Dell EMC VxBlock™ Systems Upgrade Guide

from VMware vSphere 6.5 or VMware vSphere 6.7 to VMware vSphere 7.0

August 2021
Rev. 6

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.

Revision history

Date	Document revision	Description of changes
August 2021	6	Added boot LUN expansion procedure.
June 2021	5	Updated *Upgrade the compute VMware ESXi hosts* for the VMware ESXi server boot policy recommendation.
June 2021	4	Added support for VMware vSphere Life Cycle Management (vLCM) and updated VIB content.
May 2021	3	Removed *Change legacy boot mode to UEFI (optional)*.
April 2021	2	Updated *Support and requirements* about Cisco UCS C2xx M3 server support.
November 2020	1	Initial version

Contents

1

Introduction

Upgrade your VxBlock System from RCM releases that support VMware vSphere 6.5 and VMware vSphere 6.7 to VMware vSphere 7.0. Adhere to prerequisites and strategies to minimize system downtime.

See the RCM Portal for supported RCM releases for the VxBlock Systems.

You cannot upgrade directly from VMware vSphere 6.0 to VMware vSphere 7.0.

See the following table for upgrade instructions:

Product to upgrade	Document
VMware vSphere 6.5 to 6.7	*Dell EMC Converged System Upgrade Guide from VMware vSphere 6.0 or VMware vSphere 6.5 to VMware vSphere 6.7*
VMware vSphere 6.0 to 6.5	*Dell EMC Converged System Upgrade Guide from VMware vSphere 6.0 or VMware vSphere 6.5*
VxBlock Central	*Dell EMC VxBlock Central Upgrade Guide*
One RCM release to another within the same RCM train.	Dell EMC upgrade guide for the Converged System you must upgrade

The upgrade procedures apply to the following systems:

- VxBlock System 240
- VxBlock System 340
- VxBlock System 350
- VxBlock System 540
- VxBlock System 740
- VxBlock System 1000

The upgrade procedures apply to the following management platforms:

- AMP-2V
- AMP-2P
- AMP-2S
- AMP-3S
- AMP Central
- AMP-VX

The audience for this document includes build teams, deployment and installation personnel, Dell Technologies Sales Engineers, field consultants, advanced services specialists, and customers.

The Glossary provides terms, definitions, and acronyms.

2

Before you upgrade

Follow the practices of your company to perform upgrades.

Before you begin your upgrade, review the contents of this guide and any referenced documents.

Be familiar with the following:

- Microsoft Windows administration of the system architecture
- VM technology
- Data center operations
- VxBlock System concepts, terminology, and troubleshooting

Upgrade guidelines

Plan and prepare for the VMware vSphere 7.0 upgrade to ensure minimum impact on production traffic.

To prepare for the upgrade, follow these guidelines:

- Verify that your system has network access to the VxBlock System and the management systems.
- Perform the upgrade during a scheduled maintenance window, if possible. Schedule adequate downtime for system maintenance. Downtime applies to all virtual infrastructure hosts, servers, and VMs that are running in the environment.
- Power off VMs before upgrading to the latest recommended virtual hardware version. Restart VMs after completing the VMware Tools upgrade.
- See https://kb.vmware.com/s/article/78205 for VMware vSphere 7.0 upgrade best practices.
- Do not change the system configuration during the upgrade.
- Keep AMP-VX, AMP Central, and VxBlock System 1000 on the same RCM version.

To prepare for the upgrade, verify the following:

- The cluster where the target VMware ESXi host resides is not set to **Fully Automated DRS** during the upgrade process.
- For components in a cluster configuration, upgrade and verify the subordinate component before you upgrade the primary component. After you successfully upgrade the subordinate and primary components, verify the status of the components to ensure that there are no new alarms.
- NTP is properly configured and functioning on all upgrade-related components or services. Ensure that clocks (time, time zone, and dates) on all hosts and that AMP VMs are synchronized before beginning the upgrade.
- DNS (including type A and PTR records) and any local hosts files are properly configured for all upgrade-related components or services.
- The connection between the VMware vCSA and the domain controller is working.
- When upgrading the VNXe software used for management, check the lockdown status on all management VMware ESXi servers. If the lockdown status is enabled, disable it before upgrading and enable it after upgrading.

If there is a question regarding ability and skills, contact Software Deployment Services (SDS) to perform the upgrade.

Support and requirements

Support and requirements to upgrade to VMware vSphere 7.0 are described.

Support

VMware vSphere 7.0 supports stand-alone or integrated Cisco UCS C-Series M4 Rack Servers or higher.

VMware vSphere 7.0 does not support:

- Cisco UCS B-Series or C-Series M3 servers.
- VMware ESXi 7.0 on AMP-VX with VMware vSAN
- VMware vSphere HA with IPv6

- VMware vCenter Server Appliance (vCSA) with External PSCs. VMware vCenter Servers with External PSCs are converged to VMware vCSA with Embedded PSCs during the VMware vSphere 7.0 upgrade.

For the VxBlock System 240:

- The RCM 6.5 train supports Cisco UCS C-Series M3 Rack Servers as AMP servers and production servers.
- The RCM 6.7 train supports Cisco UCS C-Series M3 Rack Servers only as AMP servers.
- The RCM 6.7 train does not support production servers.

Plan the necessary server hardware upgrades.

Requirements

Go to VMware Docs and search for *System Requirements for the New vCenter Server Appliance* to verify that the VMware vCSA meets the hardware, required disk storage, and memory requirements. Obtain one temporary IP address on the same subnet as the VMware vCenter Server to migrate configuration and services data from the source VMware vCSA. Disable the host TPM attestation alarm definition to suppress attestation errors when TPM modules are installed but not in use.

Verify the following:

- Cisco UCS B-Series Blade Servers and Cisco UCS C-Series Rack Servers VxBlock System firmware version is compatible with VMware vSphere 7.0. See the *VxBlock System Release Certification Matrix* and the *Release Certification Matrix 7.0 Release Notes*.
- There is enough physical memory on the AMP hosts.
- All components are in a ready state and free from errors and alarms.

Upgrade to VMware NSX-T 3.0 before upgrading the VMware vCenter Server to VMware vSphere 7.0. VMware NSX-T 2.5 is not compatible with VMware vCenter Server 7.0. For more information, go to VMware Docs and search for the following:

- *NSX-T Data Center Upgrade Guide* for VMware NSX-T Upgrade procedures.
- *VMware Product Interoperability Matrices* for compatibility between VMware NSX and VMware vSphere.
- *VMware Compatibility Guide*

Expand boot LUNs

Expand the boot LUNs before you upgrade to VMware vSphere 7.0. Perform the following task before you upgrade the compute host for both VMware vLCM and interactive upgrade scenarios.

VMware vSphere 7.0 provides increased boot bank sizes and consolidated system partitions. In VMware vSphere 6.x, VMware ESXi creates the VMFS partition from the remaining space after installation. The VMFS partition is located directly behind one of the last partitions in VMware ESXi storage layout which are merged into the operating system data during the VMware vSphere 7.0 ESXi upgrade. This VMFS partition stops the growing of the VMware vSphere 7.0 ESXi partition and the boot bank and prevents the partitions from expanding to the VMware recommended sizes.

1. Repoint the scratch location from VMFS datastore to a non-VMFS location on the RAM using a command similar to the following:

   ```
   vim-cmd hostsvc/advopt/update ScratchConfig.ConfiguredScratchLocation string /tmp/scratch
   ```

   ```
   ln -sfnv /tmp/scratch /scratch
   ```
2. Reboot the server and confirm the new scratch location on a non-VMFS datastore location.
3. Delete the VMFS datastore from the Boot LUN.
4. Expand the Boot LUN from storage array to 32 GB.
5. Rescan the storage to confirm that the volume size has been expanded.

See *Upgrade VMware ESXi hosts* to complete the task.

Increase the maximum LUN per target

Increase the maximum LUN value for FC Adapter policy to 1024.

Steps

1. In Cisco UCS Manager, select **SAN** > **Policies** > **root** > **Fibre Channel Adapter Policies**.
2. Select the adapter policy of the ESXi hosts and select **Options**.

3. Set the **MAX LUN per Target** to `1024`.

   NOTE: Updating the MAX LUN may cause traffic disruption for all hosts, so update the MAX LUN before upgrading to ESXi 7.0.

4. After upgrading to ESXi 7.0, log in to VMware vCenter using the HTML5 client.
5. Select **Host** > **Manage** > **Advanced System Settings** > **Edit**.
6. In **Filter type**, set the **disk.maxLUN** to `1024` for each host.

Download VMware vSphere upgrade files

Download upgrade files for VMware vSphere 7.0. Each item is listed in the VxBlock System Release Certification Matrix (RCM) 7.0.

Download the following files on a VxBlock System from the Dell Download Center:

- VMware vCenter Server Appliance ISO
- Dell Technologies Custom ESXi ISOs (AMP and compute)

For AMP Management VMware vSphere ESXi hosts only, verify that the image does not contain PowerPath modules.

Back up the system and hosts

Back up the VxBlock System configuration and hosts.

Steps

1. See the appropriate *Administration Guide* to back up the VxBlock System configuration and hosts.
2. To back up and restore options for the VMware vCenter Server, see https://kb.vmware.com/s/article/2149237 or the *VMware vCenter Server Installation and Setup Guide*.
3. (Optional) To back up VMware vCSA 6.5 or 6.7 certificates on the AMP, see https://kb.vmware.com/s/article/2091961.
4. Inspect all hardware components to verify that there are no visible faults (amber lights). All components should be in the ready state and free from errors and alarms.
5. Take a snapshot of all VMware vSphere management VMs:
   - For VMware vSphere 6.5, see Taking a Snapshot.
   - For VMware vSphere 6.7, see Take a Snapshot of a Virtual Machine.
6. Clone the management VMs during the maintenance window.

Upgrade components to the minimum required RCM versions

Ensure the source VMware vCSA and VMware ESXi are in the minimum supported build version to upgrade to VMware vSphere 7.0. Avoid back-in-time upgrade restrictions.

See the upgrade matrix outlined in the VMware KB article: https://kb.vmware.com/s/article/67077.

Upgrade all VxBlock System components to the required versions in the VxBlock System Release 7.0 RCM to which you are upgrading.

See the respective VxBlock System *Software and Firmware Upgrade Guides* for the process and order of upgrading these components.

Prepare for the VMware vCenter Server upgrade

To prepare for the VMware vCenter Server upgrade, address the configuration requirements.

Review system requirements for the VMware vCSA in the VMware vCenter Server Upgrade Guide.

Prepare for the VMware Enhanced Link Mode upgrade

Upgrading a VxBlock System in a VMware Enhanced Link Mode (ELM) configuration with VMware vSphere 6.x requires an upgrade for any other VxBlock System joined to the same VMware SSO domain.

1. Create a backup of all VMware PSCs configured in the VMware ELM. Create simultaneous backups of all VMware PSCs and VMware vCenter Servers in the VMware ELM ring topology.
2. Record all VMware PSCs and VMware vCenter Servers participating in the same VMware SSO domain.
3. Configure NTP for all VMware PSCs.
4. Log in as `root` to the interface of each VMware PSC to verify the status.
5. Go to the **Summary** screen and verify the following:
   - The build version is correct.
   - The **Overall Health** status is **Good**.
   - The VMware SSO Domain Status is **RUNNING**.
6. If the status does not meet the conditions, do not proceed with the upgrade until each VMware PCS meets these conditions.
7. Enable SSH access to the VMware PSC.
8. Ensure the partner server is 0 changes behind. If any of the VMware PSC is not synchronized with each other, do not proceed with the upgrade until each VMware PSC displays **Partner is 0 changes behind**.

Estimate upgrade time

Review the following considerations to ensure that you provide adequate scheduled maintenance windows to complete the upgrade.

Estimates do not include the time for preparation, configuration, backup, and download. Estimated times are may differ depending on applications running on your VxBlock System. Calculate the time to upgrade the software and firmware on each component.

- For cluster configurations, include both the primary and the subordinate components in the calculated time for the component.
- Plan your upgrade maintenance windows according to your environment. Do not upgrade all hosts at the same time. Retain an adequate number of hosts in a connected state to reduce impact to production traffic.
- For each upgrade task, record the total estimated upgrade time in the *Your Calculated Time* column in the following table:

Order	Component	Minimum upgrade time (minutes)	Restart Required	Your Calculated Time
1	VMware vCSA	45	No	
2	VMware vCSA with VMware vCHA	60	No	
3	VMware ESXi hosts	35 per host	Yes	
4	VMs hardware version and VMware Tools	10	Yes	

If the VxBlock System does not have a specific component in the table, skip that component.

Upgrade to VMware vSphere 7.0

Some VxBlock System components are optional or specific to environments. If you do not have a specific component, skip that component. When the component is in a cluster configuration, upgrade the subordinate component before you upgrade the primary component.

Upgrade the AMP before you upgrade the VxBlock System. You can upgrade the AMP in a separate maintenance window. Make sure your VxBlock System is upgraded according to the RCM. See *Upgrade Converged System components to the minimum versions*.

VMware vCenter Server upgrade considerations

You cannot upgrade and migrate VMware vCenter Server 6.x on Windows to VMware vCenter Server 7.0 on Windows.

The following table provides upgrade scenarios:

Scenario	VMware vSphere 6.x	VMware vSphere 7.0
VMware vCSA with Embedded PSC	VMware vCSA 6.x with: ● Embedded PSC ● Embedded database - vPostgres ● Internal VUM	VMware vCSA 7.0 with: ● Embedded PSC ● Embedded database - vPostgres ● Internal VMware vSphere Lifecycle Manager (vLCM)
VMware vCSA with External PSC	VMware vCSA 6.x with: ● External PSC ● Embedded database - vPostgres ● Internal VUM	VMware vCSA 7.0 with: ● Embedded PSC ● Embedded database - vPostgres ● Internal vLCM

1. If there are multiple VMware vCenter Servers in the same domain, complete upgrade steps on each VMware vCenter Server.
2. If upgrading the AMP-VX or AMP Central components, first upgrade the management VMware vCSA and then upgrade all production VMware VCSAs.

If deploying, upgrading, migrating, or restoring to VMware vCSA 7.0 release fails, see Troubleshooting a vSphere Upgrade.

Upgrade sequence for VMware vSphere on the AMP

Upgrade AMP-VX and AMP Central before you upgrade the VxBlock System.

For AMP-VX or AMP Central, upgrade the VMware vSphere components in the following sequence:

1. AMP Management VMware vCenter Server
2. AMP ESXi host
3. AMP VMware vSAN cluster (AMP-VX)
4. Production VMware vCenter Server
5. Production VMware ESXi

Upgrade VMware vCSA 6.5 or 6.7 to 7.0

Upgrade VMware vCSA 6.5 or 6.7 to 7.0 with Embedded VMware PSC.

About this task

Perform this upgrade only if you can resolve the VMware vCSA FQDN using DNS. Ensure all the prerequisites of DNS with FQDN and NTP are configured according to VMware guidelines.

To upgrade the VMware vCSA, first deploy the OVA, then, set up the VMware vCSA.

Deploy the OVA

Deploy the OVA for the VMware vCSA.

Prerequisites

- See the VMware vCenter Server Upgrade Guide to verify that all prerequisites are complete.
- Identify the IP address on same subnet as the existing VMware vCSA VM for temporary assignment during the upgrade process.

Steps

1. Download the VMware vCSA installer ISO file and mount it to a network VM or physical server for the image upgrade: **`VMware-VCSA-all-version_number-build_number.iso`**
2. Confirm that the **md5sum** is correct.
3. Mount or extract the ISO image to the Element Manager VM.
4. In the vCSA installation directory, go to the **vcsa-ui-installer\win32** folder, click **installer.exe**.
5. Click **Upgrade**.
6. On the **Introduction** page, click **Next**.
7. Accept the license agreement and click **Next**.
8. Connect to the VMware vCSA that you want to upgrade.
    a. Enter the information about the source VMware vCSA and click **Connect to Source**.
    b. Enter the information about the VMware SSO administrator and root user.
    c. Enter the information about the source VMware ESXi host or VMware vCenter Server instance with the vCSA and click **Next**.

    For VMware vCSA with VMware vCHA, specify the source VMware vCSA for VMware vCenter Server instance that manages the source.

    Use the information in the following table:

Connect to source appliance	Selection
Appliance FQDN or IP address	FQDN of vCenter Server
Appliance HTTPS port	443 (default)
VMware SSO User name	administrator@vsphere.local
VMware SSO Password	SSO Password
Appliance (operating system) root password	Root password
VMware ESXi host or VMware vCenter Server name	vCenter FQDN
HTTPS port	443 (default)
User name	administrator@vsphere.local
Password	SSO password

9. Verify that the certificate warning displays the SHA1 thumbprints of the SSL certificates that are installed on the source appliance and source server. Click **Yes** to accept the certificate thumbprints.

10. For VMware vCSA with External PSC, click **Yes** to **Accept Convergence of External PSC to Embedded PSC**.
11. Connect to the target server on which you want to deploy the VMware vCSA using the following table:

Appliance deployment target	Selection
Temporary VMware ESXi host or VMware vCenter Server name	FQDN or IP address of the ESXi host
HTTPS port	443 (default)
ESXi host User name	root
SSO Password	root Password
SSL Cert	Accept SSL Cert warning

    If your AMP has VMware VDS, you cannot deploy the VMware vCSA directly on a VMware ESXi host with nonephemeral distributed virtual port groups. Port groups are not shown in the **Network** selection during OVA deployment stage. Specify the VMware vCSA as the deployment target for upgrades when VMware vCHA is enabled.

12. Select **Virtual Datacenter**.
13. At the **Select folder** page, click **Next**.
14. On the **Setup target appliance VM** page, enter a VMware vCSA name and set the **`root`** password. Click **Next**.
15. For your VMware vSphere inventory, select the **deployment size**.
16. Select the storage size and click **Next**.
17. If more than 512 LUNs and 2,048 paths to the VMware vCSA is required, set the appliance size to large or extra large.
18. From the list of datastores, select the location to store the VM configuration files and virtual drives.
19. Select **Enable Thin Disk Mode** and click **Next**.
20. See the following table to configure the temporary network for communication:

Network settings	Selection
Network	ESXi MGMT VLAN
IP Version	IPv4
IP Assignment	Static
Temporary IP Address	Temporary IP address on the ESXi MGMT subnet
Subnet Mask or Prefix Length	Subnet mask
Default Gateway	Default GW on the ESXi MGMT subnet
DNS Server	DNS server IP address

21. Click **Next**.
22. On the **Ready to complete stage 1** page, review the deployment settings and click **Finish**.
23. Click **Continue** and set up the VMware vCSA.

Set up the VMware vCSA

Set up the VMware vCSA to transfer the data from the old appliance and start the services of the new appliance.

Steps

1. On the **Introduction** page, review the details of the upgrade and click **Next**. Wait for the preupgrade check to finish.
2. On **Connect to Source vCenter Server** page, see following table to enter information:

Source VMware vCenter Server	Description
Appliance FQDN or IP address	FQDN of vCenter Server
SSO User name	administrator@vsphere.local
SSO Password	SSO password

Source VMware vCenter Server	Description
Appliance (operating system) root password	Root password
ESXi host or vCenter Server	Manages the source vCenter Server
ESXi host or VMware vCenter Server name	ESXi or vCenter FQDN
HTTPS port	443 (default)
Username	administrator@vsphere.local
Password	SSO password

NOTE: The username is `root` if ESXi is managing the source VMware vCenter Server.

3. For VMware vCSA with External PSCs, select **This is the first vCenter Server in the topology that I want to converge** and click **Next**.
4. If VMware vCenter Server is subsequent for Enhanced Linked Mode, enter the IP address of its partner VMware vCenter Server and the HTTPS port. Click **Next**.
5. On the **Select Upgrade data** page, select the data that you want to copy, and click **Next**.
6. On the **Configure CEIP** page, click **Next**.
7. On **Ready to Complete** screen check **I have backed up the source vCSA**. Click **Finish** to initiate the upgrade.
8. Click **OK** to acknowledge the shutdown warning.
9. After the upgrade is complete, log in to the VMware vCenter Server to verify that the upgrade was successful.
10. Repeat the upgrade individually for VMware vCenter Servers in the same domain.
11. Log in to the VMware vSphere HTML5 Client to validate that the VMware vCSA is operational.
12. To manually decommission External PSCs, go to VMware Docs and see *Decommission External Platform Service Controllers*.
13. To create the agreement between the first and last VMware vCenter Servers, enter:

    ```
    /usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement -2 -h <first_upgraded_vc> -H
    <last_upgraded_vc> -u administrator
    ```

    When multiple VMware vCenter Servers with External PSCs are upgraded, replication partnerships are specified between the embedded VMware vCenter Servers during the upgrade configuration. These agreements form a consecutive ring topology.

Upgrade VMware ESXi hosts

This section defines the workflow to upgrade AMP hosts and compute hosts for VMware vSphere.

Upgrade AMP VMware ESXi hosts

Upgrade VMware ESXi hosts in the AMPs using VMware vSphere Lifecycle Manager (vLCM) and the VMware VUM baseline. VMware vLCM single image upgrades are supported in VMware vSphere 7.0 U2 or later.

About this task

This does not apply to AMP-2V. Go to VMware Docs and search *Upgrade Hosts Interactively* in the *VMware ESXi Upgrade Guide*.

- Use VMware vLCM and a custom VMware AMP-specific ESXi ISO image to upgrade the VxBlock System hosts.
- When you upgrade from VMware ESXi 6.x to 7.0 with async driver VIBs, the `vmkapi DependencyError` may impact the upgrade. For more information, see https://kb.vmware.com/s/article/78389
- If your system is running RCM version 6.7.0.1 through 6.7.7.0, upgrade to RCM 6.7.7.1 or later before upgrading to VMware vSphere 7.0. RCM 6.7.7.1 includes VMware ESXi 6.7 P03, which fixes an issue with NIC ordering after upgrades.

  CAUTION: There is an issue that may impact NIC ordering after you upgrade to VMware vSphere 7.0 if systems were not previously upgraded to the VMware vSphere 6.7.7.1 RCM. The VMware ESXi 6.7 P03 build has the fix for this issue which is available in VMware vSphere 6.7.7.1 RCM, and later.
- If upgrading a non-HA AMP with a single Cisco UCS C-Series Rack Server, shut down all the AMP VMs and upgrade the Cisco UCS C-Series Rack Server interactively. Use the AMP-specific ESXi ISO image obtained in preupgrade tasks. Go to VMware Docs and search *Upgrade Hosts Interactively* in the *VMware ESXi Upgrade Guide*.

Prerequisites

To ensure that the upgrade is successful, perform the following:

- Remove any PowerPath modules.
- For VMware vSphere 6.x systems, enable CDN in the Cisco IMC to ensure predictable NIC ordering that is inline with the source VMware ESXi after you upgrade. To enable CDN support for the VIC in the Cisco IMC, perform the following:
  - For Cisco UCS C220 M4 servers, go to **Compute** > **BIOS** > **Advanced** > **LOM and PCIe Slots Configuration** > **CDN Support for VIC** for each host.
  - For Cisco UCS C220 M5 servers, go to **Compute** > **BIOS** > **Server Management** > **CDN Control**.

Temporarily disable the following settings in the **Remediation Cluster Settings**:

- VMware Distributed Power Management (DPM)
- VMware HA admission control
- VMware Fault Tolerance (FT)
- VMware DRS affinity and anti-affinity rules (if there are rule conflicts)

If the VMware vLCM displays a warning about incompatibility, confirm that the NTP client is configured and clocks are synchronized. If not, configure NTP, reboot, and rescan against the custom ISO upgrade image. See the *Dell EMC VxBlock System 1000 Administration Guide* to configure NTP.

If upgrading an VMware HA AMP, place one Cisco UCS C-Series Rack Server in maintenance mode and upgrade the VMware ESXi host.

- Verify access to the AMP VMware ESXi ISO image obtained in the preupgrade tasks.
- Use the VMware vLCM to complete the upgrade to VMware vSphere 7.0.

Steps

1. Log in to the VMware vCenter Server.
2. Record the VMware ESXi host and datastore locations of all management AMP VMs.
3. Under **Menu**, select **Lifecycle Manager**.
4. On the **Lifecycle Manager** page, select the **Imported ISOs** tab and click **Import ISOs**.
5. On the **Import ISOs** window, locate the AMP ESXi 7.0 ISO and click **Import**.

   For AMP-VX, use the custom PowerEdge AMP-VX ESXi image only.
6. After the import completes, select the **Baselines** tab and click **NEW** > **New Baseline**.
7. On the **Create Baseline** page, perform the following:
   a. Under **Name**, enter **`AMP Upgrade <RCM_version>`**.
   b. Under **Description**, enter **`AMP baseline`**.
   c. Under **Content**, select **Upgrade** and click **Next**.
8. On the **Select ISOs** page, select the AMP ESXi 7.0 ISO and click **Next**.
9. On the **Summary** page, validate the details and click **FINISH**.
10. To attach the baseline, under **Hosts and Clusters**, select **AMP Cluster**.
11. Select **Updates** > **Hosts** > **Baselines**.
12. In the **Baselines** page, scroll down to the attached baselines.
13. Under **Attached Baselines**, click **Attach Baseline** or **Baseline Group**, and then select **AMP Upgrade** baseline.
14. Under **Inventory**, select the first compute host in the compute cluster and place into maintenance mode.
    A VMware vSphere vMotion is performed on compute VMs to the other hosts in compute cluster. For AMP-VX VMware ESXi hosts, select **ENSURE ACCESSIBLITY for vSAN data migration** when entering maintenance mode.
15. Go to **Updates** > **Hosts** > **Baselines**.
16. In the **Baseline** page, click **Check Compliance**. If errors display due to VIBs (for example, NENIC, NFNIC) missing dependencies, perform the following to remove VIBs:
    a. Use SSH to access the AMP.
    b. Run the `esxcli` software VIB list and record the VIB name reported in the compliance check.

       Uninstall NENIC (VMware vSphere 6.x) and NFNIC (VMware vSphere 6.5) VIBs even if missing dependency errors do not display when upgrading to the first VMware vSphere 7.0 RCM release. This release supports VMware inbox drivers. The VMware vSphere 6.x OEM (higher version) to 7.0 Inbox (lower version) upgrade leaves the higher OEM VIBs on the previous version after upgrade. This issue is not seen with lower OEM to higher inbox version upgrades.

    c. To remove the VIBs individually on VMware vSphere 6.5, enter:

```
esxcli software vib remove --vibname=nenic
```

d. To remove the VIBs individually on VMware vSphere 6.7, enter:

```
esxcli software vib remove --vibname=nfnic

esxcli software vib remove --vibname=nenic
```

e. To remove the VIBs individually on AMP-VX, enter:

```
esxcli software vib remove --vibname=i40en

esxcli software vib remove --vibname=qedf

esxcli software vib remove --vibname=scsi-qedi
```

17. Reboot the host to complete VIB removal.
18. To change the baseline status to noncompatible from noncompliant, click **Check Compliance**.
19. Select the **AMP Upgrade** baseline and click **Remediate**.
20. In the **Remediate** window, select the host that is being upgraded and click **REMEDIATE**.
21. Accept the VMware EULA and click **OK**.
22. Verify that the VMware ESXi host successfully reconnects to VMware vCenter and exit maintenance mode.
23. Repeat Steps 13 to 22 for the other the AMP hosts.
24. Enable the following features:
    - VMware DPM
    - VMware HA admission control
    - VMware FT

Upgrade the compute VMware ESXi hosts

Load VMware ESXi ISO images into VMware vSphere Lifecycle Manager (vLCM) to create baselines and perform VMware ESXi upgrades on compute hosts. VMware vLCM single image upgrades are supported in VMware vSphere 7.0 U2, or later.

About this task

- Do not upgrade all hosts simultaneously. Keep enough hosts online to reduce impact to production traffic.
- If upgrade warnings display on the VMware vLCM, upgrade the hosts interactively. Go to VMware Docs and search for *Upgrade Hosts Interactively* in the *VMware ESXi Upgrade for VMware vSphere 7.0*.

Prerequisites

- Disable the following features in the **Remediation Cluster Settings** if in use:
    - VMware Distributed Power Management (DPM)
    - VMware HA admission control
    - VMware Fault Tolerance (FT)
    - VMware DRS affinity and anti-affinity rules (if there are rule conflicts)
- Verify that CDN is enabled in the service profile BIOS policy to ensure predictable NIC ordering that is inline with the source VMware ESXI.
- From the Cisco UCS Manager, go to: **Servers>Policies>root>Maintenance Policies>default**. Under **Properties**, select **On Next Boot** for the **Reboot Policy**.
- If the VMware vLCM displays an incompatibility warning, confirm that the NTP client is configured and clocks are synchronized. If not, configure NTP, reboot, and rescan against the custom ISO upgrade image. See the *Dell EMC VxBlock System 1000 Administration Guide* to configure NTP.

Steps

1. Log in to the VMware vCenter Server.
2. Record the VMware ESXi host and data store locations of all production compute VMs.
3. Under **Menu**, select **Lifecycle Manager**.

4. On the **Lifecycle Manager** page, select the **Imported ISOs** tab and click **Import ISOs** to upload the compute ESXi image.
5. On the **Import ISO** window, locate the compute ESXi 7.0 ISO and click **Import**.
6. After the import completes, select the **Baselines** tab and click **NEW** > **New Baseline**.
7. On the **Create Baseline** page, perform the following:
   a. Under **Name**, enter `Compute Upgrade <RCM_version>`.
   b. Under **Description**, enter `Compute baseline`.
   c. Under **Content**, select **Upgrade** and click **Next**.
8. On the **Select ISO** page, select the Compute/VxBlock ESXi 7.0 Block ISO and click **Next**.
9. On the **Summary** page, validate the details and click **FINISH**.
10. To attach the baseline, under **Hosts and Clusters**, select **Compute Cluster**.
11. Select **Updates** > **Hosts** > **Baselines**.
12. In the **Baselines** page, scroll to attached baselines.
13. Under **Attach Baselines**, click **Attach Baseline** or **Baseline Group** and select **Compute Upgrade** baseline.
14. Under **Inventory**, select the first compute host in the compute cluster and place it into maintenance mode.
    A VMware vSphere vMotion is performed on compute VMs to the other hosts in compute cluster.
15. Go to **Updates** > **Hosts** > **Baselines**.
16. In the **Baseline** page, click **Check Compliance**. If `Incompatible` is displayed due to VIBs (for example, PowerPath, NENIC, NFNIC) missing dependencies, perform the following to remove VIBs:
    a. Use SSH to access the compute hosts.
    b. Run the esxcli software VIB list and record the VIB name reported in the compliance check.
    c. To remove the VIBs individually on VMware vSphere 6.5, enter:

    ```
    esxcli software vib remove --vibname=nenic

    esxcli software vib remove --vibname=powerpath.cim.esx

    esxcli software vib remove --vibname=powerpath.lib.esx

    esxcli software vib remove --vibname=powerpath.plugin.esx
    ```

    Uninstall NENIC (VMware vSphere 6.x) and NFNIC (VMware vSphere 6.5) VIBs even if you do not see the missing dependency errors when upgrading to the first VMware vSphere 7.0 RCM release. This release supports VMware inbox drivers for compute blades. As VMware vSphere 6.x OEM (higher version) to 7.0 Inbox (lower version) upgrade leaves the higher OEM VIBs on the previous version after upgrade. This issue is not seen with lower OEM to higher inbox version upgrades.
    d. To remove the VIBs individually on VMware vSphere 6.7, enter:

    ```
    esxcli software vib remove --vibname=nfnic

    esxcli software vib remove --vibname=nenic

    esxcli software vib remove --vibname=powerpath.cim.esx

    esxcli software vib remove --vibname=powerpath.lib.esx

    esxcli software vib remove --vibname=powerpath.plugin.esx
    ```

17. Reboot the host to complete VIB removal.
18. Click **Check Compliance**. The baseline status should change from to `noncompatible` from `Non-compliant`.
19. Select the **Compute Upgrade** baseline and click **Remediate**.
20. In the **Remediate** window, select the host that is being upgraded and click **REMEDIATE**.
21. Accept the VMware EULA and click **OK**.
22. Verify that the VMware ESXi host reconnects to VMware vCenter successfully and exit maintenance mode.
23. Repeat Steps 13 to 22 for the other compute hosts.
24. Enable the following features:
    - VMware Distributed Power Management (DPM)
    - VMware HA admission control
    - VMware Fault Tolerance (FT)

Upgrade the VMware vSphere Distributed Switch

Upgrade the VMware vSphere Distributed Switch (VDS) using VMware vSphere 7.0 documentation.

Steps

1. Log in to VMware vCenter Server using `https://<fqdn-vCenter>/ui` in the browser.
2. From the *VMware vSphere Networking* Guide, perform Upgrade a vSphere Distributed Switch to a Later Version for each VMware VDS.

Upgrade the VMware vSAN disk format on an AMP-VX cluster

About this task

Upgrade the VMware vCenter Server, VMware ESXi hosts, and the vSAN disk format, in that order, to upgrade the AMP-VX cluster.

⚠ CAUTION: **Failure to follow the sequence of upgrade tasks may lead to data loss and cluster failure.**

Prerequisites

- Ensure you have a full backup of all data that is stored on the vSAN.
- Ensure that enough free space is available. The space available must equal the logical consumed capacity of the largest disk group. You need a separate disk group with the available capacity from the one you are migrating.
- Verify that the disks are in a healthy state. Go to the **Disk Management** page to verify the object status.

Once you upgrade the on-disk format, you cannot roll back software on the hosts or add certain older hosts to the cluster. See About the vSAN Disk Format

Steps

1. Go to the VMware vSAN cluster.
2. Select the **Configure** tab.
3. Under **vSAN**, select **Disk Management**.
4. Click **Pre-check Upgrade**.

   ⓘ NOTE:

   The upgrade precheck analyzes the cluster to uncover any issues that might prevent a successful upgrade. Some of the items that are checked are host status, disk status, network status, and object status. Upgrade issues are displayed in the **Disk pre-check status** text box.

5. Click **Upgrade**.

   The disk groups are upgraded one at a time. For each disk group upgrade, all data from each device is evacuated and the disk group is removed from the vSAN cluster. The disk group is then added back to vSAN with the new on-disk format.

   ⚠ WARNING: **While the upgrade is in progress, do not remove or disconnect any host, and do not place a host in maintenance mode. When any member host of a vSAN cluster enters maintenance mode, the member host no longer contributes capacity to the cluster. The cluster capacity is reduced, and the cluster upgrade might fail.**

6. Click Yes on the **Upgrade** dialog box to perform the upgrade of the on-disk format. See Upgrade vSAN Disk Format Using vSphere Client

Verify VMware vSAN disk format and cluster upgrades

Before you complete the upgrade of the disk format and VMware vSAN cluster, verify that your VxBlock System is using latest version of VMware vSphere and vSAN.

Steps

1. Go to the vSAN cluster.
2. Select the **Configure** tab, verify that the vSAN is listed.

   ⓘ **NOTE:** You can also go to the ESXi host, and select **Summary** > **Configuration**. Verify that the latest version of the ESXi host is in use.

3. Under **vSAN**, click **Disk Management**. All disks should be running version 11.0.

Update VMware tools and virtual hardware version

Upgrade the VMware tools and virtual hardware version on the AMP management VM.

Prerequisites

Perform this task during an application maintenance window to power off and reboot the VM.

ⓘ **NOTE:** Before upgrading, back up each VM.

Steps

1. Upgrade the VMware tools for the Management VMs with Windows Server operating system (Element or Fabric Manager VMs). See *Upgrade Virtual Machines and VMware Tools* in the vCenter Server Upgrade Guide.
2. Upgrade the VM hardware to latest available version for the AMP management VMs with Windows Server operating system (Element or Fabric Manager VMs). See the *Upgrade the Compatibility of a Virtual Machine Manually* in the vCenter Server Upgrade Guide.

   ⓘ **NOTE:** If upgrading the Element Manager, launch the vCenter HTML5 client from an off-platform browser.

3. Power on the VM.

4

After you upgrade

Once the upgrade is complete, perform post-upgrade tasks.

Decommission external VMware Platform Service Controllers

Decommission external VMware Platform Service Controllers (PSCs) after converging VMware vCenter upgrades with external VMware PSC. Unregister external VMware PSC services from VMware vCenter after converging to embedded VMware PSC during upgrade to vSphere 7.0.

About this task

Any products or solutions using the VMware PSC for authentication must be registered again. Register the products or solutions with the embedded VMware vCSA deployment before decommissioning the external VMware PSC.

Do not decommission an external VMware PSC until all VMware vCenter Server management nodes registered to that PSC have been converged.

Steps

1. Log in as root to the appliance shell of the upgraded VMware vCSA.
2. To identify the PSC that was managing the VMware vCSA, enter:

   ```
   /usr/lib/vmware-vmdir/bin/vdcrepadmin -f showservers -h <vCSA_FQDN> -u administrator -w
   <Administrator_Password>
   ```

3. See https://kb.vmware.com/s/article/75177 to decommission an external VMware PSC after successful converge and migration.
4. Repeat these steps to delete the remaining external VMware PSCs.

Install the VMware Enhanced Authentication plug-in

Install the VMware Enhanced Authentication plug-in.

About this task

See Install the VMware Enhanced Authentication Plug-in to install the enhanced plug-in.

Register the solution in VMware vCenter Server after the upgrade or migration

After the certificate is regenerated during the upgrade or migration, register a previously registered solution and any third-party client plug-in packages with VMware vCenter Server.

About this task

Reregister VMware vCenter extensions after an upgrade. From the vCenter Server Upgrade, go to *After Upgrading or Migrating vCenter Server>Re-register Plug-In Solution in vCenter Server After Upgrade or Migration*

Consult the vendor documentation for any solution-based VMware vCenter extensions and client plug-ins for instructions to reregister after a VMware vCenter upgrade.

Verify VMware vCenter Server Appliance

Ensure that the VMware vCenter Server components are upgraded correctly.

About this task

If the VxBlock System does not have a specific component, skip that component and proceed with the next component.

Ensure that the VMware vCenter Server Appliance (vCSA) successfully upgraded for the AMP and Converged System by verifying the following:

- VMware vCSA instances are accessible.
- Inventory data is successfully migrated.
- VMware vCSA version comply with the supported versions in the VxBlock Systems Release Certification Matrix.
- All VMware licenses are applied and are not running in evaluation mode. The **Updates** tab in VMware vSphere vCenter Server is available on the HTML5 client.
- The updated versions comply with the supported versions in the VxBlock Systems Release Certification Matrix.
- VMware vSphere ESXi build numbers on the management environment and VMware ESXi hosts comply with the supported versions in the Converged Systems Release Certification Matrix.
- There is network connectivity to virtual machines, VLAN, and VSAN, if applicable.
- The time, date, and time zones are synchronized across all VMs and hosts.

Verify compliance with the RCM

Verify that the upgraded components match the versions that are listed in the RCM.

Confirm that the Converged System components match the versions of software, firmware, and hardware listed in the *Release Certification Matrix* for your Converged System.

See the appropriate *Release Notes* for information about installing necessary patches or updates.

Install VMware vCenter Server root certificates on the web browser

Verify that root certificates are installed. If not, follow the steps to install them.

About this task

Install the trusted root certificate authority (CA) certificates. Perform this procedure on Internet Explorer (IE) only. For browsers other than Internet Explorer, see the respective browser documentation.

Steps

1. Open web browser and go to **`https://`*`<vcsa_fqdn>`***.
2. In the VMware vCenter **Getting Started** page, select **Download trusted root CA certificates** and save the file locally.
3. Unzip the downloaded files.
4. Go to the **win** folder inside the unzipped folder.
5. Right-click each `.crt` file and click **Open**.
6. In the dialog box, click **Install Certificate**.
7. Select **Local Machine** > **Next** > **Finish**.

Verify VMware ESXi advanced settings

Verify that the NFS settings are configured for optimal Converged System performance.

In VMware vSphere ESXi 7.0, the number of outstanding I/O requests with competing parameters is limited to the `MaxQueueDepth` of a device. Depending on the storage array, the system may require a change to the `Disk.SchedNumReqOutstanding` (DSNRO) on ESXi.

See the *Configure advanced settings* section of the *Administration Guide* for your Converged System.

The vStorage APIs for array integration (VAAI) primitives are enabled by default upon the initial installation of VMware vSphere ESXi. They should remain set to their current value (enabled or disabled) for all VMware ESXi hosts, except for the following conditions:

- If there is a specific reason for disabling primitives
- If there is a recall of a primitive based on outstanding issues in related software releases

The following table provides standalone array settings:

Setting	Default VMware vSphere 7.0	Dell EMC Unity	VMAX or PowerMAX	XtremIO X2
UCS FC Adapter Policy	256	default	default	1024
lun_queue_depth_per_path	32	default	default	128
Disk_SchedNumReqOutstanding	32	default	default	128
Disk_SchedQuantum	8	default	default	64
Disk_DiskMaxIOSize	32767	default	default	4 MB
XCOPY (Primitive)	4 MB	16 MB	16 MB	4 MB
XCOPY (Claim Rule)	4 MB	16 MB	240 MB	N/A
vCenter Concurrent Clones	8	default	default	Based on bricks in a cluster

The following table provides mixed array settings:

Setting	Default VMware vSphere 7.0	Dell EMC Unity with XtremIO X2	VMAX or PMAX with XtremIO X2	Dell EMC Unity and VMAX or PowerMAX with XtremIO X2
UCS FC Adapter Policy	256	default	default	default
lun_queue_depth_per_path	32	default	default	default
Disk_SchedNumReqOutstanding	32	default	default	default
Disk_SchedQuantum	8	default	default	default
Disk_DiskMaxIOSize	32767	default	default	default
XCOPY (Primitive)	4 MB	4 MB	4 MB	4 MB
XCOPY (Claim Rule)	4 MB	16 MB	240 MB	240 MB
vCenter Concurrent Clones	8	default	default	default

Create Cisco UCS adapter settings

Review and verify that the Ethernet Adapter policy and Virtual Machine Queue (VMQ) connection policies are configured in the Cisco UCS Manager using standard practices. Verify that the service profiles are updated. Create VMQ policies and apply them to the Ethernet adapters.

About this task

Verify that the policies exist and values are set as described in this procedure. If they do not exist, create them using the steps in this procedure. The steps apply only to a VxBlock System with a Cisco UCS Ethernet Adapter Policy for compute Cisco UCS B-Series Blade Servers running VMware ESXi. A service-profile that is associated with the respective compute blades uses the policy.

Steps

1. From the UCS Manager, select **Servers**.
2. Select **Policies** > **root** > **Adapter Policies**.
3. Select **Add a new Ethernet Adapter Policy** to provide a name and description (for example: VMQ-Default).
4. Under **Resources**, enter the following settings:
   - **Transmit Queues = 8** (The number of transmit queue resources to allocate.)
   - **Receive Queues = 4** (The number of receive queue resources to allocate.)
   - **Completion Queues = 12** (The number of completion queue resources to allocate. In general, allocate the number of completion queue resources equal to the number of transmit queue resources plus the number of receive queue resources.)
   - **Interrupts = 14**
5. Under **Options**, select **Enabled** for **Receive Side Scaling (RSS)**. All other values remain as default.

Create the VMQ connection configuration settings

Verify that the VMQ policies exist. If not, create them using the steps in this procedure.

Steps

1. In the **UCSM Navigation** window, click **LAN**.
2. Expand **LAN** > **Policies**.
3. Expand the node for the organization where you want to create the policy.
4. If the system does not include multitenancy, expand the root node.
5. Right-click the **VMQ Connection Policies** node and select **Create VMQ Connection Policy**.
6. In the **Create VMQ Connection Policy** dialog box, complete the following fields:
   - **Name field**: The VMQ connection policy name
   - **Number of VMQs: 16** (The number of VMQs per adapter must be one more than the maximum number of VM NICs)
   - **Number of Interrupts: 34** (The number of CPU threads or logical processors available in the server)
7. Click **OK**.

Assign a virtualization preference to a vNIC

Assign the VMQ connection policy to a vNIC.

Steps

1. In the **UCSM Navigation** window, click **Servers**.
2. On the **Servers** tab, expand **Servers** > **target service profile** > **root** > **vNICs**.
3. Select the **vNIC** name.
4. In the **Connection Policies** section, click **VMQ** and select the **VMQ Connection Policy** from the drop-down.
   In the **Properties** area, the **Virtualization Preference** for the vNIC changes to **VMQ**.

Review system security

Ensure that the VxBlock System adheres to established security settings.

The *Dell EMC VxBlock System Security Configuration Guide* and the *Dell EMC AMP Security Configuration Guide* contains security hardening controls.

The upgrade does not change security for VxBlock System. See the following links for important security considerations:

- *Status of TLSv1.1/1.2 Enablement and TLSv1.0 Disablement across VMware products*: https://kb.vmware.com/s/article/2145796
- Managing TLS Protocol Configuration with the TLS Configurator Utility

VMware vSphere 6.7 and later disables the TLS 1.0 and TLS 1.1 protocols for improved security.

> **NOTE:** Some applications only support the older protocols. To revert to the less secure TLS 1.0 and TLS 1.1 protocols, run the TLS Reconfigurator tool.

To run the tool, go the following locations:

- VMware vCenter Server Appliance: `/usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator`
- VMware vCenter Server on Windows: `%VMWARE_CIS_HOME%\TlsReconfigurator\VcTlsReconfigurator`

See the following KB article for more information: https://kb.vmware.com/kb/2147469

For security issues related to speculative execution in Intel processors, see https://kb.vmware.com/s/article/55806.

For a description of those security issues, see the following:

- *CVE-2018-3646 (L1 Terminal Fault - VMM)*
- *CVE-2018-3620 (L1 Terminal Fault - OS)*

Remove the management VMs

Power off and remove the VMs that are no longer needed.

Steps

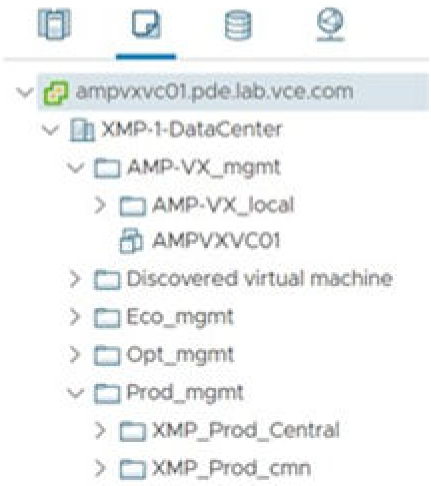
1. Power off and remove the unused management VMs from the VMware vCenter.
2. Rename the VMware vCSA from the temporary name to permanent names in VMware vSphere HTML5 client.

Validate folders for AMP-VX

Validate that the folder hierarchy is created for the placement of the VMs for the AMP-VX.

Steps

1. Log in to the management VMware vCenter using the VMware vSphere HTML5 client.
2. Select **VMs and Templates** tab.
3. Verify the following folder structure:



ampvxvc01.pde.lab.vce.com

- XMP-1-DataCenter
  - AMP-VX_mgmt
    - AMP-VX_local
    - AMPVXVC01
  - Discovered virtual machine
  - Eco_mgmt
  - Opt_mgmt
  - Prod_mgmt
    - XMP_Prod_Central
    - XMP_Prod_cmn

4. Edit the placement using the following information:

Host/VM	Primary folder	Secondary folder	Subfolder
M01VCSA01 or LCS equivalent	AMP-VX_mgmt	NA	NA
VxBlock 1000 V01VCProd01	PROD_mgmt	XMP_PROD_central	XMP_prod01

Perform a full backup of the system

After the VMware vSphere environment successfully upgrades, back up all VMware vSphere components. See the respective *Administration Guide* for your Converged System.

Update VMware tools and virtual hardware version for compute VMs

Upgrade the VMware tools and virtual hardware version on the compute VM.

About this task

Perform this task during an application maintenance window, because it requires powering off and rebooting the VM. When the upgrade is complete, power on the VM.

NOTE: Before upgrading, back up each of the VMs.

Steps

1. See Upgrade the VMware Tools Version of Virtual Machines to upgrade the VMware tools for the management VMs with Windows Server operating system (compute VMs).
2. See Upgrade the VM Hardware Compatibility of Virtual Machines to upgrade the VM hardware to Version 17 for the management VMs with Windows Server operating system (compute VMs).

Upgrade the compute VM

Upgrade the VMware tools and virtual hardware version on the compute VM.

About this task

Update the compute VM during an application maintenance window.

Prerequisites

Before you upgrade the compute VM, perform the following:

- Back up each of the compute VMs.
- Power off the compute VMs.

Steps

1. To upgrade the VMware tools for the management VMs with Windows Server operating system (compute VMs), see Upgrade the VMware Tools Version of Virtual Machines.
2. To upgrade the VM hardware to Version 17 for the management VMs with Windows Server operating system (compute VMs), see Upgrade the VM Hardware Compatibility of Virtual Machines.
3. When the upgrade is complete, power on the compute VM.