



VMware vSphere 5 Competitive Reviewer's Guide

VMware vSphere 5

REVIEWER'S GUIDE

Table of Contents

Getting Started	3
About This Guide	3
Intended Audience	3
Requirements	3
Help and Support During the Review	3
Key New Features in vSphere 5	4
Infrastructure Services (Compute, Storage and Network)	4
Application Services (Availability, Security and Scalability)	5
Management Services	5
VMware vSphere 5 Compared to the Competition	6
ESXi Hypervisor (new/updated features)	6
Large Virtual Machines for Tier 1 Application Support (new/updated features) ..	9
Small Business Bundles (new/updated features)	9
vShield Security (new/updated features)	11
Resource and Performance Controls (new/updated features)	13
Networking Features	17
Storage Features (new/updated features)	18
Business Continuity Features (new/updated features)	21
Management and Provisioning Features (new/updated features)	24
Top 20 vSphere 5 Advantages Over the Competition	28

Getting Started

About This Guide

The purpose of this guide is to support a hands-on comparison of VMware® vSphere™ 5 to competing virtualization products such as Microsoft Hyper-V, Citrix XenServer, or Red Hat Enterprise Virtualization (KVM). This guide can also be used by reviewers without hands-on access to a live vSphere installation. You will find the key VMware competitive advantages called out in the “VMware Differentiators” section associated with each feature described in this guide.

Intended Audience

This guide is designed for press reviewers, technology analysts, and IT professionals who are comparing VMware vSphere 5 to other virtualization products for the purposes of writing reviews or making product selection decisions. This guide points out and describes important differentiating features in vSphere 5 that are missing from competing products.

Requirements

This guide should be used in conjunction with the vSphere 5 Evaluators Guide. The Evaluators Guide provides detailed step-by-step guidance needed to configure and use key features of vSphere 5 in a realistic environment. The Evaluators Guide recommends that vSphere 5 be configured with a minimum of three hosts and a Storage Area Network (SAN) to enable its key features.

Ensure that vSphere 5 is installed on hardware that has been validated against the VMware Hardware Compatibility List (HCL). Also install VMware vCenter™ Server and vSphere Client in the evaluation environment to manage the VMware vSphere hosts. Virtual machines used for the evaluation should be pre-configured and installed with properly licensed Guest Operating Systems.

For detailed information regarding installation, configuration, administration, and usage of VMware vSphere 5, please refer to the online documentation: <http://www.vmware.com/support/pubs/>.

The vSphere 5 evaluation license available from the VMware evaluation portal provides Enterprise Plus functionality for 60 days and is the best choice for performing a vSphere 5.0 competitive review.

Help and Support During the Review

This guide provides a high-level overview of the unique features of VMware vSphere 5 that differentiate it from competing products. It is not meant to substitute for product documentation. Please refer to the online product documentation for vSphere for more detailed information (see below for links). You may also consult the online Knowledge Base if you have any additional questions. Press and analyst reviewers that require further assistance may contact the VMware Public Relations team (PRinquiries@vmware.com) to be placed in contact with technical resources at VMware. Customers that require further assistance should contact a VMware sales representative or channel partner.

VMware vSphere and vCenter Resources:

- vSphere 5 Evaluators Guide
<http://www.vmware.com/tryvmware/?p=vmware-vsphere5-ent>
- Product Documentation:
<http://www.vmware.com/support/pubs/>
- Online Support:
<http://www.vmware.com/support/>
- Support Offerings:
<http://www.vmware.com/support/services>
- Education Services:
<http://mylearn1.vmware.com/mgrreg/index.cfm>
- Support Knowledge Base:
<http://kb.vmware.com>

- VMware vSphere Management Assistant—VMware Command-Line Interface Documentation
<http://www.vmware.com/support/developer/vcli/>
- PowerCLI Toolkit Community:
<http://communities.vmware.com/community/vmtn/vsphere/automationtools/powercli>
(or type Get-VIToolkitCommunity within PowerCLI)
- PowerCLI Blogs:
<http://blogs.vmware.com/vipowershell>

VMware Contact Information

For customers seeking additional information or to purchase VMware vSphere, VMware's global network of solutions providers is ready to assist. If you would like to contact VMware directly, you can reach a sales representative at 1-877-4VMWARE (650-475-5345 outside North America) or email sales@vmware.com. When emailing, please include the state, country and company name from which you are inquiring. You can also visit <http://www.vmware.com/vmwarestore/>.

Press and analyst reviewers conducting comparative reviews of VMware vSphere and competing virtualization products should contact the VMware Public Relations team (PRinquiries@vmware.com). The VMware PR team can arrange access to special technical support resources.

Providing Feedback

We appreciate your feedback on the material included in this guide. In particular, we would be grateful for any guidance on the following topics:

- How useful was the information in this guide?
- What other specific topics would you like to see covered?
- Overall, how would you rate this guide?

Please send your feedback to the following address: tmdocfeedback@vmware.com, with "VMware vSphere 5 Competitive Reviewer's Guide" in the subject line. Thank you for your help in making this guide a valuable resource.

Key New Features in vSphere 5

Customers, as well as press and analyst reviewers, should be sure to use the new vSphere 5 release to experience the latest enhancements offered by VMware. vSphere 5 enables users to run business-critical applications with confidence and respond to business needs faster. vSphere 5 accelerates the shift to cloud computing for existing datacenters and underpins compatible public cloud offerings, forming the foundation for the industry's only hybrid cloud model.

Infrastructure Services (Compute, Storage and Network)

Compute

- **vSphere ESXi convergence**—vSphere 5 is converging on the ESXi hypervisor architecture. ESXi—the gold standard in hypervisors— enables vSphere users to leverage a thinner architecture, a more secure footprint, and a streamlined patching and setup model. For more information visit the ESXi and ESX info center at <http://www.vmware.com/products/vsphere/esxi-and-esx/overview.html>.
- **vSphere Auto Deploy**—Auto Deploy is a new deployment and patching model for new vSphere hosts running the ESXi hypervisor. Deploy more vSphere hosts in minutes and update them more efficiently than ever before.
- **New virtual-machine format (Version 8)**—The new virtual machine format in vSphere 5 has several new features, including support for
 - 3D graphics for Windows Aero
 - USB 3.0 devices
- **Support for Apple products**—vSphere 5 supports Apple Xserve servers running OS X Server 10.6 (Snow Leopard) as a guest operating system.

Storage

- **vSphere Storage DRS**—Improve management and enable more-efficient use of storage resources through grouping, placement and balancing.
- **Profile-Driven Storage**—Identify the appropriate storage to use for a given virtual machine depending on service level. The result is a streamlined approach to selecting the correct storage and ensuring its delivery.
- **vSphere File System**—Leverage enhanced scalability and performance through a non-disruptive upgrade to the platform's latest clustered file system version.
- **vSphere Storage I/O Control**—Improve management and enforcement of service-level agreements (SLAs) through extension of limits and shares in Network File System (NFS) datastores.
- **vSphere Storage API Program**—Take advantage of extensions to the Array Integration API that support thin provisioning. Leverage the new Storage Awareness and Discovery API to interface with arrays when using the new vSphere Storage DRS and Profile-Driven Storage features.

Application Services (Availability, Security and Scalability)

Availability

- **vSphere High Availability**—New architecture enables superior guarantees, simplified setup and configuration, and expanded scalability.
- **vSphere vMotion**—Migration of virtual machines over higher latency network links is now supported.

Security

- **ESXi Firewall**—New service-oriented and stateless firewall engine restricts access to specific services by IP address or subnet. This is particularly useful for third-party components that require network access.

Scalability

- **Larger virtual machines**—Virtual machines can now grow four times larger than in any previous release to support even the largest applications. Virtual machines can now have up to 32 virtual CPUs and 1TB of RAM.

Management Services

Core Management

- **vSphere Web Client**—Access vSphere from any Web browser anywhere in the world.
- **VMware vCenter Server Appliance**—Run vCenter Server as a Linux-based virtual appliance.

VMware vSphere 5 Compared to the Competition

In the comparison tables of this section, new/updated vSphere 5 features are shown in bold font.

ESXi Hypervisor (new/updated features)

Feature Description

VMware ESXi—the industry's first x86 “bare-metal” hypervisor—is the most reliable and robust hypervisor. Launched in 2001 and now in its fifth generation, VMware ESXi has been production-proven in tens of thousands of customer deployments all over the world.

The purpose-built, thin ESXi hypervisor at the core of vSphere is the base software layer on each host and it is designed for the sole purpose of virtualization. With vSphere 5, VMware has completed its transition to the truly thin ESXi architecture, which completely eliminates any reliance on a general-purpose operating system. Competing hypervisors treat virtualization as an add-on to a general-purpose operating system “parent partition.” This mixed architecture introduces reliability concerns as the parent OS has a much larger attack surface and becomes a single point of failure. The far thinner VMware ESXi hypervisor architecture removes dependence on a general-purpose OS in the virtualization layer and requires no patching or maintenance to secure generic operating system code that has nothing to do with virtualization.

VMware ESXi Differentiators

Small ESXi Code Footprint

As shown in Figure 1 below, the code footprint differences between VMware ESXi 5 and other hypervisors are dramatic. Citrix XenServer 5.6 and the Linux operating system it requires measures over 1GB. KVM installations require a Linux installation and are similarly sized. A typical Microsoft Windows Server 2008 R2 Hyper-V installation has a nearly 10GB footprint and the more stripped-down Windows server Core still requires 3.4GB. Those differences represent millions of lines of code, each of which increases the chances of bugs and vulnerabilities. None of the vendors of those products have announced any plans to remove dependence on general-purpose operating systems and approach the truly thin design of VMware ESXi.

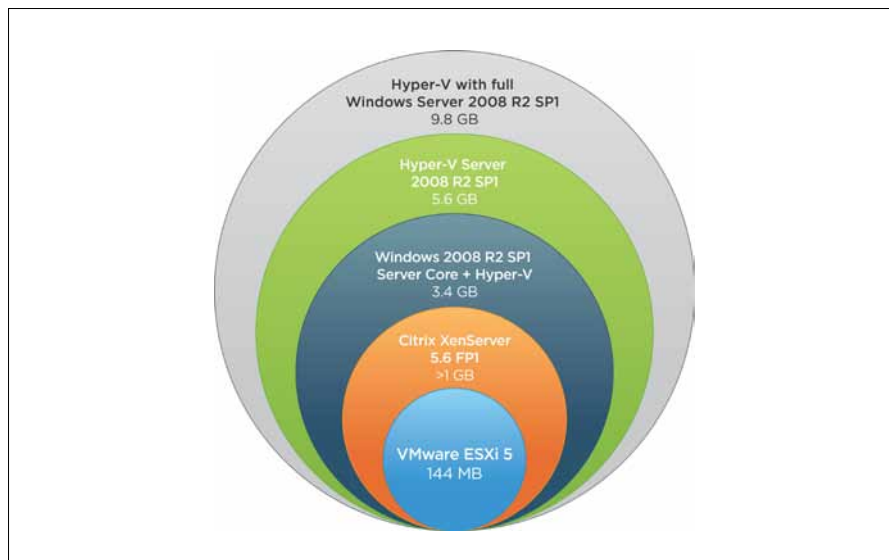


Figure 1. Comparative hypervisor disk footprints

Another benefit of the reduced code footprint of ESXi is the reduction in patching requirements. Applying patches on data center servers requires arranging for production downtime windows and administrator overtime. Patching interruptions are even more disruptive for virtualized hosts running many server applications. Hypervisor hosts dependent on a general-purpose operating system must be patched even for issues that are unrelated to virtualization. As Table 1 shows, Microsoft Hyper-V users must patch and reboot their hosts most months, even though those patches rarely relate to Hyper-V.

Microsoft Hyper-V Systems Require Frequent Patching

	MAY 2010	JUNE 2010	JULY 2010	AUG 2010	SEPT 2010	OCT 2010	NOV 2010	DEC 2010	JAN 2011	FEB 2011	MAR 2011	APR 2011
"Important" and "Critical" Server Core Patches	1	5	1	8	4	6	0	9	1	7	2	8
# of Patches Related to Virtualization Functionality	0	0	0	0	0	0	0	1	0	0	0	0
Reboot Required?	No	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes

Table 1.

ESXi Direct Driver Architecture

The VMware ESXi I/O architecture has important differences from the approach taken by Hyper-V and Xen, as shown in Figure 2. ESXi uses a direct driver model that locates the device drivers that link virtual machines to physical devices directly in the ESXi hypervisor. Hyper-V and Xen have an indirect driver design that routes virtual machine I/O through device drivers in the Windows or Linux management operating systems. The ESXi direct driver design utilizes certified and hardened I/O drivers that must pass rigorous testing and optimization steps performed jointly by VMware and the hardware vendors before they are certified for use with VMware vSphere. With the drivers in the hypervisor, VMware ESXi can provide them with special treatment, in the form of CPU scheduling and memory resources, that they need to process I/O loads from multiple virtual machines. Conversely, the Xen and Microsoft architectures rely on routing all virtual machine I/O to generic drivers installed in the Linux or Windows OS in the hypervisor's management partition. These generic drivers can be overtaxed by the activity of multiple virtual machines. Windows Server 2008 R2 with Hyper-V and Xen-based products both use generic drivers that are not optimized for many virtual machine workloads that are running concurrently. Considering that, "device driver failures are responsible for about 85 percent of crashes on Windows machines," (according to [Technology Review](#)) the Hyper-V indirect driver design puts its virtual machines at risk from the least reliable component of Windows.

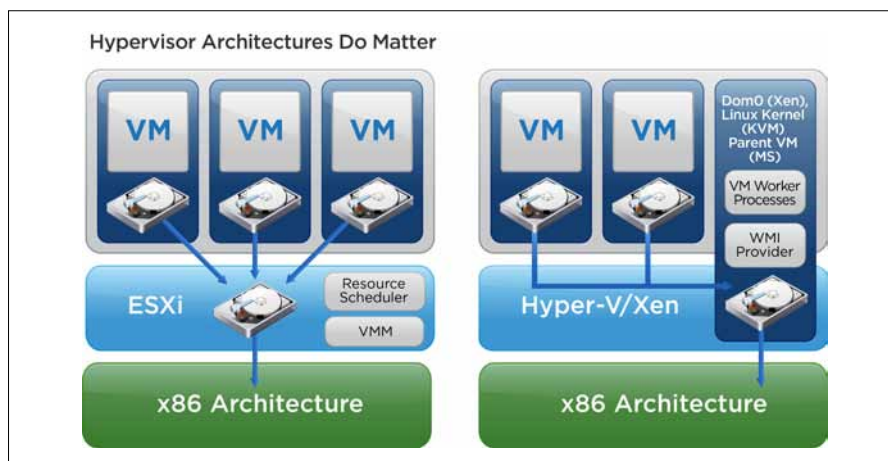


Figure 2. VMware ESXi direct driver design compared to the indirect driver design of Hyper-V and Xen

ESXi Memory Management

Sophisticated and effective memory management has always been a key strength of the ESXi hypervisor that powers VMware vSphere. ESXi employs a multi-layered approach to memory management that delivers the most efficient memory usage, best VM densities and lowest costs to users. vSphere lets users provide critical VMs with guaranteed memory. The memory "Shares" and "Reservation" settings prioritize memory allocated to each VM and ensure enough host RAM is reserved for the active working memory of each guest OS. ESXi efficiently reclaims memory from less busy virtual machines when needed by more active virtual machines using [four techniques](#): transparent page sharing; in-guest ballooning; memory compression; and, hypervisor-level swapping. Those technologies permit aggressive memory oversubscription with minimal performance impact using any supported ESXi guest operating system.

Citrix XenServer and Microsoft Hyper-V rely solely on in-guest ballooning – they call it "Dynamic Memory" – to reclaim memory and permit memory oversubscription. Development work at VMware and [independent testing](#) of Citrix XenServer 5.6 shown in Figure 3 and [independent testing of Microsoft Hyper-V R2 SP1](#) shown in Figure 4 demonstrate that ballooning alone cannot respond fast enough and provide enough memory savings to prevent performance slowdowns when memory is oversubscribed.

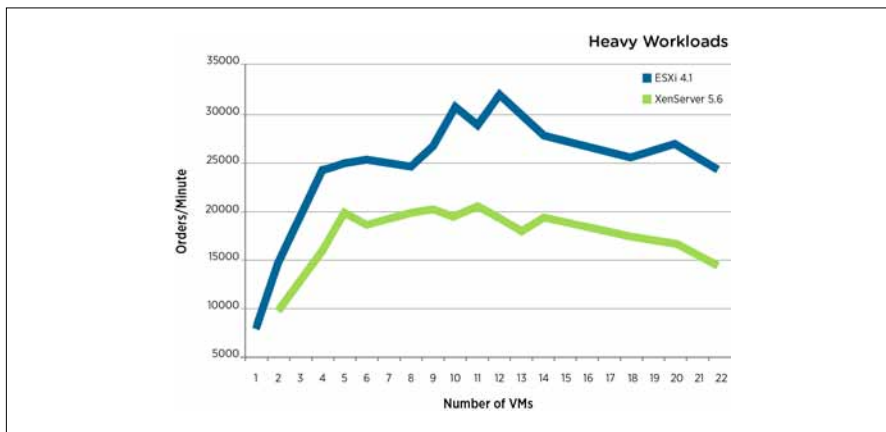


Figure 3. ESXi uses multiple memory management techniques for better performance than Citrix XenServer when memory is oversubscribed

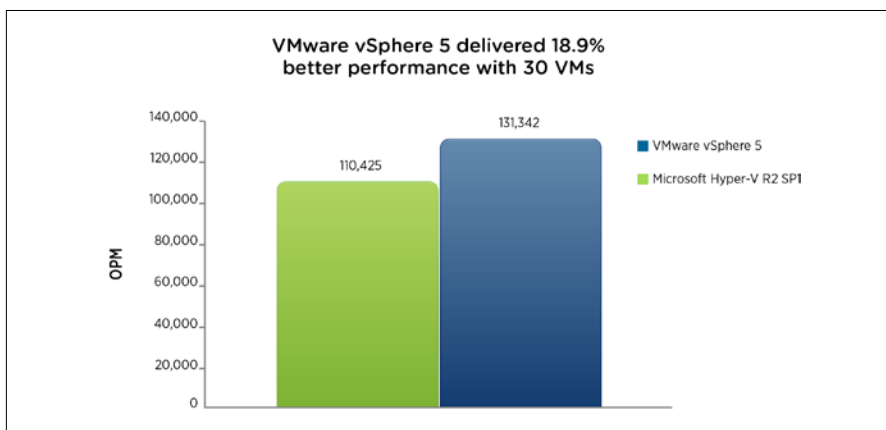


Figure 4. ESXi delivers 18.9% higher aggregate performance than Microsoft Hyper-V at high virtual machine densities

Microsoft's Dynamic Memory feature is incompatible with many Microsoft guest operating systems and applications and there is no support for non-Microsoft guests. To use Dynamic Memory, Microsoft recommends that Hyper-V virtual machines be configured with minimal memory and memory is hot added as their needs increase. Many applications and management tools are unable to use the hot added memory or are confused by varying memory configurations seen in virtual machines.

Hypervisor Feature/Function Comparison

HYPERVISOR DIFFERENTIATORS	VMWARE VSPHERE 5	MICROSOFT HYPER-V R2 SP1	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
Small footprint hypervisor	Yes, ESXi <144MB	No, 3.4-9.8GB	No, >1GB	No, full Linux OS needed
Direct driver I/O design	Yes, uses optimized drivers in ESXi hypervisor	No, uses generic Windows drivers in parent partition	No, uses generic Linux drivers in Domain 0	No, uses generic Linux drivers in host OS
Advanced memory management	Yes, uses four levels of memory saving technology for best VM density and performance, supports any guest OS	No, relies only on in-guest ballooning, limited guest OS support, guest memory artificially changed using hot-add RAM	No, relies only on in-guest ballooning	No, must manually reclaim memory from guests using ballooning

Large Virtual Machines for Tier 1 Application Support (new/updated features)

Feature Description

VMware vSphere 5 now supports virtual machines with four times the CPU and memory capacity of previous versions to customers can virtualize their largest Tier 1 workloads. vSphere 5.1 virtual machines can scale up to 32 virtual CPUs and 1TB of RAM to support the largest databases, email servers and scientific applications. vSphere 5 also provides the availability and disaster recovery features such large and mission-critical applications require.

Large Virtual Machine Feature/Function Comparison

LARGE VIRTUAL MACHINE DIFFERENTIATORS	VMWARE VSPHERE 5	MICROSOFT HYPER-V R2 SP1	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
Large scale processor configurations for virtual machines	Yes, up to 32-way virtual SMP, supported on any guest OS	No, limited to 4-way virtual machines, supported only on selected guest OSs	No, limited to 4-way virtual machines when managed by XenCenter	Partial, limited to 16-way virtual machines
Large scale memory configurations for virtual machines	Yes, up to 1TB RAM per virtual machine	No, only 64GB per virtual machine	No, maximum 32GB per virtual machine, some guest OSs limited to 4-16GB	No, only 256GB per virtual machine

Small Business Bundles (new/updated features)

Feature Description

Often overlooked in comparisons of vSphere with other virtualization products are the VMware product bundles designed for small and midsize businesses. The [VMware vSphere Essentials](#) and [vSphere Acceleration kits](#) provide complete solutions at very attractive price points and are responsible for the widespread adoption of vSphere as the preferred virtualization platform by small and midsize businesses. Starting as low as \$83 per processor, vSphere Essentials combines powerful vSphere virtualization features with vCenter management for up to three dual processor servers. vSphere Acceleration kits provide customers with the features found in higher-level vSphere editions for host clusters totaling six to eight processors.

The compelling features and pricing delivered by VMware vSphere Essentials and Acceleration kits have made VMware the market share leader in the small and midsize business segment – a position that many assumed would go to Microsoft because of their historical strengths there. In their most recent [Magic Quadrant for x86 Server Virtualization Infrastructure](#) report, Gartner states, “VMware seems to be winning at least 60% of new midmarket customers.”

Small Business Bundle Feature/Function Comparison

SMALL BUSINESS BUNDLE DIFFERENTIATORS	VMWARE VSPHERE 5 ESSENTIALS & ACCELERATION KITS	MICROSOFT HYPER-V R2 SP1 WITH SYSTEM CENTER ESSENTIALS 2010	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
Virtualization bundles designed for small and midsize businesses	Yes, 5 vSphere Essentials and Acceleration kits	No, limited to 4-way virtual machines, supported only on selected guest OSs	No SMB bundle offered	No SMB bundle offered
Limits on number of managed virtual machines	No	Yes, hard limit of 50 Windows virtual machines, SQL Server required if >15 virtual machines	N/A	N/A
Upgrades to higher-level editions	Yes, Essentials and Essentials Plus upgrades credit customers for purchase price when upgrading to higher Acceleration Kit editions	No, customers must purchase full System Center licenses, no credit offered for System Center Essentials purchase	N/A	N/A
Low-cost shared storage solution	Yes, vSphere Storage Appliance turns server disks into shared storage, extra cost option	No	No	No
Live migration and high availability	Yes, vMotion and HA included in Essentials Plus and above	Yes	N/A	N/A
Advanced memory management support	Yes, full support for vSphere multiple memory management technologies in all kits	No, System Center Essentials 2010 does not support Dynamic Memory	N/A	N/A

SMALL BUSINESS BUNDLE DIFFERENTIATORS	VMWARE VSPHERE 5 ESSENTIALS & ACCELERATION KITS	MICROSOFT HYPER-V R2 SP1 WITH SYSTEM CENTER ESSENTIALS 2010	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
Role-based security	Yes, full vCenter role-based access controls supported	No, requires full System Center Operations Manager	N/A	N/A
Virtual network configuration	Yes, vCenter	No, requires full System Center Virtual Machine Manager	N/A	N/A
Virtual machine import and cloning	Yes	No, requires full System Center Virtual Machine Manager	N/A	N/A

vShield Security (new/updated features)

Feature Description

The VMware vShield family provides adaptive and cost-effective security services within a single management framework for securing virtual datacenters and cloud environments at all levels —host, network, application, data and endpoint. The vShield products are built from the ground up to protect virtualized infrastructure more efficiently and economically than legacy physical approaches to security relied upon by vSphere competitors. vShield products enforce security at the ESXi hypervisor level and are managed by specialized virtual appliances to make security virtualization-aware. The vShield product family includes:

- **VMware vShield Zones:** Provides an application firewall with policies based on basic traffic information for basic protection from network threats, (included with vSphere Enterprise and Enterprise Plus, other vShield components are extra cost)
- **VMware vShield App:** Protects applications in the virtual datacenter against network-based threats
- **VMware vShield App with Data Security:** Adds to vShield App Sensitive Data Discovery across virtualized resources
- **VMware vShield Edge:** Enhances protection for the virtual datacenter perimeter
- **VMware vShield Endpoint:** Improves performance by offloading key antivirus and anti-malware functions to a security virtual machine, eliminating the antivirus agent footprint in virtual machines
- **VMware vShield Manager:** Security management framework included with all vShield products

VMware Security Differentiators

- VMware competitors lack purpose-built virtualization-aware security solutions like vShield. Microsoft Hyper-V, Citrix XenServer and Red Hat Enterprise Virtualization are limited to legacy security solutions based on physical appliances. Compared to that legacy approach, VMware vShield offers important advantages
- **Simpler management:** Physical approaches to security require separate hardware appliances, interfaces and sets of expertise to manage protection for networks, firewalls, load balancers and applications. vShield replaces that complexity with a centralized security management implemented in a single interface that eliminates the need for multiple point solutions.
- **Virtual rather than physical security appliances:** Hardware appliances used by legacy security solutions are expensive and limited in bandwidth and port capacity. vShield consolidates security operations onto a single virtual appliance that scales without the costs and constraints of physical implementations.

- **Hypervisor-based Layer 2 firewall:** Traditional methods for securing virtual machines in the same cluster use VLAN and port mapping rules to restrict communications. However, as virtual machines are added VLANs proliferate to the point where network switch ports are exhausted, and migration of virtual machines between hosts requires manual reconfiguration of security settings. vShield App avoids those limitations with a hypervisor-based firewall that protects networks at the virtual NIC level and is change-aware so security settings move with virtual machines as they migrate within a cluster.
- **Hypervisor-level introspection offloads antivirus protection:** Today's practice of deploying an antivirus agent on each virtual machine cannot cope with the demands of cloud computing. Too many simultaneous security scans create "AV storms" that saturate processors, memory and storage. vShield Endpoint uses an agentless approach where all virtual machines are inspected and protected concurrently at the ESXi hypervisor level to improve performance and scalability.
- **Adaptive trust zones eliminate need for air gapped servers:** Microsoft's [Hyper-V Security Guide](#) recommends users, "place virtual machines of a similar trust level on the same physical computer." Such "air gap" approaches weld virtual machines to hosts and defeat the benefits of virtual machine mobility and dynamic load balancing that are essential to cloud computing. vShield App turns security policies into logical constructs that move with virtual machines permitting adaptive trust zones that protect and isolate virtual machines even if they share the same hosts.
- **Automated, continuous compliance checking:** Traditional security tools require specialists in each of many regulatory protocols to manually ensure data governed by standards like PCI, SOX and HIPAA is properly protected. vShield App with Data Security automates the compliance process with over 80 regulatory templates that scan an entire vSphere infrastructure to ensure compliance and correct variances with simple one-click remediation. vShield App with Data Security makes staying in compliance with data protection regulations simpler and less costly.

Security Feature/Function Comparison

SECURITY DIFFERENTIATORS	VMWARE VSPHERE 5 WITH VSHIELD	MICROSOFT HYPER-V R2 SP1	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
Virtualization-aware application firewall	Yes, vShield Zones (included with vSphere Enterprise and Enterprise Plus) and vShield App*	No, requires legacy physical security tools	No, requires legacy physical security tools	No, requires legacy physical security tools
Hardware-free network security	Yes, vShield Edge* enforces security at the hypervisor level using a single virtual appliance	No, requires hardware firewall, VPN, DHCP, NAT and load-balancing appliances	No, requires hardware firewall, VPN, DHCP, NAT and load-balancing appliances	No, requires hardware firewall, VPN, DHCP, NAT and load-balancing appliances
Single pane of glass security management	Yes, with vShield Manager*	No, separate security tool management interfaces	No, separate security tool management interfaces	No, separate security tool management interfaces
Hypervisor-level introspection to secure virtual machines	Yes, vShield Endpoint* requires no guest agents	No, security agents needed in each virtual machine, AV storms	No, security agents needed in each virtual machine, AV storms	No, security agents needed in each virtual machine, AV storms

SECURITY DIFFERENTIATORS	VMWARE VSPHERE 5 WITH VSHIELD	MICROSOFT HYPER-V R2 SP1	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
Automated discovery and regulatory compliance for sensitive data	Yes, vShield App* with Data Protection	No	No	No
Adaptive trust zones – protection persists when virtual machines moved	Yes, vShield App* is virtualization-aware	No, must reconfigure security settings after virtual machines migrate	No, must reconfigure security settings after virtual machines migrate	No, must reconfigure security settings after virtual machines migrate
Logical security zones without air gaps	Yes, vShield App* security zones are logical constructs that can share hosts	No, traditional security approach requires zones isolated on air gapped hosts	No, traditional security approach requires zones isolated on air gapped hosts	No, traditional security approach requires zones isolated on air gapped hosts

*VMware vShield Zones is included with vSphere Enterprise and Enterprise Plus editions. vShield App, vShield Edge and vShield Endpoint are extra cost additions to VMware vSphere.

Resource and Performance Controls (new/updated features)

Keeping virtual machines isolated from “noisy neighbors” and providing them with resource guarantees to ensure they can meet service level commitments is essential to virtualization and cloud computing. VMware vSphere 5 combines unique technologies and automation features to keep virtual machines running with the resources they need even as datacenter workloads fluctuate.

Clusters and Resource Pools

Only vSphere supports true resource pools that are divisible and hierarchical. This means that the aggregated memory and CPU resources of an ESXi host cluster can be split into separate resource pools and each resource pool can be subdivided to create a hierarchical structure. Hyper-V, XenServer and Red Hat Enterprise Virtualization are missing these essential features—they can only create a single large resource pool incorporating all the CPU and memory across a host cluster. With vSphere resource pools, you can split a host cluster into multiple logical resource pools and assign each to different business units with assurance that they will be fully isolated. Additionally, each business unit can subdivide their resource pool into smaller units under their control.

Distributed Resource Scheduler

VMware Distributed Resource Scheduler (DRS) automatically load balances resource utilization across a cluster of ESXi hosts by using vMotion to migrate virtual machines from a heavily utilized ESXi host to a more lightly used ESXi host. VMware DRS analyzes the CPU and memory consumption of a virtual machine over time to determine whether to migrate it. DRS selects the best target host for a virtual machine to assure that resource guarantees are met and affinity and anti-affinity rules are honored (to keep virtual machines on the same hosts or different hosts.) vSphere 5 adds storage space and I/O capacity to the list of resources monitored when load balancing decisions are made (see below.)

Microsoft Hyper-V, Citrix XenServer, and Red Hat Enterprise Virtualization do not have anything similar to VMware DRS because they lack the concept of true resource pools. To enable workload balancing with Microsoft Hyper-V, users must leverage Microsoft PRO Tips, which in turn require System Center Operations Manager, an additional product loosely-integrated with System Center Virtual Machine Manager. With Microsoft PRO Tips, resources are monitored at the host level without coordination among nodes in the cluster, because PRO Tips lacks abstraction and aggregation capabilities. XenServer workload balancing requires complex installation of additional servers and lacks affinity rules. Red Hat's does load balancing feature also lack affinity rules and does not factor virtual machine memory usage into its decisions.

Distributed Power Management

VMware Distributed Power Management (DPM) monitors the CPU and memory resource utilization of a cluster and determines whether one or more ESXi hosts should be powered off or powered on in order to maintain a pre-defined resource utilization threshold. When cluster resource utilization is low DPM will power one or more ESXi hosts off to save power. Then when cluster resource utilization becomes high DPM will power one or more ESXi hosts back on, assuming there are any available to be powered on. Tests have demonstrated savings of 50% in power consumption when DPM is used.

VMware DPM supports three different wake protocols: Intelligent Platform Management Interface (IPMI), Integrated Lights-out (iLO) and Wake-On-LAN (WOL). DPM can selectively exclude hosts from power management and optionally implements recommendations in manual mode (Admin needs to approve) or fully automated mode. Microsoft Hyper-V with SCVMM support only "core parking" to shut off individual CPU cores, which provides only minimal power savings. Citrix XenServer Advanced Power Management is missing support for out-of-band server management protocols like IPMI that are needed to reliably restore server power. Red Hat's Power Saver feature consolidates virtual machines, but it does not power down the hosts.

Network and Storage I/O Controls

Network I/O Control (NetIOC) traffic-management prioritization enables flexible partitioning of resource pool and physical network adaptor bandwidth between different traffic types, including virtual machine, vMotion, fault-tolerant, and IP storage traffic. Storage I/O Control (SIOC) provides quality-of-service capabilities for storage I/O in the form of I/O shares and limits that are enforced across all virtual machines accessing a datastore, regardless of which host they are running on. Using SIOC, vSphere administrators can ensure that the most important virtual machines get adequate I/O resources, even in times of congestion.

Network and Storage I/O Controls solve the "noisy neighbor" problem where an overly active virtual machine can starve others of the network and storage bandwidth they need to meet service level guarantees. Products from Microsoft, Citrix and Red Hat have no method to limit storage and network resource contention.

Hot Add Virtual Machine Resources

Despite the extensive planning that goes into the initial sizing and configuration of a virtual machine, it can be difficult to predict and accommodate sudden changes in workload demands. With VMware Hot Add, capacity can be dynamically added to virtual machines while they are powered on. This enables applications to scale seamlessly without disruption or downtime. vSphere 5 allows administrators to hot add CPUs and RAM to virtual machines with no downtime, provided the guest OS supports that operation. vSphere 5 also supports hot adding and removing of virtual devices, such as virtual disks, virtual NICs and USB devices. Further, vSphere's unique ability to hot grow a VMFS volume to add capacity to a datastore and hot extend virtual disks allows administrators to respond to increasing virtual machine storage requirements without downtime.

Microsoft Hyper-V and Xen products like Citrix XenServer and Oracle VM cannot expand mounted storage devices. Storage expansions require un-mounting the storage volumes, and since those products have no live storage migration capability, VM downtime is required.

Resource and Performance Control Feature/Function Comparison

RESOURCE AND PERFORMANCE CONTROL DIFFERENTIATORS	VMWARE VSPHERE 5	MICROSOFT HYPER-V R2 SP1	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
Large cluster size	Yes, up to 32 hosts and 3000 virtual machines per cluster	No, 16 host limit of Microsoft Cluster Services	Undocumented	Undocumented
Logical resource pools	Yes	No, requires SCVMM	No, cannot subdivide resources of pooled hosts	No, cannot subdivide resources of pooled hosts
Hierarchical resource pools	Yes, organize resource pools to match business unit structure	No	No	No
Easily add capacity to resource pools	Yes, add new physical servers to a resource pool and DRS redistributes virtual machines	No, resources added at cluster level only	No, resources added at host pool level only	No, resources added at cluster level only
Resource shares and reservations	Yes, specify CPU, memory, network and storage resources; honored at resource pool level	No storage shares, shares apply only across entire host cluster	No shares, reservations apply only across entire host cluster	Network shares only, apply across entire host cluster
Virtual machine affinity/anti-affinity rules	Yes, specify hosts allowed for each virtual machine, keep virtual machines paired or separated	No	VM host affinity checked only on initial startup	No
Dynamic workload balancing	Yes, VMware DRS	Requires complex SCVMM, SCOM and PRO Tips configuration, PRO Tips to be discontinued	Workload Balancing requires additional servers and Enterprise or Platinum Editions	Only balances based on host CPU usage
Load balancing based on storage resource use	Yes, VMware Storage DRS	No	No	No

RESOURCE AND PERFORMANCE CONTROL DIFFERENTIATORS	VMWARE VSPHERE 5	MICROSOFT HYPER-V R2 SP1	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
Load balancing compatibility with memory over commitment	Yes, allows virtual machine migrations that result in overcommitted hosts if result improves balancing	No	No	No
Load balancing compatibility with High Availability and Fault Tolerance features	Yes, DRS works with virtual machines protected by VMware HA and FT	No	No	No
Host-level power management	Yes, VMware DPM consolidates virtual machines and powers off hosts using reliable WOL, IPMI and iLO protocols	Limited, core parking feature does not power down hosts, minimal power savings	Advanced Power Management feature lacks IPMI support	No, Power Saver feature does not power down hosts
Host processor power saving feature support	Yes, supports Intel SpeedStep and Turbo Mode, AMD PowerNow, and processor sleep states	No	No	No
Guarantee network resources for critical virtual machines	Yes, VMware Network I/O Controls flexibly partition specific network traffic types at Distributed Switch, resource pool and virtual machine levels	No	No	No
Guarantee storage resources for critical virtual machines	Yes, VMware Storage I/O Controls apply per virtual machine storage shares and limits to control FC, iSCSI and NFS bandwidth usage	No	No	No
Hot Add virtual machine RAM	Yes, works with any guest OS supporting hot add RAM	Yes	No	No
Hot Add virtual machine CPU	Yes, works with any guest OS supporting hot add CPU	No	No	No

RESOURCE AND PERFORMANCE CONTROL DIFFERENTIATORS	VMWARE VSPHERE 5	MICROSOFT HYPER-V R2 SP1	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
Hot Add virtual disks and NICs	Yes, add or remove virtual storage and networking devices without user disruption	Limited, only supports hot add and remove of virtual SCSI drives	No	No
Hot Extend virtual disks	Yes, extend virtual disk capacity non-disruptively	No	No	No

Networking Features

VMware vSphere 5 technology gives you the ability to create, configure and manage scalable virtual networks within VMware ESXi hosts. VMware virtual networking extends data center physical networking features, standards, and principles to virtual objects for greater granularity and control.

Integrated Network Failover and Load Balancing

VMware vSphere allows users to benefit from NIC teaming, load balancing, traffic shaping and security even when not natively supported by hardware. With vSphere, users can perform fundamental networking management tasks directly from vCenter Server. Users can set up NIC teaming and load balancing policies, shape outbound traffic from virtual switches and set up layer-2 (data link layer) networking security. Microsoft does not provide native support for NIC teaming and forces users to rely on NIC hardware capabilities which are typically managed through unfamiliar and complex Command Line Interfaces or third-party utilities. Microsoft does not directly support NIC teaming and load balancing, so users must rely on hardware vendors. Hyper-V users must also use separate Windows interfaces to configure iSCSI storage. VMware vSphere greatly reduces the complexity related to networking management by providing a hardware independent solution that gives users greater flexibility of choice and can be managed directly from vCenter in just a few easy clicks.

VMware vSphere Distributed Switch

The vSphere Distributed Switch (vDS) simplifies virtual machine networking by enabling you to set up virtual machine networking for your entire datacenter from a centralized interface. A single vDS spans many vSphere hosts and aggregates networking to a centralized datacenter level. A vDS abstracts the configuration of individual virtual switches and enables centralized provisioning, administration and monitoring through VMware vCenter Server. With a vDS, administrators no longer need to manually configure hosts with identical network settings to ensure successful vMotions. A vDS enables Network vMotion where the state of a virtual machine's network ports follow it as it is migrated between hosts. Port state includes settings for VLANs and private VLANs, bidirectional traffic shaping and NIC teaming as well as network performance counters.

Microsoft and Red Hat — have nothing equivalent to the vDS available for their hypervisors. Their users must separately configure virtual switches in each hypervisor and manually ensure they are configured properly. Citrix XenServer recommends an open source project call Open vSwitch, but it requires a separate management interface and is a single point of failure.

Cisco Nexus 1000V

The vSphere Distributed Switch is the basis for the optional Cisco Nexus 1000V, which provides vSphere with an extended Cisco Nexus/Catalyst feature set plus the familiar IOS interface. With the Nexus 1000V, it's easy for network administrators familiar with Cisco environments to manage a virtualized network infrastructure.

Private VLANs

Private VLAN support in the vSphere Distributed Switch lets you extend networking best practices for isolation and IP address conservation to the virtual domain. Only VMware vSphere supports Private VLANs—Citrix XenServer 5.6 and Red Hat Enterprise Virtualization are missing that feature. Private VLANs are in common use in datacenters to define private switch ports that are restricted to a single network uplink. vSphere Private VLANs are easily configured as port groups on a vDS.

Networking Feature/Function Comparison

NETWORKING DIFFERENTIATORS	VMWARE VSPHERE 5	MICROSOFT HYPER-V R2 SP1	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
Integrated NIC teaming and load balancing support	Yes, Integrated native support for active/active and active/passive network adaptor teaming and load balancing policies	No	NIC teaming supported but limited configurability, no load balancing (lacks LACP support)	No
Distributed virtual switch	Yes, vSphere Distributed Switch centralizes network configuration across many hosts	No, must configure virtual switches on each host	Limited, Open vSwitch is a single point of failure, poorly integrated with XenServer	No, must configure virtual switches on each host
Third-party virtual switch	Yes, Cisco Nexus 1000V implements an IOS switch on the vSphere Distributed Switch	No	No	No
Private VLANs	Yes, implemented in vSphere Distributed Switch	Yes	No	No

Storage Features (new/updated features)

VMware vSphere storage virtualization is a combination of VMware vSphere features and APIs that provide an abstraction layer for physical storage resources to be addressed, managed and optimized in a virtualization deployment. vSphere storage is unique in providing a high performance distributed cluster file system (VMFS) and support for over 1,200 storage array varieties.

Storage vMotion

VMware Storage vMotion relocates virtual machine disk files from one shared storage location to another shared storage location with zero downtime, continuous service availability and complete transaction integrity. Storage vMotion enables organizations to perform proactive storage migrations, simplify array maintenance and migrations, improve virtual machine storage performance and free up valuable storage capacity. Storage vMotion is fully integrated with VMware vCenter Server and supports migrations of virtual machines with snapshots or those based on linked clones. Citrix XenServer and Red Hat Enterprise Virtualization offer no live storage migration features. Hyper-V R2 offers only “Quick Storage Migration, which requires VM downtime to complete migrations.

Storage Distributed Resource Scheduler

The new VMware Storage DRS feature in vSphere 5 adds storage I/O resources and space capacity to the CPU and memory resources monitored when making load balancing decisions. Storage DRS optimizes placement of newly provisioned virtual machines across a collection of datastores aggregated in to a single datastore cluster and it automates monitoring ongoing balancing of the storage environment. Storage DRS provides affinity rules to control which virtual disks should or should not be placed on the same datastore. No competing virtualization products offer anything comparable to VMware Storage DRS.

Profile-Driven Storage

Another exclusive vSphere storage feature, Profile-Driven Storage lets users with multiple tiers of storage performance ensure that virtual machines always use the datastores that match their service level requirements. vSphere administrators classify their datastores into Storage Profiles based on the service levels they provide. Virtual machines are assigned a Storage Profile when provisioned, and vSphere then ensures that they are initially placed on a matching datastore and that any Storage DRS migrations are limited to eligible storage tiers. vSphere Storage Profiles can even use Storage vMotion to move virtual disks on noncompliant datastores to the correct storage tiers. Microsoft Hyper-V, Citrix XenServer and Red Hat Enterprise Virtualization have no similar storage features, so administrators using those products must manually assign virtual machines to available storage.

Thin Provisioning

VMware vSphere Thin Provisioning allows over-allocation of storage capacity for increased storage utilization, enhanced application uptime and simplified storage capacity management. You'll lower capital and operating expenditures by reducing disk purchase and cutting the power and cooling cost of the excess disk. In addition to the capability of creating thin provisioned disks, VMware vSphere also provides a built-in consumption-based monitoring system with which administrators can control disk space availability levels. Consumption-based monitoring is essential to the use of thin provisioning without the risk of unexpectedly running out of space. Microsoft Hyper-V supports thin provisioned disks, but does not provide any consumption-based monitoring system making thin provisioning extremely risky—and therefore unlikely to be adopted in production. In fact Microsoft recommends against use of Hyper-V Dynamic Expanding virtual disks in production. Red Hat also [recommends against](#) use of thin disks for server virtual machines. Citrix XenServer supports thin disks only on the small number of arrays supporting their StorageLink feature.

vSphere Storage Appliance

VMware vSphere Storage Appliance is extra cost software for vSphere 5 that delivers shared storage benefits without the cost and complexity of shared storage hardware. VMware vSphere Storage Appliance extends the benefits of virtualization to all SMBs by transforming internal storage from several server hosts into a protected shared storage resource. Easily installed with a simple five-click configuration, vSphere Storage Appliance combines the local disks on up to three vSphere hosts into a virtual storage array managed by vCenter. All vSphere shared storage applications are supported, including vMotion, High Availability and Fault Tolerance. Small business users of Microsoft Hyper-V, Citrix XenServer and Red Hat Enterprise virtualization face the costs and complexity of physical shared storage arrays if they want access to such features.

Storage Feature/Function Comparison

STORAGE DIFFERENTIATORS	VMWARE VSPHERE 5	MICROSOFT HYPER-V R2 SP1	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
Cluster file system	Yes, updated VMFS high performance distributed cluster file system included with vSphere enables virtual machine mobility and high availability	Cluster Share Volumes required for shared storage live migration is a hybrid file system on NTFS	No	Red Hat GFS is extra cost, not integrated with RHEV
Broad array support	Yes, vSphere supports over 1,200 FC, iSCSI and NAS arrays	No storage management features	Limited, only 98 arrays supported	Not documented
Live storage migration	Yes, Storage vMotion enables live virtual disk migrations between datastores of any type: FC, iSCS, NFS and local disk	No, Quick Storage Migration requires extended virtual machine downtime	No	No
Automated storage load balancing	Yes, Storage DRS optimizes virtual machine data placement, includes Affinity/Anti-Affinity rules for virtual disks	No	No	No
Automated assignment of virtual machines to datastores meeting necessary service levels	Yes, Profile-Driven Storage ensure virtual machines are on correct storage, remediates compliance using Storage vMotion	No	No	No
Thin disk support with low backing storage alerts	Yes, vSphere Thin Provisioning, supports snapshots and linked clones, consumption-based monitoring alerts when physical storage runs low	Thin disks not recommended in production, no low storage alerts	Limited, requires StorageLink and supported SAN, no NAS support	Documentation recommends against thin disks for server VMs
Software-based shared storage	Yes, vSphere Storage Appliance* combines local storage of three vSphere hosts into a virtual SAN	No	No	No

*vShield Zones ivSphere Storage Appliance is an extra cost addition to vSphere.

Business Continuity Features (new/updated features)

VMware has taken a holistic approach to business continuity, enabling customers to protect all applications running on vSphere with simple and cost-effective solutions to support various types of business continuity objectives including: high availability, data protection and disaster recovery. The high availability and data protection features described below are integral to vSphere 5. Reviewers concerned with disaster recovery should investigate [VMware vCenter Site Recovery Manager](#) – a product sold separately from vSphere.

vMotion

vMotion technology, deployed in production by 80% of VMware customers, leverages the complete virtualization of servers, storage, and networking to move an entire running virtual machine instantaneously from one server to another. vMotion uses the VMware VMFS cluster file system to control access to a virtual machine's storage. During a vMotion, the active memory and precise execution state of a virtual machine is rapidly transmitted over a high speed network from one physical server to another, and access to the virtual machines disk storage is instantly switched to the new physical host. Since the network is also virtualized by the VMware host, the virtual machine retains its network identity and connections, ensuring a seamless migration process. vMotion allows users to avoid downtime when performing hardware maintenance or balancing virtual machines across hosts.

Unique to VMware vMotion is support for up to eight concurrent high speed virtual machine migrations per host. Microsoft, Citrix and Red Hat hosts support only one slower speed migration, meaning evacuating virtual machines from hosts takes far longer and physical maintenance downtime windows are extended. With vSphere 5, vMotion is now compatible with higher latency network links so that "Metro vMotion" spanning greater distances is supported.

High Availability

VMware vSphere High Availability (HA) utilizes heartbeats between vSphere hosts and virtual machines in the cluster to check that they are functioning. When a host or virtual machine failure is detected, VMware HA automatically restarts affected virtual machines on other production servers, ensuring rapid recovery from failures. Once VMware HA is configured, it operates without dependencies on operating systems, applications, or physical hardware.

While vSphere 5 has made HA even easier to setup, Microsoft Hyper-V requires separate tools to create highly available clusters (Microsoft Failover Cluster Manager) and to enable high availability on Hyper-V hosts (Microsoft Virtual Machine Manager). In addition, to allow highly available virtual machines to share LUNs, users need to deploy Microsoft Cluster Shared Volumes, a hybrid cluster file system that greatly complicates storage administration. Hyper-V also lacks virtual machine restart priority needed to ensure critical workloads are recovered first.

Fault Tolerance

vSphere Fault Tolerance (FT) provides continuous availability for applications in the event of server failures, by creating a live shadow instance of a virtual machine that is in virtual lockstep with the primary instance. By allowing instantaneous failover between the two instances in the event of hardware failure, FT eliminates even the smallest chance of data loss or disruption. vSphere FT is a unique VMware feature. It is the simplest and most cost effective solution to enable zero down time and zero data loss protection against hardware failures.

- **Easiest to use:** vSphere FT enables continuous availability for virtual machines and applications in a matter of few clicks with the same simple process as vSphere HA. Once a virtual machine is made Fault Tolerant with vSphere FT, vSphere will automatically place the "shadow virtual machine" on the most appropriate secondary host and maintain the two virtual machines in perfect lock-step down to the CPU instruction level.
- **Most cost effective:** vSphere FT does not require specialized hardware or additional third-party software. It is an integral part of vSphere, works with all 80+ supported guest OSs and is compatible with other key features such as VMware vMotion and DRS.
- **Citrix relies on an expensive, poorly integrated 3rd-party product for fault tolerance.** XenServer users must purchase Marathon everRun VM at a cost of almost \$3000 per server. everRun VM's management is not integrated, guest OS support is very limited and it reduces I/O performance of VMs.
- **There are no fault tolerance options available for Microsoft Hyper-V or Red Hat Enterprise Virtualization.**

VMware Data Recovery

VMware Data Recovery is a disk-based backup and recovery solution that provides complete data protection for virtual machines. VMware Data Recovery is fully integrated with VMware vCenter Server to enable centralized and efficient management of backup jobs and includes data de-duplication to minimize disk usage. VMware Data Recovery includes powerful features such as full and incremental disk-based backup and recovery, image level and individual file restore (including Linux guests,) and VSS support for consistent backups of Microsoft operating systems and applications. VMware Data Recovery de-duplicates data to conserve disk space and it supports any type of storage—Fibre Channel, iSCSI, NAS or local disk.

To get similar capabilities for Hyper-V, you'd need to purchase and configure System Center Data Protection Manager, an extra cost server that is not integrated with Hyper-V. Citrix XenServer and Red Hat Enterprise Virtualization both lack comparable backup features.

Business Continuity Feature/Function Comparison

BUSINESS CONTINUITY DIFFERENTIATORS	VMWARE VSPHERE 5	MICROSOFT HYPER-V R2 SP1	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
Multiple concurrent live migrations	Yes, 8 concurrent vMotions on 10Gb and 4 concurrent vMotions on 1Gb networks	No, hosts support only one live migration at a time	No, hosts support only one live migration at a time	No, hosts support only one live migration at a time
Metro area live migrations	Yes, "Metro vMotion" supported with up to 10ms round trip latency between hosts	No	No	No
Live migrations between different processors supported	Yes, Enhanced vMotion Compatibility uses Intel FlexMigration and AMD-V Extended Migration features, older processors also supported	Limited, Hyper-V R2 CPU Compatibility Mode degrades all virtual machines to Pentium 4	Requires XenServer Enterprise Edition and Intel FlexMigration or AMD Extended Migration support	Limited, virtual CPUs masked to Pentium II features
Virtual machine restart in case of host failure	Yes, updated vSphere HA works with all supported guest OSs	Yes, requires Microsoft failover clustering, limited guest OS support	Yes	Yes
Virtual machine restart in case of guest failure	Yes	Yes, Hyper-V R2 will monitor VM heartbeat	No	Yes
Virtual machine restart in case of application failure	Yes, with Symantec ApplicationHA (3rd-party add-on)	Yes	No	No

BUSINESS CONTINUITY DIFFERENTIATORS	VMWARE VSPHERE 5	MICROSOFT HYPER-V R2 SP1	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
No single point of failure for high availability	Yes, vSphere HA ensures virtual machine restart even if vCenter Server is unavailable	Yes, requires Microsoft failover clustering	Yes	No, VMs won't restart if RHEV Manager is down
Virtual machine restart priority	Yes, ensure the most critical virtual machines are restarted first	No	Yes	No
Resource checks to ensure all virtual machines can restart if a host fails	Yes, vSphere HA continuously monitors capacity use and "reserves" spare capacity for virtual machine restarts	No	No	No
High availability protection for large clusters	Yes, up to 32 hosts and 3000 virtual machines per cluster	No, Failover Clustering limited to 16 hosts/cluster	Undocumented	Undocumented
Zero downtime, zero data loss continuous availability	Yes, vSphere FT automatically detects server failures and triggers instant stateful failover	No	Requires extra cost Marathon Technologies everRun VM, no management integration	No
Maintain protection levels after failover	Yes, FT creates a new secondary virtual machine after failover	No	No, Marathon everRun does not assign new secondary hosts after a failure	No
Continuous availability with all types of shared storage	Yes, FT supports FC, iSCSI, NAS and vSphere Storage Appliance	No	No NAS support	No
Continuous availability for all guest operating systems	Yes, FT compatible with all 80+ vSphere supported guests	No	No, Windows Server 2003 and 2008 only	No

BUSINESS CONTINUITY DIFFERENTIATORS	VMWARE VSPHERE 5	MICROSOFT HYPER-V R2 SP1	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
Continuous availability is compatible with live migration and HA	Yes, FT supports vMotion, Storage vMotion, DRS, HA	No	No	No
Disk-based backup and recovery for virtual machines	Yes, VMware Data Recovery is fully integrated with vSphere	Requires System Center Data Protection Manager, extra cost and not integrated with Hyper-V	No	No
Full and incremental virtual machine backup	Yes, VMware Data Recovery	SCDPM treats virtual machines as physical	No	No
Image level and individual file restore	Yes, VMware Data Recovery	Requires SCDPM	No	No
Backup data de-duplication	Yes, de-duplication in VMware Data Recovery reduces backup size and time	No	No	No
VSS backup support	Yes, VMware Data Recovery VSS support enables consistent backups of Windows virtual machines	Requires SCDPM	No	No

Management and Provisioning Features (new/updated features)

The VMware vCenter Server platform is the industry's most robust virtualization management solution. Advanced capabilities provide the greatest visibility, proactive management and scalability for your virtual environment. vCenter Server is a foundation you can easily extend for end-to-end integration with your physical environment and upon which you can build a private cloud infrastructure.

vCenter Server Appliance

Quickly deploy vCenter Server and manage vSphere using a Linux-based virtual appliance. The vCenter Server Appliance (vCSA) provides full vCenter Server functionality packaged as an Open Virtualization Format (OVF) template that installs in less than five minutes. The vCSA shares the same capabilities as a Windows-based vCenter Server (exceptions are linked mode and SQL Server support.) Enterprises that have standardized on Linux will find the vCSA offers a streamlined deployment experience free of Microsoft Windows. The vCSA makes vSphere a more attractive solution for Linux shops compared to Citrix XenServer and Red Hat Enterprise Virtualization, both of which require Window-based management servers.

vSphere Web Client

The vSphere Web Client enables managing the essential functions of vSphere from any browser anywhere in the world. It is a full-function alternative to the Windows-based vSphere Client that offers even greater scalability and extensibility for vSphere users looking for alternatives to thick Windows clients for managing their vSphere environments. Only VMware offers the choice of a platform-neutral browser management interface. Microsoft, Citrix and Red Hat all support only thick Windows clients with their virtualization platforms.

vCenter Linked Mode

VMware vCenter Linked Mode provides a scalable architecture and visibility across multiple vCenter Server instances, with roles, permissions and licenses replicated across the infrastructure so you can simultaneously log in, view and search the inventories of all vCenter Servers from a single vSphere Client. Linked Mode uses a common directory of global vCenter Server data to permit sharing of administrative user roles and licenses across all linked vSphere datacenters.

vCenter Linked Mode accommodates customized permissions ranging from limited access on just a single vCenter Server to global administrator access to every vSphere object in a Linked Mode group.

Microsoft requires System Center Virtual Machine Manager to manage multiple Hyper-V hosts, but multiple SCVMM servers cannot be linked. System Center Virtual Machine Manager supports only 400 hosts and 8,000 VMs, so a single vCenter Server can manage larger infrastructures (1,000 hosts and 10,000 virtual machines) and Linked Mode scales to far larger sizes. Citrix XenCenter can manage multiple XenServer resource pools, but those pools are limited to just 16 hosts. Red Hat Enterprise Virtualization is limited to only 50 hosts, which is the maximum supported by the RHEV Manager.

Auto Deploy

Auto Deploy allows you to deploy more vSphere hosts running the ESXi hypervisor architecture “on the fly” to diskless servers. Once running, completely eliminate patching by pushing out updated images rather than scheduling patch windows. Microsoft Hyper-V requires addition of System Center Configuration Manager and complex, fragile configuration steps to automate host installations. Citrix XenServer can do basic PXE boot of hosts, but —unlike vSphere Auto Deploy—it has no features to automate selection and customization of fully configured host images. Red Hat Enterprise Virtualization hosts can only boot from local disks, so auto deployment to diskless hosts is not possible.

Host Profiles

Host Profiles creates a profile that encapsulates the host configuration and helps to manage the host configuration, especially in environments where an administrator manages more than one host in vCenter Server. Host profiles eliminates per-host, manual, or UI-based host configuration and maintains configuration consistency and correctness across the datacenter. Host profile policies capture the blueprint of a known, validated reference host configuration and use this to configure networking, storage, security, and other settings on multiple hosts or clusters. You can then check a host against a profile's configuration and automatically remediate any deviations.

Neither Microsoft Virtual Machine Manager (SCVMM) nor Citrix XenCenter provides host configuration capabilities out of the box. Microsoft users must deploy System Center Configuration Manager (SCCM), a separate non-integrated product, to obtain configuration management capabilities for physical servers. SCCM—a very complex product to install and setup—requires extensive configuration, scripting and customization to provide the same functions as Host Profiles. With Resource Pools, Citrix XenCenter only provides the ability to share cluster level settings (such as VLANs) among groups of hosts. Citrix Resource Pools (not be confused with vSphere Resource Pools that enable true abstraction and aggregation of CPU and memory resources) do not provide host level configuration monitoring and remediation. Red Hat Enterprise Virtualization also has nothing comparable to VMware Host Profiles.

vApps

vApps simplify the deployment and ongoing management of an n-tier application in multiple virtual machines by encapsulating it into a single virtual service entity. vApps encapsulate not only virtual machines but also their interdependencies and resource allocations allowing for single-step power operations, cloning, deployment, and monitoring of the entire application. vCenter Server includes support for creating and running vApps as well as importing and exporting them in compliance with the Open Virtualization Format (OVF) standard. Microsoft Hyper-V has no OVF or vApp support and Citrix XenServer OVF support is available only as a technology preview.

vSphere Update Manager

VMware vSphere Update Manager is a vCenter plug-in patch management solution for VMware vSphere. Update Manager provides a single patch management interface for ESXi hosts allowing administrators to ensure their virtual infrastructure is compliant with baselines they define. Update Manager provides a simple way of ensuring cluster-wide patch compliance. Update Manager patches one host at a time in the cluster using vMotion to migrate virtual machines away from the host that it is patching to other hosts in the cluster.

Update Manager is a fully integrated module of VMware vCenter Server. It does not require a complex installation or additional infrastructure. Microsoft's System Center Virtualization Machine Manager (SCVMM) does not have integrated patching capabilities for virtual environments. To obtain any patching capability, users must purchase and install System Center Configuration Manager (SCCM), which requires dedicated infrastructure, is complex to install, and uses a separate UI. Microsoft customers must also use a non-integrated Offline Virtual Machine Servicing Tool to patch Windows virtual machines. In contrast, VMware Update Manager is a simple plug-in module for vCenter that can be rapidly installed, does not require additional infrastructure (beyond what already in use for vCenter), and can be accessed directly from the vSphere Client. VMware Update Manager is included even in the most basic bundle of VMware vSphere. Citrix XenServer only provides a patch tracking system that reports on the latest patch applied to a virtual machine. Users must manually keep track of patch availability, manually download patches and install them. Red Hat can only patch running Red Hat guests with Red Hat Network subscriptions. RHEV Manager has no integrated host or guest update features and no Windows guest updates are supported.

Virtual Device Support

vSphere 5 adds support for the latest virtual devices to let users test and run the latest hardware and software with their virtual machines. vSphere 5 now supports:

- USB 3.0 devices (with Linux guests) connected to vSphere Clients or vSphere Web Clients
- UEFI virtual BIOS to support guest operating systems requiring that boot environment
- Software 3D graphics in virtual machines for applications like Windows Aero
- Smart-card readers for virtual desktops in secure environments
- Apple Mac OS X guests running on Apple server platforms

With Microsoft Hyper-V R2, features such as 3D support require expensive graphics cards on each host, and virtual machines do not have USB support. Mac OS X guest support in Hyper-V is missing as well. Citrix XenServer and Red Hat Enterprise Virtualization virtual machines have the same limitations.

Management and Provisioning Feature/Function Comparison

MANAGEMENT AND PROVISIONING DIFFERENTIATORS	VMWARE VSPHERE 5	MICROSOFT HYPER-V R2 SP1	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
Management server contained in a virtual appliance	Yes, the vCenter Server Appliance is packaged as an OVF appliance	No, Hyper-V and System Center require full Windows Server installations	No, XenCenter installs on Windows	No, RHEV Manager requires a Windows server installation
Windows-free management	Yes, vCSA is Linux-based	No	No, XenCenter management client is Windows-based	No, RHEV Manager is Windows-based
Full management functionality from any browser	Yes, vSphere Web Client	No, Hyper-V Manager and System Center clients are thick Windows applications	No, XenCenter management interface runs only on Windows	No, RHEV requires a Windows management client
Large-scale virtual infrastructure/cloud management	Yes, vCenter Linked Mode supports management of up to 10 linked vCenter Servers, 3,000 hosts and 50,000 virtual machines from a single pane	No, System Center Virtual Machine Manager servers cannot be linked, limited to 400 hosts and 8,000 virtual machines	XenCenter scalability limited to 16 hosts, no linked mode	RHEV Manager supports multiple datacenters/ clusters but limited to 50 hosts

MANAGEMENT AND PROVISIONING DIFFERENTIATORS	VMWARE VSPHERE 5	MICROSOFT HYPER-V R2 SP1	CITRIX XENSERVER 5.6	RED HAT ENTERPRISE VIRTUALIZATION 2.2 (KVM)
Centrally manage provisioning of diskless hosts	Yes, vSphere Auto Deploy	Complex System Center Configuration Manager setup required	Limited, XenServer can boot from FC SAN only, not iSCSI	No, boots only from local storage
Define standard host configurations and enforce compliance	Yes, VMware Host Profiles establish standard vSphere host configurations and automate compliance	Complex System Center Configuration Manager setup required	No host-level configuration monitoring and remediation	No
Simplified deployment of multi-tier applications in virtual machines	Yes, vApps encapsulate virtual machines and their interdependencies, comply with OVF standard	No OVF support in Hyper-V	Limited to an OVF technology preview	Basic OVF import support
Automated host patching	Yes, vSphere Update Manager keeps vSphere hosts and guest tools updated, automates guest migrations during patching, keeps snapshots for rollbacks	Requires SCVMM and SCCM	No	No
USB 3.0 devices	Yes, Linux guests can access USB 3.0 devices connected through vSphere Windows or Web clients	No USB support	No	No
UEFI virtual BIOS	Yes	No	No	No
Software 3D graphics support for virtual machines	Yes	No, RemoteFX requires hardware 3d acceleration card in Hyper-V host	No	No
Apple Mac OS X guest support	Yes, on Apple Xserve systems	No	No	No

Top 20 vSphere 5 Advantages Over the Competition

1. The Most Trusted Hypervisor in the Industry Just Got Better – VMware ESXi 5

VMware ESXi™5 extends the VMware legacy of highly reliable, highly scalable virtualization by delivering even better robustness, security and performance. Already, over 94 percent of ESX and ESXi deployments are in production environments—an example of how both large and small companies trust VMware for their business-critical workloads. ESXi 5 has an exclusive thin virtualization form factor with no dependence on a general-purpose server operating system in the virtualization layer. With a 144MB disk footprint, ESXi 5 dramatically shrinks the code base that needs to be maintained and secured, ultimately resulting in a more secure environment. In contrast, all versions of Microsoft Hyper-V R2 rely on Windows Server 2008 running inside the parent partition. Therefore, the smallest version of Hyper-V R2 (Windows Server 2008 R2 with Server Core installation) still has a disk footprint of approximately 3.6GB—representing millions more lines of code to maintain and secure. Hyper-V R2's dependence on Windows means it faces performance and scalability limitations, especially when running many concurrent virtual machines on the same host. With Hyper-V, the security and stability of your datacenter will always be dependent on the security and stability of Windows.

2. Virtualize 100 Percent of Your Applications – Support for 32 Virtual CPUs and 1TB per Virtual Machine

Per-virtual machine CPU and memory maximums four times greater than previous versions allow companies to virtualize the most resource-intensive Tier 1 applications in their datacenters on vSphere 5. vSphere 5 enables a single virtual machine to simultaneously use up to 32 logical processors (32-way virtual SMP) and 1TB of RAM. With 32-way virtual SMP, even the most processor-intensive applications, such as databases and messaging servers, can be virtualized with no impact on performance. With 1TB per virtual machine, companies can run the most memory-intensive workloads in virtual machines. Microsoft Hyper-V R2 SP1 is limited to 64GB of RAM per virtual machine. It only supports up to 4-way virtual SMP on Windows Server 2008 virtual machines, and all other guest operating systems are limited to 2-way virtual SMP. Citrix XenServer 5.6 is limited to 8-way virtual SMP and 32GB. These limitations mean that users can virtualize only a subset of their applications.

3. Get Reliable, Cost-Effective Solutions for Small Offices – vSphere Essentials Editions

The robust, proven capabilities of VMware vSphere are also available in two cost-effective packages designed for small offices, starting at just \$83 per processor. vSphere Essentials Edition enables server consolidation and centralized provisioning, management, and patching for immediate savings on hardware and operational costs. It also includes integrated physical-to-virtual conversion. vSphere Essentials Plus Edition is an easy-to-deploy “Always on IT” package that includes everything from Essentials and adds vMotion™ live migration, High Availability to dramatically improve application uptime, and Data Recovery for fast backup and recovery of virtual machine data with built-in data deduplication to save on storage costs. With vSphere Essentials and Essentials Plus, small offices get the industry's most proven, complete virtualization platform in an integrated package that solves their most pressing needs—application uptime and data protection. The “free” Hyper-V R2 offering from Microsoft is just a hypervisor missing key management features, and small businesses must add the cost and complexity of Microsoft System Center to make it manageable.

4. Use a Better Way to Enforce Security in a Virtual Environment – VMware vShield 5

Virtualization offers new and better ways to secure applications and networks. Rather than inheriting legacy approaches based on costly physical appliances, brittle network settings and performance-sapping agents, VMware vShield transforms security from complex to disruptively simple by applying security policies at the virtualization layer, where every aspect of virtualized applications can be inspected and protected using a single vShield Manager interface. The vShield approach makes security simpler, more adaptive and more virtualization-aware. vShield Zones (included with certain vSphere editions) makes security-zone settings a logical construct so you can safely mix virtual machines from different trust zones on common hosts and keep those settings intact, even as virtual machines are migrated. The rest of the vShield product family (available separately) applies unique hypervisor-level introspection to protect virtual machines and networks with no need for hardware appliances or in-guest agents. The new vShield App Sensitive Data Discovery feature automates regulatory-compliance scans with more than 80 templates that identify protected data. Microsoft Hyper-V R2 and Citrix XenServer support only legacy physical-machine approaches to security and have nothing comparable to VMware vShield. Users deploying those products can only enforce security zones by setting up wasteful silos of physical hosts. Hyper-V and XenServer network security is dependent on VLANs—an approach that cannot scale to meet the needs of even midsize clouds, and their users are also dependent on in-guest agents that can trigger “antivirus storms.”

5. Enable Automated Private Clouds in the Datacenter – Logical Resource Pools and Storage DRS

VMware vSphere 5 cluster-level management capabilities (e.g., vSphere Distributed Switch, vShield Zones, and Distributed Power Management)—and the automation provided by vSphere Distributed Resource Scheduler (DRS) and the new Storage DRS—all improve the effectiveness and flexibility of VMware Logical Resource Pools. These resource pools aggregate and share resources across many servers—the essence of cloud computing. Companies can create a logical, shared pool of resources for a specific business group and guarantee resource availability while maintaining isolation from other pools. vSphere DRS enables intelligent, automated load balancing so applications get the right level of resources at the right time. New Storage DRS extends that load balancing to dynamically automate placement of virtual disks on available datastores to balance disk use and prevent storage bottlenecks. DRS and Storage DRS are essential to enabling logical resource pools that comply with SLAs. Microsoft Hyper-V R2 SP1 and Citrix XenServer have nothing comparable. Hyper-V and XenServer deployments require dedicated silos of hosts or clusters for each business group—a rigid infrastructure that is time-consuming and costly to maintain. The Microsoft and Citrix products also lack the virtual machine and virtual-disk affinity and anti-affinity rules found in vSphere, so they cannot guarantee datacenter policies and licensing compliance when load balancing is automated.

6. Achieve Higher Consolidation Ratios at Lower Cost – Virtual Machine Density Optimizations

Better performance and utilization lead to higher virtual machine consolidation ratios, which lead to lower capital expenditures. vSphere 5 employs unique performance and resource management features to let customers reliably run production workloads at the highest virtual machine densities. vSphere 5 uses four levels of memory management technology—in-guest ballooning, memory compression, transparent page sharing and fast host paging—to accommodate the highest densities with any supported guest operating systems. The “Dynamic Memory” features in Microsoft Hyper-V R2 and Citrix XenServer use only a simple ballooning method that works with a select few guests and can’t deliver comparable virtual machine densities, as shown by [independent testing](#). vSphere further adds a more efficient direct driver I/O model, true logical resource pools with Dynamic Resource Scheduler for dynamic load balancing and a high-performance “gang” CPU scheduler to extend its cost advantage over even “free” versions of Hyper-V, Xen and Red Hat KVM.

7. Match Applications to Appropriate Storage Tiers – Profile-Driven Storage

Operating multiple tiers of storage lets enterprises reduce costs by matching applications to storage hardware, providing just the right service levels. But assigning virtual machines to the correct storage tiers as they are provisioned is a manual operation prone to misconfiguration. vSphere 5 Profile-Driven Storage streamlines and automates storage provisioning by letting administrators classify their datastores into Storage Profiles based on the service levels they provide. Virtual machines are assigned a Storage Profile when provisioned, and vSphere then ensures that they are initially placed on a matching datastore and that any Storage DRS migrations are limited to eligible storage tiers. vSphere Storage Profiles can even use Storage vMotion to move virtual disks on noncompliant datastores to the correct storage tiers. Microsoft and Citrix have nothing equivalent for the critical task of managing storage. In fact, Hyper-V and System Center Virtual Machine Manager 2008 R2 have no storage-management features at all.

8. Reduce OpEx Costs During Planned Maintenance – High-Performance Live Migrations with vMotion and Storage vMotion

The need to perform planned maintenance during nonpeak hours is a significant contributor to higher operational costs. Overtime pay for nights and weekends is compounded with time spent coordinating among business owners to schedule a maintenance window. vSphere 5 improves on the market-proven vMotion and Storage vMotion capabilities that allow IT administrators to perform planned maintenance during normal business hours without a maintenance window. vMotion supports up to eight concurrent live migrations per host, greatly reducing time to evacuate virtual machines prior to maintenance. Microsoft Hyper-V, Citrix XenServer and Red Hat KVM are limited to a single live migration per host. vMotion also distributes migration traffic across multiple 1Gb or 10Gb links to further shorten maintenance windows, and it now supports high-latency links. Only vSphere Storage vMotion allows virtual machine storage to be live-migrated between datastores—even across different types of storage (Fibre Channel, iSCSI, NFS, DAS)—with no downtime to accommodate storage maintenance and upgrades during production hours. Storage vMotion now even supports virtual machines with snapshots and linked clones. For storage migration, Hyper-V R2 has an inferior capability called “Quick Storage Migration” that requires application downtime, and Citrix and Red Hat have no storage-migration solution at all.

9. Ensure Service Levels for Business-Critical Applications – Network and Storage I/O Control

Enterprises running critical applications in private or public clouds need assurance that those workloads are protected from “noisy neighbors”—badly behaved virtual machines sharing the same hosts or clusters that indiscriminately consume resources. Microsoft Hyper-V and Citrix XenServer offer only basic CPU and memory controls for virtual machines that are insufficient to protect critical applications. Only vSphere 5 provides control for all key resources—CPU, memory, network and storage—needed to guarantee that service levels are met at the virtual machine, virtual switch, datastore and resource-pool levels. vSphere 5 Network I/O Control lets you prioritize vSphere Distributed Switch traffic, and new per-virtual machine settings ensure that I/O-intensive workloads get the network bandwidth they need. vSphere 5 Storage I/O Control enforces virtual machine storage I/O shares and limits on any type of datastore, including new NFS support, to ensure the storage performance of important applications even in times of congestion.

10. Centrally Manage Provisioning of Diskless Hosts – New vSphere Auto Deploy

Easily and quickly add capacity to a vSphere 5 cluster by simply booting a diskless server. vSphere Auto Deploy uses Host Profiles, vSphere host images and your custom provisioning rules centrally managed by vCenter to bring a new host online in minutes. Auto Deploy also lets you rapidly upgrade hosts to the latest vSphere release. Microsoft makes it much more difficult to provision Hyper-V hosts with requirements to purchase and install System Center Configuration Manager and apply complex configuration settings. Citrix XenServer can do basic PXE boot of hosts, but—unlike vSphere Auto Deploy—it has no features to automate selection and customization of fully configured host images.

11. Enable Shared Storage for Everyone – vSphere Storage Appliance

Until now, the cost of shared storage arrays has kept the high-availability and virtual machine mobility benefits of virtualization out of reach for small businesses. The new vSphere Storage Appliance changes that by enabling virtual shared storage volumes spanning low-cost internal disks on up to three vSphere hosts. Advanced vSphere features including vMotion, High Availability, Fault Tolerance, DRS and Storage vMotion are supported after just a five-click configuration and without the need for dedicated shared storage hardware. The vSphere Storage Appliance is implemented entirely in software and can be added to any vSphere host or acquired in an attractively priced vSphere Enterprise Plus bundle. Using live migration and high availability with Microsoft Hyper-V and Citrix XenServer requires expensive Fibre Channel or iSCSI arrays, making vSphere a lower-cost and more capable solution for small businesses that want the best protection and automation for their applications.

12. Manage Virtual Networking for Private Clouds – vSphere Distributed Switch

With vSphere Distributed Switch, IT can manage one virtual switch that spans an entire cluster instead of managing a separate virtual switch for each host—a time-saving way to manage virtual networks. It creates a single distributed switch that spans a cluster of vSphere hosts and retains network runtime state when virtual machines move between hosts. This capability is a critical enabler for building private clouds, because it allows cluster-level network settings to be managed and policies to be enforced centrally. Networking vendors have built third-party virtual switches, such as the Cisco Nexus 1000V, based on vSphere Distributed Switch to make it easier to integrate virtualized environments and manage physical and virtual networks with a common set of tools. Microsoft Hyper-V R2 has nothing comparable to vSphere Distributed Switch. Those who deploy Hyper-V R2 must manually manage virtual networks on a host-by-host basis. Citrix offers a vSwitch, but it is not fully integrated with XenServer and lacks third-party support from networking vendors.

13. Configure Virtualization Hosts the Easiest Way – VMware Host Profiles

VMware Host Profiles greatly simplify vSphere host configuration management, thereby reducing operational costs because IT administrators spend less time manually configuring and compliance-checking each individual host. Host Profiles automatically apply a “gold” host-configuration profile (includes networking, storage and security settings) to multiple vSphere hosts. They also monitor compliance to “gold” host-configuration profiles and can remediate noncompliant hosts with the push of a button. Microsoft Hyper-V R2 has no automated, out-of-box host-profiling capability. Host configuration and remediation requires a manual installation and complex configuration of System Center Configuration Manager.

14. Ensure Zero Downtime, Zero Data Loss for Applications – vSphere Fault Tolerance

With VMware vSphere Fault Tolerance (FT) ensuring that protected applications are always available, even in the event of hardware failure, your applications may never go down again. FT creates a shadow copy of a protected virtual machine and automatically triggers a seamless, stateful failover if the virtual machine stops responding because of hardware failure. After the failover, FT automatically creates a new shadow copy on another host to ensure continuous protection. FT works with all types of shared storage (Fibre Channel, NAS or iSCSI) and with all operating systems supported by VMware vSphere. No complex setup is required, and applications do not need to be cluster-aware. Microsoft, Oracle and Red Hat have no equivalent functionality. Microsoft claims that active-active clustering can address the same need, but active-active clustering is complex to set up and only works with a small set of cluster-aware guest operating systems and applications. Citrix offers only a poorly integrated and much more expensive fault-tolerance solution from Marathon Technologies.

15. Add Virtual Machine Resources with No Downtime – Hot-Add CPU/Memory, Hot-Extend Disks

Even with the best planning, applications sometimes require more resources than originally expected. VMware vSphere 5 delivers hot-add virtual CPU and memory and hot-add/extend virtual disks to dynamically add virtual machine resources. The ability to hot-add and hot-extend allows IT to increase the resources available to an application by provisioning additional CPU, memory and disk to the virtual machine without disrupting the application or the end users. Hot-add/extend of virtual disk is supported on all virtual machines. Hot-add of virtual CPU/memory is supported on any guest operating system that natively supports hot-add CPU/memory on a physical server. Microsoft Hyper-V R2 SP1 supports hot-add memory only with certain guests. Neither Microsoft nor Citrix supports hot-add virtual CPU or hot-extend disks.

16. Reduce Storage Costs – vSphere Storage Thin Provisioning with Comprehensive Alerts

VMware vSphere Storage Thin Provisioning lowers capital and operating expenditures by reducing storage needs and cutting the power and cooling costs of excess storage. Thin provisioning enables IT administrators to create virtual machines without needing to dedicate all the storage up front. When a virtual machine is created, the thin-provisioned disk only consumes what's needed. Then, the virtual disk grows over time when more storage space is required. Now with vSphere 5, thin provisioning (and other storage tasks) can be offloaded to arrays having their own integrated thin storage features that support the vSphere Storage APIs for Array Integration. vSphere Storage Thin Provisioning comes with comprehensive consumption-based monitoring and alerting. IT administrators can set alerts to trigger when they need to procure more storage or rebalance virtual machines across the available storage with Storage vMotion or Storage DRS. These monitoring and alerting capabilities prevent systems from accidentally running out of storage space. Microsoft Hyper-V R2 has thin provisioning of disks but lacks the built-in monitoring and alerting capabilities that make it safe to use.

17. Save Even More Energy – vSphere Distributed Power Management

vSphere Distributed Power Management (DPM) reduces datacenter energy consumption during nonpeak hours by consolidating workloads within a cluster and turning off unneeded servers. Think of it as cluster-wide power management. Whereas other offerings only focus on power savings for individual servers, DPM provides a holistic, cluster-wide approach to power savings that is built into vSphere. To conserve energy during periods of low utilization, such as evenings and weekends, DPM consolidates workloads and powers off unused host servers. When utilization is expected to increase before the next work day, DPM brings servers back online to ensure that service levels are met. Microsoft Hyper-V R2 has nothing comparable. The Core Parking feature in Hyper-V R2 achieves only minimal power savings, and the PRO Tips approach that requires complex integration with System Center Operations Manager does not work at the host cluster level and has been dropped from Microsoft's product roadmap. Power management with Citrix XenServer requires additional servers and lacks the affinity rules needed to control virtual machine placement.

18. Run the Operating Systems You Want – Broadest Guest OS Support, New vSphere Web Client and vCenter Server Appliance

VMware has always supported the broadest set of guest operating systems in the industry—including new and old versions of Windows, Linux, Solaris, Mac OS, NetWare, FreeBSD, OS/2 and more—so companies can virtualize their existing applications and maintain flexibility for future applications. In all, vSphere supports more than 80 guest operating systems or versions—more versions of Windows than even Microsoft Hyper-V R2 supports and more versions of Linux than Citrix XenServer supports. Unlike other hypervisors, vSphere 5 achieves full performance with unmodified guest operating systems without the need for paravirtualized guests that limit support options. vSphere 5 also gives more choice in platforms for management servers and clients with the new option of a Linux-based vCenter Server Appliance and the vSphere Web Client, which can run in any browser. Microsoft and Citrix support only thick Windows clients with their hypervisors and management servers, and even Red Hat KVM requires a Windows management server.

19. Leverage Built-In Network Adapter Failover and Load Balancing – Integrated NIC Teaming

vSphere provides built-in network-adapter failover and load balancing to each networked virtual machine, enabling greater hardware availability and fault tolerance in case of network-adapter failure. It works with any network adapter that vSphere supports. NIC teaming policies allow users to configure multiple active and standby adapters, and teaming configurations can vary per port groups on the same virtual switch and uplinks. Microsoft Hyper-V R2 still does not have integrated NIC teaming and relies instead on third-party network-adapter drivers for this functionality. This third-party approach is unsatisfactory because the drivers only work with network adapters from that same third party; it requires a separate installation; and it is unclear whether Microsoft or the third party provides support should an issue arise.

20. Use the Latest Hardware and Software with Your Virtual Machines – New vSphere 5 Virtual Device Support

Sometimes you need virtual machines that support the latest computing features, such as: 3D graphics for Windows Aero on virtual desktops; USB 3.0 devices for hardware testing and USB devices connected through the vSphere Client; smart-card readers for virtual desktop infrastructure in secure environments; or Mac OS X support for virtualizing on Apple server platforms. vSphere 5 adds those capabilities so enterprises can now virtualize even those more specialized cases that once required dedicated hardware. With Microsoft Hyper-V R2, features such as 3D support require expensive graphics cards on each host, and virtual machines do not have USB support. Mac OS X guest support in Hyper-V is missing as well. Citrix XenServer virtual machines have the same limitations. Enterprises embarking a program to virtualize 100 percent of desktop and server workloads will find that only vSphere 5 meets their requirements.



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

Copyright © 2011 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-RG-vSPHR5-COMPETITIVE-A4-102