

Dell EMC VxBlock™ Central Version 3.0

Upgrade Guide

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Chapter 1: Revision history	5
Chapter 2: Introduction	6
Chapter 3: VxBlock Central upgrade overview	7
Pre upgrade tasks.....	7
Verify system requirements.....	7
Upgrade verification tasks.....	8
Supported upgrade paths.....	9
Download VxBlock Central upgrade files.....	10
Collect the custom display names.....	10
Take a snapshot of VMs.....	10
Take a snapshot of VMs in the cluster.....	10
Configure the VMs to use the NTP server.....	11
Upgrade a single MSM VM using the simplified upgrade	11
Upgrade a single site cluster with a single MSM VM.....	13
Start a Core VM upgrade.....	13
Verify a Core VM upgrade.....	14
Start an MSM VM upgrade.....	14
Update the MSM credential manager service.....	15
Verify the MSM VM upgrade.....	15
Verify the MSM VM configuration file.....	16
Start the MSP VM upgrade.....	16
Verify the MSP VM upgrade.....	16
Upgrade a single-site cluster containing multiple MSM VMs.....	17
Start a Core VM upgrade.....	18
Verify a Core VM upgrade.....	19
Start the MSP VM upgrade.....	19
Verify the MSP VM upgrade.....	20
Identify the MSM VM acting as the Cassandra seed node.....	20
Start an MSM VM upgrade.....	20
Update the MSM credential manager service.....	21
Verify the MSM VM upgrade.....	21
Upgrade a multisite cluster.....	22
Start a Core VM upgrade.....	23
Verify a Core VM upgrade.....	24
Start the MSP VM upgrade.....	24
Verify the MSP VM upgrade.....	24
Identify the MSM VM acting as the Cassandra seed node.....	25
Start an MSM VM upgrade.....	25
Update the MSM credential manager service.....	26
Verify the MSM VM upgrade.....	26
Post upgrade tasks.....	27
Retype the custom display names.....	27

Remove a VM snapshot.....	27
Upload compliance content.....	27
Perform post configuration steps.....	27
Chapter 4: Upgrade VxBlock Central Orchestration Services.....	29
Chapter 5: Upgrade the VxBlock Central Operations Management Pack.....	31
Chapter 6: Install the VxBlock Central 3.0 hotfix.....	32
Take a snapshot of VxBlock Central Core VM.....	32
Install the VxBlock Central 3.0 hotfix	32
Chapter 7: Troubleshoot the VxBlock Central upgrade.....	34
Review log files	34
Recover the MSM cluster.....	34
Services do not start after Core VM upgrade.....	35

Revision history

Date	Document revision	Description of changes
May 2020	1.2	Document updated with: <ul style="list-style-type: none">• Description of the issue (ESTCISW-12221) resolved by the VxBlock Central 3.0 hotfix.• Steps on how to revert to the default CPU count when installing the hotfix.
April 2020	1.1	Document updated with the: <ul style="list-style-type: none">• Installation procedure for the VxBlock Central 3.0 hotfix.• Server requirement for VxBlock Central Workflow Automation in the <i>Verify system requirements</i> topic.
March 2020	1.0	Release of VxBlock Central 3.0.

Introduction

This document provides instructions to upgrade from VxBlock Central 1.0 or later, to version VxBlock Central 3.0.

The target audience for this document includes customers, internal teams working with customers, and professional services.

For a single-site environment, use the *VxBlock Central simplified upgrade*. For a multisite environment, upgrade manually using the classic upgrade. You can upgrade single VMs (Base) , single-site environment, and multisite environment.

For a high-level understanding about the upgrade and estimated time to complete tasks, see *Dell EMC VxBlock Central Getting Started Guide*.

The following table lists resources to upgrade related components:

Component	Document
AMP-VX	Dell EMC AMP-VX Software and Firmware Upgrade Guide
Vblock System 100	Dell EMC Vblock® System 100 Software and Firmware Upgrade Guide
VxBlock and Vblock Systems 200 and 240	Dell EMC VxBlock™ and Vblock™ Systems 200 and 240 Software and Firmware Upgrade Guide
VxBlock and Vblock Systems 340 and 350	Dell EMC VxBlock™ and Vblock™ Systems 340 and 350 Software and Firmware Upgrade Guide
VxBlock and Vblock Systems 540	Dell EMC VxBlock™ and Vblock™ Systems 540 Software and Firmware Upgrade Guide
VxBlock and Vblock Systems 720 and 740	Dell EMC VxBlock™ and Vblock™ Systems 720 and 740 Software and Firmware Upgrade Guide
VxBlock System 1000	Dell EMC VxBlock™ System 1000 Software and Firmware Upgrade Guide
VMware vSphere 6.5 to 6.7	Dell EMC Converged Systems Upgrade Guide from VMware vSphere 6.0 or VMware vSphere 6.5 to VMware vSphere 6.7

 **NOTE:** Do not copy and paste the commands that are outlined in this guide without first modifying them to suit your needs.

The [Glossary](#) provides terms, definitions, and acronyms that are related to Converged Systems.

VxBlock Central upgrade overview

The VxBlock Central upgrade can be performed for the Core VM, MSM VM, and MSP VM in single site or multisite clusters.

You can use a script to upgrade a single site cluster with a single MSM VM. From the script, the MSM VM initiates the upgrade for the Core VM and the MSP VM. For more information, see *Upgrade a single MSM VM using the simplified upgrade*.

You can also perform a classic upgrade by running the steps that are provided in *Upgrade a single-site cluster with a single MSM VM*.

A classic upgrade includes the following procedures:

- *Upgrade a single-site cluster with a single MSM VM*
- *Upgrade a single-site cluster containing multiple MSM VMs*
- *Upgrade a multisite cluster*

Select the appropriate upgrade procedure which is based on your environment.

Before an upgrade, there are system checks and information that must be recorded in case there are issues during the upgrade.

After the upgrade is complete, there are tasks that you must perform to verify the upgrade.

Pre upgrade tasks

Complete these tasks to ensure an uninterrupted upgrade for VxBlock Central and create a back-up of information that may not persist.

Verify system requirements

System, hardware, and license requirements require that minimums are met to support the VMs.

The following table provides memory requirements, vCPUs, disk size, and license information:

Components	Memory requirements (GB)	vCPUs	Disk size (GB)	Version	License requirements
Core VM	8	2	200	3.0	Base
MSM VM	12	4	250	3.0	Base
MSP VM (optional)	1	2	350	3.0	Base
VxBlock Central Orchestration Services VM	4	2	100	Download the latest file from the <i>Download Center</i> .	Workflow Automation
VxBlock Central Workflow Automation plug-in	N/A	N/A	N/A	Download the latest file from the <i>Download Center</i> .	Workflow Automation
VMware vRO	6	2	17	7.3, 7.5, and 7.6	Included with VMware vSphere license
VxBlock Central Operations Management Pack	N/A	N/A	N/A	2.0	Analytics
VMware vROps	Follow VMware guidelines.	N/A	N/A	7.5	Separate VMware vROps license required.
VxBlock Central Lifecycle Management	N/A	N/A	N/A	1.1	Lifecycle Management

Storage requirements

Install Core VM, MSM VM, and MSP VMs on one of the following:

- AMP-2S with VNXe
- AMP-3S or AMP Central with Dell EMC Unity
- AMP-VX with VMware vSAN

Install VxBlock Central Orchestration Services VM on one of the following:

- AMP-3S or AMP Central with Dell EMC Unity and Dell EMC Unity XT
- AMP-VX with VMware vSAN

Hardware requirements

Consider the following when deploying VxBlock Central:

- The minimum RAM size on the AMP is 128 GB. If the RAM is less than 128 GB, contact Dell EMC Support for assistance to upgrade the AMP.
- Use the NFS mount from the storage array for the MSP VM, where available.
- Use the local storage capacity for the AMPs, VNXe3100, and VNXe3150. You can add storage (see Cisco documentation) but doing so might add downtime.

VxBlock Central Workflow Automation has the following minimum server requirement on all supported VxBlock Systems:

- Expansion use case - one server
- New cluster provisioning - two servers

Upgrade verification tasks

The verification tasks help to ensure an uninterrupted VxBlock Central upgrade.

About this task

Perform the following verification tasks before and after you upgrade:

- Verify VM versions.
- Verify that services are up and running.
- Verify the SLIB connection between the MSM VM and the MSP VM.
- Ensure that the specified FQDN is in lower case, for smooth execution of the discovery process.

 **NOTE: If the FQDN is in upper case, then contact Dell EMC Support.**

When verifying, the package version is displayed instead of the release version. The supported versions are:

- Package version: 6.0.0.0
- VxBlock Central release version: 3.0

Steps

1. SSH to the VMs and log in as root.
2. Use the following table to verify the Core VM:

Core VM	Command
Version	<code>echo "Checking the version information" ; getFMagentInfo</code>
Service status	<code>echo -e "\nChecking the services in CORE VM" ; vision status</code>
Discovery completion status Results of the last five discovery cycles	<code>echo -e "\nChecking the discovery completion status and showing the last 5 successful cycle completion result" ; cat /opt/vce/fm/logs/FMAgent.log grep -i "current status" grep -i "100%" tail -5</code>

3. Use the following table to verify the MSM VM:

MSM VM	Command
Version	<code>echo -e "\nChecking the version installed" ; visionver</code>
Service status	<code>echo -e "\nChecking the services in MSM VM" ; vision status</code>
Credential manager CLI service status	<code>echo -e "\n" ; /opt/vce/credential-management/bin/credential-manager-cli status</code>
Validate credentials	<code>echo -e "\n" ; /opt/vce/credential-management/bin/credential-manager-cli validate</code>
Cassandra database connection	<code>echo -e "\nChecking the connection to Cassandra DB" ; /opt/vce/multivbmgmt/install/getConnectInfo.sh -e "select * from systeminfo.appinfo"</code>
Core VM connection with MSM VM	<code>/opt/vce/multivbmgmt/install/listSlibNodes.sh</code>

4. Type the following commands to verify MSP VM:

MSM VM	Command
MSP VM version	<code>echo -e "\nChecking the version installed" ; visionver</code>
Service status	<code>echo -e "\nChecking the status of the services in MSP VM" ; vision status</code>
Communication between MSM VM and MSP VM (check for the number of RabbitMQ connections) NOTE: The count of RabbitMQ connections must be equal to four. If not, then no connection is established.	<code>echo -e "\nChecking if we have rabbitmq connections between MSM and MSP VM" ; count=\$(netstat -ntp grep -i ":5672" wc -l); if [[\$count != 4]]; then echo "\$count is INCORRECT, check rabbitmq on MSM"; else echo "\$count is CORRECT"; fi</code>
MSP VM configuration file has the MSM VM hostname listed and display on the screen.	<code>echo -e "\nChecking if MSM hostname is listed correctly in the MSP configuration file" ; echo -e "PARAMETER remote.vce.amqp.rabbitHostnames is set to \$(cat /opt/vce/msp/conf/msp-common.properties grep -i "remote.vce.amqp.rabbitHostnames" cut -d '=' -f2)"</code>

Supported upgrade paths

Review the supported paths to upgrade VxBlock Central.

The following upgrade paths are supported:

- Vision 3.6.2 > VxBlock Central 1.5 > VxBlock Central 2.1 > VxBlock Central 3.0
- VxBlock Central 1.0 > VxBlock Central 2.0 > VxBlock Central 2.5 > VxBlock Central 3.0
- VxBlock Central 1.5 > VxBlock Central 2.1 > VxBlock Central 3.0
- VxBlock Central 2.0 > VxBlock Central 2.5 > VxBlock Central 3.0

If you are on a version of Vision earlier than Vision 3.6.2, skip up to two versions for the upgrade. For example, if you are upgrading from Vision 3.6.1, you must first upgrade to VxBlock Central 1.0. After which, upgrade to VxBlock Central 2.0, and next upgrade to VxBlock Central 2.5. And finally upgrade to VxBlock Central 3.0. See the *Dell EMC VxBlock Central 1.0 Upgrade Guide*.

Download VxBlock Central upgrade files

To upgrade VxBlock Central, download the required files to upgrade the Core VM, MSM VM, and the MSP VM to the latest software version.

Prerequisites

Obtain access to the [Download Center](#) to download files.

Steps

1. For the simplified upgrade of a single MSM VM, download the `VxBlock-Central_upgradeBundle` file from the Download Center and copy to the `/root` directory on the MSM VM.
2. For Core VM upgrade, download the `VxBlock-Central_core_upgrade-<buildnumber>.vce` file and copy to the `/root` directory on the Core VM.
3. For MSM VM upgrade, download the `VxBlock-Central_msm_upgrade-<buildnumber>.vce` file and copy to the `/root` directory on the MSM VM.
4. For MSP VM upgrade, download the `VxBlock-Central_msp_upgrade-<buildnumber>.vce` file.
5. Download the .zip files with the latest version of the compliance content. From VxBlock Central 1.0 or later, the RCM content and technical content are combined as one file. Download the .tar file to use the *VxBlock Central simplified upgrade*.

Collect the custom display names

In a single MSM VM deployment, custom display names are not retained after an upgrade.

Steps

1. Collect any custom display names (data center or clustered environment names) defined for your existing installation.
2. Retain the custom display names so that you can reenter them after the upgrade completes.

Take a snapshot of VMs

Before upgrading, create a snapshot of a Core or MSM VM. If you encounter problems during the upgrade process, you can use the snapshot to revert the VM.

Steps

1. Connect to the VM and power off.
2. To power off the VM, type: `shutdown -h now`
Do not power on the VMs until snapshots have been taken of the other VMs.
3. Log in to VMware vSphere Client using administrative privileges.
4. Under **Navigation**, select **Home > Inventory > Hosts and Clusters**.
5. Right-click the VM and select **Snapshot > Take Snapshot**.
6. Enter a name and description for the snapshot.
7. Clear the checkboxes to snapshot the VM memory and forget the guest file system, if available.
8. Click **OK**.
9. Power on and log in to the respective VM which is upgraded.

Take a snapshot of VMs in the cluster

Before upgrading, create a snapshot of each VM in the cluster. If you encounter problems during the upgrade process, you can use the snapshot to revert the VM.

Steps

1. For the Core VM and the MSP VM, power off and take a snapshot of every VM being upgraded.
2. For the MSM VM, perform the following:
 - a. Record the order in which the MSM VMs are shut down.
 - b. Power off the MSM VM that is acting as the Cassandra seed node last.

- c. Shut down the MSM VMs in the cluster one by one, in five minute intervals.
3. In the powered-off state, take a snapshot of each MSM VM being upgraded.
Do not power on the MSM VMs until snapshots have been taken of the other VMs.
4. Power on and log in to each Core VM associated with the MSM VMs in the cluster.
5. Power on all MSM VMs in the reverse sequence of how they were shut down, starting with the seed node. Allow five minute intervals between powering up each MSM VM.
6. Power on and log in to the MSP VM, if associated with the cluster.

Configure the VMs to use the NTP server

Ensure that each VM is configured to use an NTP server. If redeploying an MSM VM, specify an NTP server IP address when configuring the server.

Determine the NTP server to use for the data center. Use the VLAN gateway or the gateway of the Converged System.

Ensure you have your MSP VM IP address and VxBlock Central Core root passwords.

Steps

1. Use SSH to access the VM as the root user.
2. To verify access to the NTP server, type:

```
ntpdate -u <NTP_IP_address>
```
3. Edit `/etc/ntp.conf`.
4. Comment out the default CentOS server entries, and add the following entry: **server <IP_address>**
If the lines are already commented out, skip this step and run `service ntpd status` to check if the NTP daemon is running. If the daemon is running, skip the remaining steps and move to the next VM.
5. To save the changes and start the NTPD service, type:

```
service ntpd restart
```
6. To start ntpd service on reboot, type:

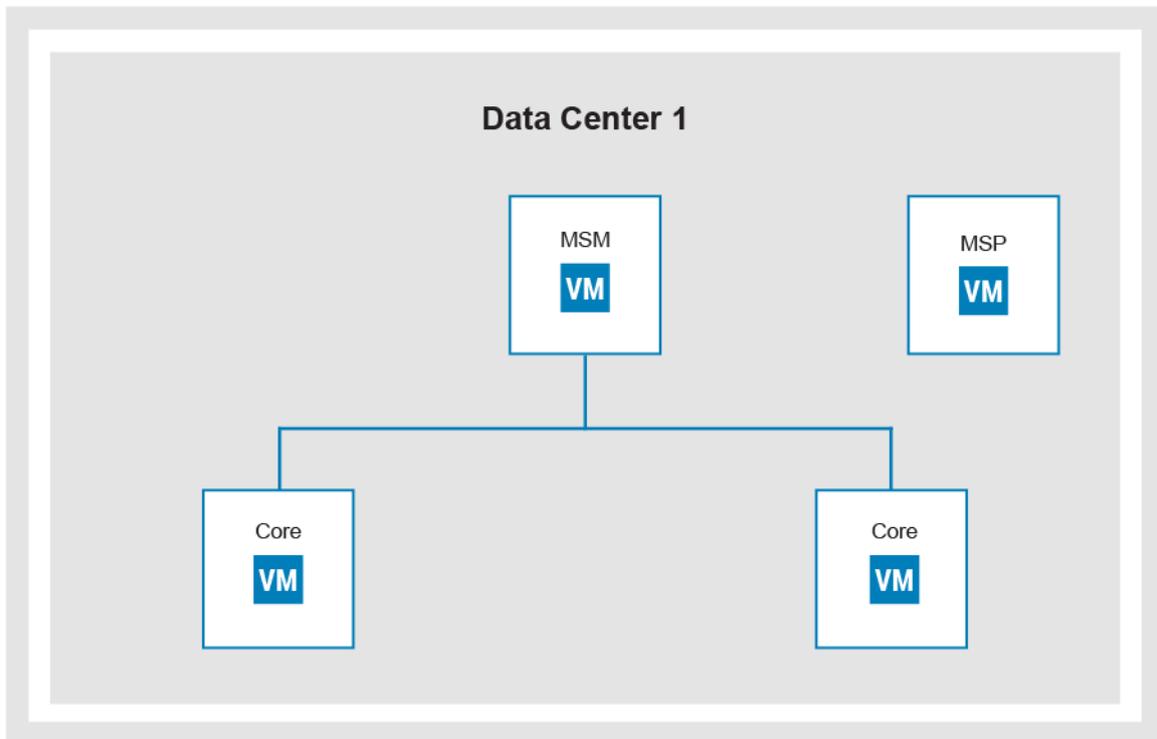
```
chkconfig ntpd on
```

Upgrade a single MSM VM using the simplified upgrade

Upgrade in a data center environment with multiple Core VMs mapped to a single MSM VM.

About this task

The following illustration is an example of a single-site cluster:



Prerequisites

Ensure you complete the following steps for a VxBlock Central simplified upgrade:

1. Collect the custom display names.
2. Take a snapshot of the VMs.
3. Configure the NTP server.

Steps

1. Download the `VxBlock-Central_upgradeBundle` file from the Download Center for the MSM VM and copy to the root directory on the MSM VM:
2. Obtain file permission and type:

```
sh VxBlock-Central_upgradebundle_<buildnumber>.vce
```

This script runs the MSP VM, Core VM, and MSM upgrades.

3. A series of prompts instruct you to input the following:
 - a. SLIB\MSP root passwords.
 - b. Confirm OVA snapshot (y/n).
 - c. Confirm to connect (y/n).

To change details of an accepted EULA, type: `/opt/vce/fm/bin/resetEulaAcceptance`, and then `/opt/vce/fm/bin/startEulaAcceptance`.

If the confirmation for the OVA snapshot is **n** or any of the system upgrade fails, the script stops and you need to revert to the snapshot and rerun the command from MSM again.

Once all the systems are updated, the command displays a summary of the execution. The output of the run is written into a logfile: `/opt/vce/multivbmgmt/logs/upgradeLogFile-{date}.log`

4. At the end of the run, MSM reboots. Log in again and check all services are working.
5. See *Verify a Core VM upgrade* to verify the upgrade.
6. See *Verify the MSP VM upgrade* to verify the upgrade.
7. See *Verify the MSM VM upgrade* to verify the upgrade.
8. Enable permission for CLM data sync by typing: **chmod 775 /opt/tomcat/temp**
9. Restart the MSM services by typing **vision stop; vision start;**

Next steps

Retype the custom display names.

Upgrade a single site cluster with a single MSM VM

Upgrade one data center environment with multiple Core VMs mapped to a single MSM VM.

About this task

You can use the simplified script for the single site upgrade. To perform a classic upgrade, follow the procedures to upgrade the Core VM, MSM VM and MSP VM.

You can upgrade the Core VM associated with MSM VMs in the cluster simultaneously.

Start a Core VM upgrade

Run `VxBlock-Central_core_upgrade-<buildnumber>.vce` to upgrade the Core VM.

Prerequisites

- Verify that the Core VM can be directly upgraded.
- From the list of supported upgrade paths, determine which path best suits your system.
- Verify that you have the CAS administrator and VNXe service account password.
- To validate the components and login credentials for all components in the `vblock.xml` file, type:

```
configTool.sh -v vblock.xml
```

Steps

1. SSH to the Core VM using SSH using root credentials.
2. Copy `VxBlock-Central_core_upgrade-<buildnumber>.vce` to the `/root` directory on the Core VM.
3. (Optional) To verify that the Core VM meets the minimum requirements for the upgrade, to check the version, or to get help for the command, type:

```
sh VxBlock-Central_core_upgrade-<buildnumber>.vce --argument
```

The following lists optional arguments:

Argument	Description
<code>choice</code>	Performs a check for minimum requirements, such as available disk space.
<code>noprompt</code>	Runs the upgrade process without prompting you to confirm: <ul style="list-style-type: none">• You have a VM snapshot.• You want to reboot the VM after upgrade. <p> NOTE: On ping, the upgrade process is triggered immediately.</p>
<code>version</code>	Displays the installed version, the version of the upgrade, and the list of RPM files that the upgrade bundle includes.
<code>help</code>	Displays help usage.

4. To start the upgrade, enter:

```
sh VxBlock-Central_core_upgrade-<buildnumber>.vce
```

5. Follow the prompts.

At the EULA prompt, if you type **y** go to step 6 or type **n** and continue to step 7.

6. Complete the EULA acceptance. The fields in the EULA cannot exceed 500 characters or contain angle brackets.
 - a. Scroll through the EULA until you see the `Enter Name:` prompt.

- b. Enter your name and press **Enter**.
- c. Enter your job title and press **Enter**.
- d. Enter the name of the licensee company and press **Enter**.
- e. Optional: Enter the name of the accepting company and press **Enter**. If you do not specify an accepting company, the value defaults to the licensee company.
- f. Enter **Yes** to accept the EULA.
- g. Authenticate to the CAS and enter the CAS password.

i **NOTE: If you enter an incorrect CAS password after three attempts, the upgrade process stops and you must restart the upgrade.**

7. When do you want to delete existing storage volume data as it improves the performance? is displayed, type **y** or **n** as needed.

Verify a Core VM upgrade

After upgrading, verify the correct version of the Core VM is installed.

Steps

1. Connect to the Core VM and enter: `getFMagentInfo`
2. Ensure that the **Version** field contains the version of Core VM that you installed.
i **NOTE: The OVA version that is displayed may differ.**
3. For VPLEX, if the configuration is a metro setup, after upgrade, run the script `/opt/vce/fm/bin/showWANPortsforVplex.sh` to discover WAN COM ports for the same.
Wait 30 to 45 minutes for VPLEX WAN ports to show in MSM VM.

Start an MSM VM upgrade

Start the MSM VM upgrade file on the MSM VM.

Prerequisites

- Verify that the MSM VM can be directly upgraded.
- Check the list of supported upgrade paths to determine which path best suits your system.

About this task

After the MSM VM cluster upgrade process starts in a data center, do not:

- Add any Core VMs to any MSM VM in the cluster.
- Join MSM VMs to the MSM VM cluster.

Steps

1. SSH to the MSM VM with root credentials.
2. Ensure that all Core VMs connected to the MSM VM being upgraded are powered on.
3. Copy `VxBlock-Central_msm_upgrade-<buildnumber>.vce` to the `/root` directory on the MSM VM.
4. (Optional) To verify that the MSM VM meets the minimum requirements for the upgrade, type:

```
sh VxBlock-Central_msm_upgrade-<buildnumber>.vce --argument
```

Where *argument* is one of the following optional arguments:

Argument	Description
<code>check</code>	Performs a check for minimum requirements such as available disk space.
<code>noprompt</code>	Runs the upgrade process without prompting you to confirm:

Argument	Description
	<ul style="list-style-type: none"> You have a virtual machine snapshot. You want to reboot the virtual machine after upgrade.
version	Displays the currently installed version, the version of the upgrade, and the list of RPM files that the upgrade bundle includes.
help	Displays help usage.

5. To start the upgrade, type:

```
sh VxBlock-Central_msm_upgrade-<buildnumber>.vce
```

6. When prompted to take a snapshot, enter **y** or **n**.

All Core VMs that are connected to the MSM VM being upgraded must be powered on.

7. When the upgrade is complete, a summary is displayed. Type **y** to restart the VM.

Rerun all compliance scans after the upgrade. In a clustered environment, compliance scan results previous to the upgrade are retained. In a single MSM deployment, the details are not retained. See the online help for information about compliance scans.

Update the MSM credential manager service

If the root or VxBlock Central user password has been changed on the Core VM, update the MSM credential manager service with the password.

Ensure that the system configuration is consistent with the system configuration on VxBlock Central UI. If not, then you must update the same configuration on VxBlock Central UI.

Start an SSH session to the MSM VM and complete the following steps:

1. Log in to the MSM VM as the root user.

2. To change the Core VM root user password for MSM VM, type:

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

where *core_IPaddress* is the IP address for the Core VM where the password was changed.

3. Type **yes**.

4. Type **root** (or press **Enter**) for the username.

5. Type the new password for the Core VM.

6. After successful update, exit from CLI.

Verify the MSM VM upgrade

After completing the upgrade process, use the VxBlock Central dashboard to verify that the version number of the MSM corresponds to the version that you installed.

Prerequisites

- Obtain the FQDN of the MSM VM.
- Verify that you have access to the VxBlock Central dashboard.

Steps

1. Use Google Chrome to access the MSM VM at: **https://<FQDN>**

The MSM VM should be able to ping the FQDN of the Core MV. If not, a host file entry for the Core VM must exist on the MSM VM.

2. Log in with default credentials to the VxBlock Central dashboard, then change the default password.

3. Click **About** to verify that the version number is correct.

If the message `Unable to execute search` is displayed when you log in to the MSM VM, the database rebuild is not complete. Wait 15 minutes and log in to the MSM VM again.

Verify the MSM VM configuration file

After the MSM VM upgrade is complete, verify that the configuration file contains the correct content.

Steps

1. Open the file: `/opt/vce/multivbmgmt/conf/cvm-config.properties` and verify the following lines are displayed:
 - `operationSettingFileLocation = /opt/vce/multivbmgmt/conf`
 - `operationSettingFile = operations-configuration.xml`If not, add them.
2. Restart the `tomcat` service.

Start the MSP VM upgrade

Execute `VxBlock-Central_msp_upgrade--<buildnumber>.vce` to upgrade.

Prerequisites

- Verify that all Core VMs connected to the MSM VM being upgraded are powered up.
- Verify the MSP VM can be directly upgraded.

Steps

1. SSH to the MSP VM using root credentials.
2. Copy `VxBlock-Central_msp_upgrade--<buildnumber>.vce` to the `/root` directory on the MSP VM.
3. (Optional) To verify that the MSP VM meets the minimum requirements for the update, check the version. To get help for the command, type:

```
sh VxBlock-Central_msp_upgrade--<buildnumber>.vce --argument
```

Where *argument* is one of the following optional arguments:

Argument	Description
<code>check</code>	Performs a check for minimum requirements such as available disk space.
<code>noprompt</code>	Runs the upgrade process without prompting you to confirm: <ul style="list-style-type: none">· You have a virtual machine snapshot.· You want to reboot the virtual machine after upgrade.
<code>version</code>	Displays the currently installed version, the version of the upgrade, and the list of RPM files that the upgrade bundle includes.
<code>help</code>	Displays help usage.

4. To start the upgrade, type:

```
sh VxBlock-Central_msp_upgrade--<buildnumber>.vce
```
5. When prompted to take a snapshot, enter **y** or **n**.
6. When the upgrade is complete, a summary is displayed. Type **y** to restart the VM.

Verify the MSP VM upgrade

Verify the status of the MSP VM.

Steps

1. Connect to the MSP VM.
2. To verify that the component services are running, type:

```
service https status
service vision-assetmanager status
service vision-contentshare status
service vision-contentsource status
service vision-downloader status
```

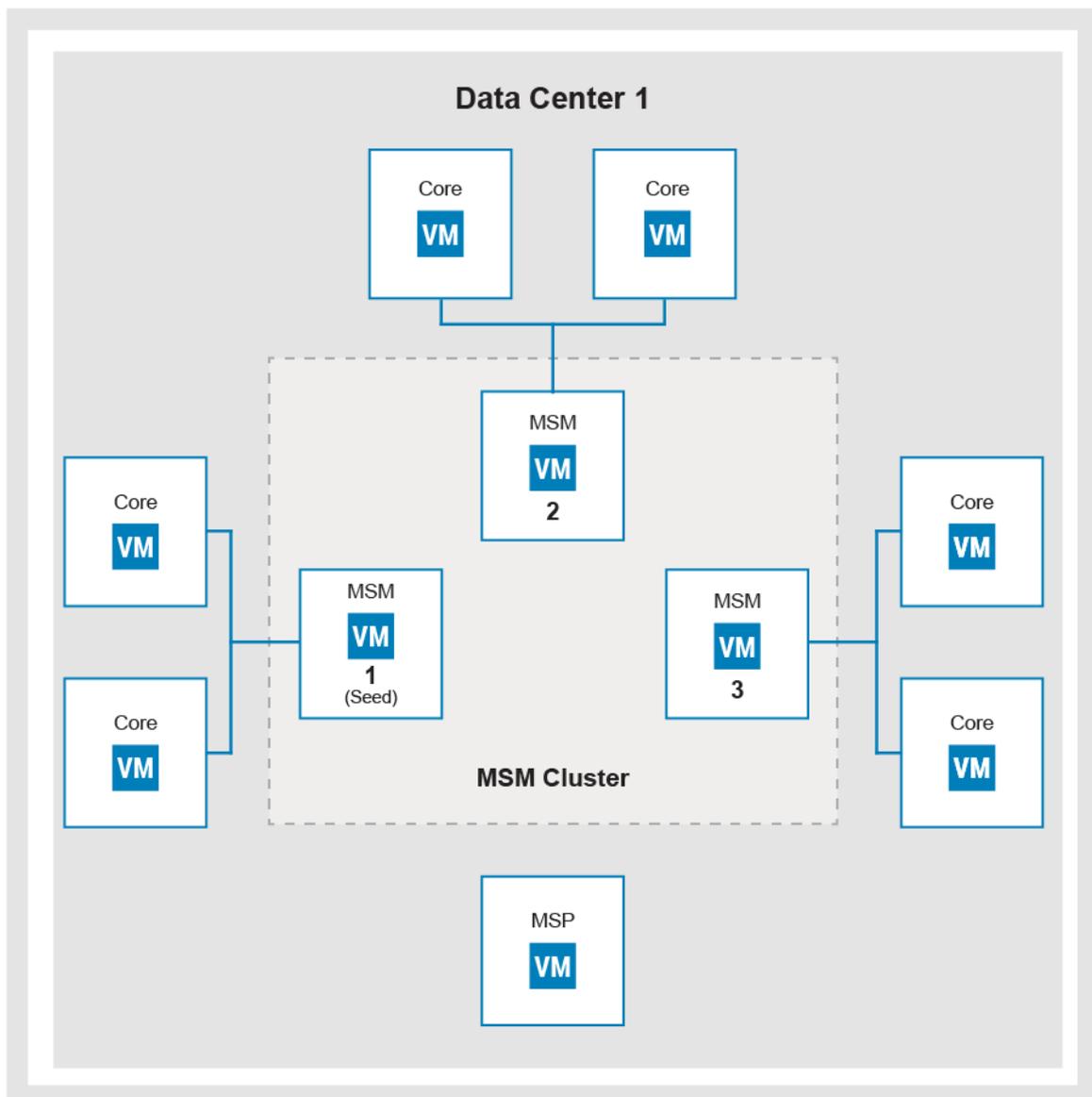
3. If you updated the MSP VM password, change the CAS password for the MSP VM to match the CAS password on the MSM VM.

Upgrade a single-site cluster containing multiple MSM VMs

Upgrade one data center environment with multiple MSM VMs, each associated with up to two Core VMs.

About this task

The following figure is an example of a single-site cluster with multiple MSM VMs:



When performing the classic upgrade, you can upgrade the Core VM associated with MSM VMs in the cluster simultaneously. Identify the MSM VM acting as the Cassandra seed node and determine the MSM VM with which to start the upgrade.

Once the upgrade process begins, do not:

- Add any Core VMs to any MSM VMs in the cluster.
- Join any additional MSM VMs to the MSM VM cluster.

After an MSM VM in a cluster is upgraded, exceptions might be displayed in the `/opt/vce/multivbmgmt/logs/CollectionManager.log` until all MSM VMs are upgraded. Collections can temporarily fail on all MSM VMs until they are upgraded. Until both data centers are upgraded, an MSM VM upgrade in one data center impacts collections by MSM VMs running in the other data center.

Start a Core VM upgrade

Run `VxBlock-Central_core_upgrade-<buildnumber>.vce` to upgrade the Core VM.

Prerequisites

- Verify that the Core VM can be directly upgraded.
- From the list of supported upgrade paths, determine which path best suits your system.
- Verify that you have the CAS administrator and VNXe service account password.
- To validate the components and login credentials for all components in the `vblock.xml` file, type:

```
configTool.sh -v vblock.xml
```

Steps

1. SSH to the Core VM using SSH using root credentials.
2. Copy `VxBlock-Central_core_upgrade-<buildnumber>.vce` to the `/root` directory on the Core VM.
3. (Optional) To verify that the Core VM meets the minimum requirements for the upgrade, to check the version, or to get help for the command, type:

```
sh VxBlock-Central_core_upgrade-<buildnumber>.vce --argument
```

The following lists optional arguments:

Argument	Description
<code>choice</code>	Performs a check for minimum requirements, such as available disk space.
<code>noprompt</code>	Runs the upgrade process without prompting you to confirm: <ul style="list-style-type: none">• You have a VM snapshot.• You want to reboot the VM after upgrade. <p> NOTE: On ping, the upgrade process is triggered immediately.</p>
<code>version</code>	Displays the installed version, the version of the upgrade, and the list of RPM files that the upgrade bundle includes.
<code>help</code>	Displays help usage.

4. To start the upgrade, enter:

```
sh VxBlock-Central_core_upgrade-<buildnumber>.vce
```

5. Follow the prompts.

At the EULA prompt, if you type **y** go to step 6 or type **n** and continue to step 7.

6. Complete the EULA acceptance. The fields in the EULA cannot exceed 500 characters or contain angle brackets.
 - a. Scroll through the EULA until you see the `Enter Name:` prompt.
 - b. Enter your name and press **Enter**.
 - c. Enter your job title and press **Enter**.
 - d. Enter the name of the licensee company and press **Enter**.
 - e. Optional: Enter the name of the accepting company and press **Enter**. If you do not specify an accepting company, the value defaults to the licensee company.
 - f. Enter **Yes** to accept the EULA.
 - g. Authenticate to the CAS and enter the CAS password.

NOTE: If you enter an incorrect CAS password after three attempts, the upgrade process stops and you must restart the upgrade.

- When Do you want to delete existing storage volume data as it improves the performance? is displayed, type **y** or **n** as needed.

Verify a Core VM upgrade

After upgrading, verify the correct version of the Core VM is installed.

Steps

- Connect to the Core VM and enter: **getFMagentInfo**
- Ensure that the **Version** field contains the version of Core VM that you installed.

NOTE: The OVA version that is displayed may differ.

- For VPLEX, if the configuration is a metro setup, after upgrade, run the script `/opt/vce/fm/bin/showWANPortsforVplex.sh` to discover WAN COM ports for the same.

Wait 30 to 45 minutes for VPLEX WAN ports to show in MSM VM.

Start the MSP VM upgrade

Execute **VxBlock-Central_msp_upgrade--<buildnumber>.vce** to upgrade.

Prerequisites

- Verify that all Core VMs connected to the MSM VM being upgraded are powered up.
- Verify the MSP VM can be directly upgraded.

Steps

- SSH to the MSP VM using root credentials.
- Copy **VxBlock-Central_msp_upgrade--<buildnumber>.vce** to the `/root` directory on the MSP VM.
- (Optional) To verify that the MSP VM meets the minimum requirements for the update, check the version. To get help for the command, type:

```
sh VxBlock-Central_msp_upgrade--<buildnumber>.vce --argument
```

Where *argument* is one of the following optional arguments:

Argument	Description
check	Performs a check for minimum requirements such as available disk space.
noprompt	Runs the upgrade process without prompting you to confirm: <ul style="list-style-type: none">You have a virtual machine snapshot.You want to reboot the virtual machine after upgrade.
version	Displays the currently installed version, the version of the upgrade, and the list of RPM files that the upgrade bundle includes.
help	Displays help usage.

- To start the upgrade, type:

```
sh VxBlock-Central_msp_upgrade--<buildnumber>.vce
```

- When prompted to take a snapshot, enter **y** or **n**.
- When the upgrade is complete, a summary is displayed. Type **y** to restart the VM.

Verify the MSP VM upgrade

Verify the status of the MSP VM.

Steps

1. Connect to the MSP VM.
2. To verify that the component services are running, type:

```
service https status  
service vision-assetmanager status  
service vision-contentshare status  
service vision-contentsource status  
service vision-downloader status
```

3. If you updated the MSP VM password, change the CAS password for the MSP VM to match the CAS password on the MSM VM.

Identify the MSM VM acting as the Cassandra seed node

Find the seed node to determine the MSM VM to start the upgrade. If the MSM VM cluster spans multiple data centers, perform the upgrade on each data center separately.

Steps

1. To identify the Cassandra seed node, SSH session using the root credentials to any MSM VM cluster.
2. Enter: `grep seeds: /opt/cassandra/conf/cassandra.yaml`
3. From the output, identify the IP address acting as the Cassandra seed node.

Start an MSM VM upgrade

Start the MSM VM upgrade file on the MSM VM.

Prerequisites

- Verify that the MSM VM can be directly upgraded.
- Check the list of supported upgrade paths to determine which path best suits your system.

About this task

After the MSM VM cluster upgrade process starts in a data center, do not:

- Add any Core VMs to any MSM VM in the cluster.
- Join MSM VMs to the MSM VM cluster.

Steps

1. SSH to the MSM VM with root credentials.
2. Ensure that all Core VMs connected to the MSM VM being upgraded are powered on.
3. Copy `VxBlock-Central_msm_upgrade-<buildnumber>.vce` to the `/root` directory on the MSM VM.
4. (Optional) To verify that the MSM VM meets the minimum requirements for the upgrade, type:

```
sh VxBlock-Central_msm_upgrade-<buildnumber>.vce --argument
```

Where *argument* is one of the following optional arguments:

Argument	Description
check	Performs a check for minimum requirements such as available disk space.

Argument	Description
noprompt	Runs the upgrade process without prompting you to confirm: <ul style="list-style-type: none"> You have a virtual machine snapshot. You want to reboot the virtual machine after upgrade.
version	Displays the currently installed version, the version of the upgrade, and the list of RPM files that the upgrade bundle includes.
help	Displays help usage.

5. To start the upgrade, type:

```
sh VxBlock-Central_msm_upgrade-<buildnumber>.vce
```

6. When prompted to take a snapshot, enter **y** or **n**.

All Core VMs that are connected to the MSM VM being upgraded must be powered on.

7. When the upgrade is complete, a summary is displayed. Type **y** to restart the VM.

Rerun all compliance scans after the upgrade. In a clustered environment, compliance scan results previous to the upgrade are retained. In a single MSM deployment, the details are not retained. See the online help for information about compliance scans.

Update the MSM credential manager service

If the root or VxBlock Central user password has been changed on the Core VM, update the MSM credential manager service with the password.

Ensure that the system configuration is consistent with the system configuration on VxBlock Central UI. If not, then you must update the same configuration on VxBlock Central UI.

Start an SSH session to the MSM VM and complete the following steps:

1. Log in to the MSM VM as the root user.
2. To change the Core VM root user password for MSM VM, type:

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

where *core_IPaddress* is the IP address for the Core VM where the password was changed.

3. Type **yes**.
4. Type **root** (or press **Enter**) for the username.
5. Type the new password for the Core VM.
6. After successful update, exit from CLI.

Verify the MSM VM upgrade

After completing the upgrade process, use the VxBlock Central dashboard to verify that the version number of the MSM corresponds to the version that you installed.

Prerequisites

- Obtain the FQDN of the MSM VM.
- Verify that you have access to the VxBlock Central dashboard.

Steps

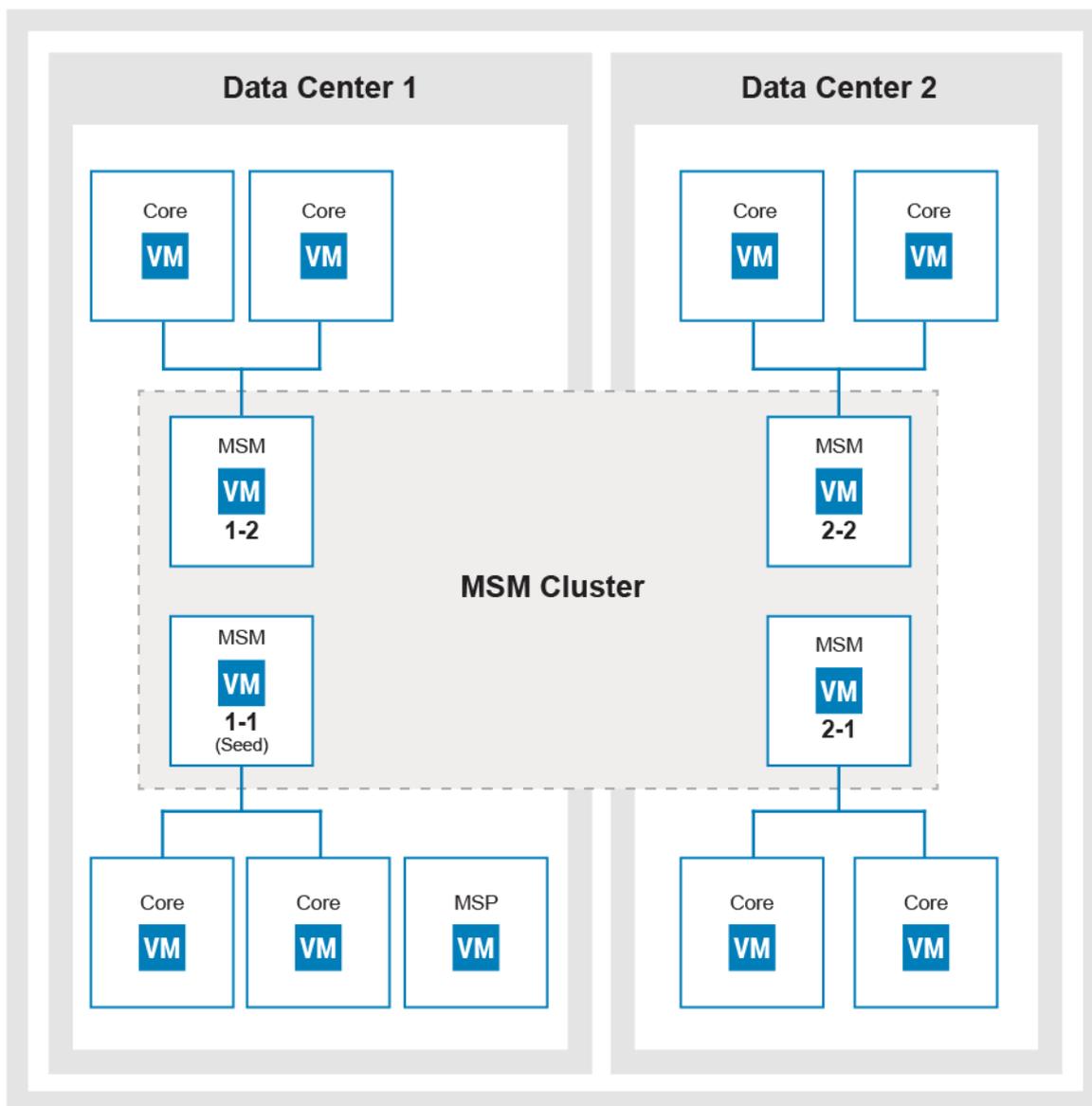
1. Use Google Chrome to access the MSM VM at: **https://<FQDN>**
The MSM VM should be able to ping the FQDN of the Core MV. If not, a host file entry for the Core VM must exist on the MSM VM.
2. Log in with default credentials to the VxBlock Central dashboard, then change the default password.
3. Click **About** to verify that the version number is correct.
If the message `Unable to execute search` is displayed when you log in to the MSM VM, the database rebuild is not complete. Wait 15 minutes and log in to the MSM VM again.

Upgrade a multisite cluster

Upgrade up to three data centers in an environment, each having up to two MSM VMs. These MSM VMs can each be associated with up to two Core VMs.

About this task

The following figure shows multisite cluster data center environment:



Upgrade the VMs in each data center starting with the data center containing the MSM VM acting as the Cassandra seed node. The Core VMs can be upgraded across data centers before the MSM VM upgrades to minimize the time between upgrading the MSM VM.

Once the upgrade process begins, do not:

- Add any Core VMs to any MSM VMs in the cluster.
- Join any additional MSM VMs to the MSM VM cluster.

After an MSM VM cluster is upgraded, exceptions may display in the `/opt/vce/multivbmgmt/logs/CollectionManager.log` until all MSM VMs are upgraded. Collections may fail on MSM VMs until they are upgraded. Until both data centers are upgraded, an MSM VM upgrade in one data center impacts collections by MSM VMs running in the other data center.

Start a Core VM upgrade

Run `VxBlock-Central_core_upgrade-<buildnumber>.vce` to upgrade the Core VM.

Prerequisites

- Verify that the Core VM can be directly upgraded.
- From the list of supported upgrade paths, determine which path best suits your system.
- Verify that you have the CAS administrator and VNXe service account password.
- To validate the components and login credentials for all components in the `vblock.xml` file, type:

```
configTool.sh -v vblock.xml
```

Steps

1. SSH to the Core VM using SSH using root credentials.
2. Copy `VxBlock-Central_core_upgrade-<buildnumber>.vce` to the `/root` directory on the Core VM.
3. (Optional) To verify that the Core VM meets the minimum requirements for the upgrade, to check the version, or to get help for the command, type:

```
sh VxBlock-Central_core_upgrade-<buildnumber>.vce --argument
```

The following lists optional arguments:

Argument	Description
<code>choice</code>	Performs a check for minimum requirements, such as available disk space.
<code>noprompt</code>	Runs the upgrade process without prompting you to confirm: <ul style="list-style-type: none">• You have a VM snapshot.• You want to reboot the VM after upgrade. <p>NOTE: On ping, the upgrade process is triggered immediately.</p>
<code>version</code>	Displays the installed version, the version of the upgrade, and the list of RPM files that the upgrade bundle includes.
<code>help</code>	Displays help usage.

4. To start the upgrade, enter:

```
sh VxBlock-Central_core_upgrade-<buildnumber>.vce
```

5. Follow the prompts.

At the EULA prompt, if you type **y** go to step 6 or type **n** and continue to step 7.

6. Complete the EULA acceptance. The fields in the EULA cannot exceed 500 characters or contain angle brackets.
 - a. Scroll through the EULA until you see the `Enter Name:` prompt.
 - b. Enter your name and press **Enter**.
 - c. Enter your job title and press **Enter**.
 - d. Enter the name of the licensee company and press **Enter**.
 - e. Optional: Enter the name of the accepting company and press **Enter**. If you do not specify an accepting company, the value defaults to the licensee company.
 - f. Enter **Yes** to accept the EULA.
 - g. Authenticate to the CAS and enter the CAS password.

NOTE: If you enter an incorrect CAS password after three attempts, the upgrade process stops and you must restart the upgrade.

7. When Do you want to delete existing storage volume data as it improves the performance? is displayed, type **y** or **n** as needed.

Verify a Core VM upgrade

After upgrading, verify the correct version of the Core VM is installed.

Steps

1. Connect to the Core VM and enter: `getFMagentInfo`
2. Ensure that the **Version** field contains the version of Core VM that you installed.

NOTE: The OVA version that is displayed may differ.

3. For VPLEX, if the configuration is a metro setup, after upgrade, run the script `/opt/vce/fm/bin/showWANPortsforVplex.sh` to discover WAN COM ports for the same.
Wait 30 to 45 minutes for VPLEX WAN ports to show in MSM VM.

Start the MSP VM upgrade

Execute `VxBlock-Central_msp_upgrade--<buildnumber>.vce` to upgrade.

Prerequisites

- Verify that all Core VMs connected to the MSM VM being upgraded are powered up.
- Verify the MSP VM can be directly upgraded.

Steps

1. SSH to the MSP VM using root credentials.
2. Copy `VxBlock-Central_msp_upgrade--<buildnumber>.vce` to the `/root` directory on the MSP VM.
3. (Optional) To verify that the MSP VM meets the minimum requirements for the update, check the version. To get help for the command, type:

```
sh VxBlock-Central_msp_upgrade--<buildnumber>.vce --argument
```

Where *argument* is one of the following optional arguments:

Argument	Description
<code>check</code>	Performs a check for minimum requirements such as available disk space.
<code>noprompt</code>	Runs the upgrade process without prompting you to confirm: <ul style="list-style-type: none">• You have a virtual machine snapshot.• You want to reboot the virtual machine after upgrade.
<code>version</code>	Displays the currently installed version, the version of the upgrade, and the list of RPM files that the upgrade bundle includes.
<code>help</code>	Displays help usage.

4. To start the upgrade, type:

```
sh VxBlock-Central_msp_upgrade--<buildnumber>.vce
```

5. When prompted to take a snapshot, enter **y** or **n**.
6. When the upgrade is complete, a summary is displayed. Type **y** to restart the VM.

Verify the MSP VM upgrade

Verify the status of the MSP VM.

Steps

1. Connect to the MSP VM.

2. To verify that the component services are running, type:

```
service https status
service vision-assetmanager status
service vision-contentshare status
service vision-contentsource status
service vision-downloader status
```

3. If you updated the MSP VM password, change the CAS password for the MSP VM to match the CAS password on the MSM VM.

Identify the MSM VM acting as the Cassandra seed node

Find the seed node to determine the MSM VM to start the upgrade. If the MSM VM cluster spans multiple data centers, perform the upgrade on each data center separately.

Steps

1. To identify the Cassandra seed node, SSH session using the root credentials to any MSM VM cluster.
2. Enter: `grep seeds: /opt/cassandra/conf/cassandra.yaml`
3. From the output, identify the IP address acting as the Cassandra seed node.

Start an MSM VM upgrade

Start the MSM VM upgrade file on the MSM VM.

Prerequisites

- Verify that the MSM VM can be directly upgraded.
- Check the list of supported upgrade paths to determine which path best suits your system.

About this task

After the MSM VM cluster upgrade process starts in a data center, do not:

- Add any Core VMs to any MSM VM in the cluster.
- Join MSM VMs to the MSM VM cluster.

Steps

1. SSH to the MSM VM with root credentials.
2. Ensure that all Core VMs connected to the MSM VM being upgraded are powered on.
3. Copy `VxBlock-Central_msm_upgrade-<buildnumber>.vce` to the `/root` directory on the MSM VM.
4. (Optional) To verify that the MSM VM meets the minimum requirements for the upgrade, type:

```
sh VxBlock-Central_msm_upgrade-<buildnumber>.vce --argument
```

Where *argument* is one of the following optional arguments:

Argument	Description
<code>check</code>	Performs a check for minimum requirements such as available disk space.
<code>noprompt</code>	Runs the upgrade process without prompting you to confirm: <ul style="list-style-type: none">• You have a virtual machine snapshot.• You want to reboot the virtual machine after upgrade.
<code>version</code>	Displays the currently installed version, the version of the upgrade, and the list of RPM files that the upgrade bundle includes.

Argument	Description
help	Displays help usage.

- To start the upgrade, type:

```
sh VxBlock-Central_msm_upgrade-<buildnumber>.vce
```

- When prompted to take a snapshot, enter **y** or **n**.
All Core VMs that are connected to the MSM VM being upgraded must be powered on.
- When the upgrade is complete, a summary is displayed. Type **y** to restart the VM.
Rerun all compliance scans after the upgrade. In a clustered environment, compliance scan results previous to the upgrade are retained. In a single MSM deployment, the details are not retained. See the online help for information about compliance scans.

Update the MSM credential manager service

If the root or VxBlock Central user password has been changed on the Core VM, update the MSM credential manager service with the password.

Ensure that the system configuration is consistent with the system configuration on VxBlock Central UI. If not, then you must update the same configuration on VxBlock Central UI.

Start an SSH session to the MSM VM and complete the following steps:

- Log in to the MSM VM as the root user.
- To change the Core VM root user password for MSM VM, type:

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

where *core_IPaddress* is the IP address for the Core VM where the password was changed.

- Type **yes**.
- Type **root** (or press **Enter**) for the username.
- Type the new password for the Core VM.
- After successful update, exit from CLI.

Verify the MSM VM upgrade

After completing the upgrade process, use the VxBlock Central dashboard to verify that the version number of the MSM corresponds to the version that you installed.

Prerequisites

- Obtain the FQDN of the MSM VM.
- Verify that you have access to the VxBlock Central dashboard.

Steps

- Use Google Chrome to access the MSM VM at: **https://<FQDN>**
The MSM VM should be able to ping the FQDN of the Core MV. If not, a host file entry for the Core VM must exist on the MSM VM.
- Log in with default credentials to the VxBlock Central dashboard, then change the default password.
- Click **About** to verify that the version number is correct.
If the message `Unable to execute search` is displayed when you log in to the MSM VM, the database rebuild is not complete. Wait 15 minutes and log in to the MSM VM again.

Post upgrade tasks

The post upgrade tasks enable successful upgrade of VxBlock Central.

Retype the custom display names

In a single MSM deployment, custom display names are not retained after an upgrade. You must reenter the names you defined before you began the upgrade process. Custom display names are retained in a clustered environment.

Steps

1. Retype the custom display names.
2. See the dashboard help for more information about renaming the display names.

Remove a VM snapshot

Remove VM snapshots after you successfully upgrade the VMs.

About this task

If a VM is part of a cluster, do not remove the VM snapshot until all VMs are successfully upgraded. Go to [VMware Knowledge base](#) and search for *Article 1025279* for information about best practices for snapshots in a VMware environment.

Upload compliance content

Use the VxBlock Central MSM UI to upload and install new compliance content.

About this task

- If using a single MSM VM, upload the compliance content using the VxBlock Central dashboard.
- If using a single-site cluster MSM VM, repeat upgrading MSM VM steps for non-seed MSM nodes and then upload the compliance content using the VxBlock Central dashboard.
- If using a multisite cluster MSM VM, repeat upgrading MSM VM steps for non-seed MSM nodes in the same data center, followed by non-seed MSM nodes in the second data and so on and then upload the compliance content using the VxBlock Central dashboard.

Steps

1. Download the latest compliance policy from the Dell EMC [Download Center](#) and ensure the following:
 - Ensure that all of the XML content is in a compressed ZIP file.
 - The ZIP file must contain at least one valid XCCDF file and one valid OVAL file.
2. Log on to the VxBlock Central MSM UI.
3. Select **Upload Compliance Policies**.
4. Select the appropriate Compliance Policy file on your hard drive and click **Save**.
After uploading compliance content, rerun all compliance scans. You do not need to upload separate content for VSA or VTA as new RCM content includes VSA or VTA content.
5. Set the RCM profile and risk base profile for each of the systems to run compliance against the specified base profile.
6. Set the compliance scan schedule.
The default schedule is set to every Monday at 2:00 AM GMT.

Perform post configuration steps

The post configuration tasks to complete the upgrade of VxBlock Central.

Steps

1. Follow the Administration Guide for your Converged System to complete the following steps:
 - a. Register with Secure Remote Services.

If you are using VxBlock Central 2.0 and later version, you can configure Secure Remote Services gateway in VxBlock Central. For more information about configuring, click **Settings > Configure SRS Gateway** in VxBlock Central. For version 1.5 and earlier, see the appropriate administration guide for your Converged System.

- b. To stop processing the inventory data in CloudIQ, clear **Send Data to VxBlock Central Life Cycle Management (LCM) powered by CloudIQ**.

 **NOTE: This check box is selected by default.**

- c. Configure components for real-time alerts.
 - d. Add VMware NSX components (NSX Controller and the NSX Manager) or Red Hat Enterprise Linux components to the VxBlock Central discovery process.
2. Ensure Cisco Discovery Protocol is enabled on Cisco MDS and Cisco Nexus Switches.

- a. To check that RecoverPoint Continuous Data Protection is enabled, at the global level, type the **show cdp** command:

```
switch# show cdp
Global CDP information:
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
```

- b. If RecoverPoint Continuous Data Protection is not enabled, enable it:

```
switch> ena
switch# config t
switch(config)# cdp run
```

3. Follow the online help to complete the following steps:

- a. In the **Discovery** tab, enter the values for **Switch role** and **Managed workload type** under the added network switches and vCenters components respectively.

The entered values support in processing the inventory data in CloudIQ using VxBlock Central Life-Cycle Management.

 **NOTE: VxBlock Central takes a day to send the Switch role and Managed workload type attributes to Life-Cycle Management for inventory processing.**

- b. Create alert profiles.
- c. Configure SMTP to receive email notification for real-time alerts.
- d. Configure SNMP to forward traps to any other NMS server or SNMP trap receiver.
- e. Set up URLs for workflow configuration, VMware vRealize Orchestration, and VMware vRealize Operations instances.
- f. Configure AD settings and configure roles.

Upgrade VxBlock Central Orchestration Services

Upgrade VxBlock Central Orchestration Services to the latest RCM version.

About this task

You cannot upgrade from 1.x version to 2.x version. To upgrade from 1.x to 2.x version, install the 2.x version. You can upgrade from 2.x to later version only.

Steps

1. Download the upgrade files to install the bundle on the VxBlock Central Orchestration Services VM.
2. To take a snapshot of the VM that is deployed for VxBlock Central Orchestration Services, perform the following:
 - a. Connect to the VxBlock Central Orchestration Services VM.
 - b. To power off the VM, log in to the VxBlock Central Orchestration Services and switch to the root user by entering `sudo -I`.
 - c. Enter: `shutdown -h now`.
 - d. Log in to the VMware vSphere Client using administrative privileges.
 - e. Under **Navigation**, select **Home > Inventory > Hosts and Clusters**.
 - f. Right-click the VM for the snapshot and select **Snapshot > Take Snapshot**.
 - g. Enter a name and description for the snapshot.
 - h. If necessary, clear the check boxes to snapshot the VM memory and forget the guest file system.
 - i. Click **OK**.
 - j. After completion, power on the VM and log in.
3. Download the following files from the [Download Center](#) to a temporary location:
 - `vxcos-upgrade-service-patch-x.x.x.zip` (optional)
 - NOTE:** The service patch file enables you to view the Upgrade tab in the VxBlock Central Orchestration Services UI. You must have the Upgrade tab to perform the upgrade procedure. Download this file only if the Upgrade tab is not visible in the VxBlock Central Orchestration Services UI.
 - `vxcos-upgrade-bundle-x.x.x.zip`
4. Perform the following steps to view the **Upgrade** tab on the VxBlock Central Orchestration Services UI:

If the **Upgrade** tab is visible, then ignore the following steps and continue to step 5.

 - a. Copy the `vxcos-upgrade-service-patch-x.x.x.zip` to the `/home/ciadmin` directory.
 - b. To extract `vxcos-upgrade-service-patch-x.x.x.zip`, type:


```
sudo unzip vxcos-upgrade-service-patch-x.x.x.zip
```
 - c. To go to the patch directory, type:


```
sudo cd vxcos-upgrade-service-patch-x.x.x
```
 - d. To install the patch using the install script, type:


```
sudo python UpgradePatch.py
```
 - e. Launch VxBlock Central Orchestration Services and verify that the upgrade service is available with a status of **UP**. Verify that the **Upgrade** tab is visible in the VxBlock Central Orchestration Services UI.
5. To upgrade the VxBlock Central Orchestration Services VM, perform the following steps:
 - a. In the VxBlock Central Orchestration Services, select the **Upgrade** tab.
 - b. Click **Upload Upgrade Bundle** and select the appropriate upgrade bundle.
 - c. Select **Upload**.
 - d. Verify in the **Status** column that the upgrade bundle is `Ready to Install`.

- e. In the **Actions** column, click the install icon.
The following table explains the possible upgrade status:

Status	Description
INSTALLED	Upgrade completed without any issues.
FAILED (Rollback that is done)	Upgrade detected a problem and rolled back to one or more services version before the upgrade.
FAILED (Rollback failed)	Observed unexpected behavior post upgrade. If you receive the FAILED (Rollback Failed) status, revert to the VM snapshot taken before the upgrade and contact Dell EMC Support.

Upgrade the VxBlock Central Operations Management Pack

Upgrade the VxBlock Central Operations Management Pack.

Steps

1. Download the latest PAK file from the [Download Center](#) to install on the VMware vROPs Manager.
2. To take a snapshot of the VM that is deployed for VMware vROPs Manager, perform the following:
 - a. Power off the VM.
 - b. Log in to the VMware vSphere Client using administrative privileges.
 - c. Under **Navigation**, select **Home > Inventory > Hosts and Clusters**.
 - d. Go to the VM for which you want to take a snapshot.
 - e. Right-click the VM and select **Snapshot > Take Snapshot**.
 - f. Enter a name and description for the snapshot.
 - g. If necessary, clear the check boxes to snapshot the VM memory and forget the guest file system.
 - h. Click **OK**.
 - i. After completion, power on the VM and log in.
3. Log in to the VMware vROPs Manager as **admin**.
4. Select **Administration > Solutions > Repository**.
5. In **Other Management Packs**, click the **Add Management Pack** icon (+ sign).
6. To select the PAK file to import, click **Browse**, locate the file and click **Upload**.
7. There are two options available:
 - **Install the PAK file, even if it is already installed:** If the PAK file is already uploaded, reload the PAK file using the current file, but leave user customizations in place. Do not overwrite or upgrade the solution alerts, symptoms, recommendations, and policies.
 - **Reset Default Content:** If the PAK file was already uploaded, reload the PAK file using the current file and overwrite the solution default alerts, symptoms, recommendations, and policies with newer versions provided with the current PAK file.
8. A reset overwrites customized content. If upgrading, clone customized content before upgrading.
9. Read the **End User License Agreement**.
10. Accept the terms of the agreement, and click **Next** and **Finish**.

Install the VxBlock Central 3.0 hotfix

After you complete the upgrade to VxBlock Central Version 3.0, follow the steps in this section to install the VxBlock Central 3.0 hotfix. The hotfix addresses an issue with high CPU utilization for the VxBlock Central Core VM.

For more details on the issue this hotfix resolves see the *VxBlock Central Version 3.0 Release Notes*.

Take a snapshot of VxBlock Central Core VM

Before installing the hotfix, create a snapshot of the VxBlock Central Core VM. If you encounter problems during the install process, you can revert the VM using the snapshot.

Steps

1. Connect to the VM and power off with:

```
shutdown -h now
```

NOTE: Do not power on the VM until after you take the snapshot.

2. Log in to VMware vSphere Client using administrative privileges.
3. Under **Navigation**, select **Home > Inventory > Hosts and Clusters**.
4. Right-click the VM and select **Snapshot > Take Snapshot**.
5. Enter a name and description for the snapshot.
6. Clear the checkboxes to snapshot the VM memory. Do not include the guest file system.
7. Click **OK**.

NOTE: If you have applied the workaround for the CPU utilization issue (Knowledge Base (KB) article: 000006097), revert the VM CPU count from eight to two (two is the default VM CPU count).

- a. Power off the VxBlock Central Core VM.
 - b. Right click on the VM name and select **Settings**.
 - c. Change the CPU count to 2.
8. Power on and log in to the respective Core VM where you want to apply the hotfix.

Install the VxBlock Central 3.0 hotfix

Use this procedure to install the VxBlock Central 3.0 hotfix.

Steps

1. Download the following file from the Download Center:

```
VxBlock-Central_core_hotfix_3.0.0.0.vce
```

2. Copy the file to the `/root` directory on the Core VM.
3. Run the hotfix script for the Core VM with:

```
sh VxBlock-Central_hotfix_3.0.0.0.vce
```

The script runs and prompts you with the following:

```
Self Extracting Installer
Do you wish to install the hotfix? (yes|y)
```

4. Do one of the following:
 - Type `y` to install the hotfix.

- Type `n` to stop the hotfix installation.

Results

Once you apply the hotfix and the Core VM services run, the output is written into a logfile at:

`/opt/vce/fm/logs/hotfixApply-{date}.log` and `/opt/vce/fm/logs/hotfixApply-rpm-{date}.log`

Troubleshoot the VxBlock Central upgrade

Review log files

Log files help to resolve issues sometimes encountered during an upgrade of VxBlock Central.

The following table provides the log files for VxBlock Central upgrades:

Upgrade	Log file
Core VM	/opt/vce/fm/logs/patch-<time_stamp>.log
MSM VM	/opt/vce/logs/patch/patch-<time_stamp>.log
MSP VM	/opt/vce/msp/logs/patch-<time_stamp>.log

Recover the MSM cluster

Restore an MSM cluster using the VMware vSphere Client. Restore when an error occurs when joining nodes to the cluster or when the connectivity for one of the MSM nodes in the cluster is down.

About this task

Perform this task only during the upgrade process.

Power on MSM nodes in the reverse order that they were powered off, starting with the seed node.

Prerequisites

Verify the order that the MSM nodes were powered off. If the order is unknown, begin with the MSM nodes in the seed node of VMware vCenter.

Steps

- Power on the MSM seed node using the VMware vCenter vSphere Client. Open a console connection to the VM, and wait for the login prompt.
- Perform the following steps for each MSM node in the same data center in the reverse order from shutdown:
 - Power on the next MSM node using the VMware vCenter vSphere Client. Continue powering on each MSM node in the cluster in five minute increments.
Repeat the recovery process for every MSM node in each data center of your clustered environment.
 - After all the MSM nodes in all data centers are powered back on, on each of the MSM nodes in the clustered environment, type:


```
service tomcat restart
```
 - To check the services, type:


```
vision start
```
 - To monitor the status of the cluster, type:


```
/opt/cassandra/bin/nodetool status
```
 - After all MSM nodes are up and running in the same data center, verify that the IP address of each data center MSM node is displayed. Type:


```
rabbitmqctl cluster_status
```
- After all the nodes in all data centers are powered on, perform the following:

- a. Check the VxBlock Central dashboard to ensure you can view your Converged Systems. If not, to restart the Tomcat service, type:

```
service tomcat restart
```

- b. Check the **Compliance and Remediation** of the VxBlock Central dashboard to ensure that the compliance status is displayed. If not, type:

```
service vision-mvb-compliance restart
```

Services do not start after Core VM upgrade

System library services do not start automatically when the Core VM reboots after you upgrade VxBlock Central.

If you encounter this issue, the following messages display in the terminal window:

```
Notice: Finished catalog run in 38.85 seconds
<time-stamp>: Waiting for postgresql-9.1 to start...
<time-stamp>: Waiting for jboss to start...
<time-stamp>: Waiting for rabbitmq-server to start...
<time-stamp>: Waiting for FMServer.ear to be deployed...
<time-stamp>: Timed out after 300 seconds waiting for FMServer.ear to be deployed!
<time-stamp>: Failed!
```

1. To restart the Core VM, start an SSH session to the Core VM.
2. Log in as **root**.
3. To shut down the Core VM, type: **shutdown -h now**
4. Power on the Core VM from the VMware vSphere Client.