



What's New in VMware vSphere® 6.5

TECHNICAL WHITE PAPER

Table of Contents

What's New in VMware vSphere 6.5	4
VMware vCenter Server	4
Migration	4
Improved Appliance Management	5
VMware vCenter High Availability	6
Backup and Restore	8
vSphere Web Client	8
vSphere Client	9
Content Library.....	9
vSphere Host Lifecycle Management Enhancements.....	10
vSphere Update Manager	10
VMware Tools and Virtual Hardware Upgrades	10
Previous Windows-Based Architecture Still Offered	11
Host Profiles	11
Profile Management Improvements	11
Operational Enhancements.....	12
Auto Deploy	12
Manageability Improvements	12
Performance and Resiliency Enhancements.....	14
VMware Tools 10.1 and 10.0.12	14
Signed ISO Images.....	14
Bifurcation of VMware Tools for Legacy and Current Guests	14
Bundling of Tools for Most Popular Guests Only.....	14
Guest OS Granularity Increase	15
Detailed Display of VMware Tools Type and Version in vSphere Web Client.....	15
Improved Detection of Availability of Updated VMware Tools Installers.....	15
vSphere Operations	16
Operations Management.....	16
Log Monitoring.....	17
Developer and Automation Interfaces	18
Application Program Interfaces.....	18
vCenter Server Appliance API.....	18
Virtual Machine API	18
Discover the APIs with the New API Explorer	19
Process Improvements.....	19
Command-Line Interfaces.....	20
VMware PowerCLI.....	20

Core vSphere Module	21
Storage Module	21
VMware Horizon Module	21
Security	22
Virtual Machine Encryption.....	22
Encrypted vMotion	23
Secure Boot Support.....	24
Virtual Machine Secure Boot.....	24
ESXi Host Secure Boot.....	25
Enhanced Logging	26
VM Sandboxing	27
Automation	27
vSphere 6.5 Availability Enhancements.....	28
Proactive HA.....	28
VMware vSphere High Availability Orchestrated Restart.....	28
vSphere HA Admission Control Improvements.....	29
vSphere HA Support for NVIDIA GRID vGPU Configured VMs.....	29
VMware vSphere Fault Tolerance	30
Resource Management Enhancements.....	30
Predictive DRS	30
Improved vSphere DRS Load Balancing Algorithm	30
vSphere DRS Additional Options.....	30
Network-Aware vSphere DRS.....	31
VMware vSphere Storage I/O Control Using	
Storage Policy Based Management.....	31
vSphere Integrated Containers	32
vSphere 6.5 Storage Enhancements.....	33
Advanced Format Drives and 512e Mode.....	33
Automated UNMAP.....	33
LUN Scalability.....	33
NFS 4.1 Support	33
Software iSCSI Static Routing Support.....	33
vSphere 6.5 Networking Enhancements	34
Dedicated Gateways for VMkernel Network Adapter	34
SR-IOV Provisioning	34
Support for ERSPAN	34
Improvements in DATAPATH	34
Conclusion	34
About the Authors.....	35

What's New in VMware vSphere 6.5

VMware vSphere® 6.5 is the next-generation infrastructure for next-generation applications. It provides a powerful, flexible, and secure foundation for business agility that accelerates the digital transformation to cloud computing and promotes success in the digital economy. vSphere 6.5 supports both existing and next-generation apps through its 1) simplified customer experience for automation and management at scale; 2) comprehensive built-in security for protecting data, infrastructure, and access; and 3) universal application platform for running any app anywhere. With vSphere 6.5, customers can now run, manage, connect, and secure their applications in a common operating environment, across clouds and devices.

This paper will discuss the new and enhanced features in vSphere 6.5 across various areas of technology. For additional information, see [VMware vSphere Documentation](#).

VMware vCenter Server

VMware vCenter Server® 6.5 has many new and innovative features. The installer has been overhauled, resulting in a new, modern look and feel. It is now supported on Microsoft Windows, macOS, and Linux operating systems (OSs) without the need for any plug-ins. With vSphere 6.5, the VMware vCenter Server Appliance™ has surpassed the Windows installable version. It offers the following exclusive features:

- Migration Tool
- Improved appliance management
- Native high availability
- Native backup and restore

There are also general improvements to vCenter Server 6.5, including the vSphere Web Client and the *fully supported* HTML5-based vSphere Client.

Migration

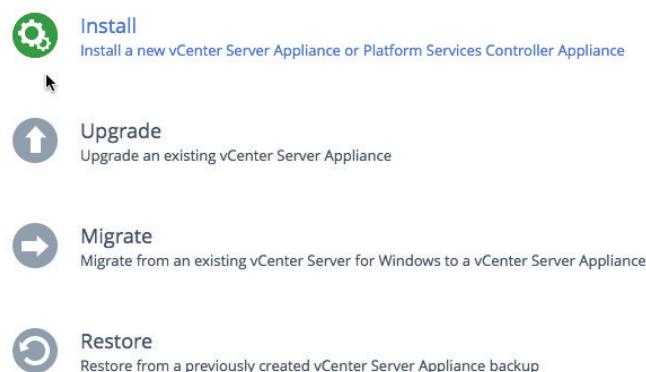


Figure 1. The New, Modern vCenter Server Appliance 6.5 Installer Including Migrate and Restore Options

The installer has a built-in Migration Tool, providing easy access to the vCenter Server Appliance 6.5. This new version of Migration Tool provides several improvements over the recent [vSphere 6.0 Update 2m](#) release, including support for Windows vCenter Server 5.5 and 6.0. And VMware vSphere Update Manager™ is now part of the vCenter Server Appliance 6.5, which is especially valuable to customers that have been waiting to migrate to vCenter Server Appliance without managing a separate Windows server for vSphere Update Manager. For customers that have already migrated to the vCenter Server Appliance 6.0, the upgrade process will migrate vSphere Update Manager baselines and updates to the vCenter Server Appliance 6.5. During the migration process, the vCenter Server configuration, inventory, and alarm data are migrated by default. vSphere 6.5 provides improvements in data selections in three areas:

- Configuration
- Configuration, events, and tasks
- Configuration, events, tasks, and performance metrics

Data is migrated from any database supported in vSphere 5.5 or 6.0 to an embedded vPostgres database. This applies to databases running embedded or remote Microsoft SQL, Oracle, or PostgreSQL databases.

Improved Appliance Management

vCenter Server Appliance 6.5 also exclusively provides improved appliance management capabilities. The vCenter Server Appliance Management interface continues its evolution and exposes additional configuration data. In addition to CPU and memory statistics, it now shows network and database statistics, disk space usage, and health data. This reduces reliance on a command-line interface for simple monitoring and operational tasks.

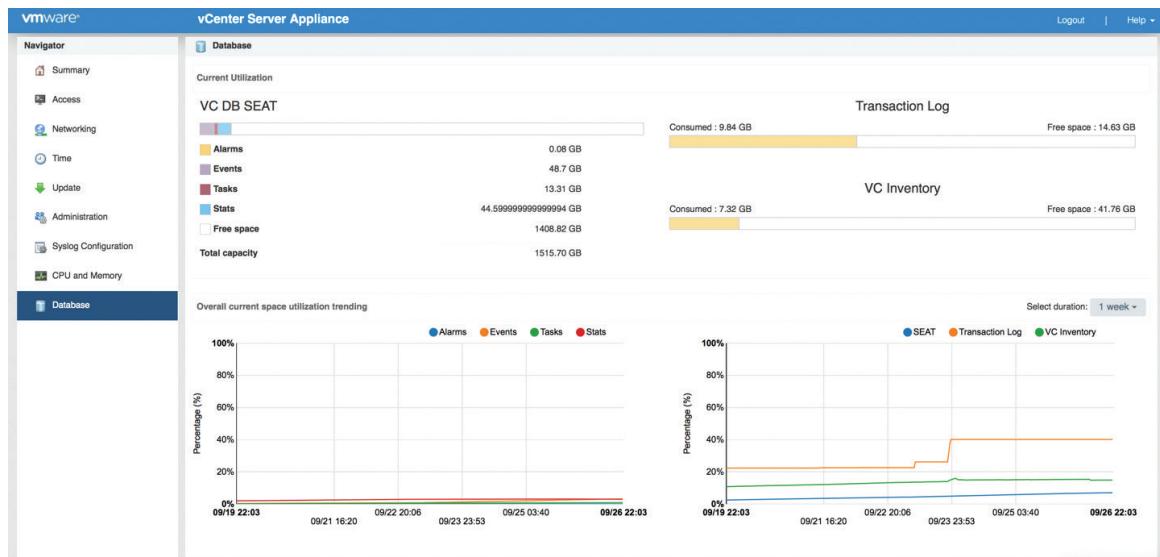


Figure 2. Improved vCenter Server Appliance Management Interface Including New vPostgres Visibility

The new vCenter Server Appliance Management interface is still accessed via port 5480 for any vCenter Server or Platform Services Controller™ appliance. Figure 2 shows the new vCenter Server database monitoring screen, which provides excellent insight into PostgreSQL database disk usage. This in turn helps prevent crashes due to the lack of available space. The vSphere Web Client provides new default warnings that alert administrators when the database is close to running out of space. It also provides a graceful shutdown mechanism at 95 percent full, which helps prevent database corruption. Customers can also configure Syslog settings in the improved vCenter Server Appliance Management interface.

VMware vCenter High Availability

vCenter Server 6.5 has a new native high availability solution that is available exclusively for vCenter Server Appliance. This solution consists of active, passive, and witness nodes that are cloned from the existing vCenter Server instance. The VMware vCenter® High Availability (vCenter HA) cluster can be enabled, disabled, or destroyed at any time. There is also a maintenance mode that prevents planned maintenance from causing an unwanted failover.

vCenter HA uses two types of replication between the active and passive nodes: Native PostgreSQL synchronous replication is used for the vCenter Server database; a separate asynchronous file system replication mechanism is used for key data outside of the database.

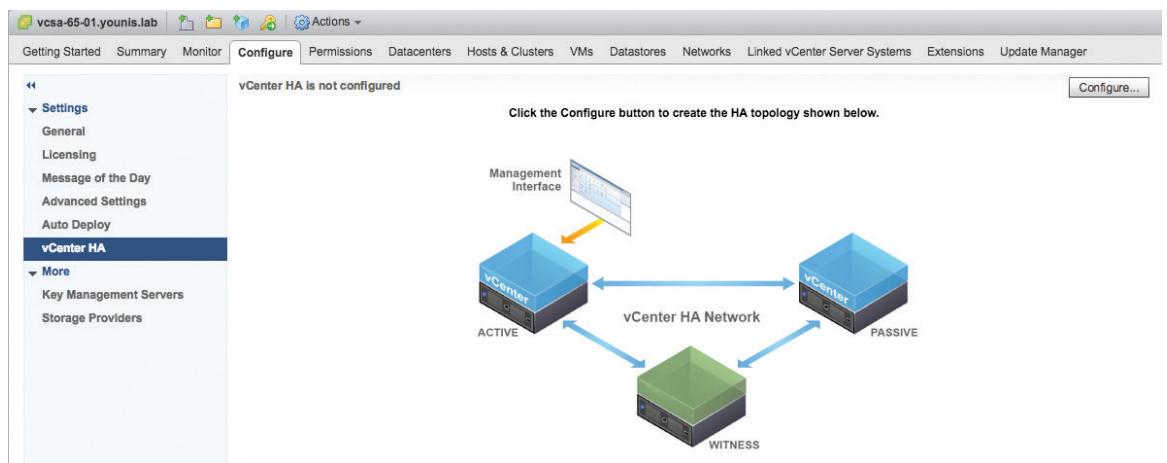


Figure 3. vCenter HA Configuration Page

Two workflows—basic and advanced—can deploy vCenter HA. The basic workflow can be used in most scenarios in which all vCenter HA nodes run within the same cluster. As its name suggests, this workflow is very simple and automatically creates the passive and witness nodes. It also creates VMware vSphere Distributed Resource Scheduler™ (vSphere DRS) anti-affinity rules if vSphere DRS is enabled on the destination cluster and uses VMware vSphere Storage DRS™ for initial placement if enabled. Some flexibility is built into this workflow, so users can choose specific destination hosts, datastores, and networks for each node. This is a very simple, easy way to get a vCenter HA cluster up and running. The alternative is the advanced workflow. This workflow can be used when the active, passive, and witness nodes are to be deployed to different clusters, vCenter Server instances, or even other data centers. This process requires the customer to manually clone the source vCenter Server instance for the passive and witness nodes and to then place those nodes in the chosen locations with the appropriate IP address settings. This is a more involved process, but it enables greater flexibility for those customers that require it.

From an architecture perspective, vCenter HA supports both embedded and external Platform Services Controller use. An embedded Platform Services Controller instance can be used when there are no other vCenter Server or Platform Services Controller instances within the single sign-on domain. In other words, an external Platform Services Controller instance is required when there are multiple vCenter Server instances in an Enhanced Linked Mode configuration. When using vCenter HA with an external Platform Services Controller deployment, an external load balancer is required to provide high availability to the Platform Services Controller instances. There is little benefit to using vCenter HA without also providing high availability at the Platform Services Controller layer. Supported load balancers for Platform Services Controller instances in vSphere 6.5 include VMware NSX®, F5 BIG-IP LTM, and Citrix NetScaler.

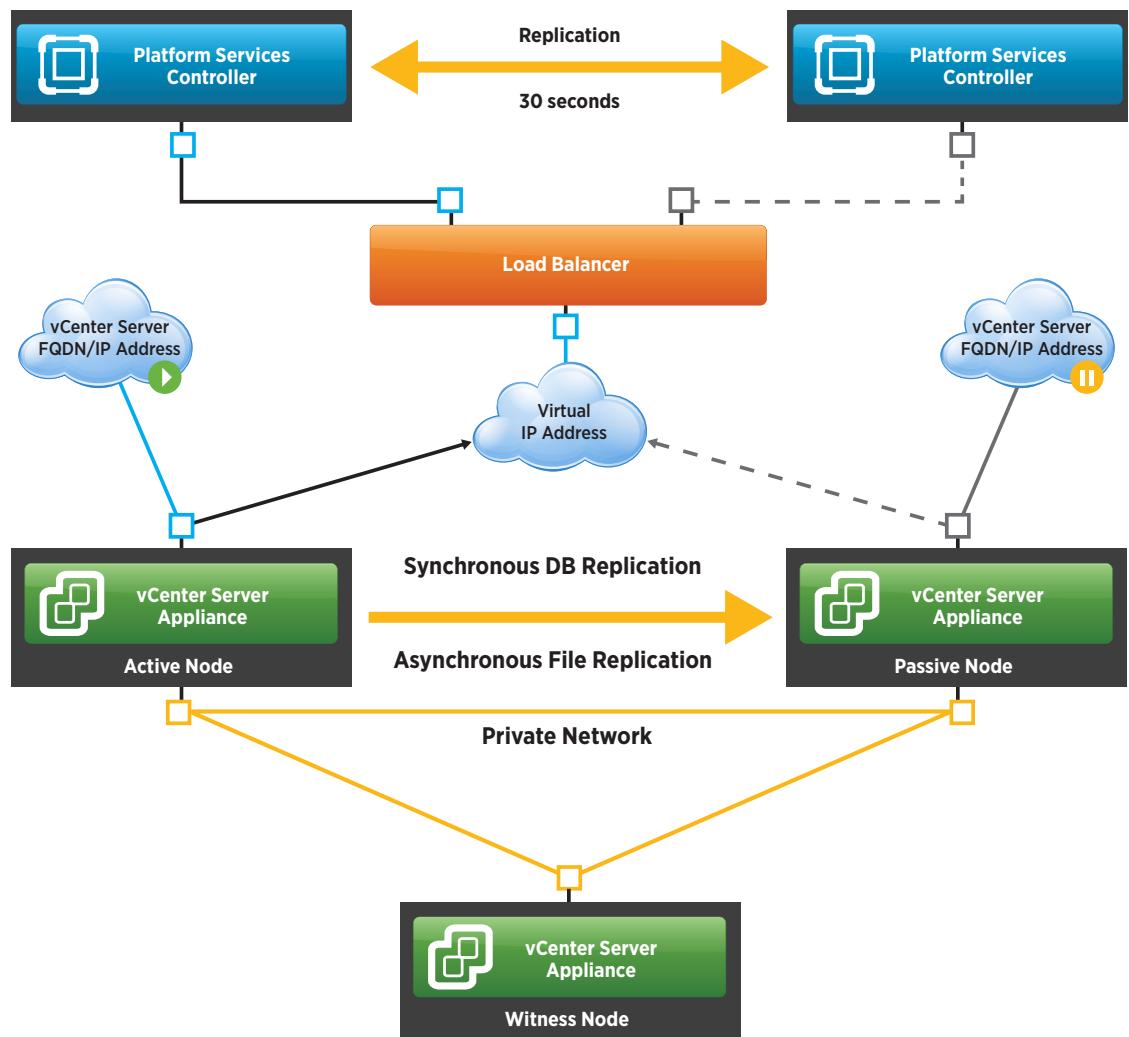


Figure 4. Architecture of vCenter HA and Platform Services Controller HA with a Load Balancer

Failover can occur when an entire node is lost—host failure, for example—or when certain key services fail. For the initial release of vCenter HA, a recovery time objective (RTO) of about 5 minutes is expected, but this can vary slightly depending on the load, size, and capabilities of the underlying hardware. During a failover event, a temporary Web page is displayed, indicating that a failover is in progress. This page then automatically refreshes to the vSphere Web Client login page when the vCenter Server instance returns online. A user who is not active during a failover might not be prompted to log in again. However, any active users will be redirected to the temporary splash page.

There are also significant availability improvements in the watchdog services department, with a new service life cycle framework called vMon. vMon unifies the previous five [watchdog services in vCenter Server 6.0](#) as a single source of truth to simplify managing and monitoring vCenter Server services. vMon also helps keep track of service dependencies, which can become extremely complex. In addition, features such as vCenter HA leverage vMon to help determine when to fail over to another node.

Backup and Restore

New in vCenter Server 6.5 is native backup and restore for the vCenter Server Appliance. This new, out-of-the-box functionality enables users to back up vCenter Server and Platform Services Controller appliances directly from the VAMI or API. The backup consists of a set of files that is streamed to a storage device of the user's choosing using SCP, HTTP(S), or FTP(S) protocols. This backup fully supports vCenter Server Appliance instances with both embedded and external Platform Services Controller instances.

The restore workflow is launched from the same ISO from which the vCenter Server Appliance or Platform Services Controller instance was originally deployed or upgraded. A new vCenter Server Appliance instance is deployed and then uses the chosen network protocol to ingest the backup files. The vCenter Server UUID and all configuration settings are retained. There is also an option to encrypt the backup files via symmetric key encryption. A simple checkbox with encrypted password is used to create the backup set; that same password then must be used to decrypt the backup set during a restore procedure. If the password is lost, there is no way to recover those backup files because the password is not stored with reversible encryption.

vSphere Web Client

VMware previously announced that the C# client would no longer ship with the next release of vSphere. That is the case with the vSphere 6.5 release. VMware continues to move toward Web- and API-based tools, including VMware PowerCLI™ and the new vCenter Server REST APIs.

The most used UI probably is the vSphere Web Client. This interface continues to be based on the Adobe Flex platform and requires Adobe Flash to use. However, VMware has continued to identify areas that will help improve the user experience until it can be retired. Through several outreach efforts over the past year, the Engineering group has identified high-value areas where customers most seek improvements.

The following high-impact improvements will enhance overall user experience with the vSphere Web Client while development continues with the HTML5-based vSphere Client. First, the inventory tree, rather than the home screen, is now the default view because it is the view a vast majority of administrators have gone to first when logging in. The home screen has been reorganized based on customer feedback. Optional plug-ins have been moved to the bottom, out of the way. Another important change is the renaming of the **Manage** tab to **Configure**. It is now more intuitive as to which operations can be performed under this tab. And to be more in alignment with expectations of administrators, adjustments have been made to the locations of some settings and workflows. The **Related Objects** tab has been removed and flattened into **Hosts**, **VMs**, **Datastores**, and **Networks**, to make the UI more intuitive and reduce the number of clicks to complete administrative tasks.

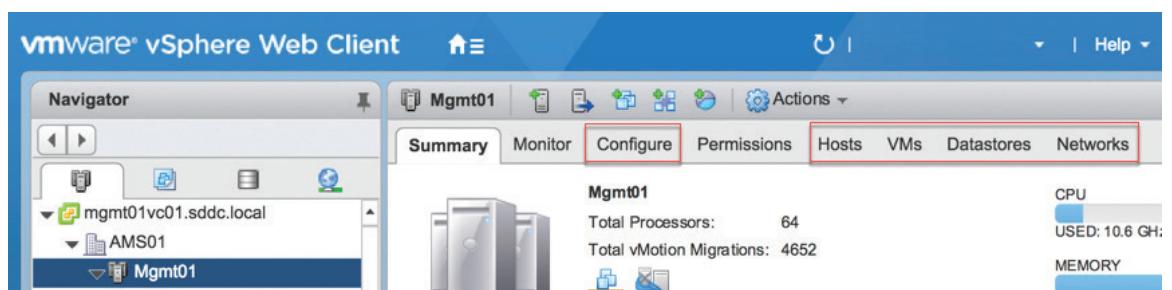


Figure 5. Improvements to the vSphere Web Client 6.5 Including Flattening of the Related Objects Tab

From a performance perspective, VMware has made improvements that will enhance the user's experience with the vSphere Web Client. Additional enhancements have produced an increase of 100 times in the number of VMs that can be displayed in the inventory tree. A significant enhancement is the live refresh ability. The vSphere Web Client can now be viewed as the single source of truth in real time for operations within the environment—automated tasks, tasks of other services, as well as activities of other administrators. Power states are also reflected in real time, enhancing the user experience with the vSphere Web Client.

A plug-in is no longer required for many common administrative tasks. This is another major improvement not only for the vSphere Web Client but also for deployment of the vCenter Server Appliance. The client integration plug-in (CIP) has been replaced via native functionality within the Web browser. Functions that previously required the CIP in vSphere 6.0 included installation of the vCenter Server Appliance and Platform Services Controller appliance, file uploads to a datastore, OVF and OVA deployment, and import and export from Content Library.

For customers that require the ability to use Windows pass-through authentication or SmartCard login with the vSphere Web Client, a new streamlined Enhanced Authentication plug-in is available. This optional plug-in provides those services for users who still require them, but it is otherwise not required. This greatly reduces the footprint and complexity of the plug-in and mitigates many browser-dependency issues.

vSphere Client

With vSphere 6.5, there is now a fully supported version of the HTML5-based vSphere Client that can run alongside the vSphere Web Client. The vSphere Client is built into vCenter Server 6.5—both Windows and appliance—and is enabled by default. The vSphere Client doesn't yet have full feature parity, but many of the day-to-day tasks of administrators have been prioritized, specifically those regarding VMs. In addition, features that enable full-time use continue to be prioritized. The vSphere Web Client continues to be accessible via <https://<vCenter Server FQDN or IP Address>/vsphere-client>. The vSphere Client is reachable via <https://<vCenter Server FQDN or IP Address>/ui>. VMware might also periodically update the vSphere Client outside of the normal vCenter Server release cycle. To ensure that customers can keep current, the vSphere Client can be updated without disruption to the rest of vCenter Server.

The following are some of the benefits of the new vSphere Client:

- Clean, consistent UI built on new VMware Clarity UI standards that will be adopted across the portfolio
- Built on HTML5, making it truly a cross-browser and cross-platform application
- No browser plug-ins to install and manage
- Integrated into vCenter Server 6.5 and fully supported
- Fully supports Enhanced Linked Mode
- Extremely positive feedback on performance from users of the Fling

The vSphere Client originated as a [VMware Fling](#) in early 2016. Customers have provided a considerable amount of feedback via the built-in feedback tool, which will remain in general availability builds. This has helped with prioritization of new features and functionality. The Fling will continue to be released, although somewhat less frequently, and can be used by customers who want to test the latest features. It will also remain as a standalone appliance and can be used simultaneously with the general availability version. However, it will continue to be unsupported, as is the case with all VMware Flings.

Content Library

Content Library with vSphere 6.5 includes some notable usability improvements. Administrators can now mount an ISO directly from the Content Library, apply a guest OS customization specification during VM deployment, and update existing templates.

Performance, recoverability, and scalability have also been improved. The new Optimized HTTP Sync option controls how a published library stores and syncs content. When enabled, it stores the content compressed, which reduces the sync time between vCenter Server instances not using Enhanced Linked Mode.

Because Content Library is part of vCenter Server, it leverages the new features included with vCenter Server 6.5, including vCenter HA and vSphere 6.5 Backup/Restore Service offered by vCenter Server Appliance.

vSphere Host Lifecycle Management Enhancements

With vSphere 6.5, administrators will find significantly more powerful capabilities for patching, upgrading, and managing the configuration of VMware ESXi™ hosts.

vSphere Update Manager

vSphere Update Manager continues to be the preferred approach for keeping ESXi hosts up to date. With vSphere 6.5, it has been fully integrated with vCenter Server Appliance. This integration eliminates the additional resources required for another virtual machine (VM), OS license, and database dependencies of the previous architecture. Integrated vSphere Update Manager leverages the vPostgres installation that is part of vCenter Server Appliance, but the data is stored using a separate schema.

The vSphere Update Manager UI is completely integrated with vSphere Web Client. Certain workflows have been streamlined to improve day-to-day operations. For example, a new checkbox enables administrators to save options that were changed during the remediation wizard so that they will be remembered in subsequent operations.

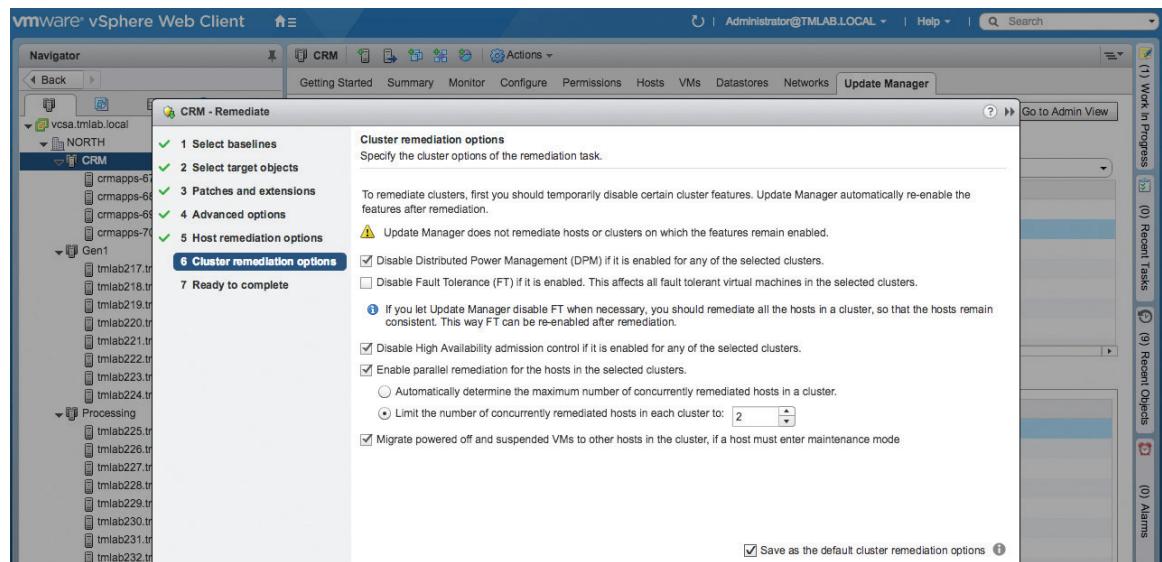


Figure 6. Updated Remediation Wizard

vSphere Update Manager is enabled by default, so it is ready to use immediately, without any additional configuration. Administrators can create baselines and upgrade existing hosts to ESXi 6.5 or apply patches to supported versions of ESXi.

Two new features of vCenter Server Appliance enable reduced downtime for vSphere Update Manager: resiliency of vCenter HA, for much improved redundancy; file-based backups of the appliance, to enable faster recovery.

The vCenter Server Appliance Migration Tool is also available to assist customers interested in transitioning from the Windows-based vCenter Server to vCenter Server Appliance 6.5.

VMware Tools and Virtual Hardware Upgrades

In addition to patching and upgrading ESXi hosts, vSphere Update Manager can be used by customers to update VMware Tools™ or VM compatibility level—that is, virtual hardware. Two changes in this functionality with vSphere Update Manager 6.5 pertain to Linux VMs.

First, Linux VMs that are using VMware Tools distributed with vSphere, often known as “Tar Tools,” no longer are needlessly rebooted by vSphere Update Manager after an update. In most cases, Linux VMs do not require a reboot after upgrading VMware Tools because the critical storage, network, and other drivers are delivered as part of the upstream kernel.

Second, Linux VMs using guest-managed VMware Tools, either operating system specific packages (OSPs) or Open VM Tools (OVT), can now be targeted for virtual hardware upgrades through vSphere Update Manager. Previously, vSphere Update Manager allowed upgrading only VMs that were running Tar Tools. This restriction has been relaxed now that the upstream Linux drivers are sufficiently mature.

Previous Windows-Based Architecture Still Offered

Although vCenter Server Appliance is the recommended deployment model for vCenter Server, those customers that are not yet ready to migrate from the Windows version of vCenter Server can continue to operate under the previous vSphere Update Manager architecture. vSphere Update Manager 6.5 can be installed in a separate Windows VM and can be connected to vCenter Server on Windows, but it cannot be connected to a vCenter Server Appliance instance.

Host Profiles

Host Profiles was introduced with vSphere 4 and has steadily matured since then. This release offers notable improvements in management of the profiles themselves, as well as in day-to-day operations.

Profile Management Improvements

An updated graphical editor that is part of vSphere Web Client now has an easy-to-use search function. It also now can mark individual configuration elements as favorites for quick access.

In addition, administrators can now create a hierarchy of Host Profiles by leveraging the new capability to copy settings from one profile to one or many others, verifying differences in the process.

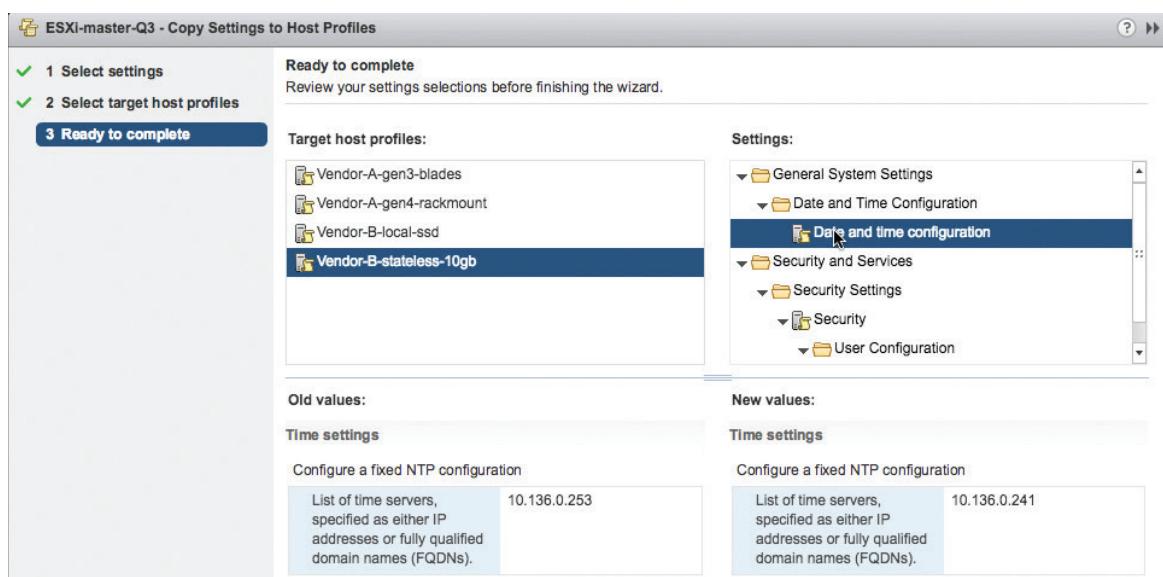
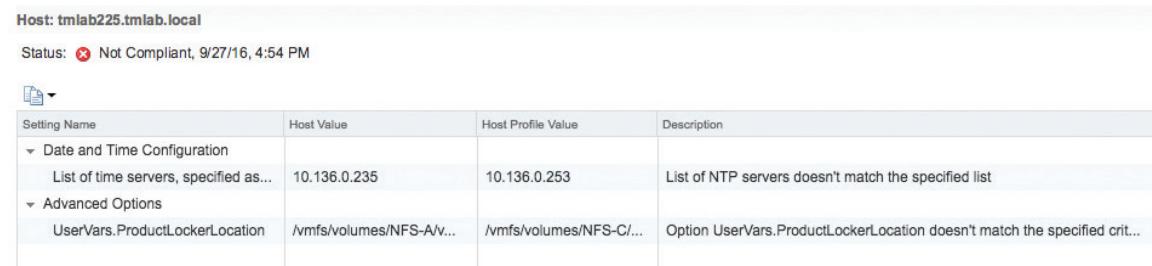


Figure 7. Copying Settings from One Host Profile to Four Target Host Profiles

Even when part of a cluster, each ESXi host can still have distinct characteristics—a static IP address, for example—that must be accommodated. The process of setting these per-host values is known as host customization. With this release, it is now possible to manage these settings for groups of hosts via CSV file. This will certainly be appealing to customers with larger environments.

Operational Enhancements

Compliance checks are more informative as well, displaying a detailed, side-by-side comparison of values from a profile versus the actual values on a host.



The screenshot shows a compliance report for a host named 'tmab225.tmlab.local'. The status is 'Not Compliant' at 9/27/16, 4:54 PM. The report lists two configuration items:

Setting Name	Host Value	Host Profile Value	Description
Date and Time Configuration List of time servers, specified as...	10.136.0.235	10.136.0.253	List of NTP servers doesn't match the specified list
Advanced Options UserVars.ProductLockerLocation	/vmfs/volumes/NFS-A/v...	/vmfs/volumes/NFS-C/...	Option UserVars.ProductLockerLocation doesn't match the specified crit...

Figure 8. Detailed Compliance Report Showing Configuration Values from Both Host and Host Profile

Before remediating, administrators can execute a pre-check, to ensure that all mandatory host customizations are in place and to determine whether or not a particular configuration change requires maintenance mode.

Finally, the process of effecting configuration change is greatly optimized in vSphere 6.5. This is a result of vSphere DRS integration for scenarios that require maintenance mode and of speedy parallel remediation for changes that do not.

Auto Deploy

Auto Deploy is a vSphere feature that uses industry-standard PXE technology to enable ESXi hosts to boot from the network rather than from local disks. Hosts match deploy rules based on a variety of attributes such as IP address or host name, which determine the correct ESXi image to boot. Because vSphere administrators can easily update these deployment rules, Auto Deploy enables quick patching or upgrading, using one single workflow for any type of update.

Manageability Improvements

Auto Deploy is now easier to manage in vSphere 6.5 with the introduction of a full-featured graphical interface. Administrators no longer are required to use VMware PowerCLI to create and manage deploy rules or to customize ESXi images, but it is still an available management interface. For the Auto Deploy GUI to be visible in vSphere Web Client, both the Image Builder and Auto Deploy services must be running when logging in to vCenter Server.

One key component of the new GUI is the Image Builder, which enables administrators to download ESXi images from the VMware public repository or to upload zip files containing ESXi images or drivers. These images can then be customized by adding or removing components, and they optionally can be exported to ISO or zip for use elsewhere. A comparison tool that is part of the interface enables administrators to determine how the contents of two images differ.

The screenshot shows the 'Auto Deploy' interface with the 'Software Depots' tab selected. On the left, there is a list of software depots with their names and types: ESXi 6.5 4415946 (ZIP), ESXi 6.0 4192238 (ZIP), Corporate (Custom), qa4xxx 644.6.06.0-1 (ZIP), and VMware Public (Online). On the right, details for the 'VMware Public' depot are shown, including its URL (<https://hostupdate.vmware.com/software/VUM/PRODUCTION/main/vmw-depot-index.xml>) and a table of image profiles. The table includes columns for Name, Acceptance Level, Vendor, and Last Modified. The 'ESXi-6.0.0-20160801001s-no...' profile is highlighted.

Figure 9. Auto Deploy Software Depots Graphical Interface

The new **Deployed Hosts** interface tab lists all hosts that have been provisioned with Auto Deploy. It is the single source of truth when determining the association between hosts, images, host profiles, and other attributes. This interface also enables administrators to interactively test and remediate those associations, which is typically required after a deploy rule has been edited.

The screenshot shows the 'Auto Deploy' interface with the 'Deployed Hosts' tab selected. A message indicates that the image profile, host profile, and location associated with the hosts are listed below. Below this, a table displays host associations. The table has columns for Host, Associated Image Profile, Associated Host Profile, Associated Location, and Associated Script Bundle. The 'tmilab208.tmlab.local' host is highlighted in blue.

Host	Associated Image Profile	Associated Host Profile	Associated Location	Associated Script Bundle
tmilab204.tmlab.local	ESXi-6.5.0-4152506-no-tools	ESXi-stateless-rev6	Processing	
tmilab205.tmlab.local	ESXi-6.5.0-4152506-no-tools	ESXi-stateless-rev6	Processing	
tmilab206.tmlab.local	ESXi-6.5.0-4152506-no-tools	ESXi-stateless-rev6	Processing	
tmilab207.tmlab.local	ESXi-6.5.0-4152506-no-tools	ESXi-stateless-rev6	Processing	
tmilab208.tmlab.local	ESXi-6.0.0-20160504001-no...	ESXi-stateless-patch6-rev1	DataAnalytics	
tmilab209.tmlab.local	ESXi-6.0.0-20160504001-no...	ESXi-stateless-patch6-rev1	DataAnalytics	
tmilab210.tmlab.local	ESXi-6.0.0-20160504001-no...	ESXi-stateless-patch6-rev1	DataAnalytics	

Figure 10. Auto Deploy Deployed Hosts Graphical Interface

New and unassigned hosts that boot from Auto Deploy are now collected under the **Discovered Hosts** tab while waiting for instructions. A new interactive workflow enables the provisioning of hosts without creating a deploy rule. Hosts provisioned through this workflow will still be listed under Deployed Hosts, along with any hosts that were brought online through a pattern-based deploy rule.

The screenshot shows the 'Auto Deploy' interface with the 'Discovered Hosts' tab selected. A message indicates that hosts not matching any deploy rules are listed below. Below this, a table displays discovered hosts. The table has columns for IPv4, IPv6, Hostname, MAC address, and Serial number. The first host, 'tmilab226', is highlighted in blue.

IPv4	IPv6	Hostname	MAC address	Serial number
10.136.0.226	fe80::250:56ff:fe99:68aa	tmilab226	00:50:56:99:68:aa	VMware-42 19 95 a2 5f 6a 16 ef
10.136.0.224	fe80::250:56ff:fe99:28e0	tmilab224	00:50:56:99:28:e0	VMware-42 19 29 20 bd 12 0d a
10.136.0.227	fe80::250:56ff:fe99:5d74	tmilab227	00:50:56:99:5d:74	VMware-42 19 6f e3 e6 b0 b9 c0
10.136.0.225	fe80::250:56ff:fe99:b970	tmilab225	00:50:56:99:b9:70	VMware-42 19 fb 89 81 52 2e 83

Figure 11. Auto Deploy Discovered Hosts Graphical Interface

Custom integrations and other special configuration tasks are now possible with a new Script Bundle feature that enables arbitrary scripts to be run on ESXi hosts after they boot via Auto Deploy. These scripts must be written in a scripting language that is compatible with ESXi, such as shell or Python, and bundled together in a tar gzip (tgz) archive. Script bundles must be uploaded to the Auto Deploy server via a new VMware PowerCLI cmdlet (Add-ScriptBundle) and subsequently associated with a new or existing deploy rule along with other items such as a Host Profile or cluster.

Performance and Resiliency Enhancements

Scalability has been greatly improved over previous releases. Auto Deploy can accommodate many times more concurrently booting hosts. See the *Configuration Maximums Guide for vSphere 6.5* for authoritative results.

For architects who prefer to design a front-end caching tier that offloads traffic from vCenter Server Appliance, Auto Deploy 6.5 facilitates incorporation of a set of industry-standard reverse proxy caches that are used in a round-robin manner by hosts as they boot. A new VMware PowerCLI cmdlet (Add-ProxyServer) is used to enable Auto Deploy to leverage available proxies. If no proxies are reachable, hosts revert to the default of booting ESXi images directly from vCenter Server Appliance. This feature is intended for performance optimization rather than for high availability. To be properly configured and brought online in the vSphere data center, vCenter Server Appliance and the Auto Deploy service must still be available when hosts boot.

Like vSphere Update Manager, Auto Deploy benefits from native vCenter HA for quick failover in the event of an outage. For recovery from more severe disasters, Auto Deploy configuration is also captured by the new vCenter Server Appliance file-based backup capability. The entire Auto Deploy state, including deploy rules, configuration, and SSL certificates, can be manually exported with a new VMware PowerCLI cmdlet (Export-AutoDeployState) for safekeeping.

Auto Deploy now supports both BIOS and UEFI hardware for those customers running the newest servers from VMware OEM partners. DHCP servers must be configured to properly instruct UEFI servers to boot the snponly64.efi iPXE agent rather than the usual undionly.kpxe. Auto Deploy 6.5 also works in both IPv4 and IPv6 environments.

VMware Tools 10.1 and 10.0.12

vSphere 6.5 includes the latest version of VMware Tools, the collection of in-guest drivers and agents that optimize VM performance and increase manageability. Several new features of vSphere and VMware Tools work together to improve the overall experience of managing workloads.

Signed ISO Images

VMware Tools installers are distributed as ISO images that can be mounted to individual VMs to install or upgrade. ESXi 6.5 introduces a new layer of security by cryptographically verifying these ISO images each time they are read. To facilitate this verification, VMware Tools distributions now include additional files with appropriate signatures.

Bifurcation of VMware Tools for Legacy and Current Guests

VMware Tools 10.1 is available for OEM-supported guest OSs only. Guests that have fallen out of support by their respective vendors are offered “frozen” VMware Tools version 10.0.12. The frozen VMware Tools will not receive feature enhancements going forward. For more information about support categorization for guest OSs, see [VMware Knowledge Base article 2015161](#).

Bundling of Tools for Most Popular Guests Only

ESXi 6.5 includes VMware Tools for the most commonly used guest OSs. Tools for other guests are available for download from My VMware. Similarly, VMware Tools updates for those same guests are distributed through vSphere Update Manager as needed.

VMWARE TOOLS VERSION	BUNDLED WITH vSPHERE	DOWNLOADABLE ONLY
10.1	Windows Vista+ Linux glibc2.5+	Solaris FreeBSD Mac OS X 10.11+ Mac OS X 10.11+
10.0.12	Windows Pre-Vista	Windows Pre-2000 Mac OS X Pre-10.11 Linux Pre-glibc2.5 Netware

Table 1. Bifurcation of VMware Tools 10.1 and 10.0.12

Guest OS Granularity Increase

With VMware Tools 10.1 and 10.0.12, there are now two ISO images for certain families of guest OSs, to accommodate the bifurcation previously described. Consequently, the configurable guest OS attribute for some guests has become more precise.

The most notable example of this change is CentOS: In vSphere 6.5, CentOS guest selections are available for CentOS 7, CentOS 6, and CentOS 4/5. In previous releases, these versions were all combined into a single selection: CentOS 4/5/6/7. Administrators can edit the guest OS type or leverage the new VM configuration option `tools.hint.imageName` to ensure that the proper ISO image is mounted to these VMs.

Detailed Display of VMware Tools Type and Version in vSphere Web Client

There are two different version designations for VMware Tools: One is a human-readable number, such as 10.0.7; the other is an internal code, such as 10247. With vSphere 6.5, vSphere Web Client now displays both variations of the version number as well as the specific type of VMware Tools installed in the guest OS: MSI, OSP, OVT, or Tar Tools.

**Figure 12.** Enhanced VMware Tools Information Showing More Detailed Version and Type Data

Improved Detection of Availability of Updated VMware Tools Installers

Each ESXi host uses either a local or a shared repository of VMware Tools installation ISO images. Previously, VMs checked for updated VMware Tools only during a power or migration event. In vSphere 6.5, this check is now done every 5 minutes. When newer VMware Tools installation images are found, VMs display an alert indicating that an update is available.

vSphere Operations

Operations Management

Certain editions¹ of vSphere include VMware vRealize® Operations Manager™. With the vSphere 6.5 release, vRealize Operations Manager has also been updated to version 6.4. The update includes many new dashboards, dashboard improvements, and other key features to help administrators get to the root cause more quickly and efficiently.

vRealize Operations Manager provides many dashboards out of the box, all with the goal of showing specific parts of the environment. vRealize Operations Manager 6.4 features three new dashboards: Operations Overview, Capacity Overview, and Troubleshoot a VM. Operations Overview displays pertinent environment-based information such as inventory summary, cluster update, overall alert volume, and a couple of widgets containing the top 15 VMs experiencing CPU contention, memory contention, and disk latency. Capacity Overview contains information such as capacity totals, capacity in use for the CPU count, RAM, and storage-based metrics. This dashboard also provides additional information regarding reclaimable capacity and a distributed utilization visualization. The Troubleshoot a VM dashboard is a central location that enables a view of individual VM-based information such as its alerts, relationships, and metrics based on demand, contention, parent cluster contention, and parent datastore latency.

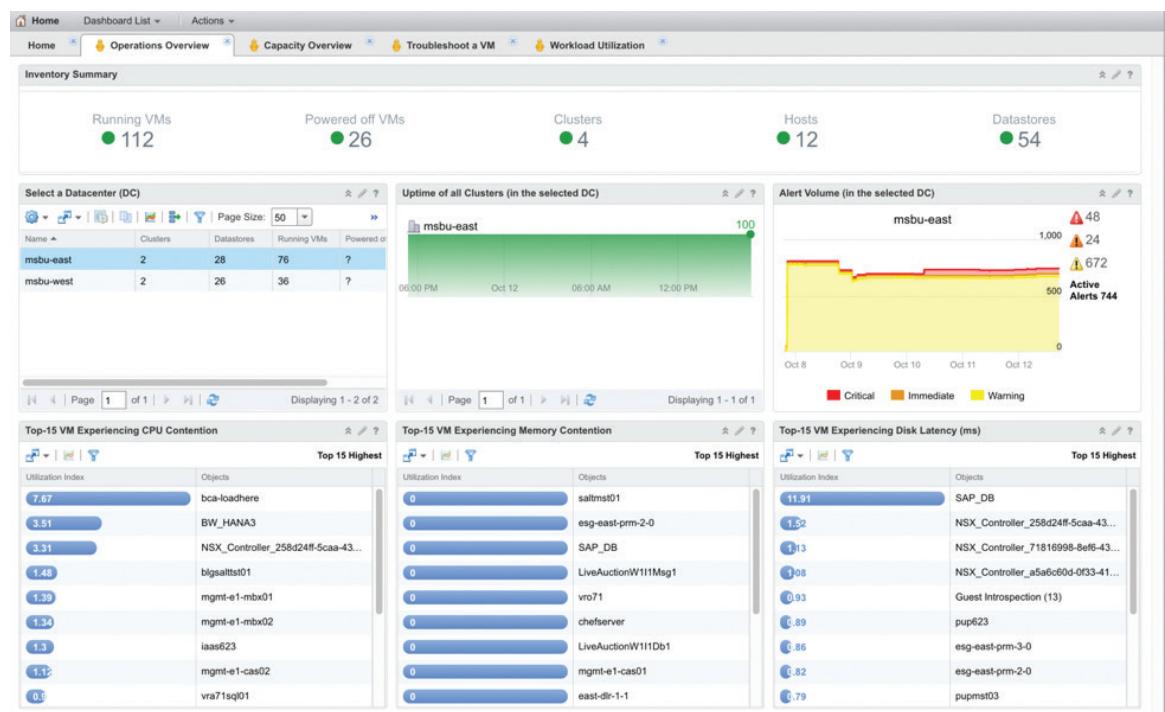


Figure 13. New Operations Overview Dashboard with vRealize Operations Manager 6.4

¹ For details on vSphere license editions, see <http://www.vmware.com/products/vsphere.html#compare>.

Another improvement, not in the form of a dashboard, to vRealize Operations Manager 6.4 is a new view for each object. This new view closely resembles the home dashboard, added in a previous version, but it focuses only on the selected object. Information displayed in this new view includes active alerts, key properties, key performance indicator (KPI) metrics, and other relational-based data.

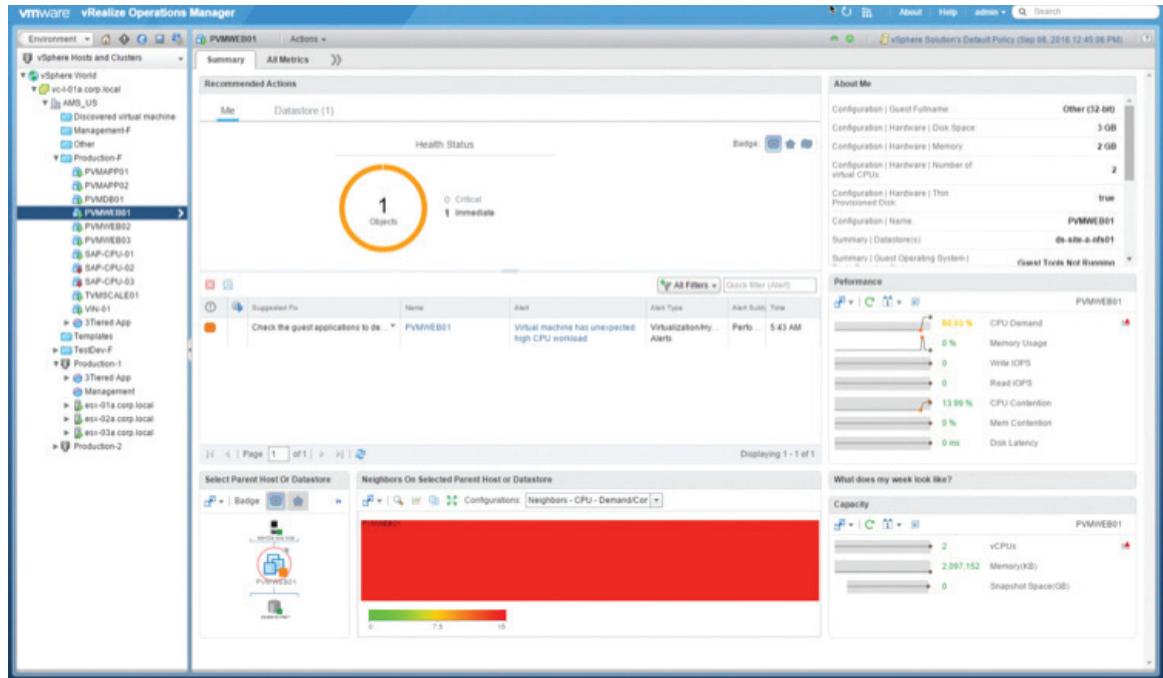


Figure 14. New Object-Based View with Streamlined Access to Available Data

vRealize Operations Manager 6.4 offers other notable improvements, such as the ability to display the vSphere VM folders within vSphere Hosts and Clusters Environment view. There is now also the capability to group alerts as to priority and prevalence. Alert groups also enable the functionality to clear alerts in a bulk manner. There are now also KPI metric groups available out of the box, to help easily chart out and correlate properties with a single click.

Log Monitoring

VMware vRealize Log Insight™ for vCenter™ is also a key piece in enabling administrators to get to the root cause of issues more quickly and efficiently. vRealize Log Insight also has been updated to version 4.0. It contains a UI based on the new Clarity UI, increased API functionality regarding the installation process, the ability to perform automatic updates to agents, as well as other general UI improvements.

Developer and Automation Interfaces

vSphere 6.5 introduces key developer- and automation-based enhancements to further simplify interactions for developer and automation specialists. These enhancements are being made across both the application program interfaces (APIs) and the command-line interfaces (CLIs) to give customers their choice of access with language bindings and automation tools.

Application Program Interfaces

vCenter Server has received new extensions to its REST-based API. In vSphere 6.0, this API set provided the ability to manage the Content Library and tagging. In vSphere 6.5, it now also provides the ability to manage and configure the vCenter Server Appliance and enables basic VM management.

vCenter Server Appliance API

vCenter Server Appliance features a new and simplified REST-based API that can consistently handle the following functions:

- Accessing the appliance
- Managing user accounts
- Verifying the health of the appliance and its services
- Managing networking configurations such as firewall rules and proxy settings
- Providing a file-based backup or restore of an appliance
- Managing system settings such as NTP
- Checking the uptime or version

Virtual Machine API

Additional functionality has been added for handling the management of VMs. Using the new REST-based interface, users can read information; create, update or delete VMs; set their power state; and work with the hardware. Hardware tasks include connecting the CD-ROM, updating the RAM allotment, adding a network adapter, removing a hard disk, and so on.

All of these functions not only are available via developer and automation tooling but also are simplified to ensure that they are easily discoverable. And the use of strong defaults means that only necessary information must be specified. For example, creating a VM is now as easy as 12 lines of JSON and a single API call.

Discover the APIs with the New API Explorer

The API Explorer on vCenter Server provides a new way to discover which APIs are available for use. To enable an understanding of the API models, the API Explorer displays information on the numerous APIs available on the current endpoint. It also enables users to expand each API call, look at the required fields, understand the request body, and see the available filter information as well as a list of response messages. Users also can utilize a “Try It Out” button directly from the API Explorer. This in turn makes the API call and presents a simple cURL command that can be run from their local system.

The screenshot shows the VMware vCenter API Explorer interface. At the top, there is a navigation bar with the VMware logo, "API Explorer", and user information ("kruddy@SDDC.LOCAL Logout"). Below the navigation bar, the "Select API" dropdown is set to "vccenter". The main content area has a title "vccenter" and a subtitle "VMware vCenter Server provides a centralized platform for managing your VMware vSphere environments". A search bar is labeled "cluster". Below the search bar, there is a "GET /vcenter/cluster Returns information about at most 1000 visible (subject to permission checks) clusters in vCenter matching the Cluster.FilterSpec." section. This section includes a "Response Class (Status 200)" heading, a description of commonly used information about clusters, and a "Model Example Value" section containing a JSON snippet:

```
[  
  {  
    "cluster": "string",  
    "drs_enabled": true,  
    "name": "string",  
    "ha_enabled": true  
  }  
]
```

Below the JSON example, there are sections for "Response Content Type" (set to "application/json"), "Parameters", and "Response Messages". At the bottom of this section are "TRY IT OUT!" and "Hide Response" buttons.

Figure 15. API Explorer with Clearly Displayed Information About Available API Calls

Process Improvements

vSphere 6.5 provides many process improvements as to how these APIs are defined. It also provides several out-of-the-box developer- and automation-based tool integrations. The software development kits (SDKs) are now automatically generated in several languages, including Java, .NET, Python, Ruby, and Perl. Their associated documentation and samples are automatically generated, fully featured, and much easier to read and understand.

vcenter

The vcenter API provides services for managing VMware vSphere environments.

cluster

The cluster service provides operations to manage clusters in the vCenter Server.

Operation	HTTP request	Description
get	GET <code>https://[server]/rest/vcenter/cluster/[cluster]</code>	Retrieves information about the cluster corresponding to cluster.
list	GET <code>https://[server]/rest/vcenter/cluster</code>	Returns information about at most 1000 visible (subject to permission checks) clusters in vCenter matching the <code>vcenter.cluster.filter_spec</code> .

datacenter

The datacenter service provides operations to manage datacenters in the vCenter Server.

Operation	HTTP request	Description
create	POST <code>https://[server]/rest/vcenter/datacenter</code>	Create a new datacenter in the vCenter inventory
delete	DELETE <code>https://[server]/rest/vcenter/datacenter/[datacenter]</code>	Delete an empty datacenter from the vCenter Server
get	GET <code>https://[server]/rest/vcenter/datacenter/[datacenter]</code>	Retrieves information about the datacenter corresponding to datacenter.
list	GET <code>https://[server]/rest/vcenter/datacenter</code>	Returns information about at most 1000 visible (subject to permission checks) datacenters in vCenter matching the <code>vcenter.datacenter.filter_spec</code> .

Figure 16. Streamlined Learning and Accessing of APIs via Received Update to API Documentation

Command-Line Interfaces

Command-line interfaces are ideal for both vSphere administrators and developers who want to maximize efficiency and effectiveness within their environments. There are two main CLI offerings, vSphere CLI and VMware PowerCLI. vSphere CLI enables administrators to run common commands against ESXi and vCenter Server systems from a remote machine. It does this via the ESXCLI and Datacenter CLI (DCLI) set of commands. VMware PowerCLI is an extension to the Microsoft PowerShell offering and contains cmdlets that operate against many of the product offerings from VMware.

vSphere CLI has received updates to both ESXCLI and DCLI commands. ESXCLI now features several new storage-based commands that handle VMware Virtual SAN™ core dump procedures, utilizing Virtual SAN iSCSI functionality, managing NVMe devices, and other core storage commands. There are also some additions on the network side to handle network adapter-based commands such as queuing, coalescing, and basic FCoE tasks. DCLI can now leverage all the new vSphere REST APIs that were referenced in the prior section.

VMware PowerCLI

One of the most anticipated updates to VMware PowerCLI in this release is that it is completely module based. VMware, with VMware PowerCLI, was one of the early adopters of PowerShell. With PowerShell v1.0, snap-ins were the only way to extend the shell for additional functionality. With each release of VMware PowerCLI, there has been a progression from snap-ins to modules, and this culminates in VMware PowerCLI 6.5.

Core vSphere Module

The core vSphere module also has received a number of new updates. The Move-VM cmdlet now supports Cross vCenter vMotion. The ability to specify the number of cores for a VM has been added to the New-VM and Set-VM cmdlets. The Open-VMConsoleWindow cmdlet now uses the latest version of the VMware Remote Client.

```

PowerCLI C:>> $sourceUC = "mgmt01vc01.sddc.local"
PowerCLI C:>> $destUC = "comp01vc01.sddc.local"
PowerCLI C:>>
PowerCLI C:>> $sourceUConn = Connect-VIServer -Server $sourceUC -Credential $creds
PowerCLI C:>> $destUConn = Connect-VIServer -Server $destUC -Credential $creds
PowerCLI C:>>
PowerCLI C:>> $vm = Get-VM -Name "MigrateUM01" -Server $sourceUConn
PowerCLI C:>>
PowerCLI C:>> $destination = Get-VMHost -Server $destUConn | Select-Object -First 1
PowerCLI C:>> $networkAdapter = Get-NetworkAdapter -VM $vm -Server $destUConn
PowerCLI C:>> $destinationPortGroup = Get-UDSwitch -Name "vDS-COMP" -Server $destUConn | Get-UDPortgroup -Name "vDS-COMP-Management" -server $destUConn
PowerCLI C:>> $destinationDatastore = Get-Datastore -Name "vsanDatastore" -Server $destUConn
PowerCLI C:>> Move-VM -VM $vm -Destination $destination -NetworkAdapter $networkAdapter -PortGroup $destinationPortGroup -Datastore $destinationDatastore
[Name          PowerState Num CPUs MemoryGB]
[MigrateUM01   PoweredOn    1       4.000]

PowerCLI C:>> _
```

Figure 17. Example vSphere vMotion Migration of VM Between vCenter Server Instances via Move-VM

Storage Module

The storage module has received some major updates as well. Many new Virtual SAN cmdlets are being introduced with this release. New functionalities include the ability to get and set Virtual SAN cluster configurations, manage Virtual SAN fault domains, update the HCL database, and perform various Virtual SAN tests. Additional cmdlets to interact with VMware vSphere Virtual Volumes™ replication have also been added to the storage module. The capabilities to retrieve and synchronize replication groups, retrieve and start the replication failover preparation, and start the replication failover itself have all been added as cmdlets.

VMware Horizon Module

The VMware Horizon® module has received the largest update, in the form of a complete rewrite. This module can now be run from anywhere rather than only on the VMware Horizon View™ Standard Edition connection server. The module is also now installed as part of the VMware PowerCLI installer. It features only two cmdlets, which give users the ability to connect or disconnect from a Horizon View connection server. When connected, however, users have complete access to the Horizon View Public API via the server's ExtensionData property. Advanced functions to be used with the module are also available on the VMware PowerCLI Example Scripts GitHub repository upon release.

Security

With new features such as VM Encryption, Encrypted vMotion, Secure Boot Support for Virtual Machines, and Secure Boot Plus Cryptographic Hypervisor Assurance for ESXi, vSphere 6.5 Security brings together security and operational efficiency that are both universal and scalable. In addition, vSphere 6.5 introduces audit-quality logging of vSphere events via Syslog.

Virtual Machine Encryption

VM Encryption is a VM-agnostic method of encryption for VMs that is scalable, easy to implement, and easy to manage.

There are numerous advantages:

1. Because encryption occurs at the hypervisor level and *not* in the VM, VM Encryption works with any guest OS and datastore type.
2. Encryption is managed via policy. The policy can be applied to many VMs, regardless of their guest OS. Verifying that the VM is encrypted can be done by confirming that the policy is applied. The policy framework being used leverages vSphere Storage Policy Based Management (SPBM).
3. Encryption is *not* managed “within” the VM. This is a key differentiator. There are no encryption “special cases” that require in-guest configuration and monitoring. Encryption keys are not contained in the memory of the VM or accessible to the VM in any way.
4. Key Management is based on the industry-standard Key Management Interoperability Protocol (KMIP). We are qualifying against KMIP version 1.1. vCenter Server is considered a KMIP client, and it works with many KMIP 1.1 key managers. This provides customers with choice and flexibility. It also provides a separation of duty between key usage and key management. In a large enterprise, key management would be done by the security team, and key usage would be done by IT, in this example via vCenter Server.
5. VM Encryption leverages the latest CPU hardware advances in AES-NI encryption. Advanced Encryption Standard Instruction Set is an extension to the x86 instruction set and provides accelerated encryption and decryption functions on a per-core basis in the CPU.

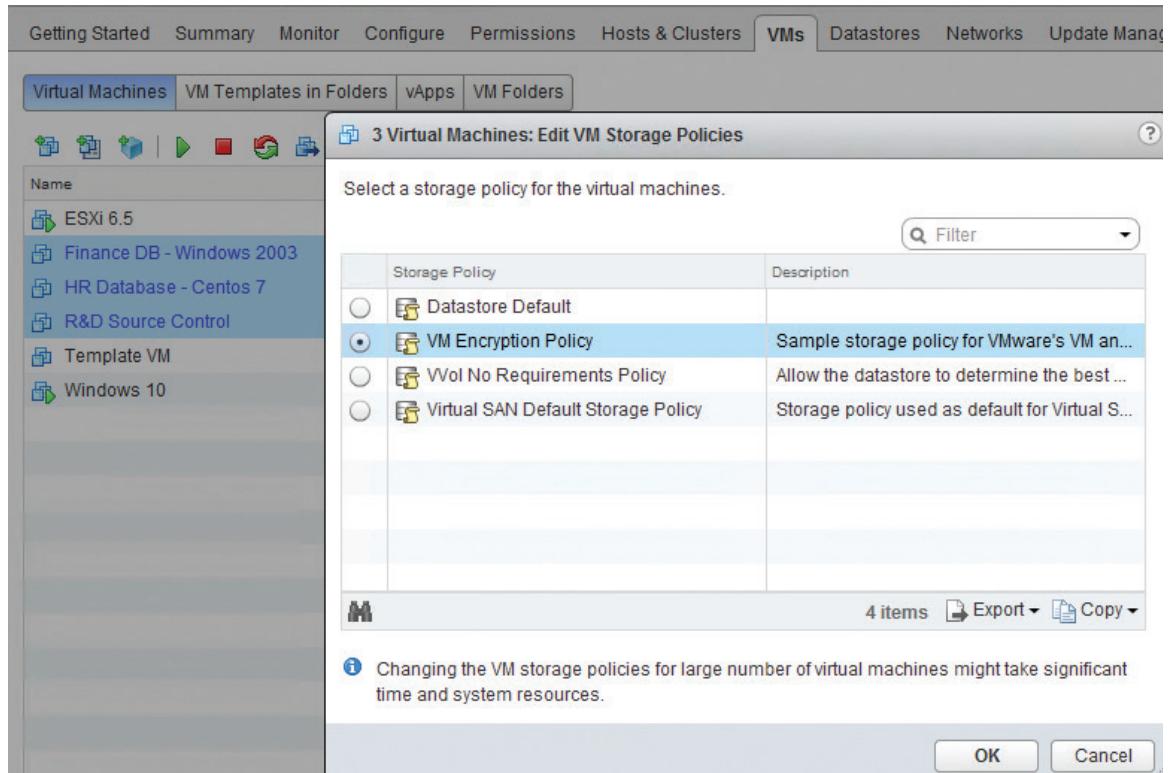


Figure 18. VM Encryption Storage Policy

Encrypted vMotion

Encrypted vMotion is set on a per-VM basis. It encrypts the data traveling over the network rather than encrypting the network itself. This enables more flexibility and easier implementation. A 256-bit random key and a 64-bit nonce, used only once for this VMware vSphere vMotion® migration, are generated. The nonce is used to generate a unique counter for every packet sent over the network. This prevents replay attacks and enables the encryption of 264 128-bit blocks of data.

The key and the nonce are packaged into a vSphere vMotion migration specification. The migration specification is sent to both systems in the cluster via the existing encrypted management connections between the vCenter Server instance and the ESXi hosts.

The vSphere vMotion traffic begins with every packet being encrypted with the key and the nonce on host A. Each uniquely encrypted packet is decrypted on the receiving host, host B, completing the vSphere vMotion migration.

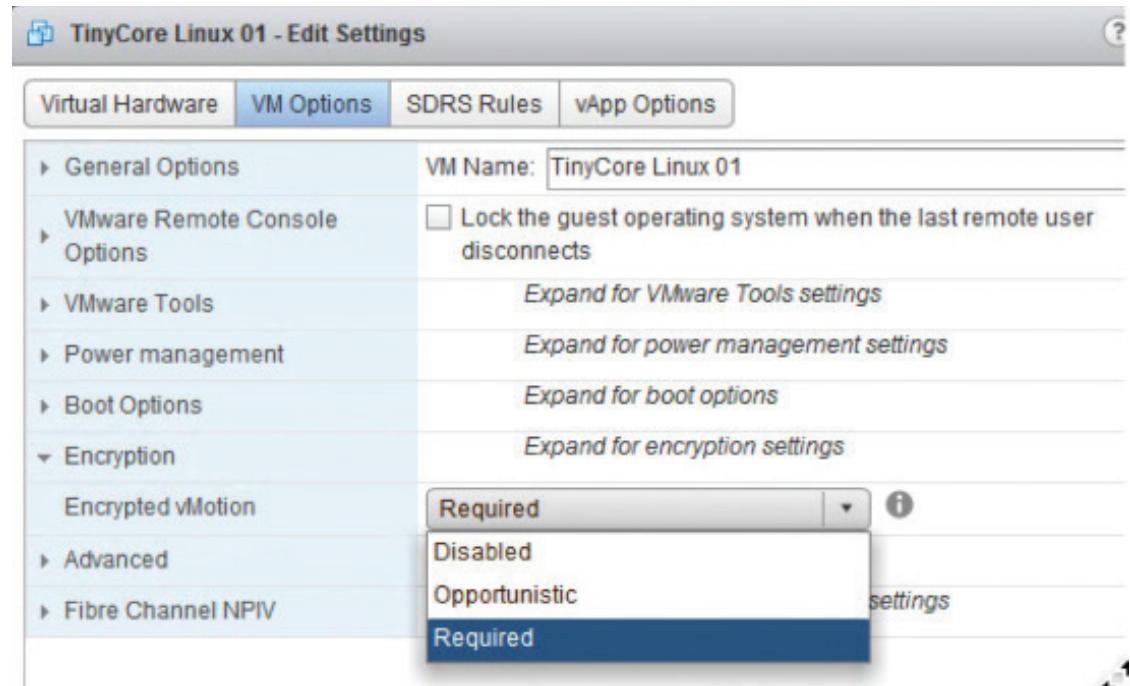


Figure 19 . Encrypted vMotion Options

Secure Boot Support

vSphere 6.5 introduces Secure Boot Support for Virtual Machines and for the ESXi hypervisor. UEFI Secure Boot is a mechanism that ensures that only trusted code is loaded by EFI firmware prior to OS handoff. Trust is determined by keys and certificates managed by the firmware. Implementation of this feature for a virtual machine enables secure boot of EFI-aware OSs in a VM.

Virtual Machine Secure Boot

Virtual machines must be booted from the EFI firmware to enable Secure Boot. EFI firmware supports Windows, Linux, and nested ESXi. For Secure Boot to work, the guest OS must also support Secure Boot. Examples include Windows 8 and Windows Server 2012 and newer, VMware Photon™ OS, RHEL/Centos 7.0, Ubuntu 14.04, and ESXi 6.5.

It is easy to enable Secure Boot for Virtual Machines by checking the box in the UI.

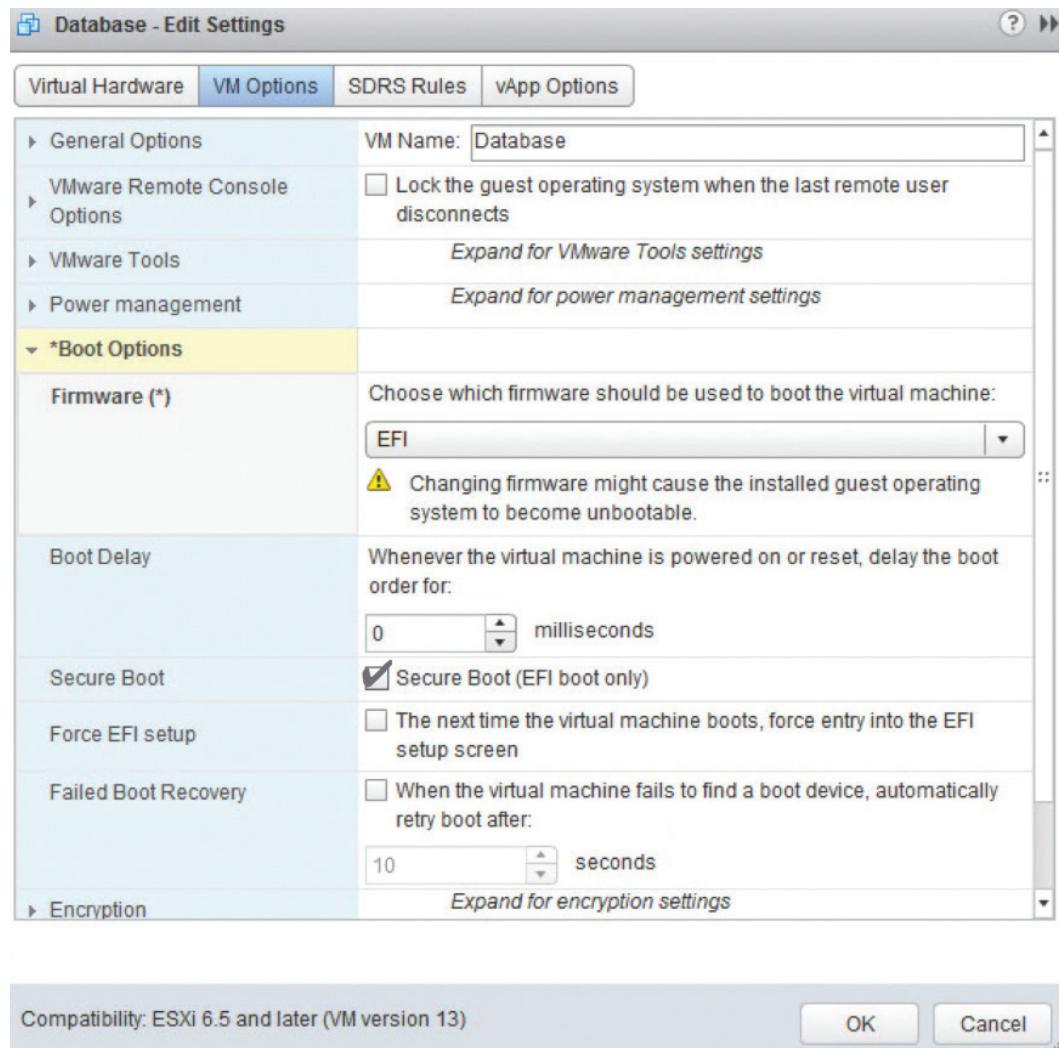


Figure 20. Secure Boot for Virtual Machine Options

ESXi Host Secure Boot

When Secure Boot is enabled, the UEFI firmware validates the digitally signed kernel of an OS against a digital certificate stored in the UEFI firmware. For ESXi 6.5, this capability is further leveraged by the ESXi kernel, adding cryptographic assurance of ESXi components.

ESXi is already composed of digitally signed packages called vSphere installation bundles (VIBs). These packages are never broken open. At boot time, the ESXi file system maps to the content of those packages. By leveraging the same digital certificate in the host UEFI firmware used to validate the signed ESXi kernel, the kernel then validates each VIB using the Secure Boot verifier against the firmware-based certificate, ensuring a cryptographically “clean” boot.

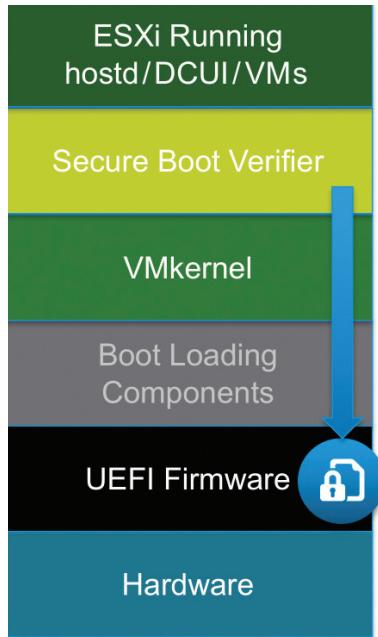


Figure 21. Secure Boot Verifier

When Secure Boot is enabled, it is not possible to install unsigned code on ESXi. This action will be prevented. To run unsigned code such as beta drivers, Secure Boot must be disabled. If an unsigned VIB is installed and Secure Boot is enabled, the Secure Boot verifier will run, detect the unsigned VIB, and crash the system. This is known as a Purple Screen of Death (PSOD) event. The crash will call out the VIB that must be removed. To remediate, boot the ESXi host with Secure Boot disabled, remove the VIB, and reboot with Secure Boot enabled.

Enhanced Logging

vSphere 6.5 introduces audit-quality logging. Prior to vSphere 6.5, logs were more focused on “troubleshooting” rather than on IT operations or security use cases. For example, if a VM were reconfigured from one network to another network, the most information revealed by the log was “Virtual Machine <name> reconfigured.” Although that was accurate, it was also incomplete.

Logs coming from vCenter Server via Syslog are now enriched with data from vCenter Server event. These logs clearly show “before” and “after” setting changes. The information now provided as to exactly what changed in the vSphere environment enhances the ability of IT and security administrators to troubleshoot issues. In Figure 23, the VM has been moved from a network labeled “PCI-vSwitch,” implying that the network is in scope for secure payment card industry (PCI) network traffic, to the “Non-PCI-vSwitch.”

Table	Event Types	Event Trends	1 to 2 out of 2 events	View ▾
			1 to 2 out of 2 events	View ▾
<pre>2016-08-12T16:37:49.586202+00:00 mgt-vc-01_vpxd_3546 -- [46197] [1-1] [2016-08-12T16:37:49.585736Z] [vim.event.VmReconfiguredEvent] [info] [VSPHERE.LOCAL\Administrator] [Datacenter] [46196] [Reconfigured TinyCore esxi-vsans-2.lab1.local in Datacenter. Modified: config.changeVersion: "2016-08-12T16:37:42.7008Z" -> "2016-08-12T16:37:45.978741Z"; config.hardware.device(4001).deviceInfo.summary: "PCI-vSwitch" -> "Non-PCI-vSwitch"; config.hardware.device(4001).backing.deviceName: "PCI-vSwitch" -> "Non-PCI-vSwitch";</pre>				

Figure 22. vSphere 6.5 Event Log

If a VM that is in scope for PCI were moved from a PCI network to a non-PCI network, it would be a serious security issue. With the enhanced logging available in vSphere 6.5, this notification would go directly via Syslog to the logging solution. There it would be parsed, and an alert would be generated to inform affected parties of the serious situation.

In vSphere 6.5, the logging of not only VM changes but of all vSphere changes has been improved. Enhanced logging includes changes to vCenter Server roles and permissions, datastore browsing functions such as downloading a VM, and actions such as creating and modifying vCenter Server clusters and hosts.

For those who have been using vSphere 5.x and 6.0 logging, these changes do not necessitate an increase to the logging level beyond “info” and do not add any measurable load to the vCenter Server instance or add to the vCenter Server database. This is because the information has already been recorded as part of the existing vCenter Server event. Enhanced logging exposes this information via the Syslog stream. Troubleshooting and support logs are unaffected and will continue to be used by support as necessary.

VM Sandboxing

An update to the ESXi architecture further ensures the safety and security of VMs by running them in an operational “sandbox” with strict controls as to hypervisor capabilities available to them. No configuration is necessary for VM sandboxing.

Automation

VM Encryption, Encrypted vMotion, and enabling Secure Boot for Virtual Machines are all fully automatable using common IT tools such as VMware PowerCLI, VMware vRealize® Automation™, and the vSphere API directly. This enables incorporation of security into existing workflows with minimal operational impact. The following are some examples:

1. Encrypting and decrypting a VM
2. Enabling Secure Boot for Virtual Machines
3. Enabling Encrypted vMotion on a per-VM basis

The following is an example of VM encryption with VMware PowerCLI:

```
#The name of the virtual machine
$vmname = "Tiny"
#Using the name of the VM, get the hard disk object
$harddisk = Get-VM -name $vmname |Get-HardDisk
#Get the encryption policy
$Encryptionpolicy = Get-SpbmStoragePolicy -Name "Encryption Policy"
#Encrypt the disk by applying the policy to the VM and its hard disk
Set-SpbmEntityConfiguration $vmname, $harddisk -StoragePolicy
$Encryptionpolicy -Confirm:$false
```

vSphere 6.5 Availability Enhancements

Proactive HA

Proactive HA integrates with select hardware partners to detect degraded components and evacuate VMs from affected vSphere hosts *before* an incident causes a service interruption.

Hardware partners offer a vCenter Server plug-in to provide the health status of the system memory, local storage, power supplies, cooling fans, and network adapters. As hardware components become degraded, Proactive HA determines which hosts are at risk and places them into a new state, Quarantine Mode. While in Quarantine Mode, VMs are migrated to healthy hosts, as long as affinity or anti-affinity rules are not violated and there is no impact to VM performance. In addition, the affected hosts are avoided when new VMs are added to the cluster.

VMware vSphere High Availability Orchestrated Restart

Orchestrated Restart improves the recoverability of applications that run across multiple VMs. This is done by creating dependency chains between VMs via VM-to-VM restart rules. These restart rules enforce the restart order for each VM within the dependency chain, increasing the likelihood that an impacted application will properly recover when VMware vSphere High Availability (vSphere HA) restarts the VMs.

vSphere HA restart rules are created and managed using vCenter Server. However, vSphere HA performs the recovery as configured and enforces the restart rules even if vCenter Server is unavailable.

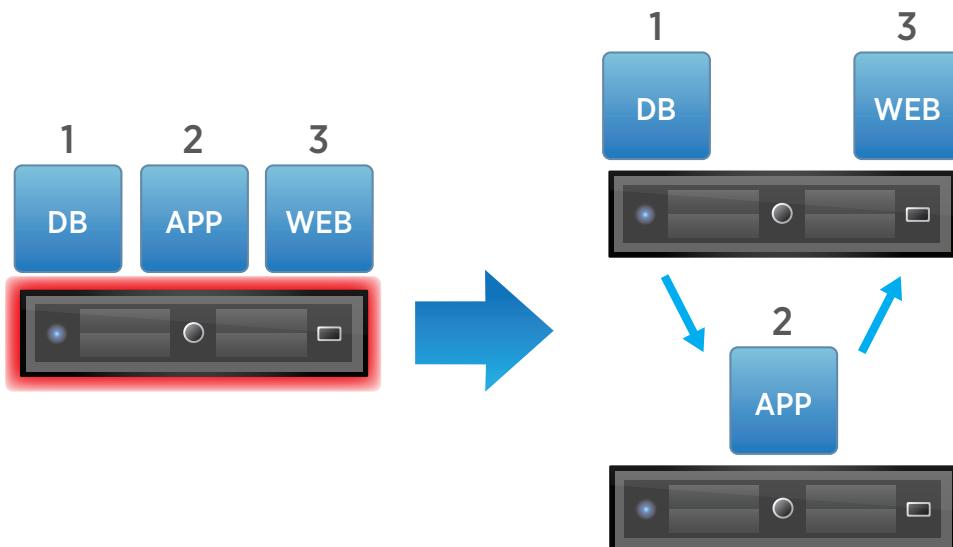


Figure 23. Multitiered VM Recovery

vSphere HA Admission Control Improvements

Several improvements have been made to simplify the configuration of vSphere HA admission control. Starting with vSphere 6.5, the default admission control policy is Cluster Resource Percentage. This policy calculates the amount of failover capacity to reserve by using a percentage of the total available CPU and memory resources in the cluster. To further simplify the configuration, this percentage is now calculated automatically by defining the number of host failures to tolerate (FTT).

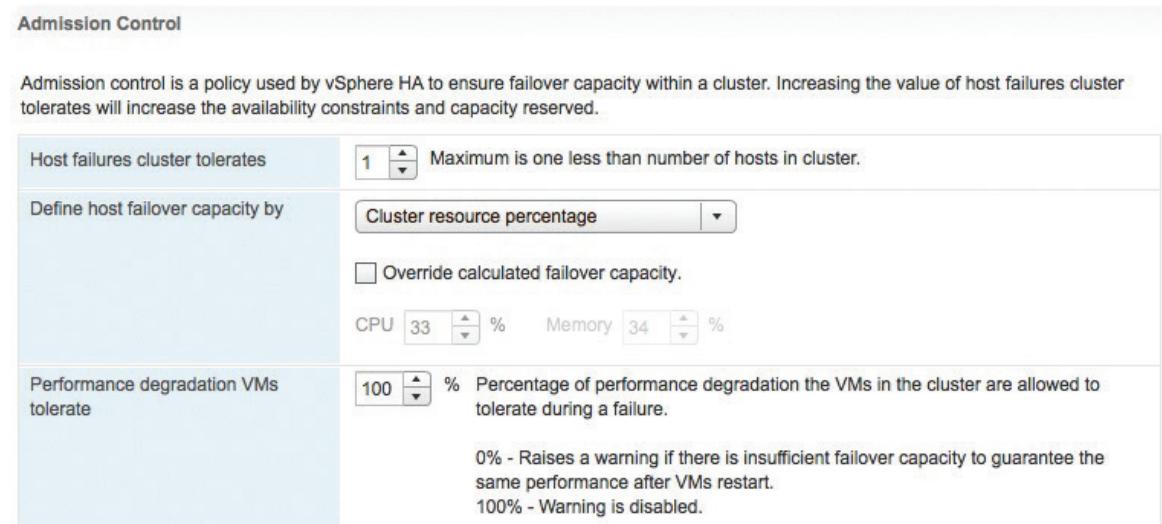


Figure 24. Admission Control Configuration

The calculated percentage dynamically changes as hosts are added or removed from the cluster to satisfy the FTT value. This simplified configuration applies to both homogeneous and heterogeneous clusters. Based on the worst-case scenario, it calculates the appropriate amount of failover capacity to reserve, considering that the host with the most resources is the one to fail.

This provides the best of both worlds when comparing slot-based and percentage-based admission control policies. These improvements eliminate the requirement for manual calculations and reduce the chance of user error.

Another new enhancement is the *Performance Degradation VMs Tolerate*. This setting controls the amount of performance reduction that is tolerated after a failure. vSphere HA uses VM performance data provided by vSphere DRS to determine whether sufficient capacity is available to maintain comparable performance after a failover. This is useful when VM reservations are not used and the consumed capacity exceeds the failover capacity. A value of 0 percent indicates that no performance degradation is tolerated; a 100 percent value disables this warning.

vSphere HA Support for NVIDIA GRID vGPU Configured VMs

vSphere HA now protects VMs with the NVIDIA GRID vGPU shared pass-through device. In the event of a failure, vSphere HA attempts to restart the VMs on another host that has an identical NVIDIA GRID vGPU profile. If there is no available healthy host that meets this criterion, the VM fails to power on.

NOTE: vSphere HA admission control policies do not take into account NVIDIA GRID vGPU resources.

VMware vSphere Fault Tolerance

VMware vSphere Fault Tolerance (vSphere FT) 6.5 improves the integration with vSphere DRS to enable better placement decisions by ranking the hosts based on the available network bandwidth and by recommending the datastore in which to place the secondary VMDK files.

Network latency between the primary and secondary VMs has been greatly decreased. This reduces the performance impact of certain types of applications that are sensitive to latency and enables a wider array of mission-critical applications that require zero downtime.

Multiple port groups can now be used to increase the overall bandwidth available for vSphere FT logging traffic. This is a similar configuration to that used by the multi-NIC feature of vSphere vMotion to provide additional channels of communication for environments that require more bandwidth than a single network adapter can provide.

Resource Management Enhancements

Predictive DRS

Predictive DRS is a new feature that leverages the predictive analytics of vRealize Operations Manager with the powerful resource scheduler algorithm of vSphere DRS. Together, these two products enable workload balancing for certain VMs before resource utilization spikes occur, potentially eliminating a great amount of resource contention that might have occurred in the past.

vRealize Operations Manager runs its dynamic thresholds algorithm nightly against the VMs on which it collects data. These dynamic thresholds create forecasted metrics for the future utilization of the VMs. The metrics are then passed to vSphere DRS to determine the best placement and balance of VMs before resource utilization spikes occur. Predictive DRS helps prevent resource contention on hosts that run VMs with predictable utilization patterns.

Improved vSphere DRS Load Balancing Algorithm

vSphere DRS uses a target standard deviation as the driving metric to perform load balancing. It monitors the current load in the cluster and generates recommendations to minimize the standard deviation. When the standard deviation is less than or equal to the target standard deviation, the cluster is considered balanced.

The standard deviation model has proven to work well in most cases. But as clusters become larger, the distribution patterns become normalized, causing outliers. Outliers are hosts for which the utilization is greater than the average utilization of the cluster but do not pose a significant impact to the standard deviation.

To detect these outliers, improvements were made to the vSphere DRS algorithm. In addition to standard deviation, vSphere DRS calculates the difference between the most utilized and least utilized host and makes additional migration recommendations to reduce this variance. This is known as a pairwise calculation, which addresses the outlier condition. It results in a better overall balance of cluster resources and individual VM performance.

vSphere DRS Additional Options

By using a checkbox in VMware vSphere Web Client, it is now easier than ever to configure the three most common advanced options used in vSphere DRS clusters:

- VM distribution: This enables vSphere DRS to evenly distribute the VMs across the hosts to minimize the impact of a single host failure. VM performance remains the top priority for placement recommendations, and vSphere DRS continues to ensure that demand is met. Under severe resource contention conditions, vSphere DRS prioritizes performance over even distribution and might not fully honor this option.
- Memory metric for load balancing: vSphere DRS uses active memory + 25 percent as its primary metric when calculating memory load on a host. This option changes the metric for memory load, using consumed memory rather than active memory. It should be used only in clusters where memory is not overcommitted—that is, the allocated VM memory does not exceed physical host memory.

- CPU overcommitment: This enforces a maximum vCPU:pCPU ratio at the cluster level. After the cluster reaches this defined value, no additional VMs will be allowed to power on. This helps prevent CPU contention in environments in which many VMs spike at the same time, such as a virtual desktop environment.

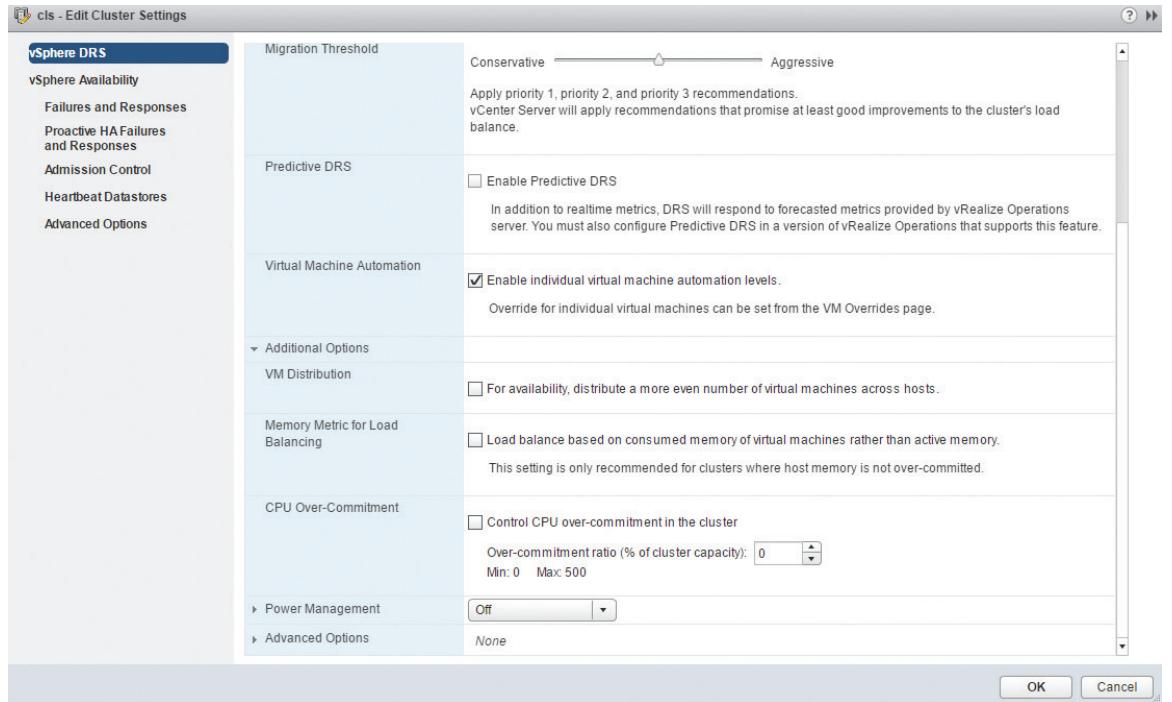


Figure 25. vSphere DRS Additional Options

Network-Aware vSphere DRS

In addition to the more than 25 metrics already used when making migration recommendations, vSphere DRS also takes network utilization into account. It monitors the Tx and Rx rates of the connected physical uplinks and avoids placing VMs on hosts that are considered network saturated—that is, more than 80 percent utilized. vSphere DRS does not reactively balance the hosts solely based on network utilization. Rather, it uses network utilization as an additional input when determining whether a host is the best recipient for a VM. This input improves vSphere DRS placement decisions, enabling optimal VM performance.

VMware vSphere Storage I/O Control Using Storage Policy Based Management

VMware vSphere Storage I/O Control (SIOC) configuration is now set using SPBM. IOPS limits are enforced using VMware vSphere Storage APIs – I/O Filtering (VAIO). The SPBM framework provides centralized administration of storage policies applied to VMs. This reduces administration overhead when varying tiers of storage services are offered, and it provides an easy way to audit and validate policy compliance.

vSphere Storage APIs – I/O Filtering enforces only the IOPS limits defined in the storage policy. IOPS reservations and shares are enforced using the mClock scheduler.

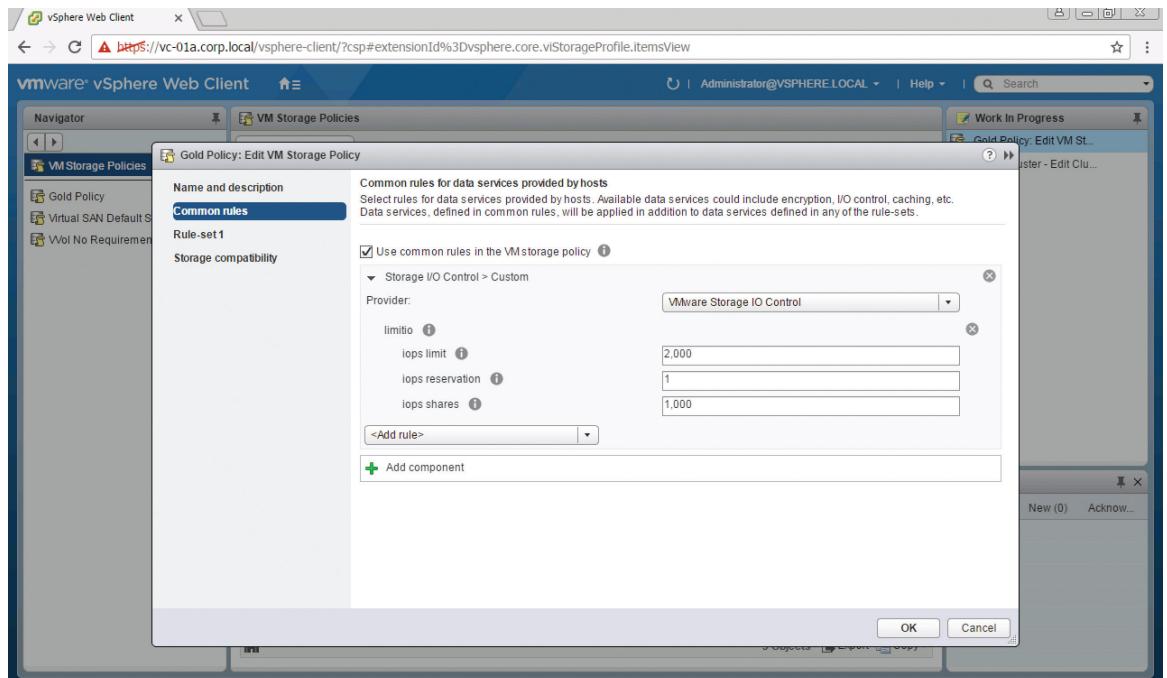


Figure 26. vSphere Storage I/O Control Configuration

vSphere Integrated Containers

vSphere is a universal application platform that supports both traditional and next-generation apps. Although these two worlds are vastly different, both require an infrastructure with the scale, performance, and availability to meet key business objectives.

To run any application, vSphere 6.5 expands its workload coverage model by focusing on both scale-up and scale-out next-generation apps that increasingly leverage evolving technology building blocks such as containers. This release delivers VMware vSphere Integrated Containers™, the easiest way for vSphere users to bring containers into an existing vSphere environment.

vSphere Integrated Containers provides an enterprise container infrastructure that offers the best of both worlds for developers and vSphere operations teams. Containers are now as easy to enable and manage as virtual machines. No process or tool changes are required.

vSphere Integrated Containers helps customers transform their business with containers without rearchitecting their existing infrastructure. It comprises three components:

- Engine provides the core container runtime.
- Harbor is an enterprise registry for container images.
- Admiral is a portal for container management by development teams.

vSphere Integrated Containers enables IT operations teams to provide their app teams with a Docker-compatible interface that runs on the existing vSphere infrastructure. It features tight integration with VMware NSX, to support best-in-class network automation and scale-out, and with Virtual SAN, to support high-performance persistent storage.

vSphere 6.5 Storage Enhancements

Advanced Format Drives and 512e Mode

The standard sector size for disks has been 512 bytes for more than a decade. To provide large-capacity drives, the storage industry is moving toward Advanced Format (AF) drives. These drives use a large physical sector size of 4,096 bytes. With this new 4K AF format, disk drive vendors can create more reliable large-capacity HDD to support growing storage needs. These drives are more cost effective because they provide a better dollar-to-gigabyte ratio.

There are two varieties of AF drives. vSphere 6.5 supports 512 emulation (512e) mode for VMware vSphere VMFS datastores and RDMS. This enables it to work with legacy OSs and applications while still providing large-capacity drives. Because it includes major changes that make VMFS metadata 4K aligned, 512e mode requires the new VMFS 6 version available with vSphere 6.5. vSphere works with storage arrays supporting 512e LUNs.

Automated UNMAP

UNMAP is a VMware vSphere Storage APIs – Array Integration primitive that enables reclamation of dead or stranded space on thinly provisioned VMFS volumes. In vSphere 6.0, this can be initiated by running a simple ESXCLI command that can free up deleted blocks from storage. vSphere 6.5 automates the UNMAP process by which VMFS tracks the deleted blocks and reclaims deleted space from the backend array in background. This background operation ensures a minimal storage I/O impact due to UNMAP operations. UNMAP works at a guest OS level with newer versions of Windows and Linux.

LUN Scalability

Customer environments are continuously growing, requiring increased scalability in storage paths and LUNs. vSphere 6.0 currently limits the maximum number of LUNs to 256 and paths to 1,024. These limits pose challenges for customers in the following situations:

- The maximum is 128 LUNs per cluster when the infrastructure has eight paths to a LUN.
- Many customers tend to have smaller-sized LUNs to segregate important data for easy backup and restore. This approach can exhaust current LUN and path limits.
- Active-active clusters can have a maximum of 128 LUNs, which is half the current supported limit. Large LUN limits can enable customers to have larger cluster sizes, reducing management overhead.

In vSphere 6.5, there is support for 512 LUNs and 2,000 paths, greatly improving storage infrastructure scalability for customers.

NFS 4.1 Support

NFS 4.1 has been supported since vSphere 6.0. It has stronger cryptographic algorithms with Kerberos authentication using Microsoft Active Directory. vSphere 6.5 introduces Kerberos integrity check (SEC_KRB5i) along with Kerberos authentication. There is also support for IPV6 with Kerberos. Host Profiles in vSphere 6.5 includes support for NFS 4.1. These enhancements provide better security for customers.

Software iSCSI Static Routing Support

There have been limitations in the past when using software iSCSI when the iSCSI initiator and target had to be on the same subnet. With vSphere 6.5, the software iSCSI initiator and target can be on different subnets. Static routes can be configured to route between the initiator and target subnets. vSphere 6.5 makes it easy to configure multipathing without requiring that the initiator and target be in the same network.

vSphere 6.5 Networking Enhancements

Dedicated Gateways for VMkernel Network Adapter

Prior to vSphere 6.5, vSphere DRS, vSphere vMotion, iSCSI, and provisioning have leveraged a single gateway. This has been an impediment because the addition of static routes on all hosts has been required. Managing these routes can be cumbersome as well as not scalable.

vSphere 6.5 provides capabilities by which different services use different default gateways. This enables end users to leverage these features without having to add static routes. vSphere 6.5 eliminates the need for static routes for all VMkernel-based services, making it more efficient and more scalable.

SR-IOV Provisioning

Prior to vSphere 6.5, VM provisioning workflow for SR-IOV devices required the user to manually assign the SR-IOV network adapter. This resulted in inflexible VM provisioning operations that were not amenable to automation at scale. In vSphere 6.5, SR-IOV devices can be added to VMs in a similar manner as any other device, making it easier to manage and automate.

Support for ERSPAN

ERSPAN mirrors traffic on one or more “source” ports and delivers the mirrored traffic to one or more “destination” ports on another switch. vSphere 6.5 includes support for the ERSPAN protocol.

Improvements in DATAPATH

vSphere 6.5 provides the following datapath improvements:

- VMkernel capability to support 2M page
- VMKAPI lock enhancement to improve scalability of VMware vSphere Distributed Switch™
- Health-check scalability upgrades

Conclusion

As the ideal platform for apps, cloud, and business, VMware vSphere 6.5 reinforces the customer’s investment in VMware. vSphere 6.5 is one of the core components of the VMware Software-Defined Data Center (SDDC) and is a fundamental building block for the VMware cloud strategy. With vSphere 6.5, customers can now run, manage, connect, and secure their applications in a common operating environment, across clouds and devices.

About the Authors

Adam Eckerle is a senior technical marketing architect for VMware vCenter Server and VMware vSphere Clients, including the vSphere Web Client and the HTML5-based vSphere Client. Find him on Twitter [@eck79](#).

Mike Foley is a senior technical marketing architect with a focus on the security of the VMware vSphere platform. He is a recognized authority on virtualization-based infrastructure security and is a patent (8,601,544) holder in this field. Find him on Twitter [@MikeFoley](#).

Eric Gray is principal technical marketing architect in the Cloud Platform business unit. He has been with VMware since 2005. His current focus is on VMware vSphere host lifecycle management. Find him on Twitter [@eric_gray](#).

Matthew Meyer is a senior technical marketing architect working on Software-Defined Data Center technologies. Matthew specializes in VMware vSphere availability and resource management. He holds many industry certifications, including VMware Certified Design Expert (VCDX#69) and CompTIA A+.

Kyle Ruddy is a senior technical marketing engineer for VMware vSphere with Operations Management™ and vSphere automation and developer interfaces. Find him on Twitter [@kmruddy](#).

Emad Younis is a senior technical marketing engineer in the Cloud Platform business unit. His current focus is on the VMware vCenter Server Appliance and vCenter Server migration. Find him 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

Copyright © 2016 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. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMW-TWP-vSPHR-6.5-USLET-102

Docsource: OIC-FP-1819