.

1. Run the following command:

   ```bash
   stopFMagent
   ```

2. Run the following command:

   ```bash
   startFMagent
   ```

Related information

[Configuring a VxBlock System or a VxRack System using the configuration editor](see page 33)

**Changing the password for the Vision shell administrator**

For security reasons, you should change the default password for the Vision shell administrator.

**About this task**

The Vision shell is supported on a Vblock System and a VxBlock System only.
Before you begin

Log on to the MSM VM as user `root`.

Procedure

1. Enter the following command:
   
   ```bash
   changeVisionShellPassword
   ```

   You are prompted to enter the current password.

2. Enter the current password for the `csadmin` username. You must enter the correct password to proceed. After entering the correct password, you are prompted to enter a new password.

3. Enter the new password and enter it again when prompted to confirm the new password.

Results

If the new and confirmation passwords match, the password is successfully changed. In a clustered environment, the new password is propagated to the other MSM nodes in the cluster.

Managing third party certificates

Using a third party signed certificate on the Vision Core VM

You can generate a new certificate with a Certificate Signing Request (CSR) and then import this certificate into JBoss for use with the Vision software.

About this task

This section describes the procedure for importing a third party SSL certificate into the application server provided with Vision software.

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 use, you may be provided with a Root CA and optionally Intermediate CA and Signing CA Certificates that will need to be installed in conjunction with the new server certificate. Your CA vendor or PKI administrators can provide details on retrieving all the certificates used in the certificate signing chain.

**NOTE:** If you change the System Library hostname after performing this procedure, you will need to 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)
You need to replace the customer-supplied-password in the steps below with the password you intend to use.

All passwords supplied in steps 1 through 6 below need to be the same.

All filenames in the procedure below, like my.keystore, and privatekey.pem, are examples.

**NOTE:** Encrypted passwords from two .dat files in /etc/vce need to be decrypted for Step 7. Contact VCE Support to get the passwords decrypted.

**Procedure**

1. Backup copies of your cryptography material in a secure location. The following files should be backed up on a Vision 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. This 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 *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 will also be removed from the file for flexibility with existing and future VCE Vision software certificate management tools.

   a. Run the following command:

   ```
   ```

   Enter the *customer-supplied-password* at the *Enter source keyword password* prompt.

   b. Run the following command to parse the PKCS12 private key and convert it to PEM format:

   ```
   /usr/bin/openssl pkcs12 -in private-key-rsa.p12 -out private-key-rsa.pem -nocerts
   ```
Run the following command to convert the private key to PKCS8 format:

```
/usr/bin/openssl pkcs8 -topk8 -nocrypt -in private-key-rsa.pem -inform PEM
-out private-key.pem -outform PEM
```

Enter the **customer-supplied-password** at the **Enter pass phrase for ./private-key-rsa.pem** prompt.

4. Run the following command to generate a CSR:

```
/usr/java/default/bin/keytool -certreq -keyalg RSA -alias jbosskey -file certreq.csr
-keystore my.keystore
```

Enter 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 provided by the CA is not a Base64 PEM encoded .cer file, it can be converted to PEM format with this command:

```
/usr/bin/openssl x509 -inform der -in <certificate>.der -out <certificate>.pem
```

If you have a .cer certificate, run this command:

```
cp <certificate>.cer <certificate>.pem
```

6. Assemble the certificate and the private key:

```
/usr/bin/openssl pkcs12 -export -in <certificate>.pem -inkey private-key.pem
-out cert-andkey.p12 -name jbosskey
```

Enter the **customer-supplied-password** at the **Enter export password** prompt.

Enter 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. Run the following command for root certificate.

```
/usr/java/default/bin/keytool -import -file <rootCert.pem> -alias jbosskey1
-keystore /usr/java/default/lib/security/cacerts
```

   b. Run the following command for intermediate certificate:

```
/usr/java/default/bin/keytool -import -file <IntermediateCert.pem>
-alias jbosskey2 -keystore /usr/java/default/lib/security/cacerts
```

**NOTE:** When prompted for a password, enter the one that you requested from VCE Support.
Run the following command to import the new certificate, this time specifying the source keystore filename, source keystore password, and source key password:

```
```

Using 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 Vision software.

About this task

This section describes the procedure for importing a third party SSL certificate into the application server provided with the Vision software.

The procedure begins with the generation of a Certificate Signing Request (CSR). Specific requirements for a CSR may vary among vendors.

Depending on the Certificate Authority (CA) vendor or internal Private Key Infrastructure (PKI) you use, you may be provided with a Root CA and optionally Intermediate CA and Signing CA Certificates that will need to be installed in conjunction with the new server certificate. Your CA vendor or PKI administrators can provide details on retrieving all the certificates used in the certificate signing chain.

**NOTE:** If you change the Vision MSM hostname after performing this procedure, you will need to 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)
- You need to replace the customer-supplied-password in the steps below with the password you intend to use.
- All passwords supplied in steps 1 through 5 below need to be the same.
- All filenames in the procedure below, like my.keystore, and privatekey.pem, are examples.

**NOTE:** Encrypted passwords from two .dat files in `/etc/vce` need to be decrypted for Step 6. Contact VCE Support to get the passwords decrypted.

Procedure

1. Backup 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. This 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 removed from the file for flexibility with existing and future VCE Vision software certificate management tools.

a Run the following command:

```
/usr/java/default/bin/keytool -importkeystore -srckeystore my.keystore -destkeystore privatekey-rsa.p12 -deststoretype PKCS12 -srcalias <your keyAlias> -storepass customer-supplied-password
```

Enter the `customer-supplied-password` at the Enter source keystore password prompt.

b Run the following command to parse the PKCS12 private key and convert it to PEM format:

```
/usr/bin/openssl pkcs12 -in private-key-rsa.p12 -out private-key-rsa.pem -nocerts
```

c Run the following command to convert the private key to PKCS8 format:

```
/usr/bin/openssl pkcs8 -topk8 -nocrypt -in private-key-rsa.pem -inform PEM -out private-key.pem -outform PEM
```

Enter the `customer-supplied-password` at the Enter pass phrase for ./private-key-rsa.pem prompt.

4 Run the following command to generate a CSR:

```
/usr/java/default/bin/keytool -certreq -keyalg RSA -alias <your keyAlias> -file certreq.csr -keystore my.keystore
```

Enter 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 provided by the CA or PKI administrator is not a Base64 PEM encoded .cer file, it can be converted to PEM format with this command:

```bash
/usr/bin/openssl x509 -inform der -in <certificate>.der -out <certificate>.pem
```

If you have a .cer certificate, run this command:

```bash
cp <certificate>.cer <certificate>.pem
```

6 Import the issuing certificate chain into the cacerts keystore (root and intermediate certificates PEM files). Rename the root and intermediate certificates as .pem (if required).

   a  Run the following command for root certificate.

   ```bash
   /usr/java/default/bin/keytool -import -file <rootCert.pem> -alias visionkey -keystore /usr/java/default/lib/security/cacerts
   ```

   b  Run the following command for intermediate certificate:

   ```bash
   /usr/java/default/bin/keytool -import -file <IntermediateCert.pem> -alias visionkey2 -keystore /usr/java/default/lib/security/cacerts
   ```

   **NOTE:** When prompted for a password, enter the one that you requested from VCE Support.

7 Run the following command to import the new certificate, this time specifying the certificate and private key filenames:

```bash
```

## Integrating Vision software with Active Directory

### Overview of Active Directory integration

You can configure Vision software to work with Active Directory for authentication and authorization.

When Vision software is integrated with Active Directory, Vision software authenticates Active Directory users and also supports a mapping between Active Directory groups and roles.

The Vision dashboard and Vision API for Vision Security allow you to perform the following functions:

- Define an Active Directory configuration that points to an Active Directory server.
- Map Active Directory groups to roles.
Roles defined in the MSM VM are independent from roles defined in the Vision Core VM. The two VMs support entirely different application functions. Therefore, the roles defined in the MSM VM do not apply to the Vision Core VM, and vice versa.

When Vision software is integrated with Active Directory, Active Directory users can authenticate to Vision software. In addition, the actions that the user is authorized to perform are controlled by the role mappings. By mapping an Active Directory group to a role, you can control which permissions the user is given. When an Active Directory user logs into Vision software, the software checks the role mappings for the Active Directory groups to which the user is assigned. The set of permissions (and access controls) available to the user depends on which roles have been mapped to the groups in which the user is a member.

To utilize Active Directory with Vision software, you must set up the vSphere Web Client to use an Active Directory identity source. After you set this up in vSphere, you need to set up Vision software to use the same Active Directory server to control the users access to Vision software. Refer to the VMware vSphere help for more information.

When Vision software is integrated with Active Directory, you do not need to create new users and passwords within the Vision software REST APIs. However, both methods of authentication and authorization are used, with the Active Directory implementation taking precedence. If an Active Directory user cannot be authenticated, the system attempts to authenticate with a Vision software user created with REST API.

NOTE: If you create a Vision software user with the REST API that has the same name as one of your Active Directory users, then that user will have roles granted both through the Active Directory integration and directly with Vision software.

Vision software supports the use of a single Active Directory configuration for a single Active Directory server. The software allows you to modify an existing Active Directory configuration, but only one configuration can be used at any point in time. This restriction is enforced by the software.

Removing groups from Active Directory

It is important to make sure roles that are mapped to a group are removed before deleting the group from Active Directory. If a group is deleted without removing the mappings first, the group's role mappings are still saved on the MSM VM. This can cause two problems:

- The mappings between the non-existant group and the roles still show up in the REST API.
- If the group is ever recreated in the future, members in that new group will be granted all of the permissions defined by the role mappings of the previous group. This could expose permissions to users in the recreated group that they are not intended to have.

If a group is recreated and inherits the former role mappings, use the dashboard to make corrections to the group’s roles. The LDAP administrator needs to communicate configuration changes with the Vision software administrator.

Related information

Roles and operations for RCM content prepositioning (see page 111)
Configuring Active Directory

Follow these steps to integrate an Active Directory configuration with Vision software. This allows Vision software authenticate Active Directory users and also supports a mapping between Active Directory groups and roles.

Before you begin

You must already have set up Active Directory. You need the following information about the Active Directory configuration to complete this task:

- IP address or host name
- Port
- SSL configuration
- Credentials required to connect to Active Directory 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 of (userPrincipalName=%u) is a simple filter that handles LDAP authentication through User Principal Names (UPNs), which are system users that take the form of email addresses. In most Active Directory environments, (userPrincipalName=%u) is the correct user filter.

However, you might need to change the user filter for your Active Directory configuration. For example, you might specify a compound filter to allow multiple attributes to be checked during LDAP authentication. This would be necessary if you wanted to be able to support authentication through service accounts that do not have email addresses. For example, you could specify a compound user filter such as the following to ensure that the sAMAccountName (User Logon Name in Pre-Windows 2000 systems) is also supported:

```
((userPrincipalName=%u)(sAMAccountName=%u))
```

Depending on the DN of your service accounts relative to the DN for your normal users, you might also need to change the Base DN for users to a common parent. For example, rather than specifying OU=Users as the Active Directory location within the Base DN for users setting, you might need to specify a higher-level DN, such as OU=Accounts that includes both the OU=Users and OU=Service locations, as shown below:

```
OU=Accounts,OU=vbadtest,DC=adtest,DC=vcemo,DC=lab
```

Procedure

1. Log on to Vision dashboard.
2. From the main toolbar, select Manage > Active Directory.
3 Complete the fields with the Active Directory information.

4 Click Save.

Mapping roles to Active Directory groups

If Vision software is configured to use Active Directory to manage users and groups, follow these steps to assign roles to the groups in Active Directory. The roles include a set of permissions that define what tasks the users in that role can perform after logging on to Vision software.

Before you begin

Configure Active Directory (see page 104)

Procedure

1 Log on to Vision dashboard.

2 Click the menu icon (⋮).

3 Under the Administration menu, click Manage > Roles.

4 For each group, select one or more roles in the appropriate column.

Results

When you are finished, click the save icon (.SaveChanges) to save your changes.

Related information

Roles and operations for the Software Module Manager (see page 182)

Default roles

The Active Directory configuration must be connected to the multisystem management (MSM) node before you can assign roles. Vision software ships with the following default roles:

Vision administrator

Administrator with full access to the Vision dashboard and REST APIs.

Vision shell administrator

Administrator with full access to Vision shell. Users with this role can run commands that make configuration changes to components in VCE Systems.

**NOTE:** Vision shell is supported only on VxBlock Systems and Vblock Systems.

Vision user

User with read access to the Vision dashboard, REST APIs, and Vision shell.
The **Vision 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><strong>System:</strong> vceSystemDescription</td>
<td>Dynamic role created to filter search results to the system identified by vceSystemDescription. Users with the Vision user role can have system roles to search and view status information for these systems in the dashboard.</td>
</tr>
<tr>
<td><strong>Attention:</strong> Do not combine system and location roles for any user group.</td>
<td></td>
</tr>
<tr>
<td><strong>Location:</strong> vceSystemGeo</td>
<td>Dynamic role created to filter search results to the systems located in vceSystemGeo. Users with the Vision user role can have location roles to search and view status information for systems by vceSystemGeo attribute.</td>
</tr>
<tr>
<td><strong>Attention:</strong> Do not combine system and location roles for any user group.</td>
<td></td>
</tr>
<tr>
<td><strong>LDAP configuration administrator</strong></td>
<td>Users with this role can create, edit, delete, and connect LDAP configurations for MSM using the <strong>Connect to Active Directory</strong> configuration page in the dashboard.</td>
</tr>
<tr>
<td><strong>Log administrator</strong></td>
<td>Users with this role can download AA logs from the Central Authentication Service using the <code>/securityweb/security/aalogs</code> REST API.</td>
</tr>
<tr>
<td><strong>Software module manager user</strong></td>
<td>Users with this role can view the settings on the <strong>Manage Software Modules</strong> page.</td>
</tr>
<tr>
<td><strong>Software module manager administrator</strong></td>
<td>Users with this role can view and change the settings on the <strong>Manage Software Modules</strong> page.</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 will not be able to log into the dashboard, regardless of any other roles they are assigned to.
Ensuring VCE System compliance

Compliance overview

Vision software can validate the compliance of VCE Systems when compared to different criteria that Dell EMC provides. For example, you can use RCM compliance to check your components to make sure they have the latest supported firmware from the latest Release Certification Matrix (RCM).

Compliance validation is assessed when you run a compliance scan on a system. You can run compliance scans from the Vision dashboard or from a REST API client using the MSM API for Compliance. After a scan has completed, a score from 0 to 100 is assigned to show overall system compliance with that policy. You can see the score for each system in the Vision dashboard. The score is also available in a downloadable compliance report that includes the result of each check performed during the scan. Use the compliance report to correct any failed compliance checks to improve the compliance score on the next scan.

Available compliance policy types

Dell EMC provides the following policy types to assess compliance for VCE Systems:

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Certification Matrix</td>
<td>RCMs define software, firmware, and hardware that Dell EMC tests and validates as supported for a VCE System. You can run compliance scans against an RCM to easily identify each system's compliance with that RCM.</td>
</tr>
<tr>
<td>Dell EMC security hardening guidelines (Security Compliance Validation)</td>
<td>Dell EMC security hardening guidelines provide security best practices that help you identify risks that might exist on VCE Systems. The scan uses the security standards based on Dell EMC security best practices.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The baseline security settings module is supported only on Vblock Systems and VxBlock Systems.</td>
</tr>
<tr>
<td>VCE Technical and Security Advisories</td>
<td>The VSA and VTA content packs provide targeted, specific technical alerts or vulnerabilities that Dell EMC has identified for particular VCE System components. The VSA enables you to rapidly identify and remediate security vulnerabilities while the VTA enables you to quickly assess and resolve technical issues.</td>
</tr>
</tbody>
</table>

One or more of these policy types might be available for each system, depending on the system configuration.

How compliance policies work

A compliance policy defines how a specific policy type, such as RCM, should be applied to a specific VCE System, for example, a Vblock System 340 or a VxRack System with FLEX. Each policy can have one or more profiles that specify which rules and values to check for the components in the system. For example, RCM 5.0.2 identifies a profile that corresponds to a specific Release Certification Matrix for firmware on specific VCE Systems. Running a compliance scan using that profile checks the system for the firmware versions defined in that release.
Each profile is a grouping of rules used to audit a system based on values defined according to Dell EMC standards. For example, the RCM 5.0.2 profile could include a rule to check the firmware version on Cisco UCS B-Series blades. It will check the blade’s firmware against the profile’s recommended value, for example, 2.2(3b). This check will fail if the values do not match.

Managing compliance across all VCE Systems

Use the Vision dashboard to perform most of the tasks required to keep your systems compliant with the policies for your business or organization.

Running compliance scans

Often you will want to run a compliance scan under the following conditions:

- New updates or configuration changes have been applied to components in a system.
- New policy content has been uploaded or a new target profile has been assigned to a system.

Use the dashboard to start a compliance scan for a system. See the Vision dashboard online help for more information.

Downloading and assessing the results of a compliance scan

When a scan is complete, the results are shown in the Compliance widget in the dashboard. If there are any failed compliance checks, the components are listed with a summary. Click on any component to get details of the compliance checks that you need to remediate. You can also download a PDF, XLS or CSV version of the full compliance scan report. See the Vision dashboard online help for more information.

After downloading the results, refer to Assessing the results of a compliance scan (see page 109) for information about changes you can make to improve the compliance score.

Checking the profile used for compliance scans

Each system is assigned a target profile for each policy. For RCM compliance, the profile specifies the release used to determine whether the components have the correct firmware versions. For security hardening compliance, the profile is based on the Dell EMC security best practices. You might use a customized copy of one of these profiles for some systems.

The target profile can be checked and assigned from the Vision dashboard. See the dashboard online help for more information.

Uploading and installing the latest compliance content

You should make sure compliance content is up to date with the most recent version before you run compliance scans on your VCE Systems. To get the latest content, log on to the VCE Support site and then navigate to the software folder for your Vblock System in the VCE Download Center. The content should always be a ZIP file with at least one XCCDF and one OVAL file.

After downloading the new content, use the menu icon in the dashboard toolbar to upload and install the content. The new compliance policies are installed to each applicable system. See the dashboard help for more information.
Customizing the compliance profile

Depending on the configuration for any system, you might need to make changes to the rules and checks in a profile to obtain a more accurate compliance score. Any changes you make to a profile are saved to a custom copy of that profile. Make sure that any subsequent changes are saved in the same custom copy to avoid multiple custom profiles with different updates.

Changes to compliance profiles are made using the Vision dashboard. See the dashboard online help for complete instructions.

Assessing the results of a compliance scan

The results of a compliance scan are shown in the Vision dashboard. Details about each check in the compliance scan are also available when you download the report. The report is available in PDF, XLS or CSV format.

Use the **Compliance** widget to see all of the checks that failed the compliance scans. If no failures are found, **Compliance** displays the message "All systems are compliant".

**NOTE:** If the RCM Compliance scan is executed while discovery is in progress, it is possible that some system components may be missing from the RCM Compliance scan report. If this happens, rerun the RCM Compliance scan after discovery is complete.

The Test Failures section of the compliance PDF report provide a quick listing of the failed checks in the scan. You can select each component to see the compliance failures for that component.

The Current system section of the compliance XLS report provides a quick list of the failed checks highlighted in green.

The Test Result section of the compliance CSV report returns a TRUE/FALSE result highlighting a pass or fail in the system.

**NOTE:** If you see discrepancies between the compliance scan and what is showing on the dashboard for scanned components, there might have been an issue with discovery. When compliance runs, it uses the list of components that were discovered. If a component was missed during discovery, it will not show in the compliance scan. Run discovery again, and then run another compliance scan.

You have two options to determine how to address each failure:

- Determine if the check that failed is valid for your system configuration. For example:
  - If the firmware for a component has been upgraded to a more recent version than the value in the RCM compliance check, you might need to update the value for the check. Do this only if you know that the updated firmware version is supported for your system configuration.
  - You might have a service like Telnet enabled for a component for certain administrative purposes. You could disable this check on the security hardening profile for that component if you have other safeguards to prevent unauthorized access.

  If you determine that a compliance check can safely be changed, refer to the online help in the Vision dashboard for instructions for making changes to the profile used for the scan.

- If a failed check is valid, use one of the following resources to address the issue.
To update firmware or software for a component, refer to Downloading RCM content (see page 110) for complete information.

Security hardening

Use the Vision Shell baseline security settings Remediation Extension Pack to resolve specific security issues. The show security command displays a list of commands that can be used to address security compliance checks. Or you can work with an individual component, using show computesystem for example, to get a list of commands to use to address security compliance checks for specific components.

Refer to Remediating security issues using the shell (see page 125) for more information about using these shell commands.

Using Vision software to download RCM content

You can use Vision software to download Release Certification Matrix (RCM) content for one or more VCE Systems, to upgrade to a new RCM, or remediate drift from your current RCM.

NOTE: In the current release, Vision software enables you to download RCM content for Vblock Systems and VxBlock Systems only.

Important: Only one MSP VM must be deployed and configured within a cluster. The MSP VM must be associated with the MSM VMs in its local data center for that cluster. If other MSP VMs have been deployed and configured, you must power down these VMs.

To download RCM content in a multisystem management environment, you must use the Vision dashboard.

Working with the multisystem prepositioning (MSP) VM

The MSP VM is a component of Vision software that lets you discover and download Release Certification Matrix (RCM) content. You interact with the MSP VM through the Vision dashboard.

The MSP VM enables you to perform the following tasks:

- Discover and download RCM content for one or more VCE Systems.
- View RCM content downloaded to one or more VCE Systems.
- Monitor the status of RCM content downloads.
- Manage downloaded RCM content.

**NOTE:** RCM content available through the MSP VM from the content distribution network is restricted to a rolling period of 12 months as of the Vision software 3.5 release (August 2016). RCM content remains available for manual download from the Download Center for releases outside of that window.

**Roles and operations for RCM content prepositioning**

Vision software provides role-based access control (RBAC) for RCM content prepositioning. You can assign roles to user groups to control which operations users can perform.

<table>
<thead>
<tr>
<th>Role</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>RCM Content Pre-positioning administrator</td>
<td>Users mapped to this role can:</td>
</tr>
<tr>
<td></td>
<td>• Access the RCM content prepositioning features in the Vision dashboard.</td>
</tr>
<tr>
<td></td>
<td>• Download RCM content.</td>
</tr>
<tr>
<td></td>
<td>• Delete RCM content.</td>
</tr>
<tr>
<td></td>
<td>• Cancel downloads.</td>
</tr>
<tr>
<td>RCM Content Pre-positioning user</td>
<td>Users mapped to this role can:</td>
</tr>
<tr>
<td></td>
<td>• Access the RCM content prepositioning features in the Vision dashboard.</td>
</tr>
</tbody>
</table>

Refer to the related topics for more information about Active Directory and mapping roles to Active Directory groups using the Vision dashboard.

**Related information**

[Overview of Active Directory integration](see page 102)
RCM content prepositioning services and components

RCM content prepositioning uses the following services and components to manage the RCM content download process.

<table>
<thead>
<tr>
<th>Components and services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Share service</td>
<td>The vision-contentshare is used to manage the inventory of RCM content that is local to the running instance of the vision-assetmanager service.</td>
</tr>
<tr>
<td>Download service</td>
<td>The vision-downloader service manages the following tasks:</td>
</tr>
<tr>
<td></td>
<td>• Acknowledges a download request.</td>
</tr>
<tr>
<td></td>
<td>• Downloads each required file from the Content Distribution Network (CDN).</td>
</tr>
<tr>
<td></td>
<td>• Provides status updates during the download process.</td>
</tr>
<tr>
<td>Content Source service</td>
<td>The vision-contentsource manages the entitlements, request notifications from the CDN, and ensures that all downloaded RCM content matches the download requests.</td>
</tr>
<tr>
<td>Asset Manager service</td>
<td>The vision-assetmanager service co-ordinates the Content Share, Content Source, and the Downloader services for working with RCM content that resides on the MSP VM.</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>PostgreSQL is a relational database management system. It is used to store the downloaded RCM content on the MSP VM.</td>
</tr>
</tbody>
</table>

Related information

- Configuring Vision software to access a proxy server (see page 114)
- Configuring the connection timeout (see page 115)
- Changing the PostgreSQL database password (see page 119)
- Changing the CAS password for the MSP VM to match the CAS password on the MSM VM (see page 90)
- Changing the password for the Proxy Server (see page 120)
- Configuring the download rate (see page 116)

Download process

The download process describes the steps required to download RCM content to one or more VCE Systems.

RCM content becomes available for download after Dell EMC uploads the files to the RCM content distribution network. Dell EMC uploads the binary files in the RCM version.
When you check for RCM content to download or start a download, Vision software establishes an **HTTPS** connection to the RCM content distribution network and then completes the following steps:

1. **Adds the RCM version to a queue.**
   
   If a download is in progress, Vision software holds subsequent downloads in the queue until the previous download is complete.

2. **Checks available disk space on the multisystem prepositioning (MSP) VM.**
   
   Vision software only downloads files if there is enough free disk space for the entire RCM version.

3. **Starts downloading the files in the RCM version.**

4. **Performs an integrity check on each downloaded file.**

5. **Stores the completed download in the repository.**

### Global download states

Global download states are the overall states that apply to an RCM version from when you start a download to when Vision software completes all download operations on that RCM version.

<table>
<thead>
<tr>
<th>Global download state</th>
<th>Vision software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initializing</td>
<td>This is the initial state for all RCM content downloads. A request to download an RCM has been received and will be validated. The request proceeds if the validation was successful.</td>
</tr>
<tr>
<td>Queued</td>
<td>Indicates that a request to download an RCM has been queued and is ready for download. This state indicates that the requested RCM was present on the Content Distribution Network (CDN) and the validation was successful.</td>
</tr>
<tr>
<td>Downloading</td>
<td>Indicates that a download is in progress. The progress of the RCM content download is displayed in a % value.</td>
</tr>
<tr>
<td>Importing</td>
<td>Indicates that the RCM content is downloaded and Vision software is completing the final steps to import and organize the content.</td>
</tr>
<tr>
<td>Completed</td>
<td>Has completed the RCM content download.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>Has cancelled a download that was either in an initializing, queued or downloading state only. Vision software has also deleted any partially downloaded files or downloaded files specific to the RCM version.</td>
</tr>
<tr>
<td>Failed</td>
<td>Indicates that the RCM content download has failed.</td>
</tr>
</tbody>
</table>

### Configuring connection and download settings

You can configure settings that Vision software uses 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**

Vision software 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, you specify the property values in these property files.

Configuring Vision software to access a proxy server

You can configure Vision software to use a proxy server to access the RCM content distribution network.

About this task

To configure the Vision software to use a proxy server, set values for the following properties in `/opt/vce/msp/conf/msp-common.properties` on the multisystem prepositioning (MSP) VM:

<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>![WARNING: 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. Refer to 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` for editing.
2. Locate the **Proxy Server Configuration settings** section.
Specify values for each property so that Vision software can access the proxy server.

The following example configures the MSP VM to use a proxy server:

```
proxy.hostname=http://example.com
proxy.port=80
proxy.username=username
proxy.password=password
```

**NOTE:** Use the `opt/vce/msp/install/update-proxy-password.sh` script to set the `proxy.password` property. Refer to the related topic for information about running this script.

4. Save and close the `msp-common.properties` file.

5. Run the following command to restart the Downloader service:

```
service vision-downloader restart
```

6. Run the following command to restart the Content Source service:

```
service vision-contentsource restart
```

**Related information**

- [RCM content prepositioning services and components](see page 112)
- [Changing the password for the Proxy Server](see page 120)

**Configuring the connection timeout**

Configure the period of time that Vision software 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 multisystem prepositioning (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 Vision software 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 remove the comment from the property, delete the hash (#) at the start of the line.
4. Specify values for the property as appropriate.
   The following example configures the MSP VM to maintain an idle connection, ensuring that the connection will not be closed:
   
   ```
   connection.timeout.millis=0
   ```
   By default, this entry is left blank, which indicates that the default value is set to 180000 milliseconds (3 minutes).
5. Save and close the msp-contentsource.properties file.
6. Run the following command to restart the Content Source service:
   
   ```
   service vision-contentsource restart
   ```

Related information

**RCM content prepositioning services and components** (see page 112)

Configuring the download rate

Configure the download rate that Vision software 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 multisystem prepositioning (MSP) VM:

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>download.rate</td>
<td>A minimum download rate of 1024 bytes is required. The default value is 0 which is interpreted as an unlimited download rate. It is recommended to set a minimum download rate of 2mb. Downloading a full RCM Content with less bandwidth may result in an incomplete RCM download after 8 hours and the RCM download will have to be initiated again to complete.</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 Downloader settings section.
3. Specify the download rate that Vision software uses to download RCM content.
   
   **NOTE:** When specifying the download rate, you must note the following:
   
   - The download rate can be specified in B, K, or Mbs, for example:
     
     - 1024B - value in bytes
     - 1K - value in kilobytes
     - 1M - 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.

   The following example configures Vision software to use a download rate of 10M:

   ```
   download.rate=10M
   ```

4. Save and close the msp-downloader.properties file.
5. Run the following command to restart the Downloader service:

   ```
   service vision-downloader restart
   ```

Related information

- [RCM content prepositioning services and components](#) (see page 112)

Configuring retry attempts and intervals

Configure the retry attempts and intervals that Vision software 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 multisystem prepositioning (MSP) VM:

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>retry.max.attempts</td>
<td>Sets the maximum number of attempts that Vision software makes to connect to the RCM content distribution network before displaying a downloading error. The default value is 10.</td>
</tr>
<tr>
<td>retry.initial.interval</td>
<td>Sets the maximum amount of time, in milliseconds, that Vision software 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>
<tr>
<td>retry.multiplier</td>
<td>Sets the multiplication factor used for attempts to connect to the RCM content distribution network. This multiplier is used if Vision software fails to connect a second time. The default value is 2.0. For example, if Vision software waited for 100 milliseconds after the initial failure and the multiplier is 2.0, Vision software will wait for 200 milliseconds before the third attempt. It will wait for 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 Vision software to the RCM content distribution network. 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 section.
3. Specify values for each property to change the default retry attempts and interval settings.
4. Save and close the `msp-downloader.properties` file.
5. Run the following command to restart the Downloader service:

   ```
   service vision-downloader restart
   ```

Managing credentials for RCM content prepositioning
Changing the PostgreSQL database password

Changing the default password for the Content Share PostgreSQL database and the Asset Manager involves running a script on each service on the MSP VM that updates the password, encrypts it, and then saves it to an internal database.

About this task

Vision software uses a PostgreSQL database to store downloaded RCM content in the multisystem prepositioning (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 following procedures explains how to run the update scripts for both the Asset Manager and the Content Share services.

Before you begin

Connect to the MSP VM.

Procedure

1. Run the following command:

   ```bash
   /opt/vce/msp/install/update-assetmanager-db-password.sh
   ```

   The script prompts you with the following message:

   ```bash
   Warning: This script will restart vision-assetmanager.
   Do you want to continue ([y/n])?
   ```

2. Enter `y` to continue. The script then prompts you with the following:

   ```bash
   Please enter new password:
   ```

3. Enter the new password for the admin user and then confirm it when prompted.

   The password:
   - Is case sensitive.
   - Must be between 8 and 20 characters in length.
   - Must include one uppercase letter, one digit, and one special character.
   - Cannot contain any of the following special characters: `\ / % + ' " ( ) ; : < > |`

   The script restarts services and displays the following message:

   ```bash
   DB password has been changed for assetmanager.
   ```
Run the following command:

```
/opt/vce/msp/install/update-contentshare-db-password.sh
```

The script prompts you with the following message:

```
Warning: This script will restart vision-contentshare.
Do you want to continue ([y/n])?
```

Enter `y` to continue. The script then prompts you with the following:

```
Please enter new password:
```

Enter the new password for the admin user and then confirm it when prompted.

The password:

- Is case sensitive.
- Must be between 8 and 20 characters in length.
- Must include one uppercase letter, one digit, and one special character.
- Cannot contain any of the following special characters: \ / % + ' " ( ) ; : < > |

The script shows the following message and restarts the services accordingly:

```
DB password has been changed for contentshare. 
Stopping service vision-contentshare, which may take up to 60secs...
```

Related information

**RCM content prepositioning services and components** (see page 112)

**Changing the password for the Proxy Server**

You can configure Vision software to use a proxy server to access the RCM content distribution network. As part of this configuration, you set a password for the user specified using the `/opt/vce/msp/install/update-proxy-password.sh` script. This script can also be used to change the proxy password if required.

**About this task**

Changing the proxy password for the specified username involves running 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. Run the following command:

```
/opt/vce/msp/install/update-proxy-password.sh
```

The script prompts you with the following message:

```
Warning: Warning: This script will restart vision-contentsource and vision-downloader services.
Do you want to continue ([y/n])?
```

2. Enter `y` to continue. The script then prompts you with the following:

```
Please enter new password (Press Ctrl C to exit):
```

3. Enter the new password for the user and then confirm it when prompted.

The script shows the following message and restarts the services accordingly:

```
Proxy password has been updated. About to restart services that are impacted...
```

Related information

- **RCM content prepositioning services and components** (see page 112)
- **Configuring Vision software to access a proxy server** (see page 114)

### Downloading RCM content using the Vision dashboard

The Vision dashboard provides a user interface for working with RCM content prepositioning to view available RCM content as well as download and manage RCM content. To work with RCM content prepositioning on the dashboard, you must be an authenticated and authorized Vision software user.

**NOTE:** In the current release, Vision software enables you to download RCM content for Vblock Systems and VxBlock Systems only.

To download RCM content on the dashboard, log on, click `>` > Manage > Download RCM Content and follow the prompts on the **RCM Content Download wizard**.

For more information, launch the **VCE Help** on the dashboard.

### Accessing downloaded RCM content

After you download RCM content, you can access the files on the Vision dashboard and the multisystem prepositioning (MSP) VM.
Procedure

1. To access downloaded RCM content on the MSP VM:
   
   - **NOTE:** Do not delete or modify RCM content files directly from the MSP VM. You should only delete RCM content using the Vision dashboard.
   
   a. Establish an SFTP connection to the MSP VM.
   b. Navigate to the following directory: `/opt/vce/msp/repository`.
   c. Select the directory for the appropriate VCE System and browse through the directory to locate the RCM content.

2. To access downloaded RCM content on the Vision dashboard
   
   a. Refer to the Vision dashboard online help for information on accessing and managing downloaded RCM content.

Structure of the repository

Review the structure of the repository where Vision software saves RCM content that is downloaded.

Vision software saves RCM content in the following directory on the multisystem prepositioning (MSP) VM: `/opt/vce/msp/repository`. This directory contains sub-directories into which Vision software organizes RCM content.

- **NOTE:** Do not delete or modify any files directly from the MSP VM. You should only delete RCM content using the Vision dashboard. Refer to the dashboard online help for more information about managing RCM content.

- **NOTE:** To avoid issues during the RCM content download process, do not delete or modify the repository folder structure, including the renaming of folders under `/opt/vce/msp/repository`.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>content</td>
<td>Stores RCM content that Vision software has successfully downloaded. Vision software stores all binary objects in a flat structure using the file ID. You should not access downloaded RCM content in this directory. You can view downloaded RCM content using the Vision dashboard.</td>
</tr>
<tr>
<td>rcms</td>
<td>Contains symbolic links to files in the <strong>content</strong> directory. The symbolic links use readable file names for each file. Vision software organizes RCM content in the <strong>rcms</strong> directory according to VCE System, RCM version, and vendor so that you can easily locate specific files.</td>
</tr>
<tr>
<td>downloads</td>
<td>Temporarily stores the RCM content that Vision software is currently downloading.</td>
</tr>
</tbody>
</table>

**NOTE:** Vision software uses an `/opt/vce/msp/repository/downloads` folder to temporarily store the RCM content that is currently downloading. Once the RCM content is committed to the content share, the RCM content is removed from the downloads folder.
The following illustration shows the structure of the repository directory, including the temporary download folder:

![Diagram of repository directory structure]

**Troubleshooting**

**Log files for RCM content prepositioning**

Vision software writes messages to log files that can assist with troubleshooting and root cause analysis with RCM content prepositioning.

**Multisystem prepositioning (MSP) API logs**

Locate log files for the multisystem prepositioning (MSP) API in the following directory on the MSM VM: /opt/vce/msp/prepositioning-api/deploy/logs

The following table lists log messages for the API:

<table>
<thead>
<tr>
<th>Log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msp-api-error.log</td>
<td>Contains error events.</td>
</tr>
</tbody>
</table>
The following log files are available on the multisystem prepositioning (MSP) VM.

**Asset Manager logs**

Locate log files for the multisystem prepositioning (MSP) Asset Manager in the following directory: `/opt/vce/msp/assetmanager/logs/`

The following table lists log messages for the Asset Manager:

<table>
<thead>
<tr>
<th>Log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>asset-manager-app-error.log</td>
<td>Contains error events.</td>
</tr>
<tr>
<td>asset-manager-app-info.log</td>
<td>Contains informational messages that indicate progress.</td>
</tr>
<tr>
<td>asset-manager-app-trace.log</td>
<td>Contains fine-grained information messages for debugging purposes.</td>
</tr>
</tbody>
</table>

**Content Source logs**

Locate log files for the multisystem prepositioning (MSP) Content Source in the following directory: `/opt/vce/msp/contentsource/logs/`

The following table lists log messages for the Content Source:

<table>
<thead>
<tr>
<th>Log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>content-source-error.log</td>
<td>Contains error events.</td>
</tr>
<tr>
<td>content-source-info.log</td>
<td>Contains informational messages that indicate progress.</td>
</tr>
<tr>
<td>content-source-trace.log</td>
<td>Contains fine-grained information messages for debugging purposes.</td>
</tr>
</tbody>
</table>

**Downloader logs**

Locate log files for the multisystem prepositioning (MSP) Downloader in the following directory: `/opt/vce/msp/downloader/logs/`

The following table lists log messages for the Downloader:

<table>
<thead>
<tr>
<th>Log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>downloader-error.log</td>
<td>Contains error events.</td>
</tr>
<tr>
<td>downloader-info.log</td>
<td>Contains informational messages that indicate progress.</td>
</tr>
<tr>
<td>downloader-trace.log</td>
<td>Contains fine-grained information messages for debugging purposes.</td>
</tr>
</tbody>
</table>
Content Share logs

Locate log files for the multisystem prepositioning (MSP) Content Share in the following directory: `/opt/vce/msp/contentshare/deploy/logs/`

The following table lists log messages for the Content Share:

<table>
<thead>
<tr>
<th>Log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vision-contentshare-error.log</code></td>
<td>Contains error events.</td>
</tr>
<tr>
<td><code>vision-contentshare-info.log</code></td>
<td>Contains informational messages that indicate progress.</td>
</tr>
<tr>
<td><code>vision-contentshare-trace.log</code></td>
<td>Contains fine-grained information messages for debugging purposes.</td>
</tr>
</tbody>
</table>

**NOTE:** When a log file reaches 10 MB in size, Vision software saves that log file and generates a new one. Vision software saves a maximum of 5 log files on the VM before overwriting older log files.

Message identifiers

Vision software includes unique identifiers for each message that it writes to a log file. These identifiers help you easily understand the severity level of the message and isolate issues.

Message identifiers have the following format:

```
[Product][Component][Message Code]
```

Where:

<table>
<thead>
<tr>
<th><strong>[Product]</strong></th>
<th><strong>[Component]</strong></th>
<th><strong>[Message Code]</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>V</code> for Vision software</td>
<td>- MSP relates to multisystem prepositioning (MSP).</td>
<td>4 digits with the format <code>NNNN</code></td>
</tr>
<tr>
<td></td>
<td>- API relates to the API.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- CSH relates to the Content Share.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- AMR relates to the Asset Manager.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- DLR relates to the Downloader.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- CSO relates to the Content Source.</td>
<td></td>
</tr>
</tbody>
</table>

Remediating security issues using the Vision shell

For most checks that fail the security hardening scan, the Shell Security Hardening Remediation Extension Pack provides commands that can be used to remediate these failures.

Enter the command `show security` in the shell to view all security remediation commands. You can also view commands available for each component by issuing the component name after the `show` command, for example:
For more information about the `show` command, refer to [Getting started with shell commands](#) (see page 63).

Some security compliance checks are listed for each component, along with the commands you can use to remediate any failures. After taking remediation steps to correct security compliance failures, wait 15 minutes before starting a new scan to check the results.

**NOTE:** Account hardening rules check for the use of default passwords in Vision software. Failures for these checks are resolved using a different set of commands that are not included in the Shell Security Hardening Remediation Extension Pack.

### Compute system security compliance checks

The following are some of the security compliance checks that are run on compute systems. Use these shell commands to take any corrective action.

**VCE-SEC042 Enable HTTPS management and disable HTTP**

This test is to ensure that the `HTTP_Enabled` attribute is set to false and the `HTTPS_Enabled` attribute is set to true. Both conditions must be true to pass this security check. Use this command to disable HTTP on all compute systems:

```
http computesystem set disabled
```

Use this command to enable HTTPS on all compute systems:

```
https computesystem set enabled
```

**VCE-SEC043 Ensure disablement of Telnet**

This test is to ensure that the `Telnet_Enabled` attribute is false. Use the following command to disable Telnet on all B-series compute systems.

```
telnet computesystem set disabled
```

**VCE-SEC044 Ensure disablement of CIM XML**

This test is to ensure that the `CimXML_Enabled` attribute is set to false. Use the following command to disable CIM XML on all B-series systems, regardless of their current setting:

```
cimxml computesystem set disabled
```

**VCE-SEC045 Enable SSH**

This test is to ensure that the `SSH_Enabled` attribute is set to true. Use this command to enable SSH for all compute systems.
VCE-SEC048 Ensure Appropriate Time Zone

This test is to ensure that the timezone attribute is not null. Use the following command to set the correct time zone for any compute system.

```
%time_zone computesystem[0] set
```

The command guides you through a series of prompts to get the correct time zone for the component.

VCE-SEC049 Configure NTP Time Synchronization

This test is to ensure that the ntpServer attribute is not null. Use the following command to set one or more NTP servers as the time source for a compute server.

```
ntp target set IP_address
```

where:

- `target` indicates a specific compute system by index number (for example, `computesystem[2]`) or by IP address.
- `IP_address` indicates one or more IP addresses for valid NTP servers. Specify a single IP address by enclosing it in quotes, or you can specify multiple IP addresses, for example:

```
["10.20.30.40","10.20.30.41","10.20.30.42"]
```

**NOTE:** To set all compute systems to use the same NTP server, or set of NTP servers, specify `computesystem` for the target of this command.

VCE-SEC050 Ensure Strong Local Passwords

This test is to ensure that the `passwordStrengthCheckEnabled` attribute is true. Use this command to enable the use of strong passwords on all B-series servers. This command does not affect C-series systems.

```
pw_strength_check set enabled
```

Networking security compliance checks

The following are some of the security compliance checks that are run on switch components. Use these shell commands to take any corrective action.

**VCE-SEC028 and VCE-SEC094: Disable Unused Service - CDP**

This test is to ensure that the `CDP_Service_Enabled` attribute is set to false for Nexus 1000V (VCE-SEC028) and Nexus OS (VCE-SEC094) switches. Use this command to disable CDP on all switches:
VCE-SEC111: Disable IP Source Routing

This test is to ensure that the IP_Source_Routing attribute is set to false for certain switches that support IP source routing. To disable IP source routing on all switches, use this command:

```
cdp switch set disabled
```

| NOTE: | Switches that do not support IP source routing will not be affected. The message returned for these switches indicates that this attribute is not supported.

VCE-SEC030 and VCE-SEC097: Banner Messages

This test is to ensure that the Banner attribute is not null. To set the banner for any switch, use this command:

```
login_banner target set string
```

where:

- `target` indicates a specific switch by index number (for example, `sw[2]`) or by IP address.
- `string` indicates the log on message to show users when they log on to the switch. The string must be enclosed by matching quotes. For example:

```
"WARNING: Unauthorized access to this system is forbidden \nand will be prosecuted by law. By accessing this system, \nyou agree that your actions will be monitored."
```

You can set the same log on message to multiple switches by assigning them to a variable, or to all switches if the same message is appropriate. Setting the log on banner for multiple switches will require longer processing time.

VCE-SEC095: Disable Unused Service - LLDP

This test is to ensure that the LLDP_Service_Enabled attribute is set to false on certain switches that support Link Layer Discovery Protocol (LLDP). To disable LLDP on all switches, use this command.

```
lldp switch set disabled
```

| NOTE: | Switches that do not support LLDP will not be affected. The message returned for these switches indicates that this attribute is not supported.

VCE-SEC110 and VCE-SEC040: Configure NTP Time Synchronization

This test is to ensure that the NTP_Enabled attribute is set to true for Nexus 1000V (VCE-SEC040) and Nexus OS (VCE-SEC110) switches. Use this command to set one or more NTP servers as the time source for a switch.
ntp target set IP_address

where:

- **target** indicates a specific switch by index number (for example, `sw[2]`) or by IP address.
- **string** indicates one or more IP addresses for valid NTP servers. Specify a single IP address by enclosing it in quotes, or you can specify multiple IP addresses, for example:

```plaintext
["10.20.30.40","10.20.30.41","10.20.30.42"]
```

**NOTE:** To set all switches to use the same NTP server, or set of NTP servers, specify `switch` for the target of this command.

**VCE-SEC093 and VCE-SEC027: Ensure the Use of Strong Passwords**

This test is to ensure that the `Strong_Password_Enabled` attribute is enabled for Nexus OS (VCE-SEC093) and Nexus 1000V (VCE-SEC027) switches. Use this command to enable the use of strong passwords on all switches.

```plaintext
pw_strength_check switch set enabled
```

**VCE-SEC037 and VCE-SEC104: SNMP Read-Only Configuration**

This test is to ensure that the `Snmp_Read_Only_Configuration` attribute is not null and is not set to 'public' for Nexus 1000v (VCE-SEC037) and Nexus OS (VCE-SEC104) switches. Both conditions must be true to pass this check. Use the following command to set the SNMP read-only community strings for a switch.

```plaintext
snmp_ro_community target set string
```

- **target** indicates a specific switch by index number (for example, `sw[2]`) or by IP address.
- **string** indicates one or more SNMP community strings. Specify a single string by enclosing it in quotes, or you can specify multiple strings, for example:

```plaintext
["east","west"]
```

**NOTE:** To set the same SNMP read-only community string for all switches, specify `switch` for the target of this command.

**VCE-SEC038 and VCE-SEC105: SNMP Read-Write Configuration**

This test is to ensure that the `Snmp_Read_Write_Configuration` attribute is not null and is not set to 'private' for Nexus 1000v (VCE-SEC038) and Nexus OS (VCE-SEC105) switches. Both conditions must be true to pass this check. If at least one read-write string is set to 'private', the compliance report will show that all read-write SNMP community strings fail. Use the following command to set the SNMP read-write community strings for a switch.
snmp_rw_community target set string

- **target** indicates a specific switch by index number (for example, `sw[2]`) or by IP address.
- **string** indicates one or more SNMP community strings. Specify a single string by enclosing it in quotes, or you can specify multiple strings, for example:

  ```
  ["east","west"]
  ```

**NOTE:** To set the same SNMP read-write community string for all switches, specify `switch` for the target of this command.

**VCE-SEC029 and VCE-SEC096: Disable Unused Service - Telnet**

This test is to ensure that the `Telnet_Enabled` attribute is false for Nexus 1000V (VCE-SEC029) and Nexus OS (VCE-SEC096) switches. Use this command to disable telnet on all switches.

```
telnet switch set disabled
```

**VCE-SEC039 Configure Remote Syslog for Cisco Nexus 1000v**

This test is to ensure that the `Remote_Syslog_Enabled` attribute is true for Nexus 1000V switches. Use the following command to enable remote system logging for a Nexus 1000V:

```
%remote_syslog_server target set string
```

- **target** indicates a specific switch by index number (for example, `sw[2]`) or by IP address.
- **string** indicates the IP address of the server where log messages should be sent. Specify a single string by enclosing it in quotes, or you can specify multiple strings, for example:

  ```
  ["11.12.13.14","21.22.23.24"]
  ```

As an alternative, you can use the following command to set the MSM node as the single remote syslog server:

```
%set_vision_as_remote_syslog_server switch[2]
```

This command replaces all remote syslog servers configured for the switch with the IP address of the MSM node.

**VCE-SEC032 and VCE-SEC102: Ensure VTY Line Timeout**

This test is to ensure that the `Vty_Line_Exec_Timeout` attribute is greater than zero and less than or equal to 5 for Nexus 1000V (VCE-SEC032) and Nexus OS (VCE-SEC102) switches. Use this command to set this attribute on all switches:

```
vty_line_exec_timeout sw set 3
```
VCE-SEC033 and VCE-SEC101: Ensure VTY Console Timeout

This test is to ensure that the Vty_Console_Exec_Timeout attribute is greater than zero and less than or equal to 5 for Nexus 1000V (VCE-SEC033) and Nexus OS (VCE-SEC101) switches. Use this command to set this attribute on all switches:

```
vty_console_exec_timeout sw set 3
``` 

Storage security compliance checks

The following are some of the security compliance checks that are run on storage arrays. Use these shell commands to take any corrective action.

VCE-SEC118 Control Station Banner Messages

This test is to ensure that the banner attribute is not null. To set the banner for any storage, use this command:

```
login_banner target set string
```

where:

- `target` indicates a specific storage array by index number (for example, sa[2]) or by IP address.

- `string` indicates the log on message to show users when they log on to the storage array. The string must be enclosed by matching quotes. For example:

```
"WARNING: Unauthorized access to this system is forbidden 
and will be prosecuted by law. By accessing this system, 
you agree that your actions will be monitored."
```

VCE-SEC123 Configure Control Station NTP Time Synchronization

This test is to ensure that the ntpServer attribute is not null. Use the following command to set one or more NTP servers as the time source for a storage array:

```
ntp target set IP_address
```

where:

- `target` indicates a specific storage array by index number (for example, sa[2]) or by IP address.

- `string` indicates one or more IP addresses for valid NTP servers. Specify a single IP address by enclosing it in quotes, or you can specify multiple IP addresses, for example:

```
["10.20.30.40","10.20.30.41","10.20.30.42"]
```

**NOTE:** To set all storage arrays to use the same NTP server, or set of NTP servers, specify `storagearray` for the target of this command.
Virtualization security compliance checks

The following are some of the security compliance checks that are run on ESXi hosts. Use these shell commands to take any corrective action.

VCE-SEC013 Configure NTP Time Synchronization

This test is to ensure that the NTP_Server attribute is not null. Use the following command to set one or more NTP servers as the time source for an ESXi host.

```
ntp target set IP_address
```

where:

- **target** indicates a specific ESXi host by index number (for example, esxi[2]) or by IP address.
- **string** indicates one or more IP addresses for valid NTP servers. Specify a single IP address by enclosing it in quotes, or you can specify multiple IP addresses, for example:

```
["10.20.30.40","10.20.30.41","10.20.30.42"]
```

**NOTE:** To set all ESXi hosts to use the same NTP server, or set of NTP servers, specify esxi for the target of this command.

VCE System security compliance checks

This check is to ensure that default passwords for the built-in accounts have been changed to prevent unauthorized access. The remediation steps depend on the account, account type, and VM that are provided in the report.

Account Hardening

The Vision shell is not used to remediate checks for the use of default passwords. Use one of the following procedures, depending on the account that needs to be corrected.

<table>
<thead>
<tr>
<th>User</th>
<th>Type</th>
<th>VM IP address</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Vision User</td>
<td>Vision Core</td>
<td>Changing the Central Authentication Service (CAS) password for Vision Core VM (see page 86)</td>
</tr>
<tr>
<td>admin</td>
<td>Vision User</td>
<td>MSM</td>
<td>Changing the Central Authentication Service (CAS) password for multi-system management (MSM) (see page 87)</td>
</tr>
<tr>
<td>admin</td>
<td>Vision User</td>
<td>MSP</td>
<td>Changing the CAS password for the MSP VM to match the CAS password on the MSM VM (see page 90)</td>
</tr>
<tr>
<td>vision</td>
<td>Operating System</td>
<td>MSM</td>
<td>Changing the default password for the root and vision accounts (see page 83)</td>
</tr>
<tr>
<td>root</td>
<td>Operating System</td>
<td>MSM and Vision Core</td>
<td>Changing the default password for the root and vision accounts (see page 83)</td>
</tr>
<tr>
<td>csadmin</td>
<td>Vision User</td>
<td>MSM</td>
<td>Changing the password for the Vision shell administrator (see page 96)</td>
</tr>
</tbody>
</table>
Working with compliance on Vision Core

Dell EMC Vision software no longer provides the Vision Core API for Compliance Checker. An upgrade to this most current release will remove the Vision Core API for Compliance Checker from your environment. You cannot upload compliance content to the Vision Core VM. You must use the dashboard for any compliance related tasks.
Health monitoring

VCE System health reflects the overall operational status of the system as well as the operational status of logical components and sub-components.

VCE System health is a bottom-up calculation that monitors health or operational status of the following:

- The physical components of the VCE System such as a chassis, disk array enclosure, fan, storage processor, or data mover.
- The compute, network, storage, and management components that logically group the physical components in a VCE System.
- The VCE System as a whole.

Physical components in the VCE System report an operationStatus or operStatus. Vision software uses the operational status from the physical components to create a calculatedStatus that is based on a set of Dell EMC-defined best practices. In this way, the calculatedStatus is an assessment of how the operationStatus impacts the overall health of the VCE System.

Use the Vision dashboard and the MSM API for multisystem services to retrieve health status for components and elements. The following table describes the different calculated health statuses:
<table>
<thead>
<tr>
<th>Health status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operable</td>
<td>All components have optimal health. The system is operating as expected.</td>
</tr>
<tr>
<td>Minor</td>
<td>An issue exists with one or more components. This status does not represent a significant impact to the overall health of a VCE System.</td>
</tr>
<tr>
<td>Degraded</td>
<td>One or more components are operating with degraded bandwidth, capacity, or redundancy. The system might be operating with decreased performance.</td>
</tr>
<tr>
<td>Major</td>
<td>One or more components has a significant issue. The system might be operating with decreased performance and at risk of failure.</td>
</tr>
<tr>
<td>Critical</td>
<td>One or more components has a fatal or otherwise serious issue. The system might not be fully operational and is at significant risk of failure.</td>
</tr>
<tr>
<td>Inoperable</td>
<td>The VCE System or one of its components is not operating as expected or a failure has occurred.</td>
</tr>
<tr>
<td>Not Applicable</td>
<td>One or more components does not report health status. This status occurs when components are disabled or excluded from health monitoring. This status does not affect the overall health of the VCE System.</td>
</tr>
</tbody>
</table>

**How health is calculated**

Vision software determines the overall health of a VCE System based on the operational status of its components in combination with the impact the components have on the ability of the VCE System to function, as defined by Dell EMC best practices.

Each major component, such as a network switch, a compute server, or a storage array, derives its health from its underlying sub-components. The health calculation takes into account the design and architecture of the VCE System, for example, how the ports are designed to be used or the fact that redundancy is built into the architecture. The calculation varies depending on the type of component and the role it plays in the operation of the VCE System.

The following methods are used to calculate the health of a Vblock System and its components:

<table>
<thead>
<tr>
<th>This method...</th>
<th>Is used when...</th>
<th>Processing performed</th>
<th>Example</th>
</tr>
</thead>
</table>
| Percentage-based | There are homogeneous components that serve as a resource pool. | • If the critical count is equal to or greater than 50%, set the calculated status to Critical.  
• If the critical and major count is equal to or is greater than 30%, set the calculated status to Major.  
• If the critical and major and degraded count is equal to or greater than 25%, set the calculated status to Degraded  
• If the critical and major and degraded and minor count is greater than 0, set the calculated status to Minor. | • UCS memory units  
• Local disks on a blade server (RAID 0) |
<table>
<thead>
<tr>
<th>This method...</th>
<th>Is used when...</th>
<th>Processing performed</th>
<th>Example</th>
</tr>
</thead>
</table>
| 1+1 Redundancy| There is a pair of components where only one unit is required to be functional and the other is a backup. | • If the status of one unit is operable and the status of the other unit is inoperable. The calculated status is Degraded.  
• If both units have a faulty condition, the calculated status will be assigned the less severe of the two. For example, if PSU A is major, and PSU B is minor, the calculated status will be Minor. | PSUs in Nexus switches       |
| N+1 Redundancy| There are a number (N) of homogeneous components that are designed to function properly even when one of the components is not functioning properly. | • If one unit is inoperable and the rest are operable, the impact is just loss of redundancy, hence the calculated status is Degraded.  
• If one unit is inoperable and the rest of the units are not all operable, the calculated status is the most severe status applied to any of the units. 
• If two or more units are inoperable, the calculated status is Major.  
• If no units are inoperable, depending on the actual condition of the faulty units, the calculated status is degraded or lower. | Fan units in a Nexus 7000   |
| Weighted      | There are different types of components that comprise a component.              | Each subcomponent contributes to the health of the component, but with different weight. For example, a sensor carries less weight than a PSU. The calculated status for the component is the most severe status assigned to any of the subcomponents. Implementation of the weighting algorithm varies across families (network, compute, storage). | A network chassis that contains modules, PSUs, fans, and sensors |

### Monitoring the health of VCE Systems and components

Use the Vision dashboard to check the health of VCE Systems and components.

The dashboard displays the health status of each VCE System.

![NOTE:](Image) Health status is not provided for Fabric Technology Extensions or Dell EMC Unity storage.

Refer to the dashboard help for more information about interpreting the health status for systems and their components.

### Locating the source of a health issue

When a system indicates a health issue in the Vision dashboard, you can view a list of components that belong to that system to locate the source of the issue in your VCE System.

**About this task**

Use the search to locate specific elements in the system that might be affecting the system's health. Use these steps from either the search field in the dashboard or by using the Vision shell.
Searching by health status

As you search for systems and components using the dashboard, you can filter your search results by health status. The following filters are available:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>healthy</td>
<td>Shows items that report a status of operable</td>
</tr>
<tr>
<td>warning</td>
<td>Shows items that report a status of minor</td>
</tr>
<tr>
<td>unhealthy</td>
<td>Shows items that report a status of major, degraded, critical, or inoperable</td>
</tr>
<tr>
<td>unknown</td>
<td>Shows items in which health status is not reported or does not apply</td>
</tr>
</tbody>
</table>

You can use any combination of these filters to refine your search results based on health status.

**Procedure**

1. Issue this search to find all components and elements of those components (descendants) of a VCE System with a calculated status that is not operable:
   
   ```plaintext
   find only descendants of vcesystem where uid = "unique_identifier" and calculatedStatus != "operable"
   ```

   You can also use other attributes of the system. For example, if you have a Vblock System 340 and you are looking specifically for elements with a calculated status of 'critical':
   
   ```plaintext
   find only descendants of vcesystem where vceSystemTag = "VB-340" and calculatedStatus = "critical"
   ```

   As an alternative, you can search one level at a time by using children in the search instead of descendants, for example:
   
   ```plaintext
   find only children of vcesystem where uid = "VB340-976-319-678" and calculatedStatus in ("major",critical)
   ```

   When you locate an element that is affecting the system's health, you can gather all of the attributes from the element to help determine the source of the problem.

2. Use one of the following options to get all of the attributes for a component or element,
   - If you are using the dashboard, you can export the search results to a CSV file to view them on your local computer. Refer to the dashboard help for more information about these steps.
   - If you are using the shell environment, use the print command to view all of the attributes for the component or element. Refer to Searching within Vision shell (see page 153) for more information.
Monitoring events and log messages

Monitoring and filtering events

Vision software monitors events, which are the alerts and notifications generated by the physical and logical components of a VCE System, such as switches, compute systems, and storage arrays.

Vision software uses standard mechanisms, such as SNMP traps and SMI indications, to monitor the events, which are protocol-dependent and can come in different types and formats. You can view these events with your network management software.

Syslog messaging

The Vision Core VM includes a data logging service that captures events as syslog messages.

Refer to the Logical Configuration Survey to verify that your VCE System components are properly provisioned to send syslog messages to Vision Core VM.

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>/var/log/cron</td>
<td>Information about cron jobs when the cron daemon starts a cron job.</td>
</tr>
<tr>
<td>/var/log/maillog</td>
<td>Log information from the mail server that is running on the VCE System.</td>
</tr>
<tr>
<td>/var/log/messages</td>
<td>Global system messages.</td>
</tr>
<tr>
<td>/var/log/secure</td>
<td>Information related to authentication and authorization privileges.</td>
</tr>
<tr>
<td>/var/log/spooler</td>
<td>Information for news and the UNIX-to-UNIX Copy Program (UUCP) system.</td>
</tr>
</tbody>
</table>

Changing syslog rotation parameters

Vision software uses a log rotation tool for syslog messages. You can modify the rotation parameters to suit your needs.

Before you begin

Connect to the Vision Core VM.
Procedure

1. Open the /etc/logrotate.d/syslog file for editing. The following example shows the default parameters:

   ```
   /var/log/cron
   /var/log/maillog
   /var/log/messages
   /var/log/secure
   /var/log/spooler
   /opt/vce/fm/logs/snmpd.log
   /opt/vce/fm/logs/jsadkagt.log
   /opt/vce/fm/logs/netsnmp.log
   {
     missingok
     notifempty
     # Rotate the log file when file size reaches 10M
     size 10M
     # Rotate the log file daily
     daily
     # Compress the rotated log file
     compress
     # Don't compress until the next time the log is rotated.
     # Should be used along with compress option
     delaycompress
     # Limit the number of log file rotation
     rotate 4
     sharedscripts
     postrotate
     /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true
     endscript
   }
   ```

2. Modify rotation parameters as appropriate.

3. Run the following command to save your changes:

   ```
   logrotate -f /etc/logrotate.d/syslog
   ```

Forwarding syslog messages to remote servers

Vision software uses the syslog protocol to store syslog messages on the VCE System. However, the local storage on the VCE System provides limited space. Forward syslog messages to a remote server for backup and archiving purposes.

About this task

You can configure Vision software with multiple forwarding entries. However, you can set only one forwarding entry per remote server. You can also apply forwarding filters based on facility type and severity level. For example, you can configure Vision software to forward all syslog messages to one remote server and then forward syslog messages of a given severity to a different remote server.
To configure custom filters, use the `MessagePattern=<(facility.severity)>` command. The facility and severity values are listed below. 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.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility</td>
<td>auth</td>
</tr>
<tr>
<td></td>
<td>authpriv</td>
</tr>
<tr>
<td></td>
<td>daemon</td>
</tr>
<tr>
<td></td>
<td>cron</td>
</tr>
<tr>
<td></td>
<td>ftp</td>
</tr>
<tr>
<td></td>
<td>lpr</td>
</tr>
<tr>
<td></td>
<td>kern</td>
</tr>
<tr>
<td></td>
<td>mail</td>
</tr>
<tr>
<td></td>
<td>news</td>
</tr>
<tr>
<td></td>
<td>syslog</td>
</tr>
<tr>
<td></td>
<td>ser</td>
</tr>
<tr>
<td></td>
<td>uucp</td>
</tr>
<tr>
<td></td>
<td>local0</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>local7</td>
</tr>
<tr>
<td></td>
<td>*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Severity</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>emerg</td>
</tr>
<tr>
<td></td>
<td>alert</td>
</tr>
<tr>
<td></td>
<td>crit</td>
</tr>
<tr>
<td></td>
<td>err</td>
</tr>
<tr>
<td></td>
<td>warn</td>
</tr>
<tr>
<td></td>
<td>notice</td>
</tr>
<tr>
<td></td>
<td>info</td>
</tr>
<tr>
<td></td>
<td>debug</td>
</tr>
<tr>
<td></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>*</td>
</tr>
</tbody>
</table>

**Before you begin**

- Obtain the IP address of the hostname for the remote syslog server and the port where the server is accepting syslog messages.

- If you are sending only some of the syslog messages to a remote server, you need to know the facility and severity of the log messages to forward.

- Connect to the Vision Core VM.
Procedure

Run the following command line script:

```
configureSyslogForward [-h|--help] [-l <host ip [port]>] [-d <host ip [port]>] [-a <host ip [port] [options]> -u <host ip [port] [options]
```

Where:

- **-[h|--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, pre-allocated array that holds pointers to queue elements.
    LinkedList – Uses asynchronous processing. This is the default.
    Direct – A non-queuing 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. The [options] values are listed above.

**Example**

The following are examples of how to configure Vision software to forward syslog messages:

Forward all syslog messages to a remote server with an IP address of 12.3.45.678 at port 10514:

```bash
configureSyslogForward -a 12.3.45.678 10514
```

Forward syslog messages that match a facility type of **auth** and any severity level:

```bash
configureSyslogForward -a 12.3.45.678 10514 --MessagePattern=auth.*
```

Forward syslog messages that match a facility type of **auth** and a severity level of **emerg**:

```bash
configureSyslogForward -a 12.3.45.678 10514 --MessagePattern=auth.emerg
```

Forward syslog messages over UPD, if the syslog message matches any facility type and a severity level of **debug**:

```bash
configureSyslogForward -a 12.3.45.678 10514 --Protocol=UDP --MessagePattern=*.debug
```

**Related information**

- [RFC 5424](#)
- [RFC 3164](#)

**Monitoring VM resources**

VM resource monitoring enables you to identify and monitor a collection of resources associated with a VM. Use the Vision dashboard or the MSM API for multisystem services to review point-in-time and historical key performance indicators (KPI) associated with those resources.
You can see the underlying physical infrastructure that supports each VM, and optimize workload placement and the existing infrastructure. For example, power consumption, storage capacity, server memory, or CPU usage.

Resource monitoring also shows the relationship between VCE System resources, such as virtual compute, physical compute, storage, network, and so on. For example, use the Vision dashboard to view related objects when monitoring resources. This is important when taking a resource offline for maintenance or replacement. It also helps determine what other items will be impacted, particularly ESXi and VMs.

Vision software shows information for each VM and the underlying physical infrastructure. The following illustration shows how the business logical resources, in this case VMs, leverage the infrastructure resources to correlate and generate fingerprint profiles for the VMs:

Use the Vision dashboard or the MSM API for multisystem services to generate the data required for monitoring the workloads associated with VM resources. The following examples show the main VM workload monitoring activities that are available:

- Monitor the performance of VMs across one or more VCE Systems in a data center, for example the logical and physical components.
- Query specific KPI for specific related elements on the data path to investigate performance issues associated with VMs.
- Query related physical elements, such as disk, arrays, and so on for a specific VM.

For more information about the KPI available, see Dell EMC Vision Intelligent Operations Key Performance Indicators and Certified Elements.

For more information about generating the data required for the workloads associated with VM resources, refer to the related topics and the Dell EMC Vision Intelligent Operations Programmer’s Guide.
Related information

Accessing KPI information (see page 164)
Vision dashboard layout (see page 57)
Overview of SNMP

Integrating Vision software with your network management system (NMS) enables you to monitor and maintain your VCE System using SNMP.

Vision software supports different SNMP versions, depending on the communication path and function. Find out what SNMP versions you can use to establish communication between the Vision 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>Vision 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></td>
<td></td>
<td></td>
<td>• SNMPv3</td>
</tr>
<tr>
<td>Components</td>
<td>Vision software</td>
<td>• Receiving traps</td>
<td>• SNMPv1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Vision software augments incoming traps with</td>
<td>• SNMPv2c</td>
</tr>
<tr>
<td></td>
<td></td>
<td>additional information.</td>
<td></td>
</tr>
</tbody>
</table>

Provisioning the SNMP name, location, and contact information fields for your VCE System

Use this procedure to modify the name, location, and contact information fields used for SNMP MIB identification and the generated traps on your VCE System. This updates SNMP Information only, and does not affect the restful API data.

Before you begin

You need to know:

- The name that you want to use to identify the VCE System.
- (Optional) The location of the VCE System.
- (Optional) The name of the contact person for the VCE System.

Procedure

1. Start an SSH session to the Vision Core VM and log on as the root user.
2 Run the following command:

**NOTE:** When using the `setSNMPParams` command, you need to surround a value with double quotes if the value includes spaces. For example, `setSNMPParams -n sysName "Vblock System 700-23" -f`.

```
setSNMPParams [-n sysName vce_system_name] [-l sysLocation vce_system_location] [-c sysContact vce_system_contact] [-h] [-v] [-f]
```

where:

- `-n sysName vce_system_name` Specifies the name of the VCE System. The default is the host name.
- `-l sysLocation vce_system_location` Specifies the location of the VCE System. The default is an empty string.
- `-c sysContact vce_system_contact` Specifies the contact name in your organization for VCE System related matters. The default is an empty string.
- `-h` Displays the usage help.
- `-v` Displays the version.
- `-f` Forces the System Library to reload the changes immediately.

**NOTE:** If you do not specify the `-f` option, the changes take effect on the corresponding SNMP MIB objects when you restart the System Library FM Agent using the following command:

```
service vce-fm-master restart
```

### Using SNMP traps, events, and CIM indications

Traps, events, and CIM indications are sent from a device to the Vision Core VM.

For traps, events, and CIM indications to be forwarded, SNMP has to be enabled on the device and the IP address for the Vision Core VM must be set as the trap target on the device.

### Accessing traps, events, and CIM indications

There are two ways that messages are accessed on the Network Management System.

- **AMQP messaging:** SNMP traps, events and CIM indications are translated into FMEvents, in XML format, using the AMQP messaging service. Augmentation is provided for the FMEvents if the required MIB is supported in the Vision Core VM and it has been successfully compiled. Third
party software, like Vision Adapter for vCenter Operations Manager, can access the translated messages.

- SNMP traps: If you want to forward raw SNMP traps to an NMS, use the configureSNMP script in Vision to set the NMS IP address as the target for the trap forwarding. Vision software forwards
the raw SNMP traps to the NMS. To translate the traps, your NMS must have the MIB files supported by Vision software.

**Communicating with the network management system**

SNMP enables communication between Vision software and the network management system (NMS). Vision software can also send SNMP traps and events to the NMS to facilitate discovery polling and report health status changes or issues with physical and logical components.

[NOTE:] Vision software supports SNMP on Vblock Systems and VxBlock Systems only.

Vision software also provides a set of Management Information Base (MIB) modules, and supports various RFC MIB modules, that define the structure of the Vblock System and VxBlock System. System Library populates these MIB modules so an NMS can access the various objects in the Vblock System and VxBlock System. The MIB modules are located on the Vision Core VM in the following file: `/opt/vce/fm/doc/mibs/mibs.zip`.

Refer to the *Dell EMC Vision Intelligent Operations Integration Guide for SNMP* for further information.

**Sending SNMP traps in readable format**

Vision software can transform SMI-compliant MIB files to send SNMP traps from AMQP queues in a readable format, instead of as object identifiers (OIDs). By default, Vision software provides a base set of MIB files only. If you want to receive other SNMP traps in human readable format, you must add the MIB files for those components on the Vision Core VM.
### About this task

The following are VCE-packaged MIB files:

<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 VCE private enterprise name space.</td>
<td>vce-smi-mib.txt</td>
</tr>
<tr>
<td>VCE-VBLOCK-HEALTH-MIB</td>
<td>Contains two tables that are both populated, and they share common indexes with the corresponding tables in the Entity MIB.</td>
<td>vce-vblock-health-mib.txt</td>
</tr>
<tr>
<td>VCE-VBLOCK-LOCATION-MIB</td>
<td>Describes the Vblock System location and where all the chasses 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 Vblock System. The sysObjectID value identifies the System Library, and the sysORTable contains the capabilities of System Library.</td>
<td>vce-agent-caps-mib.txt</td>
</tr>
<tr>
<td>VCE-VLAN-MIB</td>
<td>Defines information about VLANs in a Vblock System.</td>
<td>vce-vlan-mib.txt</td>
</tr>
</tbody>
</table>

### Before you begin

- **Ensure the MIB files you plan to import are SMI-compliant.**

  If the MIB files are not SMI-compliant, Vision software sends SNMP traps from AMQP as OIDs, not in a readable format. Additionally, an error such as the following is written to `/opt/vce/fm/logs/FMagent.log`:

  ```
  SMI ERROR: [SmiError{column=70, moduleName='/opt/vce/fm/mibs/mibRepository/CISCO-UNIFIED-COMPUTING-STORAGE-MIB.my', errorNumber=1000, message='[/opt/vce/fm/mibs/mibRepository/CISCO-UNIFIED-COMPUTING-STORAGE-MIB.my][1000]: Syntax error: Encountered "Unsigned64" at line 518, column 70:']
  ```

- **Connect to the Vision Core VM.**

### Procedure

1. **Run the following command:**

   ```
   stopFMagent
   ```

2. **Transfer the MIB files to the following directory on the Vision Core VM: `/opt/vce/fm/mibs/mibRepository`.**
3 Run the following command:

```
startFMagent
```

4 Verify the compiled MIB files in the following directory: `/opt/vce/fm/mibs/mibCompileDirectory`.

## List of generated traps

Generated traps are extracted from the `vce-fm-agent-mib.txt` file.

The following table lists generated traps:

<table>
<thead>
<tr>
<th>Trap</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>vceFmAgentEventConfigFileIssue</td>
<td>An issue was encountered by Vision software during self discovery for a physical component.</td>
</tr>
<tr>
<td>vceFmAgentEventDiscoveryIssue</td>
<td>An issue was encountered by Vision software during self discovery for a physical component.</td>
</tr>
<tr>
<td>vceFmAgentEventHealthPollIssue</td>
<td>An issue was encountered Vision software during a health polling cycle for a physical component.</td>
</tr>
<tr>
<td>vceFmAgentEventPhysicalHealthStatusChanged</td>
<td>A health state change was detected for a VCE System physical component by the Vblock Monitor during a health polling cycle.</td>
</tr>
<tr>
<td>vceFmAgentEventLogicalHealthStatusChanged</td>
<td>Indicates that a health state change was detected for a VCE System logical component by Vision software during a health polling cycle.</td>
</tr>
</tbody>
</table>
Changing settings on a VCE System

Changing discovery and health polling intervals

You can change the interval at which Vision software discovers VCE System components and the interval at which Vision software polls components for operating status.

About this task
Vision software runs the discovery process every 15 minutes. You can set the discovery interval between five and 1440 minutes.

Vision software polls VCE 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.

Before you begin
Connect to the Vision Core VM.

Procedure

1. Run the following command:
   ```shell
cd /opt/vce/fm/conf directory
```
2. Run the following command:
   ```shell
   stopFMagent
   ```
3. Open `fmagent.xml` for editing.
4. 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 VCE System component discovery.

   *HealthPollCycle* sets the interval for which Vision software polls VCE System for operating status.

5. Change the intervals for the discovery cycle and health polling as appropriate.
6. Save and close the `fmagent.xml` file.
Run the following command:

```
startFMagent
```

### Customizing logon banners for the Vision Core VM

You can add logon banners to display customized information when users log on to the Vision Core VM.

**Before you begin**

Connect to the Vision 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 logon banner as appropriate.

3. Save and close the files.
Using the search tools

You can use a *freeform query* to search for detailed information about VCE Systems, components, and elements for each component.

Tools for searching

Vision software provides Vision dashboard, Vision shell, and MSM API for Multisystem Services, for searching the VCE Systems in the data center.

- **Vision dashboard**

  After logging on to dashboard, you can enter a freeform query using the search bar or click *Advanced Search* for assistance in building more specific search terms. The menu icon at the left of the toolbar also provides links to common searches for components based on health status. The dashboard also allows you to save searches that you expect to use often.

  Issuing the query `find switch` in the dashboard returns a list of switches in the Details view and you can select which attributes that you want to display for each switch.

  The dashboard also allows you to save searches that you might need to use frequently. See the dashboard help for additional information.

- **Vision shell**

  Freeform query is available on the command line using the `find` command.

  Issuing the command `find switch` in Vision shell returns a list of switches that includes the alias, IP address, and host VCE System type (*vceSystemTag* attribute).

- **MSM API for Multisystem Services**

  For more information about using the REST API for searching, see the *Dell EMC Vision Intelligent Operations Programmer's Guide*.

Searching within Vision shell

Searching within Vision shell is similar to the search syntax used in Vision dashboard, except that it must start with the `find` command. In dashboard, the `find` keyword is optional.

**Note:** The Vision shell is supported on a VxBlock System and Vblock System only. Use these examples to become familiar with the search syntax using Vision shell. The syntax is generally the same in the Vision dashboard, except where noted.

Finding a component or element

The following examples show how to find information about a VCE System, its components and elements within the data center.

Searching for a VCE System
This search will find all systems, regardless of type. You can also search for specific system types, for example, using `vblock`, `vxblock` or `vxrack`.

**Searching for components**

You can search for components using the following strings

- `storagearray`
- `computesystem`
- `switch`
- `os` (for the ESXi host component)

**Searching for elements**
Depending on your system configuration, the following element strings can be searched:

<table>
<thead>
<tr>
<th>Category</th>
<th>Example Strings</th>
</tr>
</thead>
<tbody>
<tr>
<td>acu</td>
<td></td>
</tr>
<tr>
<td>appinfo</td>
<td></td>
</tr>
<tr>
<td>backplane</td>
<td></td>
</tr>
<tr>
<td>battery</td>
<td></td>
</tr>
<tr>
<td>cell</td>
<td></td>
</tr>
<tr>
<td>chassis</td>
<td></td>
</tr>
<tr>
<td>compute</td>
<td></td>
</tr>
<tr>
<td>computechassis</td>
<td></td>
</tr>
<tr>
<td>computeimodule</td>
<td></td>
</tr>
<tr>
<td>computeiserver</td>
<td></td>
</tr>
<tr>
<td>contactinput</td>
<td></td>
</tr>
<tr>
<td>container</td>
<td></td>
</tr>
<tr>
<td>controlStation</td>
<td></td>
</tr>
<tr>
<td>controlstationenclosure</td>
<td></td>
</tr>
<tr>
<td>dae</td>
<td></td>
</tr>
<tr>
<td>Datacenter</td>
<td></td>
</tr>
<tr>
<td>datamover</td>
<td></td>
</tr>
<tr>
<td>dataserver</td>
<td></td>
</tr>
<tr>
<td>datastore</td>
<td></td>
</tr>
<tr>
<td>director</td>
<td></td>
</tr>
<tr>
<td>disk</td>
<td></td>
</tr>
<tr>
<td>dme</td>
<td></td>
</tr>
<tr>
<td>dpe</td>
<td></td>
</tr>
<tr>
<td>engine</td>
<td></td>
</tr>
<tr>
<td>expansionmodule</td>
<td></td>
</tr>
<tr>
<td>expansionslot</td>
<td></td>
</tr>
<tr>
<td>extraattribute</td>
<td></td>
</tr>
<tr>
<td>fabricinterconnect</td>
<td></td>
</tr>
<tr>
<td>fabricmodule</td>
<td></td>
</tr>
<tr>
<td>fan</td>
<td></td>
</tr>
<tr>
<td>fanbay</td>
<td></td>
</tr>
<tr>
<td>fcport</td>
<td></td>
</tr>
<tr>
<td>fixedmodule</td>
<td></td>
</tr>
<tr>
<td>fixedslot</td>
<td></td>
</tr>
<tr>
<td>GbEPort</td>
<td></td>
</tr>
<tr>
<td>HostCluster</td>
<td></td>
</tr>
<tr>
<td>HostScsiDiskPartition</td>
<td></td>
</tr>
<tr>
<td>humidityinput</td>
<td></td>
</tr>
<tr>
<td>initiator</td>
<td></td>
</tr>
<tr>
<td>iocard</td>
<td></td>
</tr>
<tr>
<td>linkcontrolcard</td>
<td></td>
</tr>
<tr>
<td>memoryunit</td>
<td></td>
</tr>
<tr>
<td>mibe</td>
<td></td>
</tr>
<tr>
<td>module</td>
<td></td>
</tr>
<tr>
<td>network</td>
<td></td>
</tr>
<tr>
<td>networkTempSensor</td>
<td></td>
</tr>
<tr>
<td>networkchassis</td>
<td></td>
</tr>
<tr>
<td>nsxcontroller</td>
<td></td>
</tr>
<tr>
<td>os</td>
<td></td>
</tr>
<tr>
<td>outlet</td>
<td></td>
</tr>
<tr>
<td>pdu</td>
<td></td>
</tr>
<tr>
<td>pduline</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>portlink</td>
<td></td>
</tr>
<tr>
<td>powersupplybay</td>
<td></td>
</tr>
<tr>
<td>processorunit</td>
<td></td>
</tr>
<tr>
<td>protectiondomain</td>
<td></td>
</tr>
<tr>
<td>psu</td>
<td></td>
</tr>
<tr>
<td>rack</td>
<td></td>
</tr>
<tr>
<td>raidgroup</td>
<td></td>
</tr>
<tr>
<td>sfp</td>
<td></td>
</tr>
<tr>
<td>spe</td>
<td></td>
</tr>
<tr>
<td>stackport</td>
<td></td>
</tr>
<tr>
<td>storage</td>
<td></td>
</tr>
<tr>
<td>storagechassis</td>
<td></td>
</tr>
<tr>
<td>storeagerecontroller</td>
<td></td>
</tr>
<tr>
<td>storagedevice</td>
<td></td>
</tr>
<tr>
<td>storageimodule</td>
<td></td>
</tr>
<tr>
<td>storagenode</td>
<td></td>
</tr>
<tr>
<td>storagePool</td>
<td></td>
</tr>
<tr>
<td>storageprocessor</td>
<td></td>
</tr>
<tr>
<td>storagecontroller</td>
<td></td>
</tr>
<tr>
<td>storagesystem</td>
<td></td>
</tr>
<tr>
<td>storageTier</td>
<td></td>
</tr>
<tr>
<td>storageVolume</td>
<td></td>
</tr>
<tr>
<td>storagevirtualizer</td>
<td></td>
</tr>
<tr>
<td>storagevirtualizerenclosure</td>
<td></td>
</tr>
<tr>
<td>storagevirtualizerprocessor</td>
<td></td>
</tr>
<tr>
<td>switchfan</td>
<td></td>
</tr>
<tr>
<td>temperatureinput</td>
<td></td>
</tr>
<tr>
<td>vcesystemconnectivity</td>
<td></td>
</tr>
<tr>
<td>vcesystemmi</td>
<td></td>
</tr>
<tr>
<td>VIManager</td>
<td></td>
</tr>
<tr>
<td>VirtualMachine</td>
<td></td>
</tr>
<tr>
<td>vlan</td>
<td></td>
</tr>
<tr>
<td>vnxpsu</td>
<td></td>
</tr>
<tr>
<td>voltageinput</td>
<td></td>
</tr>
</tbody>
</table>

For example, to get a list of disk array enclosures (DAEs) throughout all VCE Systems:

```
Vision> find dae
{Dae 'DAE-4',
 Dae 'DAE-5',
 Dae 'DAE-8',
 Dae 'DAE-3',
 Dae 'DAE-4',
 Dae 'DAE-1',
 Dae 'DAE-6',
 Dae 'DAE-2',
 Dae 'DAE-7',
 Dae 'DAE-2',
 Dae 'DAE-7',
 Dae 'DAE-3',
 Dae 'DAE-8',
 Dae 'DAE-5',
 Dae 'DAE-6',
 Dae 'DAE-1',
}
In Vision shell, the returned results are displayed in an array as a comma-separated list enclosed in brackets.

**Getting detailed information about elements in Vision shell**

To obtain detailed information about elements that the Vision shell search returns in an array, first assign the element array to a variable, as follows:

``` Vision> enclosure1 = %find dae 
```

You can use any string for the variable name. In this case, the array is assigned to the variable `enclosure1`. Variable names cannot start with a number. The percent (%) symbol must be prefixed to the find command. Next confirm that the array assignment is correct:

``` Vision> print enclosure1
```

To gather detailed information about the attributes of any single element in the array, use the `print` command, specifying the element by index number. The elements in the array are separated by commas and assigned an index number starting with zero. In the DAE example, `DAE-1` is the fourth element in the array, has the index number 3, and is referenced as `enclosure1[3].`

In the following example, the first DAE in the list is assigned a variable name. This is optional, as the same information can be retrieved by using `print enclosure1[0].`

``` Vision>dae4 = enclosure1[0]
Vision> print dae4
All current attributes:
******************************
alias: DAE-4
calculatedStatus: inoperable
client: <vshell.convergedclient.ConvergedClient object at 0x30f6d10>
cvmHost: vision174-16.vb300swqa.example.lab
dataCenter: voltronlanddc
description: DAE-4
host: <vshell.convergedclient.ConvergedHost instance at 0x6399878>
isdeleted: False
lastOperStatus: notApplicable
lastStatusChange: 2015-04-28T03:07:32.903Z
modelName: VMAX10K
name: SYMMETRIX-++000198701339-++SB-1-++DAE-4
operStatus: inoperable
properties: {}
slibHost: vision174-106.vb700swqa.example.lab
time: 1430200567810
uid: root/
emc:Symm_EnclosureChassis.CreationClassName="Symm_EnclosureChassis",Tag="SYMMETRIX-++000198701339-++SB-1-++DAE-4"
vblockBuilding: 2635 Meridian Parkway
vblockDescription: 720w10k VB720-976-319-643
```
Finding elements by attribute value

Use the where or with keyword to include an attribute name and value to filter a search. Use the following operators to assign the value:

- `=` (or type `is`)
- `!=`
- `like`
- `>`
- `>=`
- `<` (or type `less than`)
- `<=`
- `between` (or type `and`)
- `in`

⚠️ **NOTE:** Many searches require double quotes around the attribute value.

**Example: Finding a VCE Systems with vceSystemTag = VB-720**

```bash
Vision>find vcesystem where vceSystemTag = vb-720
[VB-720]
```

**Example: Finding storage arrays with less than 1 terabyte of total raw storage**

```bash
Vision>find storagearray with totalRawCapacity < 1T
[Storage Array 'vcemoVNX5400-CS0' at 10.1.139.52 in Vblock 'VB-340',
Storage Array '000198701339' at 10.1.140.58 in Vblock 'VB-340']
```

**Example: Finding compute systems where the attribute contains a String value**

```bash
Vision>find computesystem where cvmHost like "%test22%"
[UCS 'SERVER-B' at 10.1.144.11 in Vblock 'VB-340',
UCS 'VMABO-UCS-1' at 10.1.139.30 in Vblock 'VB-340']
```

**Example: Finding storage volumes between a range of values for allocatedSpace**

```bash
```
Example: Finding switches within a collection of values

```
Vision>find switch where operStatus in (unreachable,critical)

[Switch 'M9A' at 10.1.140.20 in Vblock 'VB-720',
 Switch 'M9B' at 10.1.140.21 in Vblock 'VB-720',
 Switch 'N1A' at 10.1.144.78 in Vblock 'VB-720',
 Switch 'N1A' at 10.1.140.235 in Vblock 'VB-720']
```

Finding elements by location (vblockGeo)

Use the in keyword to specify the location for the search target. In this example, the query targets fabric interconnects located in Tokyo, Japan. The location string ("toKyo") passed to the search is not case-sensitive.

```
Vision>find fabricinterconnect in "tokyo"

[Fabricinterconnect 'U6A' at 10.1.139.31 in Vblock 'VB-340',
 Fabricinterconnect 'U6B' at 10.1.139.32 in Vblock 'VB-340']
```

Find an element belonging to a specific component

Use the find only and related to keywords to filter the search down to a specific component. In the following example, all memory units that belong to a compute system with a specific hostname.

Example: Finding an element belonging to a specific component

```
find only memoryunit related to computesystem where host = test34.example.com

[Memoryunit,
 Memoryunit,
 Memoryunit,
 Memoryunit,
 Memoryunit,
 ...,
 Memoryunit]
```

In this example, the related to keywords makes this search execute as a relational query, starting from the matching `computesystem` elements and traversing related elements to find `memoryunit` instances. The `find only` keywords omits the traversed elements from the results, including only memory units.

Example: Finding an element belonging to a specific component with a specific attribute value

Use the then only keywords to further refine a search to specific conditions.
Combining search terms

You can combine search clauses or attributes using the and and or keywords. Using the and keyword between search conditions means all conditions must be true. Using or between search conditions means at least one condition must be true.

Example: Combining attributes with AND and OR keywords

```
Vision>find storagearray with totalRawCapacity > 2T and type = "VMAX"
[Storage Array '000198701339' at 10.1.140.58 in Vblock 'VB-720']
```

```
Vision>find storagearray with totalRawCapacity > 2T or type = "VMAX"
[Storage Array '000198701339' at 10.1.140.58 in Vblock 'VB-720',
 Storage Array 'vcemoVNX5400-CS0' at 10.1.139.52 in Vblock 'VB-720']
```

Selecting attributes for the search results

Use the select attributes keywords to limit the attributes returned in the search results.

Example: Selecting and displaying specific attributes for a switch

```
Vision>switchSelect = %find select attributes host,operStatus for switch
Vision>print switchSelect[3]
All current attributes:
****************************
client                         : <vshell.convergedclient.ConvergedClient object at 0x2a5fed0>
```
Example: Combining a value range when specifying attributes

```plaintext
Vision>chassisIP = %find select attributes host, inputPower, vblockModelName computechassis where inputPower between 500 and 900
Vision>print chassisIP[1]
All current attributes:

client : <vshell.convergedclient.ConvergedClient object at 0x2a5fed0>
host : <vshell.convergedclient.ConvergedHost instance at 0x5d1ee60>
inputPower : 594.0
vblockModelName : 340w5400
```

Searching for the children or descendants of a search target

To search for the first level of components and elements that belong to a search target, use the children of keywords. The results show the first level in the system hierarchy that are contained by the search target.

```plaintext
Vision>find children of vcesystem where vceSystemTag = VB-340
[Vlan, Vlan, Vlan, Vlan, Vlan, Vlan, Vlan, Vlan, Compute, Vcesystemmi, Vcesystemconnectivity, Vlan, Vlan, Vblock 'VB-340', Vlan, Vlan, Vlan, Vlan, Vlan, Storage, Rack, Network]
```

You can expand the results by searching for all descendants of a search target using the descendants of keywords. You can expect a large set of results for a VCE System. The following example uses `computeserver`.

```plaintext
Vision>find descendants of computeserver where serialNum = "FCH16117AX9"
```
Memoryunit 'vcemo6140A/chassis-1/blade-3/board/memarray-1/mem-21',
Memoryunit 'vcemo6140A/chassis-1/blade-3/board/memarray-1/mem-9',
Port 'vcemo6140A/chassis-1/blade-3/adaptor-1/ext-eth-2',
Switch 'VB300SWQA-dVSwitch01',
Processorunit 'vcemo6140A/chassis-1/blade-3/board/cpu-1',
Memoryunit 'vcemo6140A/chassis-1/blade-3/board/memarray-1/mem-31',
Switch 'VB300SWQA-dVSwitch01',
Memoryunit 'vcemo6140A/chassis-1/blade-3/board/memarray-1/mem-7',
Storagecontroller,
Memoryunit 'vcemo6140A/chassis-1/blade-3/board/memarray-1/mem-17',
Memoryunit 'vcemo6140A/chassis-1/blade-3/board/memarray-1/mem-29',
Iocard,
Port 'vcemo6140A/chassis-1/blade-3/adaptor-1/host-fc-1',
Port 'vcemo6140A/chassis-1/blade-3/adaptor-2/host-eth-1',
Port 'vcemo6140A/chassis-1/blade-3/adaptor-2/ext-eth-2',
VirtualMachine 'fmcomp-227 (MSM Load Testing, C2 S1)',
Processorunit 'vcemo6140A/chassis-1/blade-3/board/cpu-3',
Memoryunit 'vcemo6140A/chassis-1/blade-3/board/memarray-1/mem-15',
Memoryunit 'vcemo6140A/chassis-1/blade-3/board/memarray-1/mem-27',
Memoryunit 'vcemo6140A/chassis-1/blade-3/board/memarray-1/mem-5',
Port 'vcemo6140A/chassis-1/blade-3/adaptor-2/host-fc-1',
Datacenter 'Datacenter',
HostCluster 'VB300SWQA-CLUSTER1',
VirtualMachine 'John_F_Slib(10.1.139.151)',
Processorunit 'vcemo6140A/chassis-1/blade-3/board/cpu-2',
Memoryunit 'vcemo6140A/chassis-1/blade-3/board/memarray-1/mem-1',
Memoryunit 'vcemo6140A/chassis-1/blade-3/board/memarray-1/mem-11',
Memoryunit 'vcemo6140A/chassis-1/blade-3/board/memarray-1/mem-23',
Iocard,
Port 'sys/chassis-1/blade-3/adaptor-1/mgmt',
Port 'vcemo6140A/chassis-1/blade-3/adaptor-2/host-eth-2'

Searching for the parents or ancestors of an object

Similar to finding the items that belong to a search target (children), you can also search for the items that are higher in the system hierarchy using the parents of keywords.

Vision>find parents of computeserver where serialNum = "FCH16117AX9"
[Computeserver 'vcemo6140A/chassis-1/blade-3', Computechassis 'UC6A']

You can expand the search to show all ancestors of a search target.

Vision>find ancestors of computeserver where serialNum = "FCH16117AX9"
[UCS 'VMABO-UCS-1' at 10.1.139.30 in vcesystem 'VB-340',
Computeserver 'vcemo6140A/chassis-1/blade-3',
Compute,
Vblock 'VB-340',
Computechassis 'UC6A']
Finding components based on compliance results

Use the following clauses with components to get a list of components based on compliance results:

compliant with | not compliant with
The value for this clause must be one of the compliance scan categories:

- rcm
- hardening
- vsa

Vision>find switch not compliant with hardening
[Switch 'M9A' at 10.1.140.20 in Vblock 'VB-720',
Switch 'N5A' at 10.1.140.22 in Vblock 'VB-720']

vulnerable to | not vulnerable to
Use this clause to check vulnerability to one of these specific threats

- heartbleed
- shellshock

Vision>find switch vulnerable to shellshock
[Switch 'M9A' at 10.1.140.20 in Vblock 'VB-720',
Switch 'M9B' at 10.1.140.21 in Vblock 'VB-720']

affected by | not affected by
Use this clause to determine if a component is affected by any VCE Technical and Security Advisories.

Vision>find switch affected by vce306705
[Switch 'M9A' at 10.1.140.20 in Vblock 'VB-720',
Switch 'M9B' at 10.1.140.21 in Vblock 'VB-720']

Combining search with Vision shell commands

You can issue Vision shell commands with a search using the | character.

Note: The Vision shell is supported on a Vblock System and a VxBlock System only.

If the search command returns any element that can be used as the target of a command, you can combine it directly with the command using the | character. These elements include VCE Systems, compute systems, switches, storage arrays, and VMware ESXi hosts.

Find all switches and show NTP configuration

This example shows the search find command followed by ntp get.
Find all switches and change the NTP configuration

In this example, the search `find` command is followed by the `ntp set` command to make immediate configuration changes.

```bash
Vision>find switch with alias = N1A | ntp get
[Switch 'N1A' at 10.1.140.235 in Vblock 'Vb-720';, result: ['1.1.1.1'],
Switch 'N1A' at 10.1.140.215 in Vblock 'Vb-720';, result: ['2.1.1.1']]  

Vision>find switch with alias = N1A | ntp set 24.0.112.1
[Switch 'N1A' at 10.1.140.235 in Vblock 'Vb-720';, result: "ntp servers set: ['24.0.112.1']",
Switch 'N1A' at 10.1.140.215 in Vblock 'Vb-720';, result: "ntp servers set: ['24.0.112.1']"]
```
### KPI overview

A key performance indicator (KPI) is an attribute for which Vision software maintains time-based and historical data.

KPI allow you to monitor the performance of various VCE System components and identify problems when performance degrades. For example, you can view KPI charts for one or more storage arrays through the Vision dashboard. You can also retrieve aggregated and time series key performance indicators such as capacity, performance, and utilization for a collection of VCE Systems.

Associated objects and the KPI of a specific element type can also be retrieved, for example, `storagearray`, `computeserver`, and `VirtualMachine`.

Refer to *Dell EMC Vision Intelligent Operations Version Key Performance Indicators and Certified Elements* for a detailed list of the VCE Systems KPI.

### Accessing KPI information

A KPI specifies a performance measurement for a particular element type within a VCE System.

Access KPI information using either the Vision dashboard or the MSM API for multisystem services.

#### Vision dashboard

Displays charts and graphs of KPI information for the selected element type. The following table shows examples of KPI information:

<table>
<thead>
<tr>
<th>Element type</th>
<th>Examples of KPI information</th>
</tr>
</thead>
<tbody>
<tr>
<td>storagearray</td>
<td>Remaining raw capacity</td>
</tr>
<tr>
<td></td>
<td>Total space available for user data</td>
</tr>
<tr>
<td></td>
<td>Remaining managed space</td>
</tr>
<tr>
<td></td>
<td>Total IO per second</td>
</tr>
<tr>
<td>storagepool</td>
<td>User capacity</td>
</tr>
<tr>
<td>storagevolume</td>
<td>Volume user capacity</td>
</tr>
<tr>
<td>disk</td>
<td>Disk raw capacity</td>
</tr>
<tr>
<td></td>
<td>Bandwidth</td>
</tr>
<tr>
<td>switch</td>
<td>Current bandwidth</td>
</tr>
<tr>
<td></td>
<td>Number of error inbound packets</td>
</tr>
<tr>
<td>rack</td>
<td>Monitor total energy</td>
</tr>
<tr>
<td></td>
<td>Monitor average power consumption</td>
</tr>
<tr>
<td>computeserver</td>
<td>Total memory</td>
</tr>
</tbody>
</table>
MSM API for multisystem services

Use the MSM API for multisystem services to retrieve the following KPI data:

- All existing KPI definitions in the VCE System.
- Existing KPI definitions for a particular element type.
- Existing KPI definitions for a particular element type and component category.
- Time series KPI data:
  - A particular time resolution.
  - A start time for time series queries.
  - An end time for time series queries.

Refer to the *Dell EMC Vision Intelligent Operations Key Performance Indicators and Certified Elements* document for a detailed list of the VCE Systems KPI.

Refer to the *Dell EMC Vision Intelligent Operations Programmer’s Guide* for more information about the MSM API for multisystem services.

Reference:

Monitoring VM resources (see page 142)
Working with Secure Remote Services (ESRS)

Vision software can connect to Secure Remote Services (ESRS) and automatically send system inventory and RCM fitness information through the ESRS connection to the Dell EMC Data Lake. Services and Support can use the collected data for analysis and remote troubleshooting.

Use the Vision shell ESRS Extension Pack to perform the following functions:

- Configure Vision software to use ESRS
- Deregister Vision software with ESRS
- Update an ESRS gateway configuration or Vision software ID (SWID)
- Upload information to ESRS about your VCE System:
  - Release Certification Matrix (RCM) compliance scan results (ZIP file containing CSV, XLS, PDF, and XML files) (if you have installed RCM content and selected a default profile)
  - VCE System inventory files (JSON)
- Modify the schedule Vision software uses to regularly send RCM and inventory information to ESRS

Configuring ESRS

Follow these procedures to set up the connection between Vision software and Secure Remote Services (ESRS).

To configure a Vision software MSM VM to point to an ESRS gateway, refer to Registering Vision software with an ESRS gateway (see page 166)

To add software identifiers for MSM VMs, refer to Adding a software identifier for an MSM VM (see page 169)

You can use Vision software in a configuration where multiple data centers have a local cluster of MSM VMs and replicate data to each other. This configuration requires that each MSM VM uses an ESRS gateway that is local to the MSM VM. Each MSM VM connects to one ESRS gateway.

Registering Vision software with an ESRS gateway

Use the Vision shell to register Vision software with Secure Remote Services (ESRS).

Before you begin

To register Vision software with ESRS, ensure you have received an email from Dell EMC with a license activation code (LAC). Use the LAC you received with the Vision software 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 Vision software instance with ESRS. Refer to Retrieving the software ID from the Licensing system (see page 170) if you need information on how to obtain the SWID.
Procedure

1. Establish an SSH connection to the MSM VM and log on. The default credentials are:
   - Username: root
   - Password: V1rtu@1c3!

   **Remember:** The password should be changed to protect the system from unauthorized access.

2. Execute the following script:

   /opt/vce/shell/bin/ESRSScript/esrs_setup.sh

3. The following message displays:

   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 message similar to the following appears:

   No software identifier (SWID) found for host 10.1.174.174
   Do you want to enter a software identifier (SWID) for host 10.1.174.174 (yes/no):

   a. Type **yes**. A message similar to the following appears:

      Please enter the software identifier (SWID) for host 10.1.174.174:

   b. Type the software identifier (SWID). A message similar to the following appears:

      Please enter your ESRS gateway hostname or IP address:

   c. Type the ESRS gateway IP address. The following message appears:

      Please enter your NTID:

   d. Type your Dell EMC network/Windows ID. The following message appears:

      Please wait for next token and enter your RSA PIN + Token:

   e. Type your RSA pin and token. It takes a moment to authenticate, then a message similar to the following appears:

      ESRS configuration for 10.1.174.174 for the ESRS gateway 10.1.174.148 was successful.
      ESRS gateway configuration completed, exiting setup script.

   f. Go to Step 6.
5 Type no at the prompt. A message similar to the following appears:

```
ESRS gateway configuration not found in VCE Vision System
Do you want to create a new ESRS gateway configuration {yes/[no]}:
```

a Type yes to create a new ESRS gateway configuration.

b Type the ESRS gateway hostname or IP address. Then provide your username and password for https://support.vce.com/ at the prompt for each.

Messages similar to the following appear:

```
ESRS gateway configuration has been created for 10.1.174.148
No software identifier (SWID) found for host 10.1.174.174
Do you want to enter a software identifier (SWID) for host 10.1.174.174 {yes/[no]}:
```

c Type yes to enter the software identifier (SWID).

d At the SWID prompt, type the unique software identifier (SWID) from the CLP file.

A message similar to the following appears:

```
ESRS configuration for 10.1.174.174 for the ESRS gateway 10.1.174.148 was successful.
ESRS gateway configuration completed, exiting setup script
```

6 Verify the registration status by performing the following steps.

a Run the following command: vshell

The Vision shell initializes with the following messages:

```
VCE Vision shell 3.5.0.0
Copyright 2013-2016 VCE Company, LLC. All rights reserved.
VCE, VCE Vision, VCE Vscale, Vblock, VxBlock, VxRail and the VCE logo are registered trademarks of VCE Company LLC.
All other trademarks used herein are the property of their respective owners.
MSM Hostname (Press Enter for localhost):
```

Skip the login prompts by starting shell with the following option:

```
vshell -l /opt/vce/shell/conf/ipython.conf
```

b Enter the MSM hostname to which you want to connect or press Enter for the localhost.

c When prompted, enter your username and password. The default administrative credentials for Vision shell are:

- Username: csadmin
- Password: D@ngerous1

This password should be changed to protect the system from unauthorized access.
Wait for the `deviceState` to be set to **Managed** and the `deviceStatus` to be set to **Online**. Verify the registration status is similar to the following:

```
Vision>esrs_register status
{'deviceState': 'Managed',
 'deviceStatus': 'Online',
 'ipAddress': '10.3.16.36',
 'model': 'VCEVISION',
 'responseCode': 0,
 'serialNumber': 'VCEVISIONTCOE03',
 'validationCode': '0',
 'validationError': 'No errors in general. '}
```

### Adding a software identifier for an MSM VM

Use the Vision shell to add a software ID for an MSM VM to an already configured ESRS gateway. You are prompted to enter the ESRS gateway to use from a known list of ESRS gateway IP addresses.

#### Before you begin

If you are adding a software ID to an ESRS gateway that has not been configured, refer to **Registering Vision software with an ESRS gateway** (see page 166) for what to do.

#### Procedure

1. Establish an SSH connection to the MSM VM and log on. The default credentials are:
   - Username: `root`
   - Password: `V1rtu@1c3!`

   **Remember:** The password should be changed to protect the system from unauthorized access.

2. Run the following command: `vshell`

   The Vision shell initializes with the following messages:

   ```
   VCE Vision shell 3.5.0.0
   Copyright 2013-2016 VCE Company, LLC. All rights reserved.
   VCE, VCE Vision, VCE Vscale, Vblock, VxBlock, VxRail and the VCE logo are registered trademarks of VCE Company LLC.
   All other trademarks used herein are the property of their respective owners.
   MSM Hostname (Press Enter for localhost):
   ```

   Skip the login prompts by starting shell with the following option:

   ```
   vshell -l /opt/vce/shell/conf/ipython.conf
   ```

3. Enter the MSM hostname to which you want to connect or press **Enter** for the localhost.
When prompted, enter your username and password. The default administrative credentials for Vision shell are:

- Username: `csadmin`
- Password: `D@ngerous1`

This password should be changed to protect the system from unauthorized access.

Type the following command: `esrs_register add swid=software identifier`

Any existing ESRS gateways display.

Type the number (0, 1, 2...) of the ESRS gateway to which you want to register the VM. A message displays that the product is successfully registered.

### Retrieving the software ID from the Licensing system

Use this procedure to retrieve the software ID (SWID) from the Dell EMC Licensing system. You need this software ID when configuring Secure Remote Services (ESRS) for Vision software.

#### Before you begin

Make sure you have received an email from Dell EMC with a license activation code (LAC). You also have the option of entering the sales order number in the procedure below.

If you need more information on the software activation process, refer to the product documentation located on Dell EMC Software Licensing Central.

#### Procedure

1. Connect to [Dell EMC Software Licensing Central](#).
2. Click **Activate My Software**.
3. In the **License Authorization Code** field, type (or copy and paste) the LAC code. You can alternately enter the sales order number in the **Sales Order #** field. Click **Search**. The **STEP 1: SELECT AVAILABLE PRODUCTS TO ACTIVATE** page displays products available for activation.
4. Select the product to activate and click **Start the Activation Process**. The **STEP 2: CONFIRM COMPANY & SITE** page appears.
5. Confirm the company registered for the activation. Click **Select a Machine**. The **STEP 3: SELECT A MACHINE** page appears.
6. In the **Add a New Machine** field, enter the a unique identifier for the machine name. It is recommended that this be the VCE System serial number. Click **Save Machine & Continue to Next Step**. The **STEP 4: ENTER PRODUCT QUANTITIES & MACHINE DETAILS** page appears.
7. In the **Quantity to Activate** field, enter the quantity of entitlements to activate for the machine. Click **Next: Review**. The **STEP 5: REVIEW YOUR SELECTIONS** page appears.
Review the information. Click **Activate** to generate the software identifier. The **STEP 6: ACTIVATION COMPLETE** page appears.

Obtain a copy of the software identifier needed to configure ESRS for Vision software by performing either of the following steps:

- 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 and copy the software identifier to the clipboard.

**What to do next**

Use the software identifier when configuring ESRS for Vision software.

**Updating an ESRS gateway configuration or software identifier (SWID)**

Use this procedure if you need to update either an existing Secure Remote Services (ESRS) gateway configuration or software identifier (SWID) for a host.

**Before you begin**

Ensure the following items occur:

- The ESRS host and user exist in Vision software Credential Manager.
- You have received an email from Dell EMC with a License Activation Code (LAC). Use the LAC you received with the Vision software to obtain a Common Licensing Platform (CLP) file from the EMC Electronic Licensing Management System (ELMS). This CLP contains the unique identifier (SWID) required to register a Vision software instance with ESRS.

**Procedure**

1. Establish an SSH connection to the MSM VM and log on. The default credentials are:
   - Username: **root**
   - Password: **V1rtu@1c3!**
   **Remember**: The password should be changed to protect the system from unauthorized access.

2. Execute the following script: `/opt/vce/shell/bin/ESRSScript/esrs_setup.sh`
3 The following message displays:

Are you a Dell EMC employee using a RSA token (FOB)? (yes/[no]):

4 Type no at the prompt. A message similar to the following appears:

1 ESRS gateway configuration(s) found in VCE Vision System
Do you want to update the existing ESRS gateway configuration for 10.1.174.148 (yes/[no]):

Perform one of the following actions:

– To update the ESRS gateway configuration, type yes at the prompt. Then type the ESRS gateway hostname or IP address and the username and password for support.emc.com at the prompt for each.

– If you do not want to update the ESRS gateway configuration, type no or press Enter.

Messages similar to the following appear:

Software identifier (SWID) VCEVISIONTCOE03 was found for host 10.1.174.174
Do you want to update the software identifier (SWID) for host 10.1.174.174 (yes/[no]):

5 If you want to update the SWID, type yes. A message similar to the following appears:

Please enter the software identifier (SWID) for host 10.1.174.174:

6 Type the unique software identifier from the CLP file when prompted. A message similar to the following appears:

ESRS configuration for 10.1.174.174 for the ESRS gateway 10.1.174.148 was successful.
ESRS gateway configuration completed, exiting setup script.

Updating a software identifier (SWID) (for Dell EMC employees only)

Dell EMC employees should use this procedure to update a software identifier (SWID) for a host.

Before you begin
Ensure the following items occur:

• The Secure Remote Services (ESRS) host and user exist in Vision software Credential Manager.

• You have received an email from Dell EMC with a License Activation Code (LAC). Use the LAC you received with the Vision software to obtain a Common Licensing Platform (CLP) file from the Electronic Licensing Management System (ELMS). This CLP contains the unique identifier (SWID) required to register a Vision software instance with ESRS.
Procedure

1. Establish an SSH connection to the MSM VM and log on. The default credentials are:
   - Username: root
   - Password: V1rtu@1c3!

   **Remember:** The password should be changed to protect the system from unauthorized access.

2. Execute the following script: `/opt/vce/shell/bin/ESRSScript/esrs_setup.sh`

3. The following message displays:

   Are you a Dell EMC employee using a RSA token (FOB)? (yes/[no]):

4. Type **yes** at the prompt. A message similar to the following appears:

   Software identifier (SWID) VCEVISIONTCOE03 was found for host 10.1.174.174
   Do you want to update the software identifier (SWID) for host 10.1.174.174 (yes/[no]):

5. To update the SWID, type **yes** at the prompt. A message similar to the following appears:

   Please enter the software identifier (SWID) for host 10.1.174.174:

6. Type the unique software identifier from the CLP file. A message similar to the following appears:

   Please enter your ESRS gateway hostname or IP address:

7. Type your ESRS gateway hostname or IP address. The following message appears:

   Please enter your NTID: <Your NTID>:

8. Type your Dell EMC network/Windows ID. The following message appears:

   Please wait for next token and enter your RSA PIN + Token:

9. Type your RSA pin and token. It takes a moment to authenticate, then a message similar to the following appears:

   ESRS configuration for 10.1.174.174 for the ESRS gateway 10.1.174.148 was successful.
   ESRS gateway configuration completed, exiting setup script.

**Deregistering Vision software with ESRS**

Use the Vision shell if you need to deregister a VCE System with Secure Remote Services (ESRS).
About this task

⚠️ CAUTION: When you perform this procedure, the `esrs_register delete` command removes an MSM VM instance from the ESRS gateway. It also removes the credential manager credential for the same MSM to authenticate with the ESRS gateway. If the MSM VM has already been removed from the ESRS gateway (such as through the ESRS gateway Web user interface), the command might fail and require manual cleanup of the MSM VM credential manager entry.

Procedure

1. Establish an SSH connection to the MSM VM and log on. The default credentials are:
   - Username: `root`
   - Password: `V1rtu@1c3!`

   **Remember:** The password should be changed to protect the system from unauthorized access.

2. Run the following command: `vshell`

   The Vision shell initializes with the following messages:

   ```
   VCE Vision shell 3.5.0.0
   Copyright 2013-2016 VCE Company, LLC. All rights reserved.
   VCE, VCE Vision, VCE Vsacle, Vblock, VxBlock, VxRail and the VCE logo are registered trademarks of VCE Company LLC.
   All other trademarks used herein are the property of their respective owners.
   MSM Hostname (Press Enter for localhost):
   ```

   Skip the login prompts by starting shell with the following option:

   ```
   vshell -l /opt/vce/shell/conf/ipython.conf
   ```

3. Enter the MSM hostname to which you want to connect or press Enter for the localhost.

4. When prompted, enter your username and password. The default administrative credentials for Vision shell are:
   - Username: `csadmin`
   - Password: `D@ngerous1`

   This password should be changed to protect the system from unauthorized access.

5. Run the following command: `esrs_register delete`

### Sending information to ESRS

You can send VCE System inventory and RCM compliance information to ESRS automatically at regularly scheduled intervals or on-demand through a manual upload.
By default, Vision software is set to automatically upload an inventory and compliance file one time per week on a randomly selected day. Use the Vision shell to view or modify this schedule at any time.

To view the current automatic upload schedule, refer to Viewing the current ESRS upload schedule (see page 176).

To modify the upload schedule, refer to Modifying the schedule used to send information to ESRS (see page 178).

To perform an on-demand upload to ESRS, refer to Manually uploading information to ESRS (see page 175).

**Manually uploading information to ESRS**

Perform this procedure to manually send VCE System inventory and Release Certification Matrix (RCM) compliance information to Secure Remote Services (ESRS).

**Before you begin**

Ensure the Vision software is registered with ESRS.

**Procedure**

1. Establish an SSH connection to the MSM VM and log on. The default credentials are:
   - Username: root
   - Password: V1rtu@1c3!

   This password should be changed to protect the system from unauthorized access.

2. Run the following command: vshell

   The Vision shell initializes with the following messages.

   VCE Vision shell 3.5.0.0

   Copyright 2013-2016 VCE Company, LLC. All rights reserved.
   VCE, VCE Vision, VCE Vscale, Vblock, VxBlock, VxRail and the VCE logo are registered trademarks or trademarks of VCE Company LLC.
   All other trademarks used herein are the property of their respective owners.

   MSM Hostname (Press Enter for localhost):

   ![](https://example.com/image.png)

   **NOTE:** As an alternative, you can skip the log on prompts by starting shell with the following option:

   vshell -l conf/ipython.conf

3. Enter the MSM hostname to which you want to connect, or press Enter for the localhost.
When prompted, enter your username and password. The default administrative credentials for Vision shell are:

- Username: **csadmin**
- Password: **D@ngerous1**

This password should be changed to protect the system from unauthorized access.

Run the following command:

```
esrs_devicemgmt target upload parameters
```

where:

- **target** is a python object, which can be a string, a variable, or a list of python objects. For example:
  - vcesystem: all VCE Systems in MSM
  - vb[0]: the first Vblock System by index number
  - vxblock: all VxBlock Systems in MSM
  - vblock: all Vblock Systems in MSM

- **parameters** is:
  - filename=filepath: Upload the file in the file path to ESRS
  - inventory: Upload inventory file to ESRS
  - compliance: Run a compliance scan and upload the results to ESRS
  - serviceticket=service ticket number: Include service ticket information in the uploaded file

For example, the following command specifies a file path to upload a single file:

```
esrs_devicemgmt vb[0] upload filename=/opt/vce/shell/test1.txt
```

A message similar to the following appears when a file is successfully uploaded:

```
file filepath is successfully uploaded with serial number serial number
```

**Viewing the current ESRS upload schedule**

Use this procedure to view the current schedule by which Vision software will automatically upload inventory and compliance information to ESRS. Vision software is set by default to automatically upload an inventory and compliance file one time per week on a randomly selected day.
Procedure

1. Establish an SSH connection to the MSM VM and log on. The default credentials are:
   - Username: root
   - Password: V1rtu@1c3!

   This password should be changed to protect the system from unauthorized access.

2. Run the following command: vshell

   The Vision shell initializes with the following messages.

   VCE Vision shell 3.5.0.0
   Copyright 2013-2016 VCE Company, LLC. All rights reserved.
   VCE, VCE Vision, VCE Vscale, Vblock, VxBlock, VxRail and the VCE logo are registered trademarks or trademarks of VCE Company LLC.
   All other trademarks used herein are the property of their respective owners.

   MSM Hostname (Press Enter for localhost):

   ☑ NOTE: As an alternative, you can skip the log on prompts by starting shell with the following option:

   vshell -l conf/ipython.conf

3. Enter the MSM hostname to which you want to connect, or press Enter for the localhost.

4. When prompted, enter your username and password. The default administrative credentials for Vision shell are:
   - Username: csadmin
   - Password: D@ngerous1

   This password should be changed to protect the system from unauthorized access.

5. Type either of the following commands to view the current schedule:
   - esrs_schedule get
   - esrs_schedule

   A message similar to the following appears:

   ESRS reporting schedule is set to run at 05:30 every Sunday
Modifying the schedule used to send information to ESRS

Use this procedure to modify the schedule by which Vision software automatically uploads inventory and compliance information to ESRS.

Procedure

1. Establish an SSH connection to the MSM VM and log on. The default credentials are:
   - Username: root
   - Password: V1rtu@1c3!

   This password should be changed to protect the system from unauthorized access.

2. Run the following command: vshell

   The Vision shell initializes with the following messages.

   VCE Vision shell 3.5.0.0
   Copyright 2013-2016 VCE Company, LLC. All rights reserved.
   VCE, VCE Vision, VCE Vscale, Vblock, VxBlock, VxRail and the VCE logo are registered trademarks or trademarks of VCE Company LLC.
   All other trademarks used herein are the property of their respective owners.

   MSM Hostname (Press Enter for localhost):

   ☞ NOTE: As an alternative, you can skip the log on prompts by starting shell with the following option:

   vshell -l conf/ipython.conf

3. Enter the MSM hostname to which you want to connect, or press Enter for the localhost.

4. When prompted, enter your username and password. The default administrative credentials for Vision shell are:
   - Username: csadmin
   - Password: D@ngerous1

   This password should be changed to protect the system from unauthorized access.

5. Run the following command: esrs_schedule set

   The following prompt appears:

   Current ESRS reporting schedule is set to run at 05:30 every day

   Schedule frequency (daily):
6 Type one of the following values to indicate the frequency with which you want Vision software to upload data to ESRS:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>daily</td>
<td>(Default). Set the upload frequency to occur every day.</td>
</tr>
<tr>
<td>weekly</td>
<td>Set the upload frequency to occur once a week. An additional prompt appears where you type a value to indicate the day of the week. You can type an integer between 1 and 7 or a value SUN-SAT or Sunday-Saturday (case insensitive).</td>
</tr>
<tr>
<td>monthly</td>
<td>Set the upload frequency to once a month. An additional prompt appears where you type a value between 1 and 31 to indicate the day of the month.</td>
</tr>
</tbody>
</table>

The following prompt appears:

Schedule hour of day:

7 Type a value between 0 and 23 to set the hour of day for the upload. The following prompt appears:

Schedule minute of hour:

8 Type a value between 0 and 59 to set the minute for the upload. A message similar to the following appears:

ESRS reporting schedule is set to run at 04:30 every Sunday

Securing the connection between Vision software and ESRS

Secure Remote Services (ESRS) provides a two-way remote connection between VCE Support and Vision software. There are steps you can take to make this connection more secure.

Change the default vision user password

VCE Support uses the vision user account to remotely connect to Vision software through ESRS. You are strongly advised to change the default password for this account. Refer to Changing the default password for the root and vision accounts (see page 83) for more information.

Restricting the remote connection

To prevent remote access into Vision software, you can configure the ESRS Policy Manager to deny incoming connections to Vision software. For information on how to do this, refer to the Secure Remote Services Installation and Operations Guide.

View Vision software login history

If a two-way remote connection occurs, you can view Vision software login history to determine who logged in (note that this is the CentOS Linux vision user account), the IP address from where the remote user logged in, and the timestamp of when the login occurred and when the session ended.
To view login history, use the `last` command. It displays information similar to the following:

```
[root@vision174-32 shell]$ last
root   pts/0  128.222.169.10  Thu Oct 13 14:18 still logged in
root   pts/0  10.252.59.231   Wed Oct 12 02:09 - 05:09 (03:00)
root   pts/0  10.252.59.231   Tue Oct 11 21:39 - 00:39 (03:00)
root   pts/0  128.222.169.10  Tue Oct 11 17:58 - 20:10 (02:11)
root   pts/0  10.97.68.160   Fri Oct  7 18:29 - 21:29 (03:00)
root   pts/0  10.97.68.160   Fri Oct  7 12:47 - 16:47 (04:00)
root   pts/1  10.97.68.160   Thu Oct  6 22:46 - 02:46 (04:00)
root   pts/0  10.97.68.160   Thu Oct  6 22:37 - 02:37 (04:00)
```

**Troubleshooting ESRS connectivity issues**

If you encounter issues related to ESRS connectivity, you need to know what to do to resolve the problem.

Below are some common potential issues related to ESRS connectivity and tips on how to troubleshoot these issues.

An ESRS shell extension causes the following exception: `Exception('ERROR: No ESRS configuration found on CVM Host X.X.X.X.')`

<table>
<thead>
<tr>
<th>Cause</th>
<th>This exception occurs if the ESRS extension is not currently configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution</td>
<td>Configure ESRS by running the following command:</td>
</tr>
<tr>
<td></td>
<td><code>/opt/vce/shell/bin/ESRSScript/esrs_setup.sh</code></td>
</tr>
</tbody>
</table>

When attempting to run the `esrs_setup.sh` script, the following error appears: `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 an ESRS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution</td>
<td>Use the correct address for your ESRS server.</td>
</tr>
</tbody>
</table>

When running an ESRS shell extension command, the following error appears: `urllib2.URLError(socket.error(111, 'Connection refused'))`

<table>
<thead>
<tr>
<th>Cause</th>
<th>The ESRS gateway is not currently running or it is unreachable.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution</td>
<td>Check the ESRS gateway status to verify whether it is running. Verify network connectivity to the ESRS gateway by pinging or using <code>traceroute</code> from the same VM on which Vision shell is running.</td>
</tr>
</tbody>
</table>

When running an ESRS shell extension command, the following error appears: `urllib2.URLError(socket.gaierror(-2, 'Name or service not known'))`

<table>
<thead>
<tr>
<th>Cause</th>
<th>The ESRS 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>
Managing software modules

The baseline security settings module is supported on a Vblock System and a VxBlock System only. Vision software is packaged into Vision software features and value-add software modules, such as the RCM Management module and the baseline security settings module.

**NOTE:** In the Vision dashboard and the Vision shell, the Vision Security Compliance Module is referred to as the baseline security settings module. The Vision RCM Compliance Module is referred to as the RCM Management module.

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The RCM Management module</td>
<td>The RCM Management module consists of RCM compliance and RCM content prepositioning.</td>
</tr>
<tr>
<td></td>
<td>• RCM compliance enables you to run a RCM compliance scan to determine if one or more VCE Systems and associated components are compliant with a Release Certification Matrix (RCM).</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This module is mandatory and is enabled as part of the installation process.</td>
</tr>
<tr>
<td></td>
<td>• RCM content prepositioning enables you to retrieve software and firmware for components in a VCE System to easily maintain compliance with the current Release Certification Matrix (RCM) and more efficiently upgrade to new RCM versions. RCM content prepositioning enables you to perform the following tasks:</td>
</tr>
<tr>
<td></td>
<td>— View RCM content downloaded to a VCE System.</td>
</tr>
<tr>
<td></td>
<td>— Discover RCM content available for download.</td>
</tr>
<tr>
<td></td>
<td>— Download RCM content.</td>
</tr>
<tr>
<td></td>
<td>— Monitor the status of RCM content downloads.</td>
</tr>
<tr>
<td></td>
<td>— Manage downloaded RCM content.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> RCM content prepositioning is supported only on Vblock Systems.</td>
</tr>
<tr>
<td>The baseline security settings module</td>
<td>The baseline security settings module consists of the baseline security settings content pack and the Vision Shell Security Hardening Remediation Extension Pack.</td>
</tr>
<tr>
<td></td>
<td>• The baseline security settings compliance content pack uses Dell EMC security hardening guidelines and enables you to run a compliance scan to identify risks that might exist on the VCE System.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If purchased, the module is enabled by default.</td>
</tr>
<tr>
<td></td>
<td>• The Shell Security Hardening Remediation Extension Pack consists of a set of Vision shell extensions that enable you to remediate certain VCE System component configurations in order to bring the VCE System in compliance with Dell EMC Security best practices.</td>
</tr>
</tbody>
</table>
Roles and operations for the Software Module Manager

Vision software provides role-based access control (RBAC) to the Software Module Manager. You can assign roles to user groups to control which operations users can perform.

<table>
<thead>
<tr>
<th>Role</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Module Manager Administrator</td>
<td>Administrator with read, write, and manage access to the Software Module Manager</td>
</tr>
<tr>
<td>Software Module Manager User</td>
<td>User with read-only access to the Software Module Manager</td>
</tr>
</tbody>
</table>

Related information

Mapping roles to Active Directory groups (see page 105)

Managing software modules using the Vision dashboard

Vision software provides a Vision dashboard that can be used to manage modules. To work with the Software Modules user interface, you must be an authenticated and authorized Vision software user.

To manage modules, for example, enable or disable modules, log on to the dashboard. From the toolbar, click the menu icon (≡) and navigate to Manage > Software Modules.

The available modules are enabled.

Managing software modules using the Vision shell

The Vision shell uses a set structure of commands that allows you to manage Software Modules.

Note: The Vision shell is supported on a Vblock System and a VxBlock System only.

To manage modules, for example, enable or disable modules, log on to the Vision shell.

Use the following structure to manage modules in the Vision shell:

```
software_modules verb entity -parameter
```

Where:

- `software_modules` is the root noun for Software Module Manager.
- `verb` specifies an operation to perform.
- `entity` is an entity on which you perform an operation.
- `parameter` is one or more parameters.
Related information

**Accessing the Vision shell session** (see page 61)

## Vision shell commands

Use the following Vision shell commands to perform operations on modules.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Command format</th>
</tr>
</thead>
<tbody>
<tr>
<td>List modules</td>
<td>Lists the module name or module identifier for all modules.</td>
<td><code>software_modules list modules</code></td>
</tr>
<tr>
<td>List module states</td>
<td>Lists if modules are in an enabled or disabled state.</td>
<td><code>software_modules list states</code></td>
</tr>
<tr>
<td>Enable a module</td>
<td>Enables a module.</td>
<td><code>software_modules enable &quot;[module name]&quot; or [module id]&quot;</code></td>
</tr>
<tr>
<td>Enable the baseline security settings module</td>
<td>Enables the baseline security settings module.</td>
<td><code>software_modules enable &quot;baseline security settings Module&quot;</code></td>
</tr>
<tr>
<td>Disable a module</td>
<td>Disables a module.</td>
<td><code>software_modules disable &quot;[module name]&quot; or [module id]&quot;</code></td>
</tr>
<tr>
<td>Disable the baseline security settings module</td>
<td>Disables the baseline security settings module.</td>
<td><code>software_modules disable &quot;baseline security settings Module&quot;</code></td>
</tr>
<tr>
<td>List events types</td>
<td>Lists when modules were created, updated and or deleted.</td>
<td><code>software_modules list events</code></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The Event Date specifies the corresponding date when the Event Type was initiated.</td>
<td></td>
</tr>
<tr>
<td>List the baseline security settings module events</td>
<td>Lists when the baseline security settings module was created, updated, or deleted.</td>
<td><code>software_modules list events &quot;baseline security settings Module&quot;</code></td>
</tr>
</tbody>
</table>
Log files for the Software Module Manager

Vision software writes messages to log files that can assist with troubleshooting and root cause analysis with the Software Module Manager.

Software Module Manager logs

Locate log files for the Software Module Manager in the following directory:

/opt/vce/subscription-manager/deploy/logs

The following table lists the available log file:

<table>
<thead>
<tr>
<th>Log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>subscription-manager.log</td>
<td>The main log file for the Software Module Manager service.</td>
</tr>
</tbody>
</table>

Configuring audit log properties

You can configure the default audit log properties which the Software Module Manager service uses for its audit logging.

About this task

To configure the default audit log properties, set the values for the following properties in `audit-log.properties`:

<table>
<thead>
<tr>
<th>Property name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vce.subscription.audit.log.level=INFO</td>
<td>The logging level. It can be one of TRACE, INFO, WARN, ERROR, FATAL.</td>
</tr>
<tr>
<td>vce.subscription.audit.log.filename=/var/log/subscriptions.log</td>
<td>The absolute path for the location of the logging file.</td>
</tr>
<tr>
<td>vce.subscription.audit.log.maxbytes=100MB</td>
<td>The maximum size for the log file before rolling over to a new file.</td>
</tr>
<tr>
<td>vce.subscription.audit.log.maxbackupindex=10</td>
<td>The maximum number of log files that are stored. Older files are deleted automatically when exceeding this number.</td>
</tr>
<tr>
<td>vce.subscription.audit.log.additivity=false</td>
<td>Set to true if there is a requirement to replicate these logs into the service logging.</td>
</tr>
</tbody>
</table>

Before you begin

- Connect to the Vision Core VM.
- Back up /opt/vce/subscription-manager/conf/audit-log.properties.
Procedure

1. Open `/opt/vce/subscription-manager/conf/audit-log.properties`.
2. Update the property values as appropriate.
3. Save and close the `audit-log.properties`.

Software Module Manager message identifiers

Vision software includes unique identifiers for each message that it writes to a log file. These identifiers help you easily understand the severity level of the message and isolate issues.

Message identifiers have the following format:

```
[Product][Component][Message Code][Level]
```

For example, `VSMM4509E`

Where:

<table>
<thead>
<tr>
<th>Product</th>
<th>Component</th>
<th>Message Code</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>V</td>
<td>SMM relates to</td>
<td>4 digits</td>
<td>⚠️ for Fatal</td>
</tr>
<tr>
<td></td>
<td>Software Module</td>
<td>with format</td>
<td>⚠️ for Error</td>
</tr>
<tr>
<td></td>
<td>Manager</td>
<td>NNNN</td>
<td>⚠️ for Warning</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>🚹 for Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>🚹 for trace</td>
</tr>
</tbody>
</table>

Collecting logs

You can collect component logs for troubleshooting purposes using the Vision dashboard and the REST API.

Devices for log collection

The following devices are supported for log collection:

- Compute system
- Compute chassis
- Switch
- VIManager
- OS
• Storage array

**NOTE:** Log collection is not supported on a VMAX storage array.

• Storage processor

• Control Station Enclosure

**NOTE:** Not every component for each device is supported for log collection. For example, log collection is not supported on any component that is configured on AMP-2P, AMP-2RP, AMP-2HA, AMP-2LP, AMP-2S, or AMP-3S.

### Using the Vision dashboard

You can select components to collect logs on the Vision dashboard.

If logs can be collected for a component in the search results, **Download Log Files** is shown in the Actions list.

Click **Download Log Files** and select which components you need log files for. When the process is complete, select the Success task in the notifications to download the ZIP file.

Log files are automatically archived after one week and can no longer be downloaded.
Using the REST API

The API for Tech Support provides a set of RESTful resources for component log collection that allow you to:

- Find VCE System components that support log collection
- Trigger log collection
- Monitor log collection tasks
- Download the log bundle

The log bundles are produced as ZIP files.

**NOTE:** Collecting logs using the REST API is supported on a Vblock System and a VxBlock System only.

Refer to the *Dell EMC Vision Intelligent Operations Programmer’s Guide* for more information.
Backing up and restoring

For instructions on redeploying the Vision Core VM, the MSM VM, or the MSP VM, refer to the Dell EMC Vision Intelligent Operations Installation Guide.

Backing up and restoring the Vision Core VM

Vision Core software backups

Vision Core software backs up configuration and environment data so that you can restore the Vision Core VM to a working state, if required. This topic describes the files and data that Vision Core software backs up and the format and location of backup files.

Vision Core software backs up the following:

- System Library configuration files in the `/opt/vce/fm/conf` directory in addition to the following:
  - `/etc/snmp/snmpd.conf`
  - `/etc/logrotate.d/syslog`
  - `/etc/srconf/agt/snmpd.cnf`
- JBoss configuration files, including keystore files
- System Library administrative, configuration, and model database schemas and data files
- PostgreSQL database schema and data

During the manufacturing process, Dell EMC creates backups on the Vision Core VM so that they are available when the VCE System is delivered to your site. After the VCE System is up and running at your site, Vision software automatically runs backup tasks according to the default schedules.

Backup file format and location

Vision Core software creates backups in `tar.gz` file format on the Vision Core VM, as follows:

- System Library 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, Vision Core software stores:

- A maximum of seven System Library and JBoss configuration backups.
- PostgreSQL database backups for the current day and the previous two days. The following example describes how Vision software stores PostgreSQL database backup files:
  - At 11:59 PM on Tuesday, Vision Core software stores backup files for Tuesday, Monday, and Sunday.
At 12:00 AM on Wednesday, Vision Core software stores backup files for Wednesday, Tuesday, and Monday. Vision Core software deletes the backup files for Sunday.

**Default backup schedule**

By default, backup tasks occur:

- Daily at 12:00 AM for the Vision Core software configuration files.
- Every 10 minutes for the PostgreSQL database schema and data.

You can change the schedule and frequency of the backup tasks. Likewise, you can run backups on demand outside of the scheduled tasks.

**Changing the backup schedule and frequency**

Vision software 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 Vision Core VM.

**Procedure**

1. Run the following command to view the current cron tasks:

   ```bash
crontab -l
   ```

   The following cron tasks display, as in the following example:

   ```
   # HEADER: This file was autogenerated at <time_stamp> by puppet.
   # HEADER: While it can still be managed manually, it is definitely not recommended.
   # HEADER: Note particularly that the comments starting with 'Puppet Name' should
   # HEADER: not be deleted, as doing so could cause duplicate cron jobs.
   00 00 * * * /opt/vce/fm/install/backupConfig.sh > /dev/null 2>&1
   30 1,13 * * * /opt/vce/fm/bin/collectConfig.sh > /dev/null 2>&1
   # Puppet Name: vce-puppet
   */1 * * * * /usr/bin/puppet apply $(puppet config print manifest) > /dev/null 2>&1
   */10 * * * * /opt/vce/fm/install/backupDatabase.sh > /dev/null 2>&1
   ```

2. Run the following command to change a cron task:

   ```bash
crontab -e
   ```

   The default editor is vi.
3 Make the required changes to the cron tasks and then save the file.

Ensure that you do not edit or remove the Puppet apply line:

```
# Puppet Name: vce-puppet
*/1 * * * * /usr/bin/puppet apply $(puppet config print manifest) > /dev/null 2>&1
```

What to do next

Run the following command to review and verify the cron tasks:

```
crontab -l
```

Vision software backup cron tasks

Vision software uses cron tasks to run scripts at set intervals to back up configuration files.

Vision software 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 Vision software configuration files.</td>
</tr>
<tr>
<td>collectConfig.sh</td>
<td>Backs up VCE 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 between 0-59 for the corresponding minute of the hour or * for every minute.</td>
</tr>
<tr>
<td>Hour of the day</td>
<td>A number between 0-23 for the corresponding hour of the day or * for every hour.</td>
</tr>
<tr>
<td>Day of the month</td>
<td>A number between 1-31 for the corresponding day of the month or * for every day.</td>
</tr>
<tr>
<td>Month of the year</td>
<td>A number between 1-12 for the corresponding month of the year or * for every month. You can also use the name of the month.</td>
</tr>
<tr>
<td>Day of the week</td>
<td>A number between 0-7 for the corresponding day of the week. Sunday is 0 or 7. You can also use the name of the day.</td>
</tr>
<tr>
<td>Path to the script</td>
<td>The path to the script.</td>
</tr>
</tbody>
</table>

Backing up configuration files on demand

You can back up configuration files for Vision software outside of the automatically scheduled backup task.

Before you begin

Connect to the Vision Core VM.
Procedure

1. Run the following command:
   ```
   cd /opt/vce/fm/install
   ```

2. Run the following command with the appropriate parameters:
   ```
   sh backupConfig.sh
   ```
   To view help usage, run:
   ```
   sh backupConfig.sh -h
   ```

Results

The script runs the backup task, as in the following example:

```
initialize /opt/vce/fm/backup/snapshots/time_stamp/backup...

backup slib configurations: /opt/vce/fm/backup/snapshots/time_stamp/backup...

_backup jboss configuration
backup Jboss /opt/vce/fm/backup/snapshots/time_stamp/backup...
backup Jboss /opt/vce/fm/backup/snapshots/time_stamp/backup done

Backup FMAgent
backup FMAgent /opt/vce/fm/backup/snapshots/time_stamp/backup...

Exported following FMagent config files
/export/vce/fm/conf/log4j_slib_sec.xml
/export/vce/fm/conf/configcollector.xml
/export/vce/fm/conf/vblock-simulator.xml
... done with /opt/vce/fm/backup/snapshots/time_stamp/backup
for details, check log file: /opt/vce/fm/backup/snapshots/time_stamp/backup.log
```

The script creates backup files in the following directory: `/opt/vce/fm/backup/snapshots`.

Vision software names backup files `backup.tar.gz` and organizes each backup file into a sub-directory with a time stamp. The sub-directory contains the backup file in addition to a log file and MD5 hash for the backup file.

What to do next

Change to the backup directory and verify the backup files are successfully created.
Backing up databases on demand

You can back up the PostgreSQL database schema and data outside of the automatically scheduled backup task.

Before you begin

Connect to the Vision Core VM.

Procedure

1. Run the following command:
   ```
   cd /opt/vce/fm/install
   ```

2. Run the following command:
   ```
   sh ./backupDatabase.sh
   ```

Results

The script runs the backup task, as in the following example:

```
Making backup directory in /opt/vce/fm/backup/postgres/backup-YYYY-MM-DD/
Performing schema and data backups
--------------------------------------------
The following databases were matched for schema and data backup:
compliance
model
Schema and data backup of model
```

The script creates backup files in the following directory: `/opt/vce/fm/backup/postgres/`

Backup files have the following name format:

```
time_stamp_database_name_DB.sql.tar.gz
```

Where:

- `time_stamp` has the following format: `YYYY-MM-DD_HH:MM:SS`
- `database_name` is the name of the database that the script backs up.

An example backup file name is as follows: `1856-07-10_15:01:02_model_DB.sql.tar.gz`.

What to do next

Change to the backup directory and verify the backup files are successfully created.

Restoring the Vision software configuration

You can restore the Vision software configuration from a backup file.
About this task
Restoring the Vision software configuration overwrites the current configuration. To ensure you can recover your settings, you should back up the current configuration before proceeding.

Before you begin

- Back up your current configuration files.
- Connect to the Vision Core VM.

Procedure

1. Run the following command:

   ```bash
cd /opt/vce/fm/install
   ```

2. Run the following command with the appropriate parameters:

   ```bash
sh restoreConfig.sh
   ```

   To view help usage, run:

   ```bash
sh restoreConfig.sh -h
   ```

   The script prompts you to confirm the restoration, as in the following example:

   ```
   --------------------------------------------
   | WARNING!!
   | This restoration will shut down Jboss and FMAgent applications
   | and overwrite current configurations
   --------------------------------------------
   Do you really want to restore /opt/vce/fm/backup/snapshots/time_stamp/backup.tar.gz?
   1) Yes
   2) No
   #?
   ```

3. Do one of the following:

   - Enter 1 to continue restoring the Vision software configuration.
   - Enter 2 to quit.

Results
Vision software restores configuration files from the back up.

What to do next
Check the following log file to ensure the restoration was successful: `opt/vce/fm/backup/restore_logs/restore_file_name.log`
Restoring databases

You can 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 Vision 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.
   
   Vision software stores database backups as tar.gz files in directories with the following format: YYYY-DD-MM.
3. Run the following command to extract the tar.gz file:

   ```
   tar -zxvf ./file_name -C /tmp
   ```
4. Confirm that the file is extracted.
   - Change to the /tmp directory.
   - Run the following command:

     ```
     ls -l
     ```

     The backed up SQL file displays in the terminal window as follows:

     ```
     database_name_DB.sql
     ```
5. Run the following command to switch to the Postgres user:

   ```
   sudo su - postgres
   ```
6. Drop all schema in the database to which you are restoring. Before you restore the database, you must 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 Vision software backs up:

<table>
<thead>
<tr>
<th>Database name</th>
<th>Schema</th>
</tr>
</thead>
<tbody>
<tr>
<td>model</td>
<td>- admin</td>
</tr>
<tr>
<td></td>
<td>- model</td>
</tr>
<tr>
<td></td>
<td>- rbac</td>
</tr>
</tbody>
</table>

   - Log on to the database: `psql database_name`
   - List all schema in the database: `select schema_name from information_schema.schemata where schema_owner='admin';`
c  Drop the schema: `drop schema if exists schema_name cascade;`

d  Confirm the drop was successful: `select schema_name from information_schema.schemata where schema_owner='admin';`

e  Exit: `\q`

7  Run the following command to restore the database:

```bash
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.

The following is an example of the restore command:

```bash
psql -d model -U postgres -f /tmp/model_DB.sql
```

**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, refer to the appropriate PostgreSQL documentation.

What to do next

Repeat the preceding steps for each backed up SQL file you want to restore.

**Backing up the Vision Core VM**

To maintain a low recovery time objective (RTO), it is critical that you back up the Vision software at the VM level. If you do not back up the Vision Core VM, you can experience slow recovery and limited visibility into the management plane of your VCE System.

**Procedure**

1. Perform daily backups of the Vision 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.

**Backing up and restoring the MSM VM**

To back up the MSM VM, perform an agent-less VM backup using whatever backup software you currently use.
Backing up and restoring the MSP VM

To back up the MSP VM, perform an agent-less VM backup using whatever backup software you currently use.

Backing up component configuration files

**NOTE:** Backing up component configuration files is supported on a Vblock System and a VxBlock System only.

How VCE System backups work

Every VCE System is deployed with backups of the VCE System component configuration files. To ensure you can recover from the loss of a single component or an entire VCE System, you should back up VCE System configuration files on a daily basis. To facilitate this process, Vision software includes the VCE System Configuration Collector that automatically gathers every configuration file in a VCE System component.

The VCE System Configuration Collector automatically collects and stores configuration files on the Vision Core VM so that you only need to do the following for disaster recovery:

- Save VCE System configuration files to a remote system.
- Back up the VMware vCenter SQL server.

Each VCE System is deployed with configuration backups for each component, as follows:

<table>
<thead>
<tr>
<th>VCE System</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vblock System 100</td>
<td>Cisco Catalyst 3750-X Switch</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 3064-T Switch</td>
</tr>
<tr>
<td></td>
<td>Vblock compute servers (CIMC)</td>
</tr>
<tr>
<td></td>
<td>Management servers (CIMC)</td>
</tr>
<tr>
<td>Vblock System 200 series</td>
<td>Cisco Nexus 5000 Switch</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 1000V Switch</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 3000</td>
</tr>
<tr>
<td></td>
<td>Cisco C-Series server(s)</td>
</tr>
<tr>
<td></td>
<td>VNX</td>
</tr>
<tr>
<td></td>
<td>Vblock compute servers (CIMC)</td>
</tr>
<tr>
<td></td>
<td>Management servers (CIMC)</td>
</tr>
<tr>
<td>VCE System</td>
<td>Component</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vblock System 300 series</td>
<td>Cisco MDS 9000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 5000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 1000V</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 3000</td>
</tr>
<tr>
<td></td>
<td>Cisco UCS fabric interconnects (UCS Manager)</td>
</tr>
<tr>
<td></td>
<td>VNX</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 340</td>
<td>Cisco MDS 9000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 5000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 1000V</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 3000</td>
</tr>
<tr>
<td></td>
<td>Cisco UCS fabric interconnects (UCS Manager)</td>
</tr>
<tr>
<td></td>
<td>VNX</td>
</tr>
<tr>
<td></td>
<td>Management servers (CIMC)</td>
</tr>
<tr>
<td></td>
<td>Technology Extension for Storage</td>
</tr>
<tr>
<td>VxBlock System 350</td>
<td>Cisco MDS 9000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 5000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 1000V</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 3000</td>
</tr>
<tr>
<td></td>
<td>Cisco UCS fabric interconnects (UCS Manager)</td>
</tr>
<tr>
<td></td>
<td>Management servers (CIMC)</td>
</tr>
<tr>
<td></td>
<td>Technology Extension for Storage</td>
</tr>
<tr>
<td></td>
<td>Converged Technology Extension for Cisco UCS compute</td>
</tr>
<tr>
<td>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>VCE System</td>
<td>Component</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</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>VMAX</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>VMAX</td>
</tr>
<tr>
<td></td>
<td>Management servers (CIMC)</td>
</tr>
<tr>
<td></td>
<td>Technology Extension for Storage</td>
</tr>
<tr>
<td>Vblock Specialized Systems for Extreme Applications</td>
<td>Cisco UCS fabric interconnects (UCS Manager)</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 3000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 5000</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 1000V</td>
</tr>
<tr>
<td></td>
<td>XtremIO</td>
</tr>
<tr>
<td></td>
<td>Management servers (CIMC)</td>
</tr>
</tbody>
</table>

**Configuration files you must manually back up**

Due to component limitations or known issues, the Vblock System Configuration Collector does not back up configuration files for:

- Dell EMC Unity storage array on VCE Systems
• VNXe storage array on a Vblock System 100

Refer to the Backing up the VNXe configuration topic in the Vblock System 100 Administration Guide.

• Cisco Nexus OS switches

Refer to the Backing up Cisco Nexus OS switches topic in the Administration Guide that is relevant to your Vblock System.

• VMware vCenter Server

Refer to the Backing up the VMware vCenter SQL server database section of the Administration Guide that is relevant to your Vblock System.

Backup schedule, location, and retention period

By default, the Vblock System Configuration Collector 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

Vision software retains backed up configuration files for seven days by default. However, you can configure the retention period within a range of 3 to 30 days. Use the collectConfig.sh script in the /opt/vce/fm/bin directory on the Vision Core VM to run the Vblock System Configuration Collector and specify the retention period. To view help usage, run sh collectConfig.sh -h.

Saving VCE System configuration files

Use the following Vision software REST resource to export an archive of the VCE System configuration files: https://FQDN:8443/fm/configcollector

Where FQDN is the fully qualified domain name of the Vision Core VM.

This REST resource exports an archive of all configuration files under the /opt/vce/backup directory.
System requirements

The system requirements specify the minimum support required for the Vision Core VM, the multisystem management (MSM) VM, and the multisystem prepositioning (MSP) VM.

<table>
<thead>
<tr>
<th>VM</th>
<th>Memory requirement (GB)</th>
<th>vCPUs</th>
<th>Disk size (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vision Core VM</td>
<td>8</td>
<td>2</td>
<td>200</td>
</tr>
<tr>
<td>MSM VM</td>
<td>12</td>
<td>4</td>
<td>250</td>
</tr>
<tr>
<td>MSP VM</td>
<td>1</td>
<td>2</td>
<td>250</td>
</tr>
</tbody>
</table>

The Vision Core VM, MSM VM, and MSP VMs can be installed on the following Advanced Management Platforms (AMP) and storage types:

- Logical AMP - Vblock System storage array
- HA-AMP version 1 - VNXe3100
- HA-AMP version 2 - VNXe3150
- AMP-2V - Vblock System storage array
- AMP-2P - C-Series local storage
- AMP-2RP - C-Series local storage
- AMP-2HA - VNXe3200
- AMP-2LP - C-Series local storage
- AMP-2S - VNXe storage

**NOTE:** Use the attended configuration tool to configure AMP-2S on the Vblock System 240. Use the unattended configuration tool to configure AMP-2S on the following systems:

- VxBlock System 240
- VxBlock and Vblock Systems 350
- VxBlock and Vblock Systems 540
- VxBlock and Vblock Systems 740

- AMP-3S - Unity 300 or Unity 350
- AMP-VX
- VxRack Controller - Management servers local storage
You must consider the following when deploying the Vision Core VM, MSM VM, and MSP VMs:

- When deploying on AMP, the RAM size must be greater than or equal to 128 GB. If the RAM is less than 128 GB, the AMP must be upgraded to a minimum of 128 GB of RAM. Contact VCE Support for assistance when upgrading the AMP: https://support.vce.com/

- It is recommended to use NFS mount from the storage array for the MSP VM, where available.

- For AMP, VNXe3100 and VNXe3150 leverage the local storage capacity. Storage can be added and is documented by Cisco but this might add downtime.

Depending on the VCE System, the Vision Core, MSM, and MSP VMs can be installed on either a logical or physical AMP as described in the following table:

<table>
<thead>
<tr>
<th>VCE System</th>
<th>Logical AMP</th>
<th>Physical AMP</th>
<th>AMP-VX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vblock System 100</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Vblock System 200</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Vblock System 240</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>VxBlock System 240</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Vblock System 300 series</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>VxBlock System 340</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>VxBlock System 350</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Vblock System 540</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>VxBlock System 540</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Vblock System 700 series</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>VxBlock System 740</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>VxBlock System 1000</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VxRack FLEX</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Ports and protocols**

Review ports and protocols for communicating with Vision software.

Communication with Vision software occurs through northbound traffic over an external network and through southbound traffic to VCE System components.

Review the ports and protocols to help troubleshoot issues after installation.

**Open port assignments**
The MSM VM runs a number of 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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Linux Application</th>
<th>Usage</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>SSH</td>
<td>Secure shell (SSH)</td>
<td>Vision software</td>
</tr>
<tr>
<td>80</td>
<td>UDP</td>
<td>Apache HTTP</td>
<td>Web server providing access to the Vision dashboard and all Vision REST APIs. Requests are redirected to Port 443</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Apache HTTP</td>
<td>HTTPS access to the dashboard and all Vision REST APIs</td>
<td></td>
</tr>
<tr>
<td>5672</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>Message service used by Vision software</td>
<td></td>
</tr>
<tr>
<td>7000</td>
<td>TCP</td>
<td>SSL</td>
<td>Cassandra SSL inter-node communication</td>
<td></td>
</tr>
<tr>
<td>9042</td>
<td>TCP, UDP</td>
<td>Cassandra</td>
<td>Cassandra native client port</td>
<td></td>
</tr>
<tr>
<td>9160</td>
<td>TCP</td>
<td>Cassandra</td>
<td>Cassandra thrift client port</td>
<td></td>
</tr>
<tr>
<td>9301</td>
<td>TCP</td>
<td>Elasticsearch</td>
<td>Elasticsearch node-to-node communication</td>
<td></td>
</tr>
</tbody>
</table>

If the port 9301 is not open:

1. In the command line interface, type `vi /etc/sysconfig/iptables`.
2. Add the following line:

   ```bash
   -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 Vision software.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Usage</th>
<th>Source</th>
<th>Destination</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>HTTP</td>
<td>Vision software</td>
<td>RCM content distribution network (CDN) destination addresses that include the following: *.flexnetoperations.com, updates.flexnetoperations.com, vce.flexnetoperations.com, vceesd-ie.flexnetoperations.com</td>
<td>Outbound</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
<td></td>
<td></td>
<td>Outbound</td>
</tr>
<tr>
<td>22</td>
<td>TCP</td>
<td>Secure shell (SSH)</td>
<td></td>
<td>Any IP address</td>
<td>Inbound</td>
</tr>
<tr>
<td>8443</td>
<td>TCP</td>
<td>• API for System Library • API for Vision Security</td>
<td></td>
<td>Any client or application that uses these APIs.</td>
<td>Inbound</td>
</tr>
<tr>
<td>18443</td>
<td>TCP</td>
<td>Inventory Manager</td>
<td></td>
<td>Any client or application that uses this feature.</td>
<td>Inbound</td>
</tr>
<tr>
<td>4369</td>
<td>TCP</td>
<td>AMQP messaging</td>
<td></td>
<td>Any application that subscribes to the Vision software messaging service.</td>
<td>Outbound</td>
</tr>
<tr>
<td>5672</td>
<td>TCP</td>
<td>AMQP messaging</td>
<td></td>
<td>Any application that subscribes to the Vision software messaging service</td>
<td>Inbound</td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>General SNMP messages</td>
<td></td>
<td>SNMP client or NMS</td>
<td>Inbound</td>
</tr>
<tr>
<td>Default Port 162</td>
<td>UDP</td>
<td>SNMP trap messages</td>
<td></td>
<td>SNMP client or NMS</td>
<td>Inbound</td>
</tr>
</tbody>
</table>

**Note:** Refer to the *Dell EMC Vision Intelligent Operations Integration Guide for SNMP* for instructions on configuring Port 162 for SNMP trap messages.
## Southbound ports and protocols

Vision software uses specific ports and protocols for southbound communication with VCE System components.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Usage</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>69</td>
<td>UDP</td>
<td>TFTP traffic from the Configuration Collector to back up VCE System component configuration</td>
<td>VCE System components</td>
<td>Vision software</td>
</tr>
<tr>
<td>162</td>
<td>UDP</td>
<td>SNMP trap messages</td>
<td></td>
<td></td>
</tr>
<tr>
<td>514</td>
<td>UDP</td>
<td>syslog messages</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Compute components

Review the ports and protocols that Vision software uses for communication with compute components.

#### Dell iDRAC

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Usage</th>
<th>Source</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>Vision software</td>
<td>iDRAC</td>
</tr>
</tbody>
</table>

### Network components

Review the ports and protocols that Vision software uses for communication with network switches, including physical and virtual switches.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Usage</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>Secure shell (SSH)</td>
<td>Vision software</td>
<td>Network switches</td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>General SNMP messages</td>
<td>Vision software</td>
<td></td>
</tr>
</tbody>
</table>

### Storage components

Review the ports and protocols that Vision software uses for communication with various storage components.

#### ScaleIO

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Usage</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>REST API</td>
<td>Vision software</td>
<td>ScaleIO</td>
</tr>
</tbody>
</table>
Management components

Vision software communicates with management components using certain ports and protocols.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Usage</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>161</td>
<td>TCP</td>
<td>SNMP</td>
<td>Vision software</td>
<td>IPI appliance</td>
</tr>
</tbody>
</table>

Virtualization components

Review the ports and protocols that Vision software uses for communication with virtualization components.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Usage</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>XML API</td>
<td>Vision software</td>
<td>VMware vCenter Server</td>
</tr>
</tbody>
</table>

**Configuring the NTP server**

Use this procedure to configure each MSM VM and Vision Core VM to use an NTP server.

**NOTE:** If you are redeploying an MSM VM, specify an NTP server IP address when configuring the server.

Before you begin

Determine the NTP server to be used for the data center. Use the VLAN gateway or the gateway of the VCE System.

Procedure

For each MSM VM and Vision Core VM, perform the following steps:

1. SSH to the VM as the root user.
2. Type the following command to verify that the NTP server is accessible:

   ```bash
   ntpdate -u <IP_address>
   ```

   where `IP_address` is the NTP server IP address.

   Result:

   ```
   9 Sep 15:13:59 ntpdate[30770]: adjust time server IP_address offset 0.000154 sec
   ```

3. Edit the `/etc/ntp.conf` file.
4 Comment out the default CentOS server entries and add the following entry: `server IP_address`, where `IP_address` is the NTP server IP address.

**NOTE:** 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.

```
#server 0.centos.pool.ntp.org iburst
#server 1.centos.pool.ntp.org iburst
#server 2.centos.pool.ntp.org iburst
#server 3.centos.pool.ntp.org iburst
server IP_address
```

5 Save the changes and run the following command to start the ntpd service:

```
service ntpd restart
```

6 Type the following command for the ntpd service to start on reboot:

```
chkconfig ntpd on
```

### Verifying the Elasticsearch configuration

After deploying the OVA for MSM, you need to verify that Elasticsearch is properly installed and configured. Elasticsearch is a distributed search server that provides a full-text search engine that is included with MSM.

**About this task**

You may need to verify the Elasticsearch configuration again if you modify the MSM environment by including additional virtual machines in the cluster. The Elasticsearch configuration file (`elasticsearch.yml`) is configured automatically during OVA deployment. You should not need to make any changes to the configuration. 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 host name 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 listed above.

```yaml
...

# Cluster name identifies your cluster for auto-discovery. If you're running multiple clusters on the same network, make sure you're using unique names.
# cluster.name: florencecluster

# Node names are generated dynamically on startup, so you're relieved from configuring them manually. You can tie this node to a specific name:
# node.name: techpubdeploy24

# Unicast discovery allows to explicitly control which nodes will be used to discover the cluster. It can be used when multicast is not present, or to restrict the cluster communication-wise.
#
# 1. Disable multicast discovery (enabled by default):
#    discovery.zen.ping.multicast.enabled: false
# 2. Configure an initial list of master nodes in the cluster to perform discovery when new nodes (master or data) are started:
#    discovery.zen.ping.unicast.hosts: ["host1", "host2:port"]

...
```

2. If necessary, run the following command to restart the Elasticsearch service:

```bash
sudo service elasticsearch restart
```
The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2018 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA in August 2018.

Dell EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.