UPGRADING TO VMWARE VSPHERE 6.7

Tips and tricks for planning and executing a successful upgrade

Contents

What’s New in VMware vSphere 6.7

vSphere: The Efficient and Secure Platform for Your Hybrid Cloud

As a VMware vSphere® administrator, you know the platform can support new workloads and use cases while keeping pace with the growing needs and complexity of your infrastructure.

Now, with the wealth of new features and functionality introduced in vSphere 6.7, there’s never been a better time to upgrade. Organizations across the globe of all sizes are making the move to VMware vSphere 6.7 to easily run, manage, connect, and secure applications in a common operating environment across their hybrid cloud.

The Top 10 Reasons to Upgrade to vSphere 6.7

Why Upgrade to vSphere 6.7

vSphere 6.7 delivers key capabilities to enable IT organizations to address key trends that are placing demands on IT infrastructure:

- Explosive growth in quantity and variety of applications, from business-critical apps to new intelligent workloads
- Rapid growth of hybrid cloud environments and use cases
- On-premises data centers growing and expanding globally, including at the edge
- Security of infrastructure and applications attaining paramount importance

Simple and Efficient Management at Scale

The streamlined topology enables enhanced linked mode, so multiple VMware vCenter Server® Appliances™ can be linked together for seamless visibility. Users also benefit from 2X faster performance in vCenter operations per second, 3X reduction in memory usage, and 3X faster DRS-related operations (for example, power-on virtual machine). The introduction of Single Reboot Upgrades and VMware vSphere Quick Boot™ also reduces time required for patching and updates.

Comprehensive Built-In Security

The release of vSphere 6.7 includes the introduction of TPM 2.0, Virtual TPM, Virtualization-Based Security (VBS), Encrypted Cross-vCenter vMotion, and enhanced VM Encryption workflows.

Universal Application Platform

The vSphere Universal Application Platform supports intelligent workloads including HPC, AI, and ML. vSphere 6.7 includes enhancements to our NVIDIA GRID vCPU, VMware vSphere Persistent Memory™, Native 4Kn Disk Support, RDMA Support, and Instant Clone Technology.

Seamless Hybrid Cloud Experience

The new vCenter Server Hybrid Linked Mode enables a single pane of glass between on-premises and VMware Cloud™ on AWS environments. Workload migrations are more seamless by using Per-VM EVC and Cross-Cloud Cold and Hot Migration.

How to Make the Most of This eBook

This eBook is written for vSphere administrators looking for additional information to help plan and execute the upgrade process.

These pages contain reference scenarios that explain upgrade concepts that can be applied to nearly every situation, including upgrading from vSphere 6.0 and vSphere 6.5 to vSphere 6.7.

This eBook covers the three phases that comprise the upgrade process:

Phase 1: Pre-Upgrade
Activities to complete prior to upgrading

Phase 2: Upgrade
Identifying all components and mapping out the step-by-step upgrade process

Phase 3: Post-Upgrade
Activities to complete after completing an upgrade

Throughout this eBook are helpful resources, which also are listed in in the Resources Repository.

Phase 1: Pre-Upgrade

Phase 1: Pre-Upgrade includes the key information to be reviewed prior to beginning the upgrade process: Product Release Notes, Product Documentation, Interoperability Matrices, and the VMware Compatibility Guide. It is also important to verify the health of the environment using a health check, and to understand what is involved to perform a rollback in the event of a migration or upgrade issue.

Product Release Notes

Product Release Notes, which are published for every product released by VMware, are a key resource and must be reviewed before getting started.

Here is a summary of what you will find in the vCenter Server 6.7 Product Release Notes referenced throughout this eBook:

- **What's New** – Highlights of what is new in the current release
- **Earlier Releases of vCenter Server 6.7** – Links to release notes of previous releases
- **Patches Contained in This Release** – Links to VMware Knowledge Base documentation for patches, which contains details such as filename, build, download size, and checksums
- **Upgrade Notes for This Release** – This very important section covers incompatible upgrade or migration paths for releases, such as the inability to upgrade from vCenter Server 6.5U2 to vCenter Server 6.7
- **Resolved Issues** – Includes all resolved items in a product release, or security-related issues for a security update
- **Known Issues** – Outlines any issues to consider prior to upgrading that may impact your environment once your upgrade is complete

Product Documentation

Be sure to review product documentation prior to beginning an install, an upgrade, or patching. Product documentation contains links to product release notes, configuration maximums, vCenter and VMware ESXi™ install and upgrade guides, and more. The process to perform common tasks can change between releases, so it is helpful to review the documentation for any updated or deprecated workflows.

Find more information in the Using the VMware Product Interoperability Matrices knowledge base article KB2006028.

Interoperability Matrices

VMware Interoperability Matrices are a key component to a successful upgrade, and can help confirm that your upgrade path or product versions will be compatible when performing an upgrade.

There are three kinds of Interoperability Matrices: Product, Database, and Upgrade Path interoperability.

- Product Interoperability Matrices verify that two VMware product versions are compatible with one another.
  - **Example:** Can I run vCenter Server 6.0 Update 3 and Site Recovery Manager 8.1?
- Database Interoperability Matrices verify that when a solution requires an external database you are using a supported version and edition.
  - **Example:** Can I use Microsoft SQL Server 2016 for vCenter Server?
- Upgrade Path Interoperability Matrices validate that when doing an in-place upgrade you are executing an upgrade between supported versions.
  - **Example:** Can I upgrade from vCenter Server 6.5 Update 2 to vCenter Server 6.7?

VMware Compatibility Guide

Did you know that one of the most common reasons for a vSphere diagnostic crash is due to incompatible firmware and or driver versions? The VMware Compatibility Guide can help you to understand if your physical hardware will be compatible with the ESXi version to which you plan to upgrade. To use the tool you will first need to get the device IDs of your adapters. Knowledge Base article KB1027206 explains this process and how to obtain the driver or firmware version via the 'esxcfg' vCLI command. Once hardware details are gathered, enter them into the Hardware Compatibility Guide to review the supported versions for your hardware including the necessary firmware and drivers for any peripheral devices you may have.

Automating this process is also possible. VMware recently released a VMware Fling titled ESXi Compatibility Checker. The fling connects to a vSphere environment and automatically validates your server hardware against the VMware Hardware Compatibility Guide.

Note: Many hardware vendors maintain a separate Hardware Compatibility Guide that should be referenced during upgrade planning to ensure proper hardware compatibility.

Third-Party Solution Compatibility

Be sure to consider software from other vendors that may touch your vSphere environment, such as backup tools, monitoring tools, and other non-VMware software. Consult with the respective vendors to ensure that they are compatible with the version of vSphere to which you are planning to upgrade.

Health Checks

When performing a vSphere upgrade it is recommended to perform a health check. If an environment is not in a healthy state, errors can occur that may require a rollback.

Common mistakes that could cause a failure may be invalid DNS or NTP settings, hard disk capacity, or the possibility of a critical service that may have stopped. Being able to review the health of your vSphere environment could save time, give insight to unknown issues, as well as prevent further errors from occurring.

It is recommended that you use a health check such as VMware vRealize® Operations™, community-based tools such as vCheck, or engage VMware Professional Services or a VMware Partner for further assistance.

Backing Up Your Environment

It is crucial that you back up your vSphere environment prior to upgrading—making sure you have successful backups is key. Not only should you think about backing up Platform Service Controller(s) and vCenter Server(s), you should also be confident that all components have been backed up so as to not forget ESXi Configuration, Distributed Virtual Switches, and other VMware products like VMware NSX® or VMware Horizon®.

If leveraging the vCenter Server Appliance on vSphere 6.5 or vSphere 6.7, VMware recommends using the built-in File-Based Backup. If your environment is running vCenter Server for Windows, it's recommended to use a supported image-based backup tool. Any issues encountered during a vCenter Server migration or upgrade can easily be corrected via a rollback rather than a restore. When migrating from vCenter Server for Windows to vCenter Server Appliance (VCSA), a rollback is as simple as shutting down the newly deployed VCSA and removing it from inventory, powering on the vCenter Server for Windows, then re-joining the server back to Active Directory. When performing an upgrade from VCSA to VCSA, the rollback process is the same: Shut down the new appliance and then power-on the original.

When rolling back vCenter Server for Windows, do not rely on cached domain credentials. Make sure you have access to a local administrator account.

You should also back up the configuration of your ESXi Server. In the event you perform an upgrade or patching process and it fails that change, you will have the ability to restore the configuration from a known good backup. Currently the backup can only be triggered through CLI tools. Learn more about backing up ESXi host configurations in the VMware Knowledge Base article KB2042141.

Resources

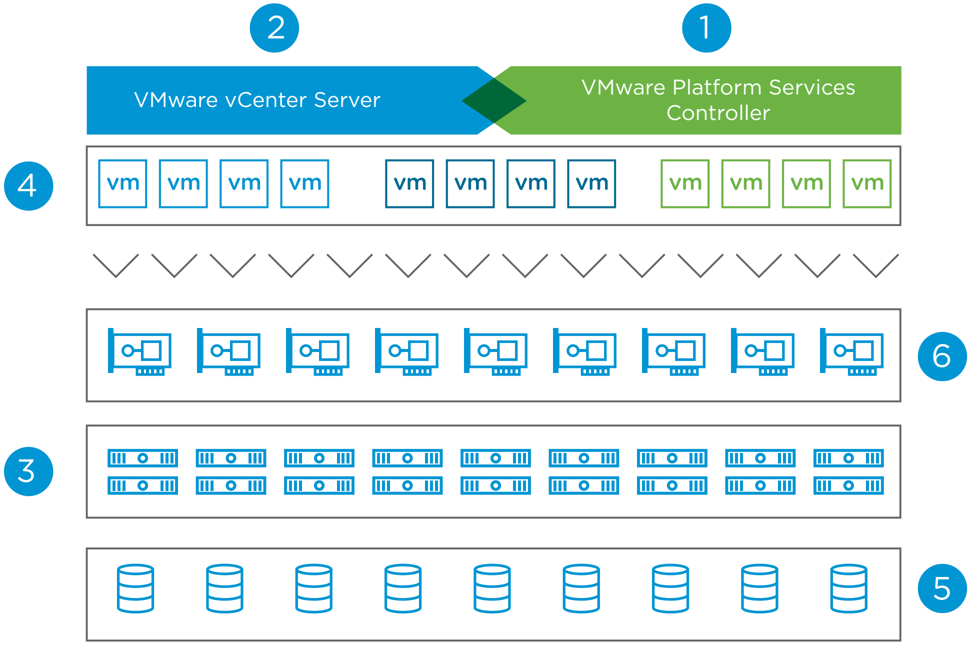
- vSphere 6.7 Upgrade FAQs on vSphere Central
- vCheck vSphere
- vSphere Optimization Assessment
- File-Based Backup Walkthrough
- VMware Professional Services – Certified members of the VMware Professional Services team are available to conduct a vSphere health check on your environment. Check with your VMware representative for more information or visit the website.

Phase 2: Upgrade

In **Phase 2: Upgrade**, we will review four sample upgrade scenarios that each include popular VMware products. Keep in mind, however, that these are not reflective of all vSphere environments.

Upgrade Process Overview

The vSphere Upgrade order of operations is an important but often overlooked process. This overview breaks down the process into the following six steps:


2
1
VMware vCenter Server
VMware Platform Services Controller
4
vm vm vm vm vm vm vm vm vm vm vm vm
6
3
5

Step 1: Platform Services Controller
Step 2: vCenter Server

Step 4: VM Tools / Compatibility

Step 6: Virtual Distributed Switch

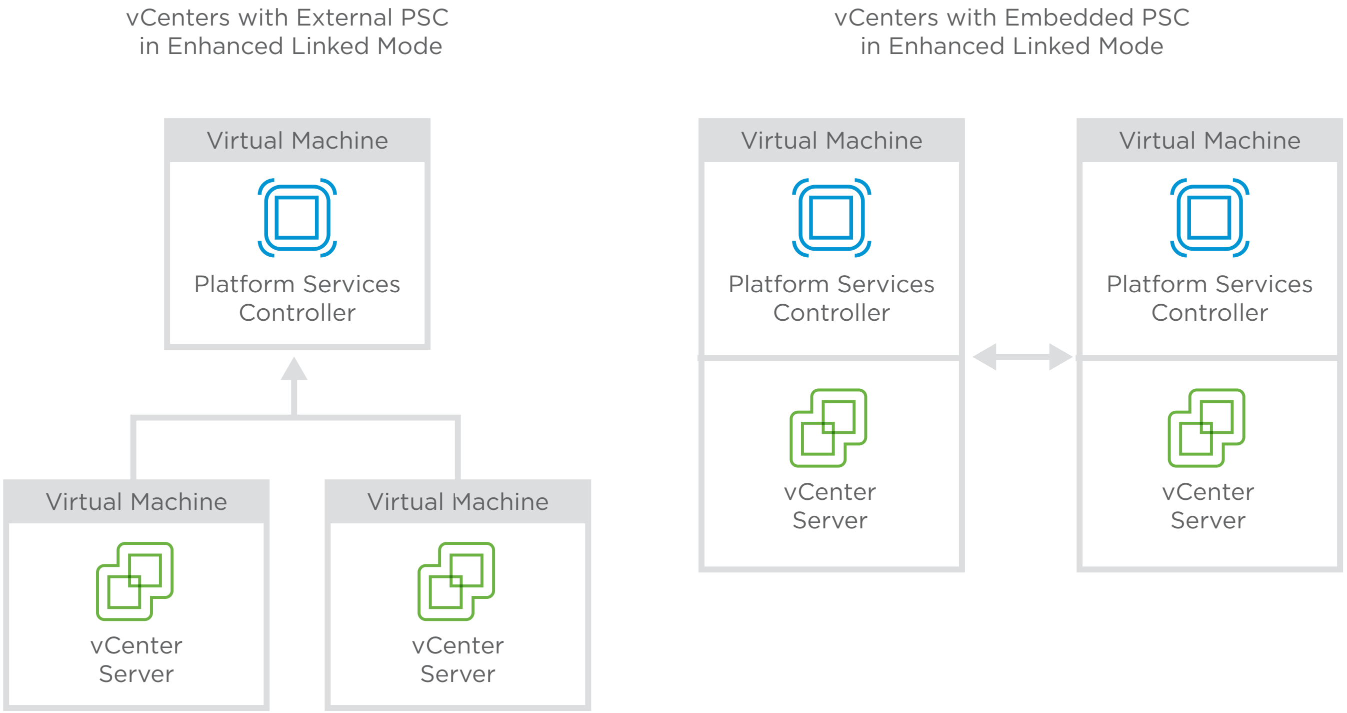
Step 3: Hypervisor - ESXi

Step 5: Storage - VMFS

Platform Services Controller and vCenter Server

Steps 1 and 2 of the vSphere Upgrade process include upgrading the Platform Services Controllers (PSC) and the vCenter Servers. Before jumping into the order of upgrades, it is necessary to explain the difference between embedded and external deployments.

Prior to vSphere 6.5 Update 2 and vSphere 6.7, enhanced linked mode required the use of an external PSC. However, the introduction of Embedded Linked Mode support means that Embedded Platform Services Controller can now be used.



If using an external PSC, then first upgrade the PSCs within the vSphere single sign-on (SSO) domain before moving on to the vCenter Server. If the topology consists of multiple external PSCs, then all PSCs within the same SSO domain must be upgraded prior to upgrading any vCenter Servers within that SSO domain.

TIP:
Platform Services Controllers and vCenter Servers must be the same vSphere version when in the same SSO domain before upgrading ESXi hosts.

BLOG POST:
Understanding the Impacts of Mixed-Version vCenter Server Deployments

When the vCenter Server is deployed in an embedded topology, the PSC is no longer another VM. Rather, it runs as a set of services within the vCenter Server. When upgrading an embedded vCenter Server, start with Step 2 and complete the upgrade of the Platform Services Controller and the vCenter Server in a single step.

Mixed versions are when vCenter Server or PSC versions do not match with each other in the environment. A mixed-version vCenter Server configuration is only supported during upgrades and not for production environments. This happens when upgrading the vCenter Server with an external PSC, and is the reason we require all external PSCs to be upgraded before starting any vCenter Server upgrades. Using vCenter Servers with embedded PSCs in enhanced linked mode is also considered a mixed-version configuration, and we recommend upgrading these within the same maintenance window if possible.

Hypervisor – ESXi Hosts

VMware ESXi hosts are upgraded as Step 3 in the overall process of a vSphere upgrade. Before upgrading your ESXi hosts, it is always best to check the hardware against the Hardware Compatibility Guide (HCL) to make sure it will be compatible with the version you are upgrading to. When upgrading ESXi hosts you have a few options to choose from, each with its own set of requirements or considerations. Upgrades for ESXi hosts can be accomplished by using:

- vSphere Update Manager (VUM)
- Interactively with a CD/DVD or USB drive
- vSphere Auto Deploy
- esxcli commands

All methods might have different requirements which should be reviewed. The recommended approach is to use vSphere Update Manager to handle the automation of patching and upgrades for hosts in your vSphere environment.

TIP:

A careful consideration is that vSphere Update Manager can only upgrade hosts to the version of vCenter Server, so if you wish to upgrade to a previous ESXi version you must use the interactive or esxcli method.

VMware Tools and VM Compatibility

VMware Tools and Virtual Machine Compatibility hold much value for virtual machines (VM) when upgraded, and caution should always be at the forefront of upgrading the VM Compatibility version. This is because upgrading the VM Compatibility version might not always be necessary, unless specific features are needed.

VMware Tools is a set of services and modules that enable several features in VMware products for better management of, and seamless user interactions with, guest operating systems. Although a guest operating system can run without VMware Tools, it is recommended that you always run the latest version of VMware Tools in your guest operating systems to access the latest features and updates. There are a few different ways to do so:

- Via the status bar of the VM, which displays a message when a new version is available
- Manually initiating an update through the VMware vSphere Client™
- Using VUM by configuring the virtual machine to check and install on reboot, or by using PowerCLI
- If using open-vm-tools on most modern major Linux distributions, these should be upgraded through the package manager of choice, such as yum or apt.

VM Compatibility determines the virtual hardware available to the VM, which corresponds to the physical hardware available on the vSphere host. Upgrading the compatibility level will allow the VM to take advantage of additional features available to the virtual machine. For example, hardware version 14, introduced with vSphere 6.7, supports 256 virtual disks as well as per-VM Enhanced vMotion Compatibility (EVC).

NOTE:

Update your VMware Tools prior to updating VM Compatibility, just in case any of the enhanced features require a newer version of drivers.

Storage – Virtual Machine File System (VMFS) Datastores

There are two versions of Virtual Machine File System (VMFS) data stores for Sphere 6.7: VMFS-5 and VMFS-6.

VMFS-6 offers several enhancements in regard to space reclamation as well as better support for larger snapshots. Just make sure prior to upgrading to VMFS-6 that all hosts have been upgraded to at least ESXi 6.5.

FEATURE / FUNCTION	VMFS6 (6.5 OR 6.7)	VMFS5 (5.X OR 6.X)
Access for ESXi 6.5 or 6.7 hosts	Yes	Yes
Access for ESXi hosts version 6.0 and earlier	No	Yes
Datastores per host	512	512
Automatic space reclamation	Yes	No
Space reclamation from guest OS	Yes	Limited
MBR storage device partitioning	No	Yes
Block size	1 MB	1 MB
Default snapshots	SEsparse	VMFSsparse (virtual disks < 2 TB SEsparse (virtual disks > 2 TB)

Upgrading from VMFS-5 to VMFS-6 requires a datastore migration, which can be done in one of two ways:

- If enough capacity exists on your existing storage array, you can create a new datastore and do a vSphere Storage vMotion of virtual machines from the old datastore to the new datastore.
- If space is limited, you can use Storage DRS to empty an existing datastore. At this point you can delete the datastore and recreate it as a VMFS-6 version. Using Storage vMotion, you can migrate those VMs and repeat until all datastores have been upgraded. This can be done manually through the GUI, or automated via a PowerCLI cmdlet that has been created for this called **Update-VMFSDatastore.**

For more information, see the VMware knowledge base article, Migrating VMFS 5 datastore to VMFS 6 datastore (KB2147824).

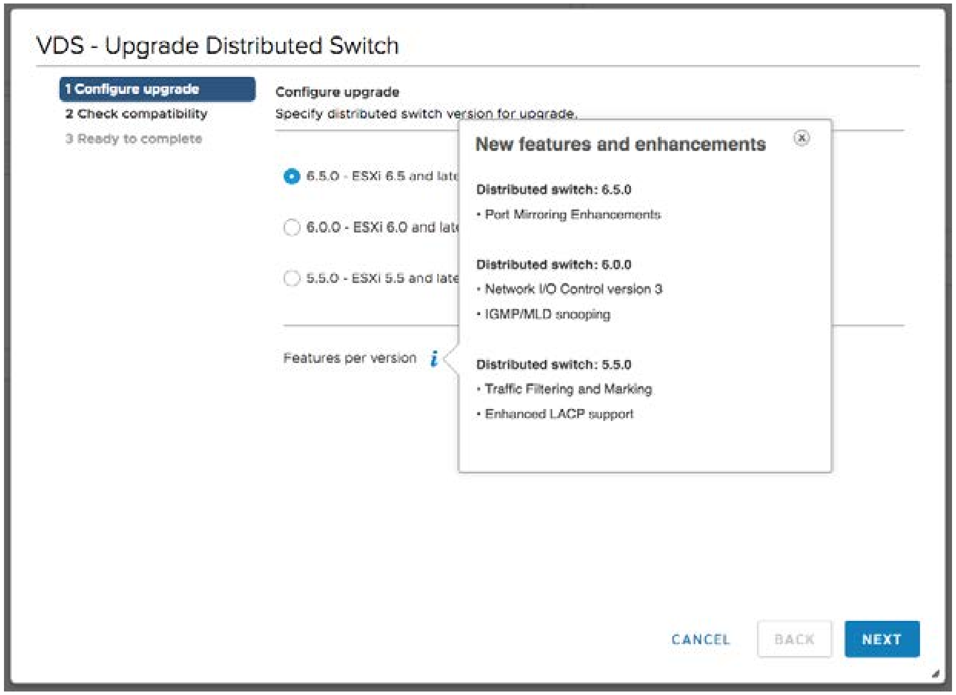
Networking – Virtual Distributed Switch (VDS)

Prior to upgrading to vSphere 6.7, it is necessary to ensure that the Virtual Distributed Switch has been upgraded to at least a 6.x version. Otherwise the upgrade will fail.

There are three options available when creating or updating a virtual distributed switch on vSphere 6.7:

1. vSphere 6.0
2. vSphere 6.5
3. vSphere 6.6

Most updates to networking have been within ESXi itself, but some features require upgrading your VDS as outlined previously. Please keep in mind that once you have upgraded your vCenter and ESXi versions, you must make sure to also update your VDS to the latest version to have the latest features available.



VDS - Upgrade Distributed Switch

1 Configure upgrade
2 Check compatibility
3 Ready to complete

Configure upgrade
Specify distributed switch version for upgrade.

● 6.5.0 - ESXi 6.5 and late
○ 6.0.0 - ESXi 6.0 and late
○ 5.5.0 - ESXi 5.5 and late

Features per version

New features and enhancements

Distributed switch: 6.5.0
- Port Mirroring Enhancements

Distributed switch: 6.0.0
- Network I/O Control version 3
- IGMP/MLD snooping

Distributed switch: 5.5.0
- Traffic Filtering and Marking
- Enhanced LACP support

Upgrading to VDS version 6.0 or 6.5 can be done with no disruption. However, upgrading to VDS version 6.6 requires some additional steps.

Find out more about upgrading to VDS version 6.6 in the VMware knowledge base article, Known issues while upgrading to DVS version 6.6 (52621).

Note that there is not a version 6.7 of VDS because vSphere 6.7 is based on similar code as VMware Cloud on AWS and there were no new features introduced for a version change.

Upgrade Components

A successful vSphere upgrade includes the following five steps:

1. **Environment Discovery and Assessment** – It is important that we properly discover all components and their associated current version and upgrade version within our vSphere environment.
2. **Requirements and Decision** – Another key component of a successful upgrade is to meet with stakeholders and compile a list of requirements that could impact our decisions. This could include SSO domain architecture, as well as introducing any new features such as enhanced linked mode of VMware vCenter Server High Availability.
3. **Compatibility** – In Step 1, it was important that we properly discovered all of our components. Once we have gathered that data, it is important to use the Interoperability Matrices to ensure compatibility.
4. **Upgrade Order** – Once we have discovered our environment, met with stakeholders to identify requirements, and validated our version compatibility, the next step is to plan our upgrade order. This can be validated using our KB on the update sequence for vSphere and its supported products.
5. **Validation** – Last but not least, to understand we had a successful upgrade, we want to make sure it is validated. Here we can follow some of the health assessment steps we performed in our pre-upgrade check to make sure everything is still functioning as needed.

Resources

- Distributed Switch documentation
- Upgrading ESXi Hosts

Scenario 1: Migrating vCenter Server for Windows from vSphere 6.0 Update 3 to vCenter Server Appliance, vSphere 6.7 Update 1

Environment Discovery and Assessment

In this scenario, the customer is currently running vSphere 6.0 Update 3 using the vCenter Server for Windows with vSphere Update Manager (VUM) co-installed with the vCenter Server. The VUM server and all ESXi hosts in this environment are currently at vSphere 6.0 Update 3.

The SSO topology is embedded with no external single sign-on (SSO) servers within this environment.

Requirements and Decision

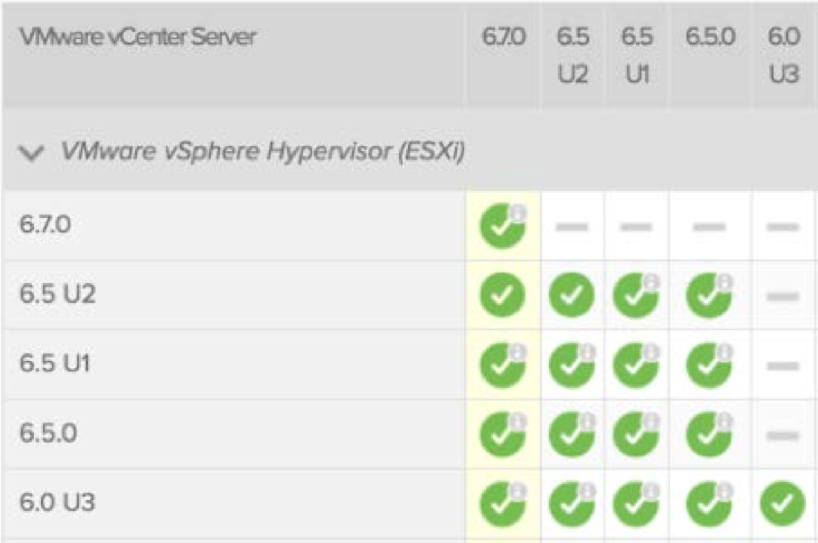
During the discovery phase, we were able to identify the current versions of vCenter Server, vSphere Update Manager (VUM), and ESXi in the environment. The customer is currently running the vCenter Server for Windows and will need to plan a vCenter Server migration to the appliance (VCSA).

A VUM migration will save the current baselines and move them to the VCSA for use later. No installation files (VIBs, ISOs, etc.) will be migrated during this process as that would only increase the upgrade and migration times.

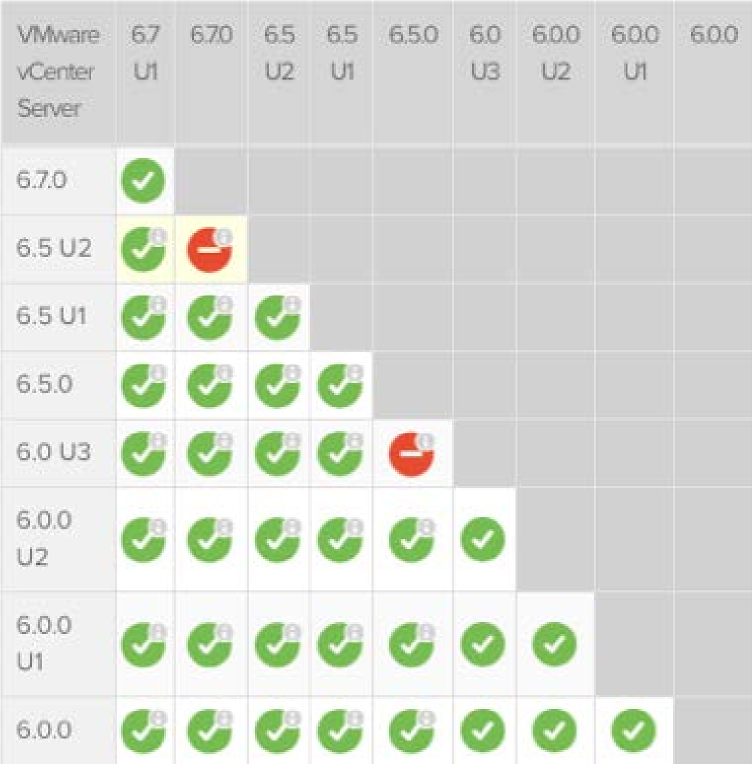
PRODUCT	CURRENT VERSION	UPGRADE VERSION
vCenter Server for Windows	6.0 Update 3	6.7 Update 1
vSphere Update Manager	6.0 Update 3	6.7 Update 1
ESXi	6.0 Update 3	6.7 Update 1

Compatibility

Making sure all products are compatible is the best way to have a successful upgrade the first time. Failure to confirm product interoperability can lead to issues during and after upgrades that could also result in requiring a rollback of systems.



VMware vCenter Server	6.7.0	6.5 U2	6.5 U1	6.5.0	6.0 U3
VMware vSphere Hypervisor (ESXi)					
6.7.0	✓	—	—	—	—
6.5 U2	✓	✓	✓	✓	—
6.5 U1	✓	✓	✓	✓	—
6.5.0	✓	✓	✓	✓	—
6.0 U3	✓	✓	✓	✓	✓



VMware vCenter Server	6.7 U1	6.7.0	6.5 U2	6.5 U1	6.5.0	6.0 U3	6.0.0 U2	6.0.0 U1	6.0.0
6.7.0	✓								
6.5 U2	✓	⛔							
6.5 U1	✓	✓	✓						
6.5.0	✓	✓	✓	✓					
6.0 U3	✓	✓	✓	✓	⛔				
6.0.0 U2	✓	✓	✓	✓	✓	✓			
6.0.0 U1	✓	✓	✓	✓	✓	✓	✓		
6.0.0	✓	✓	✓	✓	✓	✓	✓	✓	

Upgrade Order

Upgrade order is once again an important piece of the upgrade process. Upgrade vCenter Server first, before upgrading the ESXi hosts. Because VUM is now part of the vCenter Server Appliance (VCSA), it will be part of the vCenter Server upgrade and migration. The vCenter Server in this environment is running on Windows, so this will require a vCenter Server Migration to the vCenter Server Appliance.

To begin our upgrade, we will download and mount the vCenter Server Appliance installer ISO to our management machine. Using the ISO we will run the installer, which launches the workflow to migrate our vCenter Server for Windows to the new vCenter Server Appliance. When the migrate wizard is finished, the installer deploys a new appliance using a temporary IP. It will then export data from the Windows vCenter Server instance and import it into the new vCenter Server Appliance. At this point, the appliance is reconfigured to use the same information such as the FQDN, IP, certificates, and all reference IDs.

The next step is to import the ESXi ISO into vSphere Update Manager and create an upgrade baseline to remediate our hosts to the latest version.

When hosts are upgraded to ESXi 6.7, we will upgrade our distributed switch version to vSphere 6.6. Now the vSphere upgrade is complete and we can move to validation.

Validation

A complete vSphere health assessment was completed prior to executing the upgrade and migration. The environment running vSphere 6.0 Update 3 was reviewed for any issues, as well as for the presence of third-party tools or VMware products such as VMware Site Recovery Manager™ (SRM) or View Composer. Any discovered products were noted to be externalized prior to executing the upgrade.

To validate the upgraded environment, we perform the same tasks using the vSphere health assessment tool make sure no new faults exist within your vSphere 6.7 Update 1 environment. It is also a good practice to rename the original vCenter Server for Windows that was migrated to the VCSA, and also remove or disconnect the network card of the virtual machine to mitigate the risk of any accidental power operations.

If any issues are encountered during validation, you have some options. Depending on the severity of the issue and the time in your maintenance window, you can open a support case with Global Support Services (GSS). An alternate solution might be to initiate a rollback, but remember that this might be more impactful because the entire environment has been upgraded at this point.

Scenario 2: Upgrading vCenter Server Appliance from vSphere 6.5 Update 2 to vSphere 6.7 Update 1

Environment Discovery and Assessment

In this scenario, the customer is currently running vSphere 6.5 Update 2 with vCenter Server High Availability. The current version of all ESXi hosts is also 6.5 Update 2.

The SSO topology is embedded with no external single sign-on (SSO) servers within this environment.

PRODUCT	CURRENT VERSION	UPGRADE VERSION
vCenter Server Appliance	6.5 Update 2	6.7 Update 1
ESXi	6.5 Update 2	6.7 Update 1

Requirements and Decision

Requirements for this environment are simple as they are already in their preferred topology and configuration. Because this environment was previously backed up with the file-based backup and restore, the administrator must make sure to reconfigure the backup jobs using the new built-in scheduler.

Also, becase our vCenter Server 6.5 was configured for vCenter Server HA, we must make sure we understand the proper procedure. When updating to vSphere 6.7 Update 1, we now have the logic to detect if vCenter Server HA is enabled. If it is enabled, we will automatically disable vCenter Server HA, perform the upgrade, and then re-enable vCenter Server HA when the upgrade is complete. However, when upgrading to vSphere 6.7 GA, we must make sure that we first destroy our vCenter Server HA cluster as it is not supported to upgrade a vCenter Server HA cluster in place with that release. If using the Basic vCenter Server HA deployment, when you remove vCenter Server HA the passive and witness nodes are automatically shut down and deleted. However, if you are using an Advanced vCenter Server HA deployment, once you remove vCenter Server HA you are required to manually shut down and delete the passive and witness nodes.

NOTE:

There is no supported upgrade path from 6.5 Update 2 to 6.7 GA. You must upgrade to 6.7 Update 1 or later.

Compatibility

Because vSphere 6.7 GA was released before vSphere 6.5 Update 2, there previously was no supported upgrade path. Now, with the introduction of vSphere 6.7 Update 1, there is a supported upgrade path to move forward to the latest release.

Upgrade Order

Simplified deployments using the vCenter Server with Embedded Platform Services Controller make upgrade easy. The inclusion of VMware vSphere Update Manager in the appliance also makes this a single-step process.

To begin our upgrade, we will download and mount the vCenter Server Appliance installer ISO to our management machine. Using the ISO we will run the installer, which launches the workflow to upgrade our appliance. When the upgrade wizard is completed, the installer deploys a new appliance using a temporary IP. We will then export data from the vCenter Server 6.5 instance and import it into the new vCenter Server 6.7. At this point, the appliance is reconfigured to use the same information such as the FQDN, IP, certificates, and all reference IDs.

The next step of our upgrade is to import the ISO into vSphere Update Manager and create an upgrade baseline to remediate our hosts to the latest version. Because we are upgrading from version 6.5 to version 6.7, we will be able to take advantage of the Single Reboot Upgrade enhancements to reduce our maintenance windows.

Once all of our hosts are upgraded to the ESXi 6.7, we will proceed to upgrade our distributed switch version to 6.6, making sure to keep in mind the considerations we mentioned previously when we upgrade as there is a chance disruption can occur.

Now, the vSphere Upgrade is complete and we can proceed with validation.

Validation

A complete vSphere health assessment was completed prior to executing the upgrade and migration. We determined that no faults existed in the environment and thus we were able to successfully log in to the vSphere Client.

To validate our upgraded environment, we will perform the same tasks using your health assessment tool to make sure you do not see any faults in your vSphere 6.7 Update 1 environment. If the assessment is successful, then the upgrade is now complete.

If any issues are encountered during validation, you have some options. Depending on the severity of the issue and the time in your maintenance window, you can open a support case with Global Support Services (GSS). An alternate solution might be to initiate a rollback, but remember this might be more impactful because the entire environment has been upgraded at this point.

Scenario 3: Upgrading vSphere 6.0 Update 3 Environment Using View in Horizon 7 to vSphere 6.7

Environment Discovery and Assessment

In this scenario, the customer is currently running vSphere 6.0 U3 using the vCenter Server Appliance (VCSA) with an external vSphere Update Manager (VUM) and VMware Horizon® 7 version 7.2.

The SSO topology is embedded with no external Platform Services Controllers (PSC) within this environment.

Environment Overview

During the discovery phase, we were able to identify the current versions of vCenter Server, VUM, ESXi, and Horizon 7 in the environment. The customer is currently running the vCenter Server Appliance and will not need to plan a vCenter Server migration. The VUM server is external to the VCSA of course, and must be migrated to the 6.7 vCenter Server during the upgrade. A VUM migration will save the current baselines and move them to the VCSA for use later. No installation files (VIBs, ISOs, EXEs, etc.) will be migrated during this process as that would only increase the upgrade and migration times.

PRODUCT	CURRENT VERSION	UPGRADE VERSION
vCenter Server Appliance	6.0 Update 3	6.7 Update 1
vSphere Update Manager	6.0 Update 3	6.7 Update 1
ESXi	6.0 Update 3	6.7 Update 1
Horizon 7	7.2	7.5

Requirements and Decision

Meeting with key stakeholders of the company has allowed us to discuss the expected outcomes as well as have a better understanding of the customer requirements. Requirements for this environment are as follows:

1. **Support for Instant Clones in Horizon 7 and vSphere 6.7**

   The customer is interested in using Instant Clone Technology in Horizon 7 for increased deployment speed, and is looking to move away from Linked Clones and View Composer. They are also interested in leveraging Instant Clones in vSphere 6.7 for server workloads.

   Instant Clones has been available in Horizon 7 for quite some time, but the API changes in vSphere 6.7 affected Instant Clones in Horizon 7.4. The customer was planning to use Horizon 7 version 7.4 during their upgrade, but after reviewing compatibility matrices as well as Product Release Notes, they discovered Horizon 7.4 was incompatible for the moment with vSphere 6.7. After stakeholder meetings, it was decided to use Horizon 7 version 7.5 as it was updated to support Instant Clones and vSphere 6.7.

2. **Simplified Architecture Using Enhanced Linked Mode with an Embedded PSC**

   The stakeholders expressed a desire for a simplified architecture and did not wish to implement any extra complexity. The embedded vCenter Server topology that they already had in place works well and the customer will stay embedded. This will also give them the flexibility to leverage enhanced linked mode (ELM) with an embedded PSC(s) in the future when they scale out their VDI infrastructure.

3. **vCenter Server Backups**

   In the event of a failure, management wanted an easy way to restore the vCenter Server.

   vSphere 6.7 greatly enhanced the built-in file-based backup and restore utility. Not only do we have a method to back up our PSC and vCenter Server to an external HTTP/S, FTP/S, or SCP directory, vSphere 6.7 now has a built-in scheduler and backup retention.

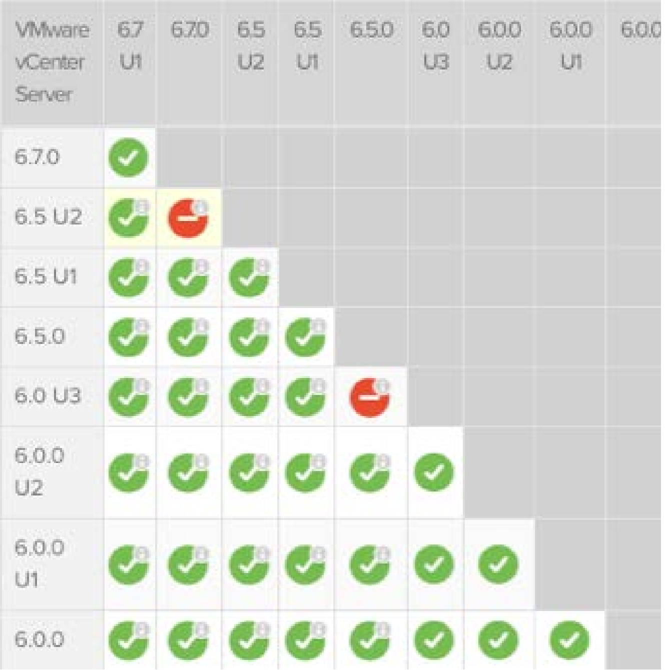
4. **Orchestrated ESXi Updates**

   VMware Update Manager (VUM) is included in the appliance in version 6.5 and later. The customer currently has an external VUM server installed in their environment. After upgrading from vCenter Server 6.0 U3 to vCenter Server 6.7 U1, VUM will be included in the VCSA and any VUM baselines from 6.0 server will be migrated to the new 6.7 VCSA to leverage for both upgrades and patching.

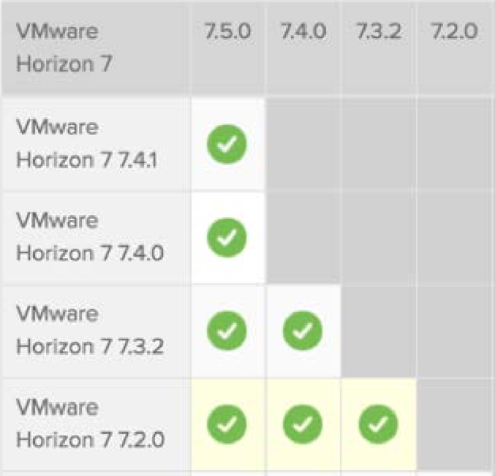
Compatibility

Making sure products are compatible is the best way to have a successful upgrade the first time around, instead of finding out later and requiring a rollback.

Our first steps are to make sure that versions are compatible. vCenter Server 6.0 U3 can be upgraded to vCenter Server 6.7 and Horizon 7 version 7.2 can be upgraded to version 7.5, as shown in the VMware Product Interoperability Matrices.

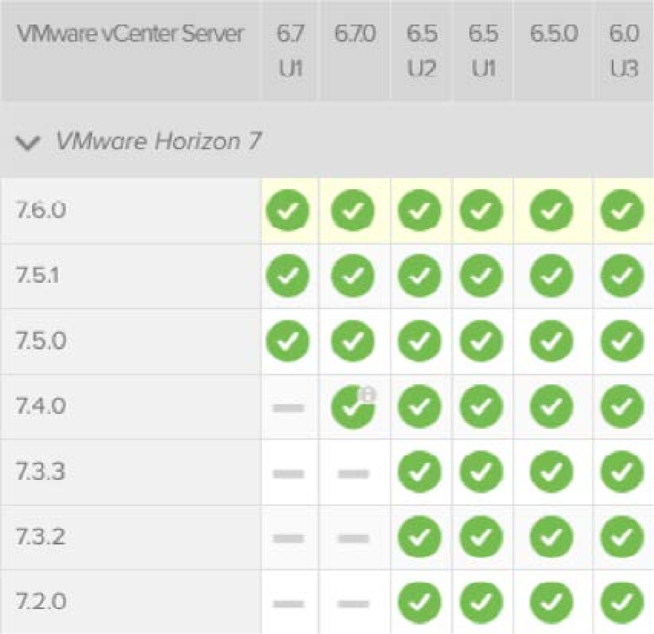


VMware vCenter Server	6.7 U1	6.7.0	6.5 U2	6.5 U1	6.5.0	6.0 U3	6.0.0 U2	6.0.0 U1	6.0.0
6.7.0	✓								
6.5 U2	✓	⊖							
6.5 U1	✓	✓	✓						
6.5.0	✓	✓	✓	✓					
6.0 U3	✓	✓	✓	✓	⊖				
6.0.0 U2	✓	✓	✓	✓	✓	✓			
6.0.0 U1	✓	✓	✓	✓	✓	✓	✓		
6.0.0	✓	✓	✓	✓	✓	✓	✓	✓	



VMware Horizon 7	7.5.0	7.4.0	7.3.2	7.2.0
VMware Horizon 7 7.4.1	✓			
VMware Horizon 7 7.4.0	✓			
VMware Horizon 7 7.3.2	✓	✓		
VMware Horizon 7 7.2.0	✓	✓	✓	

We can also see that Horizon 7 version 7.5 is compatible with VMware vSphere ESXi 6.7. These confirmations assure us that vSphere 6.7 and Horizon 7 version 7.5 are compatible before moving forward with an upgrade.



VMware vCenter Server	6.7 U1	6.7.0	6.5 U2	6.5 U1	6.5.0	6.0 U3
VMware Horizon 7						
7.6.0	✓	✓	✓	✓	✓	✓
7.5.1	✓	✓	✓	✓	✓	✓
7.5.0	✓	✓	✓	✓	✓	✓
7.4.0	—	✓	✓	✓	✓	✓
7.3.3	—	—	✓	✓	✓	✓
7.3.2	—	—	✓	✓	✓	✓
7.2.0	—	—	✓	✓	✓	✓

Upgrade Order

Upgrade order could be considered one of the most important things to understand during a vSphere upgrade. Along with upgrade order, backup verification is also critical. Now is the best time to review any required backups on systems to be upgraded. (**Examples:** View Composer database, View Composer TLS/SSL certificates, Horizon Connection Server LDAP database, Horizon Connection and Security Server VMs, vCenter Server.)

In order to identify the proper upgrade order, we will consult the VMware knowledge base article Update sequence for vSphere 6.7 and its compatible VMware products (KB53710) as well as the Horizon 7.5 Upgrades guide. Horizon 7 has some components that will be upgraded prior to the vCenter Server and ESXi hosts. Please review this order as it is important to follow it for success.

1. **View Composer Upgrade**
   a. Disable provisioning on desktop pools that leverage linked clones.
   b. Change any desktop pools that are set to refresh the OS disk on logout. Change the setting "Delete or refresh machine on logoff" to Never.
   c. Run the View Composer installer and be sure to verify port 18443 when prompted for Composer operations.
2. **Connection Server Upgrade**
   a. Export the LDAP database via the vdmexport.exe utility.
   b. Disable the Connection Server via Horizon Administrator if the Connection Servers to be upgraded are behind a load balancer.
   c. Run the Connection Server installer from the Connection Server to be upgraded.
   d. Verify the new Horizon 7 version installed from the Horizon Administrator.
   e. If the Connection Server that was upgraded is behind a load balancer, re-enable the Connection Server via Horizon Administrator before moving to the next Connection Server.
3. **Security Server Upgrade**
   a. Disable or remove IPSec rules for the paired Security Server via Horizon Administrator, and also remove the server from any load-balancing groups.
   b. Run the Connection Server installer and choose Security Server from the menu during the upgrade.
   c. Return the server to its load-balancing groups, if required.
   d. From the Horizon Administrator, verify the new Security Server version installed.

4. **vSphere Update Manager (VUM) Migration**
    a. Using the Migration Assistant tool on the VUM server will prepare it for migrating the needed baselines.
5. **vCenter Server Upgrade 6.0 U3 > 6.7 U1**
    a. Using the vCenter Server 6.7 U1 VCSA ISO, launch the installer and choose the upgrade option. This will deploy a new vCenter Server 6.7 U1 appliance, export the configuration from the old appliance, and import it into the new appliance. VUM Baselines will also be migrated.
6. **Update Horizon 7 ADMX Templates**
    a. Download and update all ADMX files that provide group policy settings for Horizon 7 within Active Directory,
7. **ESXi Upgrade 6.0 U3 > 6.7 U1**
    a. VUM is now migrated and part of the new VCSA 6.7. Use Update Manager to upgrade all ESXi hosts.
    b. Upload the ESXi 6.7 U1 ISO. Then, create an upgrade baseline with the ISO and any additional patches or extensions and have these installed on our hosts, bringing them to the latest version.
    c. Remediate all 6.0 U3 ESXi hosts to vSphere 6.7 U1.

Validation

A complete vSphere health assessment was completed prior to executing the upgrade and migration. The environment running vSphere 6.0 Update 3 was reviewed for any issues, as well as for the presence of third-party tools or VMware products such as Site Recovery Manager (SRM) or View Composer. Any discovered products were noted to be externalized prior to executing the upgrade.

To validate the upgraded environment, we perform the same tasks using the vSphere health assessment tool make sure no new faults exist within your vSphere 6.7 Update 1 environment. It is also a good practice to rename the original vCenter Server for Windows that was migrated to the VCSA and also remove or disconnect the network card of the virtual machine to mitigate the risk of any accidental power operations.

If any issues are encountered during validation, you have some options. Depending on the severity of the issue and the time in your maintenance window, you can open a support case with Global Support Services (GSS). An alternate solution might be to initiate a rollback, but remember this might be more impactful because the entire environment has been upgraded at this point.

Scenario 4: Upgrading vSphere 6.0 Update 2 Environment Using Site Recovery Manager to vSphere 6.7

Environment Discovery and Assessment

In this scenario, the customer is currently running 6.0 U2 using the vCenter Server appliance.

An external deployment is currently being used for enhanced linked mode for the production and disaster recovery site.

Environment Overview

During our discovery phase, we were able to identify the current versions of vCenter Server, ESXi, and SRM in our environment. Through discovery we also found out the customer was not currently using VUM as they currently were upgrading ESXI hosts via the CLI. Also, because the customer is currently running the vCenter Server Appliance, we do not need to plan any migration steps.

PRODUCT	CURRENT VERSION	UPGRADE VERSION
External Platform Services Controller Appliance	6.0 Update 2	6.7 Update 1
vCenter Server Appliance	6.0 Update 2	6.7 Update 1
ESXi	6.0 Update 2	6.7 Update 1
Site Recovery Manager	6.1.1	8.1

Requirements and Decision

After meeting with key stakeholders, we were able to get an understanding of the new requirements for this environment. Based on these conversations, the new requirements for this environment are as follows.

1. **vCenter Server High Availability**

   Because we are using SRM, management wants the vCenter to be highly available. In the event of a vCenter failure, their environment would be degraded. To accomplish this requirement, we will use vCenter Server HA.

2. **Simplified Architecture Using Embedded Linked Mode**

   Our first requirement is to use vCenter Server HA. Because we currently have an external PSC, in order to use vCenter Server HA we are required to deploy an additional PSC and implement a load balancer. While meeting with the stakeholders, they expressed a desire for a simplified architecture and did not wish to implement any extra complexity.

   Prior to vSphere 6.7 U1 there was no way to modify your external PSC to make it an embedded PSC. Embedded linked mode was only for greenfield or expanded deployments. With 6.7 U1, we have now provided a converge tool that can embed an external PSC. Because of this updated feature, we can now use vCenter Server HA and enhanced linked mode using an embedded PSC.

3. **vCenter Server Backups**

   In the event of a failure, management wanted an easy way to restore the vCenter Server. With VMware Data Protection being deprecated with vSphere 6.7, the customer needed another solution.

   vSphere 6.7 greatly enhanced the built-in file-based backup and restore utility. Not only do we have a method to back up our PSC and vCenter Server to an external HTTP/S, FTP/S, or SCP directory, but vSphere now has a built-in scheduler and built-in retention.

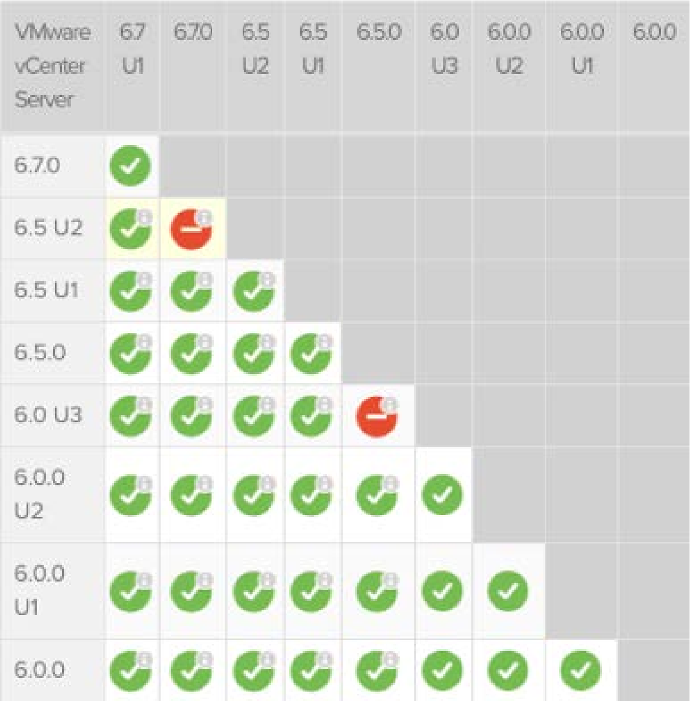
4. **Orchestrated ESXi Updates**

   VMware Update Manager (VUM) is included in the appliance in version 6.5 and later. Because the customer currently does not have VUM installed in their environment, when they upgrade from vCenter Server 6.0 U2 to vCenter Server 6.7 U1, VUM will be included, and they can use baselines for both upgrades and patching.

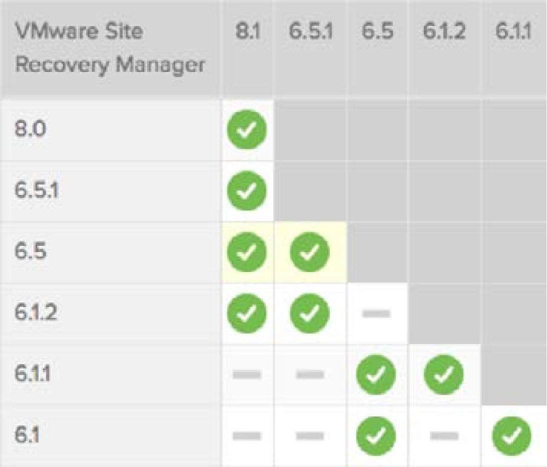
Compatibility

Making sure products are compatible is the best way to have a successful upgrade the first time around, instead of finding out later and requiring a rollback.

In this scenario, we want to make sure that our versions are compatible. As we can see from the first image that follows, we are able to upgrade from vCenter Server 6.0 U2 to vCenter Server 6.7 U1. However, in the second image, we can see SRM 6.1.1 is unable to upgrade directly to SRM 8.1; it requires us to be at 6.1.2.



VMware vCenter Server	6.7 U1	6.7.0	6.5 U2	6.5 U1	6.5.0	6.0 U3	6.0.0 U2	6.0.0 U1	6.0.0
6.7.0	✓								
6.5 U2	✓	⊖							
6.5 U1	✓	✓	✓						
6.5.0	✓	✓	✓	✓					
6.0 U3	✓	✓	✓	✓	⊖				
6.0.0 U2	✓	✓	✓	✓	✓	✓			
6.0.0 U1	✓	✓	✓	✓	✓	✓	✓		
6.0.0	✓	✓	✓	✓	✓	✓	✓	✓	

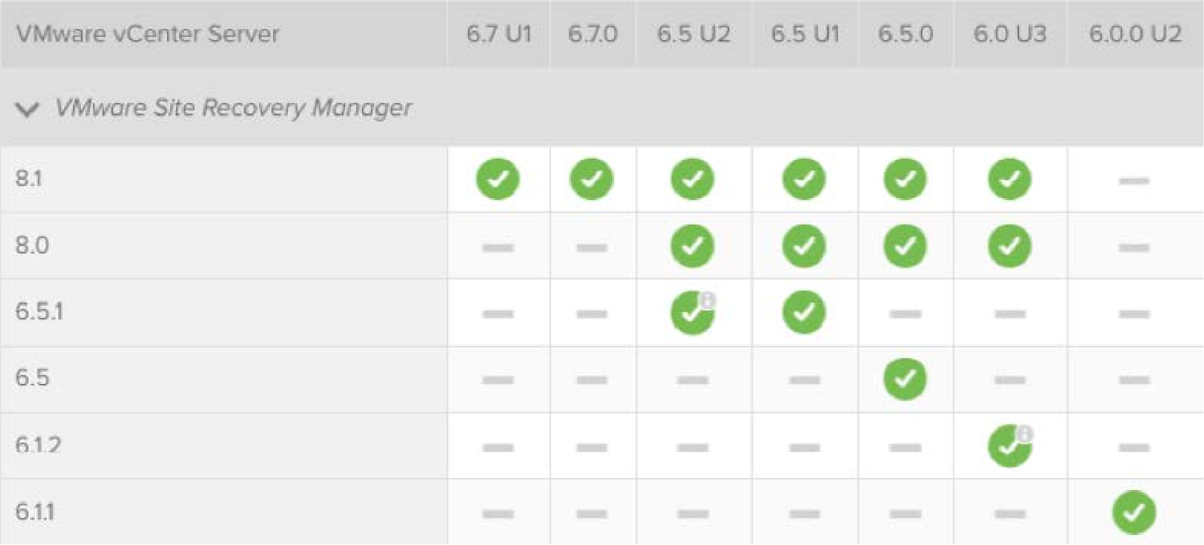


VMware Site Recovery Manager	8.1	6.5.1	6.5	6.1.2	6.1.1
8.0	✓				
6.5.1	✓				
6.5	✓	✓			
6.1.2	✓	✓	—		
6.1.1	—	—	✓	✓	
6.1	—	—	✓	—	✓

Through our first compatibility check, we have identified our first issue. If we look at the vCenter Compatibility Matrix for SRM 6.1.2 we can also see that it is not compatible with vCenter Server 6.0 U2; it requires us to be at vCenter Server 6.0 U3. The good news is that we can see that SRM 8.1 is compatible with both vCenter Server 6.0 U3 and vCenter Server 6.7 U1, so that upgrade will be compatible once we are at that step. Based on this information, we can establish the correct upgrade order to maintain compatibility.

Upgrade Order

Through our compatibility checks we have identified that we must be at SRM 6.1.2 prior to upgrading to SRM 8.1. We also identified that in order to get to SRM 6.1.2, we must first upgrade our vCenter Server from 6.0 U2 to vCenter Server 6.0 U3. Because the customer will not have VUM in their environment until the vCenter is at vCenter Server 6.7 U1, we will hold off patching until the final step. ESXI 6.0 U2 is compatible with vCenter Server 6.0 U3 and vCenter Server 6.7 U1.



VMware vCenter Server	6.7 U1	6.7.0	6.5 U2	6.5 U1	6.5.0	6.0 U3	6.0.0 U2
VMware Site Recovery Manager							
8.1	✓	✓	✓	✓	✓	✓	—
8.0	—	—	✓	✓	✓	✓	—
6.5.1	—	—	✓	✓	—	—	—
6.5	—	—	—	—	✓	—	—
6.1.2	—	—	—	—	—	✓	—
6.1.1	—	—	—	—	—	—	✓

In order to identify the proper upgrade order we will consult the VMware knowledge base article, Update sequence for vSphere 6.7 and its compatible VMware products (53710).

1. **vCenter Server Update 6.0 Update 2 > 6.0 Update 3**
    a. Update vCenter Server 6.0 Update 2 to 6.0 Update 3 using the vCenter Appliance Management Interface (VAMI).
2. **Site Recovery Manager Update 6.1.1 > 6.1.2**
    a. Update SRM 6.1.1 to 6.1.2 by downloading the executable and installing it, making sure to upgrade any incompatible SRA adapters.
3. **Site Recovery Manager Upgrade 6.1.2 > 8.1**
    a. Upgrade SRM 6.1.2 to 8.1 by downloading the executable and installing it, making sure to upgrade any incompatible SRA adapters.
4. **vCenter Server Upgrade 6.0 Update 3 > 6.7 Update 1**
    a. Using the vCenter Server 6.7 Update 1 VCSA ISO, launch the installer and choose the upgrade option. This will deploy a new vCenter Server 6.7 Update 1 appliance, export the configuration from the old appliance, and import it into the new appliance.
5. **ESXi Upgrade 6.0 Update 2 > 6.7 Update 1**
    a. VUM is now installed in the environment. Use Update Manager to upgrade the hosts. Upload the ESXi 6.7 Update 1 ISO. Then, create a baseline with the ISO and any additional patches or extensions, and have these installed on the hosts, bringing them to the latest version.

Validation

Prior to executing our upgrade, we were able to successfully complete a health assessment. We reviewed that no faults existed in the environment and that we were able to successfully fail over workloads between sites using Site Recovery Manager.

To validate our upgraded environment, perform the same tasks using the health assessment tool to make sure you do not see any faults in your vSphere 6.7 Update 1 environment. At this point, you will also perform a test failover of your SRM workloads and make sure everything is functioning. If this is successful, your upgrade is now complete.

If you encounter an issue with your validation, you have two options. Depending on the severity of the issue and the time in your maintenance window, you can open a support case. An alternative solution is to rollback, but because you have upgraded all components an upgrade at this point might be more impactful.

Phase 3: Post-Upgrade

After the upgrade is complete, the next step is to complete “day 2 operations” that will ensure you an optimal vSphere 6.7 experience.

vCenter Server Converge Tool

vCenter Server 6.7 and 6.5 Update 2 now support Embedded Deployments with Enhanced Linked Mode (ELM) in a greenfield environment. Embedded deployment of the vCenter Server is now the recommended topology going forward. Previously, external deployments of the Platform Services Controller (PSC) was the only way to achieve Enhanced Linked Mode (ELM).

With vSphere 6.7 Update 1 comes the Converge Tool. The Converge Tool allows those in an external PSC topology to change to a more simplistic embedded topology where the PSC is part of the VCSA node as a single VM versus multiple VMs.

This tool is only available with the vCenter Server Appliance 6.7 Update 1 installer or ISO. This new tool allows administrators to simplify vCenter Server architecture and move from an external Platform Services Controller (PSC) to an embedded PSC topology. Converge Tool has a few requirements that should be considered prior to use. The converge tool is only supported on the VCSA and PSC if they are running 6.7 Update 1 code. This means that if your environment is using the vCenter Server for Windows, you will have to migrate to the VCSA first before considering convergence. Another requirement is to disable vCenter Server High Availability (VCHA) if enabled prior to running the tool. Be sure to review and understand any other VMware products in the environment that may be communicating with the PSC (Horizon, NSX, SRM, vRealize Operations, etc.) as they will need to be re-registered after the convergence of the PSC and before the final decommission process completes.

This is just a short list of the Converge Tool features and requirements. To learn more, review vCenter Server Documentation.

For more information on using the Converge Tool, see http://www.vmware.com/go/ vSphere67u1 ConvergeTool

Cross-Domain Repoint

vCenter Server 6.7 also includes a way to consolidate vSphere single sign-on (SSO) domains. Initially in vSphere 5.5 any consolidatation of SSO domains had to be done prior to upgrade, but with the release of vSphere 6.7 it is supported to consolidate vSphere SSO domains once all Platform Services Controllers and vCenter Server components are running vSphere 6.7. Unlike vSphere 5.5, consolidating SSO domains on vSphere 6.7 must be done after all components are upgraded to vSphere 6.7. vSphere 6.7 GA supports consolidation of vSphere SSO domains using external PSCs and vSphere 6.7 Update 1 now supports this when using an embedded PSC(s).

It is no longer required to deploy and configure a new SSO domain in order to consolidate. The cross-domain repoint tool supports the consolidation and merging of two existing SSO domains. Using cmsso-util, you can run a precheck which will identify any conflicts such as tags, tag categories, licenses, or roles. **Note:** If repointing to a new SSO domain, all global permissions are lost and must be recreated, but if repointing to an existing SSO domain, then global permissions will be inherited.

A situation where this strategy makes sense is a company acquisition. If you had two separate vSphere environments or had different SSO domain names, you can now merge these to a shared SSO domain and take advantage of Enhanced Linked Mode.

File-Based Backup and Restore

In case you were wondering how to protect your vCenter Server Appliance (VCSA) in case of failure, we have a built-in file-based backup and restore. This is an important feature: In the event of a failure we can perform a successful restore of our Platform Services Controller (PSC) or vCenter Server. With vSphere 6.7, we improved the backup and restore process by introducing new features such as a built-in scheduler with retention and a new file explorer for restores.

We recommend you use the file-based backup and restore when using a vCenter Server HA cluster, as we have built-in logic to make sure configurations are properly backed up and, in the event of a restore, we are able to restore just a standalone node.

vCenter Server High Availability (VCHA)

Another exclusive feature to the vCenter Server Appliance (VCSA) is vCenter Server HA. VCHA allows the creation of a vCenter Server cluster that is high availability for protecting vCenter Server from failure. The HA cluster includes a peer and witness node. In this configuration synchronous replication of the database and asynchronous replication of files and configuration are handled. Due to these replication formats, VMware suggests a near 0 RPO and a 5-minute RTO, which can vary with the size of inventory and database. When an active vCenter Server fails, VCHA can perform an automatic failover to the peer node.

Transitioning to the vSphere Client

vSphere 6.7 Update 1 HTML5-based client boasts new features, workflow improvements, and delivers better performance.

The vSphere Client now includes vCenter High Availability (vCenter HA), and introduces a Cluster Quickstart forimproved HCI deployments, along with an improved vSphere Update Manager. As a result, it has been announced that the vSphere Web Client (Flash) will no longer be available past vSphere 6.7. All users should transition to the vSphere Client.

Resource Repository

Pre-Upgrade Resources

Review these blog posts for help preparing and planning your upgrade.

Upgrade Considerations for VMware vSphere 6.7

Upgrading your vCenter Server Appliance from 6.5 to 6.7

vSphere Upgrade Technical Webcast Series

vSphere Upgrade – FAQs Now Available

vSphere Upgrade Series Part 1: Preparing to Upgrade

Automating Your vSphere Upgrade

Upgrade Resources

Review these documents for help executing your upgrade.

vSphere Upgrade

vSphere Upgrade Series Part 2: Upgrading vCenter Server

Upgrading Your vSphere Environment with Site Recovery Manager and vSphere Replication

Upgrading Your vCenter Server from 6.5 to 6.7

Introduction to Automating Your vSphere Upgrade

Post-Upgrade Resources

Review these documents for help with post-upgrade tasks.

After Upgrading or Migrating vCenter Server

File-Based Backup and Restore of vCenter Server Appliance

vCenter High Availability

Use Encryption in Your vSphere Environment

Changing a vCenter Server Deployment Type After Upgrade or Migration

Reconfiguring vCenter Server with an External Platform Services Controller to a vCenter Server with an Embedded Platform Services Controller

Knowledge Base Articles

VMware vSphere Upgrade Policies (2149713)

Important information before upgrading to vSphere 6.7 (53704)

Update Sequence for vSphere 6.7 and its compatible VMware products (53710)

Best practices for upgrading to vCenter Server 6.7 (54008)

Supported and deprecated topologies for VMware vSphere 6.5 (2147672)

Supported upgrade paths for vSAN 6.6 (2149840)

Migrating VMFS 5 datastore to VMFS 6 datastore (2147824)

vSphere 6.7 Resources

What’s New in vSphere 6.7 Update 1

vSphere 6.7 Technical White Paper

vSphere 6.7 Product Documentation

vSphere 6.7 Configuration Maximums

vSphere 6.7 Training

vSphere Upgrade Webcasts

About the Authors

Nigel Hickey

Nigel Hickey is a Technical Marketing Engineer and VCIX7-DTM in the Cloud Platform business unit at VMware. He is a subject matter expert for vSphere upgrades and a trusted advisor to VMware customers and partners. Nigel can be found blogging on nigelhickey.com or on Twitter via @vCenterNerd.

David Stamen

David Stamen is a Technical Marketing Engineer and VCIX6.5-DCV in the Cloud Platform business unit at VMware.

In his role, he covers vSphere Lifecycle. This includes the Installation, Patching, Upgrading and Configuration of vCenter Server and ESXi components.

David can be found blogging at http://davidstamen.com and on Twitter via @davidstamen.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com