What's New in the VMware vSphere® 6.0 Platform

VERSION 1.1/TECHNICAL WHITE PAPER

MARCH 2015

Table of Contents

Introduction

VMware vSphere® 6.0 introduces many enhancements to VMware vSphere Hypervisor, VMware virtual machines, VMware vCenter Server™, virtual storage, and virtual networking. This paper will discuss these improvements that further extend the core capabilities of the vSphere platform.

vSphere Hypervisor Enhancements

Scalability Improvements

VMware ESXi™ 6.0 has dramatically increased the scalability of the platform. With vSphere Hypervisor 6.0, clusters can scale to as many as 64 hosts, up from 32 in previous releases. With 64 hosts in a cluster, vSphere 6.0 can support 8,000 virtual machines in a single cluster. This enables greater consolidation ratios, more efficient use of VMware vSphere Distributed Resource Scheduler™ (vSphere DRS), and fewer clusters that must be separately managed.

Each vSphere Hypervisor 6.0 instance can support as many as 480 logical CPUs, 12TB of RAM, and 1,024 virtual machines. By leveraging the newest hardware advances, ESXi 6.0 enables the virtualization of applications that were once thought to be nonvirtualizable.

ESXi Security Enhancements

Account Management

ESXi 6.0 enables management of local accounts on the ESXi server, using new ESXCLI commands. The ability to add, list, remove, and modify accounts across all hosts in a cluster can be centrally managed using a vCenter Server system. Previously, the account and permission management functionality for ESXi hosts was available only with direct host connections. Setting, removing, and listing local permissions on ESXi servers can also be centrally managed.

Account Lockout

There are two new settings available in ESXi **Host Advanced System Settings** for the management of local account failed login attempts and account lockout duration. These parameters affect SSH and vSphere Web Services connections but not DCUI and console shell access.

Password Complexity Rules

In previous versions of ESXi, password complexity changes had to be made by hand-editing the `/etc/pam.d/passwd file` on each ESXi host. In vSphere 6.0, this has been moved to an entry in **Host Advanced System Settings**, enabling centrally managed setting changes for all hosts in a cluster.

Improved Auditability of ESXi Administrator Actions

Prior to vSphere 6.0, actions at the vCenter Server level by a named user appeared in ESXi logs with the “vpxuser” username—for example, [user=vpxuser].

In vSphere 6.0, all actions at the vCenter Server level against an ESXi server appear in the ESXi logs with the vCenter Server username—for example, [user=vpxuser:DOMAIN\User].

This provides a better audit trail of actions that were run on a vCenter Server instance that conducted corresponding tasks on the ESXi hosts.

Flexible Lockdown Modes

Prior to vSphere 6.0, there was one lockdown mode. Feedback from customers indicated that this lockdown mode was inflexible in some use cases. With vSphere 6.0, the introduction of two lockdown modes aims to improve that.

The first mode is “normal lockdown mode.” The DCUI access is not stopped, and users on the “DCUI.Access” list can access DCUI.

The second mode is "strict lockdown mode." In this mode, DCUI is stopped.

There is also a new functionality called "exception users." These are local accounts or Microsoft Active Directory accounts with permissions defined locally on the host where these users have host access. These exception users are not recommended for general user accounts but are recommended for use by third-party applications—"Service Accounts," for example—that need host access when either normal or strict lockdown mode is enabled. Permissions on these accounts should be set to the bare minimum required for the application to perform its task and with an account that needs only read-only permissions to the ESXi host.

Smart Card Authentication to DCUI

This functionality is for U.S. federal customers only. It enables DCUI login access using a Common Access Card (CAC) and Personal Identity Verification (PIV). An ESXi host must be part of an Active Directory domain.

NVIDIA GRID Support

NVIDIA GRID™ delivers a graphics experience that is equivalent to dedicated hardware when using VMware Horizon®. Horizon with NVIDIA GRID vGPU™ enables geographically dispersed organizations to run graphics-intensive applications with 3D at scale.

Horizon with GRID vGPU

Using GRID vGPU technology, the graphics commands of each virtual machine are passed directly to the GPU, without translation by the hypervisor. This enables the GPU hardware to be time sliced, to deliver the ultimate in shared virtualized graphics performance.

GRID vGPU offers the most flexibility of any solution, enabling deployment of virtual machines across a wide range of users and graphics applications, including Microsoft PowerPoint slides and YouTube videos, to the most-demanding engineer using intensive 3D CAD software.

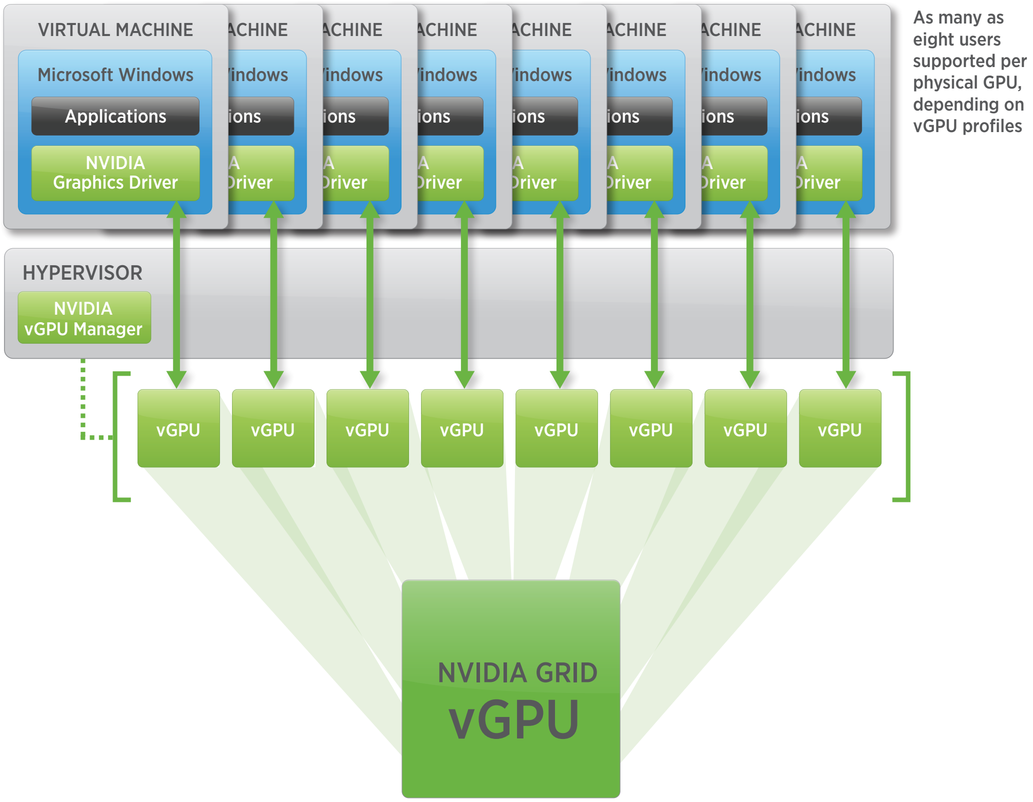
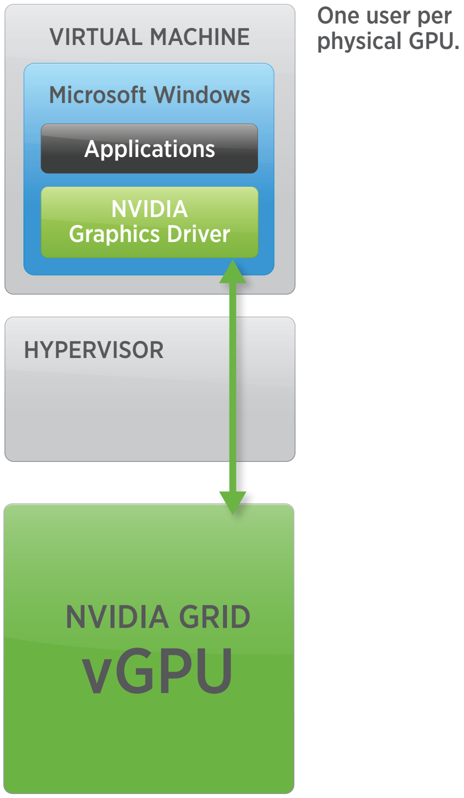


Figure 1. NVIDIA GRID Support

Horizon with GRID vDGA

NVIDIA GRID with Horizon Virtual Dedicated Graphics Acceleration (vDGA) is ideal for 3D graphics–intensive applications. vDGA is highly recommended for dedicated one-to-one GPU mapping and workstation-equivalent performance without the need for a workstation. This enables designers, engineers, and architects to work remotely.



One user per physical GPU.

Figure 2. Horizon with NVIDIA GRID vDGA

Virtual Machine Enhancements

Virtual Machine Compatibility Level with ESXi 6.0

vSphere 6.0 introduces a new virtual machine compatibility level with several new features such as support for 128 vCPUs and 4TB of RAM, hot-add RAM enhancements to vNUMA, WDDM 1.1 GDI acceleration, a USB 3.0 xHCI controller, and several serial and parallel port enhancements.

Table 1 summarizes the virtual machine compatibility levels supported in vSphere 6.0.

vSPHERE RELEASE	VIRTUAL MACHINE HARDWARE VERSION	vSPHERE COMPATIBILITY
vSphere 4.0	Version 7	VMware ESX®/ESXi 4.0 and later
vSphere 4.1	Version 7	VMware ESX/ESXi 4.0 and later
vSphere 5.0	Version 8	VMware ESXi 5.0 and later
vSphere 5.1	Version 9	VMware ESXi 5.1 and later
vSphere 5.5	Version 10	VMware ESXi 5.5 and later
vSphere 6.0	Version 11	VMware ESXi 6.0 and later

Table 1. Virtual Machine Compatibility Levels

vNUMA Enhancements

When a vNUMA virtual machine with the hot-add memory option is enabled and memory is hot-added to it, that memory is now allocated equally across all NUMA regions. In previous releases, all new memory was allocated only to region 0. This enhancement ensures that all regions benefit from the increase in RAM, enabling the virtual machine to scale without requiring any downtime.

Serial and Parallel Port Enhancements

Serial and parallel ports can now be removed from a virtual machine when using compatibility 6 (vHW 11). In addition, the maximum number of serial ports has been increased to 32. Security-conscious organizations like the ability to control all aspects of the hardware that the applications are running on. With vSphere 6.0, they can remove unused serial and parallel ports. Point-of-sale systems often require a large number of serial devices. With vSphere 6.0, each virtual machine can contain as many as 32 serial ports, enabling virtualization of more point-of-sale systems.

Expanded Guest OS Support

vSphere 6.0 introduces support for the following guest operating systems (OSs):

- Oracle Unbreakable Enterprise Kernel Release 3 Quarterly Update 3
- Asianux 4 SP4
- Solaris 11.2
- Ubuntu 12.04.5
- Ubuntu 14.04.1
- Oracle Linux 7
- FreeBSD 9.3
- Mac OS X 10.10

A full list of supported guest OSs can be found at
http://www.vmware.com/resources/compatibility/search.php?deviceCategory=guestos.

Windows Server Failover Clustering Enhancements

Support for workloads that must be protected using Windows Server Failover Clustering (WSFC) has been improved. In addition to the currently supported platforms, Microsoft Windows Server 2012 R2 and Microsoft SQL Server 2012 have been added. This includes support for both WSFC and AlwaysOn Availability Groups.

vSphere 6.0 introduces support for the PVSCSI adapter with virtual machines running WSFC. This provides performance superior to that with the standard SCSI adapter. This enhancement helps deliver the storage I/O needed for the most-demanding applications.

VMware vSphere vMotion® is now fully supported with Windows Server 2008 and later when using WSFC virtual machines that are clustered across physical hosts using physical-mode RDMs. There is no need to fail over applications to another host during vSphere maintenance activities, enabling higher levels of manageability and availability. vSphere DRS is also fully supported for use with WSFC, ensuring best placement for virtual machines on vSphere hosts and delivering best application performance.

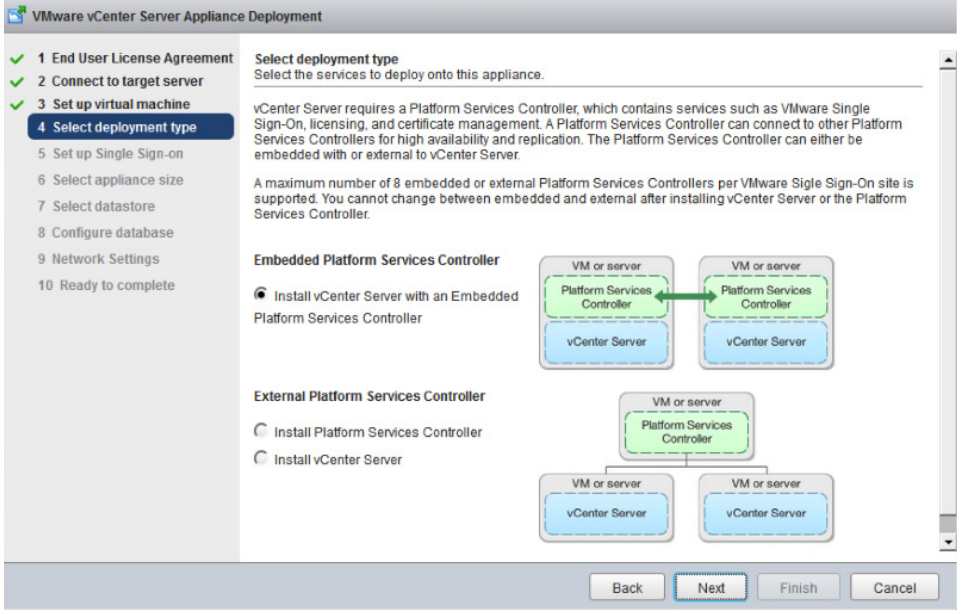
vCenter Server Enhancements

vCenter Server Architecture Changes

vCenter Server 6.0 simplifies planning and deployment by offering two deployment models. The first, embedded, deploys the new Platform Services Controller (PSC) and the vCenter Server system on the same machine. The second, external, deploys the PSC and the vCenter Server instance on separate machines.

All vCenter Server services—such as VMware vCenter™ Inventory Service, VMware vSphere Web Client, auto deploy, and so on—are installed along with vCenter Server. There are no longer separate installers for these components, simplifying the architecture by combining functions onto a single machine. VMware vSphere Update Manager™ remains as a standalone Microsoft Windows installation.

Both deployment models support use of an embedded PostgreSQL database. For external database use, Windows vCenter Server deployments support SQL Server and Oracle Database; VMware vCenter Server Appliance™ supports Oracle Database.



Select deployment type
Select the services to deploy onto this appliance.

vCenter Server requires a Platform Services Controller, which contains services such as VMware Single Sign-On, licensing, and certificate management. A Platform Services Controller can connect to other Platform Services Controllers for high availability and replication. The Platform Services Controller can either be embedded with or external to vCenter Server.

A maximum number of 8 embedded or external Platform Services Controllers per VMware Sigle Sign-On site is supported. You cannot change between embedded and external after installing vCenter Server or the Platform Services Controller.

Embedded Platform Services Controller

● Install vCenter Server with an Embedded Platform Services Controller

External Platform Services Controller

○ Install Platform Services Controller

○ Install vCenter Server

Figure 3. VMware vCenter Server Appliance Deployment

Platform Services Controller

The PSC includes common services used across VMware vCloud Suite®. This includes VMware vCenter Single Sign-On™, licensing, and certificate management.

PSCs replicate information such as licenses, roles and permissions, and tags with other PSCs.

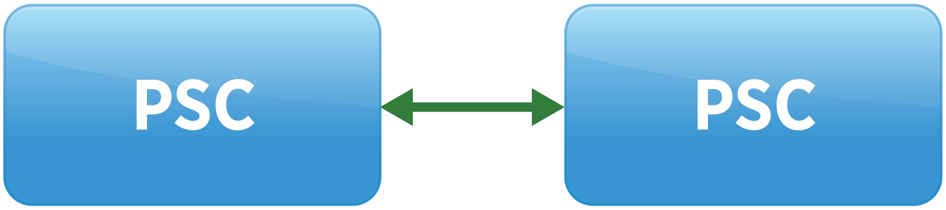


Figure 4. Replicated Information Between Platform Services Controllers

Enhanced Linked Mode

Because PSCs replicate all the information traditionally required for linked mode, linked mode is now automatically enabled for any vCenter Server deployment. This is true when using a Windows install, vCenter Server Appliance, or a mix of the two, as long as all vCenter Server instances are joined to the same vCenter Single Sign-On domain. This eliminates extra configuration steps traditionally required to establish linked mode and enables vCenter Server Appliance to now utilize it.

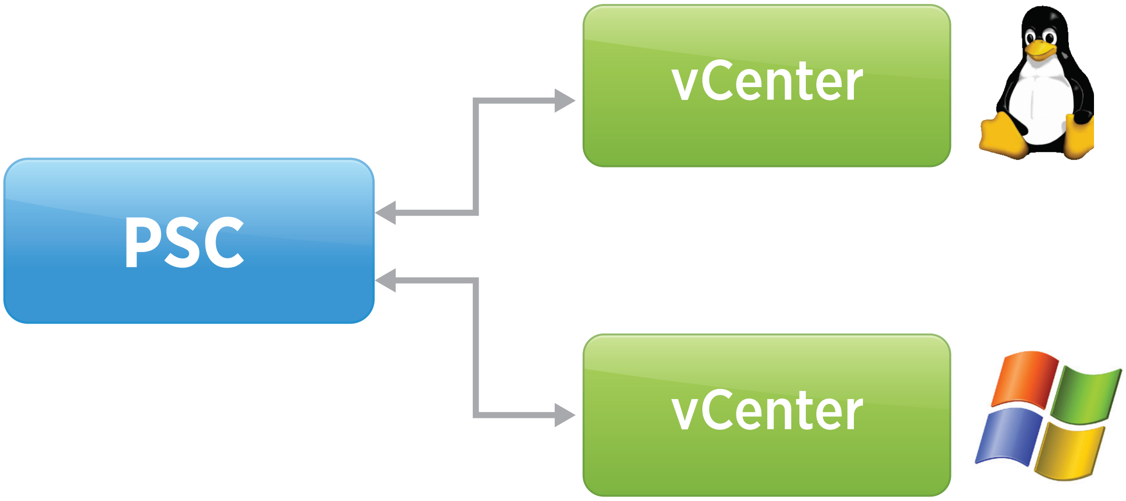


Figure 5. Enhanced Linked Mode

Certificate Management

In vSphere 6.0, “solution users”—the users created when a solution such as vCenter Server, vCenter Inventory Service, and so on, is registered with vCenter Single Sign-On—are utilized as certificate endpoints. These users are issued certificates instead of individual services. This enables the services associated with a solution user to utilize the same certificate, substantially reducing the number of certificates required to manage in the environment.

The PSC contains the VMware Certificate Authority (VMCA). The VMCA is a root certificate authority (CA) that issues signed certificates to all vSphere 6.0 components via the solution users. This secures the environment by using a CA to generate certificates as opposed to using self-signed certificates as in previous releases.

The VMCA can also be configured as a subordinate CA, enabling it to issue certificates based on an existing enterprise CA. Organizations that have an investment in a CA can easily incorporate the VMCA into their existing infrastructure.

vCenter Server Appliance

vCenter Server Appliance now has the same scalability numbers as the Windows installable vCenter Server: 1,000 hosts and 10,000 virtual machines. This is supported with the embedded PostgreSQL database or an external Oracle Database. This enables organizations to choose the platform that is best for them without sacrificing vCenter Server performance.

METRIC	WINDOWS	APPLIANCE
Hosts per vCenter Server System	1,000	1,000
Powered-on Virtual Machines per vCenter Server System	10,000	10,000
Hosts per Cluster	64	64
Virtual Machines per Cluster	8,000	8,000
Linked Mode	✓	✓

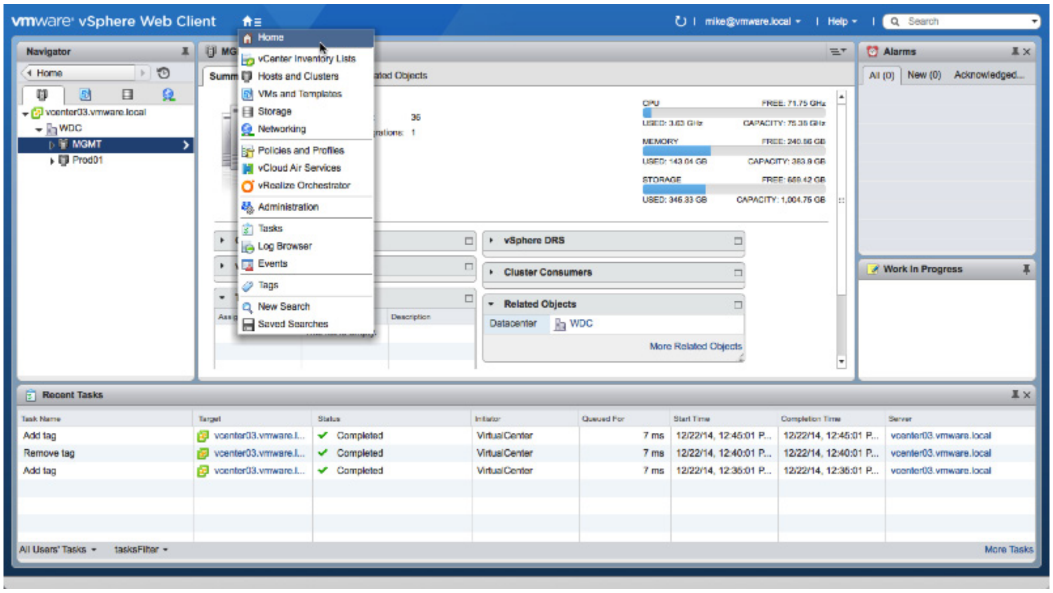
Table 2. vCenter Server Platform Scalability Numbers

vSphere Web Client

vSphere Web Client includes significant performance and usability improvements.

The performance improvements include login times that are up to 13 times faster, right-click menus that are visible and usable four times faster, and other actions that are now at least 50 percent faster. This puts vSphere Web Client on a par with the standalone VMware vSphere Client™.

The usability improvements include a new drop-down menu that enables users to navigate to any area of vSphere Web Client regardless of which area they currently are operating in. The right-click menu has also been flattened, which enables right-click operations to be consistent across the UI. The task pane has been relocated to the bottom of the screen, making it easier to view **Recent Tasks**, which update in real time. The UI is also dockable, enabling administrators to customize their UI.



Recent Tasks

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Server
Add tag	vcenter03.vmware.l...	✓ Completed	VirtualCenter	7 ms	12/22/14, 12:45:01 P...	12/22/14, 12:45:01 P...	vcenter03.vmware.local
Remove tag	vcenter03.vmware.l...	✓ Completed	VirtualCenter	7 ms	12/22/14, 12:40:01 P...	12/22/14, 12:40:01 P...	vcenter03.vmware.local
Add tag	vcenter03.vmware.l...	✓ Completed	VirtualCenter	7 ms	12/22/14, 12:35:01 P...	12/22/14, 12:35:01 P...	vcenter03.vmware.local

Figure 6. vSphere Web Client – Usability Improvements

vSphere vMotion

vSphere vMotion capabilities have been enhanced in this release, enabling users to perform live migration of virtual machines across virtual switches, vCenter Server systems, and long distances of up to 150ms RTT.

These new vSphere vMotion enhancements enable greater flexibility when designing vSphere architectures that were previously restricted to a single vCenter Server system due to scalability limits and multisite or metro design constraints. Because vCenter Server scale limits no longer are a boundary for pools of compute resources, much larger vSphere environments are now possible.

vSphere administrators now can migrate across vCenter Server systems, enabling migration from a Windows version of vCenter Server to vCenter Server Appliance or vice versa, depending on specific requirements. Previously, this was difficult and caused a disruption to virtual machine management. It can now be accomplished seamlessly without losing historical data about the virtual machine.

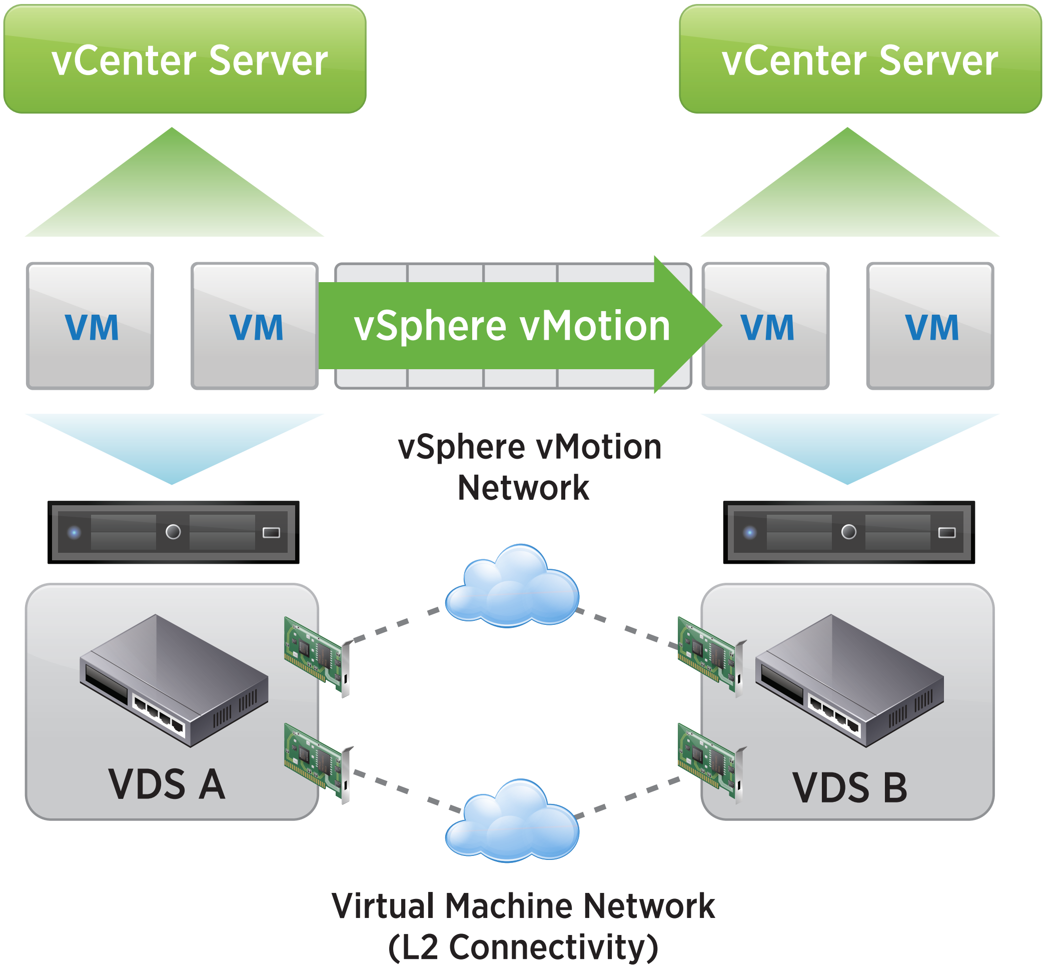


Figure 7. VMware vSphere vMotion Enhanced Capabilities

When a virtual machine is migrated across vCenter Server instances, its data and settings are preserved. This includes the virtual machine UUID, event, alarm, task history, as well as resource settings including shares, reservations, and limits. VMware vSphere High Availability (vSphere HA) and vSphere DRS settings are also retained, including affinity and antiaffinity rules, automation level, start-up priority, and host isolation response. This maintains a seamless experience as the virtual machine moves throughout the infrastructure.

MAC addresses are also preserved as they are moved across vCenter Server instances. When a virtual machine is moved out of a vCenter Server instance, the MAC address is added to an internal blacklist to ensure that a duplicate MAC is not generated.

Increasing the latency thresholds for vSphere vMotion enables migration across larger geographic spans, targeting intracontinental distances. This feature plays a key role for data center migrations, disaster avoidance scenarios, and multisite load balancing.

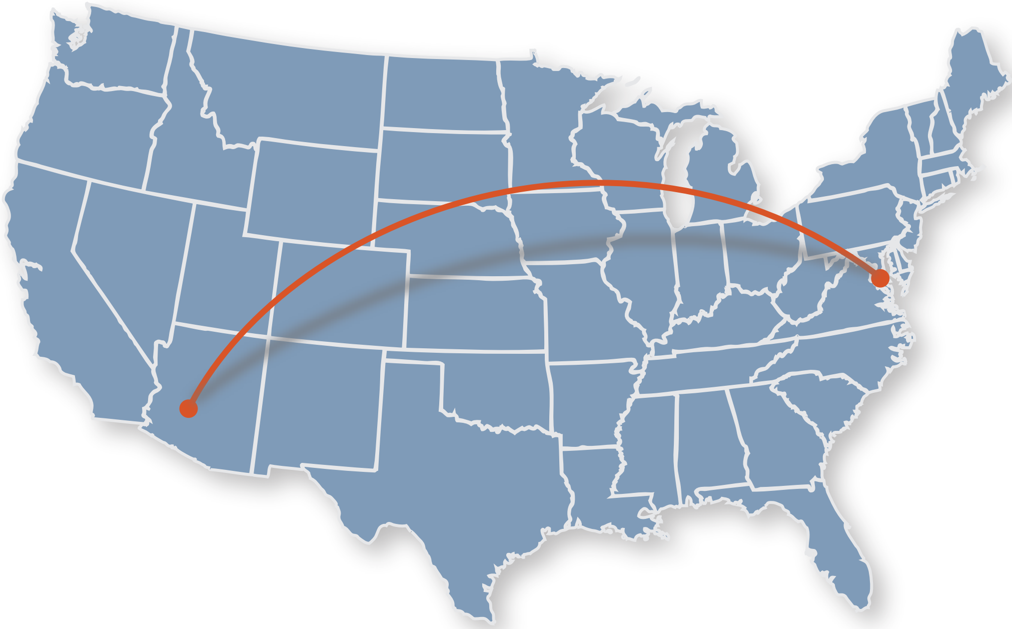


Figure 8. Enabling vSphere vMotion Migration Across Longer Distances

With these dynamic new vSphere vMotion features, vSphere administrators now can simultaneously change the compute resource, storage resource, virtual machine network, and vCenter Server instance without disrupting applications that reside on the virtual machine, enabling a wide array of new design opportunities.

VMware vSphere Fault Tolerance Enhancements

VMware vSphere Fault Tolerance (vSphere FT) provides continuous availability for applications in the event of physical server failures by creating a live shadow instance of a virtual machine that is always up to date with the primary virtual machine. In the event of a hardware outage, vSphere FT automatically triggers failover, ensuring zero downtime and preventing data loss. vSphere FT is easy to set up and configure and does not require any OS-specific or application-specific agents or configuration. It is tightly integrated with vSphere and is managed using vSphere Web Client.

Previous versions of vSphere FT supported only a single vCPU. Through the use of a completely new fast-checkpointing technology, vSphere FT now supports protection of virtual machines with up to four vCPUs and 64GB of memory. This means that the vast majority of mission-critical customer workloads can now be protected regardless of application or OS.

VMware vSphere Storage APIs – VMware vSphere Data Protection™ can now be used with virtual machines protected by vSphere FT. An in-guest agent is required to back up the previous version of vSphere FT. vSphere FT 6.0 empowers vSphere administrators to use VMware Snapshot–based tools to back up virtual machines protected by vSphere FT, enabling easier backup administration, enhanced data protection, and reduced risk.

There have also been enhancements in how vSphere FT handles storage. It now creates a complete copy of the entire virtual machine, resulting in total protection for virtual machine storage in addition to compute and memory. It also increases the options for storage by enabling the files of the primary and secondary virtual machines to be stored on shared as well as local storage. This results in increased protection, reduced risk, and improved flexibility.

In addition, improvements have been made to vSphere FT virtual disk support and host compatibility requirements. Prior versions required a very specific virtual disk type: eager-zeroed thick. They also had very limiting host compatibility requirements. vSphere FT now supports all virtual disk formats: eager-zeroed thick, thick, and thin. Host compatibility for vSphere FT is now the same as for vSphere vMotion. This makes it much easier to use vSphere FT.

vSphere High Availability Enhancements

vSphere HA delivers the availability required by most applications running in virtual machines, independent of the OS and application running in it. It provides uniform, cost-effective failover protection against hardware and OS outages within a virtualized IT environment. It does this by monitoring vSphere hosts and virtual machines to detect hardware and guest OS failures. It restarts virtual machines on other vSphere hosts in the cluster without manual intervention when a server outage is detected, and it reduces application downtime by automatically restarting virtual machines upon detection of an OS failure.

With the growth in size and complexity of vSphere environments, the ability to prevent and recover from storage issues is more important than ever. vSphere HA now includes Virtual Machine Component Protection (VMCP), which provides enhanced protection from All Paths Down (APD) and Permanent Device Loss (PDL) conditions for block (FC, iSCSI, FCoE) and file storage (NFS).

Prior to vSphere 6.0, vSphere HA could not detect APD conditions and had limited ability to detect and remediate PDL conditions. When those conditions occurred, applications were impacted or unavailable longer and administrators had to help resolve the issue. vSphere VMCP detects APD and PDL conditions on connected storage, generates vCenter alarms, and automatically restarts impacted virtual machines on fully functional hosts. By doing this, it greatly improves the availability of virtual machines and applications without requiring more effort from administrators.

vSphere HA can now protect as many as 64 ESXi hosts and 8,000 virtual machines—up from 32 and 4,000—which greatly increases the scale of vSphere HA supported environments. It also is fully compatible with VMware Virtual Volumes, VMware vSphere Network I/O Control, IPv6, VMware NSX™, and cross vCenter Server vSphere vMotion. vSphere HA can now be used in more and larger environments and with less concern for feature compatibility.

Multisite Content Library

The Content Library simplifies virtual machine template management and distribution for organizations that have several vCenter Server systems across geographic locations. It centrally manages virtual machine templates, ISO images, and scripts, and it performs the content delivery of associated data from the published catalog to the subscribed catalog at other sites.

As content is updated within the published catalog, the changes automatically are distributed to all subscribed catalogs at other sites. This feature guarantees that all sites have access to the approved standard templates across an entire organization. As content is updated, old versions are automatically purged and replaced with the newest version, offering life cycle management capabilities for virtual machine templates and related files.

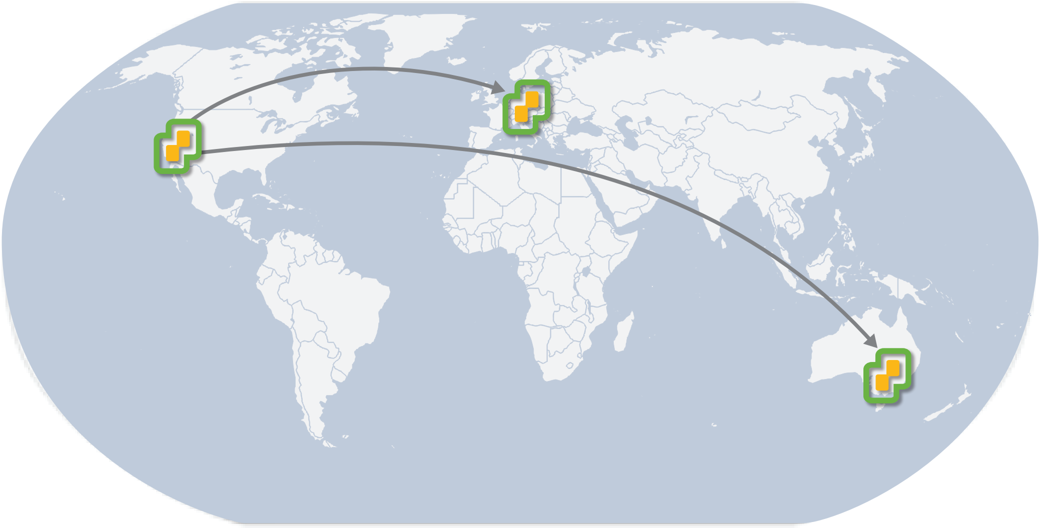


Figure 9. Multisite Content Library Access Capabilities

This “store once, share many” architecture reduces the time associated with distributing templates manually, enabling more time to be spent performing more-important administrative tasks.

Additionally, the number of simultaneous transfers and the consumed bandwidth are configurable to prevent the saturation of WAN connections in bandwidth-constrained environments. Synchronization tasks can be scheduled to be performed during nonpeak hours when more bandwidth is available for content replication.

vSphere Storage Enhancements

Virtual Volumes

Virtual Volumes is a new virtual machine disk management and integration framework that enables array-based operations at the virtual disk level. It transforms the data plane of SAN and NAS storage systems by aligning storage consumption and operations with virtual machines. In other words, Virtual Volumes makes SAN and NAS storage systems capable of being managed at a virtual machine level and enables the leveraging of array-based data services and storage array capabilities with a virtual machine–centric approach at the granularity of a single virtual disk.

Virtual Volumes implements a significantly different and improved storage architecture, enabling operations to be conducted at the virtual machine level using native array capabilities. With Virtual Volumes, most data operations are offloaded to the storage arrays.

Virtual Volumes eliminates the need to provision and manage large numbers of LUNs or volumes per host. This reduces operational overhead while enabling scalable data services on a per–virtual machine level.

Storage Policy–Based Management (SPBM) is a key technology that works in conjunction with Virtual Volumes. This framework delivers an orchestration and automation engine that translates the storage requirements expressed in a virtual machine storage policy into virtual machine granular provisioning capabilities with dynamic resource allocation and management of storage-related services.

Through the integration of VMware vSphere API for Storage Awareness™, storage array capabilities are pushed through the vSphere stack and are surfaced in the vCenter Server management interface. Using virtual machine storage policies, vSphere administrators can specify a set of storage requirements and capabilities for any particular virtual machine to match service levels required by hosted applications. SPBM leverages Virtual Volumes to recommend compliant datastores for virtual machine placement and to transparently turn on the necessary data services based on native array capabilities. Through SPBM, virtual machine tailored data services are executed by the array. Coupled with Virtual Volumes, SPBM ensures policy compliance throughout the virtual machine life cycle.

vSphere Data Protection Enhancements

vSphere Data Protection is a backup and recovery solution for VMware virtual machines. It is fully integrated with vCenter Server and vSphere Web Client, providing easy, disk-based backup and recovery for VMware virtualized environments. All functionality previously available with VMware vSphere Data Protection Advanced™ has been consolidated into vSphere Data Protection 6.0.

vSphere Data Protection features industry-leading EMC® Avamar® variable-length segment deduplication to minimize backup data storage consumption. vSphere Data Protection virtual appliances can be deployed with up to 8TB of deduplicated backup data capacity. Changed block tracking (CBT) is utilized for backup and restore to reduce time and network bandwidth requirements.

vSphere Data Protection now includes agents that enable application-consistent backup and reliable recovery of Microsoft SQL Server, Microsoft Exchange Server, and Microsoft SharePoint Server, including SQL Server clusters and Exchange Server database availability groups. Individual databases can be selected for backup and restore, and it is possible to restore individual Exchange Server mailboxes.

Secure, efficient replication of backup data between vSphere Data Protection virtual appliances provides an easy, reliable method to move backup data offsite for disaster recovery. Replicated backup data can be restored at the target location or replicated back to the source location for restore. This functionality provides several retention and recovery options to satisfy a wide variety of business requirements.

The best way to ensure backup data integrity is to perform regular “practice” restores. This important activity is seldom performed in many organizations. vSphere Data Protection now includes automated backup verification—scheduled jobs that routinely restore virtual machines, boot the guest OSs, check for VMware Tools™ heartbeats to verify that the virtual machines have been recovered successfully, and then delete the restored virtual machines.

vSphere Data Protection features support for storing backup data on EMC Data Domain®, providing increased reliability and backup data capacity. EMC DD Boost™ is utilized to minimize network bandwidth impact and improve performance.

External proxies are now available with vSphere Data Protection. They can be deployed to remote locations such as other vSphere clusters within the same site or across sites to help minimize network bandwidth requirements. External proxies also enable support for as many as 24 concurrent backup streams and for Red Hat Enterprise Linux Logical Volume Manager (LVM) and the Ext4 file system.

vSphere Data Protection 6.0 is included with vSphere Essentials Plus Kit 6.0 and later editions of vSphere, all VMware vSphere with Operations Management™ 6.0 editions, and all vCloud Suite 6.0 editions.

VMware vSphere Replication Enhancements

VMware vSphere Replication™, the VMware proprietary replication engine, provides data protection and disaster recovery for the vSphere platform by replicating virtual machines within the same site and across sites. It is tightly integrated with vSphere and is managed using vSphere Web Client. It is included with vSphere Essentials Plus Kit and later editions of vSphere. Multiple points in time recovery can be enabled to provide as many as 24 recovery points for a replicated virtual machine. vSphere Replication is used as a standalone solution and as a replication engine for VMware vCenter Site Recovery Manager™ and VMware vCloud® Air™ Disaster Recovery.

The recovery point objective (RPO) can be set on a per–virtual machine basis and can range from 15 minutes to 24 hours. After initial synchronization between the source and the target locations, only changes to the virtual machines are replicated, enabling vSphere Replication to minimize network bandwidth consumption. New to vSphere Replication in vSphere 6.0 to further improve efficiency is the option to compress replicated data as it is sent across the network.

It is now possible to easily isolate network traffic associated with vSphere Replication. This enables vSphere administrators to control bandwidth by configuring more than one network interface card in a vSphere Replication virtual appliance and by using vSphere Network I/O Control to separate network traffic. The result is improved performance and security.

Enhancements have been made to the way vSphere Replication performs a full synchronization. Previous versions of vSphere Replication requested and compared remote checksums with local checksums to determine the regions of a virtual disk that had to be replicated. With some storage platforms and vSphere 6.0, vSphere Replication can query vSphere for storage allocation information, to reduce the amount of time and network bandwidth required to perform a full synchronization.

vSphere Replication is fully compatible with VMware vSphere Storage vMotion® at both the source and target locations. Prior to vSphere 6.0, moving a replica at the target location required vSphere Replication to perform a full synchronization. With vSphere 6.0, migrating a replica with vSphere Storage vMotion no longer requires this. That makes it much easier to balance storage utilization with vSphere Storage vMotion and VMware vSphere Storage DRS™ while avoiding RPO violations.

Improvements have also been made to VMware Tools for Linux virtual machines. With some Linux OSs, VMware Tools features the ability to quiesce the guest OS during replication and backup operations. vSphere Replication can utilize this new functionality to enable file system–consistent recovery of Linux virtual machines.

vSphere Networking Enhancements

vSphere Network I/O Control Enhancements

vSphere Network I/O Control Version 3 enables administrators or service providers to reserve—that is, guarantee—bandwidth to a vNIC in a virtual machine or an entire distributed port group. This ensures that other virtual machines or tenants in a multitenancy environment do not impact the SLA of other virtual machines or tenants sharing the same upstream links—that is, bandwidth.

vSphere Multiple TCP/IP Stacks

vSphere 6.0 introduces multiple TCP/IP stacks, which can be assigned to separate vSphere services. Each stack operates with its own

- Memory heap
- ARP table
- Routing table
- Default gateway

This enables finer control of network resource usage—for example, operations such as vSphere vMotion can operate over a layer 3 boundary; NFC operations such as cloning can be sent over a dedicated network rather than sharing the management network.

About the Authors

Mike Brown is a senior technical marketing manager in the VMware Cloud Infrastructure Technical Marketing group. Mike has worked in the IT industry for more than 17 years. His focus is on reference architectures for VMware vCloud Suite and the software-defined data center (SDDC) as well as VMware vCenter Server, vCenter Single Sign-On, VMware vSphere Web Client, and resource management technologies such as vSphere Distributed Resource Scheduler, vSphere Network I/O Control, vSphere Storage DRS, and VMware vSphere Storage I/O Control. Mike has multiple industry certifications, including VMware Certified Design Expert (VCDX).

Follow Mike on Twitter @vMikeBrown.

GS Khalsa is a senior technical marketing manager in the VMware Storage and Availability Technical Marketing group. GS has worked in the IT industry for more than 13 years. Prior to VMware, he spent time as both a customer and a VMware partner. His focus is on VMware availability solutions such as VMware vSphere High Availability, vSphere Fault Tolerance, and VMware vCenter Site Recovery Manager.

Follow GS on the vSphere Uptime blog and on Twitter @gurusimran.

Jeff Hunter is a senior technical marketing architect at VMware with a focus on availability solutions. Jeff has been with VMware for 7 years. Previously, he spent several years in systems engineering roles, expanding the virtual infrastructures at a regional bank and at a Fortune 500 insurance company.

Matthew Meyer is a senior technical marketing architect working on software-defined data center technologies and specializing in VMware vSphere cloud platform products and services. Matthew previously was an architect in the VMware Cloud Infrastructure and Management Professional Services organization, where he consulted on projects for VMware Fortune 100 clients. Matthew holds many industry certifications, including VMware Certified Design Expert (VCDX#69).

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