VMware Certified Professional vSphere 5 Blueprint

By Josh Coen and Jason Langer

Contents

Section 1 – Plan, Install, Configure and Upgrade vCenter Server and VMware ESXi

Objective 1.1 – Install and Configure vCenter Server

Knowledge

- **Identify available vCenter Server editions**
    - *vCenter Server Essentials* – Provides the same features as vCenter Foundation, integrated with the Essentials and Essentials Plus kits
    - *vCenter Server Foundation* – Provides powerful management tools for smaller environments (up to 3 vSphere hosts) looking to rapidly provision, monitor, and control virtual machines
    - *vCenter Server Standard* – Provides large scale management of VMware vSphere deployments for rapid provisioning, monitoring, orchestration, and control of virtual machines

Includes	vCenter Server Essentials	vCenter Server Foundation	vCenter Server Standard
Management Server	X	X	X
Database Server	X	X	X
Search Engine	X	X	X
VMware vSphere Client	X	X	X
VMware vCenter API's and .NET Extension	X	X	X
vCenter Orchestrator			X
vCenter Server Linked Mode			X

Further details see page 8 of the *VMware vSphere 5.0 Licensing, Pricing and Packaging* white paper

- **Deploy the vCenter Appliance**
    - As an alternative to installing vCenter Server on a Windows machine, you can download the VMware vCenter Server Appliance. The vCenter Server Appliance is a preconfigured Linux-based virtual machine optimized for running vCenter Server and associated services.

      Microsoft SQL Server and IBM DB2 are not supported for the vCenter Server Appliance. The vCenter Server Appliance does not support Linked Mode configuration nor does it support IPv6

For further information see page 201 of the *vSphere Installation and Setup* document and pages 41 thru 48 of the *vSphere Server and Host Management* document

- **Install vCenter Server into a virtual machine**
    - When installing vCenter Server on a virtual machine the "hardware" recommendations and software prerequisites do not change. The following are advantages when doing so:
        - Rather then dedicating a separate server to the vCenter Server system, you can place it in a virtual machine running on the same host where your other virtual machines run
        - You can provide high availability for the vCenter Server system by using vSphere HA
        - You can migrate the virtual machine containing the vCenter Server system from one host to another, enabling maintenance and other activities
        - You can create snapshots of the vCenter Server virtual machine and use them for backups, archiving, and so on

- **Size the vCenter Server Database**
    - The size of your vCenter Database is dependent on how many host you have, have many VM's you have, and the level of statistics you are using. From within vCenter Server under *Administration -> vCenter Server Settings -> Statistics* there is a section for *Database Size*. You can plug in your environments specifics and get a DB size. Also, on VMware's website there is a *Database Sizing Calculator*. Currently available is the calculator for vSphere 4

- **Install additional vCenter Server components**
    - Besides vCenter Server there are several additional components you may wish to install. Full details on pages 204 thru 211 of the *vSphere Installation and Setup* document.
        - *vSphere Client*- Windows program that you can use to configure the host and to operate its virtual machines
        - *vSphere Web Client* – Allows you to connect to a vCenter Server system to manage an ESXi host through a web browser
        - *Update Manager Server* – Allows for the patching of ESXi hosts as well as virtual machines. Can be installed on the same computer as vCenter Server or a different computer.
        - *vSphere ESXi Dump Collector* – ESXi can be configured to dump its vmkernel memory to a network server instead of writing it to disk when the system has had a critical failure (Purple Screen of Death). ESXi Dump Collector can be used as the network server
        - *vSphere Syslog Collector* – Allows ESXi hosts to be configured for their system logs to be captured on a network server
        - *vSphere Auto Deploy* – Allows for the deployment and customization of ESXi hosts by loading the ESXi image into the hosts memory
        - *vSphere Authentication Proxy* – Enables ESXi hosts to join a domain without using Active Directory credentials. Enhances security for PXE-booted hosts and hosts that are provisioned using Auto Deploy, by removing the need to store Active Directory credentials in the host configuration.

- **Install/Remove & Enable/Disable vSphere Client plug-ins**
    - After the server components of a plug-in is installed and registered with vCenter Server, its client component is available to vSphere clients. Client component installation and enablement are managed through the Plug-in Manager dialog box. The Plug-in Manager lets your perform the following actions:

- View available plug-ins that are not currentl installed on the client
- View installed plug-ins
- Download and install available plug-ins
- Enable and disable installed plug-ins

See page 27 of the *vCenter Server and Host Management* document for step by step

- **License vCenter Server**
  - To license a single vCenter Server 5.0, you need a vCenter Server 5.0 license key with a capacity for one instance. If you have vCenter Server systems in Linked Mode group, you can purchase a vCenter Server license key with a larger capacity and assign the key to all vCenter Server systems in the group.

    See pages 70 thru 97 of the *vCenter Server and Host Management* document for additional information and procedures.

- **Determine availability requirements for a vCenter Server in a given vSphere implementation**
  - Obviously you want as little down time as possible for your vCenter server. Just be aware of the options to allow vCenter Server to highly available
    - Run vCenter Server in a VM to take advantage of VMware HA/DRS
    - vCenter Server Cluster Heartbeat
    - Cold standby vCenter Server (virtual or physical)

- **Determine use case for vSphere Client and Web Client**
  - vSphere Client – As VMware Administrators we are quite familiar with the traditional vSphere Client. It is the one stop shop to configure and maintain your entire environment. Using this client may not be suitable for non-administrators (think VM owners or Operations staff).
  - Web Client – Better suited for your non-administrative users. Uses a java based web page to allow for the basic tasks of managing VM's.

  See page 17 of the *vCenter Server and Host Management* document for further details

<u>Tools</u>

- VMware vSphere Basics Guide
- vSphere Installation and Setup guide
- vCenter Server and Host Management guide

Objective 1.2 – Install and Configure VMware ESXi

Knowledge

- **Perform an interactive installation of ESXi**
  - ESXi can be installed either using CD/DVD or USB flash drive. Regardless of which media type you use, the following prerequisites should be applied:
    1. Verify that the server hardware clock is set to UTC in the system BIOS
    2. 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
    3. Consider disconnecting your network storage. This action decreases the time it takes the installation to search for available disk drives.
  - I thought about including screen shots, but as I assume most are familiar with the ESXi installation I will outline the general procedure:
    1. Place the CD/DVD into the ROM drive of the host or connect your USB flash drive that contains the ESXi installer files
    2. Boot the host (if needed set the appropriate BIOS boot order, CD/DVD drive or USB)
    3. Press *Enter* to select ESXi 5 Installer or allow the timer to finish counting down
    4. Press *Enter* on the "*Welcome to the VMware ESXi 5.0.0 Installation*" screen
    5. Read and press *F11* to Accept the End User License Agreement (EULA)
    6. Highlight the appropriate disk on the "*Select a Disk to Install or Upgrade*" and press *Enter* to continue

       Note – If the drive you are installing to currently has an installation of ESXi you will be provided with additional choices:

       - Upgrade ESXi, preserve VMFS datastore
       - Install ESXi, preserve VMFS datastore
       - Install ESXi, overwrite VMFS datastore
       - Select the appropriate option for your host installation and press *Enter* to continue

    7. Select the appropriate keyboard layout, press *Enter* to continue
    8. Set a root password (note this is not required but recommended), press *Enter* to continue

    See pages 37 thru 40 of the *vSphere Installation and Setup* document for further information

- **Deploy an ESXi host using Auto Deploy**
  - vSphere Auto Deploy is a new feature of vSphere 5 that allows for provisioning ESXi hosts on a large scale. With this feature you are able to install ESXi on a new host (first boot), reboot hosts, or reimage an existing host with an upgraded image. The procedure to install on a new host (first boot):

1. Power on the host – The host will attempt to contact the DHCP server and download the gPXE. The Auto Deploy server will install the new host with the image specified and apply a Host Profile if one is provided. To finish up, Auto Deploy will add the host to vCenter
2. (Optional) – If Auto Deploy applies a host profile that requires user input such as an IP address, the host is placed in maintenance mode.

The brief description is just a very small part of the functionality of Auto Deploy and also does not discuss the infrastructure setup to implement this feature. Refer to pages 57 thru 115 of the *vSphere Installation and Setup* document for further reading. Also, Duncan Epping @ Yellow-Bricks.com has an excellent write up on setting Auto Deploy in your home lab. Link HERE - http://www.yellow-bricks.com/2011/08/25/using-vsphere-5-auto-deploy-in-your-home-lab/

- **Configure NTP on an ESXi Host**
  - Via the vSphere Client you can configure the startup mode for the NTP service as well as list the hosts you wish to query:
    1. Within the vSphere Client select the host and click the *Configuration* tab
    2. Under *Software* select *Time Configuration*
    3. Click *Properties* in the upper right
    4. Click *Options* and select *Start and stop with host*
    5. In left hand pane you can select *NTP Settings* to add your list of NTP hosts
    6. Click *OK*

- **Configure DNS and Routing on an ESXi Host**
  - Via the vSphere Client you can configure the DNS servers your host will use as well as the default gateway:
    1. Within the vSphere Client select the host and click the *Configuration* tab
    2. Under *Software* select *DNS and Routing*
    3. Click *Properties* in the upper right
    4. Under *Use the following DNS server address* set your DNS servers
    5. Click the *Routing* tab
    6. Specify the default gateway for the VMkernel
    7. Click *OK*

- **Enable/Configure/Disable hyperthreading**
    1. Within the vSphere Client select the host and click the *Configuration* tab
    2. Under *Hardware* select *Processors*
    3. Click *Properties* in the upper right
    4. Select or Deselect *Enable Hyperthreading*
    5. Click *OK*

Note – For this option to be available your CPU's need to support hyperthreading and it needs to be enabled in the system BIOS

- **Enable/Size/Disable memory compression cache**
    - One of the memory management techniques ESXi uses is Memory *Compression*. When a give ESXi host is under memory strain ESXi will compress virtual pages and store them in memory. Using this memory management technique allows for better performance the accessing memory that has been swapped to disk. You can all set the size of the compression cache as percentage of the assigned memory to a VM.

    - Enable/Disable Memory Compression
        1. Within the vSphere Client select the host and click the *Configuration* tab
        2. Under *Software* select *Advanced Settings*
        3. In the left hand pane select *Mem* and scroll down till you find *Mem.MemZipEnable*
        4. The default value is 1 (enabled), to disable change the value to 0 (disabled)
        5. Click *OK*

    - Sizing the Memory Compression Cache
        1. Within the vSphere Client select the host and click the *Configuration* tab
        2. Under *Software* select *Advanced Settings*
        3. In the left hand pane select *Mem* and scroll down till you find *Mem.MemZipMaxPct*
        4. The default value is 10 with a minimum of 5 and a maximum of 100. Set the value to desired percentage
        5. Click *OK*

- **License an ESXi host**
    - You can assign a license to a host in one of two ways, either with using vCenter Server or without.
    - With vCenter Server
        1. Within the vSphere Client click *Inventory* in the navigation bar
        2. Expand the inventory tree and select the location were you would like to add the new host
        3. Right-click and select *Add Host*
        4. When completing the Add New Host Wizard at the licensing screen allocate an existing license key or add a new key if needed

    - **Without vCenter Server**
        1. Within the vSphere Client select the host and click the *Configuration* tab
        2. Under *Software* select *Licensed Features*
        3. Click *Edit* in the upper right hand corner
        4. Configure a license key either with an existing key or select *Assign a new key to this host*
        5. Click *OK*

    For further information about ESXi licensing refer to pages 65 thru 94 of the *vCenter Server and Host Management* documentation

Tools

- VMware vSphere Basics guide
- vSphere Installation and Setup Guide
- vCenter Server and Host Management guide

Objective 1.3 – Plan and Perform Upgrades of vCenter Server and VMware ESXi

Knowledge

- **Identify upgrade requirements for ESXi hosts**
    1. Hardware Requirements
        - Supported server platform – Check the Hardware Compatability List (HCL)
        - ESXi 5. 0 will install and run only on servers with 64-bit x86 CPUs
        - ESXi 5.0 requires a host machine with at least two cores
        - ESXi 5.0 supports only LAHD and SAHF CPU instructions
        - Known 64-bit processors
        - 2GB RAM minimum
        - One or more Gigabit or 10GB Ethernet controllers – Again check the HCL
        - Any combination of one or more of the following controllers
            - Basic SCSI controllers
            - RAID controllers
        - SCSI disk or a local, non-networked, RAID LUN with unpartitioned space for the virtual machines
        - For Serial ATA (SATA), a disk connected through supported SAS controllers or supported on-board SATA controllers
    2. ESXi 5.0 supports installing on and booting from the following storage systems:
        - SATA disk drives – SATA disk drives connected behind supported SAS controlles or supported on-board SATA controllers (See page 12 of the vSphere Upgrade Guide for full listing)
        - Serial Attached SCSI (SAS) disk drives
        - Dedicated SAN disk on Fibre Channel or iSCSI
        - USB Device – Check the HCL for supported devices

- **Identify steps required to upgrade a vSphere implementation**
    - See each perspective environment is different, the *vSphere Upgrade* documentation outlines several example upgrade scenarios. Including the following:
        - Upgrading environments with Host Clusters
        - Upgrading environments without Host Clusters
        - Moving virtual machines using vMotion during an upgrade
        - Moving powered off or suspended virtual machines during an upgrade with vCenter Server
        - Upgrading to vCenter Server on a new machine
        - Migrating ESX 4.x or ESXi 4.x hosts to ESXi 5.0 in a PXE-booted Auto Deploy Installation

- Upgrading vSphere components separately in a VMware View environment

These examples are discussed on pages 159 thru 165 of the *vSphere Upgrade* documentation

- **Upgrade a vNetwork Distributed Switch**
  1. Within the vSphere Client from the *Home* screen select *Networking* from the *Inventory* section
  2. In the left hand pane select the virtual Distributed Switch to be upgraded
  3. Under the *Summary* tab in the right hand pane click *Upgrade* next to *Version*
  4. The wizard *Upgrade vDS to newer version* will launch
  5. Select the vSphere Distributed Switch version to upgrade to

     Note – Depending on what version you currently running your upgrade options maybe different

Option	Description
vSphere Distributed Switch Version: 4.1.0	Compatible with ESX/ESXi versions 4.1 and later
vSphere Distributed Switch Version: 5.0.0	Compatible with ESXi version 5.0 and later

  6. Click *Next*

     The upgrade wizard lists the hosts associated with the vDS and whether or not they are compatible with the upgraded vDS. You can only continue with the upgrade if all hosts are compatible

  7. Click *Next*
  8. Verify that the upgrade information listed is correct and click *Finish*

For further information read pages 24 thru 25 of the *vSphere Networking* documentation

- **Upgrade from VMFS3 to VMFS5**
  - Prerequisites
    - If you use a VMFS2 datastore, you must first upgrade to VMFS3 prior to upgrading to VMFS5
    - All hosts accessing the datastore must support VMFS5
    - Verify that the volume to be upgraded has at least 2MB of free blocks available and 1 free file descriptor
  - Procedure
    1. Within the vSphere Client select a host and click on the *Configuration* tab
    2. In the left hand pane under *Hardware* select *Storage*
    3. In the right hand pane select the VMFS3 datastore you wish to upgrade
    4. Click the link that says *Upgrade to VMFS5* in the lower right
    5. Click *Ok* on the *Upgrade to VMFS-5* dialog box
    6. Verify that the *Upgrade VMFS* task has completed
    7. Rescan all hosts that are presented the datastore

For further information read pages 120 thru 124 of the *vSphere Storage* documentation

- **Upgrade VMware Tools**
  - Since VMware supports several client operating systems, I will only be covering the process for upgrading VMware tools on Windows based guest. For further examples and instructions for other operating systems refer to pages 137 thru 158 of the *vSphere Upgrade* documentation.
  - Prerequisites
    - Make sure that the VM is powered on and booted into the operating system
    - Verify the current running version of VMware tools on the *Summary* tab of the VM
  - Installation
    1. Within the vSphere Client select the VM you wish to install VMware Tools
    2. Right click on the VM and select *Guest -> Install/Upgrade VMware Tools*
    3. Select if you would like to do an *Interactive Tools Upgrade* or a *Automatic Tools Upgrade*. For this example we will be selecting *Interactive Tools Upgrade*
    4. Once the VMware tools ISO has been mounted connect to the system via console or RDP
    5. If autorun has not been enabled, manually lunch the CD-ROM
    6. Click *Next* on the VMware Tools welcome screen
    7. After the installer has completed click *Finish*
    8. Click *Yes* if now is a good time to reboot the system. If not click *No*
    9. After the system reboot verify that the upgraded version of VMware Tools is displayed on the *Summary* tab of the VM

- **Upgrade Virtual Machine Hardware**
  - Hardware version 8 is the newest version in ESXi 5. VMware recommends that all VM's running on a ESXi 5 host run hardware version 8.
  - Prerequisites
    - Create a backup or snapshot of the virtual machine. If you have a snapshot of the VM it is possible to reverse the upgrade if there are issues
    - Upgrade VMware Tools first. On Microsoft Windows VM's if you upgrade the hardware prior to upgrading VMware Tools, networking settings maybe lost
    - Verify that all .vmdk files are available to the ESX/ESXi hosts on a VMFS3, VMFS5, or NFS datastore
    - Determine the current version of the virtual hardware by selecting the VM's *Summary* tab and checking the *VM Version* value

  - Installation
    1. Within the vSphere Client select the VM you wish to upgrade
    2. Power down the VM
    3. Right click on the VM and select *Upgrade Virtual Hardware*
    4. Click *Yes* on the *Confirm Virtual Machine Upgrade* dialog box
    5. Verify the upgrade task has completed and power on the VM
    6. For Windows operating systems upon boot up new hardware devices will be detected requiring another system reboot.
    7. Within the vSphere Client select the VM and verify on the *Summary* tab that the *VM Version* has been updated

For further information read pages 154 thru 156 of the *vSphere Upgrade* documentation

- **Upgrade an ESXi Host using vCenter Update Manager**
    - This is a long section to discuss. In the effort of saving time and space be sure to read pages 92 thru 103 of the *vSphere Upgrade* documentation

Tools

- VMware vSphere Basics Guide
- vSphere Installation and Setup Guide
- vSphere Upgrade Guide

Objective 1.4 – Secure vCenter Server and ESXi

Knowledge

- **Identify common vCenter Server privileges and roles**
    - Common Privileges

Create a Virtual Machine	On the destination folder or datacenter: • Virtual Machine.Inventory.Raw Create • Virtual Machine.Configuration.Add New Disk (If creating new VMDK) • Virtual Machine.Configuration.Add Existing Disk (If using existing VMDK) • Virtual Machine.Configuration.Raw Device (If using a RDM) On the destination host, cluster or resource pool: • Resource.Assign Virtual Machine to Resource Pool On the destination datastore or folder containing a datastore: • Datastore.Allocate Space On the network that the virtual machine will be assigned to: • Network.Assisgn Network
Take a virtual machine snapshot	On the virtual machine or a folder of virtual machines: • Virtual Machine.State.Create Snapshots On the destination datastore or folder of datastores • Datastore.Allocate Space
Mirgrate a VM with Storage vMotion	On the virtual machine or folder of virtual machines: • Resource.Migrate On the destination datastore • Datatstore.Allocated Space
Move a host into a cluster	On the host: • Host.Inventory.Add Host to Cluster On the destination cluster • Host.Inventory.Add Host to Cluster

For further examples of common privileges see pages 56 thru 58 *vSphere Security* documentation

- Default Roles in ESXi and vCenter Server

Role	Role Type	Description of User Capabilities
No Access	system	Cannot view or change the assigned object vSphere Client tabs associated with an object appear without content. Can be used to revoke perissions that would otherwise be propagated to an object from a parent object Available in ESXi and vCenter Server
Read Only	system	View the state and details about the object View all the tab panels in the vphere Client except the Console tab Cannot perform any actions through te menus and toolbars Available on ESXi and vCenter Server
Administrator	system	All privileges for all objects Add, remove, and set access rights and privileges for all the vCenter Server users and all the virtual objects in the vSphere environment Available in ESXi and vCenter Server
Virtual Machine Power User	sample	A set of privileges to allow the user to interact with and make hardware changes to virutal machines, as well as perform snapshot operations. Privileges granted include: ● All privileges for the scheduled task privileges group ● Selected privileges for global items, datastore, and virtual machine privileges groups ● No privileges for folder, datacenter, network, host, resource, alarms, sessions, performance, and permissions privileges groups. Usually granted on a folder that contains virtual machines or on individual virtual machines Available on vCenter Server
Virtual Machine User	sample	A set of privileges to allow the user to interact with a virtual machine's console, insert media, and perform power operations. Does not gratn privileges to make virtual hardware changes to the virtual machine. Privileges granted include: ● All privileges for the scheduled taks privileges group ● Selected privileges for the global items and virtual machines privileges groups ● No privileges for the folder, datacenter, datastore, network, host, resource, alarms, sessions, performance, and permissions privileges groups Usually granted on a folder that contains virtual machines or on individual virtual machines. Available on vCenter Server
Resource Pool Administrator	sample	A set of privileges to 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 virtual machines to the parent or child resource pools. Privileges granted include:

		• All privileges for folder, virtual machine, alarms, and scheduled task privileges groups • Selected privileges for resource and permissions privileges groups • No privileges for datacenter, network, host, sessions, or performance privileges groups Additional privileges must be granted on virtual machines and datastores to allow provisioning of new virtual machines Usually granted on a cluster or resource pool Available on vCenter Server
Datastore Consumer	sample	A set of privileges to allow the suer to consume space on the datastores on which this role is granted. To perform a space-consuming operation, such as creating a virtual disk or taking a snapshot, the use msut also have the appropriate virtual machine privileges granted for these operations Usually granted on a datastore or a folder of datastores Available on vCenter Server
Network Consumer	sample	A set of privileges to allow the user to assign virtual machines or hosts to networks, if hte appropriate permissions for the assignment are alos granted on the virtual machines or hosts Usually granted on a network or folder of networks Available on vCenter Server

- **Describe how permissions are applied and inherited in vCenter Server**

  vSphere allows the assignment of permissions to objects in the vSphere Client. When assigning permissions you select to have the permissions propagate down through the object tree or not. If you allow for propagation objects lower in the tree "inherit" the set permissions. However, if a permission is set at the child object it will take prescedance over an inherited permission.

For further information read pages 48 thru 53 (and the great diagram on pg 49) of the *vSphere Security* document.

- **Configure and administer the ESXi firewall**
- Enable/Configure/Disable services in the ESXi firewall
  1. Within the vSphere Client select a host and click on the *Configuration* tab
  2. In the left hand pane under *Software* select *Security Profile*
  3. In the right hand pane select *Properties* to the right of the *Firewall* section
  4. Check or uncheck the services you wish to enable or disable
  5. (Optional) With a service highlighted click *Options* in the lower right
  6. (Optional) Select a *Startup Policy* from the following:
     a. *Start Automatically if any ports are open, and stop when all ports are closed*
     b. *Start and stop with host*
     c. *Start and stop manually*
  7. (Optional) Click *OK*
  8. (Optional) Click the *Firewall* button in the lower right

9. (Optional) Select to *Allow connections from any IP address* or *Only allow connections from the following networks*
10. (Optional) Click *OK*
11. Click *OK*

For further information, including command line syntax, refer to pages 34 thru 40 of the *vSphere Security* document

- **Enable Lockdown Mode**

  - Enabled via the vSphere Client

    1. Within the vSphere Client select a host and click on the *Configuration* tab
    2. In the left hand pane under *Software* select *Security Profile*
    3. In the right hand pane select *Edit* to the right of *Lockdown Mode*
    4. Check the box *Enable Lockdown Mode*
    5. Click *OK*

  -Enabled via the Direct Console User Interface (DCUI)

    1. From the DCUI press *F2* and log in
    2. Select the option *Configure Lockdown Mode* and press *Enter*
    3. Press the *ESC* to back out of the menus till you are back at the DCUI

- **Configure network security policies**
  - MAC Address Changes - With this policy set to *Accept* (Default), ESXi allows the changing of effective MAC address to something other than the initial MAC address. When set to *Reject* ESXi does not allow for those changes to occur. This prevents host against MAC spoofing.
  - Forged Transmissions - With this policy set to *Accept* (Default), ESXi does not compare source and effective MAC addresses. When set to *Reject* the ESXi host does compare the source and effective MAC addresses of the client. If they do not match the ESXi host drops the packet
  - Promiscuous Mode - With this policy set to *Reject* (Default) guest operating systems are not allowed to receive all network traffic on the wire. When set to *Accept* the guest operating system can receive all network packets. Helpful when doing troubleshooting with a tool such as WireShark. Note however, this does introduce some security concerns

- **View/Sort/Export user and group lists**
  1. Connect the vSphere Client directly to an ESXi host
  2. Select the host and click the *Local Users & Groups* tab
  3. Sort the columns either by *UID, User*, *Name*, *GID*, or *Group*
  4. Right click any where in the right hand pane and click *Export List*
  5. Provide a *File Name* as well as the *Location* in the *Save As* dialog box
  6. Click *Save*

For further information read page 45 of the *vSphere Security* documentation

- **Add/Modify/Remove permissions for users and groups on vCenter Server inventory objects**
    1. Connect the vSphere Client directly to an ESXi host or vCenter Server
    2. Select an inventory object and select the *Permissions* tab
    3. In the right hand pane right click anywhere and select *Add Permission*
    4. Select a given roll from the *Assigned Role* menu
    5. Under *Users and Groups* click *Add*
    6. Add the required user or groups to the role (either local or Active Directory)
    7. Click *OK*
    8. Click *OK*
    9. Verify that permissions have been applied correctly

- **Create/Clone/Edit vCenter Server Roles**
    - Create a vCenter Server Role
        1. Within the vSphere Client select the *Home* page and click *Roles*
        2. In the upper left corner click *Add Role*
        3. Provide a name of the new role in the *Name*
        4. Select the privileges you would like to provide the roll from the tree
        5. Click *OK* when completed

    - **Clone a vCenter Server Role**
        1. Within the vSphere Client select the *Home* page and click *Roles*
        2. Under *Roles -> Name* right click the role you wish to clone
        3. Select *Clone* from the options menu
        4. A new role is created with the name *Copy of <role name>*

    - **Edit a vCenter Server Role**
        1. Within the vSphere Client select the *Home* page and click *Roles*
        2. Under *Roles -> Name* right click the roll you wish to edit
        3. In the *Edit Role* screen you can change the roll name as well as change the roles privileges
        4. When edits are completed click *OK*

For further information read pages 61 thru 63 of the *vSphere Security* documentation

- **Add an ESXi Host to a directory service**
    1. Within the vSphere Client select a host and click on the *Configuration* tab
    2. In the left hand pane under *Software* select *Authentication Services*
    3. In the right hand pane select *Properties* to the right of *Authentication Services Settings*
    4. Change the drop down to *Active Directory* under *User Directory Service*
    5. *Under Domain Settings* enter the FQDN of the domain you wish to join in the *Domain* field
    6. Click the *Join Domain* button
    7. Enter a user name and password for account that has the rights to join the system to the Active Directory domain.
    8. Click *OK*
    9. Click *OK* to close the *Directory Services Configuration* window

For further information read pages 63 thru 70 of the *vSphere Security* documentation.

- **Apply permissions to ESXi Hosts using Host Profiles**
    1. Within the vSphere Client select the *Home* page and click *Host Profiles*
    2. Right click an existing host profile in the left hand pane and select *Edit Profile*
    3. Expand the profile tree, and then expand *Security Configuration*
    4. Right-click the *Permission rules* folder and select *Add Profile*
    5. Expand *Permission Rules* and select *Permission*
    6. On the *Configuration Details* tab in the right hand pane, click the *Configure a permission* drop-down menu and select *Require a Permission Rule*
    7. Enter the name of a user and group
    8. Enter the assigned role name for the user or group
    9. Select the *Propagate permission* check box and click *OK*

- **Determine the appropriate set of privileges for common tasks in vCenter Server**

  See section “Common Privileges” above

<u>Tools</u>

- vSphere Installation and Setup guide
- vCenter Server and Host Management guide
- vSphere Security guide
- Solutions and Examples for VMware vSphere 5 guide

Objective 1.5 – Identify vSphere Architecture and Solutions

Knowledge

- **Identify available vSphere editions and features**
  - VMware vSphere Editions

	Standard	Enterprise	Enterprise Plus
Entitlements per CPU License			
vRam Entitlement	32 GB	64 GB	96 GB
vCPU/VM	8 Way	8 Way	32 Way
Features			
Hypervisor	x	x	x
High Availability	x	x	x
Data Recovery	x	x	x
vMotion	x	x	x
Virtul Serial Port Concentrator		x	x
Hot Add		x	x
vShield Zones		x	x
Fault Tolerance		x	x
Storage APIs for Array Integration		x	x
Storage vMotion		x	x
Distributed Resource Scheduler		x	x
Distributed Power Management		x	x
Distributed Switch			x
I/O Controls (Network & Storage)			x
Host Profiles			x

Auto Deploy			x
Policy-Driven Storage			x
Storage DRS			x

- Two additional version of vSphere are available:
  - VMware vSphere Hypervisor - Free version of the hypervisor that consists of a subset of the functionality and has maximum RAM allocation of 32GB
  - VMware vSphere Desktop - Used for licensing vSphere in VDI deployments. Provides all Enterprise Plus features

- Acceleration Kits

	Essenitials	**Essentials Plus**	**Standard AK**	**Enterprise AK**	**Enterprise Plus AK**
Includes	6 CPUs	6 CPUs	8 CPUs	6 CPUs	6 CPUs
Entitlements per CPU License					
vRam Entitlement	32 GB	32 GB	32 GB	64 GB	96 GB
vCPU/VM	192GB Max 8 Way	192GB Max 8 Way	256GB Max 8 Way	384GB Max 8 Way	576GB Max 32 Way
Features					
Hypervisor	x	x	x	x	x
High Availability				x	x
Data Recovery				x	x
vMotion				x	x
Virtul Serial Port Concentrator		x	x	x	x
Hot Add		x	x	x	x
vShield Zones		x	x	x	x
Fault Tolerance		x	x	x	x
Storage API for Array Integration				x	x

Storage vMotion					
Distributed Resource Scheduler				x	x
Distributed Power Management				x	x
				x	x
Distributed Switch					x
I/O Controls (Network & Storage)					x
Host Profiles					x
Auto Deploy					x
Policy-Driven Storage					x
Storage DRS					x

For further information read pages 6 thru 8 of the *VMware vSphere 5.0 Licensing, Pricing and Packaging* white paper

- **Explain ESXi and vCenter Server architectures**
    - In a VMware vSphere deployment if you want to take full advantage of the features available to you vCenter Server most be used. vCenter Server is the single point that allows you to centrally manage your connected ESXi hosts as well as deploy new virtual machines at the basic level. As you move up through the vSphere licensed editions vCenter Server allows for the use of vMotion, Fault Tolerance, DRS, etc. Without it, you are just connecting directly to an ESXi host and managing them in a singular fashion and without the more advanced features outlined above

- **Explain Private/Public/Hybrid cloud concepts**
    - Private Cloud - Datacenter virtualization that is managed by and running on internal assets
    - Public Cloud - Datacenter virtualization that is managed by and running on 3rd party equipment housed in there facility. Compute resources are accessed via the Internet
    - Hybrid Cloud - A combination of both Private and Public clouds. You may have pieces of your business running on internal compute resources, but for DR/BC you may leverage a 3rd party facility

- **Determine appropriate vSphere edition based on customer requirements**
    - For the exam (and in your career) beware of what features are available based on the different vSphere editions (host profiles only with Enterprise Plus, etc). Also with the

changes in licensing know the vRAM entitlements (and maximums for Acceleration Kits) for each vSphere edition.

Tools

- VMware vSphere Basics guide
- vCenter Server and Host Management guide

Section 2 – Plan and Configure vSphere Networking

Objective 2.1 – Configure vNetwork Standard Switches

Knowledge

- **Identify vNetwork Standard Switch (vSS) capabilities**
  - A lot of the capabilities you find in a virtual switch are the same as a physical switch
    - Routes traffic internally between virtual machines and links to external networks
    - Allows for multiple port groups configured with different policies
      - Allows for VLANs
      - Create network labels for virtual machine virtual adapters to attach to (is unique within the current datacenter)
    - Balance communication across multiple network adapters
    - Configurable to handle physical NIC failure by failing over to another physical NIC
    - Maximum of 4096 total ports per host (vSS and vDS)
    - Maximum of 1016 total active ports per host (vSS and vDS)
    - Maximum of 4088 virtual network switch create ports
    - Maximum of 256 port groups

- **Create/Delete a vNetwork Standard Switch**
  - You can create/delete a vNetwork Standard Switch from the VI Client either connected directly to the host or through vCenter. The steps should be the same regardless of the management point.

    1. From within the VI Client select a host on the left
    2. Select the Configuration tab on the right
    3. Select Networking in the left column of the center pane
    4. Click Add Networking on the top right
    5. Choose Virtual Machine or VMkernel as connection type > click next
    6. Choose Create a vSphere standard switch and select any physical adapters you want to use > click next
    7. Fill in a Network Label and VLAN ID (optional) > click next
    8. Click Finish

- **Deleting a vNetwork Standard Switch**
    1. From within the VI Client select a host on the left
    2. Select the Configuration tab on the right
    3. Select Networking in the left column of the center pane
    4. Find the vNetwork Standard Switch you want to delete
    5. Choose Remove next to its name
    6. Click Yes to confirm you want to remove it

- **Add/Configure/Remove vmnics on a vNetwork Standard Switch**
    - You can Add/Configure/Remove vmnics from the VI Client either connected directly to the host or through vCenter. The steps should be the same regardless of the management point

        1. From within the VI Client select a host on the left
        2. Select the Configuration tab on the right
        3. Select Networking in the left column of the center pane
        4. Find the vNetwork Standard Switch on the right > click Properties
        5. Select the Network Adapters Tab
        6. Click Add to add a vmnic
            a. Select the adapter you want from the list below > click next
            b. Select the NIC order that you want > click next
            c. Click Finish
        7. To configure a vmnic select the adapter and click Edit (the only things you can configure are configured speed and duplex)
            a. Select your speed and duplex and click Ok
        8. To remove a vmnic select the adapter and click Remove

- **Configure vmkernel ports for network services**
    - You can configure a vmkernel port on an existing vNetwork Standard Switch or a new vNetwork Standard Switch. The three network services you can select are vMotion, Fault Tolerance logging and management traffic. It is best practice to segregate this each of these over different physical adapters, unless you are using converged networking (FCoE) or a lab environment.

        1. From within the VI Client select a host on the left
        2. Select the Configuration tab on the right
        3. Select Networking in the left column of the center pane
        4. Click Add Networking on the top right
        5. Select VMkernel > click Next
        6. Create a new vSphere standard switch or select an existing vSwitch > click next
        7. Enter in a Network Label (such as vMotion)
        8. Enter in an optional VLAN ID
        9. Select which network services you want this vmkernel to provide, in this case we will check Use this port group for vMotion > click Next
        10. Choose obtain IP settings automatically (not recommended unless you are using DHCP reservations) or choose Use the following IP settings

11. Enter in an IP address and Subnet Mask
12. You can choose to change your VMkernel Default Gateway by clicking the Edit button or you can leave it at the default, usually the default is good > click Next
13. Click Finish

- The new vmkernel port (it's really a port group) will now show up with a under your vNetwork Standard Switch. You will notice is has a vmk number which is in numeric order with any other vmkernels you have already created. You will also see the IP address you set next to the vmkernel port number.

- **Add/Edit/Remove port groups on a vNetwork Standard Switch**
  - Adding port groups on a vNetwork Standard Switch is straight forward and follows the same relative procedures and the previous tasks

1. From within the VI Client select a host on the left
2. Select the Configuration tab on the right
3. Select Networking in the left column of the center pane
4. Click Add Networking on the top right
5. Select Virtual Machine or VMkernel > click Next
6. Choose an existing vSwitch > click Next
7. Enter in the Network Label and VLAN ID (optional) – if you chose the vmkernel option choose one of the three network services > click Next
8. Click Finish

- Creating a Virtual Machine Port Group without a physical adapter will allow virtual machines connected to the same port group to communicate with each other, but they will not be able to access any external networks

  - Edit a port group on a vNetwork Standard Switch
    1. From within the VI Client select a host on the left
    2. Select the Configuration tab on the right
    3. Select Networking in the left column of the center pane
    4. Find the vSwitch that houses the port group(s) you want to edit and click Properties
    5. By default you are on the Ports tab, find the port group you want to edit within the list, select it and click Edit
    6. From here there are four different tabs you can configure options from; General, Security, Traffic Shaping, NIC Teaming. We will go over all of these in future objectives (all detailed on pages 43-60 of the vSphere Networking guide)
  - Remove a port group on a vNetwork Standard Switch
    1. From within the VI Client select a host on the left
    2. Select the Configuration tab on the right
    3. Select Networking in the left column of the center pane

4. Find the vSwitch that houses the port group(s) you want to remove and click Properties
5. By default you are on the Ports tab, find the port group you want to remove within the list, select it and click Remove
6. Click Yes to confirm you want to remove that selected port group
7. Close the vSwitch Properties dialog box when complete

- **Determine use case for a vNetwork Standard Switch**
  - There are a few use cases for using a vNetwork Standard Switch in your environemnt
    - The biggest one has to be licensing. To utilize a vNetwork Distributed Switch (vDS) you must be an Enterprise Plus customer or you have to us the vSS.
    - Regardless of licensing its good to place a redundant management network for each host on their own vNetwork Standard Switch. This will ensure your management network is available in case a you have a physical NIC failure and/or a vNetwork Distributed Switch
    - If you only have one host that needs access to a separate network that can't be provided through an existing vNetwork Distributed Switch then you would use a vNetwork Standard Switch

Tools

- Configuration Maximums for VMware vSphere 5.0
- vSphere Installation and Setup guide
- vSphere Networking guide

Objective 2.2 – Configure vNetwork Distributed Switches

Knowledge

- **Identify vNetwork Distributed Switch (vDS) capabilities**
  - A vNetwork Distributed Switch has the same capabilities as a vNetwork Standard Switch and much more. Keep in mind you must have an enterprise plus license to use this feature
    - Functions as a single switch across all hosts
      - Allows virtual machines to maintain consistent networking configuration regardless of the host they reside on
    - Can forward traffic to other virtual machines or link to an external network
    - Allows you to have one or more distributed port groups
      - Allows for VLANs
      - Create network labels for virtual machine virtual adapters to attach to (is unique within the current datacenter)
    - Network resource pools
      - You can manage traffic by the type of network traffic

- 4096 Maximum network switch ports per host (vDS and vSS)
- 1016 Maximum active ports per host (vDS and vSS)
- 30000 Maximum distributed virtual network switch ports per vCenter
- 350 Maximum hosts per vDS
- 32 Maximum distributed switches per vCenter

- **Create/Delete a vNetwork Distributed Switch**
  - Creating and deleting a vNetwork Distributed Switch is a bit different than a vNetwork Standard Switch. It is done from a different area from within the VI Client and can only be done using vCenter

    1. Log in to vCenter using the VI Client
    2. Go to the Networking view by clicking the View menu > Inventory > Networking (or Ctrl+Shift+N)
    3. Right-click on the Datacenter where you want to create the vDS and click New vSphere Distributed Switch
    4. Select the version of the vDS you want to create (4.0, 4.1.0 or 5.0.0) > click Next
    5. Give it a descriptive name and specify the number of uplink ports > click Next
    6. You can choose to add hosts now or later. If you choose to Add now select the host(s) and the associated physical adapters you want to use as uplinks > click Next
    7. Determine whether you want the wizard to create a default port group or not. If you plan on having multiple port groups, I advise NOT creating a default port group. Leave the *Automatically create a default port group* option checked, or uncheck it depending on your situation
    8. Click Finish

- **Add/Remove ESXi hosts from a vNetwork Distributed Switch**
  - Once you have created a vNetwork Distributed Switch you can go back and add new hosts or remove them from said switch.

    - Adding a host

      1. Log in to vCenter using the VI Client
      2. Go to the Networking view by clicking the View menu > Inventory > Networking (or Ctrl+Shift+N)
      3. Right-click on the vNetwork Distributed Switch you want to add and select *Add Host*
      4. Select the host(s) you want to add and their corresponding physical adapter(s) you want to use > click Next
      5. At this point you can assign any existing vmkernel ports (virtual adapters) from the vNetwork Standard Switch port groups to an existing port group on the vNetwork Distributed Switch. You can do this by selecting the virtual adapter and clicking *Assign port group…* button and selecting a port group, or, use the

drop down to select the new port group which is located in the *Destination port group* column > click Next

6. During this step you can elect to migrate virtual machine networking of an existing VMs from the vNetwork Standard Switch to the vNetwork Distributed Switch. Make the proper selection(s) > click Next
7. Click Finish

- Removing a host

1. Log in to vCenter using the VI Client
2. Go to the Networking view by clicking the View menu > Inventory > Networking (or Ctrl+Shift+N)
3. Click on the *Hosts* tab in the right pane
4. Right-click the host you want to remove and click *Remove from vSphere Distributed Switch…* > click *Yes* to confirm

- **Add/Configure/Remove dvPort groups**
  - At some point you may need to Add/Configure/Remove dvPort groups from your vNetwork Distributed Switches

- Adding a dvPort group

1. Log in to vCenter using the VI Client
2. Go to the Networking view by clicking the View menu > Inventory > Networking (or Ctrl+Shift+N)
3. Right-click on the vNetwork Distributed Switch you want to add the dvPort group to and click and click *New Port Group*
4. Specify the *Name, Number of Ports* and *VLAN type* (VLAN, VLAN Trunking or Private) > click Next
5. Click Finish

- Configure a dvPort group

1. Log in to vCenter using the VI Client
2. Go to the Networking view by clicking the View menu > Inventory > Networking (or Ctrl+Shift+N)
3. Right-click on dvPort group you want to configure and select *Edit Settings*
4. From here you can configure three different settings; *General, Policies,* and *Advanced*. There are 7 different options under *Policies* which we will dive into in **Objective 2.3**
5. Make any changes needed in any of the three settings (and their child settings)
6. Click *OK* or *Cancel*

- Removing a dvPort group

1. Log in to vCenter using the VI Client
2. Go to the Networking view by clicking the View menu > Inventory > Networking (or Ctrl+Shift+N)
3. Right-click on dvPort group you want to configure and select *Delete*
4. Click *Yes* to confirm the deletion

- **Add/Remove uplink adapters to dvUplink groups**

1. Log in to vCenter using the VI Client
2. Select the *Configuration* tab on the right
3. Select *Networking* in the left column of the center pane
4. Click on the *vSphere Distributed Switch* button at the top
5. Click the *Manage Physical Adapters* hyperlink
6. From the left side of the window is where you can *Add/Remove* physical adapters. If all your uplinks are taken up with physical adapters, and you need to add more physical adapters, add more uplink ports to your vNetwork Distributed Switch
7. Click *OK* or *Cancel* when finished

- **Create/Configure/Remove virtual adapters**

  - Creating a virtual adapter

1. Log in to vCenter using the VI Client
2. Select a host from the left pane and then click the *Configuration* tab on the right
3. Select *Networking* in the left column of the center pane
4. Click on the *vSphere Distributed Switch* button at the top
5. Click the *Manage Virtual Adapters* hyperlink
6. Click the *Add* hyperlink at the top
7. Select *New virtual adapter* > click *Next*
8. Select *VMkernel* > click *Next*
9. Select the appropriate port group from the drop down or select an individual port
10. If you want this virtual adapter to run any network services (vMotion, FT logging or management) select the appropriate checkbox(s) > click *Next*
11. Select *Obtain IP settings automatically* or *Use the following IP settings*
    a. If you select *Use the following IP settings*, input the *IP Address* and *Subnet Mask* and the *VMkernel Default Gateway* (typically you leave this at the default)
12. Click *Next*
13. Click *Finish*

  - Configuring an existing virtual adapter

1. Log in to vCenter using the VI Client
2. Select a host from the left pane and then click the *Configuration* tab on the right
3. Select the *Configuration* tab on the right
4. Select *Networking* in the left column of the center pane
5. Click on the *vSphere Distributed Switch* button at the top
6. Click the *Manage Virtual Adapters* hyperlink
7. Select the name of the virtual adapter you want to configure and click the *Edit* hyperlink
8. From here there are two tabs; *General* and *IP Settings*. From the *General* tab you can change the port group or port settings, the network services settings (vMotion, FT logging, management) and you can also set the MTU size for the virtual adapter. The IP settings are self-explanatory.
9. Click *OK* or *Cancel* when complete

- Removing a virtual adapter

1. Log in to vCenter using the VI Client
2. Select a host from the left pane and then click the *Configuration* tab on the right
3. Select *Networking* in the left column of the center pane
4. Click on the *vSphere Distributed Switch* button at the top
5. Click the *Manage Virtual Adapters* hyperlink
6. Select the virtual adapter you want to delete and click the *Remove* hyperlink
7. Click *Yes* to confirm you the deletion
8. Click *Close* when finished

- **Migrate virtual adapters to/from a vNetwork Standard Switch**

    - Migrate *To* a vNetwork Distributed Switch

    1. Log in to vCenter using the VI Client
    2. Select a host from the left pane and then click the *Configuration* tab on the right
    3. Select *Networking* in the left column of the center pane
    4. Click on the *vSphere Distributed Switch* button at the top
    5. Click the *Manage Virtual Adapters* hyperlink
    6. Click the *Add* hyperlink at the top
    7. Select *Migrate existing virtual adapters* > click *Next*
    8. Select the virtual adapter(s) you want to migrate > select a *port group* from the drop down under the *Port Group* column > click *Next*
    9. Click *Finish*

    - Migrate *From* a vNetwork Distributed Switch to a vNetwork Standard Switch

    1. Log in to vCenter using the VI Client
    2. Select a host from the left pane and then click the *Configuration* tab on the right
    3. Select *Networking* in the left column of the center pane

4. Click on the *vSphere Distributed Switch* button at the top
5. Click the *Manage Virtual Adapters* hyperlink
6. Select the virtual adapter you want to migrate and click the *Migrate* hyperlink
7. Select the vSphere Standard Switch > click *Next*
8. Enter in a *Network Label* and an *Optional VLAN ID* > click *Next*
9. Click *Finish*

- **Migrate virtual machines *to/from* a vNetwork Distributed Switch**

    - Migrate virtual machines *To/From* a vNetwork Distributed Switch

        1. Log in to vCenter using the VI Client
        2. Go to the Networking view by clicking the View menu > Inventory > Networking (or Ctrl+Shift+N)
        3. Right-click on the vNetwork Distributed Switch you want to migrate to and select *Migrate Virtual Machine Networking…*
        4. For the *Source Network* you can choose to *Include all virtual machine network adapters that are connect to the following network:* (pick that network from the drop down) or you can I*nclude all virtual machine network adapters not connect to any network*. Also select a *Destination Network* from the drop down > click *Next*
        5. Select the virtual machine(s) you want to migrate; you can also select all or only certain network adapters if needed > click *Next*
        6. Click Finish

- **Determine use case for a vNetwork Distributed Switch**

    - The first thing I want to mention is that you must have an Enterprise Plus license if you want to use the vNetwork Distributed Switch (even if you choose the Cisco Nexus 1000v).
    - If you have many hosts it's simpler and makes more sense to implement a vNetwork Distributed Switch for management and virtual machine flexibility. Without it, you have to ensure all port groups and policies match for each hosts vNetwork Standard switch—a management nightmare!
    - If you need to perform NetFlow functions, Port Mirroring or have Private VLANs, you need a vNetwork Distributed Switch
    - If you want to utilize the *Route based on physical NIC load* Load Balancing policy (allows a single TCP flow over multiple NICs if utilization is high)
    - If you have a need to control network traffic; vSphere 5 has improved Network I/O Control (NOIC) and has introduced Network Resource Pools, both features require a vNetwork Distributed Switch

<u>Tools</u>

- vSphere Installation and Setup guide

- vSphere Networking guide

Objective 2.3 – Configure vSS and vDS Policies

Knowledge

- **Identify common vSS and vDS policies**
  - When looking at vSS and vDS policies there is some overlap. Instead of breaking it down by each type, I will list the common policies (at least these are what I envision as common) and at the end of each tell what they can be applied to; vSS, vDS or both
  - Common Policies
    - *Security* – applies to vSS and vDS
      - Policy exceptions include *Promiscuous Mode*, *MAC Address Changes* and *Forged Transmits*
    - *Traffic Shaping* – can be applied to outbound traffic on a vSS and can be applied to outbound and/or inbound traffic on a vDS
      - Policy exceptions include *Average Bandwidth* (Kbits/sec), *Peak Bandwidth* (Kbits/sec) and *Burst Size* (Kbytes)
    - *NIC Teaming* (on vSS) and *Teaming and Failover* (on vDS) – both contain same policies
      - Policies include *Load Balancing*, *Network Failover Detection*, *Notify Switches*, *Failback* and *Failover Order*
  - Some other common policies that only apply to the vDS are *Monitoring* and *Resource Allocation*

- **Configure dvPort group blocking policies**
  - You can configure an individual dvPort group on a vDS to block all ports (this can't be done on a vSS)

    1. Log in to vCenter using the VI Client
    2. Go to the Networking view by clicking the *View* menu > *Inventory* > *Networking* (or Ctrl+Shift+N)
    3. Right-click on the dvPort group you want to block ports on and select *Edit Settings…*
    4. Select the *Miscellaneous* policy under the *Policies* tree
    5. Change the drop down for *Block all ports* to *Yes* – **Changing this option to Yes will shut down all the ports for this port group**
    6. Click *OK*

- **Configure load balancing and failover policies**
  - The load balancing policies are used to determine how outbound traffic spread across multiple physical adapters (vmnics). Inbound load balancing is handled by the physical switch the physical uplinks are connected to
  - Editing these policies for the vSS and vDS are done in two different locations within the VI Client. I will first explain how to get to them for each, then explain the policies (policies are the same with one exception, which will be identified)

    - vNetwork Standard Switch (vSS)

      1. Log in to vCenter or directly to the host using the VI Client
      2. Select a host from the left pane and then click the *Configuration* tab on the right
      3. Select *Networking* in the left column of the center pane
      4. Click the *Properties* hyperlink next to the vSS you want to modify
      5. Select the vSwitch or port group you want to modify and click *Edit*

         NOTE: All settings from the vSwitch are propagated to individual port groups. Modifying settings on an individual port group will override the settings propagated by the vSwitch

      6. Select the *NIC Teaming* tab

    - vNetwork Distributed Switch (vDS)

      1. Log in to vCenter using the VI Client
      2. Go to the Networking view by clicking the *View* menu > *Inventory* > *Networking* (or Ctrl+Shift+N)
      3. Right-click on the dvPort group you want to configure and select *Edit Settings…*
      4. Under Policies select *Teaming and Failover*

    - Load Balancing and Failover Policies

      1. The first Policy Exception is Load Balancing; there are four/five options (vSS and vDS respectively):

         i. *Route based on the originating port ID*: This setting will select a physical uplink based on the originating virtual port where the traffic first entered the vSS

ii. *Route based on IP hash*: This setting will select a physical uplink based on a hash produced using the source and destination IP address. When using IP hash load balancing:
    - The physical uplinks for the vSS must be in an ether channel on the physical switch
    - All port groups using the same physical uplinks should use IP hash load balancing policy
iii. *Route based on source MAC hash*: This setting is similar to IP hash in the fact that it uses hasing, but it uses hashing based on the source MAC address and does not require additional configuration on the physical switch
iv. *Use explicit failover order*: This setting uses the physical uplink that is listed first under Active Adapters
v. *Route based on Physical NIC load* **(vDS ONLY)**: This setting determines which adapter traffic is routed to based on the load of the physical NICs listed under Active Adapters. This is my personal favorite as it requires ZERO physical switch configurations and is true load balancing

2. The next policy exception is Network Failover Detection; there are two options:

    i. *Link Status only*: Using this will detect the link state of the physical adapter. If the physical switch fails or if someone unplugs the cable from the NIC or the physical switch, failure will be detected and failover initiated. *Link Status only* is not able to detect misconfigurations such as VLAN pruning or spanning tree
    ii. *Beacon Probing*: This setting will listen for beacon probes on all physical NICs that are part of the team (as well as send out beacon probes). It will then use the information it receives from the beacon probe to determine the link status. This method will typically be able to detect physical switch misconfigurations as initiate a failover. **Do not use beacon probing when using the IP hash load balancing policy**

3. Select *Yes* or *No* if for the Notify Switches policy. Choosing *Yes* will notify the physical switches to update its lookup tables whenever a failover event occurs or whenever a virtual NIC is connected to the vSS. **If using Microsoft NLB in unicast mode set this setting to *No***
4. Select *Yes* or *No* for the Failback policy. Choosing *Yes* will initiate a failback when a failed physical adapter becomes operational. If you choose *No* then a failed physical adapter that becomes operational will only become active again if/when the standby adapter that was promoted fails
5. The last policy is Failover Order; this has three sections

i. *Active Adapters*: Physical adapters listed here are active and are being used for inbound/outbound traffic. Their utilization is based on the load balancing policy. These adapters will always be used when connected and operational
ii. *Standby Adapters*: Physical adapters listed here are on standby and only used when an active adapter fails or no longer has network connectivity.
iii. *Unused Adapters*: Physical adapters listed here will not be used

6. Once finished click *OK* or *Cancel*

- **Configure VLAN settings**
  - VLAN settings on virtual switches allow traffic flowing to/from virtual machines to be a part of a physical VLAN

- vNetwork Standard Switch (vSS)

1. Log in to vCenter or directly to the host using the VI Client
2. Select a host from the left pane and then click the *Configuration* tab on the right
3. Select *Networking* in the left column of the center pane
4. Click the *Properties* hyperlink next to the vSS you want to modify
5. Select port group you want to modify and click *Edit*
6. On the *General* tab you can modify the *VLAN ID* (optional) if you want to perform VLAN tagging at the vSS layer. Enter in a *VLAN ID* for this particular port group
7. Click *OK* or *Cancel* when finished

- vNetwork Distributed Switch (vDS)

1. Log in to vCenter using the VI Client
2. Go to the Networking view by clicking the *View* menu > *Inventory* > *Networking* (or Ctrl+Shift+N)
3. Right-click on the dvPort group you want to configure and select *Edit Settings…*
4. Under Policies select *VLAN*
5. There are four options for VLAN type:
   i. *None*: VLAN tagging will not be performed by this dvPort group
   ii. *VLAN*: Enter in a valid VLAN ID (1-4094). The dvPort group will perform VLAN tagging using this VLAN ID
   iii. *VLAN Trunking*: Enter a range of VLANs you want to be trunked

iv. *Private VLAN*: Select a private VLAN you want to use – the Private VLAN must be configured first under the dvSwitch settings prior to this option being configurable
    - You can learn more about Private VLANs on pages 27-28 of the vSphere Networking document listed in the tools section

6. Click *OK* or *Cancel* when finished

- **Configure traffic shaping policies**
  - Traffic shaping can be configured for both the vSS and the vDS. When configuring on the vSS you can configure of for the entire vSwitch and those settings will be propagated down to all port groups (can be overridden per port group); traffic shaping applies only to egress traffic on a vSS. You can only configure traffic shaping on the vDS per dvPort group; traffic shaping can be applied to egress and ingress traffic on the vDS.
  - Except for the fact that you can configure ingress/egress traffic shapping on the vDS, the policies are the same when configuring a vSS or vDS. Therefore, I will list how to navigate to traffic shaping separately, but the policies and their configurations will be explained as one

- vNetwork Standard Switch (vSS)

1. Log in to vCenter or directly to the host using the VI Client
2. Select a host from the left pane and then click the *Configuration* tab on the right
3. Select *Networking* in the left column of the center pane
4. Click the *Properties* hyperlink next to the vSS you want to modify
5. Select the vSwitch or port group you want to modify and click *Edit*

NOTE: All settings from the vSwitch are propagated to individual port groups. Modifying settings on an individual port group will override the settings propagated by the vSwitch

6. Select the *Traffic Shaping* tab

- vNetwork Distributed Switch (vDS)

1. Log in to vCenter using the VI Client
2. Go to the Networking view by clicking the *View* menu > *Inventory* > *Networking* (or Ctrl+Shift+N)
3. Right-click on the dvPort group you want to configure and select *Edit Settings…*
4. Under Policies select *Traffic Shaping*

- Traffic Shaping Policies

1. Once you navigate to the appropriate location you will see four different settings (on a vDS you will see these settings twice; one for ingress and one for egress)
2. The first option is Status and you can choose *Enabled* or *Disabled*. These should be self-explanatory
3. *Average Bandwidth* (defined in Kbits/sec): this setting is used to determine the allowed number of Kbits/sec to traverse each individual port and is averaged over time
4. *Peak Bandwidth* (defined in Kbits/sec): Workloads tend to have periods of burst; meaning network traffic will increase for a short period of time. The number you enter for *Peak Bandwidth* determines the maximum amount of Kbits/sec that can traverse each individual port
5. *Burst Size* (defined in Kbytes/sec): Ports gain a burst bonus when it does not use all of the bandwidth it is allocated. When the port needs additional bandwidth then defined in *Average Bandwidth*, it can use its burst bonus. The *Burst Size* setting will limit the number of Kbytes gained by the burst bonus
6. Click *Ok* or *Cancel* when finished

- **Enable TCP segmentation Offload support for a virtual machine**
  - TCP segmentation Offload (TSO) can be enabled at the virtual machine level for VMs running the following guest operating systems
    - Microsoft Windows 2003 EE with SP2 (32 bit and 64 bit)
    - RHEL 4 (64 bit)
    - RHEL 5 (32 bit and 64 bit)
    - SUSE Linux Enterprise Server 10 (32 bit and 64 bit)
  - TSO is enabled by default on the VMkernel interface
  - You must use the enhanced vmxnet virtual network adapter
  - If you are replacing an existing virtual adapter be sure to record the network settings and MAC address of the old adapter

1. Login to vCenter or directly to an ESXi host using the VI Client
2. Navigate to the Hosts and Cluster view by clicking the *View* menu > *Inventory* > *Hosts and Clusters* (or Ctrl+Shift+H)
3. Right-click on the virtual machine you want to enable TSO on > click *Edit Settings…*
4. On the Hardware tab click *Add* (if replacing an existing adapter; record network settings and MAC and remove the Network Adapter on the list first)
5. Select *Ethernet Adapter* > click *Next*
6. For type, choose *VMXNET 3* under the dropdown
7. Specify the Network to connect to using the dropdown and whether you want the adapter to be connected at power on > click *Next*
8. Click *Finish*
9. Upgrade VMware Tools manually if necessary (VMware tools are required to use the vmxnet virtual adapters)

NOTE: If TSO somehow gets disabled on a VMkernel interface you must delete said interface and recreate it with TSO enabled

- **Enable Jumbo Frames support on appropriate components**
  - Jumbo Frames can be enabled at the vSS layer, the vDS layer, the VM layer and the VMkernel interface
  - A jumbo frame is a 9KB (9000 bytes) frame that enables less frames to be sent and push more throughput on a physical interface.
  - In order to take full advantage of jumbo frames your physical infrastructure must not only support them, but be configured for them, end-to-end

- vNetwork Standard Switch (vSS)

1. Log in to vCenter or directly to the host using the VI Client
2. Select a host from the left pane and then click the *Configuration* tab on the right
3. Select *Networking* in the left column of the center pane
4. Click the *Properties* hyperlink next to the vSS you want to modify
5. Select the vSwitch vmkernel interface you want to modify and click *Edit*
6. Change the *MTU* from 1500 to *9000*
   a. If modifying the virtual switch this is located on the *General* tab under *Advanced Properties*
   b. If modifying a vmkernel interface this is located on the *General* tab under *NIC Settings*
7. Click *OK* or *Cancel* when finished

- vNetwork Distributed Switch (vDS)

1. Log in to vCenter using the VI Client
2. Go to the Networking view by clicking the *View* menu > *Inventory* > *Networking* (or Ctrl+Shift+N)
3. Right-click on the dvSwitch you want to configure and select *Edit Settings…*
4. On the *Properties* tab select *Advanced*
5. Change the *Maximum MTU* from 1500 to *9000*
6. Click *OK* or *Cancel* when finished

- Virtual Machine (VM)

1. Login to vCenter or directly to an ESXi host using the VI Client

2. Navigate to the Hosts and Cluster view by clicking the *View* menu > *Inventory* > *Hosts and Clusters* (or Ctrl+Shift+H)
3. Right-click on the virtual machine you want to enable TSO on > click *Edit Settings…*
4. On the Hardware tab click *Add* (if replacing an existing adapter; record network settings and MAC and remove the Network Adapter on the list first)
5. Select *Ethernet Adapter* > click *Next*
6. For type, choose *VMXNET 3* under the dropdown
7. Specify the Network to connect to using the dropdown and whether you want the adapter to be connected at power on > click *Next*
8. Click *Finish*
9. Upgrade VMware Tools manually if necessary (VMware tools are required to use the vmxnet virtual adapters)
10. Configure jumbo frames for the virtual network adapter within the guest operating system
11. Ensure all physical switches are configured for jumbo frames

- **Determine appropriate VLAN configuration for a vSphere implementation**
  - There is no blanket VLAN configuration for a vSphere implementation. As I'm sure you have heard before, it all depends on your environment and what your requirements are. A few principals to keep in mind though:
    - There are three VLAN configuration options when it comes to VLAN tagging
      - *External Switch Tagging* (EST): all VLAN tagging of packets happens at the physical switch and all VLAN IDs in the virtual switches should be set to 0 (zero)
      - *Virtual Switch Tagging* (VST): all VLAN tagging occurs at the virtual switch. This requires the ports that the physical uplinks are connected to be configured as a trunk port. VLAN IDs must be specified at the port group level
      - *Virtual Guest Tagging* (VGT): VLAN tagging is done by the virtual machine. The 802.1Q VLAN trunking driver must be installed on the VM for this to work properly. All the ports on the physical switch connected to the physical adapters on the vSwitch must be configured as trunk ports
  - Consider the three VLAN tagging methods above and apply them to your environment. If you decide to use Virtual Switch Tagging (VST) be aware the physical ports they are connected to not only must be configured as a trunk, but should not have a native VLAN either or you can run into conflicts (i.e. tagged with the same VLAN by the vSwitch and pSwitch)

<u>Tools</u>

- vSphere Installation and Setup guide
- vSphere Networking guide

Section 3 – Plan and Configure vSphere Storage

Objective 3.1 – Configure Shared Storage for vSphere

Knowledge

- **Identify storage adapters and devices**
  - List of storage adapters includes:
    - SCSI adapter
    - iSCSI adapter
    - RAID adapter
    - Fibre Channel adapter
    - Fibre Channel over Ethernet (FCoE) adapter
    - Ethernet adapter
  - Device drivers are part of the VMkernel and are accessed directly by ESXi
  - In the ESXi context, devices, also sometimes called Logical Unit Numbers (LUNs) are represented by a SCSI volume that is presented to the host. Some vendors expose this as a single target with multiple storage devices (LUNs), and others expose this as multiple targets with on device (LUN) each. As far as ESXi is concerned, a device is a SCSI volume presented to a host

- **Identify storage naming conventions**
  - There are three different types of device identifiers used that make up part of the storage naming convention. Here they are along with their corresponding device ID formats:
    - SCSI INQUIRY Identifiers: these will be unique across all hosts and are persistent. The host uses the SCSI INQUIRY command in order to use the page 83 information (Device Identification) to generate a unique identifier
      - *naa.number*
      - *t10.number*
      - *eui.number*
    - Path-based Identifier: When a device is queried and does not return page 83 information, the host generates an mpx.*path* name. *Path* represents the path to that particular device. This is created for local devices during boot and is not unique or persistent (could change upon next boot)
      - Example: mpx.vmhba1.C0:T0:L0
    - Legacy Identifier : ESXi also generates an legacy name as an alternative with the following format:
      - Vml.*number*
        - The *number* are digits unique to the device and can be taken from a part of the page 83 information if it's available

- **Identify hardware/dependent hardware/software iSCSI initiator requirements**

- A hardware iSCSI adapter offloads the network and iSCSI processing from the host. There are two types of hardware iSCSI adapters; dependent hardware iSCSI adapter and independent hardware iSCSI adapter (ensure these are listed on the HCL)
  - Dependent Hardware iSCSI Adapter
    - these types of adapters depend on VMware networking and the iSCSI management interfaces within VMware
    - dependent upon the host's network configuration for IP and MAC
  - Independent Hardware iSCSI Adapter
    - These types of adapters are independent from the host and VMware
    - Provides its own configuration management for IP and other network address assignment
- The software iSCSI adapter is built into VMware's code, specifically the VMkernel. Using this type of adapter you can connect to iSCSI targets using a standard network adapter installed on the host. Since this is a software adapter, network processing and encapsulation are performed by the host, which does use host resources

- **Compare and contrast array thin provisioning and virtual disk thin provisioning**
  - Virtual Disk Thin Provisioning
    - Allows you to create virtual disks of a logical size that initially differs from the physical space used on a datastore. If you create a 40GB thin disk, it may initially use only 20GB of physical space and will expand as needed up to 40GB
    - Can lead to over-provisioning of storage resources
  - Array Thin Provisioning
    - Thin provision a LUN at the array level
    - Allows you to create a LUN on your array with a logical size that initially differs from the physical space allocated—can expand up to logical size over time
    - Array thin provisioning is not ESXi aware without using the storage APIs for array integration (VAAI). With a VAAI capable array, the array can integrate with ESXi, which at that point ESXi is aware that the underlying LUNs are thin provisioned
    - Using VAAI you can monitor space on the thin provisioned LUNs and tell the array when files are freed (deleted or removed) so the array can reclaim that free space
  - My opinion is, if your array supports array thin provisioning and VAAI then use array thin provisioning and thick disks within vSphere. Even though you are choosing a thick disk for your virtual disk type, it is still thin by proxy of array thin provisioning

- **Describe zoning and LUN masking practices**
  - Zoning and LUN masking are somewhat similar in the fact that they are used for access control between different objects and devices that may or may not need to communicate with each other
    - Zoning – Use single-initiator zoning or single-initiator-single-target zoning (more restrictive). Each vendor will have different zoning practices/best practices

        - Defines which Host Bus Adapters (HBAs) can connect to which targets on the SAN. Objects that aren't zoned to one another, or are outside of a particular zone aren't visible
        - Reduces the number of LUNs and targets presented to a particular host
        - Controls/isolates paths in your SAN fabric
        - Prevents unauthorized systems from accessing targets and LUNs
    - LUN Masking – exact same thing as zoning, but applied only for LUN-host mapping
        - Limits which hosts can see which LUNs
        - Can be done at the array layer or the VMware layer

- **Scan/Rescan storage**
    - There are many different situations in which storage is Scanned/Rescanned; here are a few
        - When adding a new storage device, storage will be scanned/rescanned afterwords; a scan for new Storage Devices will be done and a scan for new VMFS volumes will initiate
        - After adding/removing iSCSI targets
        - You can perform a Rescan manually by performing the following steps:

            1. Log in to vCenter or directly to the host using the VI Client
            2. Select a host from the left pane and then click the *Configuration* tab on the right
            3. Select *Storage* in the left column of the center pane
            4. Click the *Rescan All…* hyper link on the top right
            5. Select which items you want to scan for; *Scan for New Storage Devices* and *Scan for New VMFS Volumes* (both are checked by default)
            6. Click OK and wait for the scan to complete, after which point any new Storage Devices or VMFS Volumes that exist will be displayed and available

- **Identify use cases for FCoE**
    - FCoE adapters are used to access fibre channel storage. FCoE encapsulates FC frames into Ethernet frames and uses 10Gbit lossless Ethernet as transport to the storage array
    - Like the iSCSI adapter, there are two types of FCoE adapters; software and hardware
        - Software FCoE Adapter:
            - Uses the native FCoE protocol stack within ESXi to process the FCoE protocol
            - Requires a physical NIC that has I/O offload and Data Center Bridging (DCB) capabilities
            - Maximum of 4 FCoE software adapters per host
        - Hardware FCoE Adapter:
            - Specialized adapter that carries Ethernet and FC over the same connectiong (SFP or SFP+)
            - For Ethernet, the hardware FCoE adapter appears as a vmnic in the networking area of ESXi
            - For Fibre Channel, the hardware FCoE adapter appears as a vmhba in the storage area of ESXi
    - When would use a hardware or software FCoE adapter?

- When your datacenter supports 10Gbit Ethernet
- When you want to reduce your footprint inside your hosts, as well as reduce the cable count coming from each host
- When you have existing DCB technologies in your datacenter (i.e. Cisco Nexus 5K/7K or Cisco MDS)

- **Create an NFS share for use with vSphere**
  - This is going to be subjective to your particular storage device, but the basic steps are:
    - Create a storage volume
    - Create a folder on that storage volume
    - Create a share for that folder
    - Allow the IP of your host(s) to access the storage
    - Give the IPs of your host read/write access to the share you created
- **Connect to a NAS device**
  - Connecting to a NAS device is similar to creating a VMFS datastore; here are the steps

    1. Log in to vCenter or directly to the host using the VI Client
    2. Select a host from the left pane and then click the *Configuration* tab on the right
    3. Select *Storage* in the left column of the center pane
    4. Click the *Add Storage…* hyperlink
    5. Choose *Network File System* > click *Next*
    6. Enter in the *Server*, *Folder*, and what the name of the *Datastore* you want
    7. Click *Next*
    8. Click *Finish*

- **Enable/Configure/Disable vCenter Server storage filters**
  - There are 4 different storage filters in vSphere 5 and they are all enabled by default
    - config.vpxd.filter.vmfsFilter
      - Filters out storage devices or LUNs that are already used by a VMFS datastore on any host managed by vCenter. These LUNs will not have the option to be formatted with another VMFS datastore and cannot be used as a RDM
    - config.vpxd.filter.rdmFilter
      - Filters out any LUNs already referenced as a RDM for any host managed by vCenter
    - config.vpxd.filter.SameHostAndTransportsFilter
      - Filters out LUNs that are unable to be used as a VMFS datastore extent
        - LUNs that aren't exposed on all the hosts that the datastore you are trying to extend is exposed to
        - LUNs that are using a different storage type than the original datastore (datastore using local storage can't use an iSCSI extent to extend the datastore)
    - config.vpxd.filter.hostRescanFilter
      - This filter, when enabled, automatically rescans and updates VMFS datastores after you perform datastore management operations
  - How to Enable/Configure/Disable

1. Log in to vCenter using the VI Client
2. Click the *Administration* menu from the menu bar
3. Select *vCenter Server Settings*
4. Choose *Advanced Settings* on the left
5. At the bottom in the textbox labeled *Key*: enter in the value of the storage filter you want to enable or disable (.vmfsFilter, .rdmFilter, .SameHostAndTransportFilter or .hostRescanFilter)
6. In the textbox labeled *Value:* type *True* to enable it or *False* to disable it
    - Keep in mind that these filters are enabled by default
7. Click *Add*
8. To edit a key that is already added in the displayed list click on the current value for the key you want to configure and change it (*True* to enable, *False* to disable)
9. Click *OK* or *Cancel* when finished

- **Configure/Edit hardware/dependent hardware initiators**
    - Independent Hardware iSCSI Adapters

1. Install the adapter based vendor documentation
2. Verify the adapter is installed correctly and configure it:
    - Log in to vCenter or directly to the host using the VI Client
    - Select a host from the left pane and then click the *Configuration* tab on the right
    - Select *Storage Adapters* in the left column of the center pane
    - If installed properly, you will see the new adapter in this list
    - Select the newly installed adapter and click the *Properties…* hyperlink
    - From here you can change the default iSCSI name, alias and IP settings
3. Click *OK* when finished

    - Dependent Hardware iSCSI Adapters: When you install a dependent hardware iSCSI adapter you will be presented with a standard network port and a storage adapter. To Configure:

1. Determine the association between the dependent hardware adapter and the physical NIC
    - Find the physical NIC listed under *Network Adapters* that is associated with your dependent hardware adapter, you'll need this for later in the configuration
2. Log in to vCenter or directly to the host using the VI Client
3. Select a host from the left pane and then click the *Configuration* tab on the right
4. Select *Storage Adapters* in the left column of the center pane
5. If installed properly, you will see the new adapter in this list
6. Select the newly installed adapter and click the *Properties…* hyperlink
7. Select the *Network Configuration* tab and click *Add*
8. Add the network adapter that corresponds to the iSCSI adapter listed
9. Click *OK*

- **Enable/Disable software iSCSI initiator**
  - Enable software iSCSI initiator: If you haven't already added a software iSCSI initiator, do so now:

    1. Log in to vCenter or directly to the host using the VI Client
    2. Select a host from the left pane and then click the *Configuration* tab on the right
    3. Select *Storage Adapters* in the left column of the center pane
    4. Click the *Add…* hyperlink
    5. Select *Add Software iSCSI Adapter*
    6. Click *OK* twice
    7. The newly added software iSCSI adapter should show in the list and is enabled by default
    8. To disable, highlight the software iSCSI adapter and click the *Properties…* hyperlink on the bottom right
    9. Click *Configure…*
    10. Uncheck the *Enabled* checkbox
    11. Click *OK*
    12. Click *Close*

- **Configure/Edit software iSCSI initiator settings**

    1. Log in to vCenter or directly to the host using the VI Client
    2. Select a host from the left pane and then click the *Configuration* tab on the right
    3. Select *Storage Adapters* in the left column of the center pane
    4. Highlight the software iSCSI adapter you want to configure and click the *Properties…* hyperlink on the bottom right
    5. Click *Configure…*
    6. Here you can change the *Status* (enabled or disabled), the *iSCSI Name* and the *iSCSI Alias*
    7. Click *OK* or *Cancel* when complete
    8. On the *Network Configuration* tab you can configure VMkernel Port Bindings (will go over in the next section)
    9. *Dynamic Discovery* tab
        - Click *Add*
        - Enter in the iSCSI target you want to dynamicall discover in the *iSCSI Server* field
        - Leave the *Port* set to 3260 unless you have changed it in your environment
        - Skip *CHAP…* if you are using it in your environment and do not have it configured to use it's parent (we will cover CHAP global configuration in a future section)
        - Click *OK*
        - Once the dynamic discovery is complete all targets for that server should populate in the *Static Discovery* tab
    10. *Static Discovery*

- Click *Add*
- Enter in the *iSCSI Server* IP, the *Port* and the *iSCSI Targert Name*
- Skip *CHAP…* if you are using it in your environment and do not have it configured to use it's parent (we will cover CHAP global configuration in a future section)
- Click *OK*

11. Click *Close* once complete

- **Configure iSCSI port binding**

1. Log in to vCenter or directly to the host using the VI Client
2. Select a host from the left pane and then click the *Configuration* tab on the right
3. Select *Storage Adapters* in the left column of the center pane
4. Highlight the software iSCSI adapter you want to configure and click the *Properties…* hyperlink on the bottom right
5. Select the *Network Configuration* tab
6. Click *Add…*
7. Select the *VMkernel Adapter* that corresponds to the *Physical Adapter* you want to bind
8. Click *OK*

NOTE: When using the dependent hardware iSCSI adapter the only VMkernel interface that will display in the list is the one associated with the physical NIC for that dependent hardware adapter

- **Enable/Configure/Disable iSCSI CHAP**
  - There are two types of CHAP you can enable within the iSCSI initiator; normal CHAP, in which the target (a SAN typically) authenticates the host connecting to it, and Mutual CHAP, in which the host also authenticates the target. Mutual CHAP is the most secure, and here is how to configure both:
    - *CHAP* (target authenticates host)

1. Log in to vCenter or directly to the host using the VI Client
2. Select a host from the left pane and then click the *Configuration* tab on the right
3. Select *Storage Adapters* in the left column of the center pane
4. Highlight the software iSCSI adapter you want to configure and click the *Properties…* hyperlink on the bottom right
5. Click the *CHAP…* button
6. Select an option
   - *Do not use CHAP* – CHAP will not be used
   - *Do not use CHAP unless required by target* – CHAP will only be used if its required by the back-end storage
   - *Use CHAP unless prohibited by target* – CHAP will always be used unless the back-end storage is not configured for it

        - *Use CHAP* – CHAP will be used all the time
    7. Either check the *Use initiator name* checkbox to use the initiator name (uses the IQN of the adapter) as a login, or enter a name in the *Name* field
    8. Enter in the CHAP secret in the *Secret* field

- *Mutual CHAP* (host authenticates target)
    - In order to use Mutual CHAP you must have the normal CHAP set to the *Use CHAP* option or else the only option available for Mutual CHAP will be Do not use CHAP

        1. Log in to vCenter or directly to the host using the VI Client
        2. Select a host from the left pane and then click the *Configuration* tab on the right
        3. Select *Storage Adapters* in the left column of the center pane
        4. Highlight the software iSCSI adapter you want to configure and click the *Properties…* hyperlink on the bottom right
        5. Click the *CHAP…* button
        6. Select an option

            - *Do not use CHAP* – CHAP will not be used
            - *Use CHAP* – CHAP will be used all the time

        7. Either check the *Use initiator name* checkbox to use the initiator name (uses the IQN of the adapter) as a login, or enter a name in the *Name* field
        8. Enter in the CHAP secret in the *Secret* field

        NOTE: the Secret for CHAP and Mutual CHAP must be different

- **Determine use case for hardware/dependent hardware/software iSCSI initiator**
    - Independent hardware iSCSI initiator
        - If you have a very heavy iSCSI environment with a lot of I/O (OLTP) you may want to use a hardware iSCSI initiator, this will off-load all network processing to the physical NIC, which will be more efficient and free up resources on the physical host
    - Dependent hardware iSCSI initator
        - You may already have NICs that support this option so there is no reason to buy another one
        - If you are in a high iSCSI I/O environment, a dependent hardware iSCSI initiator may work as iSCSI traffic bypasses the networking stack and goes straight to the hardware adapter, while the network portion of the adapter uses VMkernel networking. This leads to a lower footprint, being able to use one adapter for both functions
    - Software iSCSI initiator
        - You can leverage existing Ethernet adapters and run networking and iSCSI in the same adapter; VMkernel processes all networking and iSCSI traffic

        - Low cost

- **Determine use case for and configure array thin provisioning**
    - Configuring array thing provisioning is going to be different for each type of array so you should consult the vendor documentation in order to configure array thin provisioning
    - Use Cases
        - Uniformity – once you provision it for the LUN, it won't matter if the virtual disk created is thick or thin, it will always be thin because the LUN is thin provisioned
        - Less overhead – when integrated with storage APIs the host can inform the array when datstore space is freed up and allow the array to reclaim the freed blocks
        - Ease of use – allows an administrator to easily monitor space usage on thin provisioned LUNs

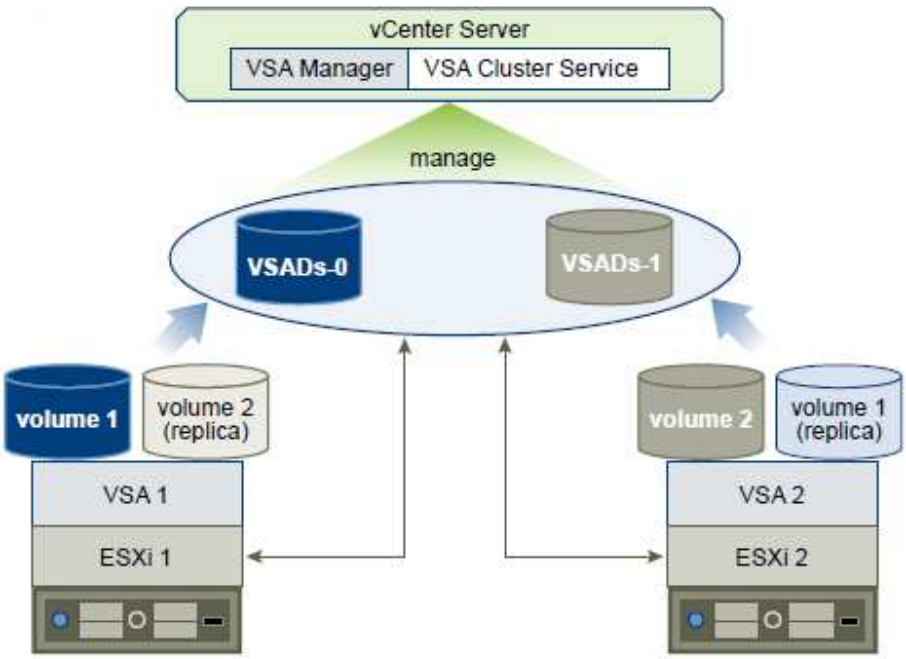
Tools

- vSphere Installation and Setup guide
- vSphere Storage guide
- VMware vSphere Examples and Scenarios guide

Objective 3.2 – Configure the Storage Virtual Appliance for vSphere

Knowledge

- **Define Storage Virtual Appliance (SVA) architecture**
    - Below is how VMware describes their two node VSA Cluster Architecture from page 9 of the VMware vSphere Storage Appliance Installation and Configuration:



- As depicted in the diagram above, the components needed for the SVA are:
  - Physical hosts with local storage running ESXi 5.0 (can only be configured in a two or three node cluster)
  - In clusters using only two nodes (like above) the VSA Cluster Service runs on the vCenter machine. In a three node cluster this is not required
  - Each host has an active volume and a replica volume of one of the other hosts
- Networking for VSA
  - Network traffic is broken up into front-end and back-end traffic
    - Front-end traffic
      - Provides communication between each VSA member cluster and the VSA cluster service
      - Provides communication between each VSA cluster member and the VSA manager
      - Provides communication between ESXi and the VSA volumes
    - Back-end traffic
      - Provides clustering communication between all VSA cluster members
      - Provides the network for vMotion traffic between hosts running the VSA
      - Provides replication between a volume and its replica that's located on another host
  - Each VSA has two virtual NICs, one for front-end traffic and one for back-end traffic; back-end uses private IP space of 192.168.*.*
- How it works:
  - Each VSA has two volumes; its own active volume and a replica volume for another VSA. This is true in a two or three node cluster. Each VSA runs an NFS server. The NFS server takes the active volume on the VSA and exports it as an NFS volume and then

presents that NFS volume back to the ESXi server. VMware states that the underlying storage needs to be in a RAID 10 configuration so half the RAID 10 volume is for the active volume, and the other half for the replica volume. The idea is basically RAID 10 for the volume, but between cluster nodes, so if you lose the physical node, the volume is still active on the secondary… (I know it is a bit convoluted!)

- Quick run-down of Hardware and Software ESXi requirements for VSA:
  - 64-bit x86 CPUs @ 2GHz or higher per core
  - Memory
    - 6GB minimum
    - 24 GB recommended
    - 72 GB maximum/tested
  - 4 NIC ports per host
  - 8 hard disks with same capacity per host, no more than 2TB each
  - RAID controller that supports RAID10
  - Must be running ESXi 5.0

- **Configure ESXi hosts as SVA hosts**
  - Your ESXi hosts need to be what the VSA installer refers to as "greenfield", which is basically a fresh install of ESXi 5 with no virtual machines and no additional configuration
  - The root password should be the same on all ESXi hosts that are joining the VSA cluster
  - Assign static IPs and VLANs (optional) to your ESXi host(s)
  - Assign a hostname and DNS servers on your ESXi host(s)
  - Install vCenter Server as a physical server or VM
    - If you install as a VM do not install it on an ESXi host that you're using for the VSA
    - Install the vSphere Client on the vCenter Server
  - If using the GUI to install the VSA
    - Create a new vDatacenter
    - Add hosts to vDatacenter
  - If using the command line to install the VSA, do not create a vDatacenter or add hosts to vCenter - - the automated installation will handle all of that
  - Install the VSA Manager on the vCenter server

For prerequisite information or step-by-step procedures of the preceding items refer to pages 29-34 of the VMware vSphere Storage Appliance Installation and Configuration document

- **Configure the storage network for the SVA**
  - You need to have at least four physical NICs per ESXi host
  - You need a Gigabit Ethernet switch
    - If you want to use VLANs it must support 802.1q VLAN trunking
  - You need a DHCP server if you plan to use DHCP to obtain the vSphere Feature IP Address automatically
  - Configuring the networks:

- Ensure the physical ports on your Gig switch are set for 802.1q VLAN trunking if you are using VLANs and that the VLAN IDs you are using aren't being pruned
- Using the GUI to install the VSA (two-member cluster without DHCP, requires 11 static IP addresses)
  - Prior to running the VSA install within the VI client you will need to IP both ESXi hosts and the vCenter server
  - Once you have started the install you will be prompted to enter the remaining IP addresses
    - The first two are global IPs, meaning not host-centric:
      - VSA Cluster IP Address
      - VSA Cluster Service IP Address
    - The next four addresses are for VSA1: these are host-centric
      - Management IP Address for VSA1 (front-end)
      - Datastore IP address for VSA1 (front-end)
      - Back- end IP address for VSA1
      - vSphere feature IP address for ESXi host 1 (can be assigned via DHCP)
      - Specify VLAN (optional)
    - The next four addresses are for VSA2: these are host-centric
      - Management IP Address for VSA2 (front-end)
      - Datastore IP address for VSA2 (front-end)
      - Back- end IP address for VSA2
      - vSphere feature IP address for ESXi host 2 (can be assigned via DHCP)
      - Specify VLAN (optional)

- **Deploy/Configure the SVA Manager**
  - There are a few steps you need to take in order to deploy/configure the SVA Manager. The first thing you will need to do is install the VSA manager on the vCenter server you are using in your VSA deploymen

  - Install VSA Manager

    - Log on to the vCenter server
    - Run the VSA Manager install file (as of this posting it is VMware-vsamanager-en-1.0.0-458417.exe)
    - Choose you language > click *OK*
    - Click *Next* twice
    - Accept the EULA > click *Next*
    - Enter in the IP address and port for the vCenter server that will manage the VSA (should default to the vCenter IP you are on and port 443) > click *Next*
    - Enter in license key or leave blank to install in evaluation mode > click *Next*
    - Click *Install*

- Click *Finish*

- Deploy/Configure the VSA

1. Log in to vCenter or directly to the host using the VI Client
2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*
3. If a vDatacenter doesn't exist, create one (right-click the vCenter object at the top and click *New Datacenter*)
4. Add the two or three hosts you want to use for the VSA to the vDatacenter (remember, these must be greenfield hosts, i.e. no configuration)
5. Click the vDatacenter on the left and select the *VSA Manager* tab in the right pane (requires Adobe Flash)
6. Select *Yes* to accept the security certificate
7. Choose *New Installation* > click *Next* > click *Next*
8. Choose the vDatacenter you want to use > click *Next*
9. Choose the hosts you want to use for the VSA by checking the checkbox next to each host (three maximum) > click *Next*
10. Enter in IPs for the *VSA Cluster IP Address* and *VSA Cluster Service IP Address*
11. Enter in the IPs for the first host; *Management IP Address* and *Datastore IP Address*. The *vSphere Feature IP Address* is set to use DHCP, but you can uncheck that and manually enter one
12. Enter a VLAN ID (optional) for the Front-end network
13. Enter in the last two octets for the Back-end IP Address
14. Enter in a VLAN ID (optional) for the Back-end network
15. Repeat steps 10-14 for each additional host (by default all IPs are auto-filled in a contiguous manner after you enter in the IPs for the VSA Cluster IP and VSA Cluster Service IP)
16. Click *Next*
17. Choose either *Format disks on first access* or *Format disks immediately* > click *Next*
18. Click *Install* > click *Yes* to confirm starting the installation

- **Administer SVA storage resources**
  - Once the install is complete you get a dashboard look of everything going on in the VSA, here is how you get into it and what items are administrable
  - The hosts that are participating in the VSA cluster are now presented with NFS datastores, two or three depending on the number of hosts part of the VSA cluster

  - The VSA Manager Tab

1. Log in to vCenter or directly to the host using the VI Client

2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*
3. Click the vDatacenter on the left and select the *VSA Manager* tab in the right pane (requires Adobe Flash)
4. Select *Yes* to accept the security certificate
5. Here you are presented with a dashboard:
    - Shows the VSA Cluster status
    - Shows you the VSA Cluster Network
    - Shows your storage capacity
6. If you want to put the VSA cluster in maintenance mode click the *Enter VSA Cluster Maintenance Mode…* hyperlink > click *Yes* to confirm > click *Close* once it is complete
7. To exit cluster maintenance mode click the *Exit VSA Cluster Maintenance Mode…* hyperlink
8. You can change the password for the cluster by click the *Change Password* hyperlink. Enter in the older username and password and then enter and confirm the new password > click *OK*
9. You can reconfigure the network by clicking the *Enter Reconfigure Network Mode…* hyperlink > click *Yes* to confirm – THE VSA CLUSTER WILLBECOME UNAVAILABLE WHILE YOU RECONFIGURE THE NETWORK
    - Enter in your new network settings
    - Click *Next*
    - Click *Install* > click *Yes* to confirm
10. You can export logs by clicking on the *Export Logs…* hyperlink. Once it completes click the *Download* button and choose a place to save the logs
11. As you can see the Datastores view in the lower portion of the pain gives you all the data for each individual datastore
12. Click the *Appliances* button to view information about the appliances
13. Click the *Enter Appliance Maintenance Mode…* if you want to place an individual VSA into maintenance mode
14. Manage the VSA datastores the same way you would manage any other NFS datastore, see Objective 3.3 for more details on how to manage/administer an NFS datastore

- **Determine use case for deploying the SVA**
    - There are a few different use cases for the SVA, with the biggest one I believe to be the SMB
    - SMBs most likely can't afford an expensive SAN; even an entry-level SAN/NAS, so even though the VSA license may be a bit expensive (~6K), it is still at least 50% cheaper than an entry-level SAN, and it enables you to utilize existing storage and get all the features in vSphere that require shared storage. There are some arguments against because of the steep price, but I won't get into that here
    - If you are limited on power or space and need a bit of shared storage, the VSA may be a good option for you to utilize power and real estate that's already being consumed

- **Determine appropriate ESXi host resources for the SVA**
  - Determining resource for your ESXi hosts resources for the SVA are, as always, going to depend on the environment, and the requirement. There will be many of design considerations that you need to take into account:
    - What kind of workloads will you be running
    - How many hosts you need is determined by how much capacity is needed
    - Each host can have a max of 8 hard disks, design capacity with that mind
    - How many VMs will you store on the VSA
    - Memory over-commitment is NOT supported for VSA ESXi hosts
    - Reserve all if the memory that is allocated to each VSA appliance VM
    - Disable a virtual machine from doing VMX swapping to a VSA datastore
      - Requires an advanced configuration setting
        - Sched.swap.vmxSwapEnabled = True

Tools

- VMware vSphere Storage Appliance Installation and Configuration guide
- VMware vSphere Storage Appliance Administration guide

Objective 3.3 – Create and Configure VMFS and NFS Datastores

Knowledge

- **Identify VMFS and NFS Datastore properties**
  - VMFS Datastore Properties
- **Identify VMFS5 capabilities**
  - VMFS5 is a major improvement over VMFS3 (IMHO) with one of the biggest improvements being the 32x increase in datastore capacity, a whopping 64TTB!
  - Here is a list of VMFS5 capabilities:
    - Supports greater than 2TB storage devices for each VMFS extent
    - All block sizes are now standard at 1MB
    - Support for greater than 2TB disks for RDM (physical compatibility mode)
    - Scalability improvements for storage devices supporting hardware acceleration (VAAI)
      - ESXi supports NAS plug-ins for array integration
    - Atomic test and set (ATS) locking on storage devices that support hardware acceleration is now the default locking mechanism
    - Can reclaim physical storage space on thin provisioned storage devices
    - Online upgrades of datastores without service disruption

- **Create/Rename/Delete/Unmount a VMFS Datastore**
  - Create a VMFS Datastore

1. Log in to vCenter or directly to the host using the VI Client
2. Select a host from the left pane and then click the *Configuration* tab on the right
3. Select *Storage* in the left column of the center pane
4. Click the *Add Storage…* hyperlink
5. Select *Disk/LUN* for the storage type > click *Next*
6. Select the disk you want to use > click *Next*
7. Select *VMFS-5* for the file system version > click *Next* > click *Next*
8. Input a *datastore name* > click *Next* (you should make it something descriptive)
9. Choose whether to use *Maximum available space* or *Custom Space* (if choosing *Custom space* enter in the amount you want to use, in GB) > click *Next*
10. Click *Finish*

- Rename a VMFS Datastore

1. Log in to vCenter or directly to the host using the VI Client
2. Select a host from the left pane and then click the *Configuration* tab on the right
3. Select *Storage* in the left column of the center pane
4. Right-click on the datastore you want to rename and select *Rename*
5. Enter in the new name and press enter or click a different area of the screen to commit the change

- Delete a VMFS Datastore

1. Log in to vCenter or directly to the host using the VI Client
2. Select a host from the left pane and then click the *Configuration* tab on the right
3. Select *Storage* in the left column of the center pane
4. Right-click on the datastore you want to delete and select *Delete*
5. Choose *Yes* to confirm the deletion operation (this will delete all files and virtual machines on this datastore

- Delete a VMFS Datastore

1. Log in to vCenter or directly to the host using the VI Client
2. Select a host from the left pane and then click the *Configuration* tab on the right
3. Select *Storage* in the left column of the center pane
4. Right-click on the datastore you want to unmount and select *Unmount*
5. At this point there are five checks that are performed before you can Unmount a datastore (If one or more of these checks fail you must remediate it and repeat this step):
    1) No virtual machines can reside on the datastore
    2) The datastore can't be part of a datastore cluster
    3) The datastore can't be managed by storage DRS
    4) The datastore must have Storage I/O control disabled
    5) The datastore can't be used for vSphere HA heartbeat
6. Click *OK*

NOTE: to mount, right-click the inactive datastore and select *Mount*

- **Mount/Unmount an NFS Datastore**
  - Mount an NFS Datastore

    1. Log in to vCenter or directly to the host using the VI Client
    2. Select a host from the left pane and then click the *Configuration* tab on the right
    3. Select *Storage* in the left column of the center pane
    4. Click the *Add Storage…* hyperlink
    5. Select *Network File System* > click *Next*
    6. Enter in the server name or IP address in the *Server* field
    7. Enter in the folder path for the NFS share in the *Folder* field
    8. Check the *Mount NFS read only* checkbox if you want to mount the NFS volume as read only
    9. Enter in a name for the datastore in the *Datastore Name* field > click *Next*
    10. Click *Finish*
    11. The new NFS datastore should now appear in the Datastores view

  - Unmount an NFS Datastore

    1. Log in to vCenter or directly to the host using the VI Client
    2. Select a host from the left pane and then click the *Configuration* tab on the right
    3. Select *Storage* in the left column of the center pane
    4. Right-click the NFS datastore you want to unmounts and select *Unmount*
    5. Click *Yes* to confirm the remove datastore operation

- **Extend/Expand VMFS Datastores**
  - Extend/Expand a VMFS Datastore – Adding Extents negates your ability to use Storage I/O Control (SIOC) for that VMFS datastore

    1. Log in directly to the host using the VI Client
    2. Select a host from the left pane and then click the *Configuration* tab on the right
    3. Select *Storage* in the left column of the center pane
    4. Right-click on the datastore you want to extend/expand and select *Properties…*
    5. Click the *Increase…* button under Volume Properties
    6. Choose the device you want to use to extend the datastore > click *Next* > click *Next*
    7. Choose the *Custom space setting* option and enter in how much space you want to use in GB or choose the *Maximum available space* option > click *Next*
    8. Click *Finish*
    9. Click *Close* to return to the Datastores view

- **Upgrade a VMFS3 Datastore to VMFS5**

- When you upgrade the datastore, the ESXi file-locking mechanism ensure that no local processes or remote hosts can access the datastore
- This is a one-way only process; no downgrading
- How to upgrade a VMFS3 Datastore to VMFS5 – will not change block size to 1MB

    1. Log in to vCenter or directly to the host using the VI Client
    2. Select a host from the left pane and then click the *Configuration* tab on the right
    3. Select *Storage* in the left column of the center pane
    4. Right-click on the datastore you want to extend/expand and select *Properties…*
    5. Click the *Upgrade to VMFS-5…* hyperlink located towards the bottom right
    6. Click *OK* to confirm and start the VMFS-5 upgrade process

- **Place a VMFS Datastore in Maintenance Mode**
    - How to place a VMFS datastore into Maintenance Mode

        1. Log in to vCenter using the VI Client
        2. Click the *View* menu at the top > select *Inventory* > select *Datastores and Datastore Clusters* (or *Ctrl + Shift + D*)
        3. Select the datastore on the left that you want to place in maintenance mode
        4. Click the *Summary* tab
        5. In the Commands pane, click the *Enter SDRS Maintenance Mode* hyperlink
        6. To exit maintenance mode click the *Exit SDRS Maintenance Mode* hyperlink

- **Select the Preferred Path for a VMFS Datastore**
    - How to select a Preferred Path for a VMFS Datastore

        1. Log in to vCenter or directly to the host using the VI Client
        2. Select a host from the left pane and then click the *Configuration* tab on the right
        3. Select *Storage* in the left column of the center pane
        4. Right-click on the datastore you want and select *Properties…*
        5. Click the *Manage Paths…* button
        6. Right-click on the path you want to set as preferred and select *Preferred*
        7. Once you do this there should be a checkbox next to *Preferred* in the context menu and an asterisk (*) next to that path under the *Preferred* column
        8. Click *Close* twice

- **Disable a path to a VMFS Datastore**
    - How to disable a particular path(s) to a VMFS Datastore

        1. Log in to vCenter or directly to the host using the VI Client
        2. Select a host from the left pane and then click the *Configuration* tab on the right
        3. Select *Storage* in the left column of the center pane
        4. Right-click on the datastore you want and select *Properties…*
        5. Click the *Manage Paths…* button
        6. Right-click on the path you want to disable and select *Disable*

7. Once you do this there should be a checkbox next to *Disable* in the context menu and the Status should say *Disabled*
8. Click *Close* twice

- **Determine use case for multiple VMFS/NFS Datastores**
  - There are a few big use cases for using multiple VMFS/NFS Datastores
    - Datastores sit on backend storage that have physical disks configured in a particular way. If you have a requirement where some applications need more space, or need to be faster than others, creating multiple datastores with different characteristics will solve that requirement
    - Disk contention could be a problem, having different datastore will allow you to spread those workloads over different physical disks
    - HA and resiliency – having multiple datastores allows you to spread your VMs across them. If you lose a datastore, all of your VMs won't go down, only VMs located on that particular datastore

- **Determine the appropriate Path Selection Policy for a given VMFS Datastore**
  - Determining the appropriate Path Selection Policy (PSP) for a given VMFS Datastore, or course, depends on the situation:
    - Different storage back-ends support different PSP, some are active/passive, some are active/active (ALUA)
    - Number of physical storage adapters also is a factor; if you have on physical adapter with paths to 2 storage processor, you are protected againast a storage processor failure, but if the physical NIC fails, you get into an All Paths Down(APD) scenario, which = not good!
    - If you are using virtualized storage, such as EMC VPLEX or NetApp Metro-Cluster, you may not want to use Round-Robin
    - There are also third-party pathing plug-ins, such as EMC PowerPath/VE, which will dynamically load balance, perform failback, and is VM/Storage aware

Tools

- vSphere Installation and Setup guide
- vSphere Storage guide

Section 4 – Deploy and Administer Virtual Machines and vApps

Objective 4.1 – Create and Deploy Virtual Machines

Knowledge

- **Identify capabilities of virtual machine hardware versions**

Virtual Hardware Version	Memory Limits	CPU Limits	Description
8	1011GB (5.x)	32	Compatible with ESXi 5.0 and later hosts. Provides the latest virtual machine features.
7	255GB (4.x)	8	Compatible with ESX/ESXi4, 4.x, and 5.0 hosts. Recommended for sharing storage or VM;s with ESX/ESXi versions 3.5 to 4.1
4	65532MB (3.5) 16384MB (3.x)	4	Compatible with ESX/ESXi 3.0 and later hosts. Recommended for VM's that need to run on ESX/ESXi 3.x hosts

Information provided by VMware KB article KB1014006 as well as pages 81 thru 82 of the vSphere Virtual Machine Administration documentation.

- **Identify VMware Tools device drivers**

Driver Name	Description
SVGA Driver	This virual driver enabled 32-bit display, high display resolution, and significantly faster graphics performance. When you install VMware Tools, a virtual SVGA driver replaces the default VGA driver, which allows for only 640 x 480 resolution and 16-bit color On Windows guest operating systems whose operating systems is WInodws Vista or later, the VMware SVGA 3D (Microsoft - WDDM) driver is installed. This driver provides the same base funtionality as teh SVGA driver, and it adds Windows Aero support
SCSI Driver	When you create a virtual machine, if you specify that you want the virtual machine to use a BusLogic adapter, he guest operating system uses the SCSI driver that VMware Tools provides. Some recent guest operating systems, howerver, contain LSI Logic Parallel or LSI Logic SAS drivers. For example, Windows Server 2008 defaults to LSI Logic SAS, which provides the best performance for that operating system. In this case, the LSI Logic SAS driver provided by the operating system is used
Paravirtual SCSI Driver	This driver is for PVSCSI adapters, which enhance the perfromance of some virtualized applications
VMXNet NIC Drivers	The vmxnet and vmxnet3 networking drivers improve netwokr perfomrance. Which driver is used depends on how you configure devices settings for the virtual machine. When you install VMware Tools, a VMXNet NIC driver replaced the default vlance driver
Mouse Driver	The virtual mouse driver improves mouse performance. Tis driver is required if you use some third-party tools such as Microsoft Terminal Services
Audio Driver	This sound driver is required for all 64-bit Windows guest operating systems and 32-bit Windows Server 2003, WIndows Server 2008, and Windows Vista guest operating systems if you use the virtual machine with VMware Server, Workstation, or Fusion
Kernel Module for Sharing Folder	The host-guest file system module, called hgfs.sys on Windows guest operating systems and vmhgfs on Linux and Solaris, is required to use the virtual machine with Workstation or Fusion and share folders between hosts and guests.
ThinPrint Driver	This driver enables the virtual printing feature on Microsoft Windows virtual machines. With

	virtual printing, printers added to the operating system on the client or host appear in the list of available printers in the gust operating system. No additional printer drivers must be installed in the virtual machine
Memory Control Driver	This driver is available and recommended if you use VMware vSPhere. Excluding this driver hinders the memory management capabilities of the virtual machine in a vSphere deployment
Modules and Drivers That Support Making Automatic Backups	If the guest operating system is Windows Vista, Windows Server 2003, or other newer Windows operating systems, a Volume Shadow Copy Services (VSS) module is installed. For other, older Windows operating systems, the Filesystem Sync driver is installed. These modules enable backup applications to create application-consistent snapshots. During the snapshotting process, certain processes are paused and virtual machine disks are quiesced
VMCI and VMCI Sockets Drivers	The Virtual Machine Communication Interface driver allows fast and efficient communications between virtual machines. Developers can write client-server applications to the VMCI Sock (vSock) interface to make use of the VMCI virtual device

Chart information provided from pages 8 thru 9 of the *Installing and Configuring VMware Tools* document as well as VMware KB Article KB340.

- **Identify methods to access and use a virtual machine console**
    - In vSphere 5 there are now two ways to access a virtual machines console. First the newest way via the vSphere Web Client. To do so you need to download and install the Client Integration Plug-In. Second, and the tried and true way is via the vSphere Client.

For step by step instructions on using either of two ways refer to pages 202 thru 203 of the *vSphere Virtual Machine* Administraiton document

- **Identify virtual machine storage resources**

File	Usage	Description
.vmx	vmname.vmx	Virtual machine configuration file
.vmxf	vmname.vmxf	Additional virtual machine configuration files
.vmdk	vmname.vmdk	Virtual disk characteristics
-flat.vmdk	vmname-flat.vmdk	Prealocated virtual disk
.nvram	vmname.nvram or nvram	Virtual machine BIOS or EFI configuration
.vmsd	vmname.vmsd	Virtual machine snapshots
.vmsn	vmname.vmsn	Virtual machine snapshot data file
.vswp	vmname.vswp	Virtual machine swap file
.vmss	vmname.vmss	Virtual machine suspend file

.log	vmware.log	Current virtual machine log file
-#.log	vmware-#.log (where # is a number starting with 1)	Old virtual machine log entries

- **Place virtual machines in selected ESXi hosts/Clusters/Resource Pools**

  - Host or Cluster

    1. On the *Host/Cluster* page of the *New Virtual Machine* wizard, select the host or cluster where you want to run the virtual machine
    2. Click *Next*

  - Resource Pool

    1. On the *Resource Pool* page of the *New Virtual Machine* wizard, navigate to the resource pool where you want to run the virtual machine
    2. Select the resource pool and click *Next*

- **Configure and deploy a Guest OS into a new virtual machine**
  1. Open the vSphere Client and log in to the vCenter Server system or host on which the virtual machine resides
  2. Select an installation method:
     a. CD-ROM - Insert the installation CD-ROM for your guest operating system into the CD-ROM drive of your ESXi host
     b. ISO image - Mount the ISO image from a VMFS or NFS datastore to VM
  3. Right-click the virtual machine and select *Power -> Power On*
  4. Follow the installation instructions that the operating system vendor provides

- **Configure/Modify disk controller for virtual disks**
  1. From within the vSphere Client select a VM in your inventory
  2. Right click the VM and select *Edit Settings*
  3. Click the *Hardware* tab, select a SCSI controller, and click *Change Type* (Note, the VM needs to be powered down for this option to be available)
  4. Select a SCSI controller type and click *OK*
  5. Click *OK* to save your changes and close the dialog box

For further information refer to page 36 of the vSphere Virtual Machine Administration documentation

- **Configure appropriate virtual disk type for a virtual machine**

Option Type	Action
Thick Provision Lazy Zeroed (zeroedthick)	Space required for the virtual disk is allocatd during the creation of the disk file. Any data remaining on the physical device is not earased during creation, but is zeroed out on demand at a later time on first write from the virtual machine. The virtual machine

	does not read stale data from disk.
Thick Provision Eager Zeroed (eagerzeroedthick)	Space required for the virtual disk is allocated at creation time. In contrast to zeroedthick format, the data remaining on the physical device is zeroed out during creation. It might take much longer to create disks in this format thant ot create other types of disks
Thin Provision	Space required for the virtual disk is not allocated during creation, but is supplied and zeroed out, on demand at a later time
Raw Device Mapping (RDM)	Allows a VM to store its data directly on a SAN LUN. The RDM file (which ends in .vmdk) contains the LUN mapping information that ESXi uses to process I/O to the assigned LUN

For further information about disk types refer to VMware KB article KB1022242 as well as pages 36 thru 40 of the v*Sphere Virtual Machine Administration* document. For further information regarding Raw Device Mapping (RDM) refer to pages 135 thru 141 of the *vSphere Storage* document.

- **Create/Convert thin/thick provisioned virtual disks**
    1. From within the vSphere Client select a VM in your inventory
    2. Click the *Summary* tab and under *Resources* double click the datastore for the virtual machine to open the *Datastore Browser* dialog box
    3. Click the virtual machine folder to find the virtual disk file you want to convert. The file has the .vmdk extension
    4. Right-click the virtual disk file and select *Inflate*

- **Configure disk shares**
    1. From within the vSphere Client select a VM in your inventory
    2. Right click the VM and select *Edit Settings*
    3. Click the *Resources* tab and select *Disk*
    4. In the Resource Allocation panel, select the virtual hard disk to change
    5. Click the Shares column and change the value to allocate a number of shares of its disk bandwidth to the virtual machine
        - Low (500)
        - Normal (1000)
        - High (2000)

    6. Custom - Allows for a user-defined share value
    7. Click the *Limit - IOPS* column and enter the upper limit of storage resources to allocate to the virtual machine
    8. Click *OK* to save your changes and close the dialog box

- **Install/Upgrade/Update VMware Tools**
    1. From within the vSphere Client select a VM in your inventory
    2. Right click the VM and select *Guest -> Install/Upgrade VMware Tools*
        a. If you are perfoming a first time installation of VMware tools, click *OK* on the *Install VMware Tools* dialog box

    b. If you are perfomring an upgrade/update in the Install/Upgrade VMware Tools dialog box, select *Interactive Tools Installation* or *Interactive Tools Upgrade* and click *OK*
3. If autorun is not enabled, to manually launch the wizard, click *Start -> Run* and enter *D:\Setup.exe,* where D: is your first virtual CD-ROM drive
4. Follow the on-screen instructions
    a. If you use vSphere, to install nondefault components, select the *Custom* setup
5. If the New Hardware wizard appears, go through the wizard and accept the defaults
6. If you are installing a beta or RC version of VMware Tools and you see a warning that a package or driver is not signed, click *Install Anyway* to complete the installation
7. When prompted, reboot the virtual machine

- **Configure virtual machine time synchronization**
    1. Open a command prompt or termial in the guest operating system
    2. Change to the VMware Tools installation directory (refer to table below)
    3. Enter the command to determine whether time synchronization is enabled (refer to table below)

       utility-name timesync status

    4. Enter the command to enable or disable periodic time synchronization

       utility-name timesync <disable/enable>

Operating System	Default Path	Utility Name
Windows	C:\Program Files\VMware\VMware Tools	VMwareToolboxCmd.exe
Linux and Solaris	/usr/sbin	vmware-toolbox-cmd
FreeBSD	/usr/local/sbin	vmware-toolbox-cmd

For further information read pages 30 thru 31 of the *Installing and Configuring VMware Tools* documentation

- **Convert a physical machine using VMware Converter**
- **Modify virtual hardware settings using VMware Converter**

  Each of these topics could take several pages to fully explain and walk through. For a clear understanding of each of these processes (as well as others) read through the *VMware vCenter Converter Standalone User's Guide*.

- **Configure/Modify virtual CPU and Memory resources according to OS and application requirements**

This section is all about right sizing your virtual machines with the correct amount of available resources compared to the needed resources. Does the application require 2 vCPU's or if you present it 2 vCPU's would it properly leverage those resources? How about memory, does it need the full 4GB that is mentioned by the application vendor or after trending analysis it can run with only 3GB.

Thankfully with the options vSphere provides if you need to make these needed adjustments (if you plan accordingly ahead of time) on the fly. If need be and if supported by your guest operating system vSphere allows for the "Hot Add" of both vCPU and memory resources. If the above application was configured with 3GB of memory and truly needs 4GB you can add the additional memory without any downtime to the server or application. Same holds for CPU, if additional resources are needed and them on the fly (based guest operating system support)

For further information on both CPU and Memory resource setup and configuration refer to pages 88 thru 106 of the vSphere Virtual Machine Administration documentation.

- **Configure/Modify virtual NIC adapter and connect virtual machines to appropriate network resources**
    1. In the vSphere Client inventory, right-click the virtual machine and select Edit Settings
    2. Click the Hardware tab and select the appropriate NIC in the Hardware list
    3. (Optional) To connect the virtual NIC when the virtual machine is powered on, select Connect at power on
    4. (Optional) Click the blue information icon under DirectPath I/O to view details regarding the virtual NIC's DirectPath I/O status and capability
    5. Select an option for MAC address configuration

Option	Description
Automatic	vSphere assigns a MAC address automatically
Manual	Type the MAC address to use

6. Configure the Network Connection for the virtual NIC

Option	Description
Standard Settings	The virtual NIC connects to standard or distribured port group. Select the port group for the virtual NIC to connect to from the Network label drop-down menu
Advanced Settings	The virtual NIC connects to a specific port on a vSphere distributed switch. This option appears only when a vSphere distributed switch is available

	1. Click *Switch to advanced Settings* 2. Select a vSphere distributed switch for the virtual NIC to use from the *VDS* drop-down menu 3. Type the Port ID of the distributed port for virtual NIC to connect to

7. Click *OK* to save yoru changes and close the dialog box

- **Determine appropriate datastore locations for virtual machines based on application workloads**

  Storage can be divided into different tiers depending on a number of factors:

  - High Tier - Offers high performance and high availability. Might offer built-in snapshots to facilitate backups and point-in-time restorations. Supports replication, full SP redundancy, and SAS drives. Uses high-cost spindles
  - Mid Tier - Offers mid-range performance, lower availability, some SP redundancy, and SCSI or SAS drives. May offer snapshots. Uses medium-cost spindles
  - Lower Tier - Offers low perfomance, little internal storage redundancy. Uses low end SCSI drives or SATA

For further information read pages 26 thru 27 of the vSphere Storage documentation

Tools

- vSphere Virtual Machine Administation guide
- Installing and Configuring VMware Tools Guide

Objective 4.2 – Create and Deploy vApps

Knowledge

- **Identify vApp settings**

  - Options Tab

    - Resources - Just like with Resource Pools, with vApps you can allocate CPU and memory resources and control Shares, Reservations and Limits
    - Properties - Allows for configuration of custom properties in the OVF environment of the vApp. Defined under the *Advanced -> Properties* section

- IP Allocation Policy - Allow for the configuration of how IP addresses are allocated. Three options available; *Fixed*, *Transient*, and *DHCP*. Configured under *Advanced -> IP Allocation*
- Advanced - Allows for the setting of the Product Name, Version, Vendor URL, etc. Also as stated above the advanced configuration of *Properties* and *IP Allocation*

- Start Order Tab

- The start order tab allows you to set the Startup and Shutdown actions of groups of VM's. This allows you to control the startup order of VM's in a vApp. For example, you have a DB server that needs to be started prior to the application server coming up.

- **Create/Clone/Export a vApp**

- Create a vApp

1. Within the vSphere Client right click a cluster resource and select *New vApp*
2. Name the vApp and select an inventory location, click *Next*
3. Set the cpu and memory resource allocation, click *Next*
4. Select *Finish* to complete the *New vApp* wizard

- Clone a vApp

1. Within the vSphere Client select the vApp you wish to clone
2. In the top menu bar select *Inventory -> Clone* (be sure that all VM's have been powered down)
3. Select the destination for the cloned vApp. Click *Next*
4. Give the cloned vApp a name and select an inventory location. Click *Next*
5. Select a destination datastore and click *Next*
6. Select a disk format and click *Next*
7. Map the networks if necessary and click *Next*
8. Review your settings and click *Finish*

- Export a vApp

1. Within the vSphere Client select the vApp you wish to export
2. In the top menu bar select *File -> Export -> Export OVF Template*
3. The *Export OVF Template* dialog box is displayed
4. Provide a *Name, Directory* to export to, *Format*, and a *Description* if needed.
5. Click *OK* to begin the export

- **Configure IP pools**

- Specify an IP Address Range

1. In the inventory, select the datacenter that contains the vApp
2. In the IP Pools tab, right-click the IP pool that you want to edit and select *Properties*

If no IP Pools appear, click *Add* to add a new IP pool

3. In the *Properties* dialog box, select the IPv4 or the IPv6 tab, depending on your IP protocol
4. Enter the IP Subnet and Gateway in their respective fields
5. (Optional) Select the *Enable IP Pool* check box
6. (Optional) Enter a comma-separated list of hosts address ranges in the *Ranges* field
7. Click *OK*

- Select DHCP

1. In the inventory, select the datacenter that contains the vApp you are configuring
2. In the *IP Pools* tab, right-click the IP pool that you want to edit and select *Properties*

   If no IP Pools appear, click *Add* to add a new IP pool

3. In the *Properties* dialog box, select the *DHCP* tab
4. Select either the *IPv4 DHCP Present* or *IPv6 DHCP Present* check box to indicate that one of the DHCP servers is available on this network
5. Click *OK*

- Specify DNS Settings

1. In the inventory, select the datacenter that contains the vApp
2. In the IP Pools tab, right-click the IP pool that you want to edit and select *Properties*

   If no IP Pools appear, click *Add* to add a new IP Pool

3. In the *Properties* dialog box, select the *DNS* tab
4. Enter the DNS server information
5. Click *OK*

- Specify a Proxy Server

1. In the inventory, select the datacenter that contains the vApp
2. In the IP Pools tab, right-click the IP pool that you want to edit and select *Properties*

   If no IP Pools appear, click *Add* to add a new IP Pool

3. In the *Properties* dialog box, select the *Proxy* tab
4. Enter the server name and port number for the proxy server
5. Click *OK*

- Select Network Associations

1. In the inventory, select the datacenter that contains the vApp
2. In the *IP Pools* tab, right-click the IP pool that you wantt to edit and select *Properties*

If no IP Pools appear, click *Add* to add a new IP Pool

3. In the *Properties* dialog box, select the *Associations* tab
4. Select the networks that use this IP Pool
5. Click *OK*

For further information read pages 191 thru 193 of the vSphere Virtual Machine Administration documentation

- **Suspend/Resume a vApp**

  - Suspend a vApp

    1. From the vSphere Client select the vApp you want to place in suspended state
    2. Right-click the vApp and select *Suspend*

  - Resume a vApp

    1. From the vSphere Client select the vApp you want to resume
    2. Right-click the vApp and select *Power On*

- **Determine when a tiered application should be deployed as a vApp**

  If you environment has tiered applications running in virtual machines and have a dependency on specific start order (think first DB server, then application server, and finally web server) they are the ideal candidates for use in a vApp.

Tools

- vSphere Virtual Machine Administation guide

Objective 4.3 – Manage Virtual Machine Clones and Templates

Knowledge

- **Identify the vCenter Server managed ESXi hosts and Virtual Machine maximums**

Virtual Machine maximums

Item	*vSphere 5.x*	*vSphere 4.1*
Virtual CPUs per VM	32	8
RAM per VM	1TB	255GB

ESXi Host maxiums

Item	*vSphere 5.x*	*vSphere 4.1*
VMs per Host	512	320
Virtual CPUs per Host	2048	512
RAM per Host	2TB	1TB

This is a brief list of the maximums that are now available for vSphere 5. For a full listing refer to the *Configuration Maximums* document for vSphere 5.

- **Identify Cloning and Template options**

  Regardless of which deployment option you select both allow for the changing/setting of the virtual machine name, inventory location, host and cluster placement, resource pool, datastore, disk format, and finally guest OS customizations.

- **Clone an existing virtual machine**
  1. Right-click the virtual machine and select *Clone*
  2. Enter a virtual machine name, select a location, and click *Next*
  3. Select a host or cluster on which to run the new virtual machine
  4. Select a resource pool in which to run the virtual machine and click *Next*
  5. Select the datastore location where you want to store the virtual machine files
  6. Select the format for the virtual machine's disks and click *Next*
  7. Select a guest operating system customization option
  8. Review your selections and select whether to power on the virtual machine or edit virtual machine settings

For further information read pages 46 thru 47 of the *vSphere Virtual Machine Administration* guide

- **Create a template from an existing virtual machine**
  1. Right-click the virtual machine and select *Template -> Convert to Template*

- **Deploy a virtual machine from a template**
  1. Right-click the template, and select *Deploy Virtual Machine from this Template*
  2. Enter a virtual machine name, select a location, and click *Next*
  3. Select a host or cluster on which to run the new virtual machine
  4. Select a resource pool in which to run the virtual machine and click *Next*
  5. Select the datastore location where you want to store the virtual machine files
  6. Select the format for the virtual machine's disks and click *Next*

7. Select a guest operating system customization option
8. Review your selections and select whether to power on the virtual machine or edit virtual machine settings

For the complete details, refer to pages 50 thru 52 of the vSphere Virtual Machine Administration document.

- **Update existing virtual machine templates**
    1. From the vSphere Client switch to the *VMs and Templates* view
    2. Select the Template you wish to update and right click and choose *Convert to Virtual Machine*
    3. Make the need changes
    4. Power the VM down and convert back to a template (see steps above)

- **Deploy virtual appliances and/or vApps from an OVF template**
    1. In the vSphere Client, select *File -> Deploy OVF Template*
    2. Specify the source location and click *Next*
    3. View the *OVF Template Details* page and click *Next*
    4. If license agreements are packaged with the OVF template, the End User License Agreement page appears. Agree to accept the terms of the licenses and click *Next*
    5. (Optional) Edit the name and select the folder location within the inventory where the vApp will reside, and click *Next*
    6. Select the deployment configuration from the drop-down menu and click *Next*
    7. Select the host or cluster on which you want to deploy the OVF tempate and click *Next*
    8. Select the host on which you want to run the deployed OVF tempate, and click *Next*
    9. Navigate to, and select the resource pool where you want to run the OVF template and click *Next*
    10. (Optional) Apply a virtual machine storage profile from the VM Storage Profile drop-down menu
    11. Select a datastore to store the deployed OVF template, and click *Next*
    12. Select the disk format to store the virtual machined virtual disks, and click *Next*
    13. If the appliance that you are deploying has one or mover vService dependencids, select a binding service provider
    14. For each network specified in the OVF template, select a network by right-clicking the *Destination Network* column in your infrastructure to set up the network mapping and click *Next*
    15. On the *IP Allocation* page, configure how IP addresses are allocated for the virtual appliance and click *Next*
    16. Set the user-configurable properties and click *Next*
    17. Review your settings and click Finish

For further information read pages 68 thru 69 of the vSphere Virtual Machine Administration guide

- **Import and /or Export an OVF template**
    1. Select the virtual machine or vApp and select *File -> Export -> Export OVF Template*
    2. In the Export OVF Template dialog, type the *Name* of the template

3. Enter the *Directory* location where the exported virtual machine template is saved, or click "…" to browse for the location
4. In the *Format* field, determine how you want to store the files
    - Select *Folder of Files (OVF)* to store the OVF tempate as a set of files. This format is optimal if you plan to publish the OVF files on a web server or miage library. The package can be imported , for example, into the vSPhere cleint by publishing the URL to the .ovf file
    - Select *Single file (OVA)* to package the OVF template into a single .ova file. This might be convenient to distribute the OVF package as a single file if it needs to be explicitly downloaded from a web site or moved around using a USB key.
5. In *Description*, type a description for the virtual machine
6. Select the checkbox if you want to include image files attached to floppy and CD/DVD devices in the OVF package
7. Click *OK*

For further information read pages 69 thru 71 of the vSphere Virtual Machine Administration guide

- **Determine the appropriate deployment methodology for a given virtual machine application**
    - Create as needed virtual machines
    - Create a virtual machine template to quickly deploy standardized virtual machines
    - Clone an existing virtual machine to get an exact copy (or many copies) of a virtual machine
    - Use OVF (Open Virtual Machine Format) to deploy virtual machines,vApps, and virtual appliances

Tools

- vSphere Virtual Machine Administation guide
- VMware vSphere Examples and Secnarios guide
- OVF Tool User guide

Objective 4.4 – Administer Virtual Machines and vApps

Knowledge

- **Identify files used by virtual machines**

File	Usage	Description
.vmx	vmname.vmx	Virtual machine configuration file
.vmxf	vmname.vmxf	Additional virtual machine configuration files
.vmdk	vmname.vmdk	Virtual disk characteristics
-flat.vmdk	vmname-flat.vmdk	Prealocated virtual disk

.nvram	vmname.nvram or nvram	Virtual machine BIOS or EFI configuration
.vmsd	vmname.vmsd	Virtual machine snapshots
.vmsn	vmname.vmsn	Virtual machine snapshot data file
.vswp	vmname.vswp	Virtual machine swap file
.vmss	vmname.vmss	Virtual machine suspend file
.log	vmware.log	Current virtual machine log file
-#.log	vmware-#.log (where # is a number starting with 1)	Old virtual machine log entries

- **Identify locations for virtual machine configuration files and virtual disks**

  The default location for VM configuration files to be stored is a named folder (usually that of the VM) on the datastore that the VM was created(referred to as the "working directory"). There are two exceptions however. If adding an additional hard disk to a VM (VMDK or RDM) you have the ability to place these files on a different datastore. Also, you can relocate a VM's swap file to a different location. This can be controlled at the cluster, host, or VM level.

- **Identify common practices for securing virtual machines**
  - Install Antivirus Software
  - Disable copy and paste operations to the clipboard
  - Remove unnecessary hardware devices

These are just a few examples taken from pages 87 thru 89 of the *vSphere Security* documentation. For a more detailed security approach review the *vSphere Security Hardening Guide*, currently version 4.1

- **Hot Extend a virtual disk**

  Hot extending a virtual disk allows for increasing the size of an assigned VMDK file while the system is running. This is a two part process with the first step taking place via the vSphere Client and the other taking place in the guest VM which differs between guest OS'es.

  From vSphere Client

  1. Select the virtual machine you would like to extend
  2. Right click the VM and select *Edit Settings*
  3. On the *Hardware* tab select the *Hard Disk* you wish to extend
  4. In the right hand pane increase the hard disk to the new size
  5. Click *OK*

  For the second step on a Windows based VM you will either need to use DiskPart (Win2K3, Win2K, or XP) or the Disk Manager GUI (Win2K8 and up, Vista and up). Refer to VMware KB article KB1007266 for full details.

- **Configure virtual machine options**

  Virtual machine options allow for the configuration and setting of advanced features of a virtual machine. They are accessed via the *Options* tab after selecting a VM and selecting *Edit Settings*.

Virtual Machine Options

Options	Description
General Options	Display name and type of guest operating system. Location of the virtual machine and its configuration file
vApp Options	Options for functionality, product infromation, properties, and OVF settings specific to virtual appliances
VMware Tools	Power Controls behavior, VMware Tools scripts, and automatic updates
Power Management	Virtual machine Suspend behavior

Advanced Virtual Machine Options

Advanced Options	Description
General	Acceleration, logging, debugging and statistics
CPUID Mask	NX flag and advanced identifciation mask options
Memory/CPU Hotplug	Hot add enablement for individual virtual machines
Boot Options	Virtual machine boot options. Add a delay before booting or force entry into the BIOS or EFI setup screen
Fibre Channel NPIV	Virtual node and port World Wide Names (WWNs)
CPU/MMU Virtualization	Settings for enabling Hardware Page Tabe Virtualization. In some new processors, controls the use of hardware support for virtual MMUs
Swapfile Location	Swapfile location
SDRS Rules	Set affinity rules for virtual disks within a datastore cluster

Chart from page 80 of the *vSphere Virtual Machine Administration* docuement

- **Configure virtual machine power settings**

1. In the vSphere Client inventory, right-click the virtual machine and select *Edit Settings*
2. Click the *Options* tab and select *Power Management*
3. In the *Guest Power Management* panel, select a power option
    - *Suspend the virtual machine*
    - *Put the guest operating system in standby mode and leave the virtual machine powered on*
4. (Optional) Select *Wake on LAN for virtual machine traffic on* and select the virtual NICs to trigger this action.
5. Click *OK* to saver your changes and close the dialog box

See pages 170 thru 171 of the *vSphere Virtual Machine Administration* documentation for further details

- **Configure virtual machine boot options**
    1. In the vSphere Client inventory, right-click the virtual machine and select *Edit Settings*
    2. Click the *Options* tab and under Advanced select *Boot Options*
    3. In the *Power on Boot Delay* panel, select the time in millieseconds to delay the boot operation
    4. (Optional) Select whether to force entry into the BIOS or EFI setup screen the next time the virtual machine boots
    5. (Optional) Select whether to try to reboot after a boot failure
    6. Click *OK* to save your changes and close the dialog box

See pages 173 thru 174 of the *vSphere Virtual Machine Administration* documentation for further details

- **Configure virtual machine troubleshooting options**

    Enable Virtual Machine Logging

    1. In the vSphere Client inventory, right-click the virtual machine and select *Edit Settings*
    2. Click the *Options* tab and select *Advanced -> General*
    3. In the *Settings* pane, select *Enable logging*

    Configure Debugging and Statistics

    1. In the vSphere Client inventory, right-click the virtual machine and select *Edit Settings*
    2. To enable debugging mode, select an option from the *Debugging and Statistics* section

Option	Description
Run Normally	Collects debugging information
Record debugging information	Collects debugging and performance information

See pages 174 and 176 of the *vSphere Virtual Machine Administration* documentation for further details

- **Assign a Storage Policy to a virtual machine**
- **Verify Storage Policy compliance for virtual machines**
    1. Open the Profiles tab of a virtual machine
        - Right-click a virtual machine and select *Edit Settings*, select the *Profiles* tab
        - Right-click a virtual machine and select *VM Storage Profile -> Manage Profiles*
    2. Associate the virtual machine home files with a virtual machine storage profile from the *Home VM Storage Profile* drop-down menu
    3. (Optional) Click *Propagate to disks* to associate all virtual disks with the same virtual machine storage profile
    4. Under VM storage profiles for virtual disks, associate each virtual disk with a different virtual machine storage profile from the *VM Storage Profile* drop-down menu
    5. Click *OK*

See pages 131 and 132 of the *vSphere Virtual Machine Administration* documentation for further details

- **Determine when an advanced virtual machine parameter is required**

  Advanced settings can be added to a virtual machines .vmx file manually. The VM in question needs to be powered off to do so. However, most of the advanced options/features that are needed (NPIV, Swapfile location, etc) are configured via the Options tab and radial buttons. To add options manually select the *Options* tab, *Advanced, General* and click *Configuration Parameters*. This will open the *Configuration Parameters* window allowing you to add additional configurations to the .vmx file.

- **Adjust virtual machine resources (shares, limits and reservations) based on virtual machine workloads**
    1. In the vSphere Client inventory, right-click the virtual machine and select *Edit Settings*
    2. Click the *Resources* tab
    3. From the Resources tab you can set Shares, Reservations and Limits for CPU, Memory, Disk as well as Hyperthreaded Core Sharing

See pages 88, 100, and 121 of the *vSphere Virtual Machine Administration* documentation for further details

<u>Tools</u>

- vSphere Virtual Machine Administation guide

Section 5 – Establish and Maintain Service Levels

Objective 5.1 – Create and Configure VMware Clusters

Knowledge

- **Describe DRS virtual machine entitlement**
  - DRS will calculate CPU and memory entitlements for virtual machines. The host-local schedulers are actually responsible for supplying those resources to virtual machines and therefore also calculate CPU and memory entitlements for the virtual machines that reside on it. There are two types of entitlements, static and dynamic entitlement.
    - Static Entitlement
      - Static entitlement is user-defined
      - Defined by resource shares, limits and reservations
        - Shares: are proportional and are weighted against other running virtual machines when contention occurs
        - Limits: are the maximum amount of resource a virtual machine or resource pool can use, think of this as the max value
        - Reservations: are the minimum amount of resources a virtual machine or resource pool is entitled to. Memory entitlement backed by a reservation cannot be reclaimed even if it is not being used. CPU entitlement can be "loaned out" to other virtual machines if it is not being used
    - Dynamic Entitlement
      - Dynamic entitlement is calculated by the DRS cluster and by the host-local schedulers, specifically the host-local CPU scheduler and the host-local memory scheduler. Dynamic entitlement is flexible and will increase/decrease based on virtual machine demand, but will never increase passed its configured CPU/Memory size
        - CPU Entitlement
          - Based on the Active CPU, which is taken from %Run + %Ready MHz metrics of that virtual machine
        - Memory Entitlement – the three items below makeup memory entitlement (working set, memory overhead and 25% of idle memory)
          - Based on Active Memory; the working memory set of the virtual machine (actual physical RAM pages)
          - Includes memory overhead (this number varies)
          - Includes 25% of the idle memory
- **Create/Delete a DRS/HA Cluster**
  - Create a DRS/HA Cluster

1. Log in to vCenter using the VI Client
2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
3. Right-click on the vDatacenter you want to create your DRS cluster in and select *New Cluster* (or *Ctr+L*)
4. Type in a name for the cluster in the *Name* field

5. Check the *Turn On vSphere* HA and *Turn on vSphere DRS* > click *Next*
6. Choose an automation level (*Manual*, *Partially automated* or *Fully automated*) > click *Next*
7. Decide if you want to enable Power Management (DPM), set to *Off*, *Manual* or *Automatic* > click *Next*
8. *Enable Host Monitoring* is checked by default; this enables heartbeats between the hosts
9. Choose whether to enable or disable Admission Control (enabled by default)
10. If you chose to enable Admission Control (recommended) choose an admission control policy:
    - *Host failures the cluster tolerates* (specify number of hosts)
    - *Percentage of cluster resources reserved as failover spare capacity* (choose a percentage for both CPU and Memory)
    - *Specify failover hosts* (designate hosts to use only in case of failover)
11. Click *Next*
12. Set the *VM restart priority* (Disabled, Low, Medium and high)
13. Set the *Host Isolation response* (Leaved powered on, Power off and Shut down)
14. Click *Next*
15. Choose whether to enable *VM Monitoring* (requires VMware Tools to be installed)
16. Use the slider to choose the *Monitoring Sensitivity*
17. Click *Next*
18. Enable Enhanced vMotion Compatability (*EVC*) or leave it disabled > click *Next*
19. Choose the *Swapfile Policy for Virtual Machines*; store in same directory as virtual machine or let the host choose a datastore > click *Next*
20. Click *Finish*

- Delete a DRS/HA Cluster

1. Log in to vCenter using the VI Client
2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
3. Right-click on the DRS/HA cluster you want to delete and select *Remove*
4. Click *Yes* to confirm the removal operation

- **Add/Remove ESXi hosts from a DRS/HA Cluster**
  - There are a few ways to add a host to a DRS/HA Cluster. If you already have a host added to vCenter, but not part of a DRS/HA Cluster you can simply drag-and-drop the host into the cluster and specify the resource pool you want to use. You can put all the virtual machines in the cluster's root resource pool, or create a new resource pool utilizing the hosts existing resource pool

  - Add a new ESXi host to a DRS/HA Cluster

1. Log in to vCenter using the VI Client
2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
3. Right-click on the cluster you want to add a new host to
4. Click *Add Host*
5. Enter in the hostname or IP address in the *Host* field
6. Enter in an administrative username/password > click *Next*
7. If prompted, click *Yes* to accept the certificate of the unverified host
8. Click *Next*
9. Assign an existing product key or assign a new key for the host > click *Next*
10. If you want to enable Lockdown Mode select the *Enable Lockdown Mode* check box > click *Next*
11. Choose whether to use the cluster's root resource pool or create a new resource pool based off the hosts resource pool > click *Next*
12. Click *Finish*

- Remove an ESXi host from a DRS/HA Cluster

13. Log in to vCenter using the VI Client
14. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
15. Right-click on host you want to remove and select *Enter Maintenance Mode*
16. Remove the host
    - To remove the host only from the cluster, you can drag the host out of the cluster and drop it into the vDatacenter
    - If you want to completely remove it from vCenter, right-click the host and select *Remove* > click *Yes* to confirm removal of the host

- **Add/Remove virtual machines from a DRS/HA Cluster**
  - There are three ways to add a virtual machine to a DRS/HA Cluster and two ways to remove them

  - Add virtual machines to a DRS/HA Cluster

1. Anytime you add a host to a DRS/HA cluster all virtual machines that are registered on that host will be added to the DRS/HA cluster
2. Whenever you create a new virtual machine the wizard asks you whether you want to place it on a DRS/HA cluster or a standalone host
3. vMotioning a virtual machine will allow you to add it to a DRS/HA cluster either from a standalone host or another DRS/HA cluster

  - Remove virtual machines to a DRS/HA Cluster

1. When you remove a host from a DRS/HA cluster all of the powered-off virtual machines that are still registered on the host will be removed as well. Because you have to be the host in maintenance mode prior to removing it, powered-on virtual machines will have already been migrated to another host or powered off
2. You can vMotion a virtual machine from a host in a DRS/HA cluster to a standalone host

- **Configure Storage DRS**
  - You configure Storage DRS globally for a datastore cluster, and then you can manually disable on a per virtual machine level if needed

  - Configure Storage DRS

1. Log in to vCenter using the VI Client
2. Navigate to the *Datastores and Datastore Clusters* view (*View* > *Inventory* > *Datstores and Datastore Clusters* or *Ctrl+Shift+D*)
3. Right-click on the vDatacenter you want to create your datastore cluster in and select *New Datastore Cluster…*
4. Enter in a name in the *Datastore Cluster Name* field
5. Ensure the *Turn on Storage DRS* checkbox is checked > click *Next*
6. Choose the automation level that you want to use, either *No Automation (Manual Mode)* or *Fully Automated*
7. Click the *Advanced Options* button if you need to input any advanced options
8. Once complete click *Next*
9. To include I/O metrics in SDRS recommendations select the *Enable I/O metric for SDRS recommendations*
10. Set your Storage DRS Thresholds; *Utilized Space* (default is 80%) and *I/O Latency* (default is 15ms)
11. Click the *Show Advanced Options* hyperlink to set advanced options
    - Use the slider to set the utilization difference between the source and destination hosts before SDRS will make a recommendation (default is 5%)
    - Set frequency for which you want vSphere to check for imbalances (default is 8 hours)
    - Set the I/O imbalance threshold using the slider; this setting determins how much imbalance SDRS will allow before making recommendations
12. Click *Next*
13. Using the checkboxes select the host(s)/cluster(s) you want to add to this particular Datastore Cluster > click *Next*
14. Select the datastores you want to add to the Datastore Cluster > click *Next*
15. Review all your settings and click *Finish*

- When creating a new virtual machine you can disable SDRS when you select the datastore cluster for the virtual hard disk locations. If you leave it enabled, at the very end of the wizard you can check an option that will show you SDRS recommendations, which will recommend initial placement of the virtual hard disks and configuration file (must be stored together) and you can then apply that recommendation(s)
- Once you have virtual machines created and living on a datastore cluster you can configure SDRS rules (Intra VM Affinity rule) on a per virtual machine basis
- You can create a scheduled task to change SDRS settings during off-hours. You would want to do this in order to automatically rebalance your datastore cluster while users are out of the office and the impact is negligible

- Create SDRS Scheduled Task

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Datastores and Datastore Clusters* view (*View* > *Inventory* > *Datstores and Datastore Clusters* or *Ctrl+Shift+D*)
    3. Right-click on the datastore cluster you want to schedule > click *Edit Settings…*
    4. Choose *SDRS Scheduling* from the left menu
    5. Click the *Add* button
    6. Choose a *Start* and *End* time and the *Frequency* (days of the week) in which you want it to run > click *Next*
    7. Configure your Start Settings; enter in a *Description*
    8. Choose which Automation level you want to start when the start date/time begins
    9. Select whether you want to enable the I/O metric for SDRS recommendations
    10. Use the sliders to configure utilized space and I/O imbalance threshold
    11. Click *Next*
    12. Configure your End Settings; enter in a *Description*
    13. By default you can use the *Restore settings to the original configuration* or you can uncheck that option and configure the options described in steps 8-10
    14. Click *Next*
    15. Click *Finish*

- You can also set VMDK and VM anti-affinity rules as well as default Virtual Machine settings (default is *Full Automated* and *Keep VMDKs together* in the Datastore Cluster settings

- **Configure Enhanced vMotion Compatibility**
    - Configuring Enhanced vMotion Compatibility (EVC)

        1. Log in to vCenter using the VI Client
        2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
        3. Right-click on the DRS/HA cluster you want to enable EVC on and select *Edit Settings…*

4. From the menu on the left select *VMware EVC*
5. Click *Change EVC Mode…*
6. Choose *Enable EVC for AMD Hosts* or *Enable EVC for Intel Hosts*
7. For AMD Hosts select one of the following:
    - *AMD Opteron Generation 1*
    - *AMD Opteron Generation 2*
    - *AMD Opteron Fen. 3 (no 3DNow!)*
    - *AMD Opteron Generation 3*
    - *AMD Opteron Generation 4*
8. For Intel Hosts select one of the following options
    - *Intel "Merom" Gen. (Xeon Core 2)*
    - *Intel "Penryn" Gen. (Xeon 45nm Core 2)*
    - *Intel "Nehalem" Gen. (Xeon Core i7)*
    - *Intel "Westmere" Gen. (Xeon 32nm Core i7*
    - *Intel "Sandy Bridge" Generation*
9. Click *OK* twice

- **Monitor a DRS/HA Cluster**
    - There are multiple ways that you can monitor a DRS/HA cluster when connected to vCenter via the VI Client. There are a number of pre-defined alarms for different HA events that will trigger based on default thresholds (there are no pre-defined alarms for DRS specifically)
    - You can look at DRS Recommendations, Faults and History through the DRS tab
        - When logged into vCenter go to the Hosts and Cluster view and select the Cluster that you want to monitor, in the right pane click on the DRS tab
    - On the summary page you can view a summary of vSphere HA and vSphere DRS along with some advanced items

    - Monitor a DRS/HA Cluster from the Summary tab

        1. Log in to vCenter using the VI Client
        2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
        3. Select the DRS/HA cluster you want to monitor
        4. On the right, click on the *Summary* tab
        5. *vSphere HA* pane
            - You can view the status of the following items:
                - *Admmission Control* – enabled or disabled
                - *Current Failover Capacity* – how many hosts are available for failover
                - *Configured Failover Capacity* – items listed here will be different depending upon the Admission control policy you are using
                - *Host Monitoring* – enabled or disabled
                - *VM Monitoring* – enabled or disabled
                - *Application Monitoring* – enabled or disabled

- To view the HA Cluster Status click on the *Cluster Status* hyperlink
  - Here you are presented with three tabs, hosts, VMs and Heartbeat Datastores. These tabs are all read-only
- To view any HA configuration issues click on the *Configuration Issues* hyperlink
  - Here you are listed with configuration issues, if any, for HA
  - Cluster validity can also be visibly noticed when there is an issue, it will be marked as red if its invalid when the failover requirements are exceeded by the number of powered-on VMs

6. *vSphere DRS* pane
   - You can view the status of the following items:
     - *Migration Automation Level* – fully automated, partially automated or disabled
     - *Power Manangement Automation Level* – off, manual or automatic
     - *DRS Recommendations* – number of DRS recommendations
     - *DRS Faults* – number of DRS faults
     - *Migration Thresholds* – lists setting you are using for priority 1-5 recommendations
     - *Target host load standard deviation* – what the host load standard deviation SHOULD be
     - *Current host load standard deviation* – what the host load standard deviation is as of the last DRS invocation (default is 5 minutes)
   - Click the *View Resource Distribution Chart* to look at CPU/Memory utilizations per host

- Monitor a HA Cluster using pre-defined vCenter Alarms

1. Log in to vCenter using the VI Client
2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
3. Select the vCenter object (this is the topmost object in the tree)
4. Click the *Alarms* tab on the right
5. Click the *Definitions* button at the top
6. Here are a list of the seven pre-defined HA alarms for vCenter
   - Insufficient vSphere HA failover resources
   - vSphere HA failover in progress
   - Cannot find vSphere HA master agent
   - vSphere HA host status
   - vSphere HA virtual machine failover failed
   - vSphere HA virtual machine monitoring action
   - vSphere HA virtual machine monitoring error
7. Right-click each alarm listed above and select *Edit Settings* in order to view the triggers, reporting, and actions for the alarm. Here you can also add or remove triggers, enable reporting, and define actions to take when the alarm is invoked

- If desired, you can also create your own alarms

- **Configure migration thresholds for DRS and virtual machines**
  - Migration thresholds are typically setup when creating a DRS cluster, but they can be modified if needed, and here is how to do it

  - Configure Migration Threshold on DRS Cluster

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Right-click on the DRS/HA cluster you want to edit and select *Edit Settings…*
    4. Select *vSphere DRS* from the menu on the left
    5. Choose the desired migration threshold from the five different settings using the slider in the right-hand pane located under *Fully Automated*. Here are the different settings, from left-to-right:
       - Apply only priority 1 recommendations – vCenter only applies recommendations to satisfy cluster constraints
       - Apply priority 1 and priority 2 recommendations – vCenter applies recommendations that promise significant improvement to the cluster
       - Apply priority 1, priority 2 recommendations and priority 3 recommendations -- vCenter applies recommendations that promise good improvement to the cluster
       - Apply priority 1, priority 2 recommendations, priority 3 and priority 4 recommendations -- vCenter applies recommendations that promise moderate improvement to the cluster
       - Apply all recommendations -- vCenter applies recommendations that promise slight improvement to the cluster
    6. Click *OK* or *Cancel* when complete

- **Configure automation levels for DRS and virtual machines**
  - DRS automation levels can be set on the DRS cluster (global for that particular DRS cluster) and can be set on individual virtual machines. Setting DRS automation levels on a virtual machine will override the automation level that is set on the DRS cluster for that virtual machine

  - Setting DRS Automation Level on a DRS Cluster – normally done when creating DRS Cluster

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Right-click on the DRS/HA cluster you want to edit and select *Edit Settings…*
    4. Select *vSphere DRS* from the menu on the left
    5. Choose the desired automation level from the right- hand pane

6. Click *OK* or *Cancel* when finished

- Setting DRS Automation Level on a Virtual Machine

1. Log in to vCenter using the VI Client
2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
3. Right-click on the DRS/HA cluster you want to edit and select *Edit Settings…*
4. Select *Virtual Machine Options* from the menu on the left
5. Select the *Enable individual virtual machine automation levels* checkbox
6. The window below will display the lists of virtual machines and you can modify their automation level by clicking on the current set automation level and click the down arrow. Select from the following options:
    a. Fully Automated
    b. Partially Automated
    c. Manual
    d. Default – this is listed as what's configured globally for that DRS Cluster
    e. Disabled
7. Click *OK* or *Cancel* when finished

- **Create VM-Host and VM-VM affinity rules**
  - As you may have gathered from the topic title, there are two types of affinity rules that you can create; VM-VM affinity rules and VM-Host affinity rules
  - Within these two types of rules you can either specify them as affinity (together) or anti-affinity (separate)
  - VM-VM affinity rules – used to ensure certain virtual machines run on the same host or do not run on the same host

  - Creating a VM-VM Affinity Rule

1. Log in to vCenter using the VI Client
2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
3. Right-click on the DRS/HA cluster you want to edit and select *Edit Settings…*
4. Under *vSphere DRS* select the *Rules* option
5. Click the *Add* button
6. Type a name for the new rule in the *Name* field (try and be descriptive)
7. From the Type dropdown choose either *Keep Virtual Machines Together* or *Separate Virtual Machines*
8. Click the *Add* button
9. Select two or more virtual machines that you want to incorporate in the affinity rule > click *OK*
10. Click *OK* twice

- VM-Host affinity rules – used to keep virtual machines running on a particular host(s) or to ensure virtual machines DO NOT run on particular host(s). Before you can create a VM-Host affinity rules cannot be created until you create Virtual Machine DRS Groups and Host DRS Groups

- Creating a VM-Host Affinity Rule

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Right-click on the DRS/HA cluster you want to edit and select *Edit Settings…*
    4. Under *vSphere* DRS select *DRS Groups Manager* option
    5. Under the Virtual Machines DRS Groups click *Add*
    6. Enter in a descriptive *Name*
    7. Select virtual machine(s) you want to use in your VM-Host affinity rule from the left pane and move them to the right pane > click *OK*
    8. Under the Host DRS Groups click *Add*
    9. Enter in a descriptive *Name*
    10. Select host(s) you want to use in your VM-Host affinity rule from the left pane and move them to the right pane > click *OK*
    11. Under *vSphere DRS* select the *Rules* option
    12. Click *Add*
    13. Enter a descriptive *Name*
    14. In the Type dropdown select *Virtual Machines to Hosts*
    15. Choose which virtual machine group you want to use from the *Cluster Vm Group* dropdown
    16. Select which type of affinity you want for this rule from the dropdown, options are:
        - Must run on hosts in group
        - Should run on hosts in group
        - Must Not run on hosts in group
        - Should Not run on hosts in group
    17. Click *OK* when finished
    18. Click *OK*

- **Enable/Disable Host Monitoring**
    - Enabling/Disabling host monitoring is straight forward and it allows each of the ESXi hosts within the cluster to send heartbeats over the network between each other; here is how to do it

        1. Log in to vCenter using the VI Client
        2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
        3. Right-click on the DRS/HA cluster you want to edit and select *Edit Settings…*
        4. Click on *vSphere HA*

5. In the right-pane select or deselect the *Enable Host Monitoring* checkbox to enable or disabled host monitoring, respectively
6. Click *OK* or *Cancel* when finished

- **Enable/Configure/Disable virtual machine and application monitoring**
  - VM Monitoring will restart virtual machines if the heartbeats sent to VMware tools within the guest aren't responding or received within a set time.
  - Application monitoring will restart a virtual machine if the VMware tools APPLICATION heartbeats aren't responding or received within a set time

  - Enable/Disable/Configure VM Monitoring and Application Monitoring

1. Log in to vCenter using the VI Client
2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
3. Right-click on the DRS/HA cluster you want to edit and select *Edit Settings…*
4. Under *vSphere HA* select the *VM Monitoring* option
5. Choose which level of monitoring you want to perform, either *VM Monitoring Only* or *VM and Application Monitoring*
6. Below that you can set the Monitoring sensitivity using a slider, there are four different settings:
   - *Low* – vSphere HA restarts the VM after no heartbeats are received within 2 minutes. HA will restart the VM after each failure, but only up to 3 failures within a 7 day period
   - *Medium* -- vSphere HA restarts the VM after no heartbeats are received within 60 seconds. HA will restart the VM after each failure, but only up to 3 failures within a 24 hour period
   - *High* -- vSphere HA restarts the VM after no heartbeats are received within 30 seconds. HA will restart the VM after each failure, but only up to 3 failures within a 60 minute period
   - *Custom* (click the checkbox) – from here you can specify your own values:
     - Failure Interval (in seconds)
     - Minimum uptime (in seconds)
     - Maximum per-VM resets
     - Maximum resets time window – set to no window or specify time in hours
7. You can also change all of the settings above on a per-virtual machine basis by selecting the different options from the drop downs under *Virtual Machine Settings* in the VM Monitoring column and Application Monitoring column
8. Click *OK* or *Cancel* when finished

- **Configure admission control for HA and virtual machines**
  - I'm not going to cover how each of the admission control policies work, but I will walk you through enable/disabling and picking an admission control policy

- Configure Admission control

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Right-click on the DRS/HA cluster you want to edit and select *Edit Settings…*
    4. Click on *vSphere HA*
    5. Under Admission Control in the right-pane select *Enable* or *Disable*
    6. If you select *Enable* you will need to select an admission control policy, select from the following:
        - Host failures the cluster tolerates – specify number of hosts
        - Percentage of cluster resources reserved as failover spare capacity
            - Specify a percentage for CPU and a percentage for Memory
        - Specify failover hosts – click the *Click to edit* hyperlink to choose which hosts you want to reserve for failover purposes
    7. Click *OK* or *Cancel* when complete

- **Determine appropriate failover methodology and required resources for an HA implementation**
    - Determining which failover methodology and required resources are appropriate for vSphere HA will always depend on the environment and availability requirements of the organization. Even if you aren't using admission control, I can't think of a single reason NOT to enable HA
    - Determining your required resources and the failover methodology go hand-in-hand with each other. You need to look at the availability requirements, determine what resources you have to meet those requirements and then determine the best methodology. In some cases you may need to allocate more resources or manage expectations with stake holders
    - There is no right answer that applies to every situation, but here are my suggestions when attempting to determine failover methodology and required resources to support that methodology
        - Know your availability requirements – this will be the foundation for making a proper determination
        - Identify which failover methodology meets those availability requirements and the pros/cons for that methodology
        - Ensure you have enough resources to sustain the failover methodology you chose based on requirements. If you determine *Specify failover hosts* is the right policy, do you have idle hosts you can allocate? If you want to use the *Percentage* policy (general best practice as it's the most flexible), what percentage for CPU and Memory is free to handle your availability requirement?
    - I believe you can use the logical formula above to come up with a successful failover methodology, or you can come up with your own.

<u>Tools</u>

- vCenter Server and Host Management guide

- vSphere Availability guide
- vSphere Resource Management guide

Objective 5.2 – Plan and Implement VMware Fault Tolerance

Knowledge

- **Identify VMware Fault Tolerance requirements**
  - Figuring out VMware Fault Tolerance requirements can be a bit cumbersome, especially when browsing through all the different CPUs and their combinations. VMware has a tool called SiteSurvey (http://www.vmware.com/download/shared_utilities.html) that you can install and run and it will tell you if your hardware/software is compatible with VMware Fault Tolerance
  - VMware Fault Tolerance uses VMware's vLockstep technology which requires extensions in the physical processor that are only present in todays' (relative) processors
  - Here are some basic requirements that the SiteSurvey utility checks for
    - *CPU Compatibility* – a host must have an FT capable processor; use the SiteSurvey help page (http://www.vmware.com/support/sitesurvey/help_2_5_3.html#install) to determine FT capable processors. Both hosts that are hosting the FT virtual machines must have processors in the same processor family and the CPU speeds between the two hosts shouldn't be different more than 400Mhz +/-
    - ESXi hosts hosting FT virtual machines must be running the same version and build number
    - Hardware virtualization must be enabled in the BIOS
    - Each host participating in the Fault Tolerance cluster must have at least two physical NICs with speeds of at least 1Gbps or greater
    - Two virtual NICs, one for vMotion and one for FT logging must be present on each host in the FT cluster
    - The location of the protected virtual machine(s) must be on shared storage and that storage accessible to hosts in the FT cluster
    - Virtual machines protected by Fault Tolerance cannot have more than one vCPU
    - Thin-provisioned disks on virtual machines protected by Fault Tolerance are not supported. Thin-provisioned disks are automatically converted when FT is enabled, however, the VM needs to be in a powered-off state
    - Snapshots are not supported for FT virtual machines, which also means no snapshots can be present when you enable FT
    - Physical RDMs are not supported on virtual machines protected by FT
    - N_Port ID Virtualization (NPIV) is not supported with FT as well as paravirtualized guests
    - CD-ROMs and/or Floppy drives backed by a remote or physical device are also not supported by FT

- Vmxnet2 virtual NICs and physical NIC pass-through is not supported by FT

- **Configure VMware Fault Tolerance networking**
  - At a minimum you need at least two physical NICs for Fault Tolerance networking; one for FT Logging and one for vMotion, you should also create a vSwitch for each
  - Each NIC must be on a different IP subnet
  - Add additional NICs to add redundancy and connect the redundant NICs to separate physical switches so you have physical switch redundancy

  - Configure Networking for Fault Tolerance Logging (do this for each host)

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Select the host on the left side > click the *Configuration* tab on the right
    4. Click the *Networking* hyperlink
    5. Find the vSwitch you will use for FT Logging and click the *Properties* hyperlink above it (slightly to the right)
    6. Click the *Add…* button > select *VMkernel* > click *Next*
    7. Give it a descriptive name in the *Network Label* field
    8. Input a VLAN if necessary
    9. Check the *Use this port group for Fault Tolerance Logging* > click *Next*
    10. Enter in the *IP address* and *Subnet* mask you want to use > click *Next*
    11. Click *Finish*
    12. Click *Close* to close the vSwitch properties dialog
    13. Repeat on the second host (make sure you use a different IP!!)

  - Configure Networking for vMotion (do this for each host)

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Select the host on the left side > click the *Configuration* tab on the right
    4. Click the *Networking* hyperlink
    5. Find the vSwitch you will use for vMotion and click the *Properties* hyperlink above it (slightly to the right)
    6. Click the *Add…* button > select *VMkernel* > click *Next*
    7. Give it a descriptive name in the *Network Label* field
    8. Input a VLAN if necessary
    9. Check the *Use this port group for vMotion* > click *Next*
    10. Enter in the *IP address* and *Subnet* mask you want to use > click *Next*
    11. Click *Finish*
    12. Click *Close* to close the vSwitch properties dialog
    13. Repeat on the second host (make sure you use a different IP!!)

- **Enable/Disable VMware Fault Tolerance on a virtual machine**
  - Whenever you enable Fault Tolerance on a virtual machine any limits and reservations are discarded and a new reservation is set to whatever the configured memory about is for that virtual machine. None of these options can be changed while Fault Tolerance is enabled for that virtual machine
  - When you disable Fault Tolerance on a virtual machine, any changes that were made to the limit, reservation or shares are not reverted back to what they were prior to Fault Tolerance being enabled
  - VMware HA is required to be enabled on the cluster your Fault Tolerant hosts are in otherwise you will get an error telling you HA is not enabled on the cluster when trying to enable fault tolerance on a virtual machine

  - Enable Fault Tolerance on a Virtual Machine (for most Windows Guest Operating systems FT can only be enabled while powered-on if your physical host is running an Intel Xeon Penryn processor)

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Right-click on the virtual machine you want to enable fault tolerance on > select *Fault Tolerance* > click *Turn On Fault Tolerance*
    4. Answer *Yes* to the question about changing the memory reservation to the configured memory size of the VM (if you are using a thin provisioned disk there were also be a warning that all unused blocks will be zeroed out and that it may require more processing time)
    5. Monitor the *Recent Tasks* pane to see when the task is complete, the VM icon for the newly protected VM will change to a dark blue and a new VM will show up on the secondary host with the same name as the primary VM with a *(secondary)* at the end of the name

  - Disable Fault Tolerance on a Virtual Machine

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Right-click on the virtual machine you want to enable fault tolerance on > select *Fault Tolerance* > click *Turn Off Fault Tolerance*
    4. Answer *Yes* to the question asking you if you are sure you want to disable fault tolerance
    5. Monitor the *Recent Tasks* pane to see when the task is complete. The VM icon will revert back to a light blue

- **Test an FT configuration**
  - There are plenty of ways to test out an FT configuration. You can power off the host that is hosting the primary or secondary or you can manually move to the secondary. For the purposes of the blueprint I will focus on manually moving the primary to the secondary
    - The first thing I tested was migrating the secondary FT virtual machine to the same host as the primary virtual machine. I started going through the wizard and when I selected the same host that the primary FT virtual machine was running on I get a validation error: "*Virtual machines in the same Fault Tolerance pair cannot be on the same host*"
  - Now, VMware provides two of its own test that you can perform within the vSphere client; Test Failover and Test Restart Secondary. Let's go through those now:
  - Test Failover

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Right-click on the virtual machine you want to test failover on > select *Fault Tolerance* > click *Test Failover*

    - What happens now is that the secondary virtual machine becomes primary and the primary machine gets removed. A new secondary virtual machine is now created and synced up with the primary, the final step is it will be powered on. This is the only time in which the primary virtual machine is unprotected, and this can be seen by the alert that gets displayed for the primary virtual machine. Once the primary virtual machine is protected the alert goes away

  - Test Restart Secondary

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Right-click on the virtual machine you want to test failover on > select *Fault Tolerance* > click *Test Restart Secondary*

    - As you might imagine the secondary virtual machine gets restarted.

- **Determine use case for enabling VMware Fault Tolerance on a virtual machine**
  - Fault Tolerance is all about availability and uptime. Availability and uptime and generally determined by business requirements, which is the driving force behind most design decisions
  - Here are some broad use cases for VMware Fault Tolerance
    - Applications that require 100& uptime
    - Applications that aren't cluster-aware and need to have high availability
    - Applications that might be cluster-aware but you don't have the in-house experience to implement a cluster solution

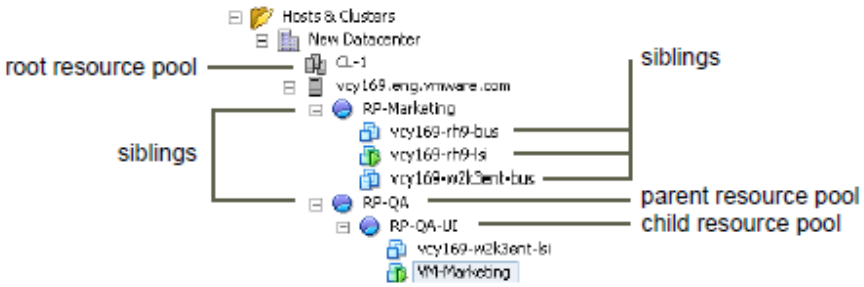
Tools

- vSphere Availability guide

Objective 5.3 – Create and Administer Resource Pools

Knowledge

- **Describe the Resource Pool hierarchy**
  - A resource pool is a pool of resources….if only that was all there was to it. The hierarchy of resource pools, whether talking about a standalone host or a cluster, starts at the root resource pool. The root resource pool exists for every standalone host and DRS cluster and is not something you can see within vCenter. By default, all resources for a host or cluster will exist in the root resource pool.
  - In the resource pool hierarchy there are three types of objects; parent resource pool, siblings and a child resource pool, with the root resource pool being *the* parent resource pool
  - Here is a graphical depiction of the resource pool hierarchy taken from chapter 8 of the vSphere Resource Management Guide:



  - The first resource pool created under the root resource pool is a child resource pool (let's call this RP1). RP1 is a child only to the root resource pool. Underneath RP1 you can add virtual machines into it, and those virtual machines will get their resources from RP1 dependent upon their shares, limits, reservations or dynamic virtual machine entitlement. A new resource pool can be added to RP1 (let's call this new resource pool RP2). RP2 is now a child resource pool of RP1, making RP1 a parent to RP2, but still a child resource pool of the root resource pool
  - The parent/child relationship can continue further as you nest more resource pools and virtual machines inside one another. Any resource pool or virtual machines created at the same level as another resource pool will be known to each other as a sibling
  - The more nesting of virtual machines and resource pools you have the more complex it will be to understand and more overhead to manage. One KEY things to remember; never use resource pools as an organizational tool, meaning don't use it as a way to logically group virtual machines (use folders for this)

- **Define the Expandable Reservation parameter**
  - When you enable the expandable reservation parameter it allows a child resource pool to asks its direct parent resource pool to borrow resources. If the child resource runs out of resources, it is possible to still provide resources to its child pools or virtual machines by asking its parent resource pool. Borrowing resources is recursive, meaning, if the child asks a parent, and the parent doesn't have any, then that parent will asks its parent to borrow resources if the expandable resource parameter is set to enable.
  - That explanation can definitely get confusing, but just know that the expandable reservation allows a child resource pool to asks its parent for more should the child need it, and it is a recursive question if the parent resource pools going up the hierarchy have the expandable parameter set to true

- **Create/Remove a Resource Pool**
  - Let's create a resource pool under a cluster that only has the root resource pool (the cluster itself is the root resource pool)
  - Create a Resource Pool

1. Log in to vCenter using the VI Client
2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
3. Right-click on the DRS cluster you want to create the resource pool in and select *New Resource Pool…* -- if you don't see this option then you must enable DRS for this cluster
4. Enter in a descriptive name for the resource pool in the *Name* field
5. Allocate CPU resources
   - Allocate CPU shares for the resource pool: shares are only relative to siblings that share the same parent resource pool
     - Low
     - Normal
     - High
     - Custom – set the number of shares
   - Use the slider to set a CPU reservation for the resource pool
     - Is represented in MHz
     - Represents the minimum amount of CPU resources this resource pool should have
   - Choose whether to enable/disable expandable reservations by checking/unchecking the *Expandable Reservation* checkbox
   - Enable/disable maximum CPU resources by checking/unchecking the *Unlimited* checkbox. If disabled, set a maximum for CPU resources this resource pool is allowed to have represented in MHz
6. Allocate Memory Resources
   - Allocate memory shares for the resource pool: shares are only relative to siblings that share the same parent resource pool
     - Low

        - Normal
        - High
        - Custom – set the number of shares
    - Use the slider to set a memory reservation for the resource pool
        - Is represented in MB
        - Represents the minimum amount of CPU resources this resource pool should have
    - Choose whether to enable/disable expandable reservations by checking/unchecking the *Expandable Reservation* checkbox
    - Enable/disable maximum CPU resources by checking/unchecking the *Unlimited* checkbox. If disabled, set a maximum for CPU resources this resource pool is allowed to have represented in MHz
7. Click *OK* when finished

- Remove a Resource Pool

1. Log in to vCenter using the VI Client
2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
3. Right-click on the resource pool you want to remove and select *Remove*
4. Click *Yes* to confirm the removal operation

- **Configure Resource Pool attributes**
    - Configuring attributes for a resource pool means changing the same attributes you configured when creating the resource pool. The attributes you can change are: the resource pool name, CPU and Memory share, CPU and Memory reservations, CPU and Memory limits and set CPU and Memory expandable reservations. Here is how to do it:

    - Configuring Resource Pool Attributes

1. Log in to vCenter using the VI Client
2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
3. Right-click on the resource pool you want to edit and select *Edit Settings…*
4. Change the name if desired
5. Change the CPU *Shares*, *Reservation*, *Expandable Reservation* and *Limit* if desired
6. Change the Memory *Shares*, *Reservation*, *Expandable Reservation* and *Limit* if desired
7. Click *OK* or *Cancel* when finished

- **Add/Remove virtual machines from a Resource Pool**
    - Adding a Virtual Machine to a Resource Pool – the virtual machines reservations and limits do not change

1. Log in to vCenter using the VI Client

2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
3. When you create a new virtual machine one of the pages in the wizard will allow you to specify a resource pool to place the virtual machine into
4. If you create a new resource pool and want to add existing virtual machines to it you can drag-and-drop a virtual machine into a resource pool as long as you have the proper permissions
    - If the resource pool does not have enough resources to guarantee the virtual machine reservation(s) then the move into the resource pool will fail (applies only to a powered-on virtual machine)

- Removing a Virtual Machine from a Resource Pool

1. Log in to vCenter using the VI Client
2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
3. Drag-and-drop the virtual machine into another resource pool. Dragging it into the root of the DRS cluster will move it into the root resource pool
4. If you no longer need the virtual machine power it off and delete it from disk or remove from inventory – this will also remove the virtual machine from a resource pool

- **Determine Resource Pool requirements for a given vSphere implementation**
    - As you may have noticed a sort of theme to this blueprint, anytime you are trying to determine requirements for a certain function always has the same general answer "it depends" and resource pool requirements are no different
    - Before you can determine you resource pool requirements you need to define the workloads that will be running in your environment and their associated priority within the organization
    - Resource pools are used to segment your resources, whether by organization, workload or some other business requirement. Once you define the workloads and their requirements, you can start to divide up the resource within the host or DRS cluster and begin to divide the resources into pools in a way that is efficient and is able to meet the requirements of the workloads running on said host or DRS cluster
    - Determine if your resource pools need to reach out to their parent resource pools should they need to provide more resources then they are allocated (expandable reservations)
    - Determine the need for reservations or limits. I strongly recommend NOT using per-virtual machine reservations as they add a lot of administrative overhead and don't play well with certain HA admission control policies (host failures the cluster tolerates). If you are going to set a reservation, do it at the resource pool level
- **Evaluate appropriate shares, reservations and limits for a Resource Pool based on virtual machine workloads**
    - Evaluating appropriate shares, reservations and limits for a resource pool based on virtual machine workloads directly relates to the previous section and the same pre-requisite applies; KNOW YOUR WORKLOADS! If you don't know what is happening in your

environment and what your virtual machines require to operate efficiently and effectively, your vSphere implementation will most likely fail

- I briefly defined what shares, reservations, and limits were previously, but let's really dig into them now
  - *Shares*: The amounts of shares you allocate to a resource pool are relative to the shares of any sibling (virtual machine or resource pool) and relative to its parent's total resources. Remember, a sibling is a virtual machine or resource pool that shares the same parent (receives resource from the same parent resource pool). When resources are allocated, shares only matter when there is contention. Contention occurs if you have overcommitted the resources in your DRS cluster (assigned more resource then you have) or during short-term spikes of workloads, which is normal. Rule of thumb, allocate more shares to your higher priority workloads and don't over-commit your resources unless you absolutely have to
  - *Reservations*: Again, reservations are the minimum amount of resources the resource pool will get. When you set a CPU or Memory reservation for a resource pool, those reservations are subtracted from the parent's available resources, making them unavailable to other siblings. If you have virtual machines that you need to guarantee a certain amount of resources for, reserve them in a resource pool and add those virtual machines to the resource pool
  - *Expandable Reservations*: Using expandable reservations gives you flexibility. If a virtual machine's workload increases and its resource pool cannot allocate more resources because there aren't any available, the resource pool will asks its parent resource pool to borrow resources. Resource pools that have virtual machines with spiking workloads may consider enabling *expandable reservations*
  - *Limits*: Limits is the maximum amount of resources a resource pool can have. If you set a 16GB memory limit for a resource pool, it will never receive anymore than 16GB. There aren't too many use cases to limit a resource pool, but one use case maybe a workload within a virtual machine that will utilize any and all resources it can get its hands on and you can't configure it otherwise, setting a limit on the resource pool is an option you may want to entertain

- **Clone a vApp**

  - Clone a vApp

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Right-click on the vApp you want to clone and select *Clone…*
    4. Select a host, cluster or resource pool for the vApp to run on/in > click *Next*
    5. Enter in a name for the vApp in the *vApp Name* field
    6. Choose an inventory location for the vApp (which vDatacenter and folder) > click *Next*
    7. Select where you want to store the new vApp, choose a datastore or datastore cluster > click *Next*
    8. Choose the disk format you want to use

        - Same format as source
        - Thin provisioned format
        - Thick format
    9. Click *Next*
    10. Map the networks for the new vApp – select the destination networks you want the new vApp to operate (source networks of original vApp are also displayed) by selecting the network from the drop down under the *Destination Networks* column > click *Next*
    11. Click *Finish*

Tools

- vSphere Resource Management guide
- vSphere Virtual Machine Administration guide

Objective 5.4 – Migrate Virtual Machines

Knowledge

- **Identify ESXi host and virtual machine requirements for vMotion and Storage vMotion**
    - There are multiple host and virtual machine requirements in order to perform vMotion and Storage vMotions on any given virtual machine.

    - Host Requirements for vMotion and Storage vMotion
        - Each host participating in a vMotion needs to have the proper licensing
        - The hosts participating in a vMotion need to meet the networking requirements for vMotion
        - The hosts participating in a vMotion must meet shared storage requirements

    - Virtual Machine Requirements for vMotion and Storage vMotion
        - The VM must not have raw disks in use for clustering
        - No virtual devices backed by physical devices that the destination host does not also have access to
        - If the VM is using a USB passthrough, ensure the device is enabled for vMotion
        - The VM must not have a virtual device backed by a device on a client computer

- **Identify Enhanced vMotion Compataibility CPU requirements**
    - In order to perform a vMotion between hosts the processors on those hosts need to meet certain requirements in order for the vMotion to take place tow work. In an effort to make

more hosts compatible with each other, which is to say more processors compatible, Enhanced vMotion Compatibility (EVC) was created. EVC allows for hosts with processors with different clock speeds, cache sizes, and other CPU differing features, to vMotion VMs between each other (processors must be from the same vendor class, i.e. AMD or Intel and the same processor family).

- Certain CPUs within the same family will not be compatible, especially if there is a major change to the instruction set
- There are multiple modes in which you can be set for EVC, see Objective 5.1 for details
- What is EVC actually doing? EVC figures out the common instructions/features amongst all hosts' CPUs and then masks the unique features from the virtual machines running in that DRS cluster. This ensures that execution of CPU instructions will successfully resume on the destination host once a vMotion has completed
- To sum up EVC CPU requirements:
  - CPUs must be in the same vendor class (can't mix Intel and AMD processors)
  - CPUs must also be from the same processor family (all CPUs within the same family may not be compatible)

- **Identify snapshot requirements for vMotion/Storage vMotion migration**
  - Basic vMotion requirements apply to virtual machines with snapshots. As long as the location of the snapshots are accessible by both source and destination host (default is virtual machine folder)
  - Basic Storage vMotion requirements apply to virtual machines with snapshots. This is new to vSphere 5 as earlier versions did not support performing a storage vMotion on virtual machines with snapshots
- **Migrate virtual machine using vMotion/Storage vMotion**
  - Migrations are pretty simple using the vSphere Client and the vSphere Web Client. For this purpose I'll only cover the thick client

  - Migrating a Virtual Machine using vMotion – has vDatacenter boundary

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Right-click on the virtual machine you want to vMotion and select *Migrate…*
    4. The *Migrate Virtual Machine* wizard will display, select *Change host* > click *Next*
    5. Choose a DRS cluster or individual host you want to migrate to > click *Next*
    6. Choose between *High priority* and *Standard priority*, High is the default > click *Next*
    7. Click *Finish*

  - Migrating a Virtual Machine using Storage vMotion

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)

3. Right-click on the virtual machine you want to storage vMotion and select *Migrate…*
4. The *Migrate Virtual Machine* wizard will display, select *Change datastore* > click *Next*
5. Choose a format for the destination virtual disk
    - Same format as source (default)
    - Thick Provision Lazy Zeroed
    - Thick Provision Eager Zeroed
    - Thin Provision
6. Choose whether you want to change the VM storage profile or not
7. Choose a new datastore or datastore cluster
8. If you selected a datastore cluster in step 7 and want to disable storage DRS check the *Disable Storage DRS for this virtual machine* checkbox and manually select a destination datastore in the pane below > click *Next*
9. Click *Finish*

- **Configure virtual machine swap file location**
    - There are three different locations that you can configure the swap file location of a virtual machine. If the host is not part of a cluster, you configure it per-host. If the host is part of a cluster, you configure it for the cluster or you can configure it for an individual virtual machine regardless if the host it runs on is part of a cluster or not

    - Configure Virtual Machine Swap Location – Cluster

        1. Log in to vCenter using the VI Client
        2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
        3. Right-click on the cluster you want to configure and select *Edit Settings…*
        4. Select *Swapfile Location* from the list on the left
        5. Select either *Store the swapfile in the same directory as the virtual machine (recommended)* or select *Store the swapfile in the datastore specified by the host*. Selecting the second option will allow you to edit the swapfile on a per-host basis
        6. Click *OK* when finished

    - Configure Virtual Machine Swap Location – Host

        1. Log in to vCenter using the VI Client
        2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
        3. Select the host you want to configure the swapfile location for from the left
        4. In the right pane select the *Configuration* tab
        5. Underneath the *Software* menu click the *Virtual Machine Swapfile Location* hyperlink
        6. In the top left of the center pane click the *Edit…* hyperlink
        7. Choose the datastore you want to store the swapfile on

8. Click *OK* when finished

- Configure Virtual Machine Swap Location – Virtual Machine

1. Log in to vCenter using the VI Client
2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
3. Right-click the virtual machine you want to configure and select *Edit Settings*
4. Choose the *Options* tab on top
5. Select *Swapfile Location*, which is the very last option in the list
6. Choose *Default*, which uses the settings of the cluster (if in a cluster), choose *Always store with the virtual machine* or choose *Store in host's swapfile datastore*
7. Click *OK* when finished

- **Migrate a powered-off or suspended virtual machine**
  - Migrating a powered-off or suspended VM is pretty straight-forward, it is a similar process to a normal vMotion

  - Migrate a Powered-off or Suspended Virtual Machine – has vCenter boundary

1. Log in to vCenter using the VI Client
2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
3. Right-click on the virtual machine you want to vMotion and select *Migrate…*
4. Leave the default option of *Change both host and datastore* or choose either host or datastore – if you are migrating to another vDatacenter you must choose the default > click *Next*
5. Choose the DRS cluster or individual host for the destination > click *Next*
6. If you select a DRS in the previous step choose now you must choose an individual host > click *Next*
7. Select the format for the virtual disk
8. If applicable select a VM Storage Profile
9. Select a datastore or datastore cluster, if you select a datastore cluster you have the option of checking the *Disable Storage DRS for this virtual machine* checkbox, doing so requires you to select an individual datastore from that datastore cluster and configuring advanced settings
10. Click *Next*
11. Click *Finish*

- **Utilize Storage vMotion techniques (changing virtual disk type, renaming virtual machines, etc.)**

- Storage vMotion has more uses than just moving data from one datastore to another. You can change the virtual disk format, apply storage profiles, split up virtual disks and disable Storage DRS
- You can change your virtual disk format to one of the three virtual disk format options:
  - *Thick Provision Lazy Zeroed* – this will allocate the space, but will not write to every block (zero it out) until first write
  - *Thick Provision Eager Zeroed* – this will allocate the space and zero out all of it up front, because of this thick provision eager zeroed disks take longer to create/storage vMotion
  - *Thin Provision* – this will logically allocate space, and the virtual machine will think it has all physical capacity, but the space is allocated as needed. Be careful of over-commitment and ensure you have proper alarms setup if you are going to over-commit using virtual disk thin provisioning
- You can change the VM Storage Profile during a storage vMotion, which an administrator will have pre-configured (this option is not available if you don't have any storage profiles defined)
- You can split up your virtual disk files also. Clicking the *Advanced* button in the storage vMotion wizard on the *Storage* page brings up another window that allows you to choose, individually, where you store your configuration file and virtual hard disks
- If you are selecting a datastore cluster as your destination storage you also have the option to disable storage DRS for that particular virtual machine. At that point you can manually choose a datastore from that datastore cluster

Tools

- vSphere Resource Management guide
- vSphere Virtual Machine Administration guide
- VMware vSphere Examples and Scenarios guide

Objective 5.5 – Backup and Restore Virtual Machines

Knowledge

- **Identify snapshot requirements**
  - A snapshot is essentially a point-in-time image of a virtual machine. I won't get deep into how they are implemented within vSphere because it can be a bit complex if this is your first time looking at them. You can either take a crash-consistent snapshot or an application consistent snapshot. Taking a snapshot and Quiescing the state will create an application consistent snapshot
  - There are different types of requirements when talking about snapshots, business requirements and hard requirements as defined by vSphere. Business requirements are more the business use/use case for them in your environment
  - Some use cases or business requirements for snapshots
    - Change management

- Patching
- Software upgrades

- vSphere Requirements for Snapshots
  - Raw disks, physical Raw Device Mapping (RDM) disks or guest operating systems utilizing iSCSI software initiators are not supported
  - PCI Direct Path I/O devices are not supported
  - VMs with independent disks are only supported for snapshots when turned off
  - Snapshots are not supported on VMs that are configured for bus sharing

- **Create/Delete/Consolidate virtual machine snapshots**

  - Create a Snapshot

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*) or navigate to the *VMs and Templates* view (*View* > *Inventory* > *VMs and Templates*)
    3. Right-click on the virtual machine you want to snapshot > select the *Snapshot* menu and click *Take Snapshot…*
    4. The Snapshot window will come up, enter in a *Name* for the snapshot – make it meaningful
    5. Enter in a *Description* for the snapshot
    6. Select whether or not to *Snapshot the virtual machine's memory*, this checked by default
    7. Select whether you want to *Quiesce guest file system*, which requires VMware tools by checking the checkbox
    8. Click *OK* and the snapshot will be created

  - Delete/Consolidate a Snapshot – deleting is consolidating

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*) or navigate to the *VMs and Templates* view (*View* > *Inventory* > *VMs and Templates*)
    3. Right-click on the virtual machine you that has a snapshot you want to delete/consolidate > select the *Snapshot* menu and click *Snapshot Manager…*
    4. Select the snapshot you want to delete
    5. Click *Delete*
    6. You can also click *Delete All* if you want to delete/consolidate all of the snapshots for that virtual machine
    7. Click *Yes* to confirm deleting/consolidating the snapshot
    8. Click *Close* to close the snapshot manager

Keep in mind that the longer you have been running on the snapshot(s) you are deleting, the longer it will take to consolidate them into the base vmdk

- **Install and Configure VMware Data Recovery**
  - Before we go over installed VMware Data Recovery lets discuss a few requirements
    - Only 100 VMs can be backed up per data recovery virtual appliance
    - 10 data recovery appliances per vCenter instance
    - 8 virtual machines can be backed up simultaneously
    - Depending upon the number of virtual disks being backed up you may have to add additional SCSI controllers to the data recovery appliance in order to hot-add more hard drives
    - The appliance connects to vCenter over port 902
    - The File Level Restore (FLR) client uses port 22024
  - There are a lot more requirements than the list above, see pages 13-17 of the *VMware Data Recovery Administration Guide* to see a complete list

  - Install VMware Data Recovery – Client Plug-in; install on the machine you want to manage Data Recovery from

    1. From the installation media run "VMwareDataRecoveryPlugin.msi" (this is the name at the time of this posting)
    2. Click *Next* three times
    3. Choose *I Agree* to the EULA and click *Next*
    4. Click *Next* to begin the install
    5. Click *Close* when the installation is complete

  - Install VMware Data Recovery – Backup Appliance

    1. Extract the OVF from the installation media for the backup appliance if you have not done so already
    2. Log in to vCenter using the VI Client
    3. Click the *File* menu and select *Deploy OVF Template…*
    4. Browse and select the OVF file you extracted from the installation media > click *Next*
    5. You will see the details of the OVF > click *Next*
    6. Accept the EULA and click *Next*
    7. Select a name for the backup appliance
    8. Select an Inventory location for the backup appliance > click *Next*
    9. Select the cluster you want to deploy the appliance to > click *Next*
    10. Choose a datastore cluster or datastore you want to store the appliance on – if you choose a datastore cluster you have the option of disabling SDRS > click *Next*

11. Select your disk format > click *Next*
12. Map out your source and destination networks for the two networks > click *Next*
13. Select a time zone setting from the dropdown > click *Next*
14. Optionally check *Power on after deployment* and click *Finish*
15. Now you can add additional hard disks to the backup appliance if you want to use that space to store backups instead of using SMB or NFS
16. Power on the backup appliance

- Configure VMware Data Recovery

1. Log in to vCenter using the VI Client
2. Open the console for the backup appliance you just deployed
3. Select *Configure Network* from the menu > press *Enter*
4. Follow the steps to configure the IP settings for the appliance, IPv4 or IPv6
5. Alternatively you can configure the network settings through a web browser if the appliance received an IP address via DHCP, check the console and go to the URL displayed (default login is root/vmw@re)
6. Log in to vCenter using the VI Client (if you aren't already)
7. Select the *View* menu > select *Solutions and Applications* > *VMware Data Recovery* – this won't be in the list of items if you haven't installed the plug-in
8. Provide a name or IP of the data recovery backup appliance > click *Connect*
9. Enter in the password for the username displayed > click *OK*
10. The *Getting Started Wizard* will display and auto-fill with the credentials you just provided > click *Next*
11. You need to add a backup destination
    - Virtual Disk attached to the Backup Appliance
      - If you added a disk during the install, it will be displayed in the list. Select it and click the *Format* hyperlink to format the volume. Once complete the volume will be mounted
    - Network Share
      - Click the *Add Network Share* hyperlink
      - Click *Continue* to the warning displayed which basically states don't use a network share greater than 500GB
      - Enter in the *URL*, *Username* and *Password* > click *Add*
      - Click *Close*
12. Choose which backup destination you want to use > click *Next*
13. The *Create a new Backup Job after completion* is checked by default; leave checked or uncheck > click *Close*

- **Create a backup job with VMware Data Recovery**
  - Alright, lets create a backup job with our newly installed Data Recovery Appliance

  - Create a Backup Job with VMware Data Recovery

1. Log in to vCenter using the VI Client (if you aren't already)
2. Select the *View* menu > select *Solutions and Applications* > *VMware Data Recovery*
3. There are a few different ways you can create a new backup job, you can right-click on a vDatacenter, a cluster, a virtual machine or a template > select *Add to Backup Job* > *New Backup Job…*
4. (this is the method I'll use) You can also click on the *Backup* tab in the right-pane > right-click anywhere in the windows > select *New*
5. The *Backup Job Wizard* opens > enter in a name for the backup job in the *Name* field – make this descriptive and meaningful > click *Next*
6. Select which objects you want to backup by placing a checkbox next to it. You can backup:
    - All objects under vCenter
    - All objects under a vDatacenter
    - All objects under a Cluster
    - Individual virtual machines with all associated virtual disks
    - Individual virtual disks from a virtual machine
7. After making your selection(s) click *Next*
8. Select the destination location for the backup > click *Next*
9. Set your backup window, this should be self-explanatory > click *Next*
10. Select the *Retention Policy* you want to use (few, more, many or custom), setting any of the first three has pre-canned settings
    - *Few* – retain 7 recent backups, retain 4 weekly backups, retain 3 monthly backups and retain 0 quarterly and yearly backups
    - *More* – retain 7 recent backups, retain 8 weekly backups, retain 6 monthly backups, 4 quarterly backups and 1 yearly backup
    - *More* – retain 15 recent backups, retain 8 weekly backups, retain 3 monthly backups, 8 quarterly backups and 3 yearly backup
    - *Custom* – set your own
11. Click *Next* > click *Finish*

- **Perform a test and live full/file-level restore with VMware Data Recovery**

    - Perform a Test of a Full Restore with VMware Data Recovery

1. Log in to vCenter using the VI Client
2. Select the *View* menu > select *Solutions and Applications* > *VMware Data Recovery*
3. Right-click on the virtual machine you want to test a full restore on > click *Restore Rehearsal from Last Backup*
4. Ensure the virtual machine and virtual disks you want to test a full restore on > click *Next*
5. If you need to provide alternate credentials click the *Restore Credentials…* hyperlink and enter in a different username and password

6. You can change some options for the restore
    - Datastore – select the datastore to use for the Virtual machine and select one for the virtual disk(s)
    - Virtual Disk Node – specify the SCSI Bus you want to use
    - Restore Configuration – select Yes or No
    - Reconnect NIC – select Yes or No
    - Power On – select Yes or No
7. Click *Next*
8. Click *Restore*
9. Once complete a new VM is spawned and powered-on (hopefully you did not answer Yes to Reconnect NIC) and you can log in and check it out
10. For some very strange reason, there is no "Done with Restore Rehearsal" option and you have to manually clean it up. Once you are done testing, power off the rehearsal VM and delete it

- Perform a Full Restore with VMware Data Recovery

1. Log in to vCenter using the VI Client
2. Select the *View* menu > select *Solutions and Applications* > *VMware Data Recovery*
3. Click on the *Restore* tab in the right pane
4. Click the *Restore* hyperlink
5. Select the virtual machine you want to restore and select which backup you want to restore from
6. Select the virtual disk(s) you want to restore > click *Next*
7. If you need to provide alternate credentials click the *Restore Credentials…* hyperlink and enter in a different username and password
8. The Datastore option will default to the datastore the disk was on before
9. You can choose whether or not to power on the virtual machine by selecting Yes or No from the Power On column
10. You can select the Virtual Disk Node for the disk(s) you are restoring
11. Click *Next*
12. Click *Restore*

- Perform a File Level Restore with VMware Data Recovery (Windows VM)

1. Log in to the virtual machine that requires the File Level Restore (FLR)
2. Run the FLR client, VMwareRestoreClient.exe (as of this posting)
3. Enter in the IP address or Name for the Data Recovery Appliance
4. Click *Login*
5. Select the virtual disk you want to restore from using the list of restore points
6. Click the *Mount* button at the top left
7. Once mounted click the *Browse* button
8. This will open an explorer Window. From here browse to the file(s) you want to restore and copy them back to the virtual machine

9. Once complete unmounts the restore point by clicking *Unmount* and close the FLR client

For instructions how to perform a FLR on a Linux VM take a look at pages 36-37 of the VMware Data Recovery Administration Guide

- **Determine appropriate backup solution for a given vSphere implementation**
  - Every implementation is different and you can't always do a cookie-cutter solution, especially when it comes to backups. Right now VMware Data Recovery will backup individual virtual machines and file.
    - Data Recovery is not application aware and therefore some applications, such as Sharepoint and MS Exchange you may want a more granular level of backup, specific to those applications
    - If your vSphere implementation includes branch offices where some hosts/VMs traverse a WAN, you may not want to use data recovery
  - Bottom line is know your environment, know what your requirements and constraints are and know the capabilities of VMware Data Recovery to determine if it is a fit for your vSphere implementation

Tools

- vSphere Virtual Machine Administration guide
- VMware Data Recovery Administration guide

Objective 5.6 – Patch and Update ESXi and Virtual Machines

Knowledge

- **Identify patching requirements for ESXi hosts and virtual machine hardware/tools**
  - Patching requirements for ESXi hosts and virtual machine hardware/tools are usually separate, but depending on the update may correspond with virtual machine hardware/tools updates, in which case follow the *Orchestrated Datacenter Upgrade* methodology described on pages 157-160 of Installing and Administering VMware vSphere Update Manager guide
  - You will need to identify whether the update manager server can download patches directly or, if the network is secure without internet access you may consider using Update Manager Download Server (UMDS)
  - Configuring baselines for your ESXi hosts and virtual machines will allow you to scan your environment and determine which entities are not compliant, and from there remediate (stage/deploy patches)
  - Determine if you have any third party virtual appliances that can be updated via update manager

- Typically the biggest requirement is to keep your hosts and virtual machine hardware/tools up-to-date with the latest patches; do that with Update Manager

- **Create/Edit/Remove a Host Profile from an ESXi host**
  - If you have read other objectives in this guide, this section will look familiar; lets start with Creating a Host Profile:

    NOTE: Host profiles require Enterprise Plus licensing

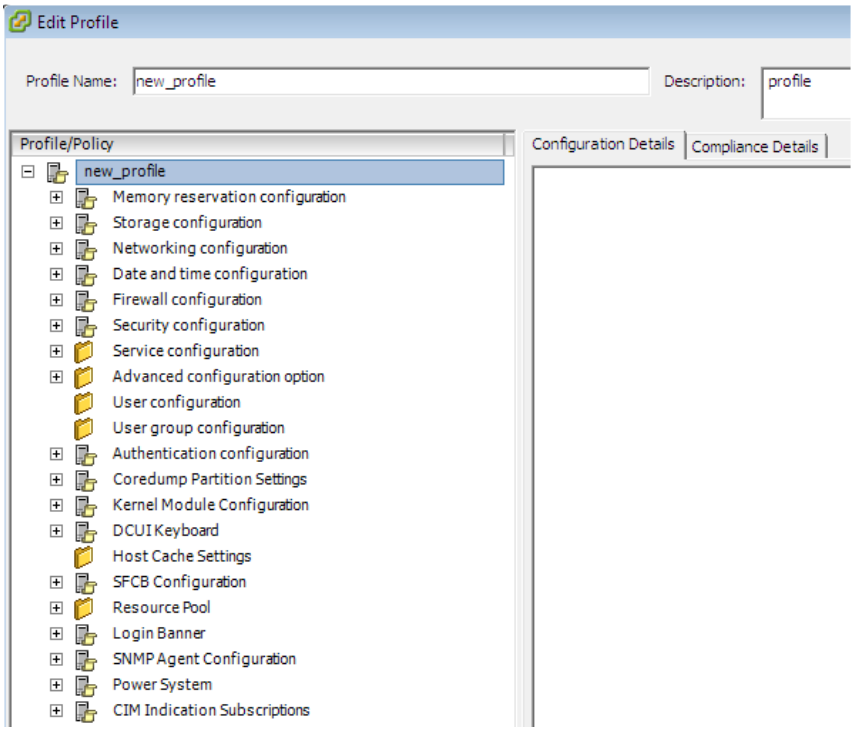
  - Creating a Host Profile

    1. Log in to vCenter using the VI Client
    2. Select the *View* menu > select *Management* > *Host Profiles* (or *Ctrl* + *Shift* + *P*)
    3. Right-click in the white area under the *Host Profiles* folder icon and select *Create Profile*
    4. You have two option, *Create Profile from existing host* or *Import profile*, for this walk-through choose *Create Profile from existing host* > click *Next*
    5. Choose which host you want to use as a reference host > click *Next*
    6. Enter in a *Name* and a *Description* for this new Host Profile > click *Next*
    7. Click *Finish*

  - Editing a Host Profile

    1. Log in to vCenter using the VI Client
    2. Select the *View* menu > select *Management* > *Host Profiles* (or *Ctrl* + *Shift* + *P*)
    3. Right-click on the host profile you want to edit and select *Edit Profile…*
    4. From here you can edit the name and description of the host profile, as well as the profile itself and the policies within
    5. Click on any policy and view the configuration and compliance details in the right-pane
    6. Click *OK* when finished

    There are 21 different policies and many more options beneath each policy so I won't go into them here, but the best way to get to know these policies is by taken a look at a host profile



- Deleting a Host Profile

    1. Log in to vCenter using the VI Client
    2. Select the *View* menu > select *Management* > *Host Profiles* (or *Ctrl* + *Shift* + *P*)
    3. Right-click on the profile you want to delete and select *Delete Profile…*
    4. Click *Yes* to confirm deletion

- **Attach/Apply a Host Profile to an ESXi host or cluster**
    - Attaching a host profile to an ESXi host or a cluster is the same basic procedure

    - Attaching a Host Profile to an ESXi Host or Cluster

        1. Log in to vCenter using the VI Client
        2. Select the *View* menu > select *Management* > *Host Profiles* (or *Ctrl* + *Shift* + *P*)
        3. Right-click on the host profile you want to attach and select *Attach Host/Cluster…*
        4. Choose the host(s) and/or cluster(s) you want to attach the host profile to in the left-pane > click *Attach*
        5. Click *OK* when complete

    - Applying a Host Profile to an ESXi Host – cannot apply directly to a Cluster

        1. Log in to vCenter using the VI Client
        2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)

3. From the left pane right-click the host you want to apply the host profile (you must attach a profile before you apply it) > click *Host Profile* > *Apply Profile…*
    a. If the host is not in maintenance mode you will get an error telling you that the host must first be in maintenance mode prior to applying the host profile
4. A screen will show you the list of configuration changes that will be made and any settings requiring user input will be displayed; you must manually enter static values for these fields
5. Once complete click *Finish* and take the host out of maintenance mode

- **Perform compliance scanning and remediation of an ESXi host using Host Profiles**
    - Compliance Scanning and Remediation using Host Profiles

1. Log in to vCenter using the VI Client
2. Select the *View* menu > select *Management* > *Host Profiles* (or *Ctrl* + *Shift* + *P*)
3. In the left pane select the profile you want to check for compliance > click the *Hosts and Cluster* tab on the right
4. Select whichever host/cluster you want to check compliance on > click the *Check Compliance* hyperlink
5. Once it completes it will see a status under the *HostPorfileCompliance* column and if non-compliant, details will be displayed in the lower pane letting you know which policies your host/cluster is out of compliance with
6. If your host/cluster comes up as non-compliant click the *Apply Profile…* hyperlink (remember the host must be in maintenance mode prior to applying a host profile)
7. Like procedure above, "Applying a Host Profile…" a screen will show you a list of configuration changes that will be applied to the host you are remediating (these should be the same changes you saw listed in step 5)
8. Once you are done reviewing the changes and are comfortable with them click *Finish*
9. Once it is complete the host/cluster should now show as *Compliant*

- **Install and Configure vCenter Update Manager**
    - You can install vCenter Update Manager in a few different configurations. First and foremost ensure that the hardware, operating system and database you are loading update manager on is supported (pages 21 – 23 of Installing and Administrating VMware vSphere Update Manager)
    - The documentation references three deployment models for update manager:
        - All-in-one model – vCenter, Update Manager and the database all on one server. Number of servers required = 1
        - Medium deployment model – vCenter and Update Manager on one server, database on another server. Number of servers required = 2
        - Large deployment model – vCenter on one server with a dedicated database server, Update Manager on its own server with a dedicated database server. Number of servers

required = 4 (recommended when you have more than 1000 virtual machines or 100 hosts

- Requires a 32bit DSN (except if you're using SQL 2008 R2 Express)

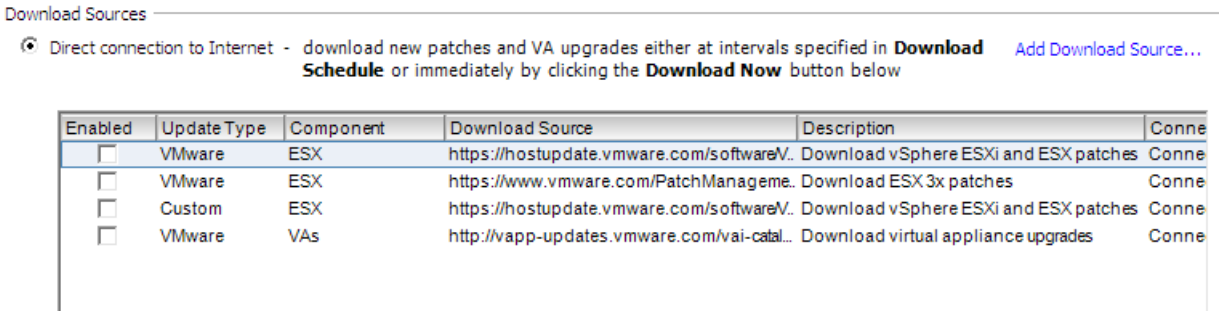
- Installing vCenter Update Manager – using SQL 2008 R2 Express and installing on same server as vCenter

    1. Locate your vCenter 5.0 media and mount to vCenter server
    2. Execute autorun.exe to bring up the menu of products on the vCenter 5.0 media
    3. Click on *VMware vSphere Update Manager*
    4. In the right pane there are two prerequisites listed, Microsoft .NET 3.5 SP1 and Windows Installer 4.5, if you do not have these installed already install them
    5. Once complete click the *Install* button
    6. Select your language and click *OK*
    7. Click *Next* twice
    8. Accept the EULA and click *Next*
    9. Select whether you want to download updates from a default source after the installation (default option is yes), do not select if you this deployment of Update Manager is air gapped > click *Next*
    10. Enter in information for the vCenter server you want to link to this instance of Update Manage, it's 1:1 ; enter *IP Address/Name*, *HTTP Port*, *Username* and *Password* > click *Next*
    11. Choose whether to install Microsoft SQL Server 2008 R2 Express or to use an existing supported database, if you choose to use an existing database you'll need to provide the 32bit DSN > click *Next*
    12. Choose how you want Update Manager to be identified on the network by making a selection from the dropdown, usually the IP or NETBIOS name
    13. If you wish to change the *SOAP Port*, *Web Port*, or *SSL Port* do so at this screen. If you have an internet connection and use a proxy, check *Yes, I have Internet connection and I want to configure proxy settings now*.
    14. If you want to change the default installation paths for the Update Manager installation or the location for downloading patches do so at this screen > click *Next* – If you have less than 120GB of disk space free you will get a warning and a link to VMwares *vSphere Update Manage Sizing Estimator* > click *OK*
    15. Click *Install*
    16. Click *Finish* once the install completes

- **Configure patch download options**
    - Before you can configure any options for Update Manager the machine you are using to connect to vCenter needs to have the Update Manager plug-in installed. Once it is installed it will appear under Solutions and Applications as *Update Manager*

- Configure Patch Download Options

1. Log in to vCenter using the VI Client
2. Select the *View* menu > select *Solutions and Applications* > *Update Manager*
3. Click on the *Configuration* tab
4. From the *Settings* menu on the left click the *Download Settings* hyperlink
5. First lets define the our download sources. By default the *Direct connection to Internet* option is enabled along with four sources



6. Add a new download source (third-party download source)
   - Click the *Add Download… Source* hyperlink
   - Enter in a *Source URL* and Description
   - Click the *Validate URL* button (clicking *OK* will also try to validate the URL)
   - If the URL can't be validated it will show as *Not Connected* and a warning will be displayed if you click *OK* with a non-validated URL letting you know that the source is not valid and asks if you still want to add it to the list
7. Instead of using the Direct Connect to the Internet option you can choose the *Use a shared repository* option
   - Enter in a URL for the shared repository and click *Validate URL*
8. Click the *Import Patches* hyperlink to manually import from a .zip file
9. Click the *Download Now* button to download available patches from your listed sources
10. If you environment requires a proxy server to access the Internet or shared repository enter in the following information as needed
    - Check the *Use Proxy* checkbox
    - Enter in the proxy server name and port
    - If your proxy server requires authentication check the *Proxy requires authentication* checkbox and enter in a Username/Password
    - Click *Test Connection* to verify you have the correct settings
    - Click *Apply*
11. From the *Settings* menu on the left click the *Download Schedule* hyperlink
12. Choose whether you want to enable/disable a download schedule by checking/unchecking the *Enable scheduled download* checkbox
13. Click the *Edit Download Schedule…* hyperlink

14. Enter in a Task Name and description
15. Choose a *Frequency* (Once, Hourly, Daily, Weekly or Monthly)
16. Choose a *Start Time*
17. Choose the *Interval* (represented in days) > click *Next*
18. Enter in the email addresses you want to be notified when new patches are downloaded; this requires that vCenter be setup with a working SMTP server > click *Next*
19. Click *Finish*
20. From the *Settings* menu on the left click the *Notification Check Schedule* hyperlink
21. Choose whether you want to enable/disable scheduled download by checking/unchecking the *Enable scheduled download* checkbox (this looks the same as download schedule, but these are for notifications)
22. Click the *Edit Notifications…* hyperlink
23. Enter in a Task Name and description
24. Choose a *Frequency* (Once, Hourly, Daily, Weekly or Monthly)
25. Choose a *Start Time*
26. Choose the *Interval* (represented in days) > click *Next*
27. Enter in the email addresses you want to be notified when new patches are downloaded; this requires that vCenter be setup with a working SMTP server > click *Next* – this will notify you of recalled patches or other alerts
28. Click *Finish*

- **Create/Edit/Delete an Update Manager baseline**
  - Creating an Update Manager Baseline

1. Log in to vCenter using the VI Client
2. Select the *View* menu > select *Solutions and Applications* > *Update Manager*
3. Select the *Baselines and Groups* tab

There are two different views for Baselines, *Hosts* and *VMs/VAs*. There are two pre-defined baselines in the *Hosts* baseline view; Critical Host Patches and Non-Critical Host Patches. There are three pre-defined baselines in the *VMs/VAs* baseline view; VMware Tools Upgrade to Match Host, VM Hardware Upgrade to Match Host and VA Upgrade to Latest

4. Depending upon what you want to create a baseline for (hosts or VMs/VAs) select the appropriate view, in our case we'll choose the *Hosts* view, which is the default
5. Click the *Create…* hyperlink
6. Enter in a *Name* and *Description*
7. Select the *Baseline Type* from the following
   - Host Baselines – Host Patch, Host Extension and Host Upgrade
   - VA Baselines – VA Upgrade

8. Click *Next*
9. Select the type of baseline
    - *Fixed* – this a set of patches that are static and manually defined
    - *Dynamic* – this is a set of patches that updated automatically when new patches are available based on user-defined criteria
10. After selecting the baseline type (I'm using *Dynamic* for this) click *Next*
11. Select which patch vendors and products you want for the dynamic baseline to update for
12. Select the *Severity* (low, moderate, important and critical) and select the *Category* (any, security, bugfix, enhancement and other)
13. Select the *Release Date* criteria; *On or After* or *On or Before* or choose both. After making you selections it will tell you, based on your selected criteria and patches you have already downloaded, how many patches meet your criteria
14. Click *Next*
15. This screen will show you each patch that met your criteria and gives you the option to exclude certain patches. Click on the patches you want to exclude and click the down arrow to add them to the exclusion list > – click the *Advanced* button to filter your selection
16. Click *Next*
17. Here you can add additional fixed patches (must already have been imported manually). Click on the fixed patches you want to include in your dynamic baseline and click the down arrow to add them – click the *Advanced* button to filter your selection
18. Click *Next*
19. Click *Finish*

- Editing an Update Manager Baseline

1. Log in to vCenter using the VI Client
2. Select the *View* menu > select *Solutions and Applications* > *Update Manager*
3. Select the *Baselines and Groups* tab
4. Click on the baseline you want to modify and click the *Edit…* hyperlink
5. All the options available in the *Create Baseline* wizard are available in this wizard, for a detailed overview see the section on Created an Update Manager Baseline above
6. Step through the wizard and make changes as needed
7. Click *Finish* when complete

- Deleting an Update Manager Baseline

1. Log in to vCenter using the VI Client
2. Select the *View* menu > select *Solutions and Applications* > *Update Manager*
3. Select the *Baselines and Groups* tab
4. Click on the baseline that you want to delete and click the *Delete* hyperlink
5. Click *Yes* to confirm the deletion operation

- **Attach an Update Manager baseline to an ESXi host or cluster**
  - You can attach a baseline to ESXi host or cluster, as well as the vDatacenter. This walk-through will take you through attaching a baseline to an ESXi host

  - Attach an Update Manager Baseline to an ESXi Host

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Select the host you want to attach an Update Manager baseline to and click the *Update Manager* tab on the right
    4. Click the *Attach…* hyperlink at the top right
    5. Select which patch baseline(s) you want to attach > click *Attach*
    6. The baseline(s) you just attached should now show in the *Attached Baselines* pane

- **Scan and remediate ESXi hosts and virtual machine hardware/tools using Update Manager**
  - Before you can scan and remediate an ESXi host you need to have attached a baseline, either pre-defined or manually created. The operations described below can also be initiated by right-clicking on the ESXi host or Virtual Machine and selecting *Scan for Updates* and *Remediate…*

  - Scanning an ESXi host

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Select the host you want to scan and click the *Update Manager* tab on the right
    4. Click the *Scan…* hyperlink at the top right
    5. Select what you want to scan for (Patches and Extensions and Upgrades)
    6. Click *Scan*

  - Remediating an ESXi host

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Select the host you want to remediate and click the *Update Manager* tab on the right
    4. Click the *Remediate…* button at the bottom
    5. Select the Basegroup or Baseline type in the right pane and place a check in the checkbox of the Baseline(s) you want > click *Next*
    6. Select the Patches and/or extensions you want to apply to this ESXi host > click *Next*

7. You will be prompted to schedule this remediation as a task, enter in a *Task Name* and *Description*
8. Under *Remediation Time* choose when you want to run the task. Choose *Immediately* (default) or specify a date and time > click *Next*
9. Choose your host maintenance options. If the patches you selected require the host to go into maintenance mode, choose the power state for the virtual machines on the host (power off, suspend, do not change)
10. If you want to retry entering maintenance mode should the first time fail, check the *Retry entering maintenance mode in case of failure* checkbox and select the *Retry delay* (in minutes) and *Number of retires*
11. Check the *Disable any removable media devices connected to the virtual machines on this host* checkbox if you want to disconnect removable media
12. If you want to remediate powered on PXE booted ESXi hosts (auto-deploy) check the *Enable patch remediation of powered on PXE booted ESXi hosts* checkbox
13. Click *Next*
14. Click *Finish*

- **Stage ESXi host updates**
  - Staging patches allows you to send the patches to the ESXi host(s) prior to performing remediation. This will lessen the total time for remediation and your host(s) being in maintenance mode because the patches will already be available locally to the host(s), therefore not having to wait for the patches to be copied.

  - Stage ESXi Host Updates

    1. Log in to vCenter using the VI Client
    2. Navigate to the *Host and Clusters* view (*View* > *Inventory* > *Hosts and Clusters*)
    3. Select the host you want to stage patches for and click the *Update Manager* tab on the right
    4. Click the *Stage…* button at the bottom (you can also right click on the host and choose *Stage Patches…* without going to the Update Manager tab)
    5. Select the baseline where the patches you want to stage are located > click *Next*
    6. Select the patches you want to stage > click *Next*
    7. Click *Finish*

<u>Tools</u>

- vSphere Host Profiles guide
- Installing and Administering VMware vSphere Update Manager guide
- Reconfiguring VMware vSphere Update Manager
- VMware vSphere Examples and Scenarios guide

Section 6 – Perform Basic Troubleshooting and Alarm Management

Objective 6.1 – Perform Basic Troubleshooting for ESXi Hosts

Knowledge

- **Identify General ESXi Host Troubleshooting Guidelines**

The *vSphere Troubleshooting* guide is the one stop shop for this section

- **Troubleshoot Common Installation Issues**

Refer to Objective 1.3 and make sure your hosts meet the hardware requirements as well as the VMware HCL. If using AutoDeploy refer to pages 20 thru 26 of the *vSphere Troubleshooting*guide and also VMware KB 2000988 (Troubleshooting vSphere Auto Deploy).

- **Monitor ESXi System Health**

With the release of ESXi back in the VI 3.5 days it provided a new way to manage your hosts, the Common Information Model (CIM). CIM allows for a standard framework to manage computing resources and presents this information via the vSphere Client. For further information read the VMware White Paper "The Architecture of VMware ESXi" as well as thisVMware Support Insider blog post.
To actually see how ESXi and vSphere Client leverages CIM read pages 25 thru 28 of the*vSphere Monitoring and Performance* documentation.

- **Export Diagnostic Information**

There are multiple ways to get at this information, but I will assume the exam is going to be geared more towards using the vSphere Client for this task. For completeness however I have included links that cover using a console session as well as PowerCLI.

Gathering vCenter Server Log Bundles (VMware KB 1011641, Collecting Diagnostic Information for VMware vCenter Server)

To generate a vCenter Server log bundle, select Start > All Programs > Vmware and select either "Generate vCenter Server Log Bundle – Extended" or "Generate vCenter Server Log Bundle" (Be sure to "Run as Administrator").

Gathering vCenter Server and ESXi Log Bundles (VMware KB 653, Collecting Diagnostic Information for Vmware ESX/ESXi Using the vSphere Client)

From within the vSphere Client connected to vCenter click Administration from the menu bar and select Export System Logs. This will allow you to export either vCenter logs, ESX/ESXi logs, are all of the above in a single zip file.

To use the vm-support command or PowerCLI refer to VMware KB 1010705 (Collecting diagnostic information for VMware ESX/ESXi using the vm-support command) and VMware KB

1027932 (Collecting diagnostic information for VMware vCenter Server and ESX/ESXi using the vSphere PowerCLI)

Tools

- vCenter Server and Host Management Guide
- vSphere Monitoring and Performance Guide
- vSphere Troubleshooting Guide

Objective 6.2 – Perform Basic vSphere Network Troubleshooting

Knowledge

- **Verify Network Configuration**

Refer to each objective under Section Two. Focus on the core concepts and configuration of both vNetwork Standard Switches and vNetwork Distributed Switches:

- Port/dvPort Groups
- Load Balancing and Failover Policies
- VLAN Settings
- Security Policies
- Traffic Shaping Policies
-

For additional information read the VMware Information Guide "VMware Virtual Networking Concepts". This document is based on VI3 but still does a good job with the core functions of a vStandard Switch.

- **Verify a Given Virtual Machine is Configured with the Correct Network Resources**

Instead of duplicating work, refer to VMware KB 1003893, "Troubleshooting Virtual Machine Network Connection Issues". More then enough information listed there.

- **Troubleshoot Virtual Switch and Port Group Configuration Issues**

One key aspect to remember is when setting up Port Groups or dvPort Groups, spelling counts (as well as upper/lower case)! If a Port Group is spelled Test on one host and is spelled test on a second host vMotion will fail. Same holds true with Security Policies, if one vSwitch on a host is set to accept Promiscuous Mode and it is set to Reject on the other host, again vMotion will fail. Also, refer to the objectives under Section Two to be sure your switches are configured correctly.

- **Troubleshoot Physical Network Adapter Configuration Issues**

This is pretty straight forward as there is not a lot of configuration done at the physical network layer. Be sure that your physical nics that are assigned to a virtual switch (vSwitch or dvSwitch) are configured the same (speed, vlans, etc) on the physical switch. If using IP Hash as your load balancing method make sure on the physical switch side link aggregation has been enabled. Refer to VMware KB 1001938 and VMware KB 1004048 for further details as well as examples. If using beacon probing for network failover detection it standard practice to use a minimum of three (or more) uplink adapters. See VMware KB 1005577 for further details.

- **Identify the Root Cause of a Network Issue Based on Troubleshooting Information**

Using the above notes as well as the linked VMware KB articles one should be able to isolate issue to one of four areas:

- Virtual Machine
- ESX/ESXi Host Networking (uplinks)
- vSwitch or dvSwitch Configuration
- Physical Switch Configuration

Tools

- vSphere Troubleshooting guide
- vSphere Networking guide

Objective 6.3 – Perform Basic vSphere Storage Troubleshooting

Knowledge

- **Verify storage configuration**

  Refer to the *vSphere Storage* and the SAN System Design and Deployment Guide (not specific to vSphere 5, but worth a read) by VMware. This will cover a lot of areas needed for working with a FC/iSCSI SAN environment with vSphere. Also a good understanding of the hardware you are using on the backend (storage arrays, FC switches, networking, etc) and there "vSphere Best Practices" documents will assist in the proper configuration.

- **Troubleshoot storage contention issues**

  We they mention "storage contention" I am taking this as I/O throughput or I/O latency issues. I find the quickest and easiest way of measuring/checking this is via esxtop/resxtop. VMware KB 1008205 and Duncan Eppings esxtop blost post covers this is in more detail.

  Metrics to be aware of:

Disk Metric	Threshold	Description
DAVG	25	This is the average response time in milliseconds per command being sent to the device.
GAVG	25	This is the response time as it is perceived by the guest operating system. This number is calculated with the formula: DAVG + KAVG = GAVG.

KAVG	2	This is the amount of time the command spends in the VMkernel

Also see pages 47 thru 50 of the vSphere Troubleshooting documentation for further information.

- **Troubleshoot storage over-commitment issues**

  Storage can be over committed in a several ways:

  - As mentioned above is with I/O latency and throughput
  - datastore usage, going over the actual amount of storage your array provides or the amount assigned to a datastore (think Thin-provisioning).
  - Amount of VM's on a datastore, can cause SCSI reservation issues
  - Datastore path thrashing
  - Inadequate LUN queue depth

- **Troubleshoot iSCSI software initiator configuration issues**

  Things to look out for:

  - Setting up a proper iSCSI Network (pg 74 thru 79 of the vSphere Storage document) Configuration of Jumbo Frames (pg 80 of the vSphere Storage document)
  - Network connectivty using vmkping (See VMware KB 1003728, Testing VMkernel network connectivity with the vmkping command)

  For further information refer to pages 107 thru 112 of the vSphere Storage documenation as well as page 51 of the vSphere Troubleshooting documenation.

- **Troubleshoot Storage Reports and Storage Maps**

  See pages 29 thru 32 of the vSphere Monitoring and Performance documentation

- **Identify the root cause of a storage issue based on troubleshooting information**

The vSphere Troubleshooting document covers several issues that you may run into. See Pages 45 thru 51.

Tools

- vSphere Storage guide
- vSphere Troubleshooting guide

Objective 6.4 – Perform Basic Troubleshooting for HA/DRS Clusters and vMotion/Storage vMotion

Knowledge

- **Identify HA/DRS and vMotion requirements**

  HA Requirements

  - All hosts must be licensed for vSphere HA
  - You need at least two hosts in the cluster
  - All hosts need to be configured with static IP addresses. If you are using DHCP, you must ensure that the address for each hosts persists across reboots
  - There should be at least on management network in common among all hosts and best practices is to have at least two. Management networks differ depending on the version of host you are using.
    - ESX hosts - service console network
    - ESXi hosts earlier than version 4.0 - VMkernel network
    - ESXi hosts version 4.0 and later - VMkernel network with the **Management Network** checkbox enabled
  - To ensure that any virtual macine can run on any host in the cluster, all hosts should have access to the same virtual machine networks and datastores
  - For VM Monitoring to work, VMware tools must be installed
  - Host certificate checking should be enabled
  - vSphere HA supports both IPv4 and IPv6. A cluster that mixes the use of both of the protocol versions, however is more likely to result in a network partition

For further information see page 22 of the vSphere Availability documentation

  DRS Requirements

  - Shared Storage
    - Storage can be either SAN or NAS
  - Shared VMFS volumes
    - Place the disks of all virtual machines on VMFS volumes that are accessible by all hosts
    - Set access mode for the shared VMFS to public
    - Ensure the VMFS volumes on source and destination host use volume names, and all virtual machines use those volume names for specifying the virtual disks
  - Processor Compatibility - Processors of both the source and destination host must be of the same vendor (AMD or Intel) and be of the same processor family. This requirement is more for the use of vMotion and allowing a VM to execute its processes from one host to the other. vCenter provides advanced features to make sure that processor compatibility requirements are met:
    - Ehnanced vMotion Compatibility (EVC) - You can use EVC to help ensure vMotion compatibility for the hosts in a cluster. EVC ensures that all hostsin a cluster present the same CPU feature set to virutal machines, even if the actual CPUs on

the hosts differ. This prevents migration with vMotion from failing due to incompatible CPUs.

- CPU Compatibility Masks - vCetner Server compares the CPU features available to a virtual machine with the CPU features of the destination hsot to deterine whether to allow or disallow migrations with vMotion. By applying CPU compatibility mask to individual virtual macines, you can hide certain CPU features from the virtual machine and potentially prevent migrations with vMotion from failing due to incompatible CPUs

For further information see pages 55 thru 56 of the vSphere Resource Management documentation

vMotion Requirements

- The virtual machine configuration file for ESXi hosts must reside on a VMware Virtual Machine File System (VMFS)
- vMotion does not support raw disks or migration of applications clustered using Microsoft Cluster Service (MSCS)
- vMotion requires a private Gigabit Ethernet (minimum) migration network between all of the vMotion enabled managed hosts. When vMotion is enabled on a managed host, configure a unique network identity object for the managed host and connect it to the private migration network
- You cannot use migration with vMotion to migrate a virtual machine that uses a virtual device backed by a device that is not accessible on the destination host
- You cannot use migration with vMotion to migrate a virtual machine that uses a virtual device backed by a device on the client computer

For further information see page 56 of the vSphere Resource Management documentation and pages 119 thru 120 of the vCenter Server and Host Management documentation

- **Verify vMotion/Storage vMotion configuration**

  See above sections for DRS and vMotion requirements. Key areas of focus will be proper networking (VMKernel interface for vMotion), CPU compatability, and shared storage access across all hosts.

- **Verify HA network configuration**
  - On legcacy ESX hosts in the cluster, vSphere HA communications travel over all networks that are designated as service console networks. VMkernel networks are not used by these hosts for vSphere HA communications
  - On ESXi hosts in the cluster, vSphere HA communications, by default, travel over VMkernel networks, except those marked for use with vMotion. If there is only one VMkernel network, vSphere HA shares it with vMotion, if necessary. With ESXi 4.x and ESXi, you must also explicitly enable the Management Network checkbox for vSphere HA to use this network

For further information see page 32 of the vSphere Availability documentation

- **Verify HA/DRS cluster configuration**

  Configuration issues and other errors can occur for your cluster or its hosts that adversely affect the proper operation of vSphere HA. You can monitor these errors by looking at the Cluster Operational Status and Configuration Issues screens, which are accessible in the vSphere Client from the vSphere HA section of the cluster's **Summary** tab.

For further information see page 31 of the vSphere Availability documentation

- **Troubleshoot HA capacity issues**

  To troubleshoot HA capacity issues first be familiar with the three Admission Control Policies:

  - Host failures the cluster tolerates (default) - You can configure vSphere HA to tolerate a specified number of host failures. Uses a "slot" size to display cluster capacity
  - Percentage of cluster resources reserved as failover spare capacity - You can configure vSphere HA to perform admission control by reserving a specific percentage of cluster CPU and memory resources for recovery from host failure
  - Specify failover hosts - You can configure vSphere HA to designate specific hosts as the failover hosts

  Things to look out for when troubleshooting HA issues:

  - Failed or disconnected hosts
  - Over sized VM's with high CPU/memory reservations. This will affect slot sizes
  - Lack of capacity/resources if you using "Specify Failover Hosts", IE not enough hosts set as failovers

See pages 31 thru 33 of the vSphere Troubleshooting documentation that outlines common failover scenarios for each of the three Admission Control Policies. For further reading on the three admission control policies see page 16 thru 21 of the vSphere Availability documentation.

- **Troubleshoot HA redundancy issues**

  Like all other components in a vSphere design, you want design redundancy for clusters HA network traffic. You can go about this one of two ways or both. The use of NIC of teaming (two physical NICs perferably connected to separate physical switches) is the most common method used. This will allow either of the two links to fail and still be able to communicate on the the network. The second option is the setup and creation of a secondary management network. This second interface will need to be attached to a different virtual switch as well as a different subnet as the primary network. This will allow for HA traffic to be communicated over both networks.

- **Interpret the DRS Resource Distribution Graph and Target/Current Host Load Deviation**

  The DRS Resource Distribution Chart is used to display both memory and CPU metrics for

each host in the cluster. Each resource can be displayed in either a percentage or as a size in mega bytes for memory or mega hertz for CPU. In the chart display each box/section represents a VM running on that host and the resources it is currently consuming. The chart is accessed from the Summary tab at the cluster level under the section for VMware DRS. Click the hyperlink for View Resource Distribution Chart.

The target/current host load deviation is a representation of the balance of resources across the hosts in your cluster. The DRS process runs every 5 minutes and analyzes resource metrics on each host across the cluster. Those metrics are plugged in an equeation:

(VM entitlements)/(Host Capacity)

This value returned is what determines the "Current host load standard deviation". If this number is higher then the "Target host load standard deviation" your cluster is imbalanced and DRS will make recommendations on which VM's to migrate to re-balance the cluster.

This is just my basic understanding of how DRS works. For complete down into the weeds explanations I would recommend reading this post as well as this one from Duncan Epping @ Yellow-Bricks.com.

- **Troubleshoot DRS load imbalance issues**

  DRS clusters become imbalanced/overcomitted for several reasons:

  - A cluster might become overcommitted if a host fails
  - A cluster becomes invalid if vCenter Server is unavailable and you power on virtual machines using a vSphere Client connected directly to a host
  - A cluster becomes invalid if hte user redueces the reservation on a parent resource pool while a virtual machine is in the process of failing over
  - If changes are made to hosts or virtual machines using a vSphere Client connected to a host while vCenter Server is unavailable, those changes take effect. When vCenter Server becomes available again, you might find that clusters have turned red or yellow because cluster requirements are not longet met.

See pages 62 thru 66 of the vSphere Resource Management documentation for further information

- **Troubleshoot vMotion/Storage vMotion migration issues**

  For vMotion refer to section above for DRS and vMotion requirements. Make sure all requirements are being met.

  For Storage vMotion be aware of the following requirments and limitations

  - 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 thin-provisioned disks during migration as lang as the destination is not an NFS datastore. If you convert the mapping file, a new virtual disk is created and

the contents of the mapped LUN are copied to this disk. For physical compatibility mode RDMs, you can migrate the mapping file only.
- Migration of virtual machines during VMware Tool installation is not supported
- The host on which the virtual machine is running 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 wth Storage vMotion
- The host on which the virtual machines is running must have access to both the source and target datastore

For further information read pages 119 thru 122 of the vCenter Server and Host Management documentation

- **Interpret vMotion Resource Maps**

  vMotion resource maps provide a visual representation of hosts, datastores, and networks associated with the selected virtual machine

  vMotion resource maps also indicate which hosts in the virtual machine's cluster or datacenter are compatible, it must meet the following criteria

  - Connect to all the same datastores as the virtual machine
  - Connect to all the same networks as the virtual machine
  - Have compatible software with the virtual machine
  - Have a compatible CPU with the virtual machine

For further information see page 144 of the vCenter Server and Host Management documentation

- **Identify the root cause of a DRS/HA cluster or migration issues based on troubleshooting information**

  Use information from above topics to help isolate the issue based on HA/DRS requirements as well pages from the reference documents listed.

<u>Tools</u>

- vSphere Availability guide
- vSphere Resource Management guide
- vSphere Monitoring and Performance guide
- vSphere Troubleshooting guide

Section 7 – Monitor a vSphere Implementation

Objective 7.1 – Monitor ESXi, vCenter Server, and Virtual Machines

Knowledge

- **Describe how Tasks and Events are viewed in vCenter Server**

  View All Tasks

  1. Display the object in the inventory
  2. Display the tasks for a single object or the entire vCenter Server
     - To display the tasks for an object, select the object
     - To display the tasts in the vCenter Server, select the root folder
  3. Click the *Tasks & Events* tab
  4. (Optional) To view detailed information for a task, select the task in the list

  View Events

1. Select the inventory object and click the *Tasks & Events* tab
2. Click *Events*
3. (Optional) Select an event in the list to see the *Event Details*, including a list of related events and errors in the error stack
4. (Optional) Click the icon next to Description to view further details and possible causes of the event

For further information on both viewing events and tasks see pages 101 thru 110 of the *vCenter Server and Host Management* documentation

- **Identify critical performance metrics**

  As you will see listed in the sections below, the critical points to monitor are CPU, memory, networking, and storage.

- **Explain common memory metrics**

Metric	Description
SWR/s and SWW/s	Measured in megabyts, these counters represent the rate at which the ESXi host is swapping memory in from disk (SWR/s) and swapping memory out to disk (SWW/s)
SWCUR	This is the amount of swap space currently used by the virtual machine
SWTGT	This is the amount of swap space that the host expects the virtual machine to use
%SWPWT	This metric represents the percentage of time that the VM is waiting for memory to be swapped in (cpu screen in esxtop/resxtop)

MCTL?	Indicates whether the balloon driver is installed in the virtual machine
MCTLSZ	Amount of physical memory that the balloon driver has reclaimed
MCTLTGT	Maximum amount of memory that the host wants to reclaim via the balloon driver

- **Explain common CPU metrics**

Metric	Description
%USED	Percentage of physical CPU time used by a group of worlds
%RDY	Percentage of time a group was ready to run but was not provided CPU resources
%CSTP	Percentage of time the vCPUs of a virtual machine spent in the co-stopped state, waiting to be co-started
%SYS	Percentage of time spent in the ESX VMkernel on behalf of the world/resource pool

- Explain common network metrics

Metric	Description
MbTX/s	Amount of data transmitted in Mbps
MbRX/s	Amount of data received in Mbps
%DRPTX	Percentage of outbound packets dropped
%DRPRX	Percentage of inbound packets dropped

- Explain common storage metrics

Metric	Description
DAVG	Average amount of time it takes a device to service a single I/O request (read or write)
KAVG	The average amount of time it takes the VMkernel to service a disk operation

GAVG	The total latency seen from the virtual machine when performing an I/O request
ABRTS/S	Number of commands aborted per second

For further information and deeper explanation of these and other metrics to monitor read VMware Communities document *Interpreting esxtop Statisics* as well as Duncan Epping's esxtop blog post

- **Compare and contrast Overview and Advanced Charts**
  - Overview Charts - Display multiple data sets in one panel to easily evaluate different resource statistics, display thumbnail charts for child objects, and display charts for a parent and a child object
  - Advanced Charts - Display more information than overview charts, are configurable, and can be printed or exported to a spreadsheet

- **Configure SNMP for vCenter Server**
  1. If necessary, select *Administration -> vCenter Server Settings* to display the vCenter Server Settings dialog box
  2. If the vCenter Server system is part of a connected group, select the server you want to configure from the *Current vCenter Server* drop-down menu
  3. In the settings list, select *SNMP*
  4. In *Receiver URL*, enter the host name or IP address of the SNMP receiver
  5. In the field next to the Receiver URL field, enter the port number of the receiver
  6. In *Community*, enter the community identifier
  7. Click *OK*

See page 37 of the *vCenter Server and Host Management* documentation for further information

- **Configure Active Directory and SMTP settings for vCenter Server**

  Configure Active Directory

  1. If necessary, select *Administration -> vCenter Server Settings* to display the vCenter Server Settings dialog box
  2. If the vCenter Server system is part of a connected group, select the server you want to configure from the *Current vCenter Server* drop-down menu
  3. In the navigation pane, select *Active Directory*
  4. In *Active Directory Timeout*, enter the timeout interval in seconds for connecting to the Active Directory server
  5. Select *Enable Query Limit* to limit the number of users and groups displayed in the Add Permissions dialog box
  6. In *Users & Groups*, enter the maximum number of users and groups to display

7. Select *Enable Validation* to have vCenter Server periodically check its known users and groups against the Active Directory server
8. In *Validation Period,* enter the number of minutes between instances of synchronization
9. Click *OK* to save your changes and close the dialog box

See page 36 of the *vCenter Server and Host Management* documentation for further information

Configure SMTP Settings

1. If necessary, select *Administration -> vCenter Server Settings* to display the vCenter Server Settings dialog box
2. If the vCenter Server system is part of a connected group, select the server you want to configure from the *Current vCenter Server* drop-down menu
3. In the navigation pane, select *Mail*
4. Enter the SMTP server infromation
5. Enter the sender account information
6. Click *OK*

See page 36 thru 37 of the *vCenter Server and Host Management* documentation for further information

- **Congfigure vCenter Server logging options**
    1. If necessary, select *Administration -> vCenter Server Settings* to display the vCenter Server Settings dialog box
    2. If the vCenter Server system is part of a connected group, select the server you want to configure from the *Current vCenter Server* drop-down menu
    3. In the settings list, select *Logging Options*
    4. From the vCenter Server Logging list select logging options (see chart below)
    5. Click *OK*

Option	Description
None (Disable logging)	Turn off logging
Error (Errors only)	Display only error log entries
Warning (Errors and warnings)	Display warning and error log entries

Info (Normal logging)	Displays information, error, and warning log entries
Verbose (Verbose)	Displays information, error, warning, and verbose log entries
Trivia (Extended verbose)	Displays information, error, warning, verbose, and trivia log entries

See page 37 thru 38 of the *vCenter Server and Host Management* documentation for further information

- **Create a log bundle**
    1. Select *File -> Export System Logs*
    2. If you are connected to vCenter Server, select the object for which you want to export data
    3. If you are connected to vCenter Server, select *Include information from vCenter Server and vSphere Client* to download vCenter Server and vSphere Client log files and host log files, and click *Next*
    4. If the selected host supports manifest drive exports of system log files, select the system log files to collect. Select the specific system log files to download
    5. Select *Gather performance data* to include performance data information in the log files. Click *Next*
    6. Click *Next*
    7. Click *Browse* and specify the location to which to save the log files
    8. Click *Next*
    9. Verify the information in the Summary and click *Finish* to download the log files
    10. If the download fails, click *Retry* to attempt to download the generated bundles again

See page 97 of the *vCenter Server and Host Management* documentation for further information

- **Create/Edit/Delete a Scheduled Task**

    Create a Scheduled Task

    1. In the navigation bar, click *Home -> Management -> Schedule Tasks*
    2. In the toolbar, click *New*
    3. In the Select a Task to Schedule dialog box, select a task and click *OK* to open the wizard for that task
    4. Complete the wizard that opens for the task
    5. Click *OK* to open the Scheduled Task wizard
    6. Enter a task name and task description and click *Next*
    7. Select a *Frequency* and specify a *Start Time*
    8. Click *Next*

9. Set up email notifications and click *Next*
10. Click *Finish*

Remove a Scheduled Task

1. In the vSphere Client navigation bar, click *Home -> Management -> Scheduled Tasks*
2. Select the task
3. Select *Inventory -> Scheduled Task -> Remove*
4. Click *OK*

Edit a Scheduled Task

1. In the vSphere Client navigation bar, click *Home -> Management -> Scheduled Tasks*
2. Select the task
3. In the toolbar, click *Properties*
4. Change task attributes as necessary
5. Click *Next* to advance through the wizard
6. Click *Finish*

See pages 101 thru 106 of the *vCenter Server and Host Management* documentation for further information

- **Configure/View/Print/Export resource maps**

  View vCenter Maps

  1. Display the object in the inventory
  2. Select the object and click the *Maps* tab

  Print vCenter Maps

  1. Select *File -> Print Maps -> Print*
  2. In the printer *Name* list, select the printer
  3. Click *Print*

  Export vCenter Maps

  1. If necessary, view the resource map
  2. Select *File -> Export -> Export Maps*
  3. Navigate to the location to save the file
  4. Type a name for the file and select a file format
  5. Click *Export*

See pages 143 thru 146 of the *vCenter Server and Host Management* documentation for further information

- **Start/Stop/Verify vCenter Server service status**

Start vCenter Server service

1. Go to the Services console for your version of Windows
2. Right-click the vCenter Server service and select *Properties*
3. In the VMware vCenter Server Services Properties dialog box, click the *General* tabe and view the service status

Restart vCenter Server service

1. Got to the Services console for your version of Windows
2. Right-click *VMware vCenter Server,* select *Start*, and wait for the startup to complete
3. Close the Properties dialog box

Stop vCenter Server service

1. Go to the Services console for your version of Windows
2. Click *VMware vCenter Server Service*
3. Right-click *VMware vCenter Server*, select *Stop*, and wait for it to stop
4. Close the Properties dialog box

See page 112 of the *vCenter Server and Host Management* documentation for further information

- **Start/Stop/Verify ESXi host agent status**

1. Shut down all virtual machines running on the ESXi host
2. Select the ESXi host you want to shut down
3. From the main or right-click menu, select *Reboot* or *Shut Down*
4. Provide a reason for the shut down

See page 111 of the *vCenter Server and Host Management* documentation for further information

- **Configure vCenter Server timeout settings**
    1. If necessary, select *Administration -> vCenter Server Settings* to display the vCenter Server Settings dialog box
    2. If the vCenter Server system is part of a connected group, select the server you want to configure from the *Current vCenter Server* drop-down menu
    3. In the settings list, select *Timeout Settings*
    4. In *Normal Operations,* enter the timeout interval in seconds for normal operations
    5. In *Long Operations*, enter the tiemout interval in minutes for long operations
    6. Click *OK*
    7. Restart the vCenter Serve system for the changes to take effect

See page 38 of the *vCenter Server and Host Management* documentation for further information

- **Monitor/Administer vCenter Server connections**

View Active Sessions

1. From the *Home* page of a vSphere Client connected to a vCenter Server system, click the *Sessions* button

Terminate Active Sessions

1. On the *Home* page of a vSPhere Client connected to a vCenter Server system, click the *Sessions* button
2. Right-click a session and select *Terminate*
3. Click *OK* to confirm the termination

Send a Message to All Active Users

1. On the *Home* page of a vSphere Client connected to a vCenter Server system, click the *Sessions* button
2. Type a message in the *Message of the day* field
3. Click *Change*

See page 28 thru 29 of the *vCenter Server and Host Management* documentation for further information

- **Create an Advanced Chart**
    1. Select an inventory object and click the *Performance* tab
    2. Click *Advanced*
    3. Click *Chart Options*
    4. Select a metric group for the chart
    5. Select a time range for the metric group
    6. Select the chart type
    7. In Objects, select the inventory objects to display in the chart
    8. In Counters, select the data counters to display in the chart
    9. Click *Apply*
    10. Click *OK*

See page 14 of the *vSphere Monitoring and Performance* documentation for further information

- **Determine host performance using resxtop and guest Perfmon**
- **Given performance data, identify the affected vSphere resource**

These two topics could easily fill pages of information. For quick and easy knowledge refer to the sections above outlining the more significant performance metrics to monitor. Read chapter 7 of the *vSphere Monitoring and Performance* documentation as well as Duncan Epping's esxtop blog and the VMware Communities document "Interpreting esxtop Statistics". One final note, if you don't have one already create a VMworld account and view "Troubleshooting using ESXTOP for Advanced Users", session TA6720 from VMworld 2010.

<u>Tools</u>

- vCenter Server and Host Management guide
- vSphere Resource Management guide

- vSphere Monitoring and Performance guide

Objective 7.2 – Create and Administer vCenter Server Alarms

Knowledge

- **List vCenter default utilization alarms**

Alarm	Description
Virtual machine memory usage	Default alarm to monitor virtual machine memory usage
Virtual machine cpu usage	Default alarm to monitor virtual machine cpu usage
Datastore usage on disk	Default alarm to monitor datastore disk usage
Host memory usage	Default alarm to monitor host memory usage
Host cpu usage	Default alarm to monitor host cpu usage

List courtesy of the *Alarms* tab at the root of vCenter

- **List vCenter default connectivity alarms**

Alarm	Description
Cannot connect to storage	Default alarm to monitor host connectivity to storage device
Host connection and power state	Default alarm to monitor host connection and power state
Host connection failure	Default alarm to monitor host connection failure

Network connectivity lost	Default alarm to monitor network connectivity on a virtual switch
Network uplink redundancy degraded	Default alarm to monitor network uplink redundancy degradation on a virtual switch
Network uplink redundancy lost	Default alarm to monitor loss of network uplink redundancy on a virtual switch

List courtesy of the *Alarms* tab at the root of vCenter

- **List possible actions for utilization and connectivity alarms**

  Host related actions

  - Send a notification email
  - Send a notification trap
  - Run a command
  - Enter maintenance mode
  - Exit maintenance mode
  - Enter standby
  - Exit standby
  - Reboot host
  - Shutdown host

  VM related actions

  - Send a notification email
  - Send a notification trap
  - Run a command
  - Power on VM
  - Power off VM
  - Suspend VM
  - Reset VM
  - Migrate VM
  - Reboot guest on VM
  - Shutdown guest on VM

- **Create a vCenter utilization alarm**

  For this excercise we are going to create a host alarm based on network utilization

  1. From the root object in vCenter select the *Alarms* tab
  2. Select the *Definitions* tab next to *View*
  3. In the right hand, right click in open a space and select *New Alarm*
  4. In the *General* tab give the alarm a *Name*, *Description,* and select *Hosts* from the *Alarm Type* drop down.

5. Select the *Triggers* tab
6. Right click in the open space and select *Add Trigger*
7. Click the trigger type to display the list of available triggers
8. From the list select *Host Network Usage (kbps)*
9. For the *Warning* and *Alert* values select what is appropriate for your environment
10. Click the *Actions* tab
11. Right click in the open space and select *Add Action*
12. Select *Send a notification email*
13. Under the *Configuration* column input your email address
14. Leave the default setting to email when going from a warning state to an alert state
15. Click *OK*

- **Create a vCenter connectivity alarm**

  For this exercise we are going to create a host alarm based on lost storage path redundancy

  1. From the root object in vCenter select the *Alarms* tab
  2. Select the *Definitions* tab next to *View*
  3. In the right hand, right click in open a space and select *New Alarm*
  4. In the *General* tab give the alarm a *Name, Description,* and select *Hosts* from the *Alarm Type* drop down.
  5. Select *Monitor for specific events occuring on this object, for example, VM powered on*
  6. Select the *Triggers* tab
  7. Right click in the open space and select *Add Trigger*
  8. Click the trigger type to display the list of available triggers
  9. From the list select *Lost Network Redundancy*
  10. Click the *Actions* tab
  11. Right click in the open space and select *Add Action*
  12. Select *Send a notification email*
  13. Under the *Configuration* column input your email address
  14. Leave the default setting to email when going from a warning state to an alert state
  15. Click *OK*

- **Configure alarm triggers**

  See sections above *Create a vCenter Connectivity* Alarm and *Create a vCenter Utilization Alarm*. Also review pages 33 thru 39 of the *vSphere Monitoring and Performance* documentation.

- **Configure alarm actions**

  See sections above *Create a vCenter Connectivity* Alarm and *Create a vCenter Utilization Alarm*. Also review pages 33 thru 39 of the *vSphere Monitoring and Performance* documentation.

- **For a give alarm, identify the affected resource in vSphere implementation**

  If using any of the default vCenter alarms the alarm name as well as the alarm description should identify which resource is being affected.

Tools

- vCenter Server and Host Management guide
- vSphere Resource Management guide
- vSphere Monitoring and Performance guide

VMware vSphere Examples and Scenarios guid