VMware ESX and VMware ESXi

The Market Leading Production-Proven Hypervisors

AT A GLANCE

VMware® ESX® and VMware ESXi™ provide the foundation for building and managing a virtualized IT infrastructure. These market leading, production-proven hypervisors abstract processor, memory, storage and networking resources into multiple virtual machines that run unmodified operating systems and applications. VMware ESX and ESXi are the most widely deployed hypervisors, delivering the highest levels of reliability and performance to companies of all sizes.

BENEFITS

- Decrease hardware, power and cooling costs by running multiple operating systems on the same physical server.
- Lower management overhead costs by reducing the hardware footprint in the datacenter.
- Guarantee high levels of performance for the most resource-intensive applications.
- Consolidate hardware resources with the peace of mind that comes with the industry's most widely deployed, production-proven and secure server virtualization platform.

KEY FEATURES

- Record-setting performance with up to 8,900 database transactions per second, 200,000 I/O operations per second, and up to 16,000 Exchange mailboxes on a single physical host
- Up to eight-way virtual SMP (symmetric multiprocessing), enabling the virtualization of multiprocessor workloads
- Memory overcommittment and deduplication, allowing higher consolidation ratios
- Broadest OS support of any hypervisor, enabling IT to virtualize numerous versions of Windows®, Linux®, Solaris®, NetWare®, and other operating systems.
- Built-in high availability through NIC teaming and HBA multipathing to protect against hardware component failures
- Up to 64 logical processing cores, 256 virtual CPUs, and 1TB RAM per host, enabling higher consolidation ratios

What are VMware ESX and VMware ESXi?

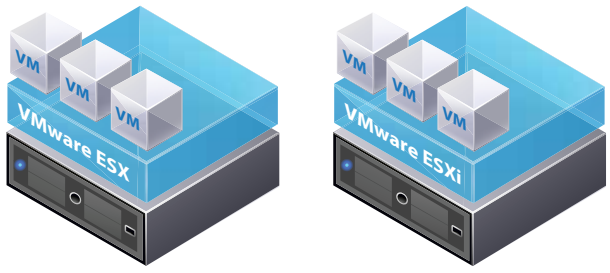
VMware ESX and VMware ESXi provide the foundation for building a reliable and dynamic IT infrastructure. These market-leading, production-proven hypervisors abstract processor, memory, storage and networking resources into multiple virtual machines that each can run an unmodified operating system and applications. VMware ESX and ESXi are the most widely deployed hypervisors, delivering the highest levels of reliability and performance to companies of all sizes.

VMware ESXi is the latest hypervisor architecture from VMware. It has an ultra-thin architecture with no reliance on a general-purpose OS, yet still offers all the same functionality and performance of VMware ESX. VMware ESXi sets a new bar for security and reliability because its smaller code base represents a smaller "attack surface" with less code to patch. This small footprint and hardware-like reliability also enable VMware ESXi to be built directly into industry standard x86 servers from leading server manufacturers such as Dell, IBM, HP, and Fujitsu-Siemens. VMware ESXi was designed with simplicity in mind. Its menu-driven startup and automatic configurations make it the easiest way to get started with VMware virtualization.

How are VMware ESX and VMware ESXi Used in the Enterprise?

VMware ESX and ESXi can be deployed as part of the VMware vSphere™ 4 platform or VMware View™ suite of products to enable centralized management and better quality of service to datacenter applications and enterprise desktops, enabling IT administrators to:

- Implement production server consolidation and containment. Contain server sprawl by running software applications in virtual machines on fewer physical servers.



VMware ESX and VMware ESXi virtualize server, storage and networking, allowing multiple applications to run in virtual machines on the same physical server.

- Provide advanced business continuity protection at lower cost. Ensure application availability during hardware failures or server and storage maintenance and upgrades.
- Manage and control centralized virtual desktops. Provide standardized enterprise desktop environments hosted in virtual machines that end users can access through thin clients or PCs.
- Streamline software development and testing. Consolidate disparate development, testing and staging environments involving multiple operating systems and multi-tier applications on the same hardware.
- Re-host legacy applications. Migrate legacy operating systems and software applications to virtual machines running on new hardware for better reliability.

VMware ESXi is also available as a free download for deployment as a single-server virtualization solution. IT administrators can use the freely available VMware vSphere™ Client to manage VMware ESXi to create and manage virtual machines.

How Do VMware ESX and VMware ESXi Work?

VMware ESX and VMware ESXi install directly on the server hardware, inserting a robust virtualization layer between the hardware and the operating system. VMware ESX and ESXi partition a physical server into multiple secure and portable virtual machines that can run side by side on the same physical server. Each virtual machine represents a complete system—with processors, memory, networking, storage and BIOS—so that an operating system and software applications can be installed and run in the virtual machine without any modification. Virtual machines are also completely isolated from each other by the virtualization layer, thus preventing a crash or configuration error in one virtual machine from affecting the others.

Sharing the physical server resources among a number of virtual machines increases hardware utilization and dramatically decreases capital costs. The bare-metal architecture gives VMware ESX and ESXi complete control over the server resources allocated to each virtual machine and provides for near-native virtual machine performance and enterprise-class scalability. VMware ESX and ESXi provide virtual machines with built-in high availability, resource management and security features to deliver improved service levels to software applications than static physical environments.

What is the difference between VMware ESX and VMware ESXi?

VMware ESX and VMware ESXi are both bare-metal hypervisors that install directly on the server hardware. Both provide industry-leading performance and scalability; the difference resides in the architecture and the operational management of VMware ESXi. VMware ESX relies on a Linux operating system, called the service console, to perform some management functions including executing scripts and installing third-party agents for hardware monitoring, backup or systems management. The service console has been removed from VMware ESXi, dramatically reducing its footprint. By removing the service console, VMware ESXi completes an ongoing trend of migrating management functionality from this local command-line interface to remote management tools. The functionally of the service console is replaced by remote command-line interfaces and adherence to system management standards.

Key Features of VMware ESX and VMware ESXi

Summary of Key New Features

- **64-bit architecture.**
  Benefit from improved performance and support for up to 1TB RAM on physical hosts.
- **Performance optimizations for virtualized workloads.**
  VMware ESX and ESXi 4.0 have undergone performance optimizations for specific business-critical applications such as Oracle Database, Microsoft SQL Server, and Microsoft Exchange. Get up to 8,900 database transactions per second, 200,000 I/O operations per second, and up to 16,000 Exchange mailboxes per host.
- **Performance improvements for iSCSI storage.**
  Leverage a combination of new in-guest virtualization-optimized SCSI drivers and VMkernel-level storage stack optimizations to dramatically improve performance for I/O-intensive applications such as databases and messaging applications.
- **Support for larger virtual machines and powerful server hardware.**
  Take advantage of hardware systems with up to 64 physical CPU cores, 256 virtual CPUs, 1TB RAM, and up to hundreds of virtual machines on a single host to facilitate large-scale consolidation and disaster recovery projects. Configure virtual machines with as much as 255GB RAM.
- **Support for eight-way virtual SMP.**
  VMware Virtual Symmetric Multiprocessing (SMP) enhances virtual machine performance by enabling a single virtual machine to use up to eight physical processors, simultaneously. VMware Virtual SMP enables virtualization of the most CPU-intensive enterprise applications such as databases, ERP and CRM.
- **VMware VMsafe™.**
  VMware VMsafe is a new security technology that helps protect virtualized workloads in ways previously not possible with physical machines. VMsafe provides a set of security APIs that enable third-party security products to gain the same visibility as VMware ESX or ESXi into the operation of a virtual machine

to identify and eliminate malware, such as viruses, trojans and key-loggers. This advanced protection is achieved by granular visibility into the virtual machine's hardware resources such as memory, CPU and disk and its I/O systems.

- **VMDirectPath for virtual machines.**
  Enhance CPU efficiency for applications that require frequent access to I/O devices by allowing select virtual machines to directly access underlying hardware devices.

- **Improved power management.**
  Improve energy efficiency with dynamic voltage and frequency scaling and support for Intel SpeedStep® and AMD PowerNow!.

Architecture

- **Bare-metal, 64-bit hypervisor architecture.**
  Achieve near-native virtual machine performance, reliability and scalability with production-proven hypervisor technology that runs directly on server hardware, without the need for a host operating system.

- **Virtual disk files.**
  Use virtual machine disk (VMDK) files to provide virtual machines access to their own private datastores while giving IT administrators the flexibility to create, manage and migrate virtual machine storage as separate, self-contained files that can reside on shared storage equipment.

- **VMware vStorage VMFS.**
  Eliminate single points of failure and balance storage resources by implementing shared storage for virtual machines with VMware vStorage Virtual Machine File System ("VMFS"), a cluster file system that allows multiple VMware ESX hosts to access a single VMDK file concurrently. VMFS is supported on a mix of Fibre Channel SAN, iSCSI SAN, and NAS storage arrays in a manner that is transparent to application owners and end users. Download the VMFS datasheet to learn more about VMFS, which provides new enhancements such as dynamic increase of VMFS volume size.

- **Boot from SAN.**
  Eliminate the need to separately backup local attached server disks by running VMware ESX hosts on diskless configurations of blade and rack mount servers.

- **Virtual networking.**
  The virtual networking capabilities in VMware ESX and ESXi allow customers to build complex networks between virtual machines residing on a single host or across multiple installations of VMware ESX and ESXi hosts for production deployments or development and testing purposes. Configure each virtual machine with one or more virtual NIC, each with its own IP and MAC address, to make virtual machines indistinguishable from physical machines. Create a simulated network within a VMware ESX host with virtual switches that connect virtual machines. Use virtual LANs (VLANs) to overlay a logical LAN on top of physical LANs to isolate network traffic for security and load segregation. Modify network configurations without having to change actual cabling and switch setups.

Advanced Resource Management

VMware ESX offers advanced resource management capabilities to improve performance and increase consolidation ratios.

- **Resource management for virtual machines.**
  Define advanced resource allocation policies for virtual machines to improve service levels to software applications. Establish minimum, maximum and proportional resource shares for CPU, memory, disk and network bandwidth. Modify allocations while virtual machines are running.

- **Intelligent CPU virtualization.**
  Manage the execution of virtual machine processes with intelligent process scheduling and load balancing across all available CPUs on the physical host.

- **RAM overcommitment.**
  Increase memory utilization by configuring virtual machine memory that safely exceeds the physical server memory, enabling a greater number of virtual machines to run on a VMware ESX or ESXi host.

- **Transparent page sharing (memory de-duplication).**
  Use physical RAM more efficiently by storing memory pages identical across multiple virtual machines only once.

- **Memory ballooning.**
  Shift RAM dynamically from idle virtual machines to active workloads. Memory ballooning artificially induces memory pressure within idle virtual machines, forcing them to use their own paging areas and release memory for active virtual machines.

- **Network traffic shaping.**
  Ensure that critical virtual machines receive priority access to network bandwidth. Network traffic from virtual machines can be prioritized on a "fair share" basis. Network Traffic Shaper manages virtual machine network traffic to meet peak bandwidth, average bandwidth and burst size constraints.

- **Storage I/O traffic prioritization.**
  Ensure that critical virtual machines receive priority access to storage devices by prioritizing I/O traffic on a "fair share" basis.

- **Improved power management.**
  Improve energy efficiency with dynamic voltage and frequency scaling and support for Intel SpeedStep® and AMD PowerNow!.

Performance and Scalability

VMware ESX and VMware ESXi deliver unparalleled performance and scalability, enabling even the most resource intensive production applications to be virtualized.

- **Performance optimizations for virtualized workloads.** VMware ESX and ESXi 4.0 have undergone performance optimizations for specific business-critical applications such as Oracle databases, Microsoft SQL Server, and Microsoft Exchange. Get up to 8,900 database transactions per second, 200,000 I/O operations per second, and up to 16,000 Exchange mailboxes per host.
- **Performance improvements for iSCSI storage.** Leverage a combination of new in-guest virtualization-optimized SCSI drivers and VMkernel-level storage stack optimizations to dramatically increase performance for I/O-intensive applications such as databases and messaging applications.
- **Support for powerful server hardware.** Take advantage of hardware systems with up to 64 physical CPU cores, 256 virtual CPUs, 1TB RAM, and up to hundreds of virtual machines on a single host to facilitate large-scale consolidation and disaster recovery projects.
- **Support for larger virtual machines.** Configure virtual machines with as much as 255GB RAM.
- **Support for eight-way virtual SMP.** VMware Virtual Symmetric Multiprocessing (SMP) enhances virtual machine performance by enabling a single virtual machine to use up to eight physical processors, simultaneously. VMware Virtual SMP enables virtualization of the most CPU-intensive enterprise applications such as databases, ERP and CRM.
- **Raw device mapping.** Optionally, map SAN LUNs directly to a virtual machine in order to enable application clustering and array-based snapshot technology while profiting from the manageability benefits of VMware vStorage VMFS.
- **Support for hardware virtualization.** VMware ESX and ESXi provide industry-leading support for next-generation virtualization hardware assist technologies such as AMD's Rapid Virtualization Indexing® or Intel's Extended Page Tables.
- **Support for large memory pages.** VMware ESX and ESXi are the only hypervisors that support large memory pages to improve efficiency of memory access for guest operating systems.
- **Networking performance optimizations.** VMware ESX and ESXi support a variety of performance offload technologies including TCP Segmentation Offloading (TSO), VLAN and checksum offloading, and jumbo frames to reduce the CPU overhead associated with processing network I/O. Additionally, virtualization optimized I/O performance features such as NetQueue is supported which significantly improves performance in 10 Gigabit Ethernet virtualized environments.
- **Support for new high performance devices and protocols.** VMware ESX and ESXi support 10Gb Ethernet network cards and storage arrays and Infiniband technology to improve virtual machine performance.
- **Support for paravirtualization.** VMware ESX and ESXi support para-virtualized Linux guest operating systems (Linux kernel 2.6.21 onwards) to improve virtual machine performance.
- **VMDirectPath I/O for virtual machines.** Enhance CPU efficiency for applications that require frequent access to I/O devices by allowing select virtual machines to directly access underlying hardware devices. Other virtualization features, such as VMware VMotion™, hardware independence and sharing of physical I/O devices will not be available to the virtual machines using this feature.

High Availability

VMware ESX delivers datacenter-class high availability for virtual machines.

- **Built-in storage access multipathing.** Ensure shared storage availability with SAN multipathing for Fibre Channel or iSCSI SAN.
- **NIC teaming.** Give each networked virtual machine built-in NIC failover and load balancing enabling greater hardware availability and fault tolerance. NIC teaming policies allow users to configure multiple active and standby adapters.
- **Support for Microsoft Clustering Services.** Cluster virtual machines running Microsoft Windows operating system across physical hosts.

Interoperability

VMware ESX and VMware ESXi are optimized, rigorously tested and certified across the complete IT stack of servers, storage, operating systems, and software applications allowing for enterprise-wide standardization.

- **Server hardware.** VMware ESX and ESXi have been certified with industry-leading rack, tower and blade servers from Dell, Fujitsu Siemens, HP, IBM, NEC, Sun Microsystems and Unisys.
- **Storage hardware.** VMware ESX and ESXi are certified with a wide range of storage systems from Dell, EMC, Fujitsu, Fujitsu Siemens, HP, Hitachi Data Systems, IBM, NEC, Network Appliance, StorageTek, Sun Microsystems and 3PAR. Internal SATA drives, Direct Attached Storage (DAS), Network Attached Storage (NAS) and both fibre channel SAN and iSCSI SAN are supported.

- **Operating systems.**
  VMware ESX and ESXi support the broadest range of unmodified operating systems, including Windows, Linux, Solaris, Novell NetWare and more. VMware recently added support for 20 new guest operating systems.
- **Software applications.**
  Run any software application in VMware virtual machines without the need to modify the application.
- **Virtual machine formats.**
  VMware ESX and ESXi can run virtual machines created in non-VMware formats. Using the free VMware vCenter Converter, users can convert and run Microsoft Virtual Server and Virtual PC, and Symantec LiveState Recovery virtual machines on VMware ESX and ESXi hosts.

Security
Advanced security features in VMware ESX and ESXi protect stored data within the virtual environment.

- **VMware VMsafe™.**
  VMware VMsafe is a new security technology that helps protect virtualized workloads in ways previously not possible with physical machines. VMsafe provides a set of security APIs that enable third-party security products to gain the same visibility as VMware ESX or ESXi into the operation of a virtual machine to identify and eliminate malware, such as viruses, trojans and key-loggers. This advanced protection is achieved by fine-grained visibility into the virtual machine's hardware resources such as memory, CPU and disk and its I/O systems.
- **VMkernel Protection.**
  VMware ESX and ESXi are protected from common attacks and exploits by assuring the integrity of the VMkernel, a core component of the hypervisor. Disk integrity techniques in ESX and ESXi protect the boot-up of the hypervisor by utilizing the Trusted Platform Module (TPM), a hardware device embedded in servers. VMkernel modules that load onto disk and memory are digitally signed and validated during load to ensure the authenticity and integrity of dynamically loaded code and protect against malware attempting to modify VMkernel as it persists on disk. VMKernel also uses memory integrity techniques at load-time coupled with microprocessor capabilities to protect itself from common buffer-overflow attacks used to exploit running code.
- **Encryption.**
  Ensure secure connection to VMware ESX and ESXi hosts with SSL encryption.
- **Enable authentication for iSCSI Devices.**
  VMware ESX and ESXi secure iSCSI devices from unwanted intrusion by requiring that either the host or the iSCSI initiator be authenticated by the iSCSI device or target whenever the host attempts to access data on the target LUN.
- **Network Security Policies.**
  Enforce security for virtual machines at the Ethernet layer. Disallow promiscuous mode sniffing of network traffic, MAC address changes and forged source MAC transmits.

Manageability
Several management interfaces are available to more efficiently manage VMware ESX and ESXi environments. The core management interfaces used by VMware ESX and ESXi administrators are:

- **VMware vSphere™ Client.**
  Manage VMware ESX or ESXi hosts, virtual machines and (optionally) VMware vCenter Server with the common user interface of the VMware vSphere Client. The vSphere Client is available as a free download and can be pointed at a VMware ESX or ESXi host for single host management, or it can be pointed at VMware vCenter™ Server for multi-host management.
- **VMware vCenter Server.**
  Enable centralized management for VMware ESX and ESXi hosts and their virtual machines. To manage an ESX or ESXi host with VMware vCenter Server, a VMware vCenter Agent license, included in all editions of VMware vSphere™, is required for that host. VMware vSphere includes many more management capabilities that improve business continuity and maximize operational efficiency such as live migration, automatic load balancing, protection against hardware failures, and virtual machine back up and restore capabilities.

Additional management tools for VMware ESX and ESXi include:

- **VMware vSphere™ Command-Line Interface 4.0 (vCLI).**
  Manage VMware ESX and ESXi through a remote execution environment. The latest version of vCLI has a number of new commands and is supported on both VMware ESX 4.0 and VMware ESXi 4.0. See the vSphere Command-Line Interface Installation and Reference Guide <http://communities.vmware.com/docs/DOC-9247>.
- **VMware vSphere™ Power Command-Line Interface 4.0 (PowerCLI).**
  Manage and configure thousands of Virtual Machines with this powerful yet easy to use interface that is based on Microsoft PowerShell technology. PowerCLI allows IT administrators to manage VMware ESX or ESXi through a scripting interface managing the same tasks done with the VMware vSphere Client.
- **VMware vSphere™ Management Assistant.**
  The VMware vSphere Management Assistant is a virtual machine that includes a VMware vSphere command-line interface and other prepackaged software that developers and administrators can use to run agents and scripts to manage VMware ESX and ESXi hosts.

- **Agent-less Hardware Management with CIM.** Common Information Model (CIM) provides a protocol for monitoring hardware health and status through VMware vCenter Server or CIM-compatible third-party tools.

Find Out More

How Can I Purchase VMware ESX and VMware ESXi?
VMware ESX and ESXi are included in all editions of VMware vSphere™. To try a free 60-day evaluation of VMware vSphere or for more information on how to purchase VMware vSphere visit the How to Buy page at http://www.vmware.com/go/vsphere.

The standalone version of VMware ESXi is also available as a free download at http://www.vmware.com/go/esxi.

Product Specifications and System Requirements
For detailed product specifications and system requirements, refer to the VMware ESX or VMware ESXi hardware compatibility guide at http://www.vmware.com/resources/compatibility/.

For information or to purchase VMware products, call 1-877-4VMWARE (outside of North America dial +1-650-427-5000), visit www.vmware.com/products, or search online for an authorized reseller.

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