Introduction to VMware vSphere

o   **vCompute** – aggregate resources
o   **vStorage** – enables the most efficient use and management of storage
o   **vNetwork** – simplify and enhance networking
o   **Fault Tolerance** – a secondary copy. Actions completed on the primary VM are also applied to the secondary VM. If the primary VM becomes unavailable, the secondary machine becomes active, providing continual availability.
o   **Distributed Virtual Switch (DVS)** – spans many hosts reduction of maintenance and increasing network capacity.
o   **Host Profiles** – host configuration management through user-defined configuration policies. Captures the blueprint and monitors compliance.
o   **Pluggable Storage Array (PSA)** – greater array certification flexibility and improved array-optimized performance. A multipath I/O framework.
o   **Cluster** – aggregate computing and memory resources of a group of physical x86 servers sharing the same network and storage arrays.
o   **Resource pools** – partitions of computing and memory resources from a single host or a cluster. can be hierarchical and nested.
o   **Storage VMotion** – enables the migration of VMs from one datastore to another datastore without service interruption
o   **Fault Tolerance (FT)** – uses vLockstep technology, continuous availability by protecting a VM (the Primary VM) with a shadow copy (Secondary VM) that runs in virtual lockstep on a separate host.
o   **vNetwork Distributed Switch (dvSwitch)** – functions as a single virtual switch across all associated hosts.
o   **dvPort (distributed virtual port)** – a port on a DVS that connects to a host's service console or VMkernel or to a VM's network adapter.
o   **vApp** – has the same basic operation as a VM, but can contain multiple VMs or appliances.
o   Web Access cannot be used to access a host running ESXi 4.0.
o   Web Access is turned off by default for ESX hosts.

Getting Started with ESX

o   ESX Service Console is held in the esxconsole.vmdk partition.
o   vCenter Server uses Microsoft SQL Server 2005 Express for small deployments with up to 5 hosts and 50 VMs.
o   If SQL Native Client is already installed, uninstall SQL Native Client before you begin the vCenter Server installation.
o   vCenter server must belong to a domain rather than a workgroup. Otherwise it's not able to discover – using such features as vCenter Guided Consolidation Service. The computer name cannot be more than 15 characters.
o   vCenter Server should not be an Active Directory domain controller.
o   The Domain user account should have the following permissions:
    o   Member of the Administrators group
    o   Act as part of the operating system
    o   Log on as a service

ESX and vCenter server installation guide

o   ESX4 will only install and run on servers with 64-bit x86 CPUs. They require a 2GB RAM minimum.
o   vCenter Server must have 2 CPUs and 3GB RAM.
o   The vCenter Server has a service called VMware VirtualCenter Management Webservices. This service requires 128MB to 1.5GB of additional memory.
o   You can use a 32-bit Windows for up 200 hosts. A 64-bit Windows can have 200-300 hosts.
o   The vSphere Client requires the Microsoft .NET 3.0 SP1 Framework.
o   vCenter server required firewall ports:

Port	Description
80	Redirects requests to HTTPS port 443.
389	LDAP port number for the Directory Services for the vCenter Server group. Needs to bind to port 389, even if you are not joining this vCenter Server instance to a Linked Mode group.
443	Listen for connections from the vSphere Client.
636	For vCenter Linked Mode, this is the SSL port of the local instance
902	Uses to send data to managed hosts. Managed hosts also send a regular heartbeat over UDP port 902 to the vCenter
902/903	Ports used by vSphere Client to display VM consoles.
8080	Web Services HTTP. Used for the VMware VirtualCenter Management Webservices.
8443	Web Services HTTPS. Used for the VMware VirtualCenter Management Webservices.

o   If ESX will not use an NTP server, make sure that the server hardware clock is set to UTC
o   IPv6 is not supported for ESX installation
o   The service console must be installed on a VMFS datastore that is resident on a host's local disk or on a SAN disk that is masked and zoned to that particular host only.
o   The evaluation period is 60 days and begins as soon as you power on the ESX machine, even if you start in license mode initially.

o   The installer creates three basic partitions: /boot, vmkcore and VMFS. The service console VMDK file contains swap, and /var/log, by default, and any other partitions that you specify.
o   The media depot is a network-accessible location that contains the ESX installation media. You can use HTTP/ HTTPS, FTP, or NFS to access the depot.
o   Scripted installation – you must point to the media depot in the script by including the install command with the nfs or url option.
o   Interactive installation – include the askmedia boot option.
o   The boot options list appears when you boot the installer and press F2.
o   Bootstrap Commands for ESX Installation

Command	Description
askmedia	Allows you to interactively select the location of the ESX installation media. This option is required if the image is hosted at an HTTP, FTP, or NFS location.
BOOTIF	Accepts the format for the boot network adapter as supplied by PXELINUX.
gateway=<ip address>	Sets this network gateway as the default gateway during the install.
ip=<ip address>	Specifies a static IP address to be used for downloading the script and the installation media. The IPAPPEND option is also supported if you PXE boot the installer.
ks=cdrom:/<path>	Performs a scripted installation with the script at <path>, which resides on the DVD in the DVD-ROM drive.
ks=file://<path>	Performs a scripted installation with the script at <path>, which resides inside the initial ramdisk image.
ks=ftp://<server>/<path>/	Performs a scripted installation with a script located at the given URL.
ks=http://<server>/<path>	Performs a scripted installation with a script located at the given URL.
ks=https://<server>/<path>	Performs a scripted installation with a script located at the given URL.
ks=nfs://<server>/<path>	Performs a scripted installation with the script located at <path> on a given NFS server.
ks=usb	Performs a scripted installation with the ks.cfg script in the root directory of the USB flash drive attached to the host. If multiple flash drives are attached, the installer cycles through each one, mounting and unmounting them until the file named ks.cfg is found.
ks=UUID:<partition-UUID>:/<path>	Performs a scripted installation with a script located on the ext partition with the given UUID.
ksdevice=<device>	Same as netdevice
nameserver=<ip address>	Specifies a domain name server as the nameserver during the install.
netdevice=<device>	Tries to use a network adapter <device> when looking for an installation script and installation media. Specify as a MAC address (for example, 00:50:56:C0:00:01). If not specified and files need to be retrieved over the network, the installer defaults to the first discovered network adapter. The IPAPPEND option is also supported if you PXE boot the installer.
netmask=<subnet mask>	Specifies subnet mask for the network interface that downloads the installation media.
noapic	Flags the kernel to use the XTPIC instead of the APIC.
text	Starts the ESX installer in text mode.
url=<url>	Looks for the installation media at the specified URL. When you are PXE booting the installer, the url= command only works with earlier versions of SYSLINUX. The command does not work with SYSLINUX/PXELINUX version 3.70 and higher.
vlanid=<vlanid>	Configures the VLAN for the network card.

o   PXE Boot the ESX Installer:
    1.   Install TFTP server software that supports PXE booting.
    2.   Put menu.c32 file in an accessible place
    3.   Install PXELINUX.
    4.   Configure the DHCP server.
    5.   Create the kernel image and ramdisk directory by copying the vmlinuz and initrd.img files from the /isolinux directory on the ESX installation DVD to a supported location.
    6.   Create the /tftpboot/pxelinux.cfg directory on your TFTP server.
    7.   Create a PXE configuration file. PXE configuration file in /tftpboot/pxelinux.cfg
o   In an interactive installation, omit the ks= option.
o   ESX 3.x supported a hybrid installation. You could supply an incomplete ESX installation script, and the installer prompts you for the missing parts. ESX 4.0 does not support this.
o   Install ESX interactively or by using a script. For interactive installation, you can use graphical mode or text mode.
o   The installer erases all content on the selected storage device.
o   Installing ESX on a USB device is not supported.
o   VMFS2 volumes are not recognized by ESX 4.0.
o   The installation log is /var/log/esx_install.log.
o   The installation script can reside in one of the following locations:
    o   Default installation script   o   HTTP/HTTPS   o   USB flash drive
    o   FTP   o   NFS   o   Local disk
o   The installer creates a /root/ks.cfg script, which reflects the choices you made in the interactive installation.
o   Installation media contains the following default installation scripts:

- o **ks-first-safe.cfg** Installs ESX on the first detected disk and preserves the VMFS datastores on the disk.
  - o **ks-first.cfg** Installs ESX on the first detected disk.
- o The default root password is mypassword.
- o /boot and vmkcore are physical partitions. /, swap, /var/log, and all the optional partitions are stored on a virtual disk called *esxconsole-<system-uuid>/esxconsole.vmdk*. The virtual disk is stored in a VMFS volume.
- o You cannot define the sizes of the /boot, vmkcore, and /vmfs partitions when you use the graphical or text installation modes. You can define these partition sizes when you do a scripted installation.
- o ESX Required Partitions

Mount Point	Type	Size	Location
/boot	ext3	1.25GB of free space and includes the /boot and vmkcore partitions. The /boot partition alone requires 1100MB.	Physical partition
N/A	swap	600MB recommended minimum 1600MB maximum.	Virtual disk in a VMFS volume
/	ext3	Based on the size of the /usr partition. By default, the minimum size is 5GB and no /usr partition is defined.	Virtual disk in a VMFS volume
N/A	VMFS3	For VMFS volumes hosting esxconsole.vmdk: 1200MB and an additional 10GB. VMFS2 is supported in read-only mode to import legacy VMs.	Physical partition.
N/A	vmkcore	See /boot	Physical partition

- o ESX Optional Partitions

Mount Point	Type	Recommended Size	Location
/home	ext3	512MB	Virtual disk in a VMFS volume
/tmp	ext3	1024MB	Virtual disk
/usr	ext3	Missing in PDF	Virtual disk
/var/log	ext3	2000MB	Virtual disk. The graphical and text installers create this partition by default.

- o vihostupdate command applies software updates to ESX4/ESXi4 hosts and installs and updates ESX/ESXi extensions (use vihostupdate35 on ESX 3.5/ESXi 3.5 hosts.)
- o The esxupdate utility is for ESX only.
- o You can use the vihostupdate utility in conjunction with offline bundles or with a depot
- o vSphere Databases:
  - o Microsoft SQL Server 2005 Express – up to 5 hosts and 50 VMs. If the machine has Microsoft SQL Native Client installed, remove it before installing vCenter Server with the bundled database. If the machine has MSXML Core Services 6.0 installed, remove it before installing
  - o Microsoft SQL Server 2005 – Windows XP, apply MDAC 2.8 SP1 to the client. Use the SQL Native Client driver (version 9.x) for the client. Ensure that the machine has a valid ODBC DSN entry. Remove MSXML Core Services 6.0 before
  - o Microsoft SQL Server 2008 – Windows XP, apply MDAC 2.8 SP1 to the client. Use the SQL Native Client driver (version 10.x) for the client. Ensure that the machine has a valid ODBC DSN entry.
  - o Oracle 10g – If necessary, first apply patch 10.2.0.3 (or later) to the client and server. Then apply patch 5699495 to the client. Ensure that the machine has a valid ODBC DSN entry.
  - o Oracle 11g – Ensure that the machine has a valid ODBC DSN entry.
- o Even though vCenter Server is supported on 64-bit operating systems, the vCenter Server system must have a 32-bit DSN. This requirement applies to all supported databases. By default, any DSN created on a 64-bit system is 64 bit. On a 64-bit system use C:\WINDOWS\SYSWOW64\odbc32.exe.
- o vCenter Server must have a computer name that is 15 characters or fewer. The data source name (DSN) and remote database systems can have names with more than 15 characters.
- o To prepare a SQL Server database to work with vCenter Server, you generally need to create a SQL Server database user with database operator (DBO) rights.
- o If you use SQL Server for vCenter Server, do not use the master database.
- o When using Microsoft SQL Server 2008 Standard Edition with vCenter Server, do not name the instance MSSQLSERVER.
- o The vCenter Server performs a silent installation of vCenter Orchestrator. If you install vCenter Server on an IPv6 operating system, the vCenter Orchestrator module is not supported.
- o The vSphere Host Update Utility is for updating and patching ESXi 4.0 hosts and upgrading ESX 3.x/ESXi 3.5 hosts to ESX 4.0/ESXi 4.0.
- o You can join multiple vCenter Server systems to form a Linked Mode group.
- o Linked Mode global data includes:
  - o Connection information (IP and ports)
  - o Certificates
  - o Licensing information
  - o User roles

o   vCenter Server instances in a Linked Mode group can be in different domains if the domains have a two-way trust relationship.
o   The installer must be run by a domain user who is an administrator on both the machines.
o   The vCenter Server installer validates that the machine clocks are not more than 5 minutes apart.
o   The instances can run under different domain accounts.
o   Windows Server 2008 automatically configures the firewall to permit access. Launch firewall.cpl and add an exception for C:\Windows\ADAM\dsamain.exe
o   When you install vCenter Server in Linked Mode, the firewall configuration on any network-based firewalls must be modified.
o   Configure Windows RPC ports to generically allow selective ports for machine-to-machine RPC communication.
o   vCenter Collector service – uses port 8181 and 8182, by default.
o   vCenter Web Server – uses ports 8080 and 8443, by default.
o   All product licenses are encapsulated in 25-character license keys that you can manage and monitor from vCenter Server.
o   vSphere Licenses – For ESX/ESXi.
o   vCenter Server Licenses – For vCenter Server.
o   vCenter Server 4.0 does not require a license server to manage ESX 4.0/ESXi 4.0 hosts. However, vCenter Server 4.0 does requires a license server to manage ESX 3.x/ESXi 3.5 hosts.
o   If a vCenter Server license expires, the managed hosts become disconnected.
o   If an ESX/ESXi host license expires, the VMs that reside on the host continue to run, but you cannot power on the VMs or reset them.

License Server Configuration for vCenter Server 4.0 – ESX 3.x licensing

o   Using vCenter Server 4.0 to manage ESX 3.x/ESXi 3.5 hosts, you have several options:
    o   A single license server for vCenter Server 4.0 and the ESX 3.x/ESXi 3.5 hosts.
    o   One license server for vCenter Server 4.0, and use another license server for the ESX 3.x/ESXi 3.5 hosts.
    o   A license server for vCenter Server 4.0, and use host-based licensing for the ESX 3.x/ESXi 3.5 hosts.
    o   Do not use a license server. Upgrade all of your hosts to ESX 4.0/ESXi 4.0.

vSphere upgrade guide

o   When you upgrade from ESX 3.x/ESXi 3.5 to ESX 4.0/ESXi 4.0, you can use either the vSphere Host Update Utility or vCenter Update Manager.
o   **EDIT** – you can also use the upgrade script (esxupgrade.sh – KB 1009440). VMware doesn't mention the option of a fresh install at any point; they are pushing the upgrade option as much as possible. You can't seem to do an upgrade with the ESX4 install CD.
o   Host Update Utility is used for upgrading ESX 3.x/ESXi 3.5 standalone hosts to ESX 4.0/ESXi 4.0 and for patching ESXi 4.0 standalone hosts. It is a standalone Microsoft Windows application recommended for smaller deployments with fewer than 10 ESX/ESXi hosts, without vCenter Server or Update Manager.
o   vCenter Update Manager is for upgrading and updating ESX/ESXi hosts that are managed in vCenter Server.
o   Orchestrated upgrades can be used to upgrade the VM hardware and VMware Tools.
o   No VMFS upgrade is required if you are upgrading from ESX 3.x
o   You must upgrade VMware Tools before upgrading virtual hardware.
o   After you upgrade to vCenter Server, you cannot revert to VirtualCenter 2.x. Take appropriate backups before starting the upgrade.
o   Upgrade VirtualCenter 2.x to vCenter Server 4.0:
    o   Make sure your database is compatible
    o   Have required permissions
    o   Take a full backup of the VirtualCenter 2.x database
    o   Back up the VirtualCenter 2.x SSL certificates
    o   Install the vSphere Client
    o   vCenter Converter, upgrade
    o   vCenter Guided Consolidation upgrade
    o   Upgrade to vCenter Update Manager 4.0.
    o   Use vCenter Update Manager to upgrade ESX 3.x hosts to ESX 4.0. (or use host update utility)
    o   Use vCenter Update Manager to upgrade your VMs. vCenter Update Manager ensures that the VMware Tools upgrade and the virtual hardware upgrade happen in the correct order
    o   Upgrade your product licenses
o   ESX 2.x hosts cannot be added to clusters.
o   Oracle 9i is no longer supported.
o   Microsoft SQL Server 2000 is no longer supported.
o   To Back Up VirtualCenter 2.x:
    o   Make a full backup of the VirtualCenter 2.x database.
    o   Back up the VirtualCenter 2.x SSL certificates. %ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter or %ALLUSERSPROFILE%\VMware\VMware VirtualCenter\.
    o   Note any non-default settings, such as the IP address, the database DSN, user name, password, and assigned ports.

- o Create a backup copy of vpxd.cfg.
- o The database upgrade log is at %TEMP%\VCDatabaseUpgrade.log.
- o By default, a vCenter Server creates a maximum of 10 simultaneous database connections.
- o Datastores and networks have their own set of privileges that control access to them.
- o Users are initially granted the No Access role on all new managed objects, including datastores and networks. All existing objects in vCenter maintain their permissions after the upgrade.
- o The upgrade process uses the datacenter's "Read-only" privilege.
  - o If the "Read-only" privilege is nonpropagating (not inherited by child objects), VMware assumes access privileges should not be assigned to datastores and networks.
  - o If the "Read-only" privilege is propagating (inherited by child objects), VMware assumes access privileges should be assigned to datastores and networks so users can view them and perform basic operations that require access.
- o The "Read-only" propagating permission on a datacenter, as well as all other permissions you have set, will continue to work as expected after the upgrade.
- o You must change "Read-only" nonpropagating datastore permissions to propagating datastore permissions in order for users to access the datastore. You can assign datastore permissions on datastore or folders containing datastore. The same goes for Network permissions.
- o The "Database Consumer" sample role assigns the "Allocate Space" privilege to the datastore. "Network Consumer" sample role assigns the "Assign Network" privilege.
- o Host Update Utility does not upgrade VMFS datastores or VM
- o Update Manager supports mass remediation.
- o During host upgrades using the Update Manager, static IP addresses are a requirement.
- o The upgrade to ESXi4 & ESX4 preserves almost all configuration data, including your networking, security, and storage configuration. The only configuration not preserved is related to licensing.
- o For ESX only, the upgrade reuses the existing /boot partition to hold the ESX 4.0 boot files. After the upgrade, the ESX 3.x installation is mounted in the new ESX 4.0 installation under the /esx3-installation directory.
- o Backup the ESX Host Configuration:
  - o Back up the files in the /etc/passwd, /etc/groups, /etc/shadow, and /etc/gshadow directories.
  - o Back up any custom scripts.
  - o Back up your .vmx files.
  - o Back up local images, such as templates, exported VMs, and .iso files.
- o Backup the ESXi Host Configuration: `vicfg-cfgbackup --server <ESXi-host-ip> --portnumber <port_number> -- protocol <protocol_type> --username username --password <password> -s <backup-filename>`
- o You cannot perform an in-place upgrade from ESX to ESXi (or from ESXi to ESX).
- o The only ESX 2.x version that has upgrade support is ESX 2.5.5 – you can perform a migration upgrade with or without VMotion.
- o Direct, in-place upgrade from ESX 2.5.5 to ESX 4.0 is not supported, even if you upgrade to ESX 3.x as an intermediary step. The default ESX 2.5.5 installation creates a /boot partition that is too small to enable upgrades to ESX 4.0. As an exception, if you have a non-default ESX 2.5.5 installation on which at least 100MB of space is available on the /boot partition, you can upgrade ESX 2.5.5 to ESX 3.x and then to ESX 4.0.
- o The upgrade logs are here:
  - o /esx3-installation/esx4-upgrade/
  - o /var/log/vmware/
- o For an unsuccessful ESX upgrade:
  - o /esx4-upgrade/
  - o /var/log/vmware/
- o You may need to reconnect the host to vCenter Server and assign an upgraded license to your product within 60 days after the upgrade.
- o The host sdX devices might be renumbered after the upgrade.
- o You must convert LUN masking to the claim rule format. Run the `esxcli corestorage claimrule convert` command. It converts the /adv/Disk/MaskLUNs advanced configuration entry in esx.conf to claim rules with MASK_PATH as the plug-in.
- o Web Access service is disabled after you upgrade the host.
- o vSphere Web Access is not supported on ESXi hosts.
- o 60-day evaluation count down starts even if the host is licensed and you are not using evaluation mode.
- o One advantage of using evaluation mode is that it offers full feature functionality.
- o After you determine that the ESX 4.0 upgrade is stable, you can remove the ESX 3.x boot option from the ESX 4.0 bootloader menu to disable the ability to roll back to ESX 3.x. If you deselected the rollback option, this procedure is not applicable. Run the `cleanup-esx3` command with the optional -f (force) flag.
- o The cleanup-esx3 script removes the following files and references from the ESX 4.0 host:
  - o ESX 3.x references in the /etc/fstab directory
  - o ESX 3.x boot files in the /boot directory
  - o The rollback-to-esx3 script in the /usr/sbin/ directory
- o After you upgrade all of your hosts to ESX4/ESXi4, you can optionally uninstall your license server and remove the license server configuration from vCenter Server.
- o For ESXi, the vSphere Host Update Utility does not support roll back.

o You can remove the ESX 4.0 boot option from the ESX bootloader menu and perform a complete roll back to ESX 3.x. Any changes made to the ESX 4.0 service console are lost after the rollback.
  o Any changes made to VMs will persist after the rollback.
  o If you upgraded the VM hardware, the VMs will not work after you perform the ESX rollback. To avoid this situation, take a snapshot of the VM before you upgrade the VM hardware.
      o Run the rollback-to-esx3 command – reconfigures the bootloader.
      o Reboot the server.
      o After the host boots into ESX 3.x, delete the ESX 4.0 service console VMDK folder from the VMFS datastore.
o Each time you update an ESXi host, a copy of the ESXi build is saved on your host.
o ESXi permits only one level of rollback.
o When you manually boot into the standby build instead of the current boot build, an irreversible rollback occurs.
o When the page that displays the current boot build appears, press Shift+r to select the standby build.
o Do not use vmware-vmupgrade.exe to upgrade VMs.
o Some VMs that you create on ESX4 hosts are supported on ESX 3.x/ESXi 3.5 hosts. If you create a VM on ESX4 and select the typical path, the virtual hardware version is version 7. Virtual machines with virtual hardware version 7 are not supported on ESX 3.x/ESXi 3.5 hosts. Select the custom path and select virtual hardware version 4
o If you create VMs that use paravirtualization (VMI) or an enhanced networking device (vmxnet), VMotion is not supported. In this case, you can only move the VM to the ESX 3.x host if the VM is powered off.
o On Windows guest operating systems, you must reboot the VM a total of three times when you upgrade VMware Tools and the virtual hardware:
  1. Power on the VM.
  2. Upgrade VMware Tools.
  3. Reboot the VM at the end of the VMware Tools upgrade.
  4. Power off the VM.
  5. Upgrade the virtual Hardware.
  6. Power on the VM.
  7. The Windows operating system detects new devices and prompts you to reboot the VM.
  8. Reboot the VM to make the devices work properly.
o During the virtual hardware upgrade, the VM must be shut down for all guest operating systems.
o When you upgrade from virtual hardware version 3 to version 7, the upgrade is irreversible, even if you take a VM backup or snapshot before performing the upgrade. 4 to version 7 the upgrade is reversible if you take a VM backup or snapshot
o Tools for installing updates and patches to ESX/ESXi hosts:
  o Host Update Utility – graphical utility for ESXi only.
  o Update Manager – for ESX and ESXi,
  o vihostupdate – command-line utility for ESX and ESXi.
  o esxupdate – command-line utility for ESX only.
o If the Host Update Utility does not meet the needs of your environment, you can customize the application the settings.config XML file, located in %PROGRAMFILES%\VMware\Infrastructure\VIUpdate 4.0
o Run vihostupdate on ESX 4.0/ESXi 4.0 hosts. Run vihostupdate35 on ESX 3.5/ESXi 3.5 hosts.
o The esxupdate utility is supported as well. It is for ESX only.
o The vihostupdate command works with bulletins.
o You can use the vihostupdate utility in conjunction with offline bundles or with a depot.
o To get the build number of an ESX4 host: `# vmware -l` (from KB 1001179).

vSphere Basic System Administration

o VMware modules (plugins) include:
  o Update Manager
  o Converter Enterprise
  o vShield Zones – an application-aware firewall built for vCenter Server integration. It inspects client-server communications and inter-virtual-machine communication to provide detailed traffic analytics and application-aware firewall partitioning.
  o Orchestrator – a workflow engine that enables you to create and execute automated workflows.
  o Data Recovery – a disk-based backup and recovery solution. Enable centralized and efficient management of backup jobs and includes data de-duplication.
o Tomcat Web server is installed as part of the vCenter Server installation. The components that require Tomcat are:
  o Linked Mode
  o CIM/Hardware Status tab
  o Performance charts
  o WebAccess

- o vCenter Storage Monitoring/Storage Views tab
- o vCenter Service Status
- o When a server is connected to other vCenter Server systems using Linked Mode, you can connect to that vCenter Server system and view and manage the inventories of all the vCenter Server systems that are linked.
- o Linked Mode uses Microsoft Active Directory Application Mode (ADAM) to store and synchronize data.
- o The following requirements apply to each vCenter Server system that is a member of a Linked Mode group:
  - o DNS must be operational.
  - o Can be in different domains if the domains have a two-way trust relationship.
  - o When adding a vCenter instance to a Linked Mode group, the installer must be run by a domain user who is an administrator on both the machines.
  - o Must have network time synchronization. The installer validates that the machine clocks are not more than 5 minutes apart.
- o The roles defined on each vCenter Server system in a linked mode group are replicated to the other systems in the group.
- o Troubleshooting:
  - o Conflicts can occur, when you clone a vCenter Server instance that is running in a VM and you do not use sysprep or a similar utility to ensure that the cloned vCenter Server instance has a globally unique identifier (GUID).
  - o The DNS name of the machine must match with the actual machine name.
  - o Joining a Linked Mode group:
    1. Verify that the vCenter Server domain name matches the machine name.
    2. Update the URLs to make them compatible with the new domain name and machine name (if required).
    3. Join the vCenter Server system to a Linked Mode group.
- o When you are logged in to a vCenter Server system that is part of a connected group, you can monitor the health of services running on each server in the group.
- o Client uses ports 80 and 443 to communicate with vCenter Server and ESX/ESXi hosts. These ports cannot be changed.
- o The SNMP traps sent by vCenter Server are defined in VMWARE-VC-EVENT-MIB.mib
- o ESX/ESXi includes an SNMP agent embedded in hostd that can both send traps and receive polling requests such as GET requests. This agent is referred to as the embedded SNMP agent. Versions of ESX prior to ESX 4.0 included a Net-SNMP-based agent. You can continue to use this Net-SNMPbased agent in ESX 4.0 with MIBs supplied by your hardware vendor and other third-party management applications. However, to use the VMware MIB files, you must use the embedded SNMP agent. By default, the embedded SNMP agent is disabled. To enable it, use the vSphere CLI command `vicfg-snmp`.
- o Both the embedded SNMP agent and the Net-SNMP-based agent available in the ESX service console listen on UDP port 161 by default. If you enable both of these agents for polling on an ESX host, you must change the port used by at least one of them.
- o Can use SNMP to monitor guest operating systems or applications running in VMs. Do not install agents in the VM that are intended to monitor physical hardware.
- o VMware MIB Files

MIB File	Description
VMWARE-ROOT-MIB.mib	Contains VMware's enterprise OID and top level OID assignments.
VMWARE-AGENTCAP-MIB.mib	Defines the capabilities of the VMware agents by product versions.
VMWARE-ENV-MIB.mib	Defines variables and trap types used to report on the state of physical hardware components of the host computer.
VMWARE-OBSOLETE-MIB.mib	Defines OIDs that have been made obsolete to maintain backward compatibility with earlier versions of ESX/ESXi. Includes variables formerly defined in the files VMWARE-TRAPS-MIB.mib and VMWARE-VMKERNEL-MIB.mib.
VMWARE-PRODUCTS-MIB.mib	Defines OIDs to uniquely identify each SNMP agent on each VMware platform by name, version, and build platform.
VMWARE-RESOURCES-MIB.mib	Defines variables used to report information on resource usage of the VMkernel, including physical memory, CPU, and disk utilization.
VMWARE-SYSTEM-MIB.mib	The VMWARE-SYSTEM-MIB.mib file is obsolete. Use the SNMPv2-MIB to obtain information from sysDescr.0 and sysObjec ID.0.
VMWARE-TC-MIB.mib	Defines common textual conventions used by VMware MIB files.
VMWARE-VC-EVENTS-MIB.mib	Defines traps sent by vCenter Server. Load this file if you use vCenter Server to send traps.
VMWARE-VMINFO-MIB.mib	Defines variables for reporting information about VMs, including VM traps.

- o ESX/ESXi System Logs

Component	Location
ESX Server 2.x Service log	/var/log/vmware/vmware-serverd.log
ESX Server 3.x or ESX Service log	/var/log/vmware/hostd.log
vSphere Client Agent log	/var/log/vmware/vpx/vpxa.log
Virtual Machine Kernel Core file	/root/vmkernel-core.<date> and /root/vmkernel-log.<date> present after you reboot your machine.

Syslog log	/var/log/messages
Service Console Availability report	/var/log/vmkernel
VMkernel Messages	/var/log/vmkernel
VMkernel Alerts and Availability report	/var/log/vmkernel
VMkernel Warning	/var/log/vmkwarning
Virtual Machine log file	In the same directory as the .vmx file for the VM.

- o vSphere Client System Logs

Component	Location
vSphere Client Installation log	Temp directory on the vSphere Client machine. e.g.: C:\Documents and Settings\<user name>\Local Settings\Temp\vmmsi.log
vSphere Client Service log	\vpx directory in the Application Data directory on the vSphere Client machine. e.g.: C:\Documents and Settings\<user name>\Local Settings\Application Data \vpx\viclient-x.log x(=0, 1, ... 9)

- o VMware Server System Logs

Component	Operating System	Location
VM Console log	Windows	Temp directory e.g.: C:\Documents and Settings\<username>\Local Settings \Temp\vmware-<username>-<PID>.log
	Linux	Temp directory e.g.: /tmp/vmware-<username>/ui-<PID>.log
VM log	Windows & Linux	vmware.log Located in the same directory as the VM .vmx file.
VM Event log	Windows	C:\Program Files\VMware\VMware Virtual Infrastructure\ vmserverdRoot\eventlog\vent- <path_to_configuration_file>.vmx.log
	Linux	/var/log/vmware/event-<path_to_configuration_file>.vmx.log
VM Conf file	Windows	<virtual_machine_name>.vmx Located in the folder where VMs are stored.
	Linux	<virtual_machine_name>.vmx Located in the folder where VMs are stored.

- o All ESX/ESXi hosts run a syslog service (syslogd).
- o ESXi hosts can use the vSphere Client or the vSphere CLI command `vicfg-syslog`
- o Cannot use the vSphere Client or `vicfg-syslog` to configure syslog behavior for an ESX host. To configure syslog for an ESX host, you must edit the /etc/syslog.conf file.
- o Libraries – Central repositories for VM provisioning media such as VM templates, ISO images, floppy images, VMDK files, guest customization files, and so on.
- o Guided Consolidation ports

Port	Protocol	Service	Description	MS Windows
135	TCP/UDP	Loc-srv/epmap	Microsoft DCE Locator service (End-point Mapper).	DHCP, DNS & WINS Server
137	TCP/UDP	Netbios-ns	NetBIOS names service.	WINS & DNS Server
138	TCP/UDP	Netbios-dgm	NetBIOS datagram	
139	TCP/UDP	Netbios-ssn	NetBIOS Session Windows File and Printer sharing.	
445	TCP/UDP	DNS	DNS Direct Hosting port.	Active Directory

- o Guided Consolidation can be installed together with vCenter Server, or can be installed on a separate host. For best performance, install Guided Consolidation on a separate host. It includes the following services:
  - o vCenter Collector Service – Discovers domains and systems within domains. Collects performance data on those systems.
  - o vCenter Provider Service – Helper service to the Collector Service. Communicates with target systems and passes the data back.
  - o vCenter Guided Consolidation – Coordinates all communication among Guided Consolidation components.
- o You can analyze up to 100 systems simultaneously.
- o The following formula is used to resize converted disks:
  - o amount of space used on physical disk * 1.25 = resultant virtual disk size
- o Virtual disks are set to a size of 4GB or larger.
- o Disconnecting a managed host does not remove it from vCenter Server; it temporarily suspends all monitoring activities performed by vCenter Server.
- o Deploying an OVF template is similar to deploying a VM from a template. However, you can deploy an OVF template from any local file system accessible from the vSphere Client machine, or from a remote web server.
- o OVF advantages:
  - o OVF files are compressed, allowing for faster downloads.
  - o The vSphere Client validates an OVF file before importing it.
- o A vApp is a container, like a resource pool and can contain one or more VMs. A vApp can power on and power off, and can also be cloned.
- o The vApp metadata resides in the vCenter Server's database
- o You can add an object, such as a VM or another vApp, to an existing vApp.

o An IP pool is a network configuration that is assigned to a network used by a vApp. The vApp can then leverage vCenter Server to automatically provide an IP configuration to its VMs.
o Each application within the service will be powered on according to how the startup order is set. When powering on a vApp within a DRS cluster in manual mode, no DRS recommendations are generated for VM placements. The power on operation performs as if DRS is run in a semi-automatic or automatic mode for the initial placements of the VMs. This does not affect VMotion recommendations. Recommendations for individual powering on and powering off of VMs are also generated for vApps that are running
o A VM's name can be up to 80 characters long. Names are case insensitive.
o Virtual machine version 4 — Compatible with ESX 3.0 and greater hosts and VMware Server 1.0 and greater hosts.
o Virtual machine version 7 — Compatible with ESX 4.0 and greater hosts. Provides greater VM functionality.
o Paravirtual SCSI (PVSCSI) adapters are high-performance storage adapters that can result in greater throughput and lower CPU utilization.
  o Best suited for high performance storage environments.
  o Not suited for DAS environments. VMware recommends that you create a primary adapter (LSI Logic by default) for use with a disk that will host the system software (boot disk) and a separate PVSCSI adapter for the disk that will store user data, such as a database.
o Paravirtual SCSI adapters are available for VMs running hardware version 7 and greater. They are supported on the following guest operating systems:
  o Windows Server 2008
  o Windows Server 2003
  o Red Hat Linux (RHEL) 5
o Features not supported with Paravirtual SCSI adapters:
  o Boot disks
  o Record/Replay
  o Fault Tolerance
  o MSCS Clustering
o SCSI controller types:
  o BusLogic Parallel
  o LSI Logic SAS
  o LSI Logic Parallel
  o VMware Paravirtual
o Thin Provisioned Format – Use this format to save storage space. If a virtual disk supports clustering solutions such as Fault Tolerance, you cannot make the disk thin. You can manually convert the thin disk into thick.
o Thick Format – This is the default virtual disk format. It is not possible to convert the thick disk into thin. (EDIT: you can via Storage VMotion)
o Automatic VMware Tools upgrade is not supported for VMs with Solaris or Netware guest operating systems.
o If you are using a WYSE thin client device to conduct remote desktop sessions using VMware VDI, installing WYSE Multimedia Support in the guest operating system improves the performance of streaming video. WYSE Multimedia Support is supported on the Windows 2003 and Windows XP guest operating systems only. WYSE Multimedia Support is installed as part of a VMware Tools installation or upgrade.
o Virtual machines with hardware versions lower than 4 can run on ESX4 hosts but have reduced performance and capabilities. In particular, you cannot add or remove virtual devices on VMs with hardware versions lower than 4 when they reside on an ESX4 host.
o Virtual Machine Hardware Versions

	Version 7	Version 4	Version 3	Compatible with vCenter Server version
ESX/ESXi 4.x	create, edit, run	create, edit, run	run	vCenter Server 4.x
ESX Server 3.x	–	create, edit, run	run	VirtualCenter Server 2.x and higher
ESX Server 2.x	–	–	create, edit, run	VirtualCenter Server 1.x and higher

o SCSI Bus Sharing list:

Option	Description
None	Virtual disks cannot be shared by other VMs.
Virtual	Virtual disks can be shared by VMs on same server.
Physical	Virtual disks can be shared by VMs on any server.

o Memory/CPU Hotplug – VMware Tools must be installed for hotplug functionality to work properly.
o VMI – A paravirtualization standard that enables improved performance for VMs capable of utilizing it.
o Enabling paravirtualization utilizes one of the VM's six virtual PCI slots
o A VM with paravirtualization enabled and that is powered off can be moved manually to a host that does not support paravirtualization. However, this can result in reduced performance.
o N-port ID virtualization (NPIV) – Provides the ability to share a single physical Fibre Channel HBA port among multiple virtual ports, each with unique identifiers. This allows control over VMaccess to LUNs on a per-VMbasis.
o NPIV support is subject to the following limitations:
  o NPIV must be enabled on the SAN switch.
  o NPIV is supported only for VMs with RDM disks.

- The physical HBAs on the ESX host must have access to a LUN using its WWNs in order for any VMs on that host to have access to that LUN using their NPIV WWNs.
  - The physical HBAs on the ESX host must support NPIV.
  - Each VMcan have up to 4 virtual ports. NPIV-enabled VMs are assigned exactly 4 NPIV-related WWNs. Can utilize up to 4 physical HBAs for NPIV purposes.
- A VM with WWNs that are already in use on the storage network is prevented from powering on.
- While hyperthreading does not double the performance of a system, it can increase performance by better utilizing idle resources.
- The advanced CPU settings are useful only for fine-grained tweaking of critical VMs.
- NUMA memory node affinity enables fine-grained control over how VM memory is distributed to host physical memory.
- Specify nodes to be used for future memory allocations only if you have also specified CPU affinity.
- The following NIC types are supported:

Flexible	Supported on VMs that were created on ESX Server 3.0 or greater and that run 32-bit guest operating systems. The Flexible adapter functions as a Vlance adapter if VMware Tools is not installed in the VM and as a Vmxnet driver if VMware Tools is installed in the VM.
e1000	Emulates the functioning of an E1000 network card. It is the default adapter type for VMs that run 64-bit guest operating systems.
Enhanced vmxnet	An upgraded version of the Vmxnet device with enhanced performance. It requires that VMware Tools be installed in the VM.
vmxnet 3	Next generation Vmxnet device with enhanced performance and enhanced networking features. It requires that VMware Tools be installed in the VM, and is available only on VMs with hardware version 7 and greater.

- Independent disks are not affected by snapshots.
- Two modes for independent disks:
  - Persistent – The disk operates normally except that changes to the disk are permanent even if the VM is reverted to a snapshot.
  - Nonpersistent – The disk appears to operate normally, but whenever the VM is powered off or reverted to a snapshot, the contents of the disk return to their original state. All later changes are discarded.
- VMDirectPath I/O allows a guest operating system on a VM to directly access physical PCI and PCIe devices connected to a host. Each VM can be connected to up to two PCI devices. PCI devices connected to a host can be marked as available for passthrough from the Hardware Advanced Settings in the Configuration tab for the host.
- Paravirtual SCSI (PVSCSI) adapters are high-performance storage adapters that can provide greater throughput and lower CPU utilization. PVSCSI adapters are best suited for environments, especially SAN environments, running I/O-intensive applications. PVSCSI adapters are not suited for DAS environments.
- Hardware requirements for customizing the guest operating system:
  - Must reside on a disk attached as SCSI 0:0 node in the VM configuration.
  - If a VM has mixed IDE and SCSI disks, the first IDE disk is considered the boot disk, and vCenter Server passes it to the customizer.
- If the new VM encounters customization errors while it is booting
- Customization errors are logged to (Windows guest) %WINDIR%\temp\vmware-imc or (Linux guest) /var/log/vmware/customization.log.
- When you migrate a suspended VM, the new host for the VM must meet CPU compatibility requirements, because the VM must resume executing instructions on the new host.
- Use of Jumbo Frames is recommended for best VMotion performance.
- Some restrictions apply when migrating VMs with snapshots. You cannot migrate a virtual machine with snapshots with Storage VMotion.
- You can migrate as long as the VM is being migrated to a new host without moving its configuration file or disks (the VM must reside on shared storage accessible to both hosts).
- Reverting to a snapshot after migration with VMotion might cause the VM to fail, because the migration wizard cannot verify the compatibility of the VM state in the snapshot with the destination host.
- During a migration with Storage VMotion, you can transform virtual disks from thick-provisioned to thin or from thin-provisioned to thick.
- Storage VMotion is subject to the following requirements and limitations:
  - Virtual machines with snapshots cannot be migrated using Storage VMotion.
  - Virtual machine disks must be in persistent mode or be raw device mappings (RDMs). For virtual compatibility mode RDMs, you can migrate the mapping file or convert to thick-provisioned or thinprovisioned disks during migration as long as the destination is not an NFS datastore. For physical compatibility mode RDMs, you can migrate the mapping file only.
  - Must have a license that includes Storage VMotion.
  - ESX/ESXi 3.5 hosts must be licensed and configured for VMotion. ESX/ESXi 4.0 and later hosts do not require VMotion configuration in order to perform migration with Storage VMotion.
  - A particular host can be involved in up to two migrations with VMotion or Storage VMotion at one time.
  - vSphere supports a maximum of eight simultaneous VMotion, cloning, deployment, or Storage VMotion accesses to a single VMFS3 datastore, and a maximum of four simultaneous VMotion, cloning, deployment, or Storage VMotion accesses to a single NFS or VMFS2 datastore. A migration with VMotion involves one access to the datastore. A migration with Storage VMotion involves one access to the source datastore and one access to the destination datastore

o   Disks are converted from thin to thick format or thick to thin format only when they are copied from one datastore to another. If you choose to leave a disk in its original location, the disk format is not converted.
o   Thin or thick provisioned – not available for RDMs in physical compatibility mode. If you select this option for a virtual compatibility mode RDM, the RDM is converted to a virtual disk. RDMs converted to virtual disks cannot be converted back to RDMs.
o   You can run the storage vmotion command in either interactive or noninteractive mode.
    o   Interactive mode, type **svmotion --interactive**.
    o   Noninteractive mode: svmotion [Standard CLI options] --datacenter=<datacenter name> --vm '<VM config datastore path>:<new datastore>' [--disks '<virtual disk datastore path>:<new datastore>, <virtual disk datastore path>:<new datastore>]'
o   A snapshot captures the entire state of the VM at the time you take the snapshot. This includes:
    o   Memory state – The contents of the VM's memory.
    o   Settings state – The VM settings.
    o   Disk state – The state of all the VM's virtual disks.
o   Snapshots of raw disks, RDM physical mode disks, and independent disks are not supported.
o   Change Disk Mode to independent to Exclude Virtual Disks from Snapshots
o   Persistent – Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
o   Nonpersistent – Changes are discarded when you power off or reset the VM. Nonpersistent mode enables you to restart the VM with a virtual disk in the same state every time. Changes to the disk are actually written to and read from a redo log file that is deleted when you power off or reset.
o   Snapshots:
    o   Delete – commits the snapshot data to the parent and removes the selected snapshot.
    o   Delete All – commits all the immediate snapshots before the You are here current state to the base disk and removes all existing snapshots for that VM.
    o   Revert to Snapshot – a shortcut to the parent snapshot of "You are here".
o   If you use Active Directory groups for permissions, make sure that they are security groups and not distribution groups.
o   Users who are currently logged in and are removed from the domain retain their vSphere permissions only until the next validation period (the default is every 24 hours).
o   A role is a predefined set of privileges. Privileges define basic individual rights required to perform actions and read properties. When you assign a user or group permissions, you pair the user or group with a role and associate that pairing with an inventory object.
o   Default roles:
    o   System roles – System roles are permanent. You cannot edit the privileges associated with these roles.
    o   Sample roles – VMware provides sample roles for convenience as guidelines and suggestions. You can modify or remove these roles.
o   You can also create completely new roles.
o   All roles permit the user to schedule tasks by default. Users can schedule only tasks they have permission to perform at the time the tasks are created.
o   Default roles :

Role	Role Type	Description of User Capabilities
No Access	system	Cannot view or change the assigned object. available in ESX/ESXi and vCenter Server.
Read Only	system	View the state and details about the object. available on ESX/ESXi and vCenter Server.
Administrator	system	All privileges for all objects. available in ESX/ESXi and vCenter Server.
Virtual Machine Power User	sample	allow the user to interact with and make hardware changes to VMs, as well as perform snapshot operations. available only on vCenter Server.
Virtual Machine User	sample	allow the user to interact with a VM's console, insert media, and perform power operations. available only on vCenter Server.
Resource Pool Administrator	sample	allow the user to create child resource pools and modify the configuration of the children, but not to modify the resource configuration of the pool or cluster on which the role was granted. Also allows the user to grant permissions to child resource pools, and assign VMs to the parent or child resource pools. available only on vCenter Server.
VMware Consolidated Backup User	sample	used by the VMware Consolidated Backup product and should not be modified. available only on vCenter Server.
Datastore Consumer	sample	allow the user to consume space on the datastores on which this role is granted. available only on vCenter Server.
Network Consumer	sample	allow the user to assign VMs or hosts to networks available only on vCenter Server.

o   If you create or edit a role on a vCenter Server system that is part of a connected group in Linked Mode, the changes you make are propagated to all other vCenter Server systems in the group. Assignments of roles to specific users and objects are not shared across linked vCenter Server systems.

o   Permissions grant users the right to perform the activities specified by the role on the object to which the role is assigned

o   By default, all users who are members of the Windows Administrators group on the vCenter Server system have the same access rights as any user assigned to the Administrator role on all objects.

o   Propagation is set per permission, not universally applied. Permissions defined for a child object always override those propagated from parent objects.

o   You cannot set permissions directly on a vNetwork Distributed Switches. To set permissions for a vNetwork Distributed Switch and its associated dvPort Groups, set permissions on a parent object, such a folder or datacenter, and select the option to propagate these permissions to child objects.

   o   If no permission is defined for the user on that object, the user is assigned the union of privileges assigned to the groups for that object.

   o   If a permission is defined for the user on that object, the user's permission takes precedence over all group permissions

o   Reports are updated every 30 minutes

o   Map views are updated every 30 minutes

o   Alarms are notifications that occur in response to selected events, conditions, and states that occur with objects in the inventory.

o   Alarms are composed of a trigger and an action.

o   Alarms have two types of triggers: condition/state triggers, and event triggers.

o   Condition or State Triggers Monitor the current condition or state of VMs, hosts, and datastores.

o   Event Triggers Monitors events that occur in response to operations occuring with any managed object in the inventory, the vCenter Server system, or the license server.

o   Condition and state triggers use one of the following operator sets to monitor an object:

   o   Is equal to and Is not equal to

   o   Is above and Is below

o   Event triggers use arguments, operators, and values to monitor operations that occur in the vServer System.

o   Alarm actions are operations that occur in response to triggered alarms.

o   The default VMware alarms do not have actions associated with them. You must manually associate actions with the default alarms.

o   You can disable an alarm action from occurring without disabling the alarm itself.

o   You disable alarm actions for a selected inventory object.

o   When you disable the alarm actions for an object, they continue to occur on child objects.

o   When you disable alarm actions, all actions on all alarms for the object are disabled. You cannot disable a subset of alarm actions.

o   The SNMP agent included with vCenter Server can be used to send traps when alarms are triggered on a vCenter Server.

o   Alarm reporting can further restrict when a condition or state alarm trigger occurs by adding a tolerance range and a trigger frequency to the trigger configuration.

o   The tolerance range specifies a percentage above or below the configured threshold point, after which the alarm triggers or clears.

o   Condition threshold + Tolerance Range = Trigger alarm

o   The trigger frequency is the time period during which a triggered alarm action is not reported again. By default, the trigger frequency for the default VMware alarms is set to 5 minutes.

o   Statistical data consists of CPU, memory, disk, network, system, and VM operations metrics.

o   Collection intervals determine the time period during which statistics are aggregated and rolled up, and the length of time the statistics are archived in the vCenter database. By default, vCenter Server has four collection intervals: Day, Week, Month, and Year.

o   Real-time statistics are not stored in the database. They are stored in a flat file on ESX/ESXi hosts and in memory on the vCenter Server systems

o   Real-time statistics are collected directly on an ESX/ESXi host every 20 seconds (60 seconds for ESX Server 2.x hosts).

   o   On ESX hosts, the statistics are kept for one hour, after which 180 data points (15 -20 second samples) will have been collected.

   o   On ESXi hosts, the statistics are kept for 30 minutes, after which 90 data points will have been collected.

o   Collection Intervals

1 Day	5 Minutes
1 Week	30 Minutes
1 Month	2 Hours
1 Year	1 Day

o   You can change the frequency at which statistic queries occur, the length of time statistical data is stored in the vCenter Server database, and the amount of statistical data collected.

o   Not all attributes are configurable for each collection interval.

o   You can assign a collection level of 1- 4 to each collection interval, with level 4 having the largest number of counters.

o   By default, all collection intervals use collection level 1.

o   Generally, you need to use only collection levels 1 and 2 for performance monitoring and analysis.

o   By default, statistics are stored in the vCenter Server database for one year. You can increase this to three years.

o   You cannot view datastore metrics in the advanced charts. They are only available in the overview charts.
o   CPU Performance Enhancement Advice
1.   Verify that VMware Tools is installed on every VM on the host.
2.   Compare the CPU usage value of a VM with the CPU usage of other VMs 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 VMs on the host.
3.   Determine whether the high ready time for the VM resulted from its CPU usage time reaching the CPU limit setting. If so, increase the CPU limit on the VM.
4.   Increase the CPU shares to give the VM 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 VMs to guarantee that they receive the required CPU cycles.
5.   Increase the amount of memory allocated to the VM. This decreases disk and or network activity for applications that cache. This might lower disk I/O and reduce the need for the ESX/ESXi host to virtualize the hardware. Virtual machines with smaller resource allocations generally accumulate more CPU ready time.
6.   Reduce the number of virtual CPUs on a VM to only the number required to execute the workload. For example, a single-threaded application on a four-way VM 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.
7.   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 VMs onto the new host.
8.   Upgrade the physical CPUs or cores on the host if necessary.
9.   Use the newest version of ESX/ESXi, and enable CPU-saving features such as TCP Segmentation Offload, large memory pages, and jumbo frames.
o   Memory Performance Enhancement Advice
1.   Verify that VMware Tools is installed on each VM. The balloon driver is installed with VMware Tools and is critical to performance.
2.   Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused VM memory by ballooning and swapping. Generally, this does not impact VM performance.
3.   Reduce the memory space on the VM, and correct the cache size if it is too large. This frees up memory for other VMs.
4.   If the memory reservation of the VM 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 VMs on the host.
5.   Migrate one or more VMs to a host in a DRS cluster.
6.   Add physical memory to the host.
o   Disk I/O Performance Enhancement Advice
1.   Increase the VM 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. To verify that VMs have adequate memory, check swap statistics in the guest operating system. 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.
2.   Defragment the file systems on all guests.
3.   Disable antivirus on-demand scans on the VMDK and VMEM files.
4.   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.
5.   Use Storage VMotion to migrate I/O-intensive VMs across multiple ESX/ESXi hosts.
6.   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.
7.   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 VM by adjusting the Disk.SchedNumReqOutstanding parameter. For more information, see the *Fibre Channel SAN Configuration Guide*.
8.   For resource-intensive VMs, separate the VM's physical disk drive from the drive with the system page file. This alleviates disk spindle contention during periods of high use.
9.   On systems with sizable RAM, disable memory trimming by adding the line MemTrimRate=0 to the VM's .VMX file.
10. If the combined disk I/O is higher than a single HBA capacity, use multipathing or multiple links.
11. 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.
12. Use the most current ESX/ESXi host hardware.
o   Networking Performance Enhancement Advice
1.   Verify that VMware Tools is installed on each VM.
2.   If possible, use vmxnet3 NIC drivers, which are available with VMware Tools. They are optimized for high performance.
3.   If VMs running on the same ESX/ESXi host communicate with each other, connect them to the same vSwitch to avoid the cost of transferring packets over the physical network.

4. Assign each physical NIC to a port group and a vSwitch.
5. Use separate physical NICs to handle the different traffic streams, such as network packets generated by VMs, iSCSI protocols, VMotion tasks, and service console activities.
6. 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 VMs to a vSwitch with a lighter load or to a new vSwitch.
7. If packets are being dropped at the vSwitch port, increase the virtual network driver ring buffers where applicable.
8. 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.
9. 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.
10. Use vNICs that are TSO-capable, and verify that TSO-Jumbo Frames are enabled where possible.
o Tasks represent system activities that do not complete immediately, such as migrating a VM.
o If you are logged in to a vCenter Server system that is part of a Connected Group, a column in the task list displays the name of the vCenter Server system on which the task was performed.

Appendix A – Defined privileges

Appendix B – Installing the MS sysprep tools

Appendix C – Performance metrics

vSphere Web Access Administrator's Guide

o Supported Operating Systems:
  o Windows 2003 SP1, XP Pro SP3, XP Home SP2, 2000 SP4
  o Linux with standard libraries, but requiring GTK+ 2.
o Supported browsers:
  o IE 6, 7 or later
  o Firefox 2, 3.0 or later
o The console webAccess service is now `vmware-webAccess`
o The Alarms tab is available only when you use vSphere Web Access to connect to vCenter Server.
o You can view the assigned tasks for a virtual machine, but you cannot assign tasks using Web Access.
o New disk policy (not available option from vSphere Client)
  o Optimize for safety – Saves all changes to the virtual disk before notifying the system.
  o Optimize for performance – Acknowledges changes to the virtual disk immediately, but saves them at a later time.
o VMI currently supports only 32-bit guests.

ESX Configuration Guide

To be continued…