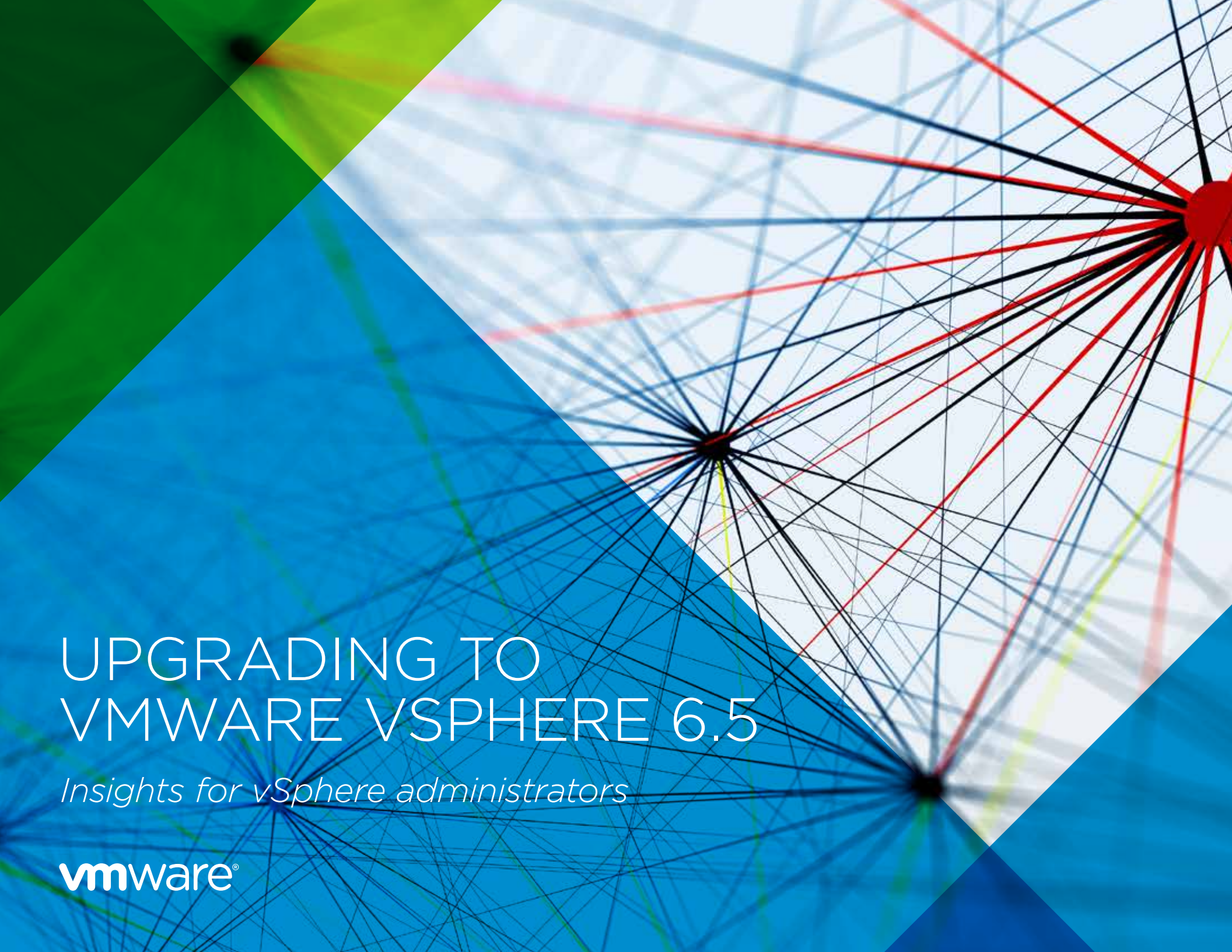


UPGRADING TO VMWARE VSPHERE 6.5

Insights for vSphere administrators

vmware®

Table of Contents

What's New in VMware vSphere® 6.5

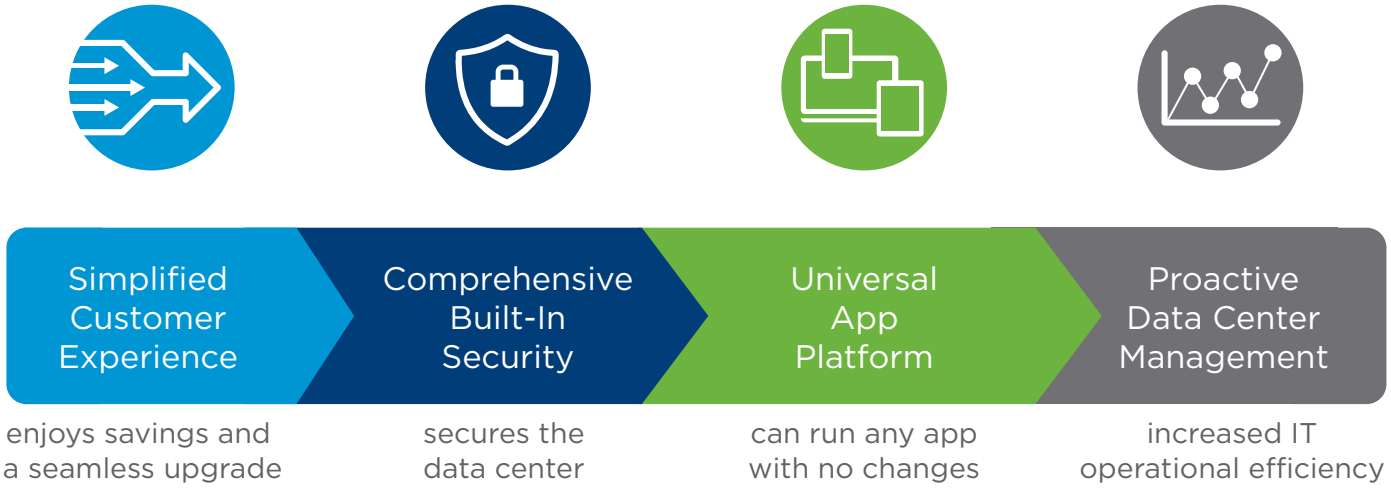
As a VMware vSphere® user, you know that it is the most widely adopted and proven virtualization platform available. In fact, 83 percent of organizations worldwide run vSphere, and rely on it to get the best performance, availability, and efficiency from their applications and infrastructure.

With the wealth of new features and functionality introduced in vSphere 6.5, there's never been a better time to upgrade. Supporting both existing and next-gen apps, vSphere 6.5 provides a simplified user experience, comprehensive built-in security, and a universal app platform. It is a solid foundation on which to adopt or scale the use of cloud across the enterprise.

VMware vSphere 6.5 highlights include:

- HTML5-based vSphere Client supports 90 percent of general workflows
- VMware vCenter® Server Foundation™ now supports 4 hosts (vs. 3) for the same price—a $5,000 savings
- Improved vSphere support and interoperability across ecosystems
- Support for vSphere 6.0 U3 to vSphere 6.5 U1 upgrade path

vSphere 6.5: The Best Foundation for Business Transformation



Keep Going

Check out these resources to learn more about vSphere 6.5.

VIDEOS

vSphere Overview

DOCUMENTS

- Infographic: Top Ten Reasons To Upgrade to vSphere 6.5
- White Paper: What's New in VMware vSphere 6.5 Technical White Paper
- Data Sheet: vSphere 6.5

BLOG POSTS

- Blog Post: Introducing VMware vSphere 6.5
- Blog Post: vSphere 6.5 Update 1 – Under the Hood

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.

In these pages are reference scenarios that explain upgrade concepts that can be applied to just about any situation, including upgrading from vSphere 5.5 to vSphere 6.5, and from vSphere 6.0 to vSphere 6.5 Update 1.

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 process

Phase 3: Post-Upgrade – Validating that the outcome reflects the upgrade plan

Short on time?

Scroll through to the **Key Resources** listed in the beginning of each section, or jump to the Resources Repository.

Prefer interactive tutorials, videos, or documents you can download and read later?

These icons will help you find the formats that work for you.

Documents

Videos

Tools

Assistance

Blog Post

Phase 1: Pre-Upgrade

With the wealth of new features and functionality introduced in vSphere 6.5, there's never been a better time to upgrade. This section will help you get started.

Key Resources

VIDEOS

- vSphere 6.5 YouTube Playlist

TOOLS

- vSphere 6.5 Product Walk Through
- VMware Validated Design Upgrade (for those using the VMware Validated Design implementation)
- VMware Workstation™ or VMware Fusion® Pro (if you have the resources to run them)
- VMware Hands-On Labs – All labs leveraging vSphere v6.5 with the Photon OS.
- In-House Lab – If you have a lab environment at your disposal, try building it as close to your production environment as possible to simulate both the upgrade process and new feature implementation.

ASSISTANCE

VMware Professional Services – Leverage the experience, expertise, and best practices from VMware Professional Services to quickly and efficiently upgrade to vSphere 6.5. Contact your representative for additional information.

Health Assessments

Doing a health assessment of your current environment is critical.

Why, you ask? Picture it. You're midway through the upgrade process and have to stop what you are doing to troubleshoot a time-consuming issue. Hours in, you realize it was related to a misconfiguration with something as simple as DNS or NTP. As a result, the upgrade is delayed, the deadline is missed, and all eyes are on you for an explanation. You don't want this story to be about you, so it's important to know that your infrastructure is ready for upgrade.

And, health assessments often shed light on unused resources—such as virtual machines—that have yet to be decommissioned. For this reason, health assessments should include all components (compute, storage, network, third party) that interact with a vSphere environment. It's also recommended to consult with compute, storage, and network vendors for health assessment best practices and tools.

Sometimes health assessments uncover issues that require the help of support and opening a ticket. Do not proceed with the upgrade until all open support tickets have been resolved. Keep in mind that health assessments shouldn't only be done when preparing for an upgrade, but also routinely.

Keep Going

The following resources provide additional information to help you assess the health of your environment.

TOOLS

Take advantage of tools that can assess and provide a report on your current environment. Most of these tools come with a free 60-day evaluation period, which is enough time to get the information needed.

- VMware vRealize® Operations Manager™ (60-day evaluation provided)
- vSphere Optimization Assessment (60-day evaluation provided)
- VMware {code} vCheck vSphere (community/not supported by VMware)
- Hardware / Storage / Network / third party (check with each of your vendors)

ASSISTANCE

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.

Phase 2: Upgrade

If you're reading this section, and have already completed the recommended actions in Phase 1: Pre-Upgrade, then congratulations! You are ready to move on to Phase 2, which includes planning, coordinating, submitting change controls, and validation.

Note: It is strongly recommended you review and complete Phase 1: Pre-Upgrade before beginning the upgrade. Check out the resources on page 6 if you haven't already.

This section details the upgrade process for two hypothetical scenarios that leverage real-world concepts for you to apply to your specific situation.

Scenario 1: Upgrading from vSphere 5.5 to vSphere 6.5

Scenario 2: Upgrading from vSphere 6.0 to vSphere 6.5 Update 1

Keep in mind, however, that these are example scenarios and not reflective of all vSphere environments.

vSphere 6.5 Upgrade Documentation

Below is a curated list of vSphere 6.5 documentation that is helpful to review prior to starting the upgrade process.

Key Resources

DOCUMENTS

Product Release Notes

- VMware vCenter Server 6.5.0
- VMware vCenter Server 6.5.0 a (Support for NSX 6.3.0)
- VMware vCenter Server 6.5.0 b (Additional functionality added to HTML5 vSphere Client)
- VMware vCenter Server 6.5.0 c (Apache BlazeDS security fix)
- VMware vCenter Server 6.5.0 d (New features for vSAN 6.6)

See the Resource Repository for additional Product Release Notes.

Key Considerations Prior to Getting Started

- Review the vSphere 6.5 release notes to fully understand the upgrade process.
- Watch the new VMware vCenter Server® light board videos to learn about vCenter Server architecture, deployment, and availability as part of the upgrade process.
- Ensure that you have a backup prior to starting the upgrade process, along with a recovery plan in case you need to revert back.
- Open a support request with VMware Support prior to starting your upgrade process—it will expedite the process should any issues come up.
- Map out the schedule for every product upgrade in your environment—it will help you to understand dependencies and prioritize accordingly.
- Plan your time accordingly.

Knowledge Base Articles

Always check the vSphere Knowledge Base site prior to starting an upgrade for the latest documentation. Below is a short list of resources currently available.

- Important information before upgrading to vSphere 6.5 (2147548)
- VMware vSphere Upgrade Policies (2149713)
- Update sequence for vSphere 6.5 and its compatible VMware products (2147289)
- Best practices for upgrading to vCenter Server 6.5 (2147686)
- 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)
- Devices deprecated and unsupported in ESXi 6.5 (2145810)

Guides

- Upgrade Guide for vSphere 6.5
- vSphere 6.5 Configuration Maximums Guide
- VMware Compatibility Guide (HCL)
- Guest Operating System Installation Guide
- vSphere 6.5 Security Configuration Guide (Hardening Guide)

Documentation

- VMware vSphere 6.5 Documentation
- VMware Product Interoperability Matrices

Scenario 1: Upgrading from vSphere 5.5 to vSphere 6.5

1. Environment Discovery and Assessment
2. Requirements and Decisions
3. Compatibility
4. Upgrade Order
5. Validation

Environment Discovery and Assessment

Let's walk through the vSphere 6.5 upgrade process for a company with three data center locations, each running vSphere 5.5 using an embedded vCenter Server deployment on Windows.

Other products in the environment include VMware NSX®, VMware vRealize Automation (vRA), VMware vRealize Operations, and VMware vRealize Log Insight™ (vRLI). Note that vRA is using a separate vCenter Server endpoint from the previously mentioned vCenter Server.

The chart below represents the current version of each product and target (upgrade to) version. Accompanying each product are comments taken from the install or upgrade section found in its release notes.

PRODUCT	CURRENT VERSION	UPGRADE VERSION	COMMENTS
vCenter Server	5.5	6.5 Patch a	vCenter Server 6.5a needed for NSX (KB 2148841)
NSX	6.3	6.3.2	vSphere 5.5 Update 3 minimum
vRealize Automation	7.0	7.3	Side-by-side upgrade
vRealize Operations Manager	6.0.1	6.6	Two-step upgrade 6.0x to 6.3.1 and then 6.6
vRealize Log Insight	N/A	4.5	New to the environment per requirements

- In chart format, make a list of all products in your environment, and specify both the current version and the target (upgrade to) versions.
- Copy the instructions and comments from the install or upgrade sections of the product release notes.
- Include third-party products to ensure they are compatible with vSphere 6.5.

Requirements and Decisions

Next up is to meet with key stakeholders and then compile a list of business requirements. The goal is to not overcomplicate the overall design yet ensure it will meet the needs of the organization.

While business requirements are specific to the unique needs of an organization, here are some to consider.

1: Single Sign-On Functionality

Having a single vSphere single sign-on (SSO) domain will simplify management of the newly upgraded environment. Starting with vSphere 6.0, licensing, global permissions, custom roles, single sign-on, and certificates are replicated throughout the vSphere SSO domain and make it easier and more efficient to manage these shared services across multiple vCenter Servers. Note that vSphere Single Sign-On Domain Consolidation can only be done in vSphere 6.5. It requires an architecture change from embedded to external PSC deployment, and will need to be done prior to the upgrade process.

2. Enhanced Link Mode

In this scenario, each of the three sites operates autonomously and is managed separately. The goal is to create a more efficient design that enables visibility to all three sites, no matter what vSphere Client is used. Doing so requires an external deployment, which will be completed along with vSphere SSO domain consolidation. Enhanced Linked Mode is automatically inherited when new vCenter Servers are added to the same vSphere SSO domain, which means there is nothing to install or configure to take advantage of Enhanced Linked Mode.

3. Simplified Operations

Upgrading to the VMware vCenter Server Appliance™ ensures you can leverage all of the new features in vSphere 6.5. And, the vCenter Server Appliance not only surpasses its Windows counterpart when it comes to features and performance, it also provides native vCenter High Availability, file-based backup and recovery, and integrated vSphere host management and patching.

4. High Availability

For this company, meeting a 10-minute recovery time objective (RTO) is mission-critical, and that means using both VMware vSphere HA and VMware vCenter Server High Availability.

This approach will ensure protection from host and vCenter Server (application) failure. vCenter Server High Availability provides a 5-minute RTO. vCenter Server HA does require a load balancer for Platform Services Controller high availability. Currently F5, NetScaler, and NSX load balancers are supported.

5. Centralized Logging

In this case there is no centralized logging within each site. The hosts and vCenter Server are using the default settings and logs are maintained on each individual node. To change this situation, the decision is made to take advantage of the 25-OSI pack included with each vCenter Server license. This will enable Dashboard and Analytics of logging data helpful for troubleshooting for vSphere products. Windows and Linux agents also are available.

Compatibility

Equally as important as gathering business requirements is validating the compatibility of the products in the environment.

This can be achieved by using the VMware Product Interoperability Matrices referenced in the Phase 1: Pre-Upgrade section.

Here are the steps to follow:

- **Select a Solution**

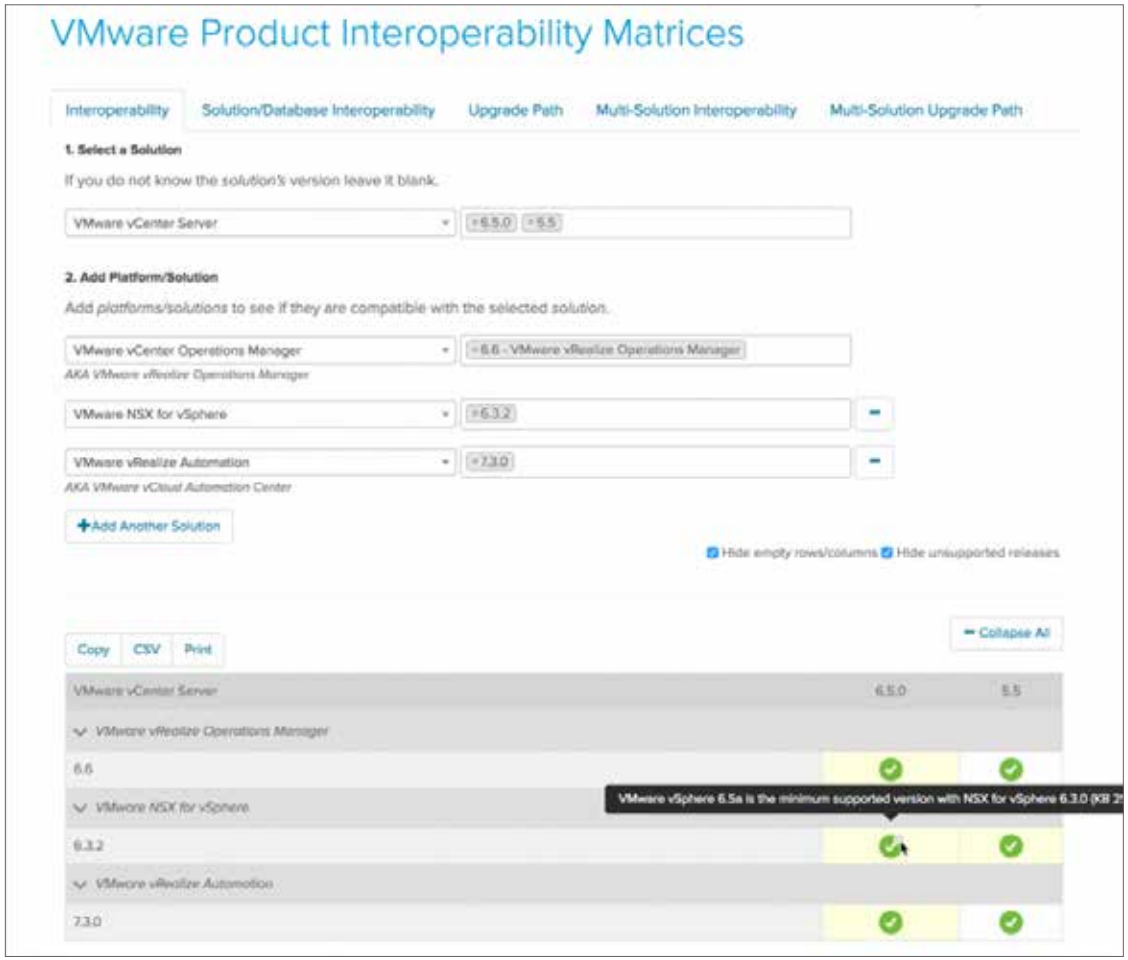
  Start with vCenter Server, given that all of the products included in this scenario communicate with it as an endpoint.

  There is the option to list all versions or specify particular version numbers. vCenter Server will now be displayed in the main horizontal header of the table.

- **Add Platform/Solution**

  List the other solutions that will also be upgraded here. It's important to include both the current version as well as the upgrade version for all solutions to ensure compatibility.

VMware NSX is the only product that has a requirement of vCenter Server 6.5a (also noted in the release notes), so this is the version to download for this scenario.



Use the VMware Product Interoperability Matrices to validate the compatibility of the products in your environment. This upgrade scenario starts with vCenter Server, given that all of the products communicate with it as an endpoint.

Upgrade Order

Now it is time to upgrade all the relevant components in the environment.

DOCUMENTS

Looking for more information on the upgrade process including mapping out the upgrade tasks? Check out the VMware vSphere 6.5 Documentation.

1. **vSphere SSO Domain Consolidation**: Here the upgrade process starts with vSphere SSO domain consolidation to enable single sign-on functionality. Keep in mind this can only be done on vSphere 5.5; once the first node is updated to vSphere 6.5 the ability to consolidate is no longer available. *For scenarios that don't require vSphere SSO domain consolidation, begin with Step 2.*

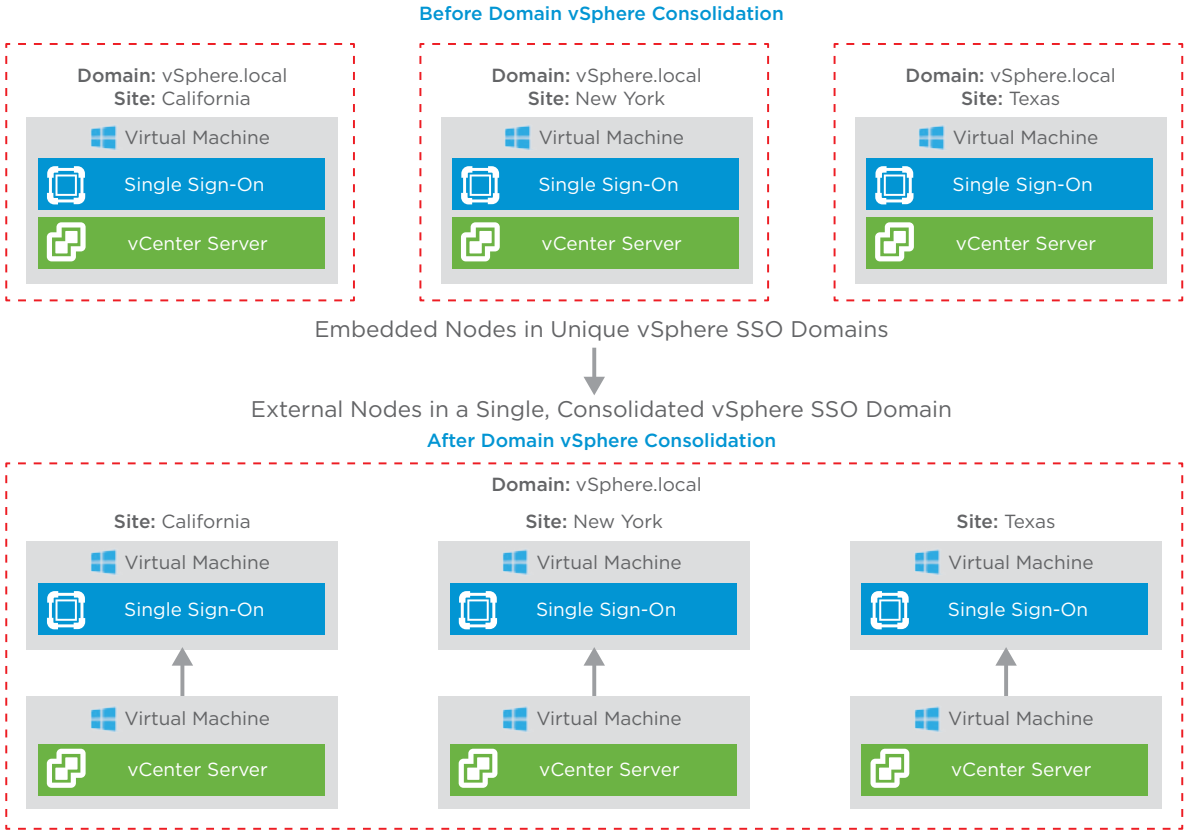


Figure 1: Performing vSphere SSO Domain Consolidation.

For More Information

- VMware Knowledge Base
  Get instructions on how to consolidate a vSphere SSO domain in vSphere 5.5.
- vSphere 6.5 Maximums Guide
  Learn more about the supported number of Single Sign-On servers in a vSphere SSO domain.

2. **Migration:** In this scenario, there is an external deployment spanning multiple sites. One of the requirements is migrating from a Windows-based vCenter Server to the vCenter Server Appliance. *If your deployment is embedded, then proceed directly with your vCenter Server upgrade.*

   A migration also falls under the upgrade category since it is not only copying data (configuration/ inventory by default) from one platform to another (Windows to Photon OS), but also going from version vSphere 5.5 to vSphere 6.5.

   The first step in an external deployment is upgrading or migrating all the Single Sign-On servers within the vSphere SSO domain. This will leave the environment in mixed mode since the Single Sign-On Servers version 5.5 have been upgraded to Platform Services Controllers version 6.5 and vCenter Servers are still on version 5.5. The migration process provides an easy rollback plan since the original source machine is not being changed. This also satisfies the requirement of Enhanced Linked Mode (ELM) because ELM was enabled through the domain consolidation procedure performed in Step 1.

   Note: If Linked Mode is configured in vSphere 5.5, you will have to uninstall it before starting the migration process.

3. **vCenter Server Upgrade:** Now that the environment is in mixed mode, it is important to upgrade or migrate all the vCenter Servers within the vSphere SSO domain as soon as possible. There is no enforced time limit on mixed mode, but it is better to get both vCenter Server Components (PSC and vCenter Server) to ease troubleshooting and to gain all the new functionality in vCenter Server 6.5.

   Begin by upgrading or migrating all the Single Sign-On servers within the vSphere SSO domain. This will leave the environment in mixed mode since the Single Sign-On Servers version 5.5 have been upgraded to Platform Services Controllers version 6.5 and vCenter Servers are still on version 5.5.

   The migration process provides an easy rollback plan since the original source machine is not being changed. This also satisfies the requirement of Enhanced Linked Mode (ELM) because ELM was enabled through the domain consolidation procedure performed in Step 1.

   TIP: If Linked Mode is configured in vSphere 5.5, you will have to break it before starting the migration process.

4. **Upgrade other products making up the management plane:** The product inventory chart completed as part of the pre-upgrade process shows that NSX, vRA, and vROPS need to be upgraded to support vSphere 6.5, as well a any 3rd party products.

5. **Upgrade all ESXi hosts:** While vSphere 5.5 ESXi hosts are supported in a vSphere 6.5 environment, they should not be left as such. Upgrading the hosts provides support for the latest server hardware, an increase in scalability, vSphere Storage vMotion enhancements, and security improvements. Complete host upgrades by using vSphere Update Manager (VUM) either at the cluster or host level.

   A vSphere Update Manager baseline applied at the cluster level can leverage DRS to automatically move the virtual machines from a host. Next place a host in maintenance mode, and automatically start the upgrade process. Once the upgrade of a host has completed, it will exit maintenance mode and move to the next host in the cluster until all hosts are within compliance of the baseline.

6. **Upgrade VMs:**
   - Up-to-date VMware Tools™ ensure maximum performance and management of virtual machines. A guest operating system can run without VMware Tools, but not installing or updating VMware Tools can result in poor operating system performance and limited features and functionality.
   - VM hardware, including the virtual machine BIOS, supported CPUs and memory, and any other hardware-related features can be upgraded in order to take advantage of new capabilities if desired. The virtual machine hardware version can remain at the current version if needed for compatibility reasons, however.
7. **Upgrade Storage:** vSphere 6.5 introduces VMFS6, which includes many enhancements over the previous version of VMFS5. There are multiple ways to migrate an earlier version of VMFS datastore to VMFS version 6.
   - If space permits, create a new datastore and migrate the virtual machines from the existing datastore via Storage vMotion.
   - If space is a constraint, first migrate all of the virtual machines from an existing datastore via Storage vMotion, then once empty, upgrade from VMFS Version 5 to VMFS Version 6, and repeat the process until all datastores have been upgraded.

For More Information

- vSphere 5.5 end of general support is 9/19/2018. Consult the VMware Lifecycle Product Matrix for more information.
- Prior to starting any upgrade make sure to consult with the VMware Product Interoperability Matrices and VMware Compatibility Guide.

8. **Upgrade vSphere licensing from vSphere 5.5 to vSphere 6.5:** Apply the new vSphere 6.x licenses to your vCenter Server and then to your ESXi hosts. There will be a 60-day grace period during the upgrade or migration to allow for the license upgrade.

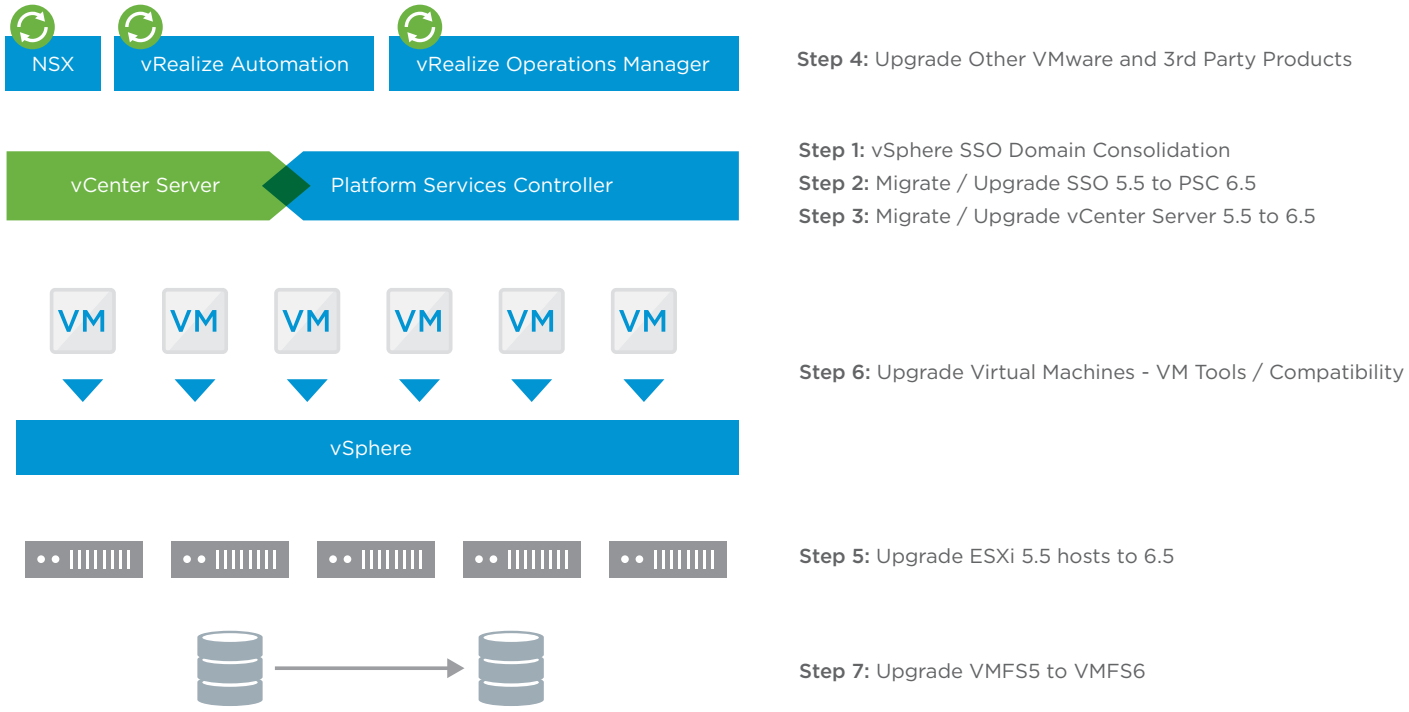


Figure 2: vSphere Upgrade Order

9. **Deploy vRLI for centralized logging at each site:** Configure VCHA to meet the vCenter Server high availability requirement. Any new VMware or third-party products or features can be deployed or configured after the entire upgrade has been completed.

- vSphere Central
  A central resource for all vSphere content including vCenter Server, Resource Management, Security, Automation, Host and Virtual Machine lifecycle, and Operations Management.
- vSphere 6.5 Topology and Upgrade Planning Tool
  Additional guidance for planning for upgrading to vSphere 6.5 as well as new deployments.
- Storage Hub
  Storage and availability technical documents including VMFS Version 6.

Scenario 2:
Upgrading from vSphere 6.0 to vSphere 6.5 Update 1

Environment Discovery and Assessment

In this scenario, the environment includes five data center sites, with three in the U.S. and two in Europe. Each site is running vSphere 6.0 using the vCenter Server Appliance.

An external deployment model is used for enhanced linked mode. There are three vSphere single sign-on (SSO) domains: U.S., Europe, and VDI. Unlike the other deployments, the VDI environment is using an embedded Windows vCenter Server.

The primary storage solution is VMware vSAN™, and SRM is used for disaster recovery in the U.S. data centers only.

Environment Overview

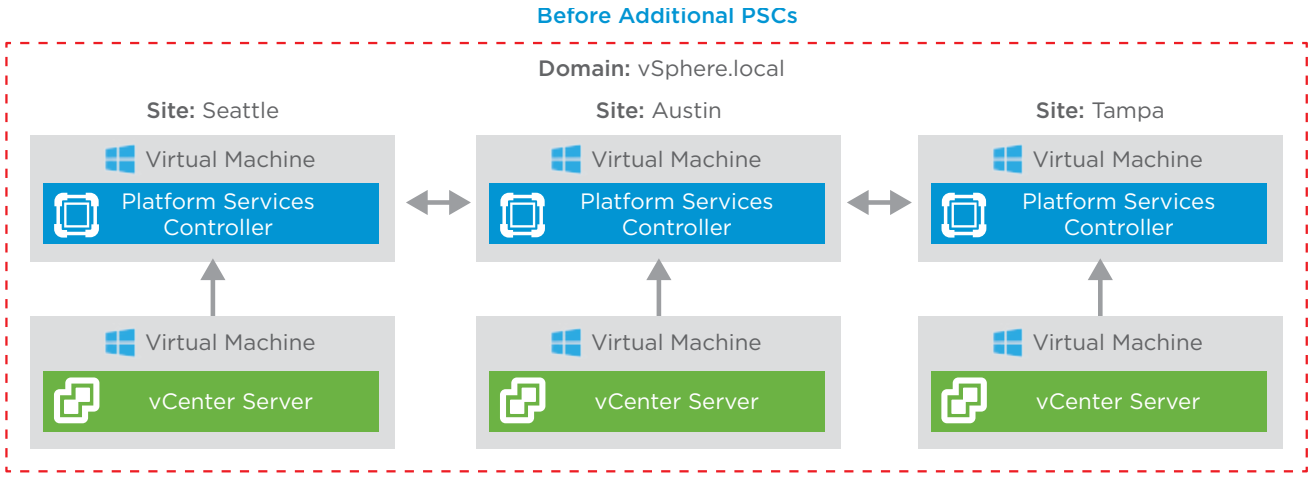


Figure 3: Environment Prior to vSphere Upgrade

- Each site only has one Platform Services Controller (PSC).
- vCenter Servers at each site are not properly backed up.
- There is a Nexus 1000v running in one of the European data centers.
- Windows vCenter Server used for VDI environment.
- SRM is only used in the U.S. data center, no DR solution in the Europe sites.
- Virtual Standard Switches used for host management and vMotion.
- No centralized management of ISOs.
- Clean up of virtual switch port names. Currently, portgroup names are inconsistent and need to be cleaned up.

Further analysis reveals that the current environment is running vSphere 6.0 Update 3, which is not upgradable to vSphere 6.5 but is upgradable to vSphere 6.5 Update 1.

Given that the Dell hardware at each data center is compatible with vSphere 6.5, per the VMware hardware compatibility list, the next step is to list the current and target version for the VMware products.

In chart format, make a list of all products in your environment, and specify both the current version and the target (upgrade to) versions. Copy the instructions and comments from the install or upgrade sections of the product release notes. Include third-party products to ensure they are compatible with vSphere 6.5.

PRODUCT	CURRENT VERSION	UPGRADE VERSION	COMMENTS
vCenter Server	6.0U3	6.5.1	Upgrade first – Has to use 6.5 Update 1 ISO
vSAN	6.2	6.6.1	Upgrade after vCenter Server is on 6.5.1
SRM	6.1.2	6.5.1	SRM upgrade 6.1.x to 6.5.1
VMware Horizon® 7	7.0	7.2	Upgrade after vCenter Server

Requirements and Decisions

1. **External Deployment with a Single PSC**

   As noted previously, there is only a single external PSC at each site and could be a single point of failure.

   The PSC provides authentication and management of the vSphere SSO domain. Based on the RPO and RTO requirements across the company and role the PSC plays in the environment, adding a secondary PSC at each site could be beneficial.

   Let's consider what happens when a PSC is not online and its role in the vSphere SSO domain.

   - Users cannot log in and manage the vCenter Server registered to the PSC that is not online. A single PSC can have as many as 15 vCenter Server appliances registered in a vSphere 6.5 Update 1 SSO domain (not recommended). vCenter Server can only be registered with one PSC at a time (1:1).
   - Workloads are still running, but no new changes or deployments can take place.
   - External PSC is required only for enhanced linked mode, otherwise, use an embedded deployment.
   - Repointing across sites is not supported in vSphere 6.5, only intra-site. This requires having a secondary PSC at each site.

- A load balancer provides automatic failover for vCenter Server and other products using PSC for authentication. The trade-off is the added complexity.
- A load balancer is optional for external deployments without vCenter Server High Availability (VCHA).
- An external deployment with VCHA requires a load balancer for the PSCs as it's not aware of the manual repoint. Also if protecting vCenter Server, PSC should be protected as well.
- Manual repoint of vCenter Server and other products using PSC for authentication via cmsso-util. The trade-off is manual intervention.
- Linear topology within the vSphere SSO domain, easier to manage and provides no extra overhead on the PSCs. The recommendation is to create a ring by adding a replication agreement using vdcrepadmin to have a secondary data path.
- During patching or upgrades repointing can reduce downtime of vCenter Server.

Important resources to help guide with vSphere topology planning and upgrades

- vSphere 6.5 Topology and Upgrade Planning Tool
- vCenter Server and Platform Services 6.5 Architecture
- vCenter Server and Platform Services Controller Deployment Types
- vCenter Server and Platform Services Controller 6.5 High Availability
- vSphere 6.5 Update 1 Maximums Guide (increased since vSphere 6.5 GA)
- Understanding the Impacts of Mixed-Version vCenter Server Deployments

2. vCenter Server Backups

In case of a vCenter Server failure, it is important to ensure a proper backup is available. In this scenario, the backup team uses a third-party backup product for all workloads. The backup solution and schedule did not include vCenter Server and PSC.

The upgraded environment needs to support VADP (VMware vSphere Storage APIs – Data Protection) and must be able to take image-level backups. The vCenter Server Appliance 6.5 has built-in file-based backup and restore. This supports both embedded and external PSC deployments and has the following characteristics:

- Backup can be taken while VCSA or PSC is running, no quiescing required.
- Restore using the VCSA 6.5 ISO which was used to deploy from, no agents needed.
- REST APIs available for automation.
- Windows vCenter Server for VDI will use third-party backup solution for image-level backups until migrated to the VCSA.

Important References for VCSA Backups

- Postgres DB only backups for VCSA are not sufficient, requires entire appliance be backed up
  - Getting Comfortable with vPostgres and the vCenter Server Appliance – Part 1
  - Getting Comfortable with vPostgres and the vCenter Server Appliance – Part 2
  - Getting Comfortable with vPostgres and the vCenter Server Appliance – Part 3
  - KB 2144536 Reinstalling / Migrating vCenter Server 6.X (Windows Only)

3. Network

During discovery it was found that a Nexus 1000v running in one of the European data centers, and vSphere 6.5 Update is the last release to support a third-party switch such as the Cisco Nexus 1000. Now is the time to migrate to the VMware Virtual Distributed Switch (VDS), and to clean up other network items:

- Move this environment to a Virtual Distributed Switch (VDS) using the Nexus 1000v to VDS migration tool.
- Write a powercli script to find and decommission any empty portgroups in the environment.
- Create more meaningful names for portgroups (currently they are listed as portgroup with a random number).
- Assign unique names for all VDS and Distributed portgroups in the same network folder, as required by vSphere 6.5. Note: Prior versions of vSphere allowed the same name (KB 2147547).
- Migrate the management and vMotion portgroups from a VSS to VDS.

Important References for VDS

- Exporting/importing/restoring Distributed Switch configs using vSphere Web Client (2034602)
- Link Aggregation Control Protocol (LACP) with VMware vSphere 5.1.x, 5.5.x and 6.x (2120663)
- FAQ: Discontinuation of third-party vSwitch program (2149722)

4. Content Management

In this scenario ISOs are placed on different vSAN datastores and in some cases stored on their business owners' local machines.

Creating a centralized library that business owners subscribe to will improve efficiency and simplify management.

- Implementing Content Library at each data center in a subscription model.
- vSphere 6.5 uses Content Library as an option to install new operating systems and applications on VMs using Content Library ISO file option. This will help ensure that ISOs don't get copied to a datastore or local machine.
- Business owners can now check their content library before downloading an ISO to avoid duplicates.
- After ISOs Kyle will look at VM templates. VM templates can be managed by content library, but currently in OVF format.

5. Upgrade Order

Now it is time to upgrade all the relevant components in the environment.

Keep Going:
Looking for more information on the upgrade process including mapping out the upgrade tasks? Check out the VMware vSphere 6.5 Documentation.

We're starting with the smallest of the vSphere SSO domains (the VDI environment), and then moving on to the European data centers, and finally the U.S. data centers.

VDI Environment

Tips:
- Back up a VDI environment prior to beginning an upgrade.
- Run this script to get a time estimate for the migration process. Add buffer to the estimated time in case of issues.

1. The embedded vCenter Server 6.0 U3 will need to be migrated to 6.5 U1. All of the components (PSC, VC, VUM) reside on one virtual machine and will be migrated to a VCSA with embedded PSC. This will be done using the migration tool included in the VCSA 6.5 Update 1 ISO.
2. Upgrade the Horizon server from 7.0 to 7.2 (be sure to upgrade the View in Horizon components in the correct order).
3. Use VUM to upgrade the ESXi hosts for the VDI environment.

4. Upgrade VM tools, then upgrade the Horizon Agent in the virtual desktops.
5. Configure vCenter Server protocol (FTP, FTPS, HTTP, HTTPS, SCP) for backup. The native backup can be done manually or can be automated using the APIs.

European Data Centers

1. Use the Nexus 1000v to VDS migration tool and complete network cleanup tasks.
2. Back up the PSCs and vCenter Servers prior to upgrading.

   Note: *It is not necessary to shut down all the PSCs to take a snapshot. The PSCs are multi-master so all the information is replicated across the vSphere domain.*
3. Upgrade all the PSCs in the vSphere SSO domain from 6.0 U3 to 6.5 U1 first. Initially there are only two in this scenario, but additional PSCs will be added later. Mount the VCSA 6.5 U1 ISO, select the upgrade option from the Installer menu, and go through the wizard to upgrade the PSCs.

   Now that the environment is in mixed mode it is important to upgrade all the vCenter Server appliances within the vSphere SSO domain as soon as possible. There is no enforced time limit on mixed mode, but it is better to get both vCenter Server components (PSC and vCenter Server) on the same version from a troubleshooting perspective and to gain all the new functionality in vCenter Server 6.5.
4. Upgrade all vCenter Server appliances within the vSphere SSO domain from 6.0 U3 to 6.5 U1 by mounting the VCSA 6.5 U1 ISO and selecting the upgrade option from the installer menu.
5. Since there are only two PSCs—one at each site—some replication agreements will need to be cleaned up using vdcrepadmin once the process is complete. This will also provide the ability to manually repoint within each site in case of a PSC failure.
   - Original PSC #1 in the London site connected to original PSC #2 in the Berlin site.
   - Deploy a new secondary PSC # 2 in the London site. Replication partner is the original PSC # 1 in the London site.
   - Deploy new a secondary PSC #2 in the Berlin site. Replication partner is the original PSC # 1 in the Berlin site.
   - Use vdcrepadmin to create a new replication agreement from PSC # 2 in the Berlin site to PSC # 1 in the London site.
   - Clean up the old replication agreement between the original PSC #1 in the London site and the original PSC #1 in the Berlin site.

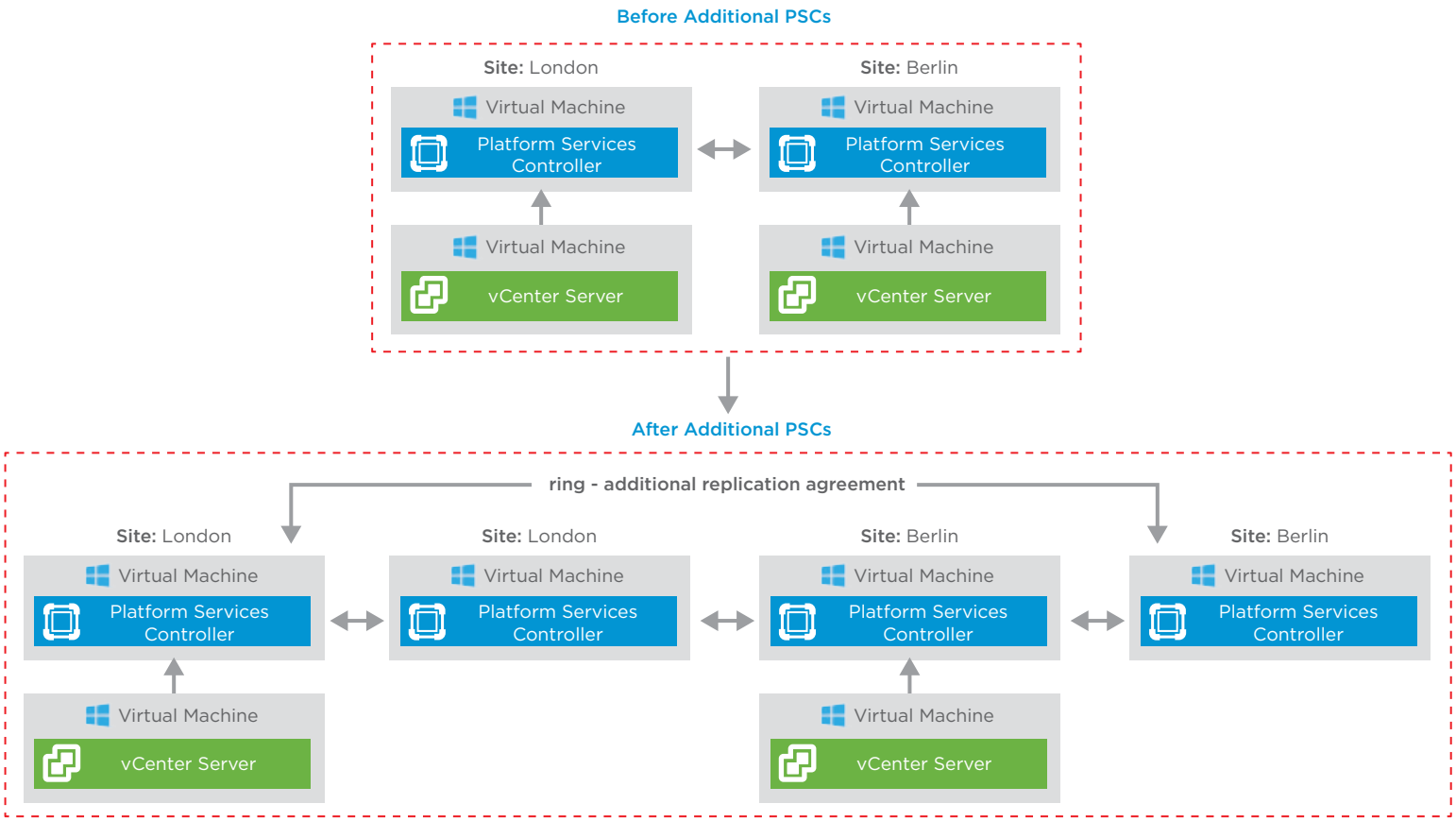


Figure 4: Before and after diagrams once additional PSCs are added and replication agreements addressed.

6. Upgrade vSAN.
7. Upgrade SRM.
8. Upgrade ESXi hosts using VUM.
9. Upgrade VM tools and compatibility.
10. Upgrade VMFS.
11. Configure vCenter Server protocol (FTP, FTPS, HTTP, HTTPS, SCP) for backup. The native backup can be done manually or can be automated using the APIs. While only one of PSCs in the vSphere SSO domain needs to be backed up, there is no harm in backing all of them up. The restore process of a PSC is only required in the scenario where all PSCs within the vSphere SSO Domain are lost. If

there is at least one surviving PSC, then the recommended recovery method is to just re-deploy fresh PSCs to replace those that failed.

U.S. Data Centers

1. Complete network cleanup tasks.
2. Back up the PSCs and vCenter Servers prior to upgrading. **Note:** It is not necessary to shut down all the PSCs to take a snapshot. *The PSCs are multi-master so all the information is replicated across the vSphere domain.*
3. Upgrade all the PSCs in the vSphere SSO domain from 6.0 U3 to 6.5 U1 first. In this case, we only have two, but will be adding additional PSCs later. Mount the VCSA 6.5 U1 ISO and select the upgrade option from the installer menu and go through the wizard to upgrade the PSCs. Now that the environment is in mixed mode, it is important to upgrade all the vCenter Server appliances within the vSphere SSO domain as soon as possible. There is no enforced time limit on mixed mode, but it is better to get both vCenter Server components (PSC and vCenter Server) on the same version from a troubleshooting perspective and to gain all the new functionality in vCenter Server 6.5.
4. Upgrade all vCenter Server Appliances within the vSphere SSO domain from 6.0 U3 to 6.5 U1 by mounting the VCSA 6.5 U1 ISO and selecting the upgrade option from the Installer menu.
5. Add a secondary PSC at each site. We will have to make sure that we clean up some replication agreements once we are done using vdcrepadmin.
   - Original PSC #1 in the Seattle site connected to original PSC #2 in the Austin site.
   - Original PSC #2 in the Austin site connected to the original PSC in the Tampa site.
   - Deploy a new secondary PSC #2 in the Seattle site. Replication partner is the original PSC #1 in the Seattle site.
   - Deploy a new secondary PSC #2 in the Austin site. Replication partner is the original PSC #1 in the Austin site.
   - Deploy a new secondary PSC #2 in the Tampa site. Replication partner is the original PSC #1 in the Tampa site.
   - Use vdcrepadmin to create a new replication agreement from PSC #2 in the Tampa site to PSC #1 in the Seattle site for the ring.
   - Create a new replication agreement between newly deployed PSC #2 in the Seattle site with PSC #1 in the Austin site.
   - Create a new replication agreement between newly deployed PSC #2 in the Austin site with PSC #1 in the Tampa site.
   - Clean up the old replication agreement between original PSC #1 in the Seattle site and the original PSC #1 in the Austin site.
   - Clean up the old replication agreement between the original PSC #1 in the Austin site and the original PSC #1 in the Tampa site.
   - Use vdcrepadmin to validate you have a linear topology.

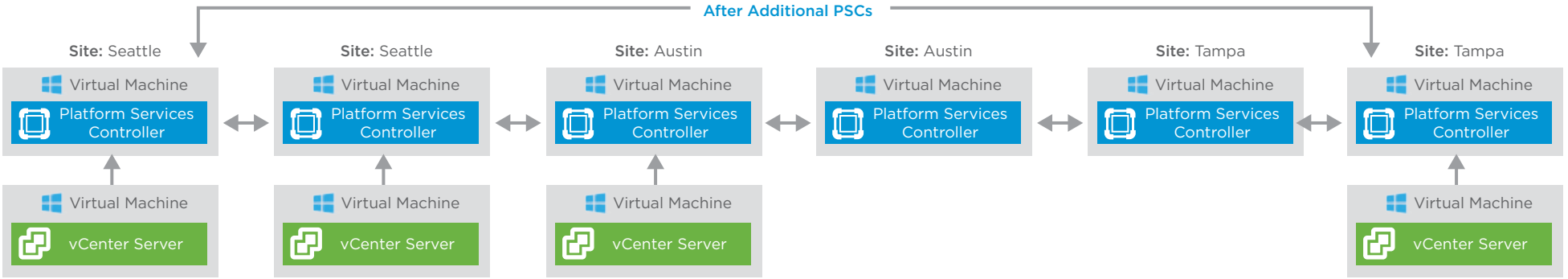


Figure 5: vSphere SSO Domain Built with a Ring Topology

6. Upgrade vSAN
7. Upgrade SRM.
8. Upgrade ESXi hosts using VUM.
9. Upgrade VM tools and compatibility.
10. Upgrade VMFS.
11. Configure vCenter Server protocol (FTP, FTPS, HTTP, HTTPS, SCP) for backup. The native backup can be done manually or can be automated using the APIs. While only one of the PSCs in the vSphere SSO domain needs to be backed up, there is no harm in backing all of them up. Remember that the restore process of a PSC is only required in the scenario where all PSCs within the vSphere SSO domain are lost. If there is at least one surviving PSC, then the recommended recovery method is to just re-deploy fresh PSCs to replace those that failed.

Phase 3: Post-Upgrade

Validating that the outcome of the upgrade accurately reflects what was planned is the final step.

Here are some tips to ensure success:

- Meet with the team to explain what the upgrade process involves and what it means for them. Ask questions to get a better understanding of their issues and requirements.
- Keep the business owners in the loop during the entire upgrade process.
- Create and submit a change control that details the validation testing required of business owners (such as testing applications in a lab environment) as well as a rollback plan. Require business owners to sign off on the document.

Resource Repository

BLOG POSTS

- Introducing VMware vSphere 6.5
- VMware Sphere 6.5 Update 1 – Under the Hood
- Getting Comfortable with vPostgres and the vCenter Server Appliance – Part 1
- Getting Comfortable with vPostgres and the vCenter Server Appliance – Part 2
- Getting Comfortable with vPostgres and the vCenter Server Appliance – Part 3
- vCenter Server Appliance 6.5 Migration Walkthrough
- Understanding the Impacts of Mixed-Version vCenter Server Deployments

DOCUMENTS

- Data Sheet: vSphere 6.5
- Documentation: Implementing Content Library
- Documentation: VMware Product Interoperability Matrices
- Documentation: VMware vSphere 6.5
- Infographic: Top Ten Reasons To Upgrade to vSphere 6.5
- Release Notes: vSphere 6.5 release notes
- Technical White Paper: What's New in VMware vSphere 6.5

GUIDES

- Guest Operating System Installation Guide
- Upgrade Guide for vSphere 6.5
- VMware vSphere 6.5 Configuration Maximums Guide
- VMware Compatibility Guide (HCL)
- Guest Operating System Installation Guide
- VMware vSphere 6.5 Security Configuration Guide (Hardening Guide)
- VMware Sphere 6.5 Update 1 Maximums Guide (increased since vSphere 6.5 GA)

Resource Repository (continued)

KNOWLEDGE BASE ARTICLES

- Best Practices for upgrading to vCenter Server 6.5 (2147686)
- Detect and update duplicate names of Distributed Virtual Switches and Distributed Virtual Portgroups before upgrading vCenter Server (2147547)
- Devices deprecated and unsupported in ESXi 6.5 (2145810)
- Exporting/importing/restoring Distributed Switch configs using vSphere Web Client (2034602)
- FAQ: Discontinuation of third party vSwitch program (2149722)
- How to consolidate a vSphere SSO domain in vSphere 5.5. (2033620)
- Information before upgrading to vSphere 6.5 (2147548)
- Link Aggregation Control Protocol (LACP) with VMware vSphere 5.1.x, 5.5.x and 6.x (2120663)
- Migrate the management and vMotion portgroups from a VSS to VDS (1010614)
- Migrating VMFS 5 datastore to VMFS 6 datastore (2147824)
- Reinstalling / Migrating vCenter Server 6.X (Windows Only) (2144536)
- Supported and Deprecated Topologies for VMware vSphere 6.5 (2147672)
- Supported Upgrade paths for vSAN 6.6 (2149840)
- Update Sequence for vSphere 6.5 and its compatible VMware products (2147289)
- VMware Lifecycle Product Matrix
- VMware vSphere Upgrade Policies (2149713)

PRODUCT RELEASE NOTES

- VMware vCenter Server 6.5.0
- VMware vCenter Server 6.5.0 a (Support for NSX 6.3.0)
- VMware vCenter Server 6.5.0 b (Additional functionality added to html5 vSphere Client)
- VMware vCenter Server 6.5.0 c (Apache BlazeDS security fix)
- VMware vCenter Server 6.5.0 d (New features for vSAN 6.6)
- VMware vCenter Server 6.5.0 e

Resource Repository (continued)

PRODUCT RELEASE NOTES (continued)

- VMware vCenter Server 6.5.0 f
- VMware vCenter Server 6.5.0 Update 1
- VMware vCenter Server 6.5.0 Update 1b
- VMware vCenter Server 6.5.0 Update 1c
- VMware vCenter Server 6.5.0 Update 1d
- VMware vCenter Server 6.5.0 Update 1e

TOOLS

- Download Migration Tool – Nexus 1000v to VDS VMware Fusion
- VMware Hands-On Labs MyVMware Portal
- VMware vRealize Operations Manager (60-day evaluation provided)
- VMware vSphere 6.5 Product Walk Through
- VMware vSphere Optimization Assessment (60-day evaluation provided)
- VMware vSphere 6.5 Topology and Upgrade Planning Tool
- vCheck vSphere (VMware {code})
- VMware Validated Design Upgrade
- VMware Workstation

VIDEOS

- VMware vSphere Overview
- VMware vSphere 6.5 YouTube Playlist
- VMware vCenter Server light board
- VMware vCenter Server and Platform Services 6.5 Architecture
- VMware vCenter Server and Platform Services Controller Deployment Types
- VMware vCenter Server and Platform Services Controller 6.5 High Availability

About the Author

Emad Younis

Emad Younis is a senior technical marketing engineer in the Cloud Platform business unit at VMware. He currently focuses on the vCenter Server Appliance, vCenter Migrations, and VMware Cloud on AWS. Previous to VMware he worked as a virtualization architect designing and implementing large enterprise vSphere environments both as a customer and partner. Emad writes for the VMware vSphere blog, as well as his personal blog, emadyounis.com. Get notifications of new blog posts and more by following Emad on Twitter @emad_younis.

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