Contents

1. Brief History of Virtualization ................................................................. 5
  1.1 What is Virtualization? ................................................................. 5
  1.2 Hypervisor ................................................................................. 6
  1.3 Reasons to Use Virtualization .................................................... 8
  1.4 A Short History of VMware and Product Overview ................. 10
  1.5 Overview of VMware’s Offerings ............................................. 10
  1.6 Storage Virtualization ............................................................... 10
  1.7 vCloud and Operations Management ....................................... 10
  1.8 Network Virtualization ............................................................. 11
  1.9 Storage, Virtual Desktops and Data Center Management ........ 11

2. Virtualization Infrastructure .............................................................. 12
  2.1 VMware Virtualization Software ............................................ 12
  2.2 VMware vSphere Components .............................................. 12
  2.3 VMware Infrastructure Diagram .......................................... 13
  2.4 VMware vSphere Application Services .................................. 15
  2.5 VMware VMotion ................................................................ 16
  2.6 VMware DRS ......................................................................... 16
  2.7 VMware HA .......................................................................... 17
  2.8 Automation Software Virtualization Architecture .................. 18

3. Implementing a Virtualized GE Automation Architecture ............... 19
  3.1 Number of Servers .................................................................. 19
  3.2 CPU Calculations .................................................................... 19
  3.3 ESXi & Automation Application Hardware Requirements for Small Size Architecture ...... 20
  3.4 ESXi & Automation Application Hardware Requirements for Medium Size Architecture ....... 22
  3.5 ESXi & Automation Application Hardware Requirements for Large Size Architecture ...... 24
  3.6 ESXi 5.5 Installation Requirements ....................................... 26
  3.7 Storage Systems ..................................................................... 27
  3.8 ESXi Booting Requirements ................................................... 27
  3.9 Storage Requirements for ESXi 5.5 Installation ....................... 28
  3.10 Solid State Storage ................................................................. 28
  3.11 Installing ESXi ...................................................................... 28
3.12 Interactive ESXi Installation .................................................................29
3.13 Install ESXi Interactively ........................................................................30
3.14 Procedure ...............................................................................................31
3.15 ESXi Autoconfiguration ............................................................................31
3.16 Configuring Network Settings .................................................................31
3.17 ESXi Networking Security Recommendations ........................................32
3.18 After You Install and Set Up ESXi ..........................................................32

4. Implementing High Availability (HA) with vSphere ..................................33
4.1 Datacenter(s) ..........................................................................................33
4.2 VMware DRS .........................................................................................33
4.3 Creating a Datacenter ..............................................................................34
4.4 Adding a Host to a Datacenter .................................................................34
4.5 Creating a vSphere HA Cluster ...............................................................35
4.6 Create a Failover Cluster .........................................................................35
4.7 DataStores ..............................................................................................36
4.8 Solid State Storage ..................................................................................36
4.9 Creating a Datastore ...............................................................................37
4.10 Configuring Networks ...........................................................................39
4.11 Creating a Virtual Machine in the vSphere Client ....................................40
4.12 Creating a Virtual Machine in vSphere Client .........................................41
4.13 To configure virtual machine properties .................................................42
4.14 Enabling vMotion for Migration ............................................................42
4.15 To enable vMotion for migration ............................................................43

5. VMware Best Practices .............................................................................44

6. Troubleshoot and Enhance Performance ..................................................45
6.1 Solutions for Consistently High CPU Usage ............................................46
6.2 Solutions for Memory Performance Problems ........................................47
6.3 Solutions for Storage Performance Problems .........................................48
6.4 Solutions for Disk Performance Problems ..............................................49
6.5 Solutions for Poor Network Performance ...............................................51

7. Glossary ....................................................................................................53
1. Brief History of Virtualization

The concept of virtualization is generally believed to have its origins in the mainframe days in the late 1960s and early 1970s, when IBM invested a lot of time and effort in developing robust time-sharing solutions. Time-sharing refers to the shared usage of computer resources among a large group of users, aiming to increase the efficiency of both the users and the expensive computer resources they share. This model represented a major breakthrough in computer technology: the cost of providing computing capability dropped considerably and it became possible for organizations, and even individuals, to use a computer without actually owning one. Similar reasons are driving virtualization for industry standard computing today: the capacity in a single server is so large that it is almost impossible for most workloads to effectively use it. The best way to improve resource utilization, and at the same time simplify data center management, is through virtualization.

1.1 What is Virtualization?

Simply put, it’s the process of creating a virtual, rather than physical, version of something. Virtualization can apply to computers, operating systems, storage devices, applications, or networks. However, server virtualization is at the heart of it.

IT organizations are challenged by the limitations of today’s x86 servers, which are designed to run just one operating system and application at a time. As a result, even small data centers have to deploy many servers, each operating at just 5 to 15 percent of capacity—highly inefficient by any standard.

Virtualization uses software to simulate the existence of hardware and create a virtual computer system. Doing this allows businesses to run more than one virtual system – and multiple operating systems and applications – on a single server. This can provide economies of scale and greater efficiency.

A virtual computer system is known as "virtual machine" (VM) is a tightly isolated software container with an operating system and application inside. Each self-contained VM is completely independent.

Putting multiple VMs on a single computer enables several operating systems and applications to run on just one physical server, or “host”.

A thin layer of software called a hypervisor decouples the virtual machines from the host and dynamically allocates computing resources to each virtual machine as needed.

Virtualization can increase IT agility, flexibility, and scalability while creating significant cost savings. Workloads get deployed faster, performance and availability increases and operations become automated, resulting in IT that’s simpler to manage and less costly to own and operate.
VMs have the following characteristics, which offer several benefits.

- Partitioning
- Run multiple operating systems on one physical machine
- Divide system resources between virtual machines
- Isolation
- Provide fault and security isolation at the hardware level
- Preserve performance with advanced resource controls

Data centers today use virtualization techniques to make abstraction of the physical hardware, create large aggregated pools of logical resources consisting of CPUs, memory, disks, file storage, applications, networking, and offer those resources to users or customers in the form of agile, scalable, consolidated virtual machines. Even though the technology and use cases have evolved, the core meaning of virtualization remains the same: to enable a computing environment to run multiple independent systems at the same time.

### 1.2 Hypervisor

If virtualization is defined as enabling multiple operating systems to run on a single host computer, then the essential component in the virtualization stack is the hypervisor. This hypervisor, also called Virtual Machine Monitor (VMM), creates a virtual platform on the host computer, on top of which multiple guest operating systems are executed and monitored. This way, multiple operating systems, which are either multiple instances of the same operating system, or different operating systems, can share the hardware resources offered by the host.

Hypervisors are commonly classified as Bare Metal (Native) or Hosted.
Native hypervisors are software systems that run directly on the host’s hardware to control the hardware, and to monitor the guest operating systems. Consequently, the guest operating system runs on a separate level above the hypervisor. Examples of this classic implementation of virtual machine architecture are Oracle VM, Microsoft Hyper-V, VMware ESX and Xen.

Hosted hypervisors are designed to run within a traditional operating system. In other words, a hosted hypervisor adds a distinct software layer on top of the host operating system, and the guest operating system becomes a third software level above the hardware. A well-known example of a hosted hypervisor is Oracle VM VirtualBox. Others include VMware Server and Workstation, Microsoft Virtual PC, KVM, QEMU and Parallels.
## 1.3 Reasons to Use Virtualization

There are many different good reasons for companies and organizations to invest in virtualization today, but it is probably safe to assume that financial motivation is number one on the list: virtualization can save a lot of money. Below is an overview of the key benefits of virtualization.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource optimization</strong></td>
<td>Today’s enterprise level computer resources are so powerful that they often have excess capacity. By virtualizing the hardware and allocating parts of it based on the real needs of users and applications, the available computing power, storage space and network bandwidth can be used much more effectively. Computers no longer need to be idle or performing below their capabilities because there are fewer connected users, or because the hosted application happens to be less demanding than the server can handle. Virtual machines offer software developers isolated, constrained, test environments. Rather than purchasing dedicated physical hardware, virtual machines can be created on the existing hardware. Because each virtual machine is independent and isolated from all the other servers, programmers can run software without having to worry about affecting other applications, or external components affecting the execution of their code.</td>
</tr>
<tr>
<td><strong>Consolidation</strong></td>
<td>It is common practice to dedicate individual computers to a single application. If several applications only use a small amount of processing power, the administrator can consolidate several computers into one server running multiple virtual environments. For organizations that own hundreds or thousands of servers, consolidation can dramatically reduce the need for floor space, HVAC, A/C power, and co-location resources. This means the cost of ownership is reduced significantly, since less physical servers and floor and rack space are required, which in turn leads to less heat and power consumption, and ultimately a smaller carbon footprint.</td>
</tr>
<tr>
<td><strong>Maximizing Uptime</strong></td>
<td>Agility is all about being able to respond to changing requirements as quickly and flexibly as possible. Virtualization brings new opportunities to data center administration, allowing users to enjoy: Guaranteed uptime of servers and applications; speedy disaster recovery if large scale failures do occur. Instant deployment of new virtual machines or even aggregated pools of virtual machines via template images. Elasticity, that is, resource provisioning when and where required instead of keeping the entire data center in an always-on state. Reconfiguration of running computing environments without impacting the users.</td>
</tr>
</tbody>
</table>

![GE Digital Logo](image-url)
| Automatically Protect Applications from Server Failure | Server virtualization provides a way to implement redundancy without purchasing additional hardware. Redundancy, in the sense of running the same application on multiple servers, is a safety measure: if for any reason a server fails, another server running the same application takes over, thereby minimizing the interruption in service. This kind of redundancy works in two ways when applied to virtual machines:

- If one virtual system fails, another virtual system takes over.
- By running the redundant virtual machines on separate physical hardware you can also provide better protection against physical hardware failure. |

| Easily Migrate Workloads as Needs Change | Migration refers to moving a server environment from one place to another. With most virtualization solutions it is possible to move a virtual machine from one physical machine in the environment to another. With physical servers this was originally possible only if both physical machines ran on the same hardware, operating system and processor. In the virtual world, a server can be migrated between physical hosts with entirely different hardware configurations. Migration is typically used to improve reliability and availability: in case of hardware failure the guest system can be moved to a healthy server with limited downtime, if any. It is also useful if a virtual machine needs to scale beyond the physical capabilities of the current host and must be relocated to physical hardware with better performance. |

| Protect Investment in Existing, Legacy Systems | Server hardware will eventually become obsolete, and switching from one system to another can be difficult. In order to continue offering the services provided by these legacy systems, you can run it as a virtual machine on new, modern hardware, while the legacy system itself still behaves as if it were running on the same legacy hardware. From an application perspective, nothing has changed. In fact, its performance may well benefit from the newer underlying hardware. This gives the organization the time to transition to new processes without worrying about hardware issues, particularly in situations where the manufacturer of the legacy hardware no longer exists or cannot fix broken equipment. |
1.4 A Short History of VMware and Product Overview

VMware is one of the biggest names in the cloud and virtualization industry with all of the Fortune 100 companies relying on its services to some extent. It also ranked as one of the fastest growing companies with revenues of almost $6 billion up by 30% compared to the year before. It was founded in 1998 by the husband wife combo of Diane Greene and Mendel Rosenblum as well as Scott Devine, Edward Wang, and Edouard Bugnion.

1.5 Overview of VMware’s Offerings

We can segment VMware’s products by platform or functionality. Going by platform for example, they offer VMware Workstation and VMware Player for the desktop and VMware ESXi for servers. But I think it makes more sense to segment by functionality instead. Going by this, VMware’s lineup falls into the following categories:

- Hardware Virtualization
- Virtualized Hardware Management
- Network Virtualization
- Cloud Management Software
- Desktop Virtualization

1.6 Storage Virtualization

There are a number of other products, but some feel that VMware is trying to consolidate with the launch of Pivotal – a new organization – in collaboration with EMC to transfer key cloud application and big data services.

VMware’s roots were in hardware virtualization with the launch of VMware Workstation in 1999. Two years later in 2001 they released their ESX and GSX hypervisors. While there’s some similarity in functionality between VMware workstation and these two new offerings, they target very different scenarios. While GSX required a host OS, ESX ran directly on the server hardware – what is known as a “bare metal” hypervisor. VMware GSX has since been retired but the ESX line is now renamed ESXi with some important architectural differences.

1.7 vCloud and Operations Management

Some of the products and terminologies used can be confusing for those still trying to wrap their heads around the full range of products VMware has. For instance, one of the most prominent packages is called vSphere, which is actually a collection of various individual products like ESXi, vCenter, etc. If you’re trying to build a private cloud, then the consolidated package called vCloud bundles together various components like vSphere, vCenter Site Recovery Manager, vCenter Operations Manager Suite, vCloud Networking and Security, vCloud Director, and vCloud Automation Center.

While vSphere itself allows you to consolidate your hardware and run virtual machines, it becomes more and more difficult to manage as your demands increase. This is where vSphere with Operations Management comes in. It allows you to manage multiple vSphere installations and obtain detailed analytics into what resources they’re using allowing you to squeeze out even greater efficiency.
1.8 Network Virtualization

VMware’s NSX on the other hand allows for the virtualization of network resources much like vSphere does with server hardware allowing you to configure new networks on the fly within seconds without having to modify any underlying networking hardware. The logic of the network is already built into the vSphere hypervisors so no additional resources or modifications are necessary.

1.9 Storage, Virtual Desktops and Data Center Management

VMware covers the entire gamut of services including storage virtualizations, desktop virtualization and all the tools necessary to manage a datacenter. There are far too many products to give even a broad overview of them all over here. Please visit the VMware website for more information about these capabilities at www.vmware.com.
2. Virtualization Infrastructure

A complete VMware vSphere virtual solution consists of both virtualization software and hardware components. This section will highlight key software products and features in addition to physical hardware.

2.1 VMware Virtualization Software

A VMware vSphere solution is comprised of a number of different components and services (depicted in below), which comprise the software platform that runs on the hardware to enable the virtualized system. ESXi is an infrastructure service, a hypervisor or basically a thin OS, that runs directly on the hardware. This is called a “bare-metal” design since there is no dependence on a general purpose operating system.

2.2 VMware vSphere Components

<table>
<thead>
<tr>
<th>vSphere Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESXi</td>
<td>A virtualization layer run on physical servers that abstracts processor, memory, storage, and resources into multiple virtual machines</td>
</tr>
<tr>
<td>VMware vCenter Server</td>
<td>The central point for configuring, provisioning, and managing virtualized environments. It provides essential datacenter services such as access control, performance monitoring, and alarm management.</td>
</tr>
<tr>
<td>VMware vSphere Client</td>
<td>An interface that enables users to connect remotely to vCenter Server on ESXi from any Windows PC</td>
</tr>
<tr>
<td>VMware View</td>
<td>Virtual Desktop Infrastructure management software that provides services for managing the access of Virtual Machines through thin-client technologies.</td>
</tr>
</tbody>
</table>
2.3 VMware Infrastructure Diagram

There are a number of application services that makeup a complete solution. Listed below are some of the key services offered in the VMware different editions offered.

VMware vSphere Essentials Kit
Delivers the industry-leading virtualization platform for small businesses at an affordable price. Small businesses can virtualize their physical servers and centrally manage these servers, reducing hardware costs and increasing operating efficiency with a low upfront investment.

Licensed Per Kit – Up to 3 Servers, 2 Processors
Includes vCenter Server Essentials & vSphere Hypervisor
VMware vSphere Essentials Plus Kit
Provides an all-in-one solution for small businesses to virtualize their physical servers and reduce hardware costs while ensuring superior high application availability and data protection.
Licensed Per Kit – Up to 3 Servers, 2 Processors
Includes vCenter Server Essentials, vSphere Hypervisor, vMotion, High Availability, Data Protection, vShield Endpoint, & vSphere Replication

VMware vSphere Standard
Provides an entry solution for basic consolidation of applications to slash hardware costs while accelerating application deployment.
Licensed Per Processor
Includes vCenter Server Standard, vSphere Hypervisor, vMotion, HA, 2 vCPU FT, Data Protection, vShield Endpoint, & vSphere Replication, Hot Add, and more!

VMware vSphere Enterprise
Provides key features for maintaining service level guarantees including minimizing downtime, protecting data, and automating resource management.
Licensed Per Processor
Includes vCenter Server Standard, vSphere Hypervisor, vMotion, HA, 2 vCPU FT, Data Protection, vShield Endpoint, & vSphere Replication, Hot Add, DRS, DPM, and more!

VMware vSphere Enterprise Plus
Includes the full range of vSphere features for transforming datacenters into dramatically simplified cloud computing environments providing the next generation of flexible, reliable IT services.
Licensed Per Processor
Includes vCenter Server Standard, vSphere Hypervisor, vMotion, HA, 4 vCPU FT, Data Protection, vShield Endpoint, & vSphere Replication, Hot Add, DRS, DPM, Advanced I/O Control, Profiles & Auto Deploy, Cloud API Integration and more!
### 2.4 VMware vSphere Application Services

<table>
<thead>
<tr>
<th>Key Application Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere vMotion</td>
<td>Enables the migration of powered-on virtual machines from one physical server to another with zero down time, continuous service availability, and complete transaction integrity. Migration with vMotion cannot be used to move virtual machines from one datacenter to another.</td>
</tr>
<tr>
<td>vSphere Storage vMotion</td>
<td>Enables the migration of virtual machine files from one datastore to another without service interruptions. The virtual machine remains on the same host during Storage vMotion. Migration with Storage vMotion lets users move the virtual disk or configuration file of a virtual machine to a new datastore while the virtual machine is running. Migration with Storage vMotion enables you to move a virtual machines storage without any interruption in the availability of the virtual Machine.</td>
</tr>
<tr>
<td>vSphere High Availability (HA)</td>
<td>A feature that provides high availability for virtual machines. If a server fails, affected virtual machines are restarted on other available servers that have spare capacity.</td>
</tr>
<tr>
<td>vSphere Fault Tolerance (FT)</td>
<td>Provides continuous availability by protecting a virtual machine with a copy. When this feature is enabled for a virtual machine, a secondary copy of the original, or primary, virtual machine is created. All actions completed on the primary virtual machine are also applied to the secondary virtual machine. If the primary virtual machine becomes unavailable, the secondary machine becomes immediately active.</td>
</tr>
<tr>
<td>Distributed Resource Scheduler (DRS)</td>
<td>Allocates and balances computing capacity dynamically across collections of hardware resources for virtual machines. This feature allows users to define rules helping prevent specific VM’s from inhabiting the same physical host.</td>
</tr>
</tbody>
</table>

VMware VMotion, VMware DRS and VMware HA are distributed services that enable efficient, automated resource management and high virtual machine availability.
2.5 VMware VMotion

As mentioned earlier, virtual machines run on and consume resources from individual physical x86 servers through VMware ESX Server. VMotion enables the migration of running virtual machine from one physical server to another without service interruption as shown below. This allows virtual machines to move from a heavily loaded server to a lightly loaded one. The effect is a more efficient assignment of resources. Hence, with VMotion, resources can be dynamically reallocated to virtual machines across physical servers.

2.6 VMware DRS

Taking the VMotion capability one step further by adding an intelligent scheduler, VMware enables the system administrator to set resource assignment policies that reflect business needs and let VMware DRS do the calculation and automatically handle the detailed physical resource assignments. VMware DRS dynamically monitors the workload of the running virtual machines and the resource utilization of the physical servers within a Cluster.

It checks those results against the resource assignment policies, if there is a potential for violation or improvement, it utilizes VMotion and dynamically reassigns virtual machines to different physical servers, as shown below, to ensure that the policies are complied with and resource allocation is optimal. If a new physical server is made available, VMware DRS automatically redistributes the virtual machines to take advantage of it. Conversely, if a physical server needs to be taken down for any reason, VMware DRS redistributes its virtual machines to other servers automatically. For more information, see the VMware DRS white paper.
2.7 VMware HA

VMware HA offers a simple and low cost high availability alternative to application clustering. It enables quick restart of virtual machines on a different physical server within a Cluster automatically should the hosting server fail. All applications within the virtual machines will benefit from high availability, not just one as with application clustering. VMware HA works by placing an agent on each physical server to maintain a “heartbeat” with the other servers in the Cluster. As shown below, loss of a “heartbeat” from one server automatically initiates the restarting of all affected virtual machines on other servers. Setting up VMware HA can be done simply by designating the priority order of virtual machines to be restarted in the Cluster. This is very simple when compared to the set up and configuration effort required for application clustering. Furthermore, even though VMware HA requires a certain amount of non-reserved resources to be maintained at all times to ensure that the remaining live servers can handle the total workload, it does not require doubling the amount of resources like application clustering. For more information, see the VMware HA whitepaper.
This architecture still applies the core infrastructure components discussed earlier but illustrates that it can be applied to not just an Enterprise Network but also a control network for Automation needs.
3. Implementing a Virtualized GE Automation Architecture

The following details are offered to help you setup & implement VMware ESXi 5.0 (and greater).
Please refer to the GE documentation for more information on Hardware & Software Specifications.
For general procedures on install guides, architectural overviews relating to virtualization in general, refer to the support team and documents located on VMware’s website at http://www.vmware.com.

3.1 Number of Servers

The minimum number of servers recommended for systems making use ESXi is 1 (a host machine with at least two cores).

The minimum number of servers recommended for systems making use of VMware FT or HA is 3. In the event that one server fails, the system will remain in a protected state across the remaining two servers. This also provides opportunities for one server to be taken offline for maintenance while maintaining protection. In both of these scenarios, the sizing of the servers must take into consideration that two servers must be sized to provide resources for the full system.

VMware limits the number of VM’s that can be VMware FT protected to 4 per server or 8 FT protected vCPUs per host, whichever limit is reached first.

If additional machines require FT protection, additional servers will need to be taken into consideration.

When purchasing hardware, take into consideration future expansion plans by possibly adding an additional 20-30% of resources. VMware makes it very simple to scale the system size upward by adding servers in the future to provide additional resources.

3.2 CPU Calculations

Virtual Machines are always limited by the megahertz capability of the physical core. A common misconception is that a VM can utilize as much CPU megahertz as needed from the combined total available. A single vCPU VM can never use more megahertz than the maximum of one CPU/core. If a VM has 2 vCPUs, it can never use more megahertz than the maximum of each CPU/core.
3.3  ESXi & Automation Application Hardware Requirements for Small Size Architecture

* Make sure the host meets the minimum hardware configurations supported by ESXi 5.0 and greater. This document will use instructions from the VMware install guide for ESXi 5.5 but 5.0 and greater are supported by GE. This does not include any High Availability Options.
## ESXi Host

<table>
<thead>
<tr>
<th>Processor</th>
<th>ESXi will install &amp; run only on servers with 64-Bit x86 CPUs. ESXi requires a host machine with at least 2 cores. 2 Cores is suggested as a minimum for small architectures &amp; 4 Cores is suggested as a minimum for medium &amp; large architectures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>ESXi 5.5 (5.0 or greater is supported)</td>
</tr>
<tr>
<td>Memory</td>
<td>20 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>SAN with 500 GB storage disk (could differ based on data archiving rates and number or archive tags) (*SSD recommended)</td>
</tr>
<tr>
<td>Network</td>
<td>For this architecture, you can use one physical network card that needs to be installed on a host computer and configured to the process control network</td>
</tr>
</tbody>
</table>

## Virtual Machine 1 – HMI/SCADA

<table>
<thead>
<tr>
<th>Processor</th>
<th>ESXi Host Compatible with 2 Cores</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual CPUs</td>
<td>2 vCPUs</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows 7 or greater (32 &amp; 64 Bit appropriate for small architectures – 64 Bit is Preferred)</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB or greater</td>
</tr>
<tr>
<td>Storage</td>
<td>100 GB (*SSD recommended)</td>
</tr>
<tr>
<td>Network</td>
<td>For smaller architectures, you can use one physical network card which is installed on a host computer and configured to the process control network</td>
</tr>
<tr>
<td>GE Product</td>
<td>GE iFix or Cimplicity- Unlimited with 1000 Tags Defined</td>
</tr>
</tbody>
</table>

## Virtual Machine 2 – Process Historian

<table>
<thead>
<tr>
<th>Processor</th>
<th>ESXi Host Compatible with 2 Cores</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual CPUs</td>
<td>2-4 vCPUs</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows 2008 R2 or Windows 2012 R2 (64 Bit Preferred for medium to large scale architectures)</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>200 GB (*SSD recommended)</td>
</tr>
<tr>
<td>Network</td>
<td>For smaller architectures, you can use one physical network card which is installed on a host computer and configured to the process control network</td>
</tr>
<tr>
<td>GE Product</td>
<td>GE Historian- Standard Edition &lt; 2500Points</td>
</tr>
</tbody>
</table>
3.4 ESXi & Automation Application Hardware Requirements for Medium Size Architecture

* Make sure the host meets the minimum hardware configurations supported by ESXi 5.0 and greater. This document will use instructions from the VMware install guide for ESXi 5.5 but 5.0 and greater are supported by GE. This does not include any High Availability Options.
## ESXi Host

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>ESXi will install &amp; run only on servers with 64-Bit x86 CPUs. EXSi requires a host machine with at least 2 cores. 2 Cores is suggested as a minimum for small architectures &amp; 4 Cores is suggested as a minimum for medium &amp; large architectures</td>
</tr>
<tr>
<td>Operating System</td>
<td>ESXi 5.5 (5.0 or greater is supported)</td>
</tr>
<tr>
<td>Memory</td>
<td>64 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>SAN with 1 TB storage disk</td>
</tr>
<tr>
<td>Network</td>
<td>For this architecture, you can use one physical network card that needs to be installed on a host computer and configured to the process control network</td>
</tr>
</tbody>
</table>

## Virtual Machine 1 – HMI/SCADA

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>ESXi Host Compatible with 2-4 Cores</td>
</tr>
<tr>
<td>Virtual CPUs</td>
<td>2 vCPUs</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows 2008 R2 or Windows 2012 R2 (64 Bit is recommended)</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB or greater</td>
</tr>
<tr>
<td>Storage</td>
<td>100 GB (*SSD recommended)</td>
</tr>
<tr>
<td>Network</td>
<td>For medium to large architectures, you can use one physical network card which is installed on a host computer and configured to the process control network</td>
</tr>
<tr>
<td>GE Product</td>
<td>GE iFix or Cimplicity- Unlimited with 1000 Tags Defined</td>
</tr>
</tbody>
</table>

## Virtual Machine 2 – Process Historian

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>ESXi Host Compatible with 2-4 Cores</td>
</tr>
<tr>
<td>Virtual CPUs</td>
<td>2-4 vCPUs</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows 2008 R2 or Windows 2012 R2 (64 Bit is recommended)</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>250 GB (*SSD recommended)</td>
</tr>
<tr>
<td>Network</td>
<td>For medium to large architectures, you can use one physical network card which is installed on a host computer and configured to the process control network</td>
</tr>
<tr>
<td>GE Product</td>
<td>GE Historian- Standard Edition with 10,000 Points</td>
</tr>
</tbody>
</table>

## Virtual Machine 3 – HMI/ Terminal Server Clients

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>ESXi Host Compatible with 2-4 Cores</td>
</tr>
<tr>
<td>Virtual CPUs</td>
<td>2 vCPUs</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows 2008 R2 or Windows 2012 R2 (64 Bit is recommended)</td>
</tr>
<tr>
<td>Memory</td>
<td>40 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>25 GB (*SSD recommended)</td>
</tr>
<tr>
<td>Network</td>
<td>For medium to large architectures, you can use one physical network card which is installed on a host computer and configured to the process control network</td>
</tr>
<tr>
<td>GE Product</td>
<td>GE iFix or Cimplicity - up to 20 Clients per server</td>
</tr>
</tbody>
</table>
3.5  ESXi & Automation Application Hardware Requirements for Large Size Architecture

* Make sure the host meets the minimum hardware configurations supported by ESXi 5.0 and greater. This document will use instructions from the VMware install guide for ESXi 5.5 but 5.0 and greater are supported by GE. This does not include any High Availability Options.
**ESXi Host**

<table>
<thead>
<tr>
<th>Processor</th>
<th>ESXi will install &amp; run only on servers with 64-Bit x86 CPUs. ESXi requires a host machine with at least 2 cores. 2 Cores is suggested as a minimum for small architectures &amp; 4 Cores is suggested as a minimum for medium &amp; large architectures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>ESXi 5.5 (5.0 or greater is supported)</td>
</tr>
<tr>
<td>Memory</td>
<td>140 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>SAN with 1 TB storage disk</td>
</tr>
<tr>
<td>Network</td>
<td>For this architecture, you can use one physical network card that needs to be installed on a host computer and configured to the process control network</td>
</tr>
</tbody>
</table>

**Virtual Machine 1 – HMI/SCADA**

<table>
<thead>
<tr>
<th>Processor</th>
<th>ESXi Host Compatible with 2-4 Cores</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual CPUs</td>
<td>2 vCPUs</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows 2008 R2 or Windows 2012 R2 (64 Bit is recommended)</td>
</tr>
<tr>
<td>Memory</td>
<td>16 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>150 GB (*SSD recommended)</td>
</tr>
<tr>
<td>Network</td>
<td>For medium to large architectures, you can use one physical network card which is installed on a host computer and configured to the process control network</td>
</tr>
<tr>
<td>GE Product</td>
<td>GE iFix or Cimplicity- Unlimited with 1000 Tags Defined</td>
</tr>
</tbody>
</table>

**Virtual Machine 2 – Process Historian**

<table>
<thead>
<tr>
<th>Processor</th>
<th>ESXi Host Compatible with 2-4 Cores</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual CPUs</td>
<td>2-4 vCPUs</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows 2008 R2 or Windows 2012 R2 (64 Bit is recommended)</td>
</tr>
<tr>
<td>Memory</td>
<td>16 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>500 GB (*SSD recommended)</td>
</tr>
<tr>
<td>Network</td>
<td>For medium to large architectures, you can use one physical network card which is installed on a host computer and configured to the process control network</td>
</tr>
<tr>
<td>GE Product</td>
<td>GE Historian- Standard Edition with &gt; 10,000 Points</td>
</tr>
</tbody>
</table>

**Virtual Machine 3 – HMI/ Terminal Server Clients**

<table>
<thead>
<tr>
<th>Processor</th>
<th>ESXi Host Compatible with 2-4 Cores</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual CPUs</td>
<td>2 vCPUs</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows 2008 R2 or Windows 2012 R2 (64 Bit is recommended)</td>
</tr>
<tr>
<td>Memory</td>
<td>100 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>50 GB (*SSD recommended)</td>
</tr>
<tr>
<td>Network</td>
<td>For medium to large architectures, you can use one physical network card which is installed on a host computer and configured to the process control network</td>
</tr>
<tr>
<td>GE Product</td>
<td>GE iFix or Cimplicity - Up to 50 Clients per server</td>
</tr>
</tbody>
</table>
3.6 ESXi 5.5 Installation Requirements

Make sure the host meets the minimum hardware configurations supported by ESXi 5.5.

To install and use ESXi 5.5, your hardware and system resources must meet the following requirements:

Supported server platform. For a list of supported platforms, see the VMware Compatibility Guide at http://www.vmware.com/resources/compatibility.

- ESXi 5.5 will install and run only on servers with 64-bit x86 CPUs.
- ESXi 5.5 requires a host machine with at least two cores.
- ESXi 5.5 supports only LAHF and SAHF CPU instructions.
- ESXi 5.5 requires the NX/XD bit to be enabled for the CPU in the BIOS.
- ESXi supports a broad range of x64 multicore processors. For a complete list of supported processors, see the VMware compatibility guide at http://www.vmware.com/resources/compatibility. ESXi requires a minimum of 4GB of physical RAM. Provide at least 8GB of RAM to take full advantage of ESXi features and run virtual machines in typical production environments.
- To support 64-bit virtual machines, support for hardware virtualization (Intel VT-x or AMD RVVI) must be enabled on x64 CPUs.
- One or more Gigabit or 10Gb Ethernet controllers. For a list of supported network adapter models, see the VMware Compatibility Guide at http://www.vmware.com/resources/compatibility.
- For Serial ATA (SATA), a disk connected through supported SAS controllers or supported on-board SATA controllers. SATA disks will be considered remote, not local. These disks will not be used as a scratch partition by default because they are seen as remote.
3.7 Storage Systems

For a list of supported storage systems, see the VMware Compatibility Guide at [http://www.vmware.com/resources/compatibility](http://www.vmware.com/resources/compatibility). ESXi 5.5 support installing on and booting from the following storage systems:

- SATA disk drives. SATA disk drives connected behind supported SAS controllers or supported on-board SATA controllers.

**Note**

ESXi does not support using local, internal SATA drives on the host server to create VMFS datastores that are shared across multiple ESXi hosts.

- Serial Attached SCSI (SAS) disk drives. Supported for installing ESXi and for storing virtual machines on VMFS partitions.
- Dedicated SAN disk on Fibre Channel or iSCSI
- USB devices. Supported for installing ESXi.
- Software Fibre Channel over Ethernet (FCoE).

3.8 ESXi Booting Requirements

vSphere 5.5 supports booting ESXi hosts from the Unified Extensible Firmware Interface (UEFI). With UEFI you can boot systems from hard drives, CD-ROM drives, or USB media. Network booting or provisioning with VMware Auto Deploy requires the legacy BIOS firmware and is not available with UEFI.

ESXi can boot from a disk larger than 2TB provided that the system firmware and the firmware on any add-in card that you are using support it. See the vendor documentation.

**Note**

Changing the boot type from legacy BIOS to UEFI after you install ESXi 5.5 might cause the host to fail to boot. In this case, the host displays an error message similar to: Not a VMware boot bank. Changing the host boot type between legacy BIOS and UEFI is not supported after you install ESXi 5.5.
3.9 Storage Requirements for ESXi 5.5 Installation

Installing ESXi 5.5 requires a boot device that is a minimum of 1GB in size. When booting from a local disk or SAN/iSCSI LUN, a 5.2GB disk is required to allow for the creation of the VMFS volume and a 4GB scratch partition on the boot device. If a smaller disk or LUN is used, the installer will attempt to allocate a scratch region on a separate local disk. If a local disk cannot be found the scratch partition, /scratch, will be located on the ESXi host ramdisk, linked to /tmp/scratch. You can reconfigure /scratch to use a separate disk or LUN. For best performance and memory optimization, VMware recommends that you do not leave /scratch on the ESXi host ramdisk.

Due to the I/O sensitivity of USB and SD devices the installer does not create a scratch partition on these devices. When installing on USB or SD devices, the installer attempts to allocate a scratch region on an available local disk or datastore. If no local disk or datastore is found, /scratch is placed on the ramdisk. After the installation, you should reconfigure /scratch to use a persistent datastore. Although a 1GB USB/SD device will suffice for a minimal installation, VMware strongly recommends using a 4GB or larger USB/SD device. The extra space will be used for an expanded coredump partition on the USB/SD device. VMware recommends using a high quality USB flash drive of 16GB or larger so that the extra flash cells can prolong the life of the boot media, but high quality drives of 4GB or larger are sufficient to hold the extended coredump partition. See VMware Knowledge Base article 2004784.

In Auto Deploy installations, the installer attempts to allocate a scratch region on an available local disk or datastore. If no local disk or datastore is found /scratch is placed on ramdisk. You should reconfigure /scratch to use a persistent datastore following the installation.

For environments that boot from a SAN or use Auto Deploy, it is not necessary to allocate a separate LUN for each ESXi host. You can co-locate the scratch regions for many ESXi hosts onto a single LUN. The number of hosts assigned to any single LUN should be weighed against the LUN size and the I/O behavior of the virtual machines.

3.10 Solid State Storage

Solid State storage is ideal for the type of I/O demands that virtual server and desktop environments bring. With extremely random I/O, the need can soon arise to deliver reads and writes more quickly from fast flash storage media than is possible with spinning disk.

[SSDs] are very fast devices, faster than disk (and) very good at read and write applications but particularly good at read and because they have no moving parts, they don’t have the latency that spinning disk does. And that means they’re very good for random I/O.

Virtualized environments typically generate quite a lot of random I/O because of the very nature of the way a number of servers are brought together. You’re bringing together, say, on a virtual desktop infrastructure, many [desktops], or on a virtual server infrastructure maybe tens of servers, and they’re all sharing the same disk so that you’ll see a lot of random I/O.

3.11 Installing ESXi

ESXi can be installed in several ways. To ensure the best vSphere deployment, understand the options thoroughly before beginning the installation.

ESXi installations are designed to accommodate a range of deployment sizes.
Depending on the installation method you choose, different options are available for accessing the installation media and booting the installer.

### 3.12 Interactive ESXi Installation

Interactive installations are recommended for small deployments of fewer than five hosts.

Note

For information on other installation methods such as Scripted, Auto Deploy & Customizing Installations with the ESXi image Builder CLI, please refer to the VMware documentation at [https://pubs.vmware.com/vsphere-55/index.jsp](https://pubs.vmware.com/vsphere-55/index.jsp).

You boot the installer from a CD or DVD, from a bootable USB device, or by PXE booting the installer from a location on the network. You follow the prompts in the installation wizard to install ESXi to disk.

In a typical interactive installation, you boot the ESXi installer and respond to the installer prompts to install ESXi to the local host disk. The installer reformats and partitions the target disk and installs the ESXi boot image. If you have not installed ESXi on the target disk before, all data located on the drive is overwritten, including hardware vendor partitions, operating system partitions, and associated data.
3.13 Install ESXi Interactively

You use the ESXi CD/DVD or a USB flash drive to install the ESXi software onto a SAS, SATA, SCSI hard drive, or USB drive.

Prerequisites

You must have the ESXi installer ISO in one of the following locations:

- On CD or DVD. If you do not have the installation CD/DVD, you can create one.
- On a USB flash drive.

Note

You can also PXE boot the ESXi installer to launch an interactive installation or a scripted installation.

- Verify that the server hardware clock is set to UTC. This setting is in the system BIOS.
- Verify that a keyboard and monitor are attached to the machine on which the ESXi software will be installed. Alternatively, use a remote management application.
- Consider disconnecting your network storage. This action decreases the time it takes the installer to search for available disk drives. Note that when you disconnect network storage, any files on the disconnected disks are unavailable at installation.
- Do not disconnect a LUN that contains an existing ESX or ESXi installation. Do not disconnect a VMFS datastore that contains the Service Console of an existing ESX installation. These actions can affect the outcome of the installation.
- Gather the information required by the ESXi installation wizard. See Required Information for ESXi Installation.
- Verify that ESXi Embedded is not present on the host machine. ESXi Installable and ESXi Embedded cannot exist on the same host.
3.14  Procedure

1. Insert the ESXi installer CD/DVD into the CD/DVD-ROM drive, or attach the Installer USB flash drive and restart the machine.
2. Set the BIOS to boot from the CD-ROM device or the USB flash drive.
3. On the Select a Disk page, select the drive on which to install ESXi and press Enter.

Note
Do not rely on the disk order in the list to select a disk. The disk order is determined by the BIOS and might be out of order. This might occur on systems where drives are continuously being added and removed.

If you select a disk that contains data, the Confirm Disk Selection page appears.
If you are installing on a disc with a previous ESXi or ESX installation or VMFS datastore, the installer provides several choices.
4. Select the keyboard type for the host.
You can change the keyboard type after installation in the direct console.
5. Enter the root password for the host.
You can leave the password blank, but to secure the system from the first boot, enter a password. You can change the password after the installation in the direct console.
6. Press Enter to start the installation.
7. When the installation is complete, remove the installation CD, DVD, or USB flash drive.
8. Press Enter to reboot the host.
9. Set the first boot device to be the drive on which you installed ESXi in Step 3.

3.15  ESXi Autoconfiguration

When you turn on the ESXi host for the first time or after resetting the configuration defaults, the host enters an autoconfiguration phase. This phase configures system network and storage devices with default settings.

By default, Dynamic Host Configuration Protocol (DHCP) configures IP, and all visible blank internal disks are formatted with the virtual machine file system (VMFS) so that virtual machines can be stored on the disks.

3.16  Configuring Network Settings

ESXi requires one IP address for the management network. To configure basic network settings, use the vSphere Web Client or the direct console.

Use the vSphere Web Client if you are satisfied with the IP address assigned by the DHCP server.
Use the direct console for network configuration in the following cases:
- You are not satisfied with the IP address assigned by the DHCP server.
• You are not allowed to use the IP address assigned by the DHCP server. ESXi does not have an IP address. This situation could happen if the auto configuration phase did not succeed in configuring DHCP.
• The wrong network adapter was selected during the auto configuration phase.

3.17 ESXi Networking Security Recommendations

Isolation of network traffic is essential to a secure ESXi environment. Different networks require different access and level of isolation.

Your ESXi host uses several networks. Use appropriate security measures for each network, and isolate traffic for specific applications and functions. For example, ensure that vSphere vMotion traffic does not travel over networks where virtual machines are located. Isolation prevents snooping. Having separate networks also is recommended for performance reasons.

• vSphere infrastructure networks are used for features such as VMware vSphere vMotion®, VMware vSphere Fault Tolerance, and storage. These networks are considered to be isolated for their specific functions and often are not routed outside a single physical set of server racks.
• A management network isolates client traffic, command-line interface (CLI) or API traffic, and third-party software traffic from normal traffic. This network should be accessible only by system, network, and security administrators. Use jump box or virtual private network (VPN) to secure access to the management network. Strictly control access within this network to potential sources of malware.
• Virtual machine traffic can flow over one or many networks. You can enhance the isolation of virtual machines by using virtual firewall solutions that set firewall rules at the virtual network controller. These settings travel with a virtual machine as it migrates from host to host within your vSphere environment.

3.18 After You Install and Set Up ESXi

After ESXi is installed and set up, you can manage the host through the vSphere Web Client and vCenter Server, license the host, and back up your ESXi configuration.
4. Implementing High Availability (HA) with vSphere

The following will guide you through the steps to setup and implement the High Availability virtualized environment for using Vsphere technology.

4.1 Datacenter(s)

A typical VMware Infrastructure data center consists of basic physical building blocks such as x86 computing servers, storage networks and arrays, IP networks, a management server and desktop clients. It provides for end-end connectivity between client machines and field devices.

The setup for Automation systems requires a minimum of two host servers and one storage server shared across the two hosts. The following procedure will help you configure a Datacenter with a Failover Cluster that has two nodes to set up a virtualized High Availability environment.

4.2 VMware DRS

Taking the VMotion capability one step further by adding an intelligent scheduler, VMware enables the system administrator to set resource assignment policies that reflect business needs and let VMware DRS do the calculation and automatically handle the detailed physical resource assignments. VMware DRS dynamically monitors the workload of the running virtual machines and the resource utilization of the physical servers within a Cluster. It checks those results against the resource assignment policies, if there is a potential for violation or improvement, it utilizes VMotion and dynamically reassigns virtual machines to different physical servers, as shown below, to ensure that the policies are complied with and resource allocation is optimal. If a new physical server is made available, VMware DRS automatically redistributes the virtual machines to take advantage of it. Conversely, if a physical server needs to be taken down for any reason, VMware DRS redistributes its virtual machines to other servers automatically. For more information, see the VMware DRS white paper at [https://www.vmware.com/pdf/vmware_drs_wp.pdf](https://www.vmware.com/pdf/vmware_drs_wp.pdf).
4.3 Creating a Datacenter

1. Start the vSphere Client. The vSphere Client dialog box appears.
2. Enter the IP Address or the hostname of the vCenter Server computer, user name and password, then click Login.
   The vSphere Client page appears.
3. On the File menu, Click New and click Datacenter.
   A new Datacenter object appears in the Inventory Panel.
4. Enter a name for the Datacenter and press Enter.

4.4 Adding a Host to a Datacenter

1. Double click on the Datacenter created in the Inventory Panel. The vSphere Client page appears
2. On the File menu, select New and then select Add Host.
   The Add Host Wizard Appears.
3. Enter the IP Address and the root credentials of the ESXi Server, then click Next.
   The Host Summary Appears.
4. Review the Host information, then click Next.
   The Assign License widow appears.
5. Select the Assign a new Key License to this host option to enter a new key and also if your ESXi host does not have a license. Click Next.
   The Lockdown Mode window appears
6. Select the Enable Lockdown Mode check box if your security policies require the host to be inaccessible to remote users, then click Next. The Virtual Machine Location Window appears.

7. Click the Datacenter that you have created and then click Next. The Ready to Complete window appears.

8. Review your selections and select Finish.

4.5 Creating a vSphere HA Cluster

vSphere HA operates in the context of a cluster of ESXi (or legacy ESX hosts). You must create a cluster, populate it with hosts, and configure vSphere HA settings before failover protection can be established.

When you create a vSphere HA cluster, you must configure a number of settings that determine how the feature works. Before you do this, identify your cluster’s nodes. These nodes are the ESXi hosts that will provide the resources to support virtual machines and that vSphere HA will use for failover protection. You should then determine how those nodes are to be connected to one another and to the shared storage where your virtual machine data resides. After that networking architecture is in place, you can add the hosts to the cluster and finish configuring vSphere HA.

You can enable and configure vSphere HA before you add host nodes to the cluster. However, until the hosts are added, your cluster is not fully operational and some of the cluster settings are unavailable. For example, the Specify a Failover Host admission control policy is unavailable until there is a host that can be designated as the failover host.

4.6 Create a Failover Cluster

1. On the vSphere Client page, right click on a Datacenter and click New Cluster.
2. Enter a name and press Enter.
3. Double click the new cluster. The New Cluster Wizard appears.
4. Select the Turn On vSphere HA check box. Select Next and the vSphere HA window appears.
5. In vSphere HA area, select the following items, then click Next.
   • Select Enable Host Monitoring check box.
   • Select an Administration Control option.
   • Select an appropriate Admission Control Policy option.
   • Select Next and the Virtual Machine Options window appears.
6. On the Virtual Machines Options page, configure the following items:
   • Under the VM restart priority list, select the appropriate restart priority setting.
   • Under the Host Isolation response list, select a host isolation response. Select Next and the VM Monitoring window appears.
7. Under the VM Monitoring page, configure the following items:
   • Under the VM Monitoring list, Select the VM Monitoring method
   • Set the Monitoring Sensitivity, if you have selected VMware Tools for VM Monitoring.
     Select Next and the VMware EVC window appears.

8. Select the Disable EVC Option.
    Select Next and the VM Swapfile Location window appears.

9. Select the Store the swapfile in the same directory as the virtual machine (recommended)
    option to speed up vMotion.
    Select Next and the Ready to Complete window appears.

10. Review the cluster configuration details, and then click Finish.
    The cluster appears on the vSphere Cluster window.

4.7 Datastores

Datastores are logical containers, analogous to file systems that hide specifics of each storage device and provide a uniform model for storing virtual machine files. Datastores can also be used for storing ISO images, virtual machine templates, and floppy images.

You use the vSphere Client to access different types of storage devices that your ESX host discovers and to deploy datastores on them.

Depending on the type of storage you use, datastores can be backed by the following file system formats:

<table>
<thead>
<tr>
<th>Datastore Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine File System (VMFS)</td>
<td>High-performance file system optimized for storing virtual machines. Your host can deploy a VMFS datastore on any SCSI-based local or networked storage device, including Fibre Channel and iSCSI SAN equipment. As an alternative to using the VMFS datastore, your virtual machine can have direct access to raw devices and use a mapping file (RDM) as a proxy.</td>
</tr>
<tr>
<td>Network File System (NFS)</td>
<td>File system on a NAS storage device. ESX supports NFS version 3 over TCP/IP. The host can access a designated NFS volume located on an NFS server, mount the volume, and use it for any storage needs.</td>
</tr>
</tbody>
</table>

If you use the service console to access your ESX host, you can see the VMFS and NFS datastores as separate subdirectories in the /vmfs/volumes directory.

4.8 Solid State Storage

Solid State storage is ideal for the type of I/O demands that virtual server and desktop environments bring. With extremely random I/O, the need can soon arise to deliver reads and writes more quickly from fast flash storage media than is possible with spinning disk.

SSDs are very fast devices, faster than disk (and) very good at read and write applications but particularly good at read and because they have no moving parts, they don't have the latency that spinning disk does. And that means they’re very good for random I/O.
Virtualized environments typically generate quite a lot of random I/O because of the very nature of the way a number of servers are brought together. You’re bringing together, say, on a virtual desktop infrastructure, many [desktops], or on a virtual server infrastructure maybe tens of servers, and they’re all sharing the same disk so that you’ll see a lot of random I/O.

The VMware vSphere storage architecture consists of layers of abstraction that hide and manage the complexity and differences of physical storage subsystems, shown below.

4.9 Creating a Datastore

1. Log on to the vSphere Client and select a host from the Inventory Panel.
2. In the vSphere Client, configure the following items to add the storage details:
   - Select the Configuration Tab, and then select Storage in the Hardware Panel. The configuration details appear in the Configuration area.
   - Select Datastores, and then select Add Storage. The Add Storage window appears.
3. Select the Disk/LUN option, and then click Next. The Select Disk/LUN window appears.
4. Select a device that you will use for your Datastore, and then select Next. The File System Version window appears.

5. Select the appropriate File System Version option and select Next. The Current Disk Layout area appears.

6. Review the current disk layout, and then click Next. The Properties window appears.

7. Type the datastore name and then select Next. The Formatting window appears.

8. Select the Custom space setting option to adjust the capacity values, and then select Next. The Ready to Complete window appears.

9. Review the Datastore configuration information and select Finish to create the datastore based on the settings you’ve selected.


4.10 Configuring Networks

You must follow the procedures below to configure multiple networks on the ESXi host.

To configure networks on the ESXi host:

1. Log on to vSphere Client and select a host from the Inventory Panel.
2. Select the Configuration tab, and then select Networking on the Hardware Panel.
   The networking details appear in the Configuration Tab window.
3. Select Add Networking.
   The Add Network Wizard appears.
4. Select the Virtual Machine option, and then select Next.
   The Network Access window appears.
5. Select the appropriate switch option, and then select the check box associated with it.
7. In the Connection Setting area, perform the following steps to specify the Port Group properties, and then select Next.
   The Summary area window appears.
   o Enter the network name in the Network Label box.
   o Enter the VLAN identification number in the VLAN ID box.
     * This is an optional field.
8. Review the switch details, and then select Finish to complete the network configuration.
4.11 Creating a Virtual Machine in the vSphere Client

When you create a Virtual Machine, you can associate it with a Datacenter, host, cluster or resource pool and a Datastore. The Virtual Machine consumes resources dynamically as the workload increases, or it returns resources dynamically as the workload decreases.

Every Virtual Machine has virtual devices that provide the same function as the physical hardware. A Virtual Machine gets the following attributes from the host with which it is associated:

- CPU and memory space
- Access to storage
- Network connectivity


4.12 Creating a Virtual Machine in vSphere Client

1. Start the vSphere Client, and then select the Virtual Machines tab.
2. Right Click on the Virtual Machines panel, and then select New Virtual Machine.
   The Create New Virtual Machine window appears.
3. Select a Configuration option for the new virtual machine, and then click Next.
   The Name and Location window appears.
4. Enter a Name and an Inventory Location for the virtual machine, and then click Next.
   The Storage window appears.
5. Select a Datastore, and then click Next.
   The Virtual Machine Version window appears.
6. Select a Virtual Machine Version option, and then click Next.
   The Guest Operating System window appears.
7. Select a Guest Operating System option and then select a version from the Version list, and then click Next.
   The CPUs window appears.
8. Select values for the Number of virtual sockets and the Number of cores per virtual socket to configure the virtual machines, and then click Next,
   The Memory window appears.
9. Enter a value for Memory Size to configure the virtual memory, and then click Next.
   The Network window appears.
10. Select the number of NICs, and then associate each NIC with a Network, and then click Next.
    The SCSI Controller window appears.
11. Select an SCSI Controller option, and then click Next.
    The Select a Disk area appears.
12. Select a Disk option that you will use. You can perform any one of the following action:
    - Create a new virtual disk
    - Use a previously configured virtual disk
    - Not create a virtual disk
    If you click either of the first two options, and then click Next,
    The Create a Disk window appears.
13. In Create a Disk Area screen, perform the following actions and then click Next:
    Enter Disk Capacity size.
Select a Disk Provisioning option.
Select a Location option to swap files. The Advanced Options area appears.

14. Select a Virtual Device Node option and then select the Independent check box.
Select a Mode option, and then click Next.
The Ready to Complete area appears.

15. Review your configuration.
Select the Edit the virtual machine settings before completion check box to configure the properties of the virtual machine, and then click Continue.
The Virtual Machine Properties window appears.

4.13 To configure virtual machine properties

1. On the Virtual Machine Properties window, select CD/DVD drive 1 under the Hardware pane on the left panel.

2. In Virtual Machine Properties window, perform any one of the following to configure the properties of a new virtual machine:
   • Select the Host Device option, and then select the host device from the list to boot from the host CD/DVD.
   • Select the Datastore ISO File option, and then click Browse.

3. The Browse Datastores window box appears.
Select the appropriate ISO file, and then click Open. The selected ISO file appears in the Datastore ISO File box.

4. Click OK, and then switch on the virtual machine to install the operating system.

4.14 Enabling vMotion for Migration

VMware vMotion enables migration of a running virtual machine from one server to another, including the VM's associated storage, network identity, and network connections. VMware vMotion enables migration of a running virtual machine from one server to another, including the VM's associated storage, network identity, and network connections as well as access to the VM's storage switches to the new physical host. Access to the VM continues with its same virtualized network identity.

Typical migration scenarios are listed below:
• Removing VMs from underperforming or problematic servers
• Performing hardware maintenance and upgrades
• Optimizing VMs within resource pools
4.15 To enable vMotion for migration

1. Log on to the vSphere Client and select the host from the Inventory panel.
2. Select the Configuration tab and then click Networking on the Hardware panel. The switch details appear on the Configuration tabbed page.
3. Select the switch that you want to enable for vMotion, and then click Properties for that switch. The vSwitch# Properties window appears.
4. Select Management Network under the Configuration pane on the left panel, and then click Edit. The Management Network Properties window appears.
5. In Management Network Properties window, perform the following steps to edit the Port Properties and NIC Settings:
   • Type or modify the name for Network Label. Enter a valid VLAN ID. *This is an optional field.
   • Select the Enabled check boxes for vMotion and Management Traffic.
   • Enter a value for MTU.
6. Click OK to accept the changes.
5. **VMware Best Practices**

The following links discuss Performance Best Practices for VMware vSphere™ 5.0 & 5.5, provides performance tips that cover the most performance-critical areas of VMware vSphere 5.0 & 5.5.

**VMware 5.0 Links**


**VMware 5.5 Links**

https://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf

https://www.vmware.com/security/hardening-guides
6. **Troubleshoot and Enhance Performance**

This section presents tips for identifying and solving performance problems. The suggestions in this section are not meant to be a comprehensive guide to diagnosing and troubleshooting problems in the virtual environment. It is meant to provide information about some common problems that can be solved without contacting VMware Technical Support.

**Subtopics**

- Solutions for Consistently High CPU Usage
- Solutions for Memory Performance Problems
- Solutions for Storage Performance Problems
- Solutions for Disk Performance Problems
- Solutions for Poor Network Performance
6.1 Solutions for Consistently High CPU Usage

Temporary spikes in CPU usage indicate that you are making the best use of CPU resources.
Consistently high CPU usage might indicate a problem. You can use the vSphere Client CPU performance
charts to monitor CPU usage for hosts, clusters, resource pools, virtual machines, and vApps.

Problem
Host CPU usage constantly is high. A high CPU usage value can lead to increased ready time and
processor queuing of the virtual machines on the host.
Virtual machine CPU usage is above 90% and the CPU ready value is above 20%. Application performance
is impacted.

Cause
The host probably is lacking the CPU resources required to meet the demand.

Solution
- Verify that VMware Tools is installed on every virtual machine on the host.
- Compare the CPU usage value of a virtual machine with the CPU usage of other virtual machines
  on the host or in the resource pool. The stacked bar chart on the host’s Virtual Machine view shows
  the CPU usage for all virtual machines on the host.
- Determine whether the high ready time for the virtual machine resulted from its CPU usage time
  reaching the CPU limit setting. If so, increase the CPU limit on the virtual machine.
- Increase the CPU shares to give the virtual machine more opportunities to run. The total ready time
  on the host might remain at the same level if the host system is constrained by CPU. If the host
  ready time doesn’t decrease, set the CPU reservations for high-priority virtual machines to
  guarantee that they receive the required CPU cycles.
- Increase the amount of memory allocated to the virtual machine. This action decreases disk and or
  network activity for applications that cache. This might lower disk I/O and reduce the need for the
  host to virtualize the hardware. Virtual machines with smaller resource allocations generally
  accumulate more CPU ready time.
- Reduce the number of virtual CPUs on a virtual machine to only the number required to execute
  the workload. For example, a single-threaded application on a four-way virtual machine only
  benefits from a single vCPU. But the hypervisor’s maintenance of the three idle vCPUs takes CPU
  cycles that could be used for other work.
- If the host is not already in a DRS cluster, add it to one. If the host is in a DRS cluster, increase the
  number of hosts and migrate one or more virtual machines onto the new host.
- Upgrade the physical CPUs or cores on the host if necessary.
- Use the newest version of hypervisor software, and enable CPU-saving features such as TCP
  Segmentation Offload, large memory pages, and jumbo frames.
6.2 Solutions for Memory Performance Problems

Host machine memory is the hardware backing for guest virtual memory and guest physical memory. Host machine memory must be at least slightly larger than the combined active memory of the virtual machines on the host.

A virtual machine's memory size must be slightly larger than the average guest memory usage. Increasing the virtual machine memory size results in more overhead memory usage.

Problem

Memory usage is constantly high (94% or greater) or constantly low (24% or less).

Free memory consistently is 6% or less and swapping frequently occurs.

Cause

- The host probably is lacking the memory required to meet the demand. The active memory size is the same as the granted memory size, which results in memory resources that are not sufficient for the workload. Granted memory is too much if the active memory is constantly low.
- Host machine memory resources are not enough to meet the demand, which leads to memory reclamation and degraded performance.
- The active memory size is the same as the granted memory size, which results in memory resources that are not sufficient for the workload.

Solution

- Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
- Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, this does not impact virtual machine performance.
- Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
- If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
- Migrate one or more virtual machines to a host in a DRS cluster.
- Add physical memory to the host.
6.3 Solutions for Storage Performance Problems

Datastores represent storage locations for virtual machine files. A storage location can be a VMFS volume, a directory on Network Attached Storage, or a local file system path. Datastores are platform-independent and host-independent.

Problem

- Snapshot files are consuming a lot of datastore space.
- The datastore is at full capacity when the used space is equal to the capacity. Allocated space can be larger than datastore capacity, for example, when you have snapshots and thin-provisioned disks.

Solution

- Consider consolidating snapshots to the virtual disk when they are no longer needed. Consolidating the snapshots deletes the redo log files and removes the snapshots from the vSphere Web Client user interface.
- You can provision more space to the datastore if possible, or you can add disks to the datastore or use shared datastores.
6.4 Solutions for Disk Performance Problems

Use the disk charts to monitor average disk loads and to determine trends in disk usage. For example, you might notice performance degradation with applications that frequently read from and write to the hard disk. If you see a spike in the number of disk read/write requests, check if any such applications were running at that time.

**Problem**

- The value for the kernelLatency data counter is greater than 4ms.
- The value for the deviceLatency data counter is greater than 15ms indicates there are probably problems with the storage array.
- The queueLatency data counter measures above zero.
- Spikes in latency.
- Unusual increases in read/write requests.

**Cause**

- The virtual machines on the host are trying to send more throughput to the storage system than the configuration supports.
- The storage array probably is experiencing internal problems.
- The workload is too high and the array cannot process the data fast enough.

**Solution**

- The virtual machines on the host are trying to send more throughput to the storage system than the configuration supports. Check the CPU usage, and increase the queue depth.
- Move the active VMDK to a volume with more spindles or add disks to the LUN.
- Increase the virtual machine memory. This should allow for more operating system caching, which can reduce I/O activity. Note that this may require you to also increase the host memory. Increasing memory might reduce the need to store data because databases can utilize system memory to cache data and avoid disk access.
- Check swap statistics in the guest operating system to verify that virtual machines have adequate memory. Increase the guest memory, but not to an extent that leads to excessive host memory swapping. Install VMware Tools so that memory ballooning can occur.
- Defragment the file systems on all guests.
- Disable antivirus on-demand scans on the VMDK and VMEM files.
- Use the vendor’s array tools to determine the array performance statistics. When too many servers simultaneously access common elements on an array, the disks might have trouble keeping up. Consider array-side improvements to increase throughput.
- Use Storage VMotion to migrate I/O-intensive virtual machines across multiple hosts.
• Balance the disk load across all physical resources available. Spread heavily used storage across LUNs that are accessed by different adapters. Use separate queues for each adapter to improve disk efficiency.
• Configure the HBAs and RAID controllers for optimal use. Verify that the queue depths and cache settings on the RAID controllers are adequate. If not, increase the number of outstanding disk requests for the virtual machine by adjusting the Disk.SchedNumReqOutstanding parameter.
• For resource-intensive virtual machines, separate the virtual machine's physical disk drive from the drive with the system page file. This alleviates disk spindle contention during periods of high use.
• On systems with sizable RAM, disable memory trimming by adding the line MemTrimRate=0 to the virtual machine’s .VMX file.
• If the combined disk I/O is higher than a single HBA capacity, use multipathing or multiple links.
• For ESXi hosts, create virtual disks as preallocated. When you create a virtual disk for a guest operating system, select Allocate all disk space now. The performance degradation associated with reassigning additional disk space does not occur, and the disk is less likely to become fragmented.
• Use the most current hypervisor software.
6.5 Solutions for Poor Network Performance

Network performance is dependent on application workload and network configuration. Dropped network packets indicate a bottleneck in the network. Slow network performance can be a sign of load-balancing problems.

Problem

Network problems can manifest in many ways:

- Packets are being dropped.
- Network latency is high.
- Data receive rate is low.

Cause

Network problems can have several causes:

- Virtual machine network resource shares are too few.
- Network packet size is too large, which results in high network latency. Use the VMware AppSpeed performance monitoring application or a third-party application to check network latency.
- Network packet size is too small, which increases the demand for the CPU resources needed for processing each packet. Host CPU, or possibly virtual machine CPU, resources are not enough to handle the load.

Solution

- Determine whether packets are being dropped by using esxtop or the advanced performance charts to examine the droppedTx and droppedRx network counter values. Verify that VMware Tools is installed on each virtual machine.
- Check the number of virtual machines assigned to each physical NIC. If necessary, perform load balancing by moving virtual machines to different vSwitches or by adding more NICs to the host. You can also move virtual machines to another host or increase the host CPU or virtual machine CPU.
- If possible, use vmxnet3 NIC drivers, which are available with VMware Tools. They are optimized for high performance.
- If virtual machines running on the same host communicate with each other, connect them to the same vSwitch to avoid the cost of transferring packets over the physical network.
- Assign each physical NIC to a port group and a vSwitch.
- Use separate physical NICs to handle the different traffic streams, such as network packets generated by virtual machines, iSCSI protocols, VMotion tasks.
- Ensure that the physical NIC capacity is large enough to handle the network traffic on that vSwitch. If the capacity is not enough, consider using a high-bandwidth physical NIC (10Gbps) or moving some virtual machines to a vSwitch with a lighter load or to a new vSwitch.
- If packets are being dropped at the vSwitch port, increase the virtual network driver ring buffers where applicable.
• Verify that the reported speed and duplex settings for the physical NIC match the hardware expectations and that the hardware is configured to run at its maximum capability. For example, verify that NICs with 1Gbps are not reset to 100Mbps because they are connected to an older switch.

• Verify that all NICs are running in full duplex mode. Hardware connectivity issues might result in a NIC resetting itself to a lower speed or half duplex mode.
7. Glossary

The VMware Technical Publications Glossary defines terms as used in VMware technical documentation.

ACE instances

The virtual machines that ACE administrators create, associate to virtual rights management (VRM) policies, and package for deployment to users. See also VRM (Virtual Rights Management), disk mode.

Activation

A step in an ACE instance setup that includes package protection and the setup of the ACE instance’s runtime authentication policy. Complete the activation to make the packaged virtual machine, with its policies and other settings, into an ACE instance. See also authorization role.

administrative lockout

A global setting that provides password protection for Windows hosts. Administrative lockout restricts users from creating new virtual machines, editing virtual machine configurations, and changing network settings.

admission control

When you power on a virtual machine, the system checks the amount of CPU and whether memory resources are reserved. Based on the available unreserved resources, the system determines whether it can guarantee the Reservation for which the virtual machine is configured.

alarm

An entity that monitors one or more properties of a virtual machine, such as CPU load. Alarms send notifications as directed by the configurable alarm definition.

anomaly

In Capacity Planner, an indicator that server performance is significantly different from the industry performance averages of like servers. Capacity Planner notes an anomaly when it detects performance that is more than three standard deviations from the industry average.

append mode

In ESX Server 2.x, a disk mode in which software running in the virtual machine appears to write changes to the disk. Changes are stored in a temporary .REDO file. If a system administrator deletes the redo-log file, the virtual machine returns to the state it was in the last time it was used in persistent mode. See also disk mode.

array-based replication

Replication of a virtual machine that is managed and executed by the storage subsystem rather than from inside the virtual machine, the VMkernel, or the service console.

asynchronous I/O (AIO)

In GSX and Workstation, a process that handles blocking system calls for asynchronous I/O, or nonblocking I/O. AIO is a form of input.

authorization role
A set of privileges grouped for convenient identification under names such as Administrator.

**base disk**
The original virtual hard disk from which a virtual machine is derived. Virtual machines created by linked clones in Lab Manager consist of a base disk and chain of delta disks that store the changes made to the original. This process addresses the potential disk consumption difficulties that can occur with virtual machine proliferation.

**boot from SAN**
Ability of a host to load its operating system over a storage area network (SAN). The boot image is stored on a remote storage array, rather than on a disk directly attached to the system. Diskless servers require the use of boot from SAN technology.

**bridged networking**
In hosted products, a type of network connection between a virtual machine and the host’s physical network. With bridged networking, a virtual machine appears to be an additional computer on the same physical Ethernet network as the host. See also custom networking, host-only networking.

**child**
A managed entity grouped by a folder object or another managed entity.

**CIMOM (CIM Object Manager)**
A component that stores class definitions and populates requests for CIM operations with information returned from specific data providers.

**clone**
(n.) A duplicate of a virtual machine. (v.) To make a copy of a virtual machine. Hosted products distinguish between full clones and linked clones. See also full clone, linked clone.

**cluster**
A server group in the virtual environment. Clusters enable a high-availability solution.

**cluster compute resource**
An extended compute resource that represents a cluster of hosts available for backing virtual machines. See also compute resource.

**cold cloning**
In VMware vCenter Converter, cloning a local physical machine while it is running in WinPE from the vCenter Converter Boot CD, not from its own operating system. See also hot cloning.

**compute resource**
A managed object that represents either a single host or a cluster of hosts available for backing up virtual machines. See also cluster compute resource.

**concurrent migrations**
In VMware vCenter Converter, the Task Manager’s ability to direct the conversion and migration of multiple virtual machines at the same time.
console
See remote console, service console, VMware virtual machine console.

CPU compatibility masks
vCenter Server compares the CPU features available to a virtual machine with the CPU features of the destination host to determine whether to allow or disallow migrations with VMotion. By applying CPU compatibility masks to virtual machines, you can hide certain CPU features from the virtual machine and potentially prevent migrations with VMotion from failing due to incompatible CPUs.

current virtual machine
A virtual machine of the latest version supported by the product in use. See also legacy virtual machine.

custom networking
In hosted products, any type of network connection between virtual machines and the host that does not use the default bridged, host-only, or network address translation (NAT) configurations. For example, virtual machines can be connected to the host by separate networks or connected to each other and not to the host. See also bridged networking, host-only networking.

datacenter
A required structure under which hosts and their associated virtual machines are added to vCenter Server. vCenter Server supports multiple datacenters. A host can be managed under only one datacenter.

datacenter folder
An optional inventory grouping structure contained within the datacenter structure. vCenter Server supports multiple datacenter folders. Datacenter folders can contain only datacenters and other datacenter folders.

data source name
An Open Database Connectivity (ODBC) object that you must configure to enable vCenter Server to access a database.

datastore
Virtual representations of combinations of underlying physical storage resources in the datacenter. A datastore is the storage location (for example, a physical disk, a RAID, or a SAN) for virtual machine files.

delta disk
Differencing disk created during the cloning process. A virtual machine created as a linked clone consists of a base disk, plus a chain of one or more delta disks that store the differences between the cloned virtual machine and the original virtual machine.

deployment lease
In ACE, a set of rules and settings associated with a package, such as Revert to Installed and Instance Customization settings. The only way to change package settings is to create a package.

deployment settings
In ACE, a set of rules and settings associated with a package, such as Revert to Installed and Instance
Customization settings. The only way to change package settings is to create a package.

**destination virtual machine**

In VMware vCenter Converter, the migrated virtual machine at its final location.

**differential backup**

A process that backs up only files that have changed since the last full backup.

**disk arrays**

Groups of multiple disk devices that make up the typical SAN disk storage device. These arrays vary in design, capacity, performance, and other features.

**disk mode**

A property of a virtual disk that defines its external behavior (how the virtualization layer treats its data). The disk mode is invisible to the guest operating system. Available modes vary by product. See also persistent mode, nonpersistent mode, undoable mode, append mode.

**dvPort (distributed virtual port)**

A port on a vDS that connects to a host's service console or VMkernel or to a virtual machine’s network adapter. See also vDS (distributed virtual switch).

**dvPort group**

A port group associated with a vDS. The port group specifies port configuration options for each member port. A dvPort group defines how a connection is made through the vDS to the network. See also vDS (distributed virtual switch).

**enumeration**

The act of discovering resources available in a virtual machine environment. In particular, discovering all resources of a given type or a list of resources discovered by enumeration.

**event**

An action that is of interest to vCenter Server. Each event triggers an event message. Event messages are archived in the vCenter Server database.

**event declaration**

Type of event (alert, error, info, warning, or user) and its name, arguments, and message format.

**existing partition**

A partition on a physical disk. See also physical disk.

**fabric**

A Fibre Channel network topology in which devices pass data to each other through interconnecting switches. A fabric is used in many SANs. Fabrics are typically divided into zones. Also called switched fabric or Fibre Channel fabric.

**fault**

A data object containing information about an exception condition encountered by an operation.
**Favorites**
A list in the main VMware Workstation window that shows the names of virtual machines that a user has added. Use the Favorites list to start a virtual machine or to connect to the configuration file and make changes in the virtual machine settings.

**file system cache**
A storage mechanism that speeds access to files stored on a disk by caching frequently accessed data. The maximum disk cache for 32-bit operating systems is 512MB; for 64-bit operating systems, the maximum is 1TB. All platforms use file system caches for improved performance.

**force delete**
To forcefully delete a virtual machine when an ESX host failure prevents the Lab Manager administrator from deleting the virtual machine.

**force undeploy**
To forcefully undeploy a virtual machine after situations such as when an ESX host goes permanently offline or someone manually removes a virtual machine from the vCenter inventory.

**Foundry**
An API for controlling virtual machines.

**full clone**
A complete copy of the original virtual machine, including all associated virtual disks. See also linked clone.

**full screen switch mode**
A display mode in which the virtual machine’s display fills the entire screen. The user cannot create, reconfigure, or start virtual machines. A system administrator performs those functions. See also quick switch mode.

**full virtual machine backup**
A process that backs up all files that make up the entire virtual machine. These files include disk images, .vmx files, and so on.

**Go to snapshot**
To restore a snapshot of the active virtual machine. See also revert to snapshot.

**GOS (guest operating system)**
See guest operating system.

**group**
A set of users who are assigned a common set of privileges. A group can contain other groups. See also service console.

**growable disk**
A type of virtual disk in which the disk space is not preallocated to its full size. The disk files begin small and increase as data is written to the disk. See also preallocated disk.
guest customization
Lab Manager customization of the network settings inside the guest operating system of a virtual machine. These settings include the machine name, IP settings, and Security Identifier (SID) for Windows guest operating systems. Lab Manager creates a package with the guest customization tools. When you power on a virtual machine for the first time, Lab Manager copies the package, runs the tools, and deletes the package from the virtual machine.

guest operating system
An operating system that runs inside a virtual machine. See also host operating system.

guest user
An unauthenticated user who can log in to a system with a temporary user name and password. A guest user has restricted access to files and folders and has a set of restricted permissions.

handle
A temporary token used by a Web service client to invoke Web service operations that require a reference to an object. Like a file handle, an object handle is a temporary handle that always refers to the same object.

headless
Describes a program that runs in the background without any interface connected to it. A running virtual machine that has no console connections is running headless.

host
A computer that uses virtualization software to run virtual machines. Also called the host machine or host computer. The physical computer on which the virtualization (or other) software is installed.

host agent
Software that performs actions on behalf of a remote client when installed on a virtual machine host.

host computer
The physical computer on which VMware Player software is installed. The host computer hosts the ACE instances.

host-based licensing
In VMware Infrastructure 3, one of two modes for licensing ESX/ESXi software. License files reside on the host. Feature availability is tied strictly to the host on which the file resides. See also server-based licensing.

hosted machine
The physical computer on which the VMware Workstation software is installed. The hosted machine hosts the VMware Workstation virtual machines.

hosted products
VMware products (including Workstation, VMware Player, VMware Server, VMware ACE, and Lab Manager) that run as applications on physical machines with operating systems such as Microsoft Windows or Linux. See also hypervisor.
**host-only networking**
In hosted products, a type of network connection between a virtual machine and the host. With host-only networking, a virtual machine is connected to the host on a private network, which normally is not visible outside the host. Multiple virtual machines configured with host-only networking on the same host are on the same network. See also bridged networking, vCenter Converter Boot CD (VMware vCenter Converter Boot CD), custom networking.

**host operating system**
An operating system that runs on the host machine. See also guest operating system.

**hot cloning**
In VMware vCenter Converter, cloning a local or remote physical machine while it is running in its own operating system. See also cold cloning.

**hot fix**
An installable file that resets a user’s password, renews an expired virtual machine, or enables a copyprotected virtual machine to run from a new location.

**hyperthreading**
A technology that allows a single physical processor to behave like two logical processors. The processor can run two independent applications at the same time.

**hypervisor**
A platform that allows multiple operating systems to run on a host computer at the same time.

**IBVP (In-Band Virtualizer Profile)**
The standard profile that the VMware Migration Server adapts to describe ESX/ESXi server. The CIM SDK version 2 is based on the IBVP.

**image-level (volume-level) backup**
A process that backs up an entire storage volume.

**incremental backup**
A process that backs up only those files that have changed since the last backup, whether it is a full or incremental backup.

**independent disk**
A type of virtual disk that is not affected by snapshots. You can configure independent disks in persistent and nonpersistent modes. See also nonpersistent mode, persistent mode.

**instance customization**
The process of customizing an ACE instance to make it unique from all other instances. The instance customization process automates the actions of the Microsoft sysprep utility. It also provides the ACE administrator with features needed to set up an automated remote domain join process of the ACE instance to a company VPN network.

**inventory**
A hierarchical structure used by the vCenter Server or the host agent to organize the entities or objects that it manages. This hierarchy is a list of all the managed objects in vCenter Server.

**inventory mapping**
Mapping between resource pools, networks, and virtual machine folders on the protection site and their destination counterparts on the recovery site.

**IP storage**
In ESX/ESXi, any form of storage that uses TCP/IP network communication as its foundation. Both Network File System (NFS) and iSCSI storage can be used as virtual machine datastores. NFS can also be used for direct mounting of .ISO files for presentation to virtual machines as CD-ROM discs.

**Lab Manager Web console**
A browser-based interface that provides access to all Lab Manager operations.

**LAN segment**
A private virtual network that is available only to virtual machines within the same team. See also *virtual network*.

**legacy virtual machine**
A virtual machine supported by the product in use but not current for that product. For example, in Workstation 5x, you can create virtual machines for use in Workstation 4.x, GSX Server 3.x, or ESX Server 2.x. New Workstation 5x features (such as clones, multiple snapshots, and teams) are not compatible with the legacy virtual machines.

**linked clone**
A copy of the original virtual machine. The copy must have access to the parent virtual machine’s virtual disks. The linked clone stores changes to the virtual disks in a separate set of files. See also *full clone*.

**local cloning**
The process of making a copy of a virtual machine residing in the system on which VMware vCenter Converter is running, or making a copy of the physical machine itself for conversion to a virtual machine. See also *remote cloning*.

**lockout**
See *administrative lockout*.

**LUN Masking**
A process that is used for permission management to make a LUN available to some hosts and not to other hosts. Also referred to as Selective Storage Presentation, access control, and partitioning, depending on the vendor.

**managed ACE instance**
An ACE instance that an ACE Management Server manages.

**managed entity**
A managed object that is present in the inventory. See also *inventory*, *managed object*.
managed object
An object that resides on a server and is passed between the client and the Web service only by reference. A managed object has operations associated with it but might not have properties. See also data source name.

managed object reference
A data object created to uniquely identify a managed object.

migration
The process of moving a virtual machine between hosts. Unless vMotion is used, the virtual machine must be powered off when you migrate it. See also migration with vMotion, migration with VMware vCenter Converter.

migration with vMotion
The process of moving a virtual machine that is powered on and meets selected requirements, including the activation of vMotion on both the source and target hosts. When you migrate a virtual machine using vMotion, the operations of the virtual machine can continue without interruption.

migration with VMware vCenter Converter
The process of moving a powered off virtual machine from a local or remote host, while reconfiguring the file format, if necessary, to accommodate the destination machine. See also migration with vMotion.

MOF (Managed Object Format)
A file format for the CIM IDL that describes model classes.

MoRef (managed object reference)
A managed object has a MoRef that is server specific. The MoRef is a pointer to an object.

NAS (network-attached storage)
A complete storage system that is designed to be attached to a traditional data network.

NAT (network address translation)
In hosted networking, a type of network connection that enables you to connect your virtual machines to an external network when you have only one IP network address and the host computer uses that address. The VMware NAT device passes network data between one or more virtual machines and the external network. It identifies incoming data packets intended for each virtual machine and sends them to the correct destination. See also bridged networking, vCenter Converter Boot CD (VMware vCenter Converter Boot CD), custom networking, host-only networking.

network access
Policies that give you detailed and flexible control over the network access you can provide to users of your ACE instances. Using a packet filtering firewall, the network access feature lets you specify exactly which machines or subnets an ACE instance or its host system may access.

network quarantine
A set of controls, governed by policies, that ensure only up-to-date virtual machines have access to specified resources on an organization's network. These controls enable administrators to specify which machines or subnets a virtual machine may access.

**NIC (network interface card)**
An expansion board that provides a dedicated connection between a computer and a network. Also called a network adapter.

**NIC teaming**
The association of multiple NIC adapters with a single virtual switch to form a team. Such teams can provide passive failover and share traffic loads between members of physical and virtual networks.

**nonpersistent mode**
A disk mode in which all disk writes that are issued by software running inside a virtual machine appear to be written to the independent disk. In fact, they are discarded after the virtual machine is powered off. As a result, a virtual disk or physical disk in independent-nonpersistent mode is not modified by activity in the virtual machine. See also disk mode, persistent mode.

**not-shared storage**
Amount of storage that is used only by a virtual machine and is not shared with other virtual machines. (This term was formerly called unshared storage.) Also, the amount of guaranteed storage that can be reclaimed if a virtual machine is migrated out of a datastore or is deleted.

**nvram (nonvolatile RAM)**
The file name used for storing BIOS settings belonging to a virtual machine.

**open virtual appliance (OVA)**
A packaging format for virtual machines that allows virtual machine templates to be distributed, customized, and instantiated on any OVA supporting VMM.

**Open Virtualization Format (OVF)**
A distribution format for virtual appliances that uses existing packaging tools to combine one or more virtual machines with a standards-based XML wrapper. OVF gives the virtualization platform a portable package containing all required installation and configuration parameters for virtual machines. This format allows any virtualization platform that implements the standard to correctly install and run virtual machines.

**package**
An installable bundle for distribution to end users. The package might include one or more virtual machines and an application used to run virtual machines.

**page file**
A component of an operating system that provides virtual memory for the system. Recently used pages of memory are swapped out to this area on the disk to make room in physical memory (RAM) for newer memory pages. Also called a swap file. See also virtual memory.

**paravirtual appliance**
Free virtual machines that are intended to demonstrate the Virtual Machine Interface (VMI) for virtual machine hypervisors. See also hypervisor.

paravirtual device
A device designed with specific awareness that it is running in a virtualized environment.

parent
The source virtual machine from which you take a snapshot or make a clone. If you delete the parent virtual machine, any snapshot becomes permanently disabled. In a VMware vSphere inventory, the managed entity that immediately encloses a given entity (considered the child entity). See also full clone, linked clone, snapshot, template.

partner activation code
In VMware Infrastructure 3, a unique code identifying orders placed through VMware partners. The code lets you register your purchase and obtain a license activation code.

partner activation portal
In VMware Infrastructure 3, a self-service Web portal used to register a purchase made from a VMware partner to your VMware store account. When you enter your partner activation code into the portal, you receive a license activation code.

performance counter
In VMware vSphere, information collected about an entity (such as a host or virtual machine). Counter information includes the group to which the counter belongs (for example, memory), counter ID, counter name, key, statistic type, rollup type, and the kind of entity for which the counter is reported. CPU usage is an example of a performance counter.

persistent mode
A disk mode in which all disk writes that are issued by software running inside a virtual machine are immediately and permanently written to a virtual disk that is configured as an independent disk. As a result, a virtual disk or physical disk in independent-persistent mode behaves like a conventional disk drive on a physical computer. See also disk mode, nonpersistent mode.

physical disk
In hosted products, a hard disk in a virtual machine that is mapped to a physical disk drive or partition on the host machine. A virtual machine's disk can be stored as a file on the host file system or on a local hard disk. When a virtual machine is configured to use a physical disk, vCenter Server directly accesses the local disk or partition as a raw device (not as a file on a file system). See also virtual disk.

physical network
A network of physical machines (plus cabling, switches, routers, and so on) that are connected so that they can send data to and receive data from each other. See also virtual network.

plain disk
A file that contains an exact image of a raw disk. VMware plain disks can also concatenate more than one raw disk into a single plain disk.

Pocket ACE
An ACE feature that allows the ACE administrator to distribute an ACE instance on a removable device such as a USB key, Apple iPod mobile digital device, or portable hard drive.

**policy**
A set of system-enforced rules that automatically run or inhibit actions upon entities such as virtual machines, processes, and users. Typically, a policy is configured and enforced in a hierarchical framework in which lower-level entities can inherit or override a policy set at a higher level. See also setting.

**port group**
A construct for configuring virtual network options such as bandwidth limitations and VLAN tagging policies for each member port. Virtual networks that are connected to the same port group share network policy configuration. See also virtual network, VLAN (virtual local area network).

**power cycle**
The process of disconnecting power from the computer and then adding power again. A power cycle generally has the effect of restarting the system.

**preallocated disk**
A type of virtual disk in which all disk space for the virtual machine is allocated at the time the disk is created.

**Preview mode**
An operating and viewing mode in which an administrator can preview the ACE instance as it will run on the user’s machine. The administrator uses this feature to see the effects of policy and configuration settings without performing the packaging and deployment steps. The preview mode displays the working copy of the policies. See also world.

**privilege**
Authorization to perform a specific action or set of actions on a managed object or group of managed objects.

**property**
An attribute of an object. In the VMware vSphere SDK, a property can be a nested data object, a managed object reference, or other data such as an integer or string.

**property collector**
A managed object used to control the reporting of managed object properties and the primary means of monitoring status on host machines.

**protected site**
The datacenter containing the virtual machines for which data is being replicated to the recovery site.

**protection group**
A group of virtual machines that are failed together during test and recovery.

**provisioned storage**
Maximum amount of storage the current entity can use.
provisioning
The process of creating a functioning virtual machine by assigning resources such as CPU, memory, and virtual hardware and then deploying a system image.

quick switch mode
A display mode in which the virtual machine’s display fills most of the screen. In this mode, tabs at the top of the screen enable you to switch quickly from one running virtual machine to another. See also full screen switch mode.

quiescing
A process of bringing the on-disk data of a physical or virtual computer into a state suitable for backups. This process might include flushing to disk dirty buffers from the operating systems in-memory cache or other higher level application-specific tasks.

raw disk
See physical disk.

RDM (raw device mapping)
A mechanism that enables a virtual machine to have direct access to a LUN on the physical storage subsystem (Fibre Channel or iSCSI only). At the same time, the virtual machine has access to the disk that is using a mapping file in the VMFS name space.

record/replay feature
Lets you record all of a Workstation 5 or 6 virtual machine's activity over a period of time. Unlike the Workstation movie-capture feature, the record/replay feature lets you duplicate the operations and state of the virtual machine throughout the time of the recording.

recovery plan
The steps to recover protected virtual machines in their assigned protection groups according to an order of priority defined in the plan.

recovery time objective
A measure of how long it takes you to recover following a disaster.

recovery site
The datacenter containing the recovery virtual machines performing work while the protected site is unavailable.

recovery virtual machine
A placeholder representing a protected virtual machine representing the virtual machines replicated from the protected site.

redo-log file
The file that stores changes made to a disk in all modes except the persistent and independent-persistent modes. For a disk in nonpersistent mode, the redo-log file is deleted when you power off or reset the virtual machine without writing any changes to the disk. You can permanently apply the changes saved in
the redo-log file to a disk in undoable mode so that they become part of the main disk files. See also disk mode.

**referential provisioning**

A process for linked clones that involves storing new changes but referring back to a chain of delta disks. For each clone, Lab Manager freezes the original delta disk and creates a new one. A linked clone operation generates a quick copy by creating a delta disk instead of copying an entire virtual hard disk.

**remote cloning**

Making a copy of a virtual machine or a physical machine accessed over the network by VMware vCenter Converter. See also local cloning.

**remote console**

An interface that provides nonexclusive access to a virtual machine from the server on which the virtual machine is running and from workstations connected to that server.

**resource pool**

A division of computing resources used to manage allocations between virtual machines.

**revert to snapshot**

To restore the status of the active virtual machine to its immediate parent snapshot. See also Go to snapshot, Snapshot Manager.

**role**

A defined set of privileges that can be assigned to users and groups to control access to VMware vSphere objects.

**sandbox**

The physical system location where the dynamic virtual environment runtime data is stored. Contents of the sandbox are tracked by the Virtual Operating System.

**scheduled task**

In a vCenter Server, an activity that is configured to occur at designated times. In VMware Converter, scheduled tasks consist of migrations and configurations of virtual machines.

**server**

(1) A system capable of managing and running virtual machines. (2) A process capable of accepting and running instructions from another process.

**server-based licensing**

In VMware Infrastructure 3, a mode of licensing VMware software in which all license keys are administered by a license server, which manages a central license pool. Feature entitlement is checked out and returned on demand. See also host-based licensing.

**service console**

The interface for ESX that enables administrators to configure the system. The service console is installed as the first component and used to bootstrap the ESX installation and configuration. The service console
also boots the system and initiates starting the virtualization layer and resource manager. You can open the service console directly on an ESX host. If the ESX host’s configuration allows Telnet or SSH connections, you can also connect remotely to the service console.

**service host**
The host on which a Web service executes.

**service instance**
In the VMware vSphere SDK, the managed entity that provides access to all other managed entities. Clients must access the service instance to begin a session.

**setting**
A configuration value or rule that determines the behavior of a specific entity, such as an application feature, or set of entities, such as virtual machines or users. A setting applies only to the specified entities. See also **policy**

**shared storage**
Amount of used storage minus the not-shared storage. Applies to virtual machines that can share storage with any other virtual machine, including linked clones.

**shrink**
To reclaim unused space in a virtual disk. If a disk has empty space, shrinking reduces the amount of space the virtual disk occupies on the host drive. Shrinking virtual disks is a way to update an older virtual disk to the format supported by the current version of vCenter Server. You cannot shrink pre-allocated virtual disks or physical disks.

**slot**
A unit of CPU and memory that can accommodate the CPU and memory reservation requirements of the largest virtual machine in your cluster. Spare capacity for failover is maintained on hosts in the cluster in slot sizes, so that any virtual machine in the cluster can fit in the slot size and be able to be failed over. The slot represents potential computing capacity on a node. A virtual machine can run in an empty slot in the event of failover.

**snapshot**
A reproduction of the virtual machine just as it was when you took the snapshot, including the state of the data on all the virtual machine’s disks and the virtual machine’s power state (on, off, or suspended).

You can take a snapshot when a virtual machine is powered on, powered off, or suspended. You can revert the configuration or virtual machine to a snapshot. If you undeploy a virtual machine and deploy it, the snapshot remains. See also **independent disk, snapshot delta, Snapshot Manager**.

**snapshot delta**
The comparison of the pre-installation and post-installation snapshots to determine what was changed on the packaging system. See also **snapshot, Snapshot Manager**.

**Snapshot Manager**
A control that enables you to take actions on any of the snapshots associated with the selected virtual machine. See also **snapshot, snapshot delta**.
source
In VMware vCenter Converter, the machine from which you import or create a virtual machine.

source virtual machine
In VMware vCenter Converter, the virtual machine to be imported, at its original location.

standalone ACE instance
An ACE instance that is not managed by an ACE Management Server. Any changes to the instance’s policies or other settings are made by the administrator’s distribution of updates to the user.

standalone virtual machine
A virtual machine that runs in VMware Workstation, VMware Server, and VMware Player. See also source virtual machine.

storage array
A storage system that contains multiple disk drives.

storage lease
The amount of time that an unused virtual machine template or configuration exists on a datastore before it is deleted or marked for deletion. This lease affects only unpublished virtual machine templates.

storage virtualizer
A system that abstracts and aggregates physical storage on behalf of a storage-using client.

storage virtualization devices
Device that aggregates capacity from multiple heterogeneous arrays and manages a logical representation of this capacity. Most of these devices can also have physical disks installed internally, which are presented to hosts as physical SAN LUNs that are not virtualized.

stub
A local procedure that implements the client side of a remote procedure call. The client calls the stub to perform a task. The stub packages the parameters, sends them over the network to the server, and returns the results to the client.

supported partition
A virtual disk partition that VMware Tools can prepare for shrinking, such as one of the drives that make up the virtual hard disk. See also shrink.

suspend
(in) A state in which settings are preserved and actions are no longer performed. (v) To turn off a virtual machine while preserving the current state of a running virtual machine.

swap file
See page file.

swapping
When you power on a virtual machine, a process in which a corresponding swap file is created and placed in the same location as the virtual machine configuration file (.vmx file). The virtual machine can power on only when the swap file is available. ESX/ESXi hosts use swapping to forcibly reclaim memory from a virtual machine when no vmmemctl driver is available.

**team**

A group of virtual machines configured to operate as one object. You can power on, power off, and suspend a team with one command. You can configure a team to communicate independently of any other virtual or real network by setting up a LAN segment. See also LAN segment, NIC teaming, virtual network.

**template**

A master image of a virtual machine. The template typically includes a specified operating system and a configuration that provides virtual counterparts to hardware components. Optionally, a template can include an installed guest operating system and a set of applications. Templates are used by vCenter Server to create new virtual machines. See also linked clone, parent, snapshot.

**templates list**

A list of virtual machines that provides a means to import and store virtual machines as templates. You can deploy the templates at a later time to create new virtual machines.

**template upload directory**

In VirtualCenter 1.x, a directory that stores copies of the original virtual machine's virtual disks. Copies of the original virtual machine's virtual disks are placed in the directory you specify as the template upload directory. This directory is used when you create templates from virtual machines that are stored locally on the VirtualCenter 1.x rather than on an ESX host or GSX Server system.

**uncommitted storage**

Amount of provisioned storage minus used storage. Uncommitted storage is a general term that can refer to unused physical capacity and unused logical capacity. Uncommitted storage includes unused logical capacity.

**undoable mode**

In ESX 2.x, a disk mode in which all write operations that are issued by software running inside the virtual machines appear to be written to the disk, but, in fact, are stored in a temporary file (.REDO) for the duration of the session. When the virtual machine is powered off, the user has these choices: permanently apply all changes to the disk; discard the changes, and restore the disk to its previous state; or keep the changes, so that further changes from future sessions can be added to the log. See also disk mode.

**unsupported partition**

A virtual disk partition that VMware Tools cannot prepare for shrinking. Unsupported partitions include read-only drive partitions, partitions on remote devices, and partitions on removable devices. See also shrink.

**uptime**

The total elapsed time since the host or virtual machine was last restarted.

**used storage**
Refers to used storage at the virtual machine or datastore level. (This term was formerly called committed storage.) At the virtual machine level, used storage refers to the space used by disks, swap, logs, cores, and so on.

**Valid cluster**

A cluster that is not overcommitted or otherwise invalid.

**VCB proxy (VMware Consolidated Backup proxy)**

In VMware Consolidated Backup, a physical or virtual machine running Microsoft Windows 2003, Consolidated Backup, and third-party backup software. VCB proxy is used to perform file-level and

**vCenter agent**

Installed on each virtual machine host, this software coordinates actions received from vCenter Server.

**vCenter Converter Boot CD (VMware vCenter Converter Boot CD)**

The means by which a user can perform a local cold clone of a physical machine. When the physical machine is booted from the vCenter Converter Boot CD, the Converter application runs on WinPE. It uses a RAM disk for its operations and leaves no footprint on the physical machine.

**vCenter Server administrator**

A role in which the user can set the user and role permissions and control vCenter Server licensing.

**vCenter Server database**

A persistent storage area for maintaining the status of each virtual machine and user that is managed in the vCenter Server environment. Located on the same machine as the vCenter Server.

**vDS (distributed virtual switch)**

An abstract representation of multiple hosts defining the same vSwitch (same name, same network policy) and port group. These representations explain the concept of a virtual machine being connected to the same network as it migrates among multiple hosts.

**vHandle**

A reference to the specific memory state of an object at a certain time. A vHandle is an object handle that has a version number associated with it. The version number determines the specific memory state.

**Vintage server**

In Capacity Planner Dashboard, a server that does not meet minimum CPU speed requirements, as defined in the Dashboard consolidation scenarios by the Information Warehouse Administrator, company Administrator, or company Power User. See also instance customization.

**Virtual appliance**

A software solution that is composed of one or more virtual machines. A virtual appliance is packaged as a unit by an appliance vendor and is deployed, managed, and maintained as a unit. Converting virtual appliances allows you to add preconfigured virtual machines to your vCenter Server, ESX/ESXi, Workstation, or Player inventory.

**Virtual disk**
A file or set of files that appears as a physical disk drive to a guest operating system. These files can be on the host machine or on a remote file system. See also growable disk, physical disk, preallocated disk.

**virtual hardware**
The devices that make up a virtual machine. The virtual hardware includes the virtual disk, removable devices such as the DVD-ROM/CD-ROM and floppy drives, the virtual Ethernet adapter, and so on. See also virtual machine settings editor.

**virtual machine**
A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. Multiple virtual machines can operate on the same host system concurrently.

**virtual machine administrator**
A role in which the user can perform all the virtual machine management functions.

**virtual machine array**
A set of virtual machines that can be operated on collectively. Currently called a VM Group or VM Folder in vCenter Server.

**virtual machine communication interface (VMCI)**
An infrastructure that provides communication between a virtual machine and the host operating system and between two or more virtual machines on the same host. The VMCI Sockets API facilitates development of applications that use the VMCI infrastructure.

**virtual machine configuration**
The specification of which virtual devices, such as disks and memory, are present in a virtual machine and how they are mapped to host files and devices. In vCenter Converter, VMware virtual machines whose disks have been populated by restoring from a backup or by some other direct means of copying undergo configuration to enable them to boot in VMware products. See also virtual machine.

**virtual machine configuration file**
A file containing a virtual machine configuration. This .vmx file is created when you create the virtual machine. It is used to identify and run a specific virtual machine.

**virtual machine console**
An interface to a virtual machine within the larger Lab Manager Web console. Use the virtual machine console to run programs within it or modify guest operating system settings.

**virtual machine disk (VMDK)**
A file or set of files that appears as a physical disk drive to a guest operating system. These files can be on the host machine or on a remote file system.

**Virtual machine group**
An optional grouping structure and a subset of a farm. vCenter Server supports multiple virtual machine groups. Virtual machine groups contain virtual machines and other virtual machine groups.

**virtual machine settings editor**
A point-and-click control panel used to view and modify the settings of a virtual machine setting.

**virtual memory**
An extension of a system’s physical memory, enabled by the declaration of a page file. See also *page file*.

**virtual network**
A network connecting virtual machines that does not depend on physical hardware connections. For example, you can create a virtual network between a virtual machine and a host that has no external network connections. You can also create a LAN segment for communication between virtual machines on a team. See also *LAN segment*, *team*.

**virtual switch**
A virtualized network switch used by ESX/ESXi to manage traffic between virtual machines, the service console (ESX only), and the physical network adapters on the ESX/ESXi host.

**VLAN (virtual local area network)**
A software-managed logical segmentation of a physical LAN. Network traffic within each segment is isolated from traffic in all other segments.

**VM**
An acronym for virtual machine.

**VMA (VMware virtual machine agent)**
The VMware vCenter Server Web service that provides a Web services interface to enable client programs to talk to each other using the SOAP protocol.

**VmCOM**
A COM binding for the legacy VMware Scripting API supported on ESX 3.0.x and GSX Server.

**VmPerl**
A Perl binding for the legacy VMware Scripting API supported on ESX 3.0.x and GSX Server.

**VMFS (Virtual Machine File System)**
A file system that is optimized for storing virtual machines. One VMFS partition is supported for each SCSI storage device or LUN.

**VMkernel**
In ESX/ESXi, a high-performance operating system that occupies the virtualization layer and manages most of the physical resources on the hardware, including memory, physical processors, storage, and networking controllers.

**VMM (virtual machine monitor)**
Software that is responsible for virtualizing the CPUs. One VMM runs in kernel space for each running virtual machine.

**VMware authorization service**
The service that authenticates users. The process is called vmware-authd.

**VMware guest operating system service**

A component installed with VMware Tools that runs commands in the virtual machine, gracefully shuts down and resets the virtual machine, sends a heartbeat to VMware Migration Server, synchronizes the time of the guest operating system with the host operating system, and passes strings from the host operating system to the guest operating system.

**VMware Management Interface**

In VMware server, a Web-based management tool that enables you to control (start, suspend, resume, reset, and stop), configure, and monitor virtual machines and the server on which they run.

**VMware registration service**

The service that manages connections to virtual machines and the management interface. This process is known as vmware-serverd.

**VMware Server Console**

An interface to a virtual machine that provides access to one or more virtual machines on the local host or a remote host running vCenter Server. You can view the virtual machine’s display to run programs within it or to modify guest operating system settings. You can also change the virtual machine’s configuration, install the guest operating system, or run the virtual machine in full screen mode.

**VMware virtual machine console**

An interface that provides access to one or more virtual machines on the local host or on a remote host running vCenter Server. You can view a virtual machine’s display to run programs within it, or you can modify guest operating system settings. You can also change the virtual machine’s configuration, install the guest operating system, or run the virtual machine in full screen mode.

**vNIC**

A virtual network interface card that is configured on top of a system's physical Network adapter. See also NIC (network interface card).

**VRM (Virtual Rights Management)**

Centralized management of security policies and access rights applied to VMware ACE running on an end-user PC.

**vSwitch**

See virtual switch.

**world**

A entity that can be scheduled and that executes on an ESX Server. It is similar to a process or thread in a traditional operating system.

**zoning**

Provides access control in the SAN topology. Zoning defines which HBAs can connect to which storage processors. You can have multiple ports to the same storage processor in different zones to reduce the number of presented paths.
About GE

GE (NYSE: GE) is the world's Digital Industrial Company, transforming industry with software-defined machines and solutions that are connected, responsive and predictive. GE is organized around a global exchange of knowledge, the "GE Store," through which each business shares and accesses the same technology, markets, structure and intellect. Each invention further fuels innovation and application across our industrial sectors. With people, services, technology and scale, GE delivers better outcomes for customers by speaking the language of industry. www.ge.com

©2016 General Electric. All rights reserved. *Trademark of General Electric. All other brands or names are property of their respective holders. Specifications are subject to change without notice.