

Dell EMC VxBlock™ Central Version 2.1

Upgrade Guide

Document revision 1.0

September 2019

Copyright © 2019 Dell Inc. All rights reserved.

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.” DELL 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 DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell Technologies, Dell, EMC, 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.

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

Contents

Revision history	5
Introduction	6
Verify system requirements	7
Upgrade verification tasks	8
Prepare to upgrade VxBlock Central	9
Supported upgrade paths.....	9
Download VxBlock Central upgrade files.....	9
Collect the custom display names.....	10
Post-upgrade steps.....	10
VxBlock Central simplified upgrade	11
Upgrade a single MSM VM using the simplified upgrade	12
Upgrade a VxBlock Central deployment	14
Upgrade a single MSM VM.....	14
Take a snapshot of VMs.....	15
Verify that the NTP server is configured on the VM	15
Upgrade a Core VM.....	15
Upgrade the MSP VM.....	16
Upgrade the MSM VM.....	16
Remove a VM snapshot.....	16
Upgrade a single-site cluster containing multiple MSM VMs.....	17
Take a snapshot of VMs in the cluster.....	18
Verify that the NTP server is configured on the VM	18
Upgrade a Core VM.....	18
Upgrade the MSP VM.....	19
Identify the MSM VM acting as the Cassandra seed node.....	19
Upgrade an MSM VM.....	19
Remove a VM snapshot.....	20
Upgrade a multisite cluster.....	20
Take a snapshot of VMs in the cluster.....	22
Verify that the NTP server is configured on the VM	22
Upgrade the data center VMs.....	22
Remove a VM snapshot.....	25
Upgrade a Core VM	26
Take a snapshot of the Core VM.....	26
Start a Core VM upgrade.....	26
Verify a Core VM upgrade.....	28
Restart the VMware vSphere Web Client.....	28
Remove a VM snapshot.....	29
Upgrade an MSM VM	30
Configure the VMs to use the NTP server.....	30
Take a snapshot of the MSM VM.....	30
Start an MSM VM upgrade.....	31

Update the MSM credential manager service..... 32

Verify the MSM VM upgrade..... 32

Upload compliance content..... 33

Retype the custom display names..... 34

Remove a VM snapshot..... 34

Upgrade the MSP VM..... 35

Take a snapshot of the MSP VM..... 35

Start the MSP VM upgrade..... 35

Verify the MSP VM upgrade..... 36

Remove a VM snapshot..... 37

Upgrade VxBlock Central Orchestration Services..... 38

Upgrade the VxBlock Central Operations Management Pack..... 40

Troubleshoot the VxBlock Central upgrade..... 41

Recover the MSM cluster..... 41

Review log files 42

Services do not start after Core VM upgrade..... 42

Revision history

Date	Document revision	Description of changes
September 2019	1.0	Release of VxBlock Central 2.1.

Introduction

This document provides instructions for upgrading from VxBlock Central 1.0, VxBlock Central 1.5, or VxBlock Central 2.0 to VxBlock Central 2.1.

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

See the following table for information about other upgrade instructions:

To upgrade this product	See this 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

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

Verify system requirements

System, hardware, and license requirements indicate the minimum required support for 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	2.1	Base
MSM VM	12	4	250	2.1	Base
MSP VM (optional)	1	2	350	2.1	Base
VxBlock Central Orchestration Services VM	4	2	100	Download the latest file from the Download Center .	Workflow Automation
VxBlock Central Workflow Automation plug-in	N/A	N/A	N/A	Download the latest file from the Download Center .	Workflow Automation
VMware vRO (vRealize Orchestrator)	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	Advanced Analytics
VMware vRealize Operations (vROps)	Follow VMware guidelines.	N/A	N/A	7.5	Separate VMware vROps license required.

Storage requirements

Install Core VM, MSM VM, and MSP VMs on AMP-2S with VNXe storage or AMP-3S with Dell EMC Unity storage or AMP-VX with vSAN storage.

Install VxBlock Central Orchestration Services VM on AMP-3S with Dell EMC Unity and storage or AMP-VX with vSAN storage.

Hardware requirements

Consider the following when deploying VxBlock Central:

- RAM size on the AMP must be greater than or equal to 128 GB. If the RAM is less than 128 GB, upgrade the AMP to a minimum of 128 GB of RAM. Contact Dell EMC Support for assistance when upgrading the AMP.
- Use the NFS mount from the storage array for the MSP VM, where available.
- For the AMPs, VNXe3100, and VNXe3150, use the local storage capacity. You can add storage (see Cisco documentation) but doing so might add downtime.

Upgrade verification tasks

The upgrade verification tasks allow you to prepare for an uninterrupted VxBlock Central upgrade process. Perform the verification tasks before and after you upgrade VxBlock Central. These tasks include verifying the VM versions, ensuring the services are up and running, and checking the connection between the MSM VM for SLIB and the MSP VM.

About this task

Note: During the version verification process, the package version is displayed instead of the release version. The supported versions are:

- Package version: 5.1.0
- VxBlock Central release version: 2.1

Procedure

1. Use Putty (or any similar application) to get a SSH session for the VMs.
2. Log in to CLI using the root username and password.
3. For the Core VM, type the following command to verify the version, service status, discovery completion status, and the results of the last five discovery cycles:

```
echo "Checking the version information" ; getFMagentInfo ; echo -e "\nChecking the services in CORE VM" ; vision status ; 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
```

4. For the MSM VM, type the following command to verify the version, service status, credential manager CLI service status, validation of the credentials, and connection with the Cassandra database :

```
echo -e "\nChecking the version installed" ; visionver ; echo -e "\nChecking the services in MSM VM" ; vision status ; echo -e "\n" ; /opt/vce/credential-management/bin/credential-manager-cli status ; echo -e "\n" ; /opt/vce/credential-management/bin/credential-manager-cli validate ; echo -e "\nChecking the connection to Cassandra DB" ; /opt/vce/multivbmgmt/install/getConnectInfo.sh -e "select * from systeminfo.appinfo"
```

5. Type the following command to verify the connection of Core VM with MSM VM:

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

6. For the MSP VM, type the following command to verify the version, service status, communication between MSM VM and MSP VM (check for the number of RabbitMQ connections), and the MSP VM configuration file has the MSM VM hostname listed and display on the screen:

```
echo -e "\nChecking the version installed" ; visionver ; echo -e "\nChecking the status of the services in MSP VM" ; vision status ; 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 ; 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) "
```

Note: The count of RabbitMQ connections must be equal to four. If not, then no connection is established.

Prepare to upgrade VxBlock Central

The pre-upgrade tasks prepare you to upgrade to the latest version of VxBlock Central.

Verify access to the [Download Center](#). Take snapshots of the Core VM, MSM VM, or MSP VM previously deployed for Vision or VxBlock Central.

The upgrade process deploys the latest version of VxBlock Central Base option. The upgrade includes the following tasks:

1. Download required files to perform the upgrade.
2. Install an upgrade bundle on each Core VM to apply security and VxBlock Central updates. Complete the Core VM upgrade before upgrading the MSM VM.
3. Upgrade the compliance content on the Core VM and MSM VM.
4. Install an upgrade bundle on each MSM VM to apply security and VxBlock Central updates.
5. Install an upgrade bundle on the MSP VM to apply security and VxBlock Central updates.

For a single-site environment, see *VxBlock Central simplified upgrade* to upgrade Core VM, MSM VM, and MSP VM.

For a multisite environment, upgrade manually.

Related information

[VxBlock Central simplified upgrade on page 11](#)

Supported upgrade paths

Review the supported paths for upgrading VxBlock Central.

Supported upgrade paths	
	<ul style="list-style-type: none"> • Vision 3.6.2 > VxBlock Central 1.5 > VxBlock Central 2.1 • VxBlock Central 1.0 > VxBlock Central 2.0 > VxBlock Central 2.1 • VxBlock Central 1.5 > VxBlock Central 2.1 • VxBlock Central 2.0 > VxBlock Central 2.1

Note: If you are on a version of Vision that is prior to Vision 3.6.2, you can 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 and next upgrade to VxBlock Central 2.0, and then to VxBlock Central 2.1. 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.

Before you begin

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

Procedure

1. Download the `VxBlock-Central_core_upgrade-<buildnumber>.vce` file for the Core VM and copy to the `/root` directory on the Core VM.
2. Download the `VxBlock-Central_msm_upgrade-<buildnumber>.vce` file for the MSM VM and copy to the `/root` directory on the MSM VM.

3. 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 together as one file. Download the `.tar` file to use the *VxBlock Central simplified upgrade*.
4. Download the `VxBlock-Central_msp_upgrade-<buildnumber>.vce` file for the MSP VM upgrade.

Related information

[VxBlock Central simplified upgrade on page 11](#)

Collect the custom display names

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

Procedure

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.


Related tasks

[Retype the custom display names on page 34](#)

Post-upgrade steps

The post-upgrade tasks enable successful upgrade to the latest version of VxBlock Central.

Procedure

1. Follow the Administration Guide for your Converged System to complete the following steps:
 - a. Register with Secure Remote Services (SRS).
 -  **Note:** If you are using VxBlock Central 2.0 and later version, you can configure SRS gateway in VxBlock Central. For more information about configuring, click **Settings > Configure SRS Gateway** in VxBlock Central. For versions earlier than 2.1, see the appropriate *Administration Guide* for your Converged System.
 - b. Configure components for real-time alerts.
2. Follow the online help to complete the following steps:
 - a. Create alert profiles.
 - b. Configure SMTP to receive email notification for real-time alerts.
 - c. Configure SNMP to forward traps to any other NMS server or SNMP trap receiver.
 - d. Download the latest compliance policy from the Dell EMC [Download Center](#).
 - e. Set the RCM profile and risk base profile for each of the systems to run compliance against the specified base profile.
 - f. Set the compliance scan schedule. (The default schedule is set to every Monday at 2:00 AM GMT.)
 - g. Set up URLs for workflow configuration, VMware vRealize Orchestration, and VMware vRealize Operations instances.
 - h. Configure AD settings and configure roles.

VxBlock Central simplified upgrade

VxBlock Central supports a simplified upgrade process for single-site environments. It does not apply to multisite environments. MSM initiates and runs the upgrade on each of the Core VMs and MSP VMs.

After the upgrade process begins:

- Do not add any VxBlock Central Core nodes to MSM VMs.
- Do not join any additional MSM VMs to an MSM cluster.

Perform the following high-level steps for a VxBlock Central simplified upgrade on a single-site cluster with a single MSM VM:

1. *Collect the custom display names* if the system is single MSM.
2. *Take a snapshot of the VMs.*
3. *Configure the VM to use the NTP server* see *Related tasks* for more information.
Ensure you have your MSP VM IP address and VxBlock Central Core root passwords.
4. Use any SCP tool to transfer the file from your local desktop to any directory in MSM VM (preferably */root*).
5. *Upgrade a single MSM VM* to run the VxBlock Central upgrade script from MSM.
6. *Retype the custom display names.*

Related tasks

[Collect the custom display names on page 10](#)

[Take a snapshot of VMs on page 15](#)

[Configure the VM to use the NTP server on page 30](#)

[Upgrade a single MSM VM on page 12](#)

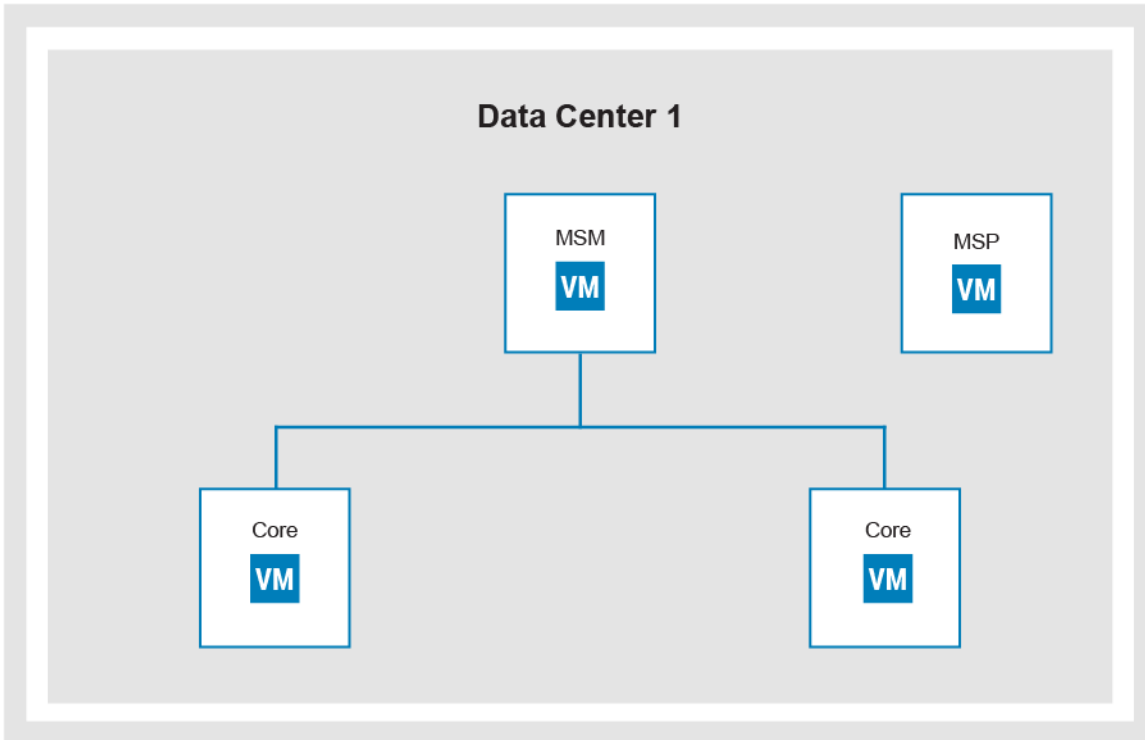
[Retype the custom display names on page 34](#)

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:



Before you begin

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.

Procedure

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.

After you finish

Retype the custom display names.

Related tasks

[Verify a Core VM upgrade on page 28](#)

[Verify the MSM VM upgrade on page 32](#)

[Verify the MSP VM upgrade on page 36](#)

[Retype the custom display names on page 34](#)

Upgrade a VxBlock Central deployment

Upgrade steps for VxBlock Central in a data center depend on whether you are using a single-site or multisite environment.

VxBlock Central has a simplified upgrade process for a single-site environment. For a multisite environment, upgrade manually.

After the VM cluster upgrade process begins:

- Do not add any Core VM nodes to MSM VMs in a cluster.
- Do not join additional MSM VMs to an MSM cluster.

Related information

[VxBlock Central simplified upgrade on page 11](#)

[Upgrade a Core VM on page 26](#)

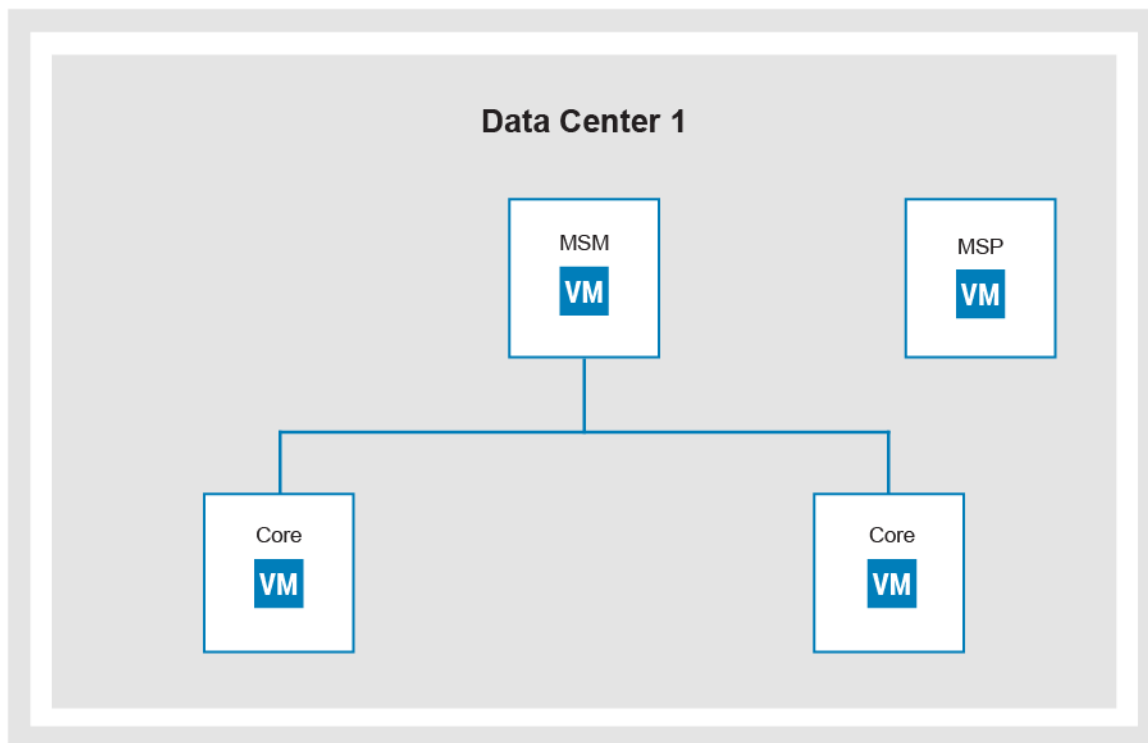
[Upgrade an MSM VM on page 30](#)

[Upgrade the MSP VM on page 35](#)

Upgrade a single MSM VM

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

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



To upgrade a single-site cluster with a single MSM VM, perform the following steps:

1. Take a snapshot of the VMs.
2. Verify that the NTP server is configured on the VM.

3. Upgrade each Core VM.
4. Upgrade the MSP VM.
5. Upgrade the MSM VM.
6. Remove the snapshots of the VMs.

Take a snapshot of VMs

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.

Procedure

1. Power off and take a snapshot of the following VMs being upgraded:
 - Each Core VM
 - MSP VM
 - Each MSM VM

Do not power on the VMs until snapshots have been taken of the other VMs.

2. Power on and log in to the following:
 - Each Core VM associated with the MSM VM.
 - MSM VM
 - MSP VM, if one is associated with the MSM VM

Related information

[Take a snapshot of the Core VM on page 26](#)

[Take a snapshot of the MSP VM on page 35](#)

[Take a snapshot of the MSM VM on page 30](#)

Verify that the NTP server is configured on the VM

Ensure that each VM is configured to use an NTP server.

Procedure

1. Check if an NTP server is configured on the Core VM, MSP VM, and MSM VM.
2. Configure the NTP server, if necessary.

Related information

[Configure the VMs to use the NTP server on page 30](#)

Upgrade a Core VM

Upgrade the Core VM.

Procedure

1. Start the Core VM upgrade.
2. Verify the Core VM upgrade.
3. Upgrade compliance content for the Core VM.

Related tasks

[Start a Core VM upgrade on page 26](#)

[Verify a Core VM upgrade on page 28](#)

Upgrade the MSP VM

Upgrade the MSP VM.

Procedure

1. Start the MSP VM upgrade.
2. Verify the MSP VM upgrade.

Related information

[Start the MSP VM upgrade on page 35](#)

[Verify the MSP VM upgrade on page 36](#)

Upgrade the MSM VM


Upgrade the MSM VM.

Before you begin

Before starting the upgrade for the MSM VM, collect the custom display names.

Procedure

1. Start the MSM VM upgrade.
2. Update the MSM credential manager service.
3. Verify the MSM VM upgrade.
4. In MSM VM, open the file: `/opt/vce/multivbmgmt/conf/cvm-config.properties`
5. At the end of the file, add the following two lines, if they are not displayed:
 - `operationSettingFileLocation = /opt/vce/multivbmgmt/conf`
 - `operationSettingFile = operations-configuration.xml`
6. Restart service `tomcat`.
7. Upload compliance content.
8. Reenter the custom display names.

 **Note:** You can use the simplified script for the single site upgrade.

Related tasks

[Collect the custom display names on page 10](#)

Related information

[Start an MSM VM upgrade on page 31](#)

[Update the MSM credential manager service on page 32](#)

[Verify the MSM VM upgrade on page 32](#)

[Retype the custom display names on page 34](#)

Remove a VM snapshot

As a best practice, 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. See VMware documentation for more information.

Procedure

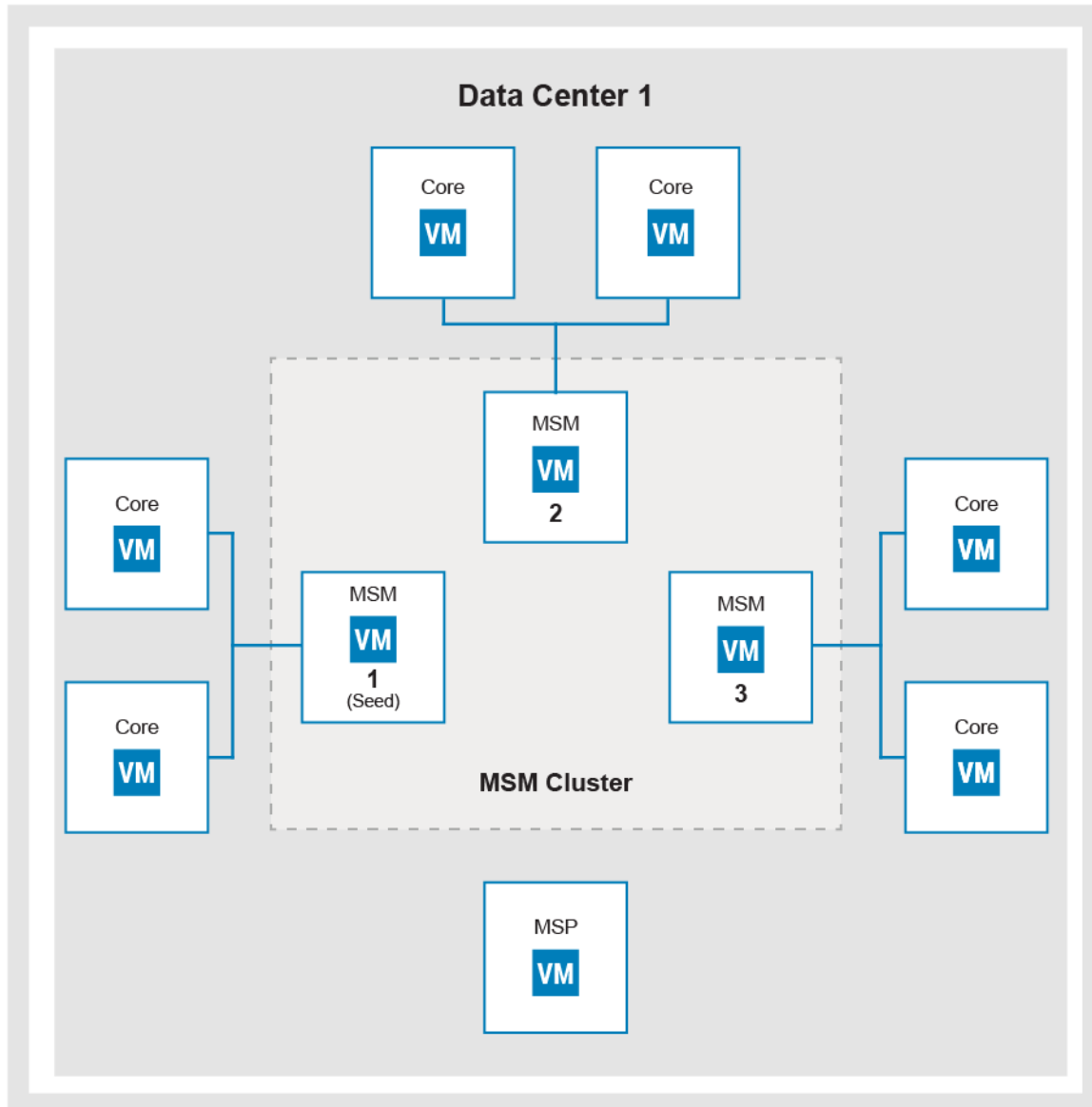
1. Go to [VMware Knowledge base](#) and search for *Article 1025279* for information about best practices for snapshots in a VMware environment.

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.

See the *VxBlock Central simplified upgrade* to upgrade for a single-site cluster.

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



The following high-level steps are required to upgrade a single-site cluster with multiple MSM VMs:

1. Take a snapshot of the VMs in the cluster in a powered-down state. Power up each in reverse sequence, in five minute intervals.
2. Identify the MSM VM acting as the Cassandra seed node.
3. Configure the NTP server.

4. Upgrade each Core VM.
5. Upgrade the MSP VM.
6. Upgrade the MSM VMs.
7. Remove the snapshots of the VMs in the cluster.

Related information

[VxBlock Central simplified upgrade on page 11](#)

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.

Procedure

1. Power off and take a snapshot of the following VMs being upgraded:
 - Each Core VM
 - MSP VM

Do not power on the VMs until snapshots have been taken of the other VMs.

2. Power off all MSM VMs in the following sequence:
 - The MSM VM that is acting as the Cassandra seed node should be the last MSM VM to be shut down.
 - Record the order in which the MSM VMs are shut down. This is used when powering on the MSM VMs.
 - Shut down the MSM VMs in the cluster one by one, in five minute intervals.

Do not power on the MSM VMs until snapshots have been taken of the other VMs.

3. In the powered-off state, take a snapshot of each MSM VM being upgraded.
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 one is associated with the cluster.

Verify that the NTP server is configured on the VM

Ensure that each VM is configured to use an NTP server.

Procedure

1. Check if an NTP server is configured on the Core VM, MSP VM, and MSM VM.
2. Configure the NTP server, if necessary.

Related information

[Configure the VMs to use the NTP server on page 30](#)

Upgrade a Core VM

Upgrade a Core VM.

Before you begin

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

Procedure

1. Start the Core VM upgrade.

2. Verify the Core VM upgrade.

Related information

[Start a Core VM upgrade on page 26](#)

[Verify a Core VM upgrade on page 28](#)

Upgrade the MSP VM

Upgrade the MSP VM.

Procedure

1. Start the MSP VM upgrade.
2. Verify the MSP VM upgrade.

Related information

[Start the MSP VM upgrade on page 35](#)

[Verify the MSP VM upgrade on page 36](#)

Identify the MSM VM acting as the Cassandra seed node

Find the MSM VM acting as the Cassandra seed node and determine the MSM VM with which to start the upgrade.

Procedure

1. Start an SSH session to any MSM VM in the cluster using the root credentials.
2. Type: `grep seeds: /opt/cassandra/conf/cassandra.yaml`

The IP address in the output is the IP address of the MSM VM acting as the Cassandra seed node. For example:
seeds: ip address

Upgrade an MSM VM

Upgrade each MSM VM.

About this task

Perform the upgrade for each MSM VM, beginning with the one acting as the Cassandra seed node. Perform the upgrade of the MSM VM cluster members sequentially.

Before you begin

Make sure that the following are complete before starting the upgrade process for the associated MSM VM cluster members:

- Upgrade of Core VMs
- Upgrade of the MSP VM

After the VM cluster upgrade process begins:

- Do not add any Core VMs to any MSM VMs in the cluster.
- Do not join any additional MSM VMs to the MSMs cluster.

Note: 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 non-upgraded MSM VMs until they are upgraded.

Note: Start the upgrade process with the MSM VM that is acting as the Cassandra seed node.

Procedure

1. Start the MSM VM upgrade.
2. Update the MSM credential manager service.
3. Verify the MSM VM upgrade.

Related information

[Identify the MSM VM acting as the Cassandra seed node on page 19](#)

[Start an MSM VM upgrade on page 31](#)

[Update the MSM credential manager service on page 32](#)

[Verify the MSM VM upgrade on page 32](#)

Remove a VM snapshot

As a best practice, 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. See VMware documentation for more information.

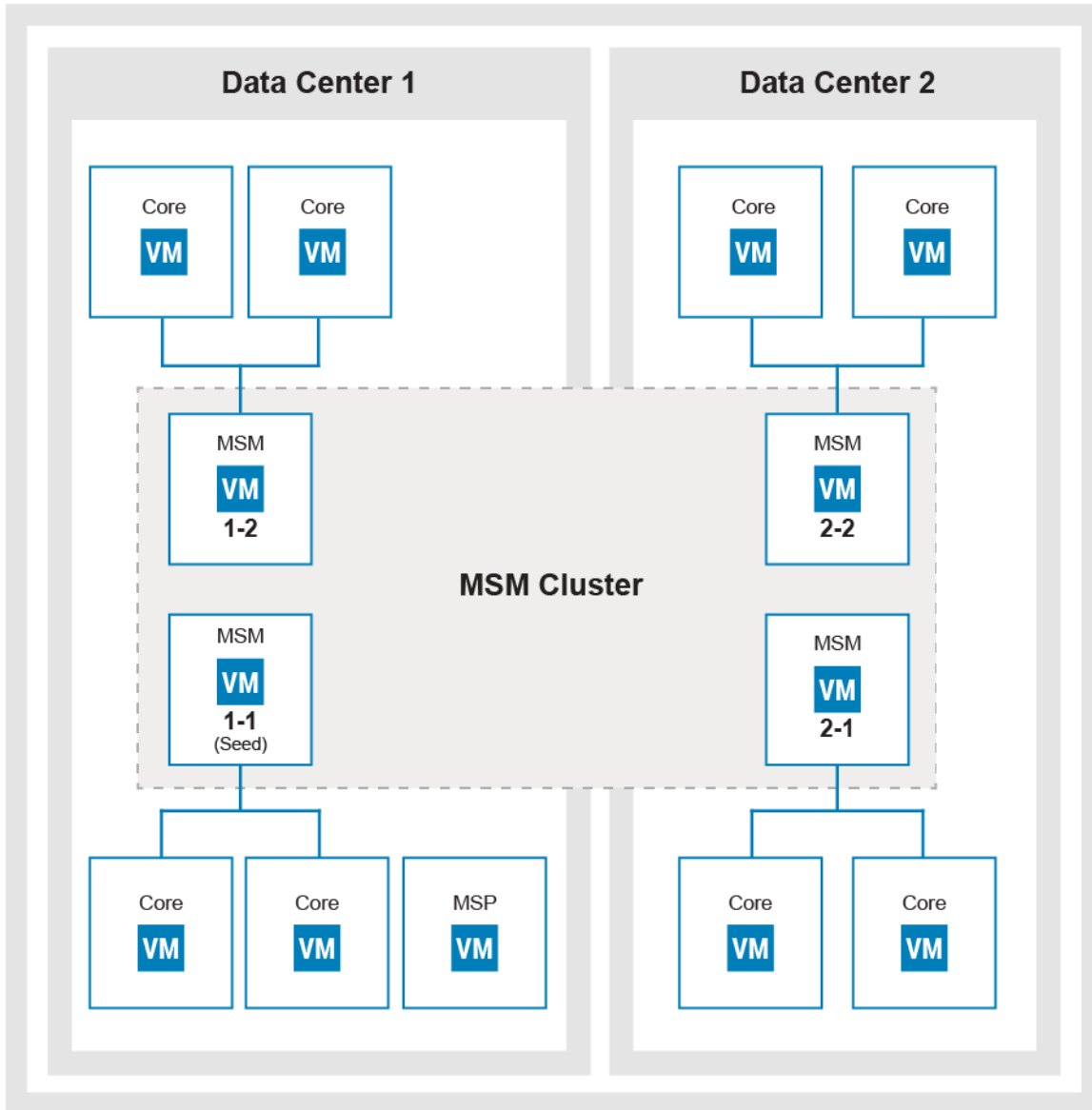
Procedure

1. Go to [VMware Knowledge base](#) and search for *Article 1025279* for information about best practices for snapshots in a VMware environment.

Upgrade a multisite cluster

Upgrade up to three data center environments, each having up to two MSM VMs. These MSM VMs can each be associated with up to two Core VMs.

The following illustration is an example of a multisite cluster data center environment:



The following high-level steps are required to upgrade a multisite cluster environment:

1. Take a snapshot of the VMs in the cluster.
2. Configure the NTP server.
3. Identify the data center.
4. Upgrade the VMs in each data center.
 - a. Upgrade each Core VM.
 - b. Upgrade the MSP VM, if present.
 - c. Upgrade each MSM VM.
5. Remove the snapshots of the VMs in the cluster.

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.

Procedure

1. Power off and take a snapshot of the following VMs being upgraded:
 - Each Core VM
 - MSP VM

Do not power on the VMs until snapshots have been taken of the other VMs.

2. Power off all MSM VMs in the following sequence:
 - The MSM VM that is acting as the Cassandra seed node should be the last MSM VM to be shut down.
 - Record the order in which the MSM VMs are shut down. This is used when powering on the MSM VMs.
 - Shut down the MSM VMs in the cluster one by one, in five minute intervals.

Do not power on the MSM VMs until snapshots have been taken of the other VMs.

3. In the powered-off state, take a snapshot of each MSM VM being upgraded.
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 one is associated with the cluster.

Verify that the NTP server is configured on the VM

Ensure that each VM is configured to use an NTP server.

Procedure

1. Check if an NTP server is configured on the Core VM, MSP VM, and MSM VM.
2. Configure the NTP server, if necessary.

Related information

[Configure the VMs to use the NTP server on page 30](#)

Upgrade the data center VMs

Upgrade the VMs in each data center starting with the data center containing the MSM VM acting as the Cassandra seed node.

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.
- Do not join more MSM VMs to the MSM cluster.

Upgrade Core VMs

The Core VMs can be upgraded across data centers before MSM VM upgrades. This process helps minimize the time between upgrading MSM VMs in different data centers.

Before you begin

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

Procedure

1. Start the Core VM upgrade.
2. Verify the Core VM upgrade.

Related information

[Start a Core VM upgrade on page 26](#)

[Verify a Core VM upgrade on page 28](#)

Upgrade the MSP VM

Upgrade the MSP VM.

Procedure

1. Start the MSP VM upgrade.
2. Verify the MSP VM upgrade.

Related information

[Start the MSP VM upgrade on page 35](#)

[Verify the MSP VM upgrade on page 36](#)

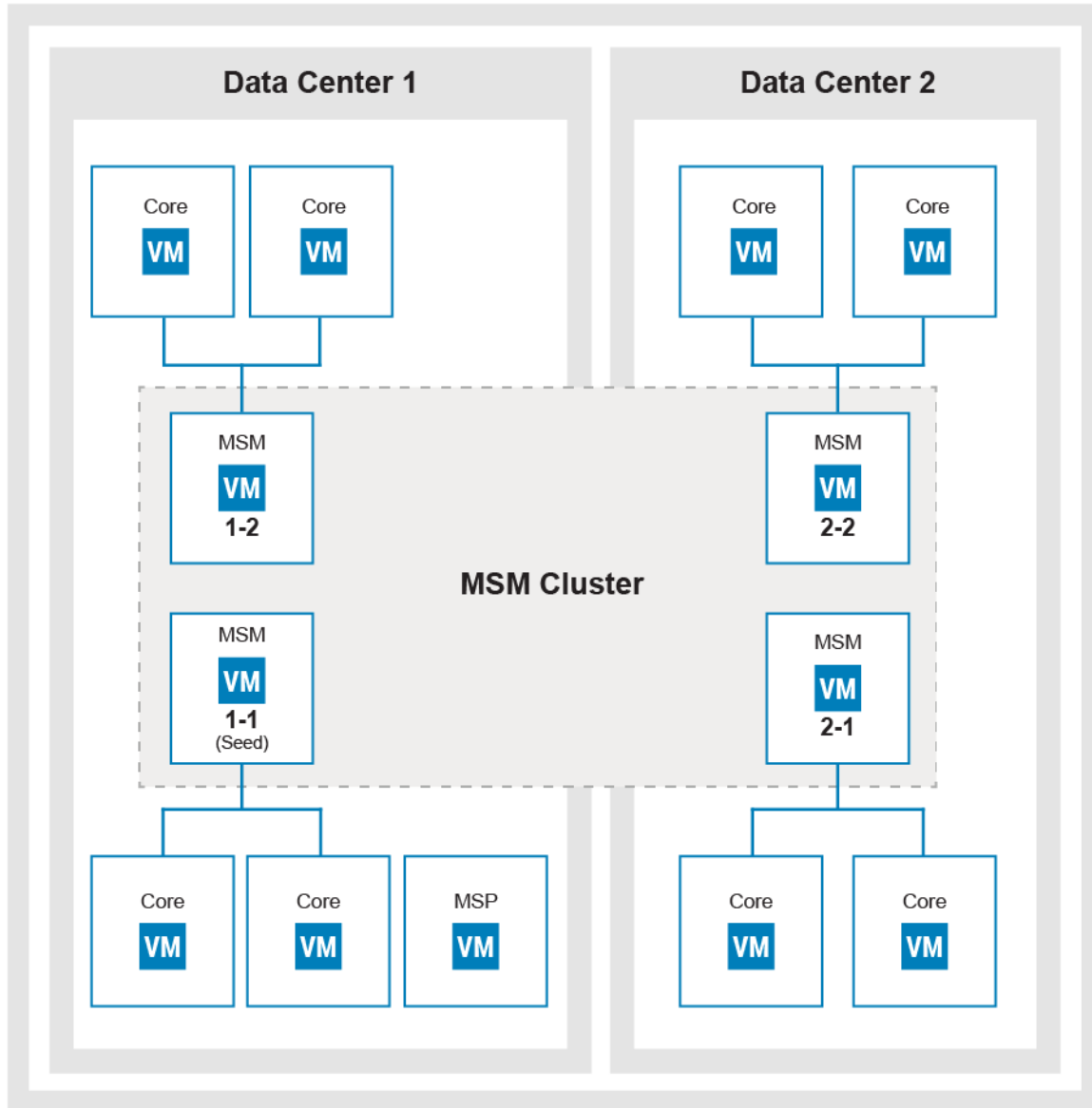
Identify the seed node in the data center

Find the seed node and determine the MSM VM with which to start the upgrade.

About this task

When the MSM cluster spans multiple data centers, perform the upgrade on each data center separately. Start the upgrade process with the MSM VM that is acting as the Cassandra seed node.

In the following illustration, the MSM VMs in data center 1 should be upgraded first, because data center 1 contains the MSM VM that is acting as the Cassandra seed node. After the MSM VMs in data center 1 are successfully upgraded, upgrade data center 2 MSM VMs.



Procedure

1. Start an SSH session to access any MSM VM in the cluster using the root credentials.
2. Type: `grep seeds: /opt/cassandra/conf/cassandra.yaml`
The IP address in the output is the MSM VM address that is acting as the Cassandra seed node.

Upgrade an MSM VM

Perform the upgrade of the MSM VM cluster members sequentially.

Before you begin

Make sure that the following are complete before starting the upgrade process for the associated MSM VM cluster members:

- Upgrade Core VMs
- Upgrade MSP VM, if one is associated with the cluster

After the MSM VM cluster upgrade process begins:

- Do not add any Core VMs to any MSM VMs in the cluster.
- Do not join any additional MSM VMs to the MSM cluster.

Note: 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 in the cluster are upgraded. Collections can temporarily fail on all nonupgraded MSM VMs until they are upgraded. This scenario means that, 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.

Note: Start the upgrade process with the MSM VM that is acting as the Cassandra seed node.

Procedure

1. Start the MSM VM upgrade.
2. Update the MSM credential manager service.
3. Verify the MSM VM upgrade.

After you finish

- Upload compliance content.
- Re-run all compliance scans. See the online help for information on compliance scans.

Related tasks

[Upload compliance content on page 33](#)

Related information

[Collect the custom display names on page 10](#)

[Identify the seed node in the data center on page 23](#)

[Start an MSM VM upgrade on page 31](#)

[Update the MSM credential manager service on page 32](#)

[Verify the MSM VM upgrade on page 32](#)

[Retype the custom display names on page 34](#)

Remove a VM snapshot

As a best practice, 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. See VMware documentation for more information.

Procedure

1. Go to [VMware Knowledge base](#) and search for *Article 1025279* for information about best practices for snapshots in a VMware environment.

Upgrade a Core VM

Complete the Core VM upgrade before you upgrade the MSM VM.

Take a snapshot of the Core VM

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

Before you begin

Connect to the Core VM.

Procedure

1. To power off the VM, type: `shutdown -h now`
2. Log in to the VMware vSphere Client using administrative privileges.
3. In the **Navigation** bar, select **Home > Inventory > Hosts and Clusters**.
4. Navigate to the VM for which you want to take a snapshot.
5. Right-click the VM and select **Snapshot > Take Snapshot**.
6. Specify a name and description for the snapshot.
7. Clear the checkboxes to snapshot the VM memory and quiesce the guest file system, if available.
8. Click **OK**.

After you finish

If the VM is not part of a cluster, power on the VM and log in.

If the VM is part of a cluster, power on the VM and log in only after the VM snapshots have been taken of the other cluster members.

Start a Core VM upgrade

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

Before you begin

1. Verify that the Core VM can be directly upgraded. Check the list of supported upgrade paths to determine which path best suits your system.
2. To validate the components and login credentials for all components in the `vblock.xml` file, type `configTool.sh -v vblock.xml`
3. Ensure that you have the following:
 - Central Authentication Service (CAS) administrator password
 - VNXe service account password

Procedure

1. Connect to the Core VM using SSH with 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
```

Where argument is one of the following 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 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_core_upgrade-<buildnumber>.vce
```

The upgrade scripts start running and then prompts you to take a snapshot.

5. Type one of the following values:

Option	Description
<code>y</code>	Proceed with the upgrade.
<code>n</code>	Stop the upgrade and take a snapshot of the Core VM.

If you type `y`, the upgrade scripts take you to the End User License Agreement (EULA) prompt

6. Type one of the following values:

Option	Description
<code>y</code>	To change the EULA agreement details before proceeding.
<code>n</code>	To continue the upgrade without changing the existing details.

If you type `y` continue with step 7. If you type `n` continue at step 8.

7. Complete the EULA acceptance. The fields in the EULA cannot exceed 500 characters or contain angle brackets.

- Scroll through the EULA until you see the `Enter Name:` prompt.
- Type your name and press **Enter**.
- Type your job title and press **Enter**.
- Type the name of the licensee company and press **Enter**.
- (Optional) Type the name of the accepting company and press **Enter**. If you do not specify an accepting company, the value defaults to the licensee company.
- Type `yes` when prompted to accept the EULA.

The script then prompts you to authenticate to the CAS (Central Authenticated Service) service, as follows:

```
timestamp: The CAS password is required to upgrade the VCE Software  
Please enter the CAS password (attempt 1 of 3):
```

g. Type the CAS password.

Note: If you enter an incorrect CAS password after three attempts, the upgrade process stops. You must then restart the upgrade.

8. When Do you want to delete existing storage volume data as it improves the performance? is displayed, type **y** or **n** as needed.
9. The system reboots and the following displays:

```
The system is going down for reboot NOW!  
VxBlock Central will now reboot to apply all updates
```

After you finish

Verify the version of the Core VM is the version that you just installed. To add VMware NSX components (NSX Controller and the NSX Manager) or Red Hat Enterprise Linux components to the VxBlock Central discovery process, see the *Administration Guide* for your system.

Verify a Core VM upgrade

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

Before you begin

Connect to the Core VM.

Procedure

1. Type the following command: `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.
Note: Wait for 30 to 45 minutes for VPLEX WAN ports to show in MSM VM.

Restart the VMware vSphere Web Client

Restart the VMware vSphere web client after you upgrade the Core VM.

Before you begin

The upgrade must be complete before you restart the VMware vSphere Web Client.

Procedure

1. Log in to the VM where VMware vSphere that is installed.

2. Go to **Administration > Deployment > System Configuration**.
3. Click **Nodes**, select the vCenter Server Appliance node and then click **Related Objects**.
4. Right-click on the service you want to restart and select **Restart**.

Remove a VM snapshot

As a best practice, 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. See VMware documentation for more information.

Procedure

1. Go to [VMware Knowledge base](#) and search for *Article 1025279* for information about best practices for snapshots in a VMware environment.

Upgrade an MSM VM

All the Core VMs must be upgraded before you start the upgrade process for the MSM VM.

Configure the VMs to use the NTP server

Configure each MSM VM and Core VM to use an NTP server. If redeploying an MSM VM, specify an NTP server IP address when configuring the server.

Before you begin

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

For each MSM VM and Core VM, perform the following steps:

Procedure

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

```
ntpdate -u <IP_address>
```

where *IP_address* is the NTP server IP address.

3. Edit `/etc/ntp.conf`.
4. Comment out the default CentOS server entries and add the following entry: `server <IP_address>`

If the lines are already commented out, skip this step and run `service ntpd status` to check if the NTP daemon is running. If the daemon is running, skip the remaining steps and move to the next VM.

5. To save the changes and start the ntpd service, type:

```
service ntpd restart
```

6. To start ntpd service on reboot, type:

```
chkconfig ntpd on
```

Take a snapshot of the MSM VM

Before upgrading, create a snapshot of the MSM VM. If you encounter problems during the upgrade process, you can revert the virtual machine using the snapshot.

 **Note:** After you revert to a snapshot, you must reboot the VM before attempting another upgrade.

Before you begin

Connect to the MSM VM.

Procedure

1. To power off the VM, type: `shutdown -h now`
2. Log in to the VMware vSphere Client using administrative privileges.
3. In the **Navigation** bar, select **Home > Inventory > Hosts and Clusters**.

4. Navigate to the VM for which you want to take a snapshot.
5. Right-click the VM and select **Snapshot > Take Snapshot**.
6. Specify a name and description for the snapshot.
7. Clear the checkboxes to snapshot the VM memory and quiesce the guest file system, if available.
8. Click **OK**.

After you finish

If the VM is not part of a cluster, power on the VM and log in.

If the VM is part of a cluster, power on the VM and log in only after the VM snapshots have been taken of the other cluster members.

Start an MSM VM upgrade

Execute the MSM VM upgrade file on the MSM VM.

Before you begin

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

Procedure

1. Connect to the MSM VM using SSH 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, to check the version, or to get help, 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.
<code>help</code>	Displays help usage.

5. To start the upgrade, type:

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

The upgrade scripts start running and then prompt you to take a snapshot.

6. Type one of the following values:

Option	Description
y	Proceed with the upgrade if you have taken a snapshot of the virtual machine.
n	Stop the upgrade and take a virtual machine snapshot.

Before proceeding with the upgrade, ensure that all Core VMs that are connected to the MSM VM being upgraded are powered on.

7. The upgrade process continues and the script displays a summary of the upgrade, as in the following example:

```
timestamp: Available disk space: 67294044160
timestamp: Patch size: 528506470
timestamp: Currently installed OVA version is 1.5.0.0
timestamp: This bundle version is 3.6.0.0-build_number
```

8. Type **y** to restart the VM.

Note: After upgrading, you need to rerun all compliance scans. 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 on compliance scans.

After you finish

Verify that the correct version of the MSM VM is installed.

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 new password.

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.

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.

Before you begin

Obtain the following information to access the dashboard:

- FQDN of the MSM VM.
- A username and password with access to the VxBlock Central dashboard.
- Google Chrome

Procedure

1. Use Google Chrome to access 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 Core VM. If it cannot, a host file entry for the Core VM must exist on the MSM VM.

2. Log in with default credentials for the dashboard.

Change this password to protect the system from unauthorized access.

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

3. Click **About** at the end of the screen and verify that the version number is correct.

Note: If the search field returns a message `Unable to execute search` when you log in to the MSM, the database rebuild has not completed. Allow 15 minutes for this process to complete and log in to the MSM VM again.

After you finish

- 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 multi-site 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.

Upload compliance content

Use the dashboard to upload and install new compliance content.

Before you begin

To install new compliance content, it must meet the following requirements:

- The compliance content must be downloaded from the Download Center.
- 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.

Procedure

1. Select **Upload Compliance Policies**.

The **Manage Compliance Policies** dialog box is displayed.

2. Select the appropriate Compliance Policy file on your hard drive and click **Save**.

After you finish

After uploading any new compliance content, rerun all compliance scans to see the latest scan results. You do not need to upload separate content for VSA or VTA as new RCM content includes VSA or VTA content.

Retype the custom display names

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

Procedure

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

Remove a VM snapshot

As a best practice, 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. See VMware documentation for more information.

Procedure

1. Go to [VMware Knowledge base](#) and search for *Article 1025279* for information about best practices for snapshots in a VMware environment.

Upgrade the MSP VM

Take a snapshot of the MSP VM

Before upgrading, power off the MSP VM and create a snapshot. Use the snapshot to revert the VM to its previous state if any problems are encountered during the upgrade process.

Before you begin

Connect to the MSP VM.

Procedure

1. To power off the VM, type: `shutdown -h now`
2. Log in to the VMware vSphere Client using administrative privileges.
3. In the **Navigation** bar, select **Home > Inventory > Hosts and Clusters**.
4. Navigate to the VM for which you want to take a snapshot.
5. Right-click the VM and select **Snapshot > Take Snapshot**.
6. Specify a name and description for the snapshot.
7. Clear the checkboxes to snapshot the VM memory and quiesce the guest file system, if available.
8. Click **OK**.

After you finish

Power on the VM and log in.

Start the MSP VM upgrade

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

Before you begin

- Verify the MSP VM can be directly upgraded. Check the list of supported upgrade paths to determine which path best suits your system.
- Connect to the MSP VM using SSH with root credentials.
- Ensure that all Core VMs connected to the MSP VM being upgraded have been powered up.

Procedure

1. Copy `VxBLOCK-Central_msp_upgrade--<buildnumber>.vce` to the `/root` directory on the MSP VM.
2. (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.

Argument	Description
<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.

- To start the upgrade, type:

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

- When prompted to take a screenshot, type one of the following values:

Option	Description
<code>y</code>	Proceed with the upgrade if you have taken a snapshot of the virtual machine.
<code>n</code>	Stop the upgrade and take a virtual machine snapshot.

- The upgrade process continues and series of messages be displayed. When you reach the end of the upgrade process, the script prompts you to restart the MSP VM.
- Type `y` to restart.

After you finish

Verify that the version of the MSP VM is the version that you installed.

Verify the MSP VM upgrade

After completing the upgrade process, verify the status of the MSP VM.

Before you begin

Connect to the MSP VM.

Procedure

- 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
```

Results

The status for each service should be displayed as `running` or provide details about running processes.

After you finish

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

Remove a VM snapshot

As a best practice, 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. See VMware documentation for more information.

Procedure

1. Go to [VMware Knowledge base](#) and search for *Article 1025279* for information about best practices for snapshots in a VMware environment.



Upgrade VxBlock Central Orchestration Services

Upgrade VxBlock Central Orchestration Services from the current version to the latest RCM version.

About this task

Download the upgrade files and install the bundle on the VxBlock Central Orchestration Services VM.


Procedure

1. Take snapshot of the VM that is deployed for VxBlock Central Orchestration Services. Perform the following:
 - a. Connect to VxBlock Central Orchestration Services VM.
 - b. To turn off the VM, login to the VxBlock Central Orchestration Services Appliance and get to the root user by entering `sudo -i` continued by entering the admin credentials and enter: `shutdown -h now`.
 - c. Log in to the VMware vSphere Client using administrative privileges.
 - d. In the **Navigation** bar, select **Home > Inventory > Hosts and Clusters**.
 - e. Navigate to the VM for which you want to take a snapshot.
 - f. Right-click the VM and select **Snapshot > Take Snapshot**.
 - g. Specify a name and description for the snapshot.
 - h. Clear the check boxes to snapshot the VM memory and quiesce the guest file system, if applicable.
 - i. Click **OK**.
 - j. After completion, turn on the VM and log in.
2. 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`
3. Perform the following steps to view the **Upgrade** tab on the VxBlock Central Orchestration Services UI:
 -  **Note:** If the **Upgrade** tab is already visible, then ignore the following steps.
 - a. Copy the `vxcos-upgrade-service-patch-x.x.x.zip` to the `/home/ciadmin` directory.
 - b. To unzip `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 install-patch-x.x.x.py
```

 -  **Note:** After successful installation of the patch, a confirmation message is displayed.

- e. Launch VxBlock Central Orchestration Services and verify that the upgrade service is available with a status as **UP**. Verify that the **Upgrade** tab is visible in the VxBlock Central Orchestration Services UI.
4. 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**.
The file is displayed in the VxBlock Central Orchestration Services UI.
 - d. Verify in the **Status** column that the upgrade bundle is *Ready to Install*.
 - e. In the **Actions** column, click the install icon to complete.


The following table explains the possible upgrade status:

Status	Description
INSTALLED	Upgrade completes without any issues.
FAILED (Rollback done)	Upgrade detects a problem and rolls back to the service(s) version prior to upgrade.
FAILED (Rollback failed)	Observes unexpected behavior post upgrade.  Note: If you receive the FAILED (Rollback Failed) status, revert to the VM snapshot taken prior to the upgrade and contact Dell EMC Support.

Upgrade the VxBlock Central Operations Management Pack

Upgrade the VxBlock Central Operations Management Pack.

Procedure

1. Download the latest PAK file from the [Download Center](#) to install on the VMware vROPs Manager.
 2. Log in to the VMware vROPs Manager as `admin`.
 3. Select **Administration > Solutions**.
 4. On the **Solutions** tab, click the **Add** icon (+ sign).
 5. To select the PAK file to import, click **Browse**, locate the file and click **Upload**.
 6. 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.
-  **Note:** A reset overwrites customized content. If upgrading, best practice is to clone customized content before upgrading.
7. Read the **End User License Agreement**.
 8. Accept the terms of the agreement and click **Next** and **Finish**.

Troubleshoot the VxBlock Central upgrade

Recover the MSM cluster

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

About this task

Perform this task only during the upgrade process.

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

Before you begin

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

Procedure

1. Power on the MSM seed node using the VMware vCenter vSphere Client. Open a console connection to the VM and wait for the log in prompt.
2. Perform the following steps for each MSM node in the same data center in the reverse order from shutdown:

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

Repeat the recovery process for every MSM node in each data center of your clustered environment.

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

```
service tomcat restart
```

- c. To check the services, type:

```
vision start
```

- d. To monitor the status of the cluster, type:

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

- e. After all MSM nodes are up and running in the same data center, verify that the IP address of each data center MSM node is displayed. Type:

```
rabbitmqctl cluster_status
```

3. After all the nodes in all data centers are powered on, perform the following:
 - a. Check the VxBlock Central dashboard to ensure you can view your Converged Systems. If not, to restart the Tomcat service, type:

```
service tomcat restart
```

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

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

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

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.