

# Upgrading to VMware vSphere 7

Tips and tricks for planning and  
executing a successful upgrade



# What's New in VMware vSphere 7

## VMware vSphere 7: Essential Services for the Modern 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.

VMware vSphere 7 delivers the essential services for the modern hybrid cloud. It powers the computing environment for modern applications, AI/ML, and business critical applications. You can deploy applications using any combination of virtual machines, containers, and Kubernetes. With vSphere 7, VMware vSphere® with VMware Tanzu™ is available through [VMware Cloud Foundation™](#), and delivers VMware Cloud Foundation services and application-focused management to meet the goals of streamlined development, agile operations, and accelerated innovation.



### THE TOP 10 REASONS TO UPGRADE TO VSPHERE 7

1. **Take the fastest path** to modern apps
2. **Secure** audits and account management
3. **Tighten** physical infrastructure security
4. **Run** artificial intelligence and machine learning (AI/ML) workload demands in real time
5. **Simplify** software patching and hardware upgrades
6. **Reduce** complexity and increase scale
7. **Maximize** performance and efficiency
8. **Get proactive support** technology and services
9. **Realize** flexibility to run any app on any cloud
10. **Build** a solid HCI for modern applications

## Why Upgrade to vSphere 7

VMware vSphere 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



### VMware vSphere Lifecycle Management

The innovations for lifecycle management in vSphere 7 allow organizations to have consistent and up-to-date systems. The major lifecycle management improvements in vSphere 7 are vCenter Server Profiles, vCenter Server Update Planner, and VMware vSphere® Lifecycle Manager™.

The introduction of Single Reboot Upgrades and VMware vSphere® Quick Boot™ in vSphere 6.7 also reduces time required for patching and updates when upgrading to vSphere 7.



### Intrinsic Security

VMware vSphere 7 builds on the security capabilities in vSphere 6.7 and leverages its unique position as the hypervisor to offer comprehensive security that starts at the core, via an operationally simple policy-driven model. Identity Federation, vSphere Trust Authority, and Simplified Certificate Management are features that help customers with vSphere security.



### Application Acceleration

VMware vSphere 7 is a universal application platform that supports a broad variety of workloads (including 3D Graphics, Big Data, HPC, Machine Learning, In-Memory, and Cloud-Native), as well as existing mission-critical applications. The platform also supports and leverages some of the latest hardware innovations in the industry, delivering exceptional performance for a variety of workloads.



### VMware vSphere with Tanzu

VMware vSphere 7 is the most feature-rich release of vSphere in over a decade. It delivers a plethora of innovations and the rearchitecting of vSphere with native Kubernetes, which VMware introduced at VMworld 2019 as Project Pacific. Kubernetes is now built into vSphere, which allows developers to continue using the same industry-standard tools and interfaces they have been using to create modern applications. VMware vSphere administrators also benefit because they can help manage the Kubernetes infrastructure with the same tools and skills they have developed around vSphere.



## 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 6.5 and vSphere 6.7 to vSphere 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 an upgrade

Throughout this eBook are helpful resources, which also are listed in the [Resource 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 stability and consistency of the environment using a health check, and to understand what is involved in performing 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 VMware vCenter Server® 7 product release notes referenced throughout this eBook:

**What's New** – Highlights of what is new in the current release

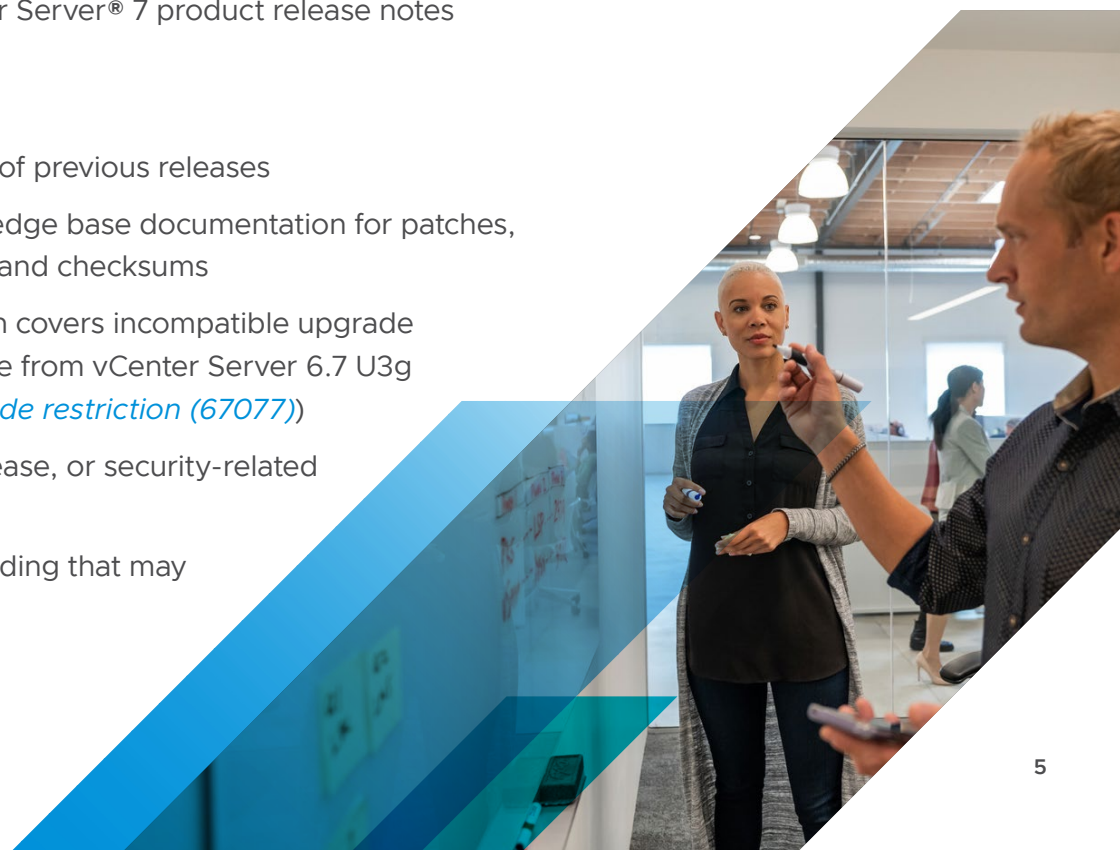
**Earlier Releases of vCenter Server 7** – Links to release notes of previous releases

**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 6.7 U3g to vCenter Server 7.0.0a ([vSphere Back-in-time release upgrade restriction \(67077\)](#))

**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 after 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 Server 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.

## Interoperability Matrices

[VMware Product 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 6.5 Update 3 and VMware 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 7?

### LEARN MORE

For more information, see the VMware knowledge base article [Using the VMware Product Interoperability Matrixes \(2006028\)](#).

## VMware Compatibility Guide

Did you know that one of the most common reasons for a vSphere diagnostic crash is incompatible firmware or driver versions? Be aware that the VMKlinux driver stack is deprecated in vSphere 7. VMware vSphere 6.7 is the last version of vSphere that contains VMKlinux drivers. For more information, see the VMware blog post [What is the Impact of the VMKlinux Driver Stack Deprecation?](#).

The [VMware Compatibility Guide](#) can help you to understand if your physical hardware is compatible with the ESXi version to which you plan to upgrade. To use the tool, you first must get the device IDs of your adapters. The VMware knowledge base article [Determining Network/Storage firmware and driver version in ESXi 4.x and later \(1027206\)](#) explains this process and how to obtain the driver or firmware version via the `esxcfg` CLI command.

**Note:** Many hardware CPUs have been deprecated in vSphere 7, and you must verify your hardware devices and details prior to an upgrade. After you gather hardware details, 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 have.

Automating this process is also possible. VMware recently released a VMware Flings titled [ESXi Compatibility Checker](#). This Flings 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 must be referenced during upgrade planning to ensure proper hardware compatibility.



## Third-Party Solution Compatibility

Ensure that you consider software from other vendors that touches 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 you perform a vSphere upgrade, we recommend that you do a health check. If an environment is not in a healthy state, errors can occur which might require a rollback.

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

Included in vSphere 6.7 GA and higher is Skyline Health for vSphere (formerly vSphere Health). VMware vSphere Health and vSAN Health have been highly instrumental in assisting organizations to triage their vSphere environments for configuration consistency, best practice information, vulnerability discovery, and proactive analytics. Now part of VMware Skyline™ Health, Skyline Health for vSphere is available to all organizations with Basic, Production, and Premier Support levels.

We recommend leveraging Skyline Health for vSphere if you are running vSphere 6.7 GA or higher, other tools such as VMware vRealize® Operations™, or community-based tools such as vCheck. 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—ensuring that you have successful backups is essential. Not only must you think about backing up Platform Services Controller™ and vCenter Server instances, but also you must be confident that all components have been backed up. Do not forget ESXi Configuration, Distributed Virtual Switch, and other VMware products like VMware NSX® and VMware Horizon®.

If you are leveraging the VMware 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, we recommend that you use a supported image-based backup tool.

Any issues encountered during a vCenter Server migration or upgrade can best be corrected with a rollback, rather than a restore. When migrating from vCenter Server for Windows to vCenter Server appliance a rollback is as straightforward as shutting down the newly deployed vCenter Server appliance and removing it from inventory, powering on the vCenter Server for Windows, then rejoining the server back to Active Directory. When performing an upgrade from vCenter Server appliance to vCenter Server appliance, the rollback process is the same: Shut down the new appliance and then power-on the original.

### Resources

[vSphere 7 Upgrade Information](#)

[vCheck vSphere](#)

[VMware Product Interoperability Matrices](#)

[vSphere Optimization Assessment](#)

[VMware Compatibility Guide](#)

[vSphere 6.7 vCenter Server Appliance File-Based Backup](#)

[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 [VMware Professional Services website](#).



#### TIP

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

You must also back up the configuration of your ESXi server. In the event you perform an upgrade or patching process, and the change fails, you will have the ability to restore the configuration from a known good backup. Currently the backup can be triggered only through CLI tools. To learn more about backing up ESXi host configurations, see the VMware knowledge base article [How to back up ESXi host configuration \(2042141\)](#).

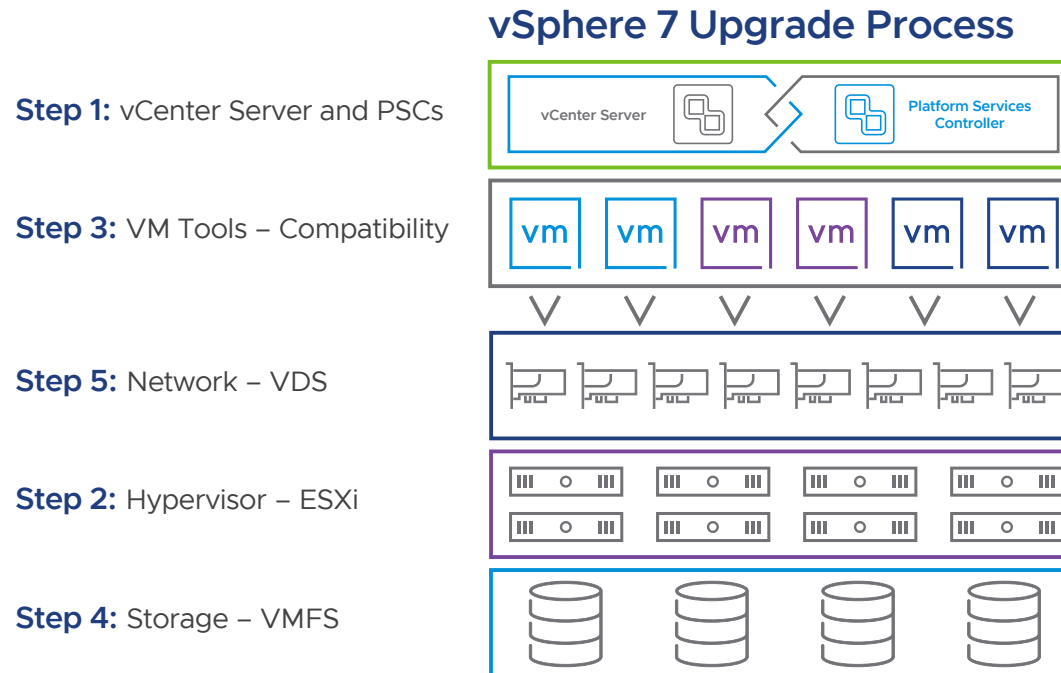
# Phase 2: Upgrade

In **Phase 2: Upgrade** we review some sample upgrade scenarios, each including popular VMware products. However, these scenarios are not reflective of all vSphere environments. The intention is to guide the vSphere administrator through sample processes.

## Upgrade Process Overview

The vSphere upgrade order of operations is an important, but often overlooked, process. This overview breaks the process into five steps.

**Note:** In vSphere 7, the upgrade process has evolved to allow the workflow to upgrade as well as converge any external Platform Services Controller (PSC) instances in the vSphere environment. No longer is this a two-step process.



## Platform Services Controller and vCenter Server

What happened to the Platform Services Controller?

Beginning in vSphere 7, deploying a new vCenter Server or upgrading to vCenter Server 7 requires the use of the vCenter Server appliance, a preconfigured virtual machine optimized for running vCenter Server.

The new vCenter Server contains all PSC services, and preserves the functionality and workflows, including authentication, certificate management, tags, and licensing. It is no longer necessary nor possible to deploy and use an external PSC. All PSC services are consolidated into vCenter Server, and deployment and administration are simplified.

Because these services are now part of vCenter Server, they are no longer described as a part of PSC. In vSphere 7, the [About vSphere Authentication](#) publication replaces the Platform Services Controller Administration publication. The new publication contains complete information about authentication and certificate management.



### TIP

Platform Services Controller instances and vCenter Server instances must be the same vSphere version when in the same SSO domain before you upgrade 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 PSC and the vCenter Server in a single step.

Mixed versions are when vCenter Server and PSC versions do not match in the environment. A mixed-version vCenter Server configuration is supported only during upgrades and not for production environments. This can happen when upgrading the vCenter Server with an external PSC, and this is the reason we require all external PSC instances to be upgraded before starting any vCenter Server upgrades. Using vCenter Servers with embedded PSC instances 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, check the hardware against the [VMware Compatibility Guide](#) to ensure that your ESXi hosts are compatible with the vSphere 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 the following resources:

- [vSphere Update Manager Documentation](#)
- [Upgrade Hosts Interactively](#)
- [Using vSphere Auto Deploy to Re provision Hosts](#)
- [ESXCLI Syntax](#)

Carefully review the requirements of the options. The recommended approach is to use VMware 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 upgrade hosts only to the version of vCenter Server, so if you want to upgrade to a previous ESXi version, you must use the interactive or `esxcli` method.



## VMware Tools and VM Hardware Compatibility

VMware Tools™ and Virtual Machine Hardware Compatibility (VM Compatibility), previously known as vHardware, can be extremely valuable for managing virtual machines. 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 allows the VM to take advantage of additional features available to the virtual machine. For example, hardware version 17, introduced with vSphere 7, supports Virtual Watchdog Timer that can assist a guest OS in recovering from crashes.

Prior to upgrading to a higher VM Hardware Compatibility version, consider your reasons. Upgrading a VM Compatibility version is not always necessary, unless you require specific features that come with the VM Compatibility version. You can upgrade the hardware of VMs to the latest hardware compatibility version that the ESXi host supports. Upgrades to the next version can run immediately or be scheduled for a time that is convenient.

VMware Tools is a set of services and modules that enables 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:

- From the status bar of the VM, which displays a message when a new VMware Tools version is available
- By manually initiating an update through the VMware vSphere® Client
- Using vSphere Update Manager to configure the virtual machine to check and install on reboot, or by using VMware vSphere® PowerCLI™
- When using `open-vm-tools` on most modern major Linux distributions, VMware Tools must be upgraded through the package manager of choice, such as YUM or APT

### NOTE

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

## Storage – Virtual Machine File System Datastores

There are two versions of VMware vSphere® VMFS (Virtual Machine File System, or VMFS) data stores for Sphere 7: VMFS5 and VMFS6.

VMFS6 offers several enhancements in regard to space reclamation, as well as better support for larger snapshots. Prior to upgrading to VMFS6, ensure that all hosts have been upgraded to at least ESXi 6.5.

The following table compares the major characteristics of VMFS5 and VMFS6. For additional information, see the [VMware Configuration Maximums](#) guide.

FEATURE / FUNCTION	VMFS5	VMFS6
Access for ESXi hosts version 6.5 and later	Yes	Yes
Access for ESXi hosts version 6.0 and earlier	Yes	No
Datastores per host	512	512
512n storage devices	Yes	Yes (default)
512e storage devices	Yes (not supported on local 512e devices)	Yes (default)
4Kn storage devices	No	Yes
Automatic space reclamation	No	Yes
Manual space reclamation through the <code>esxccli</code> command *	Yes	Yes
Space reclamation from guest OS	Limited	Yes
GPT storage device partitioning	Yes	Yes



FEATURE / FUNCTION	VMFS5	VMFS6
MBR storage device partitioning	Yes (for a VMFS5 datastore that has been previously upgraded from VMFS3)	No
Storage devices larger than 2 TB for each VMFS extent	Yes	Yes
Support for virtual machines with large-capacity virtual disks, or disks larger than 2 TB	Yes	Yes
Support for small files of 1 KB	Yes	Yes
Default use of ATS-only locking mechanisms on storage devices that support ATS **	Yes	Yes
Block size	Standard 1 MB	Standard 1 MB
Default snapshots	VMFSsparse for virtual disks smaller than 2 TB SEsparse for virtual disks larger than 2 TB	SEsparse
Virtual disk emulation type	512n	512n
VMware vSphere® vMotion®	Yes	Yes
VMware vSphere® Storage vMotion® across different datastore types	Yes	Yes
High Availability and Fault Tolerance	Yes	Yes
DRS and VMware vSphere® Storage DRS™	Yes	Yes
Raw device mapping (RDM)	Yes	Yes

\* For more details, see the [Manually Reclaim Accumulated Storage Space](#) documentation.

\*\* For more details, see the [VMFS Locking Mechanisms](#) documentation.



You cannot upgrade a VMFS5 datastore directly to a VMFS6 datastore. If you have a VMFS5 datastore in your environment, create a VMFS6 datastore and migrate virtual machines from the VMFS5 datastore to the VMFS6 datastore. You can do this 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 VMFS6 version. Using Storage vMotion, migrate the VMs and repeat until all datastores have been upgraded. You can do this manually through the GUI, or automated via a vSphere PowerCLI cmdlet that has been created for this, `Update-VMFSDatastore`.

#### LEARN MORE

For more information, see the VMware knowledge base article [Migrating VMFS 5 datastore to VMFS 6 datastore \(2147824\)](#).





## Networking – Virtual Distributed Switch

You can upgrade VMware vSphere Distributed Switch (VDS) version 6.5 to a later version. The upgrade lets the distributed switch take advantage of features that are available only in the later version. Prior to upgrading to vSphere 7, you must verify that the virtual distributed switch has been upgraded to at least a 6.5.0 version. Failing to do so may impact the upgrade process.

Three options are available when creating or updating a virtual distributed switch on vSphere 7:

- vSphere Distributed Switch 7
- vSphere Distributed Switch 6.6
- vSphere Distributed Switch 6.5

Updates to networking are traditionally within ESXi itself, but additional features require upgrading the VDS to leverage the newest features. After you upgrade your vCenter Server and host versions, verify that you have also updated your VDS to the latest version so you have the most up-to-date features. The upgrade of a distributed switch can cause the hosts and virtual machines attached to the switch to experience a brief downtime. For more information, see the VMware knowledge base article [Known issues while upgrading to DVS version 6.6 \(52621\)](#).

### DSwitch - Upgrade Distributed Switch

**1 Configure upgrade**  
2 Check compatibility  
3 Ready to complete

**Configure upgrade**  
Specify distributed switch version for upgrade.

7.0.0 - ESXi 7.0 and later  
 6.6.0 - ESXi 6.7 and later

*The multicast filtering continue with the sele*

Features per version ⓘ

#### New features and enhancements

**Distributed switch: 7.0.0**

- NSX Distributed Port Group

**Distributed switch: 6.6.0**

- MAC Learning

CANCEL BACK NEXT

Upgrade VMware vSphere Distributed Switch to take advantage of the latest features.

## Scenario 1: Migrating vCenter Server for Windows from vSphere 6.5 Update 3 to vCenter Server Appliance, vSphere 7

The first scenario was an organization migrating from

- vSphere 6.5 U3 with vCenter Server for Windows

to

- vSphere 7 and vCenter Server appliance

### Environment Discovery and Assessment

We assessed that the organization was running vSphere 6.5 Update 3 using vCenter Server for Windows with vSphere Update Manager co-installed with the vCenter Server. The vSphere Update Manager server and all ESXi hosts in this environment were at vSphere 6.5 Update 3.

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



## Requirements and Decision

During the discovery phase, we identified the current versions of vCenter Server, vSphere Update Manager, and ESXi in the environment.

A vSphere Update Manager migration would save the current baselines and move them to the vCenter Server appliance for later use. No installation files (VIBs, ISOs, and so on) would be migrated during this process because that would only increase the upgrade and migration times.

PRODUCT	CURRENT VERSION	UPGRADE VERSION
vCenter Server for Windows	vSphere 6.5 Update 3	vSphere 7
vSphere Update Manager	vSphere 6.5 Update 3	vSphere 7
ESXi	vSphere 6.5 Update 3	vSphere 7

## Compatibility

Verifying that all products in the vSphere data center are compatible is the best way to have a successful upgrade every time. Failure to verify product interoperability can lead to issues during and after upgrades that can result in a rollback of the upgraded systems.

VMware vCenter Server	7.0	6.5 U3	6.5 U2	6.5 U1	6.5.0
▼ VMware vSphere Hypervisor (ESXi)					
7.0	✓	—	—	—	—
6.5 U3	✓	✓	✓	✓	✓
6.5 U2	✓	✓	✓	✓	✓
6.5 U1	✓	✓	✓	✓	✓
6.5.0	✓	✓	✓	✓	✓

VMware vCenter Server	7.0	6.7 U3	6.7 U2	6.7 U1	6.7.0	6.5 U3	6.5 U2	6.5 U1	6.5.0
6.7 U3	✓								
6.7 U2	✓	✓							
6.7 U1	✓	✓	✓						
6.7.0	✓	✓	✓	✓					
6.5 U3	✓	✓	—	—	—				
6.5 U2	✓	✓	✓	✓	✓	—			
6.5 U1	✓	✓	✓	✓	✓	✓	—		
6.5.0	✓	✓	✓	✓	✓	✓	✓	—	

## Upgrade Order

Upgrade order is an important part of any upgrade process. You must always upgrade vCenter Server first, before upgrading any vSphere hosts (ESXi). VMware vSphere Update Manager is still used in vSphere 7 and is included in the vCenter Server appliance. Because of this, it is part of the vCenter Server upgrade and migration process. The vCenter Server in this environment was running on Windows and required a vCenter Server migration to the vCenter Server appliance.

To begin our upgrade, we downloaded and mounted the vCenter Server appliance installer ISO to our management machine. Using the ISO, we ran the installer, which launched the workflow to migrate the vCenter Server for Windows to the new vCenter Server appliance. When the migration wizard was finished, the installer deployed a new appliance using a temporary IP address. It then exported data from the Windows vCenter Server instance and imported it into the new vCenter Server appliance. The appliance was then reconfigured to use the same information from vCenter Server for Windows, such as the FQDN, IP address, certificates, and all reference IDs.

Next steps were to import the vSphere 7 ISO into vSphere Update Manager and create an upgrade baseline to remediate the vSphere 6.5 U3 hosts to vSphere 7.

After hosts were upgraded to vSphere 7, the next step was to upgrade any distributed switch versions to vSphere Distributed Switch version 7. At this point, the vSphere upgrade was complete, and we moved to validation.

### Validation

A complete vSphere health assessment was completed prior to executing the upgrade and migration. The environment running vSphere 6.5 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 or VMware View® Composer™. Any discovered products were noted, to be externalized prior to executing the upgrade.

To validate the upgraded environment, we performed the same tasks using the vSphere health assessment tool to ensure that no new faults existed within the vSphere 7 environment. Because the vCenter Server for Windows server was now turned off and sat in inventory ready to be removed, we renamed the original vCenter Server for Windows that had been migrated to the vCenter Server appliance. Additionally, we removed or disconnected the network card of the virtual machine where vCenter Server was installed to mitigate the risk of any accidental VM power operations.

If issues are encountered during validation, you have remediation 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 is to initiate a rollback, but this option can have a large impact because the entire environment has been upgraded at this point.

## Scenario 2: Upgrading vCenter Server Appliance from vSphere 6.7 Update 3 to vSphere 7

The second scenario was an organization migrating from

- vSphere 6.7 U3 with vCenter Server appliance

to

- vSphere 7 with vCenter Server appliance

### Environment Discovery and Assessment

In this scenario, the organization was running vSphere 6.7 Update 3 with VMware vCenter High Availability (vCenter HA). The current version of all vSphere hosts was also 6.7 Update 3.

The SSO topology for this environment was external, consisting of two external PSC instances in the vSphere SSO domain servers within the environment.

PRODUCT	CURRENT VERSION	UPGRADE VERSION
vCenter Server appliance	vSphere 6.7 Update 3	vSphere 7
Platform Services Controller	vSphere 6.7 Update 3	vSphere 7
ESXi	vSphere 6.7 Update 3	vSphere 7

## Requirements and Decision

Requirements for this environment were quite simple because the external topology and configuration would be converged to an embedded topology during the upgrade to vCenter Server 7.

Also, because the vCenter Server 6.7 was configured for vCenter HA, we had to ensure that we understood the proper procedure. When you are upgrading to vSphere 7, and vCenter HA is enabled, the workflow automatically disables vCenter HA, performs the upgrade, and then re-enables vCenter HA after the upgrade is complete.

## Compatibility

Before moving forward with this vSphere 7 upgrade to the latest release, we validated the compatibility of the current vSphere version (6.7 U3) against the VMware Product Interoperability Matrices to ensure that a supported upgrade path existed.

### NOTE

Currently there is no supported upgrade path from 6.7 Update 3g or 6.7 Update 3h to vSphere 7 GA. For more details, see VMware knowledge base article [vSphere Back-in-time release upgrade restriction \(67077\)](#).

VMware vCenter Server	7.0	6.7 U3	6.7 U2	6.7 U1	6.7.0
VMware vSphere Hypervisor (ESXi)					
7.0	✓	—	—	—	—
6.7 U3	✓	✓	✓	✓	✓
6.7 U2	✓	✓	✓	✓	✓
6.7 U1	✓	✓	✓	✓	✓
6.7.0	✓	✓	✓	✓	✓

VMware vSphere Hypervisor (ESXi)	7.0	6.7 U3	6.7 U2	6.7 U1	6.7.0
6.7 U3	✓				
6.7 U2	✓	✓			
6.7 U1	✓	✓	✓		
6.7.0	✓	✓	✓	✓	



## Upgrade Order

Simplified vSphere 6.7 deployments using the vCenter Server with embedded PSC make an upgrade easier. Similarly, deployments that leverage external PSC instances, like this scenario, are also easy because the vCenter Server installer can perform the upgrade of the vCenter Server and convergence of the PSC in one single workflow.

To begin the upgrade, we downloaded and mounted the vCenter Server appliance installer ISO to a management machine. Using the vCenter Server appliance ISO, we ran the installer, which launched the workflow to upgrade the appliance. When the upgrade wizard was completed, the installer deployed a new appliance using a temporary IP address. We then exported data from the vCenter Server 6.7 instance and imported it into the new vCenter Server 7. At this point, the appliance was reconfigured to use the same information, such as the FQDN, IP address, certificates, and all reference IDs.

The next step of our upgrade was to import the vSphere 7 ISO into vSphere Update Manager and create an upgrade baseline to remediate our hosts to vSphere 7. Because we were upgrading from vSphere 6.7 to vSphere 7, we were able to take advantage of the Single Reboot Upgrade enhancements to reduce maintenance windows.

After all of the hosts were upgraded to vSphere 7, we proceeded to upgrade the distributed switch version to 7, being careful of the considerations mentioned previously about a chance disruption during an upgrade.

Now, the vSphere upgrade was complete, and we proceeded 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 the upgraded environment, we performed the same tasks using the health assessment tool to make sure we did not see any faults in the vSphere 7 environment. The assessment was successful, so the upgrade was complete.

If you encounter any issues during the validation stage of migration, 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 is to initiate a rollback, but this option has a large impact because the entire environment has been upgraded at this point.



## Scenario 3: Upgrading vSphere 6.7 Environment Using Site Recovery Manager to vSphere 7

The third scenario was an organization migrating from

- vSphere 6.7 with Site Recovery Manager

to

- vSphere 7 with Site Recovery Manager

### Environment Discovery and Assessment

In this scenario, the organization was running vSphere 6.7 GA using the vCenter Server appliance.

An embedded deployment was being used for Enhanced Linked Mode for the production and disaster recovery site.

### Environment Overview

During our discovery phase, we identified the current versions of vCenter Server, ESXi, and Site Recovery Manager in the environment. Through discovery, we also found out the organization was not currently using vSphere Update Manager because they were upgrading ESXi hosts via the CLI. Also, because the organization was running the vCenter Server appliance, we did not need to plan any migration steps.

PRODUCT	CURRENT VERSION	UPGRADE VERSION
vCenter Server appliance	vSphere 6.7	vSphere 7
ESXi	vSphere 6.7	vSphere 7
Site Recovery Manager	Version 8.1	Version 8.3



## 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 requirements for the environment were as follows:

- **vCenter High Availability**

Because we were using Site Recover Manager, management wanted the vCenter Server to be highly available. In the event of a vCenter failure, their environment would have been degraded. To accomplish this requirement, the organization enabled vCenter HA after the upgrade.

- **vCenter Server Backups**

In the event of a failure, management wanted an easy way to restore the vCenter Server. VMware vSphere 6.7 and vSphere 7 have greatly enhanced the built-in file-based backup and restore utility. Not only did we have a method to back up our vCenter Server to an external HTTP/S, FTP/S, NFS, or SMB directory, but also vSphere now has a built-in scheduler and built-in retention. Image-level backups of the vCenter Server appliance are also supported.

- **Orchestrated ESXi Updates**

VMware vSphere Update Manager is included with the vCenter Server appliance in version 6.5 and later. Because the organization did not currently have vSphere Update Manager installed in their environment, when they upgraded from vCenter Server 6.7 to vCenter Server 7, vSphere Update Manager would be included, along with vSphere Lifecycle Manager, and they leveraged vSphere Update Manager baselines for upgrading ESXi hosts to vSphere 7. VMware vSphere Lifecycle Manager helps with managing the declarative state of a vSphere cluster, which avoids configuration drift.

## Compatibility

Making sure products are compatible is the best way to have a successful upgrade the first time.

In this scenario, we wanted to make sure that the versions were compatible. As you can see in the following image, we were able to upgrade from vCenter Server 6.7 to vCenter Server 7.

In the following images, you can see that vCenter Server 7 supports interoperability with Site Recovery Manager 8.3 only. You can also see that Site Recovery Manager 8.1 can upgrade directly to Site Recovery Manager 8.3, without issues.

VMware vCenter Server	7.0	6.7.0
<b>VMware Site Recovery Manager</b>		
8.3	✓	✓
8.2	—	✓
8.1.2	—	✓
8.1.1	—	✓
8.1	—	✓

VMware vCenter Server	7.0	6.7 U3	6.7 U2	6.7 U1	6.7.0	6.5 U3	6.5 U2	6.5 U1	6.5.0
6.7 U3	✓								
6.7 U2	✓	✓							
6.7 U1	✓	✓	✓						
6.7.0	✓	✓	✓	✓					
6.5 U3	✓	✓	✓	✓	—	—			
6.5 U2	✓	✓	✓	✓	✓	✗	✓		
6.5 U1	✓	✓	✓	✓	✓	✓	✓	✓	
6.5.0	✓	✓	✓	✓	✓	✓	✓	✓	✓

## Upgrade Order

Through our compatibility checks, we identified that the environment had to be at Site Recovery Manager 8.1 prior to upgrading to Site Recovery Manager 8.3.

We first upgraded Site Recovery Manager to 8.3 at the Protected site and then at the Recovery Site. Next we upgraded the vCenter Server appliance instances at each site from 6.7 to vCenter Server 7. Site Recovery Manager 8.3 supports vCenter Server versions 6.7 and 7, so this part had to be done first. Because the organization did not have vSphere Update Manager in their environment until the vCenter Server was at version 7, we held off patching until the final step.

To identify the proper upgrade order, we consulted the VMware knowledge base article [Update sequence for vSphere 7.0 and its compatible VMware products \(78221\)](#):

### 1. Site Recovery Manager Update 8.1 to 8.3

- Update vCenter Server 6.0 Update 2 to 6.0 Update 3 using the vCenter Appliance Management Interface.

### 2. vCenter Server Update 6.0 Update 2 to 6.0 Update 3

- Update Site Recovery Manager 6.1.1 to 6.1.2 by downloading the executable and installing it, being sure to upgrade any incompatible Storage Replication Adapters.

### 3. ESXi Upgrade 6.7 to 7

- VMware vSphere Update Manager is now installed in the environment. Use vSphere Update Manager to upgrade the hosts. Upload the ESXi 7 ISO. Then, create a baseline with the ISO and any additional patches or extensions, and install these on the hosts, bringing them to the latest version.

## Validation

Prior to executing the upgrade, we successfully completed 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 the upgraded environment, we performed the same tasks using the health assessment tool to make sure we did not see any faults in the vSphere 7 environment. At this point, we also performed a test failover of the Site Recovery Manager workloads and ensured that everything was functioning. This was successful, and the upgrade was now complete.

If you encounter an issue with your validation during an upgrade, 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 roll back, but because you have upgraded all components, a rollback at this point might have a large impact.



## Phase 3: Post-Upgrade

**Phase 3: Post-Upgrade** discusses what to do after the upgrade is complete. The next step is to perform “Day 2 operations,” ensuring that you have an optimal vSphere 7 experience.

### SSO Domain Repoint

VMware vCenter Server 7 also includes a way to consolidate vSphere single sign-on (SSO) domains. Initially, in vSphere 5.5, any consolidation of SSO domains had to be done prior to upgrade, but with the release of vSphere 6.7 and later, consolidation of vSphere SSO domains is supported.

You are no longer required to deploy and configure a new SSO domain in order to consolidate. The domain repoint tool supports the consolidation and merging of existing SSO domains, as well as removing a vCenter Server from a domain or creating a new SSO domain during a repoint operation.

Using `cmsso-util`, you can run a precheck which identifies any conflicts such as tags, tag categories, licenses, or roles.

**Note:** If you are repointing to a new SSO domain, you lose all global permissions, and you must recreate them. But if you are repointing to an existing SSO domain, then global permissions are inherited.

One 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

If you are wondering how to protect your vCenter Server appliance in case of failure, built-in file-based backup and restore is included with the appliance. This is an important feature: In the event of a failure, you can perform a successful restore of your PSC or vCenter Server. With vSphere 7, VMware improved the backup and restore process by introducing new features such as support for FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB to a remote system, along with a built-in scheduler, allowing retention and simpler restores.

We recommend using the file-based backup and restore when using a vCenter HA cluster, as the feature has built-in logic to ensure that configurations are properly backed up and, in the event of a restore, you are able to restore only a standalone node.

## VMware vCenter High Availability

A very helpful feature in vCenter Server appliance is vCenter HA. VMware vCenter HA allows the creation of a vCenter Server cluster that is highly available 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-zero Recovery Point Objective (RPO) and a 5-minute Recovery Time Objective (RTO), which can vary with the size of inventory and database. When an active vCenter Server fails, vCenter HA can perform an automatic failover to the peer node.

## VMware vSphere Lifecycle Manager

Another feature exclusive to vSphere 7 is VMware vSphere Lifecycle Manager. VMware vSphere Lifecycle Manager facilitates the process of managing the software on the hosts in your environment by addressing today's challenges of using multiple deployment and upgrade methods and tools.

VMware vSphere Lifecycle Manager uses images instead of baselines as vSphere Update Manager does. By introducing the concept of images, vSphere Lifecycle Manager provides a unified platform for ESXi lifecycle management. You can use vSphere Lifecycle Manager for stateful hosts only, but starting with vSphere 7.0, you can convert the Auto Deploy-based stateless hosts into stateful hosts, which you can add to clusters that you manage with vSphere Lifecycle Manager images.

When you use vSphere Lifecycle Manager images, you follow the same workflow and use the same ESXi image format for the install and upgrade, as well as update and patching operations, which significantly simplifies the lifecycle management process.

Using vSphere Lifecycle Manager images helps prevent image drifts that might occur at runtime. With vSphere Lifecycle Manager images, you define the precise software stack to run on your hosts, and no deviation is possible, because vSphere Lifecycle Manager does not allow solutions to push VIBs directly onto the hosts. VMware vSphere Lifecycle Manager images work at the cluster level, and you no longer need to work with individual hosts.

For more information, see the VMware blog post [vSphere 7—Lifecycle Management](#).

# Resource Repository

## Pre-Upgrade Resources

Review these resources for help preparing and planning your upgrade.

[VMware Compatibility Guide](#)

[VMware Product Interoperability Matrices](#)

[vSphere Upgrade: The Inside Track, Part 2: Pre-Upgrade Considerations](#)

[vSphere 7 Upgrade Best Practices \(78205\)](#)

(VMware knowledge base article)

[vSphere Upgrade Technical Webcast Series](#)

(VMware blog post)

[vSphere Upgrade FAQ](#)

## Upgrade Resources

Review these resources for help executing your upgrade.

[vSphere Upgrade](#)

[Upgrading Your vSphere Environment with Site Recovery Manager and vSphere Replication](#)

(VMware blog post)

[Introduction to Automating Your vSphere Upgrade](#)

(VMware blog post)

## 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](#)

[vCenter High Availability](#)

[Use Encryption in Your vSphere Environment](#)

[Repoint vCenter Server to Another vCenter Server in a Different Domain](#)

[Repointing vCenter Server to another SSO Domain](#)

(VMware blog post)

[vSphere 7 – Update Planner](#)

(VMware blog post)

## Knowledge Base Articles

[VMware vSphere Upgrade Policies \(2149713\)](#)

(VMware knowledge base article)

[Important information before upgrading to vSphere 7.0 \(78487\)](#)

(VMware knowledge base article)

[Update sequence for vSphere 7.0 and its compatible VMware products \(78221\)](#)

(VMware knowledge base article)

[vSphere 7 Upgrade Best Practices \(78205\)](#)

(VMware knowledge base article)

[Migrating VMFS 5 datastore to VMFS 6 datastore \(2147824\)](#)

(VMware knowledge base article)

## vSphere 7 Resources

[Introducing vSphere 7: Essential Services for the Modern Hybrid Cloud](#)

(VMware blog post)

[Introducing vSphere 7: Features & Technology for the Hybrid Cloud](#)

(VMware blog post)

[Introducing vSphere 7: Modern Applications & Kubernetes](#)

(VMware blog post)

[Announcing vSAN 7](#)

(VMware blog post)

[VMware vSphere Documentation](#)

[VMware Configuration Maximums](#)

[vSphere Academy](#)

[vSphere Upgrade Center](#)



## About the Author



### **Nigel Hickey**

Nigel Hickey is a Senior Product Line Marketing Manager and VCIX7-DTM in the Cloud Platform business unit at VMware. He is a subject matter expert for vSphere and vCenter Server helping enable the field and a trusted advisor to VMware customers and partners. Nigel can be found blogging on [NigelHickey.com](http://NigelHickey.com) or on Twitter via [@vCenterNerd](https://twitter.com/vCenterNerd).

Join us online:



vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 [www.vmware.com](http://www.vmware.com) Copyright © 2020 VMware, Inc. All rights reserved.  
This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.  
VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: FY21-5868-VMW-UPGRADING-VSPHERE7-EBOOK-USLET-20200921 9/20