

# WHAT'S NEW IN VMWARE vSPHERE® 6.7

## Contents

<b>Introduction</b> .....	<b>4</b>
Simple and Efficient Management at Scale .....	4
Comprehensive Built-In Security .....	5
Universal Application Platform .....	6
Seamless Hybrid Cloud Experience .....	7
<b>vCenter Server 6.7</b> .....	<b>8</b>
Lifecycle .....	8
Install .....	8
Migrate .....	9
Upgrade .....	10
Monitoring and Management .....	10
vSphere Client .....	12
CLI Tools .....	13
<b>vSphere 6.7 Lifecycle Management</b> .....	<b>14</b>
New vSphere Update Manager Interface .....	14
Faster Major Version Upgrades from ESXi 6.5 to 6.7 .....	17
vSphere Quick Boot .....	17
<b>vSphere with Operations Management 6.7</b> .....	<b>18</b>
vSphere Client Plug-in .....	18
New Quick Start Dashboard .....	19
Workload Optimization Dashboard Updates .....	19
Capacity Overview Dashboard Updates .....	20
<b>vSphere 6.7 Developer and Automation Interfaces</b> .....	<b>21</b>
Appliance API Updates .....	21
vCenter Server API Updates .....	22
Other API Updates .....	22

vSphere 6.7 Security .....	23
TPM 2.0 Support for ESXi Hosts .....	23
Virtual TPM 2.0 for VMs .....	24
Support for Microsoft Virtualization-Based Security .....	25
UI Updates .....	26
Multiple Syslog Targets .....	27
FIPS 140-2 Validated Cryptographic Modules by Default .....	27
vSphere 6.7 for Enterprise Applications.....	27
Persistent Memory.....	27
Remote Directory Memory Access.....	29
Conclusion .....	30
Resources.....	30
About the Authors .....	31

## Introduction

VMware vSphere® 6.7 delivers key capabilities to enable IT organizations to address the following notable trends that are putting new demands on their IT infrastructure:

- Explosive growth in quantity and variety of applications, from business-critical applications to new intelligent workloads
- Rapid increase in hybrid cloud environments and use cases
- Global expansion of on-premises data centers, including at the edge
- Heightened importance of security relating to infrastructure and applications

The following sections discuss some of the key capabilities in vSphere 6.7 that address the aforementioned trends.

### Simple and Efficient Management at Scale

vSphere 6.7 builds on the technological innovation delivered by vSphere 6.5 and elevates the customer experience to an entirely new level. It provides exceptional management simplicity, outstanding operational efficiency, and faster time to market—all at scale.

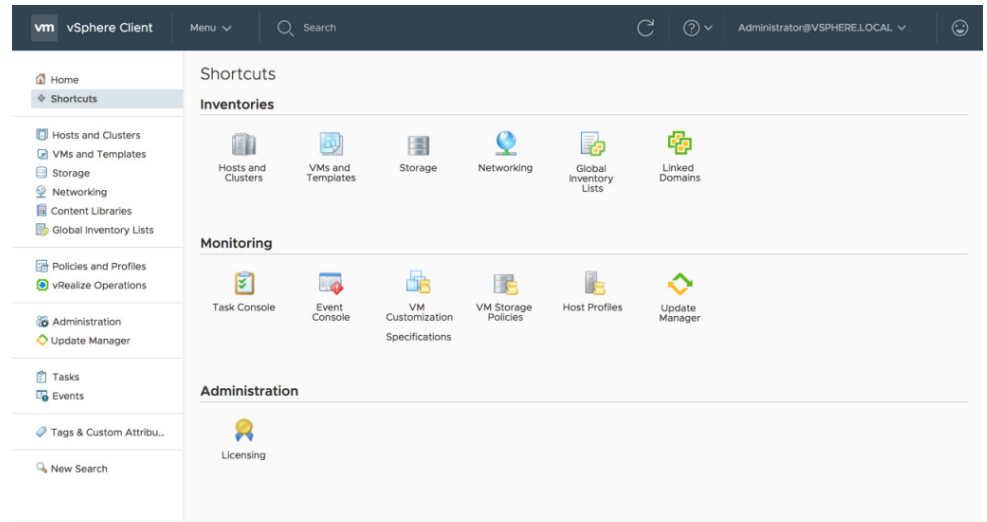
vSphere 6.7, with its improved VMware vCenter Server® Appliance™ system, delivers an extraordinary user experience. It introduces several new APIs that improve the efficiency and experience of deploying multiple vCenter Server Appliance instances based on a template. These new APIs also make management of vCenter Server Appliance systems significantly easier while facilitating a more complete backup-and-restore solution. vSphere 6.7 also simplifies the VMware vCenter Server topology through vCenter Server systems with an embedded Platform Services Controller™ instance in Enhanced Linked Mode. This enables administrators to link multiple vCenter Server instances and have seamless visibility across the environment without the need for an external Platform Services Controller instance or load balancers.

With vSphere 6.7, vCenter Server Appliance delivers major performance improvements (all metrics compared at cluster scale limits in contrast to vSphere 6.5):

- 2X faster performance in vCenter Server operations per second
- 3X reduction in memory usage
- 3X faster operations relating to VMware vSphere Distributed Resource Scheduler™ (vSphere DRS)—for example, virtual machine (VM) power-on

These performance improvements ensure a blazing fast experience for vSphere users. They deliver significant value as well as time and cost savings in a variety of use cases, such as virtual desktop infrastructure (VDI), scale-out applications, big data, High Performance Computing (HPC), DevOps, distributed cloud-native applications, and so on.

vSphere 6.7 improves efficiency at scale when updating VMware ESXi™ hosts, significantly reducing maintenance time by eliminating one of two reboots normally required for major version upgrades (single reboot). In addition, the vSphere Quick Boot innovation restarts the ESXi hypervisor without rebooting the physical host, skipping time-consuming hardware initialization.



**Figure 1.** vSphere Client Shortcuts Screen Showing the New vSphere Update Manager Plug-in

The graphical user interface (GUI) itself is another key component that enables vSphere 6.7 to deliver a simplified and efficient experience. The HTML5-based vSphere Client offers a modern user interface (UI) connection that is both responsive and easy to use. With vSphere 6.7, it includes added functionality to support not only the typical workflows customers need but also other key functions such as managing VMware NSX®, VMware vSAN™, VMware vSphere Update Manager™, as well as third-party components.

### Comprehensive Built-In Security

vSphere 6.7 builds on vSphere 6.5 security capabilities and leverages its unique position as the hypervisor to provide comprehensive security via an operationally simple policy-driven mode that starts at the core.

vSphere 6.7 adds support for Trusted Platform Module (TPM) 2.0 hardware devices for ESXi hosts and also introduces virtual TPM (vTPM) 2.0 for VMs, significantly enhancing protection and ensuring integrity for both the hypervisor and the guest operating system (OS). This capability helps prevent VMs and hosts from being tampered with. In vSphere 6.5, we introduced support for Secure Boot for ESXi hosts. This ensures that only digitally signed modules are loaded and prevents the installation of unsigned code. With vSphere 6.7, we have built upon that capability with the use of TPM 2.0 to provide measured assurance that this process has completed successfully. For virtual machines, vTPM 2.0 gives VMs the ability to use enhanced guest OS security features sought by security teams.

vSphere 6.5 introduced VM Encryption, which was very well received. With vSphere 6.7, VM Encryption is further enhanced, is more operationally easy to manage, and simplifies workflows. This is designed to protect data at rest and in motion, via a right-click, while also increasing the security posture of encrypting the VM and giving users a greater degree of control to protect against unauthorized data access.

vSphere 6.7 also improves protection for data in motion by enabling Encrypted vMotion across various vCenter Server instances as well as versions. This makes it easy to securely conduct data center migrations or to move data across a hybrid cloud environment—that is, between on-premises and public cloud—or across geographically distributed data centers.

**NOTE:** *Cross-vCenter Encrypted vMotion is supported only for VMs that are not encrypted.*

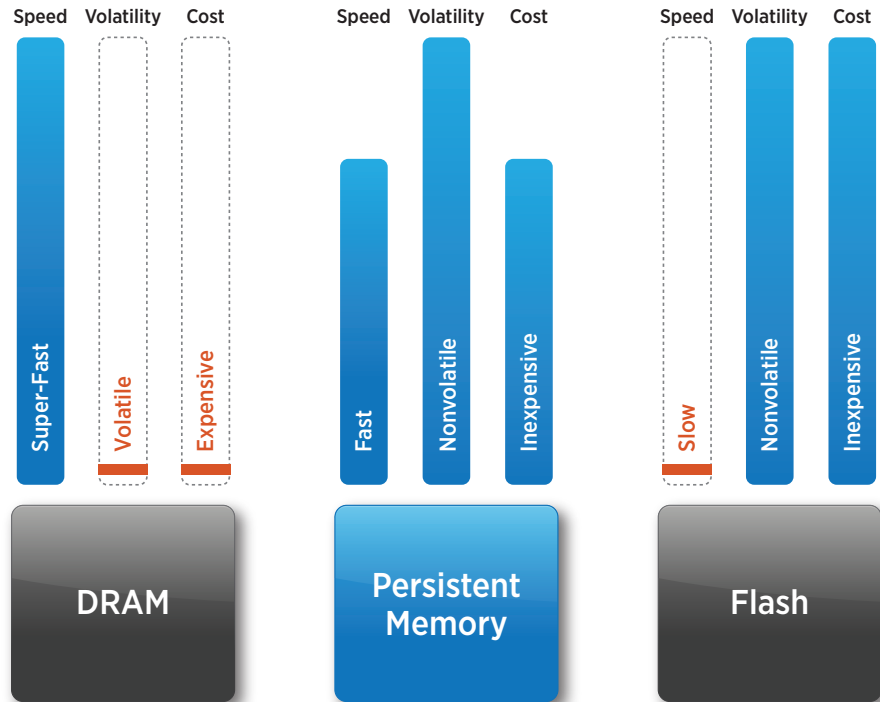
vSphere 6.7 introduces support for the entire range of Microsoft virtualization-based security technologies introduced in Windows 10 and Windows Server 2016. This is a result of close collaboration between VMware and Microsoft to ensure that Windows VMs on vSphere systems support in-guest security features while continuing to be performant and secure on the vSphere platform.

vSphere 6.7 delivers comprehensive built-in security and is the heart of a secure Software-Defined Data Center (SDDC). It has deep integration and works seamlessly with other VMware products such as NSX, vSAN, and VMware vRealize® Suite to provide a complete security model for the data center.

### Universal Application Platform

vSphere 6.7 is a universal application platform that supports existing mission-critical applications as well as new workloads such as 3D graphics, big data, HPC, machine learning, in-memory, and cloud-native. It also supports and leverages some of the latest hardware innovations in the industry, delivering exceptional performance for a variety of workloads.

vSphere 6.7 further improves the support and capabilities introduced for graphics processing units (GPUs) through the VMware collaboration with NVIDIA. It virtualizes NVIDIA GPUs even for non-VDI use cases and for computing that is other than general purpose such as artificial intelligence, machine learning, big data, and more. With enhancements to NVIDIA GRID® vGPU™ technology in vSphere 6.7, administrators can simply suspend and resume workloads running on GPUs instead of having to power off those VMs. This is especially valuable when migration of the workload or VM is required during maintenance or other operations. It enables better lifecycle management of the underlying host and significantly reduces disruption for end users. VMware continues to invest in this area, with the goal of bringing the full vSphere experience to GPUs in future releases.



**Figure 2.** vSphere Persistent Memory - More Cost-Effective than DRAM and More Performant than Flash

vSphere 6.7 continues to showcase VMware technological leadership and fruitful collaboration with our key partners by adding support for vSphere Persistent Memory, a key industry innovation poised to have a dramatic impact on the landscape. With vSphere Persistent Memory, administrators using supported hardware modules such as those available from Dell EMC and Hewlett Packard Enterprise can leverage them either as super-fast storage with high IOPS or expose them to the guest OS as nonvolatile memory (NVM). This significantly improves OS performance as well as applications across a variety of use cases, making existing applications faster and more performant and enabling administrators to create new high-performance applications that can leverage vSphere Persistent Memory.

Find more information on the [Virtual Blocks Core Storage 6.7](#) blog to learn about new storage and network features that further enhance enterprise applications running on the vSphere platform, such as 4K native (4Kn) disk support, Remote Directory Memory Access (RDMA), and Intel Volume Management Device (Intel VMD) for NVM Express (NVMe).

### Seamless Hybrid Cloud Experience

With the rapid adoption of public clouds based on the vSphere platform through VMware Cloud Provider Program partners, VMware Cloud™ on AWS, and other public cloud providers, VMware is committed to delivering a seamless hybrid cloud experience for enterprises.

vSphere 6.7 introduces vCenter Server Hybrid Linked Mode, which enables users to have unified visibility and manageability across an on-premises vSphere environment running on one version and a public cloud environment based on the vSphere platform, such as VMware Cloud on AWS, running on a different vSphere version. This ensures that the fast pace of innovation and the introduction of new capabilities in public clouds based on the vSphere platform do not force the customer to constantly update and upgrade their on-premises vSphere environment.

vSphere 6.7 also introduces cross-cloud hot and cold migration, which further enhances the ease of management across on-premises and cloud infrastructure and enables a seamless and nondisruptive hybrid cloud experience for enterprises.

As VMs migrate between various data centers or from an on-premises data center to the cloud and back, they likely move across different CPU types. vSphere 6.7 introduces per-VM Enhanced vMotion Compatibility (EVC), a key capability for the hybrid cloud that enables the EVC mode to become an attribute of the VM rather than of the specific processor generation it is booted on in the cluster. This facilitates seamless migration across various CPUs by persisting the EVC mode per VM during migrations across clusters and during power cycles.

vSphere 6.0 had introduced provisioning between vCenter Server instances. This is often called “cross-vCenter provisioning.” Using two vCenter Server instances presents the possibility that these instances are on different release versions. vSphere 6.7 enables customers to use different vCenter Server versions while allowing cross-vCenter, mixed-version provisioning operations such as VMware vSphere vMotion® migration, full clone, and cold migrate to continue seamlessly. This is especially useful for enterprises leveraging VMware Cloud on AWS as part of their hybrid cloud.

## vCenter Server 6.7

vSphere 6.7 introduces many new enhancements across several areas for vCenter Server Appliance. Users now have improved monitoring tools. The vSphere Client has many new workflows and is closer to feature parity. The vCenter Server Appliance architecture is moving to a simpler deployment model. In addition, the built-in file-based backup now includes a scheduler, and the vCenter Server Appliance UI has been updated to Clarity. This section will provide more details on these and other vCenter Server Appliance 6.7 enhancements.

### Lifecycle

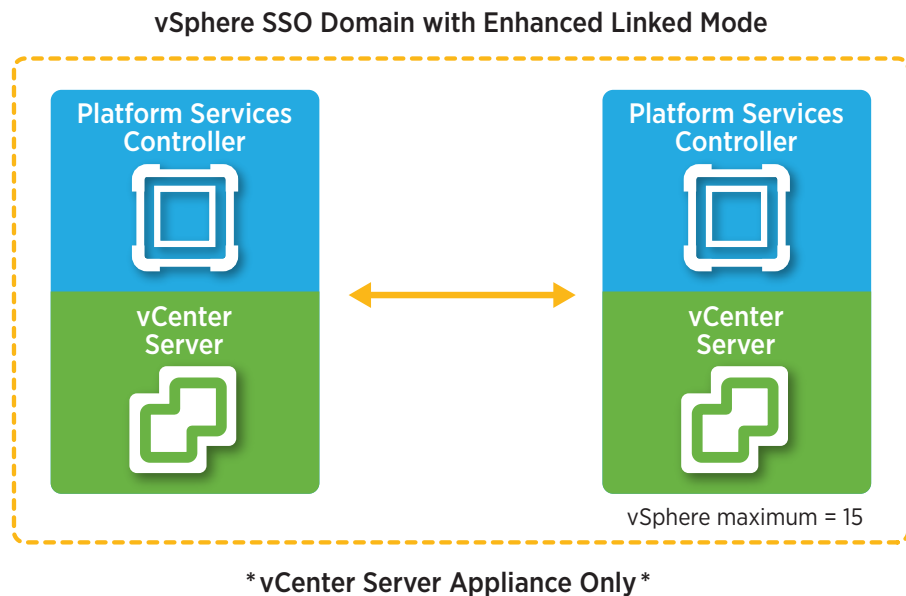
#### Install

One significant change to vCenter Server Appliance 6.7 is a simplification of the architecture and a reversion to running all vCenter Server services on a single instance. With the introduction of vCenter Server with embedded Platform Services Controller instance with Enhanced Linked Mode, this deployment model provides the following benefits:

- Requires no load balancer for high availability; fully supports native vCenter Server high availability



- Provides flexibility of placement in the vSphere single sign-on (SSO) domain with site boundary removal
- Supports vSphere scale maximums
- Allows 15 deployments in a vSphere SSO domain
- Reduces the number of nodes to manage and maintain



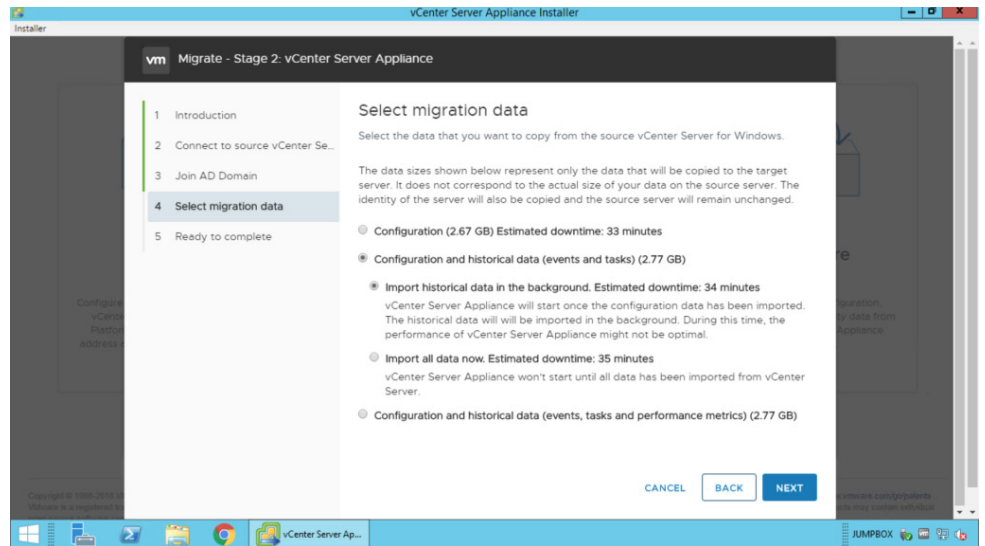
**Figure 3.** Embedded Platform Services Controller Instances with Enhanced Linked Mode

### Migrate

vSphere 6.7 is the last release to include vCenter Server for Windows, which has been [deprecated](#). Customers can migrate to vCenter Server Appliance with the built-in migration tool. vSphere 6.7 offers these options on how to import historical and performance data during a migration:

- Deploy and import all data
- Deploy and import data in the background

Users get a time estimate of how long each option will take when migrating. Estimated time will vary based on historical and performance data size in a user's environment. While importing data in the background, users can choose to pause and resume. This new ability is available in the vSphere appliance management interface (VAMI). Support of custom ports is another improvement to the migration process. Users who changed the default Windows vCenter Server ports are no longer blocked.



**Figure 4.** Background Data Migration

## Upgrade

vSphere 6.7 supports upgrades and migrations from only vSphere 6.0 or 6.5. vSphere 5.5 does not have a direct upgrade path to vSphere 6.7. Customers still on vSphere 5.5 must first upgrade to vSphere 6.0 or 6.5 and then to vSphere 6.7. Also, a vCenter Server 6.0 or 6.5 instance managing ESXi 5.5 hosts cannot be upgraded or migrated until the hosts have been upgraded to ESXi 6.0 or later.

*NOTE: [General support for vSphere 5.5 ends September 19, 2018.](#)*

## Monitoring and Management

A considerable amount of investment went into improving the monitoring for vCenter Server Appliance. These improvements started in [vSphere 6.5](#), and vSphere 6.7 adds several new enhancements. First, log in to the VAMI on port 5480. The first thing to notice is that the VAMI has been updated to the [Clarity UI](#). Also, there are several new tabs on the left-hand side compared to vSphere 6.5. There is now a tab dedicated to monitoring, for views of CPU, memory, network, and database utilization. A new section of the monitoring tab called **Disks** is now available in vCenter Server 6.7. Users can now see each of the disk partitions for a vCenter Server Appliance instance, along with its allocated space and utilization.

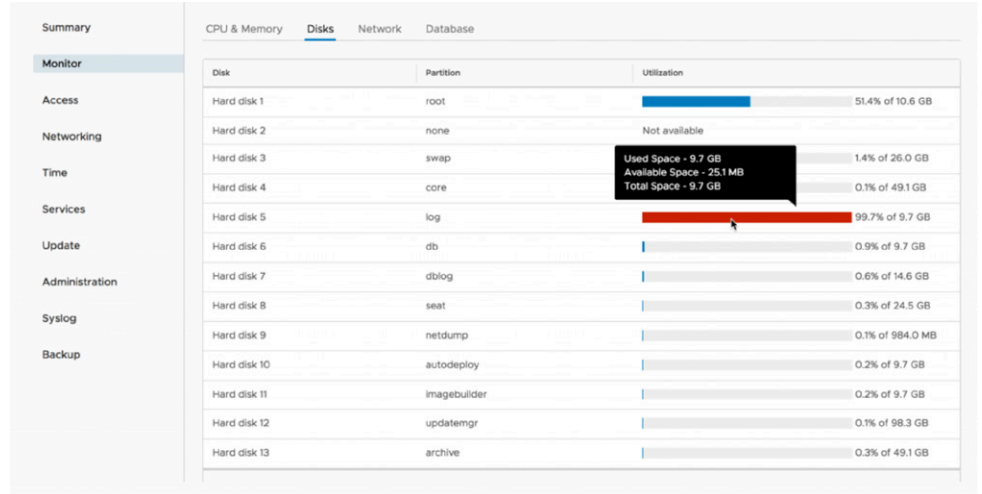


Figure 5. New Disk Utilization Screen

**File-Based Backup** was first introduced in vSphere 6.5 under the **Summary** tab; now it has its own tab. A scheduler is the first available option, front and center, when going to the **Backup** tab. Now users can schedule backups of their vCenter Server Appliance instances and can select how many backups to retain. **Activities** is another new section for **File-Based Backup**. When the backup job is complete, it is logged in the **Activities** section with detailed information. Discussion of backup leads to mention of restore. The restore workflow now includes a backup archive browser. The browser displays all backups without requiring information on the entire backup path.

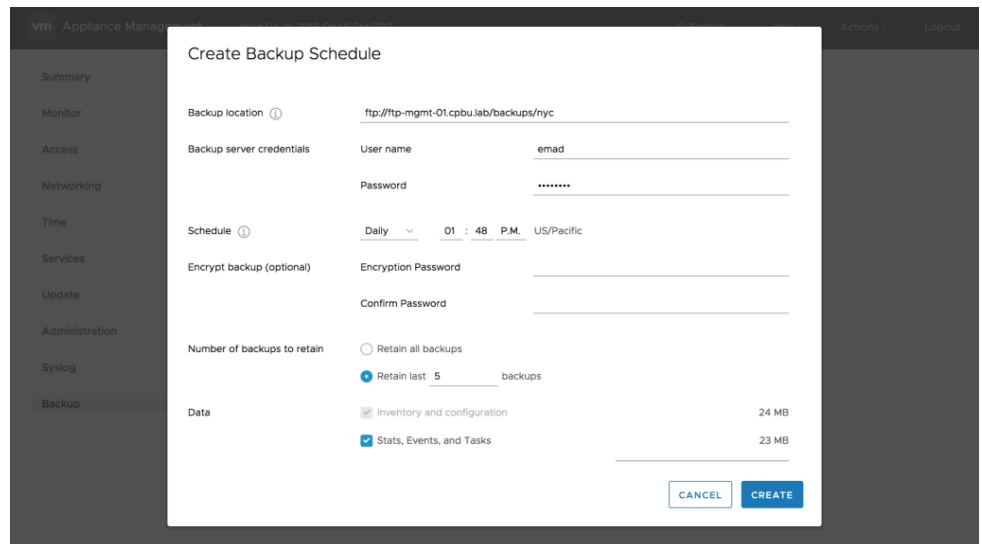


Figure 6. vCenter Server Appliance Backup Scheduler

**Services** is another new tab within the VAMI. Formerly located within VMware vSphere Web Client, it is now in the VAMI for out-of-band troubleshooting. All of the services that compose vCenter Server Appliance—startup type, health, and state—are visible here. Options are provided to start, stop, and restart services if needed.

Although the **Syslog** and **Update** tabs are not new to the VAMI, there are improvements in these areas as well. **Syslog** now supports as many as three syslog forwarding targets. vSphere 6.5 supported forwarding to only one. There is now more flexibility in patching and updating. From the **Update** tab, there is the option to select which patch or update to apply. Users also have more information, including type, severity, and if a reboot is necessary. Expanding a patch or update in the view will display more information regarding what is included. Last, we can now stage and install a patch or update from the VAMI. This capability was previously available only from the command-line interface (CLI).

### vSphere Client

Significant attention has also been given to the HTML5-based vSphere Client. With vSphere 6.5, VMware introduced a supported version of the vSphere Client. Included in vCenter Server Appliance, it had only partial functionality. The vSphere team has worked hard to get the vSphere Client closer to feature parity. Based on customer feedback, the team has been optimizing and improving workflows. vSphere 6.7 also marks the final release of the Flash-based vSphere Web Client. The following are among the newer workflows in the updated vSphere Client release:

- vSphere Update Manager
- Content library
- vSAN
- Storage policies
- Host profiles
- VMware vSphere Distributed Switch™ topology diagram
- Licensing

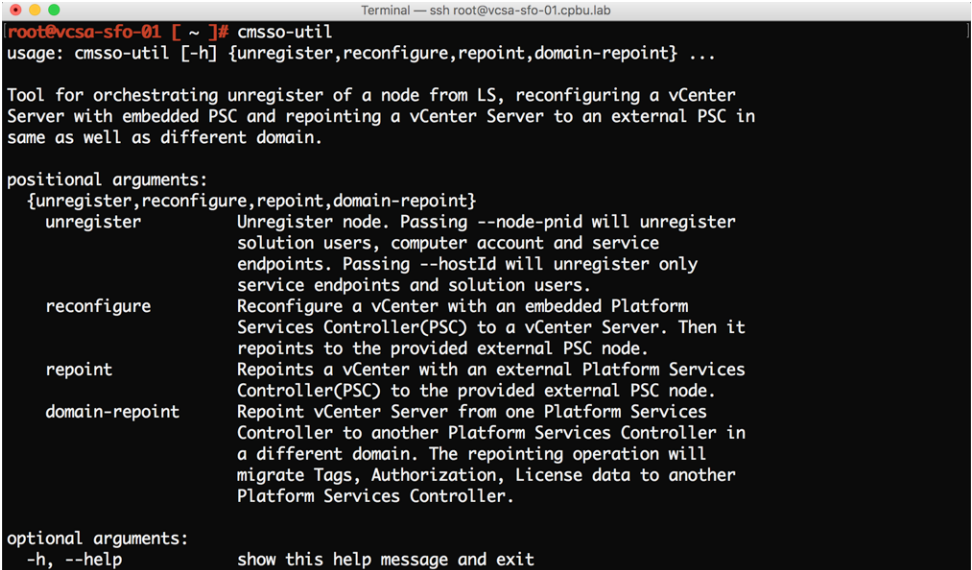
Some of these workflows are not feature complete. We will continue to update the vSphere Client in future vSphere maintenance—that is, patch and update—releases.

There is now one fewer client, because Platform Services Controller UI (/psc) functionality is now part of the vSphere Client. Located within the **Administration** menu, Platform Services Controller options are divided between two tabs: Certificate management has its own tab; all other management is under the **Configuration** tab.

## CLI Tools

The vCenter Server Appliance 6.7 CLI also has some new enhancements. The first relates to using the `cmsso-util` `repoint` command. Although repointing an external vCenter Server Appliance instance across SSO sites within a vSphere SSO domain is not a new feature, it was not available in vSphere 6.5 but makes its return in vSphere 6.7.

Administrators can now repoint their vCenter Server Appliance instance across vSphere SSO domains for consolidation. The domain repoint feature supports only external deployments running vSphere 6.7. The feature has a built-in **Pre-check** option, the use of which is strongly recommended. The pre-check compares the two vSphere SSO domains and lists any discrepancies in a conflict JSON file. This presents the opportunity to resolve any of the discrepancies before running the domain repoint tool. The repoint tool can migrate licenses, tags, categories, and permissions from one vSphere SSO domain to another.



```

Terminal — ssh root@vcsa-sfo-01.cpbu.lab
root@vcsa-sfo-01 [ ~ ]# cmsso-util
usage: cmsso-util [-h] {unregister,reconfigure,repoint,domain-repoint} ...

Tool for orchestrating unregister of a node from LS, reconfiguring a vCenter
Server with embedded PSC and repointing a vCenter Server to an external PSC in
same as well as different domain.

positional arguments:
  {unregister,reconfigure,repoint,domain-repoint}
  unregister           Unregister node. Passing --node-pnid will unregister
                       solution users, computer account and service
                       endpoints. Passing --hostId will unregister only
                       service endpoints and solution users.
  reconfigure          Reconfigure a vCenter with an embedded Platform
                       Services Controller(PSC) to a vCenter Server. Then it
                       repoints to the provided external PSC node.
  repoint              Repoints a vCenter with an external Platform Services
                       Controller(PSC) to the provided external PSC node.
  domain-repoint      Repoint vCenter Server from one Platform Services
                       Controller to another Platform Services Controller in
                       a different domain. The repointing operation will
                       migrate Tags, Authorization, License data to another
                       Platform Services Controller.

optional arguments:
  -h, --help          show this help message and exit

```

**Figure 7.** Move vCenter Server Instance to New SSO Domain via Domain-Repoint

Another CLI enhancement relates to using the CLI installer to manage the vCenter Server Appliance lifecycle. The vCenter Server Appliance ISO comes with JSON template examples. These templates can ensure consistency across installs, upgrades, and migrations. Usually, users must run one JSON template from the CLI installer at a time and in the correct order. With batch operations, this manual per-node deployment is a thing of the past. Now several JSON templates can be run in sequence from a single directory without intervention. Before running, use the **Pre-check** option on the directory to verify the templates, including sequence.

```

Terminal -- vcsa-deploy bin install --accept-eula --no-ssl-certificate-verification --verbose ~/Documents/BatchDeploy
eyounis-mac-01:mac eyounis$ ./vcsa-deploy install --accept-eula --no-ssl-certificate-verification --verbo
e ~/Users/eyounis/Documents/BatchDeploy/
Updating log file location, copying /var/folders/gz/47f6n_w16_1_klyc7pq8ddy80000gn/T/vcsaCliInstaller-201
8-04-16-19-38-5jkuwjio/vcsa-cli-installer.log' to desired location as a backup: '/var/folders/gz/47f6n_w16
_1_klyc7pq8ddy80000gn/T/vcsaCliInstaller-2018-04-16-19-38-5jkuwjio/workflow_1523907519112/vcsa-cli-install
er.log.bak'
Adding the following cli arguments to blackboard {'cli_arg_log_dir': None, 'cli_arg_no_esx_ssl_verify':
False, 'cli_arg_sub_command': 'install', 'cli_arg_operation_id': None, 'cli_arg_skip_precheck': False,
'cli_arg_no_ssl_certificate_verification': True, 'cli_arg_acknowledge_ceip': False, 'cli_arg_terse':
False, 'cli_arg_supported_deployment_sizes': False, 'cli_arg_precheck_only': False,
'cli_arg_pause_on_warnings': False, 'cli_arg_template': ['/Users/eyounis/Documents/BatchDeploy/'],
'cli_arg_verbose': True, 'cli_arg_accept_eula': True, 'cli_arg_verify_template_only': False,
'cli_arg_template_help': False}
Workflow log-dir
/var/folders/gz/47f6n_w16_1_klyc7pq8ddy80000gn/T/vcsaCliInstaller-2018-04-16-19-38-5jkuwjio/workflow_15239
07519112
CLIOptionsValidationTask: Executing CLI optionsValidation task
===== [START] Start executing Task: To validate CLI options at 19:38:39 =====
The deployment path is: /Austin/host/AUS
The deployment path is: /Austin/host/AUS
Command line arguments verified.
[SUCCEEDED] Successfully executed Task 'CLIOptionsValidationTask: Executing CLI optionsValidation task'
in TaskFlow 'template_validation' at 19:38:39

```

Figure 8. Install, Upgrade, or Migrate Multiple vCenter Server Systems with Batch Operations

## vSphere 6.7 Lifecycle Management

VMware vSphere 6.7 includes a range of improvements to accelerate host lifecycle management and save valuable time for administrators.

### New vSphere Update Manager Interface

This vSphere release includes a brand-new vSphere Update Manager interface that is part of the vSphere Client.

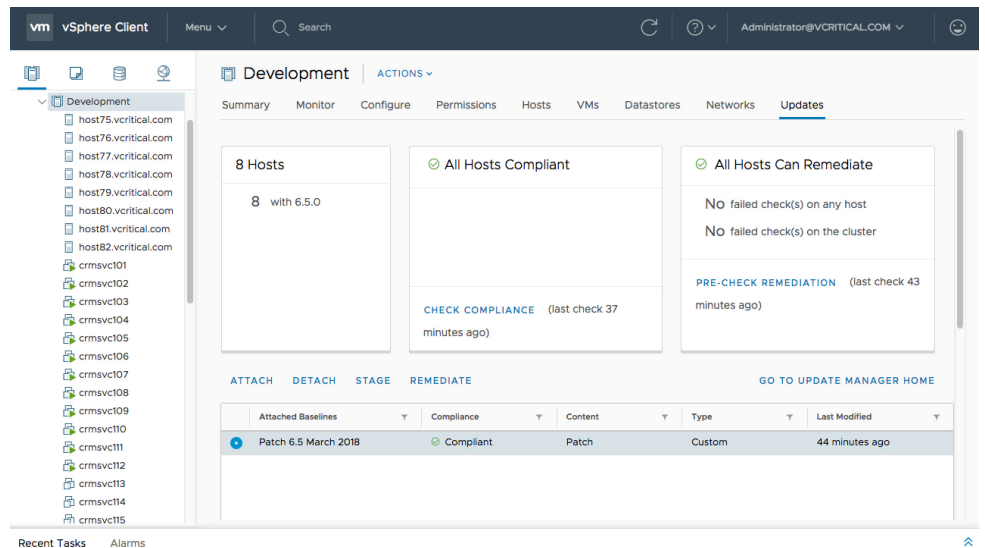
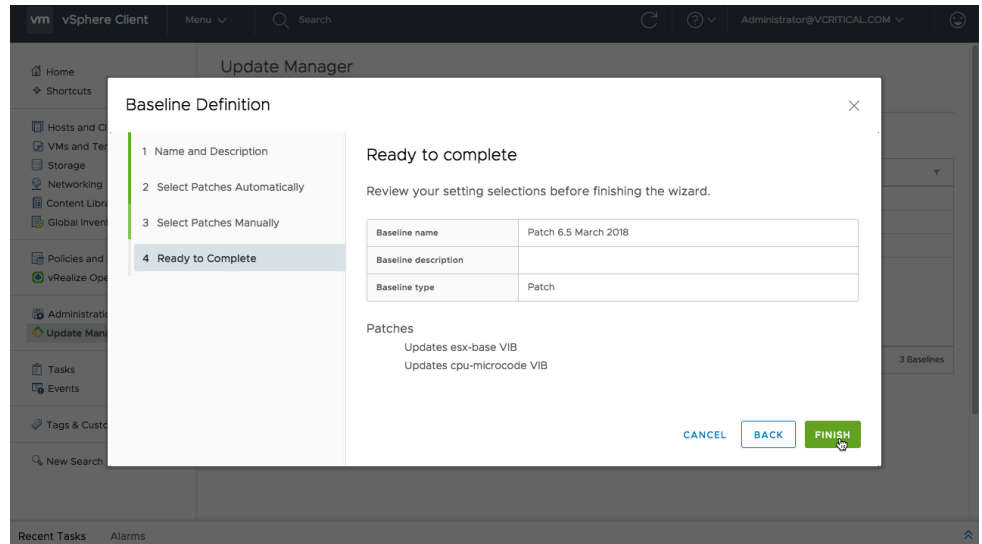


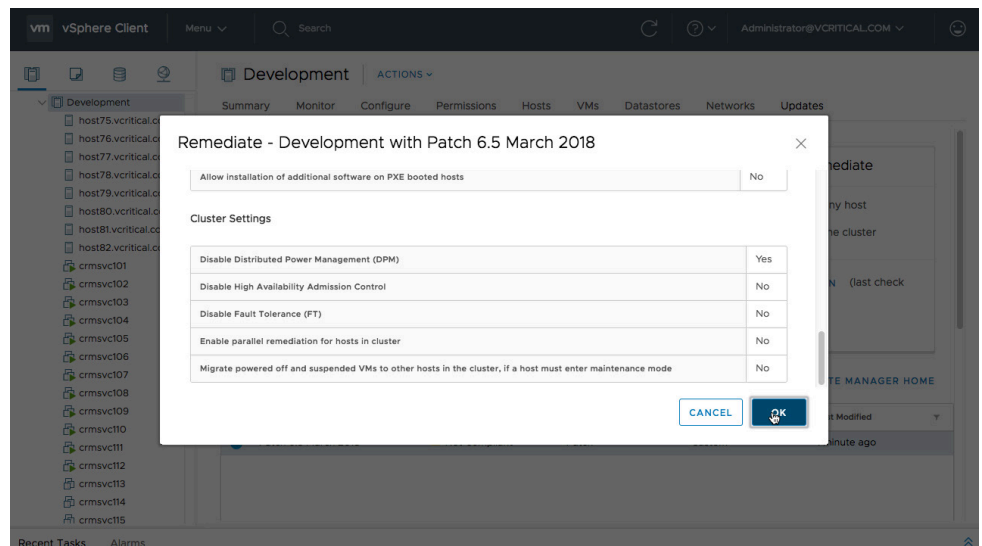
Figure 9. New vSphere Update Manager User Interface

vSphere Update Manager in vSphere 6.7 maintains reliability and security for ESXi 6.0 to 6.7 hosts by making it easy for administrators to deploy the latest patches and security fixes. And when the time comes to upgrade older releases to the latest version, ESXi 6.7, vSphere Update Manager makes that task easy too.



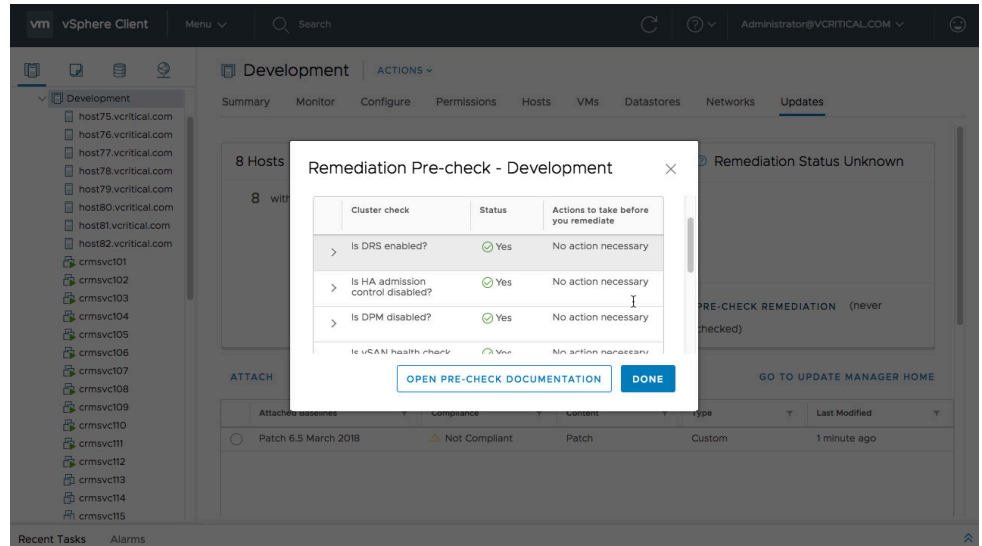
**Figure 10.** Creating a New Baseline to Patch Clusters with Preferred Patches

The new vSphere Update Manager interface is more than a simple port from the previous, Flash-based vSphere Web Client. The new UI provides a much more streamlined remediation process. For example, the previous multistep remediation wizard has been replaced by a much more efficient workflow. Only a few clicks are required to begin the procedure.



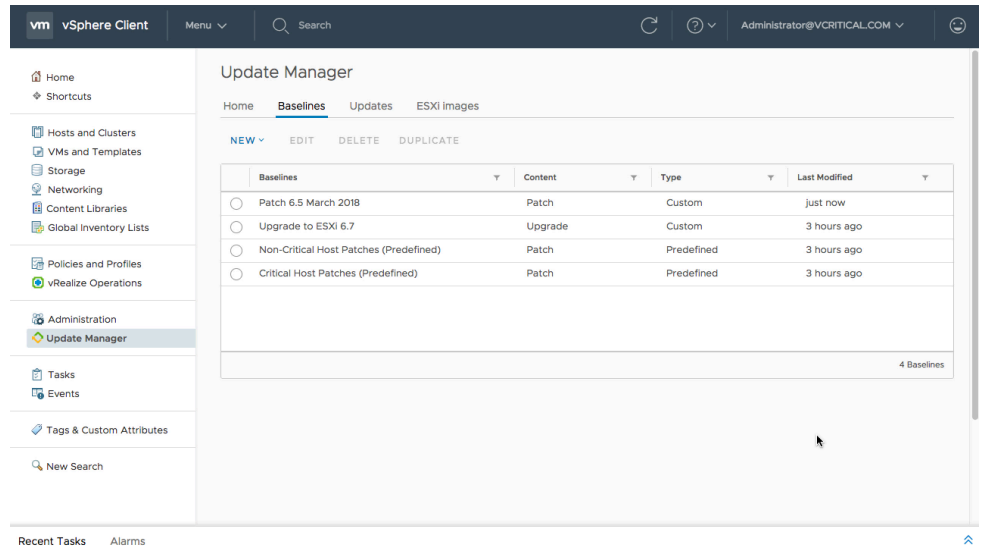
**Figure 11.** New Interface with More Streamlined Review of Remediation Actions

In addition, **Pre-check** is now a separate operation, enabling administrators to verify that a cluster is ready for upgrade before initiating the workflow.



**Figure 12.** Checking Clusters to Determine Readiness for Remediation

This initial release of the new interface supports the workflows required for upgrading and patching ESXi hosts.



**Figure 13.** New Update Manager Interface Baselines Listing

Many customers also leverage vSphere Update Manager beyond vSphere host patching and upgrading. Additional capabilities, such as upgrading VMware Tools™ and hardware compatibility, are scheduled to appear in a subsequent release.



## Faster Major Version Upgrades from ESXi 6.5 to 6.7

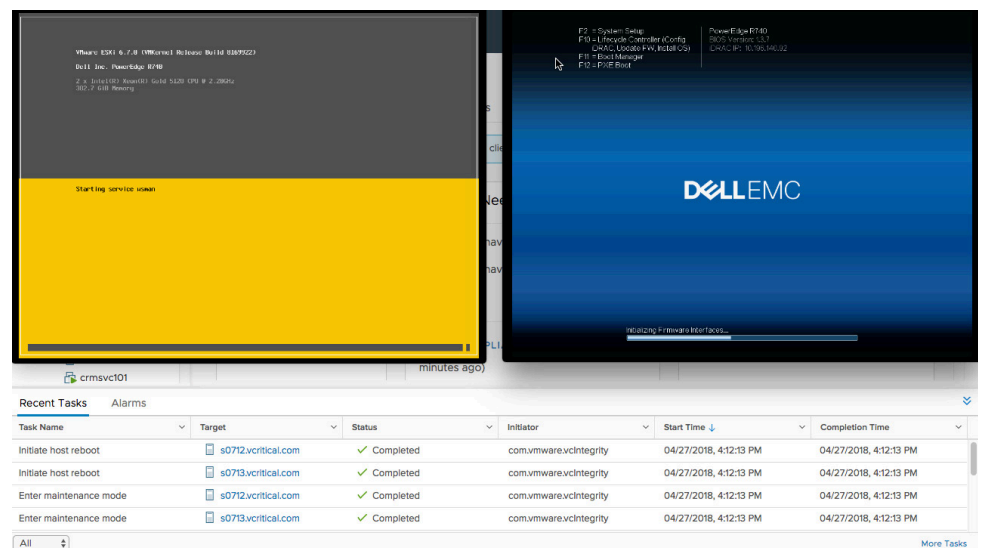
Hosts currently running ESXi 6.5 will be upgraded to ESXi 6.7 significantly faster than before. We have made several optimizations to that path, including eliminating one of two reboots traditionally required for a host upgrade. In the past, hosts that were upgraded with vSphere Update Manager were rebooted initially to prepare for the upgrade process; they were then rebooted again after the upgrade was completed. Modern server hardware, equipped with hundreds of gigabytes of RAM, typically take several minutes to initialize and perform self-tests. Initializing hardware twice during an upgrade has a cumulative effect, so this enhancement significantly shortens maintenance windows and reduces the overall time required to upgrade clusters of vSphere infrastructure. vSphere DRS and vSphere vMotion operations eliminate downtime for applications during hypervisor upgrades. VMs are moved seamlessly from host to host as needed.

## vSphere Quick Boot

vSphere 6.7 introduces vSphere Quick Boot, a new capability designed to reduce the time required for an ESXi host to reboot during update operations.

Host reboots occur infrequently but typically are necessary after activities such as applying a patch to the hypervisor or installing a third-party component or driver. Modern server hardware with large RAM capacity might take many minutes to complete device initialization and self-tests.

vSphere Quick Boot eliminates the time-consuming hardware initialization phase by shutting down an ESXi host in an orderly manner and then immediately restarting it. If it takes several minutes or more for the physical hardware to initialize devices and perform necessary self-tests, then that is the approximate time savings to expect when using vSphere Quick Boot. In large clusters that are typically remediated one host at a time, this new technology can substantially shorten time requirements for data center maintenance windows.



**Figure 14.** Two Remote Consoles Comparing vSphere Quick Boot and Standard Reboot

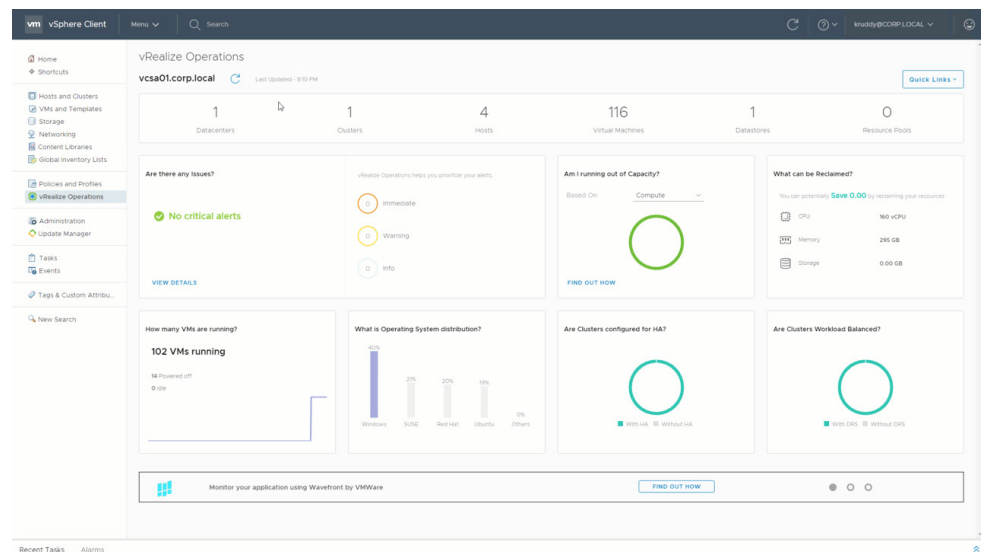
## vSphere with Operations Management 6.7

Some outstanding additions are planned for VMware vSphere with Operations Management™ 6.7—from a new plug-in for the vSphere Client, to new dashboards, to a brand-new capacity engine—making it an excellent choice for an upgrade.

The following features are included in vSphere with Operations Management 6.7.

### vSphere Client Plug-in

A new plug-in for the vSphere Client is available out of the box, providing exceptional new functionality. There are six VMware vRealize® Operations Manager™ dashboards in the vSphere Client, including an overview, cluster view, and alerts for both vCenter Server and vSAN views.



**Figure 15.** VMware vRealize Operations Manager Dashboard

To function properly, the plug-in requires vRealize Operations Manager 6.7. It then automatically connects through the vRealize Operations Manager configured user. Those not already using vRealize Operations Manager 6.7 must upgrade to use this plug-in. The plug-in can guide those without vRealize Operations Manager through the deployment process to get it up and running.

## New Quick Start Dashboard

Recent vRealize Operations Manager releases have focused on making it easier to get directly to needed data. The new vSphere **Quick Start** page accomplishes that very well by breaking the available dashboards into four use cases: **Optimize Performance**, **Optimize Capacity**, **Troubleshoot**, and **Manage Configuration**. The **Optimize Performance** use case ensures that workloads receive needed resources through workload optimization and a set of recommendations. The **Optimize Capacity** use case optimizes the current resources through the new capacity engine, reclamation opportunities, and a planning tool. The **Troubleshoot** use case is self-explanatory and provides easy access to alarms, the integrated log analytics, and helpful dashboards broken down into each high-level object type. The **Manage Configuration** use case enables verification and easy detection when an environment meets the requirements of the *vSphere Security Configuration Guide*.

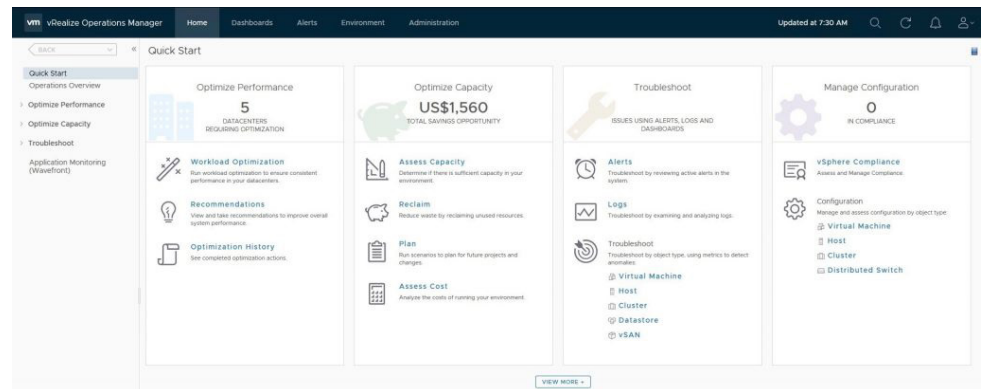


Figure 16. vRealize Operations Manager Quick Start Page – Four Use Cases

## Workload Optimization Dashboard Updates

The **Workload Optimization** dashboard has been skillfully updated. Workload optimization takes those predictive analytics and uses them in conjunction with vSphere DRS to move workloads between clusters. New with vRealize Operations Manager 6.7 is the capability to fine-tune the configuration for workload optimization. Users can control whether the goal is workload balance or consolidation, how much headroom each cluster maintains as a buffer, and prioritization to workload placement based on vSphere tags.

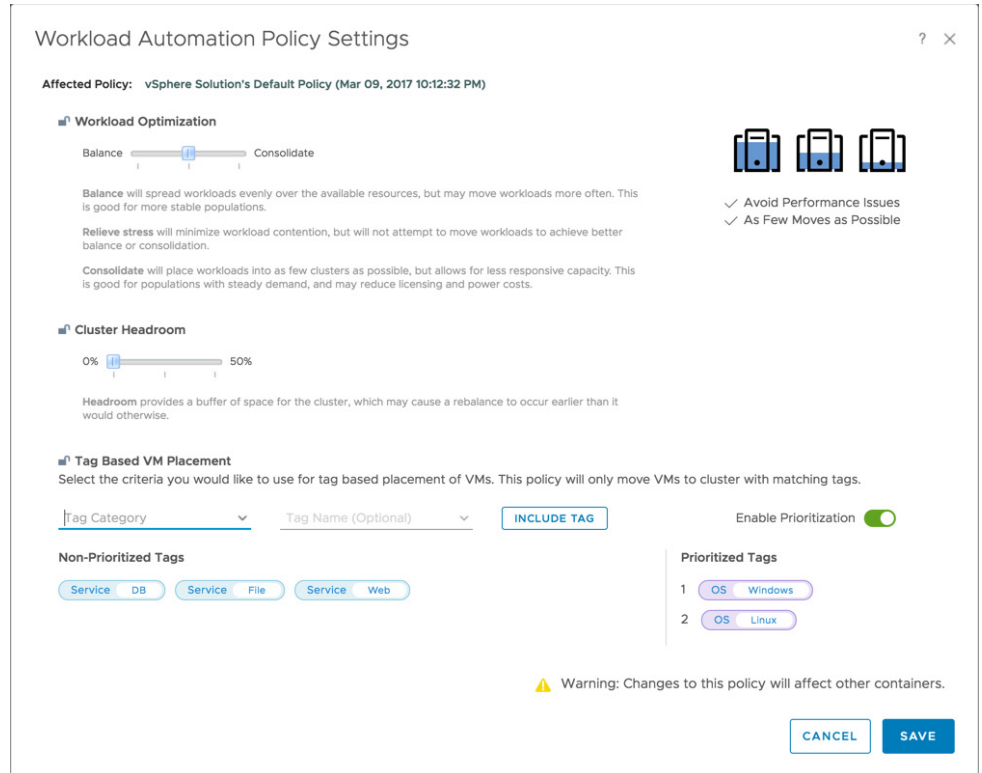
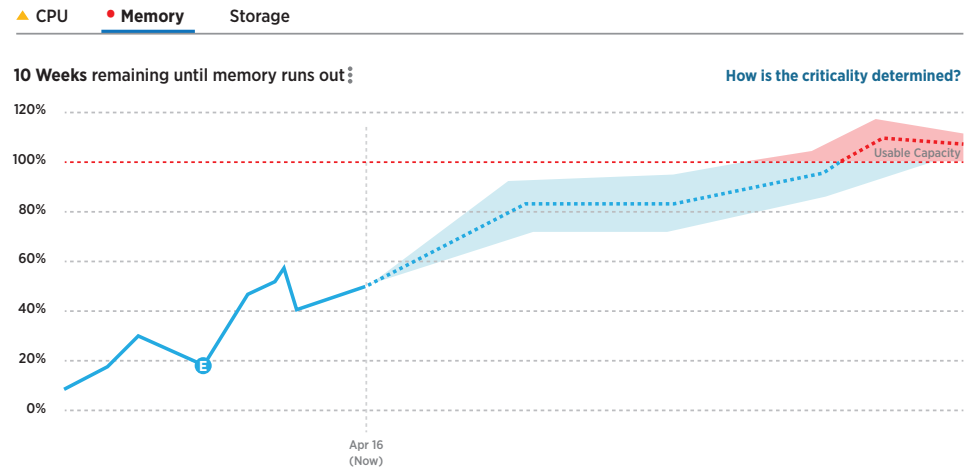


Figure 17. Workload Automation Policy Settings

## Capacity Overview Dashboard Updates

The **Capacity Overview** dashboard has been completely overhauled. vRealize Operations Manager 6.7 introduced a new capacity engine that is more intelligent and much faster. This engine can detect trends, spikes, and even workloads that occur only during specific periods. It then applies confidence boundaries to the forecast. These boundaries enable users to see both the most conservative and the most aggressive forecasts available. This dashboard also provides helpful reclamation recommendations.



**Figure 18.** New Capacity Overview Dashboard in vRealize Operations 6.7

## vSphere 6.7 Developer and Automation Interfaces

vSphere 6.7 contains numerous developer and automation updates and improvements.

With the vSphere 6.5 release, a new set of RESTful based APIs were introduced. These APIs were completely rewritten for easier usability and were made available in a more modern standard. With vSphere 6.7, we continue to add functionality to those existing APIs and expand the coverage of these APIs to several new areas.

### Appliance API Updates

We received considerable feedback on the appliance APIs. Many of those requests were incorporated into this update. The most common areas were backup and recovery as well as updates. The process of creating and monitoring backups was improved with several new methods as well as the ability to schedule backups through the API. Users can now also manage the update lifecycle through the API—from pre-checks to staging to installation and validation.

Several API methods were taken out of technical preview and are now supported: controlling the appliance-based services; managing the appliance's network configuration and NTP settings; and managing the power status of the appliance itself.

recovery/backup/schedules		Show/Hide	List Operations	Expand Operations
GET	/appliance/recovery/backup/schedules	Returns a list of existing schedules with details		
GET	/appliance/recovery/backup/schedules/{schedule}	Returns an existing schedule information based on id		
PUT	/appliance/recovery/backup/schedules/update/{schedule}	Updates a schedule		
POST	/appliance/recovery/backup/schedules/{schedule}	Creates a schedule		
POST	/appliance/recovery/backup/schedules/{schedule}?action=run	Initiate backup with the specified schedule		
DELETE	/appliance/recovery/backup/schedules/{schedule}	Deletes an existing schedule		

Figure 19. API Explorer - Backup and Recovery Methods

### vCenter Server API Updates

We also received much feedback on the vCenter Server RESTful APIs. These APIs have been increased by more than 40 new methods. New APIs have been added to interact with the VM's guest OS, view Storage Policy-Based Management (SPBM) policies, and manage vCenter Server services.

There are also a handful of new APIs to handle the deployment and lifecycle of vCenter Server. Stage 2 deployment activities are now available. We can now easily make configuration updates through the API, such as repointing a Platform Services Controller instance, reconfiguring the deployed topology, and managing updates.

deployment/upgrade		Show/Hide	List Operations	Expand Operations
GET	/vcenter/deployment/upgrade	Get the UpgradeSpec parameters used to configure the ongoing appliance upgrade.		
POST	/vcenter/deployment/upgrade?action=cancel	Cancel the appliance upgrade that is in progress.		
POST	/vcenter/deployment/upgrade?action=check	Run sanity checks using the UpgradeSpec parameters passed.		
POST	/vcenter/deployment/upgrade?action=start	Start the appliance installation.		

Figure 20. API Explorer - Deployment and Upgrade Methods

### Other API Updates

There have also been several updates to the vSphere Web Services (SOAP) APIs. There is a new method to clear all triggered alarms as well as considerable TPM functionality and some new features for EVC.

Two other areas warrant further investigation—first, the new **Instant Clone** method. Formerly known as Project Fargo and vSphere vmFork, it is now included in vSphere 6.7 and is available by API. Second, a property that has been highly requested has now been added to the **VirtualMachineConfigInfo** data object. This property, **createDate**, provides a timestamp that indicates when a VM was created.

### InstantClone\_Task(instantClone)

Creates a powered-on Instant Clone of a virtual machine. The new virtual machine will be created on the same host and start with the identical running point as the original virtual machine, sharing memory state when possible and sharing disk state. The original virtual machine must be in a powered-on state. The privilege required for Instant Clone operation are:

- VirtualMachine.Provisioning.Clone
- VirtualMachine.Interact.PowerOn
- VirtualMachine.Inventory.CreateFromExisting
- Datastore.AllocateSpace
- Resource.AssignVMToPool

**Required Privileges**  
VirtualMachine.Provisioning.Clone

**Since**  
vSphere API 6.7

#### Parameters

NAME	TYPE	DESCRIPTION
<b>_this</b>	<a href="#">ManagedObjectReference</a>	A reference to the <a href="#">VirtualMachine</a> used to make the method call.
<b>spec</b>	<a href="#">VirtualMachineInstantCloneSpec</a>	Is a <a href="#">VirtualMachineInstantCloneSpec</a> . It specifies the cloned virtual machine's configuration.

**Figure 21.** New Instant Clone API

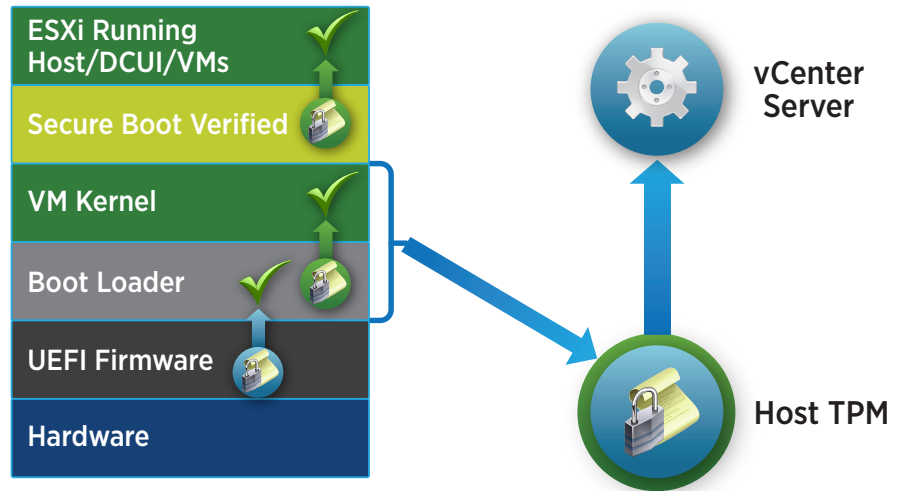
## vSphere 6.7 Security

vSphere 6.7 security goals are twofold: introduce more easy-to-use security features and meet requirements set by customers' IT and information security (InfoSec) teams. We have achieved both goals with vSphere 6.7.

The following sections discuss some of the new features and changes.

### TPM 2.0 Support for ESXi Hosts

A Trusted Platform Module (TPM) is a device on a laptop, desktop, or server system that is used to store encrypted data such as keys, credentials, and hash values. TPM 1.2 support has been available for many years on ESXi hosts, but it was primarily used by partners. TPM 2.0 is not backward compatible with TPM 1.2 and therefore required all new device drivers and API development. The Trusted Computing Group has an excellent [overview of what a TPM is and does](#).



**Figure 22.** Using TPM 2.0 to Secure an ESXi Host

Use of TPM 2.0 by ESXi hosts builds upon our work in vSphere 6.5 with Secure Boot. In brief, we validate that the system has booted with Secure Boot enabled, and we take measurements and store them in the TPM. The vCenter Server instance reads those measurements and compares them with values reported by the ESXi host itself. If the values match, the host has booted with Secure Boot enabled and the essentials such as running only signed code and the inability to install unsigned code are ensured. The vCenter Server system provides an attestation report in the vSphere Client, showing the status of each host.

### Virtual TPM 2.0 for VMs

To support TPMs for VMs, VMware engineers created a virtualized TPM 2.0 device. It appears in Windows as a normal TPM 2.0 device. Like a physical TPM, it can do cryptographic operations and store credentials. To secure data stored in the vTPM, write that data to the VM's NVRAM file and secure that file with VM Encryption. This keeps the data in the vTPM secured, and it "travels" with the VM. If a VM is copied to another data center, and if that data center is not configured to communicate with the user's key management system (KMS), the data in that vTPM is secured. All the same VM Encryption rules apply.

*NOTE: Only VM "home" files are encrypted. VMDKs are not encrypted unless the user chooses to encrypt them.*

A hardware TPM has many limitations: It's a serial device, so it's slow. It has a secured NVRAM storage size measured in **bytes**. It's not designed for accommodating 100 or more VMs on a host. It cannot store all their TPM data on the physical TPM and requires a scheduler for the cryptographic operations it performs. To illustrate this point, one need only consider 100 VMs attempting to encrypt something while depending on a serial device that can process only one at a time.



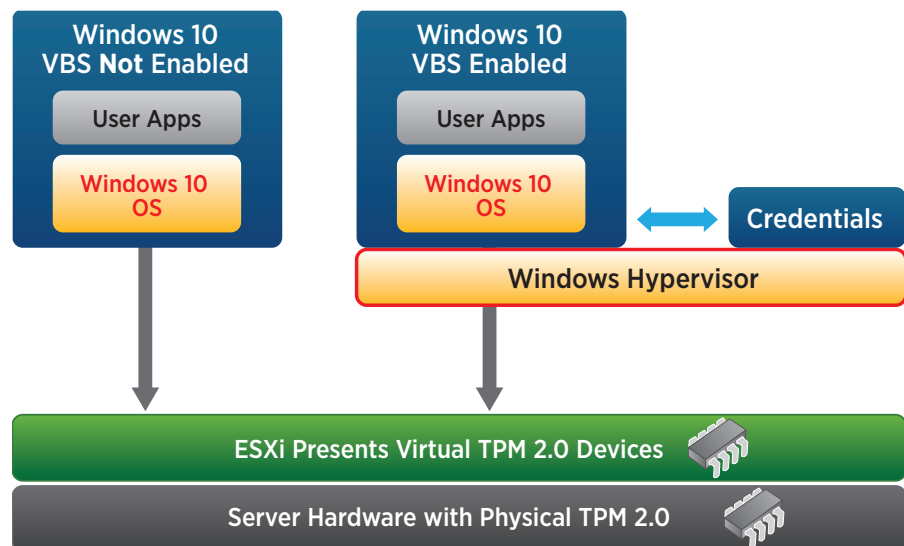
Even if the data can be physically stored, consider a vSphere vMotion migration. Data would have to be securely removed from one physical TPM and copied to another, and it would have to be re-signed with the new TPM's keys. All of these actions are very slow in practice and are fraught with additional security issues and requirements.

*NOTE: To run virtual TPMs, VM Encryption is necessary, so a third-party key management infrastructure must be in place. See the [list of supported key management systems](#) and a [blog on KMS topology](#).*

### Support for Microsoft Virtualization-Based Security

InfoSec teams frequently request or demand Windows Defender Credential Guard support. In 2015, Microsoft introduced virtualization-based security (VBS). We have worked very closely with Microsoft to provide support for these features in vSphere 6.7.

When VBS is enabled on a laptop running Windows 10, the system reboots. Rather than booting Windows 10 directly, the system boots the Microsoft hypervisor. In the case of vSphere systems, the VM that was running Windows 10 directly is now running the Microsoft hypervisor, which is now running Windows 10. This is called "nested virtualization." VMware has considerable experience with this and has been using it in VMware Hands-on Labs for years.



**Figure 23.** Supporting Virtualization-Based Security with vSphere 6.7

A single checkbox enables support for VBS along with the following vSphere features:

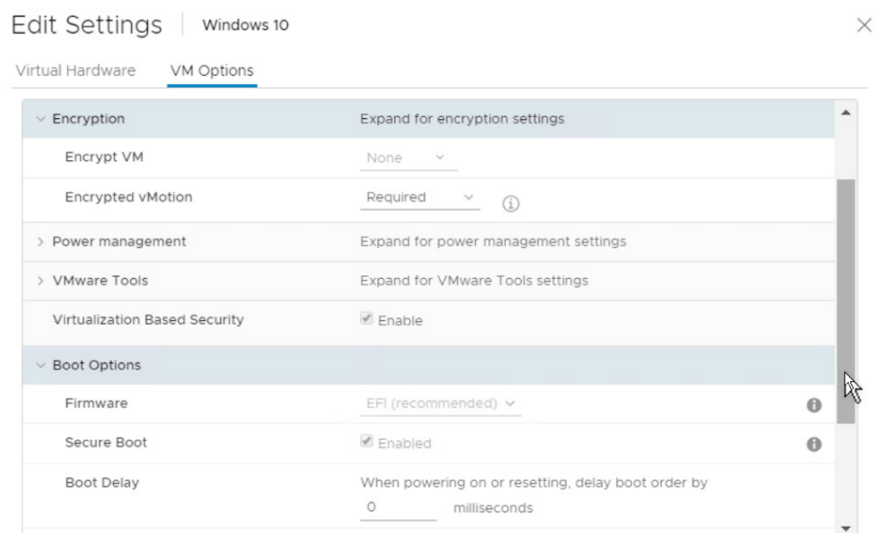
- Nested virtualization
- Input-output memory management unit (IOMMU)
- EFI firmware
- Secure Boot

This will **not** enable VBS within the VM's guest OS. To accomplish that goal, follow Microsoft guidance. This can be done with Windows PowerShell scripts, group policies, and so on. The role of the vSphere system is to provide the virtual hardware to support enablement of VBS. Combined with a vTPM, users can now enable VBS and turn on features such as Windows Defender Credential Guard.

***NOTE:** To build Windows 10 or Windows Server 2016 VMs today, we recommend building them with EFI firmware enabled. Moving from traditional BIOS/MBR to EFI (UEFI) firmware after the fact introduces some challenges later.*

## UI Updates

In vSphere 6.7, we have made a number of advances in the functionality of the vSphere Client. It's fast, well laid out, and complete for most laboratory tasks. We have made some changes to make things easier for administrators on a VM Encryption level. In the background, we still leverage storage policies, but we have combined all encryption functions—that is, VM Encryption and Encrypted vMotion—into one panel in **VM Options**. This creates a more logical workflow.



**Figure 24.** UI Enhancements for VM Encryption and Encrypted vMotion

### Multiple Syslog Targets

Customers have requested UI capability to configure multiple syslog targets when they want their syslog stream to go to two places—for example, to IT and teams. IT personnel have responded very favorably to VMware vRealize Log Insight™. InfoSec teams typically use security incident and event management systems that have specialized functions geared directly toward security operations. Now both can send an unfiltered stream of syslog events to their respective targets. The VAMI UI now supports up to three different syslog targets.

### FIPS 140-2 Validated Cryptographic Modules by Default

Within vSphere (vCenter Server and ESXi) systems, two modules are used for cryptographic operations. The VMware Kernel Cryptographic Module is used by the VM Encryption and Encrypted vSAN features; the OpenSSL module is used for functions such as certificate generation and TLS connections. These two modules have passed FIPS 140-2 validation.

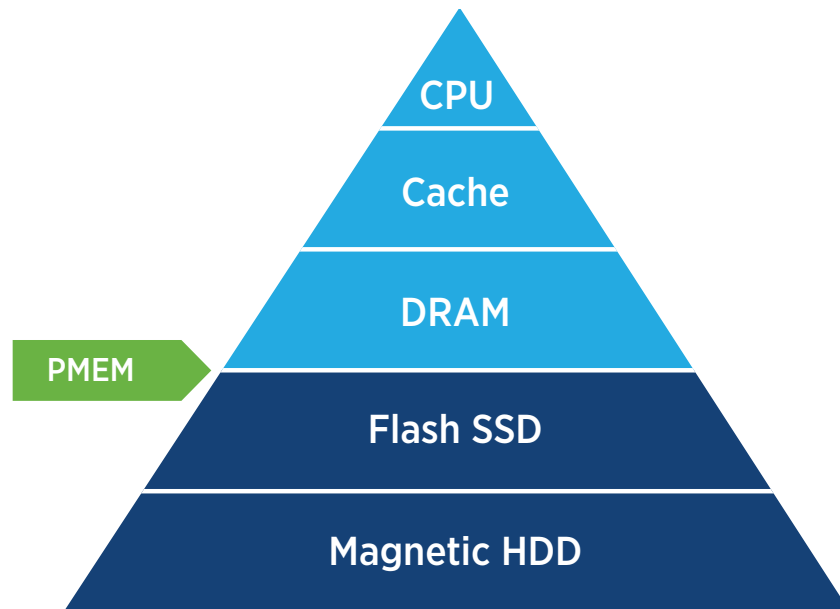
Customers have asked whether vSphere is “FIPS Certified.” FIPS Certified applies to a full solution of hardware and software that is tested and configured together. VMware has made it much easier for our partners to certify vSphere systems for FIPS operations. Cryptographic operations in vSphere systems are performed using the highest standards because all FIPS 140-2 cryptographic operations are enabled by **default**.

## vSphere 6.7 for Enterprise Applications

vSphere 6.7 introduces new storage and networking features that have a major impact on the performance of enterprise applications. These include support for persistent memory (PMEM) and enhanced support for RDMA.

### Persistent Memory

With vSphere persistent memory, enterprises using supported hardware servers can get the benefits of ultra-high-speed storage at a price point closer to DRAM-like speeds at Flash-like prices. Figure 25 shows the convergence of memory and storage.



**Figure 25.** Persistent Memory Between Flash SSD and DRAM in Performance and Price

Technology at the top of the pyramid, comprising DRAM and the CPU cache and registers, have the shortest latency—that is, the best performance—but this comes at a higher cost relative to the items at the bottom of the pyramid. All of these components are accessed directly by the application, also known as load access or storage access.

Technology at the bottom of the pyramid, comprising magnetic media (HDDs and tape) and NAND flash (SSDs and PCIe Workload Accelerators), have longer latency and lower costs relative to the technology at the top of the pyramid. These technology components have block access, so data is typically communicated in blocks of data and the applications are not accessed directly.

PMEM is a new layer called NVM and sits between NAND Flash and DRAM, providing not only faster performance relative to NAND Flash but also the nonvolatility not typically found in traditional memory offerings. This technology layer provides the performance of memory with the persistence of traditional storage.

Enterprise applications can be deployed in VMs that are exposed to PMEM datastores. PMEM datastores are created from NVM storage attached locally to each server. Performance benefits can then be attained as follows:

- vSphere systems can allocate a piece of the PMEM datastore and present it to the VM as a virtual disk, which is used as ultrafast virtual storage. In this mode, no guest OS or application change is required.

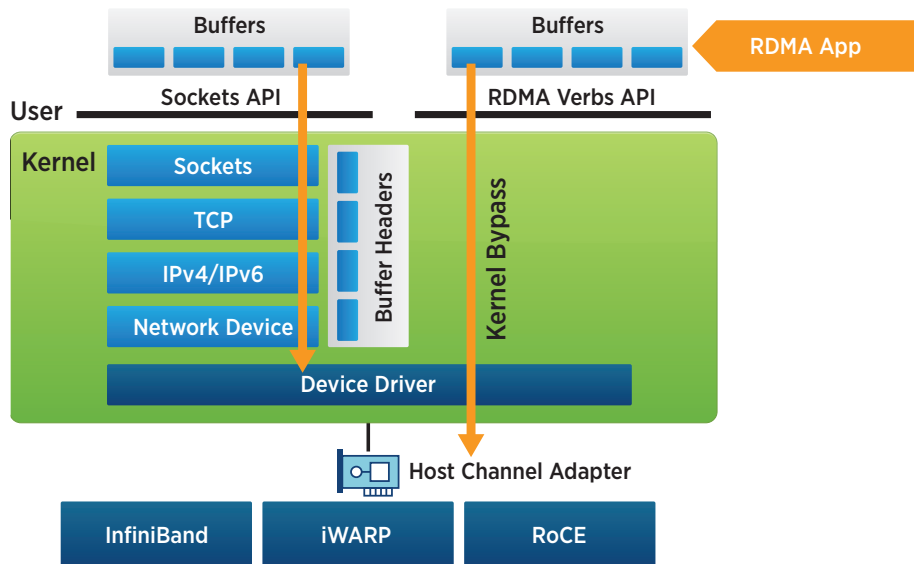
- vSphere systems can allocate a piece of the PMEM datastore in a server and present it to a VM as a virtual NVDIMM. This type of virtual device exposes a byte-addressable persistent memory to the VM.
  - Virtual NVDIMM is compatible with the latest guest OSs that support persistent memory. Applications do not change and they experience faster file access because the modified OS file system bypasses the buffer cache.
  - Applications can be modified to leverage PMEM and experience the highest increase in performance via direct and uninterrupted access to hardware.

Applications deployed on PMEM-backed datastores can benefit from vSphere vMotion live migration and vSphere DRS capability. This is not possible with PMEM in physical deployments.

## Remote Directory Memory Access

vSphere 6.7 introduces new protocol support for Remote Directory Memory Access (RDMA) over Converged Ethernet (RoCE—pronounced “rocky”—v2), a new software Fibre Channel over Ethernet (FCoE) adapter, and iSCSI Extension for RDMA (iSER). These features enable enterprises to integrate with even more high-performance storage systems, providing greater flexibility to use the hardware that best complements their workloads.

RDMA support is enhanced with vSphere 6.7 to bring even more performance to enterprise workloads by leveraging kernel and OS bypass, reducing latency and dependencies. Figure 26 illustrates this.



**Figure 26.** RDMA Leveraging Kernel Bypass to Improve Performance

When VMs are configured with RDMA in a pass-through mode, the workload is basically tied to a physical host with no vSphere DRS capability—that is, without vSphere vMotion migration capability. However, customers who want to harness the power of vSphere vMotion migration and vSphere DRS capability while still getting the benefits of RDMA, albeit at a very small performance penalty, can do so with paravirtualized RDMA software (PVRDMA). With PVRDMA, applications can run even in the absence of a host channel adapter (HCA) card. RDMA-based applications can be run in ESXi guests while ensuring that VMs can be live migrated.

Use cases for this technology include distributed databases, financial applications, and High Performance Computing.

## Conclusion

VMware vSphere 6.7 is the efficient and secure platform for the hybrid cloud. It provides a powerful, flexible, and secure foundation for business agility that accelerates the digital transformation to the hybrid cloud as well as success in the digital economy. vSphere 6.7 supports both existing and next-generation workloads through its 1) simple and efficient management at scale, to elevate the customer experience to an entirely new level; 2) comprehensive built-in security that starts at the core, via an operationally simple, policy-driven model; 3) universal application platform that supports new workloads and leverages hardware innovations for enhanced performance; and 4) seamless hybrid cloud experience with easy visibility, migration, and management of workloads between on-premises data centers and the public cloud. With vSphere 6.7, customers can now run, manage, connect, and secure their applications in a common operating environment, across their hybrid cloud.

## Resources

To learn more about VMware vSphere 6.7, see the following resources:

- [vSphere 6.7 New Features Deep Dive Blog Posts](#)
- [vSphere 6.7 Product Page](#)
- [Press Release](#)

## About the Authors

Emad Younis is a staff technical marketing architect in the Cloud Platform business unit. His current focus is on VMware vCenter Server and VMware Cloud on AWS. Find him on Twitter [@emad\\_younis](#).

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. He has been with VMware since 2005. His current focus is on VMware vSphere lifecycle management. Find him on Twitter [@eric\\_gray](#).

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](#).

Sudhir Balasubramanian is a staff solution architect specializing in all Oracle technologies on the VMware SDDC stack. Find him on Twitter [@vracdba](#).



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 [www.vmware.com](http://www.vmware.com)

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMW-WP-vSPHR-6.7-USLET-101