

---

# THE UNOFFICIAL OFFICIAL VCAP5-DCA STUDY GUIDE

---

By Jason Langer and Josh Coen



[HTTP://WWW.VIRTUALLANGER.COM](http://www.virtuallanger.com)  
[HTTP://WWW.VALCOLABS.COM](http://www.valcolabs.com)

## Contents

VCAP5-DCA Objective 1.1 – Implement and Manage Complex Storage Solutions .....	2
VCAP5-DCA Objective 1.2 – Manage Storage Capacity in a vSphere Environment.....	31
VCAP5-DCA Objective 1.3 – Configure and Manage Complex Multipathing and PSA Plug-ins .....	49
VCAP-DCA 5 Objective 2.1–Implement & Manage Complex Virtual Networks.....	60
VCAP-DCA 5 Objective 2.2 – Configure & Maintain VLANs, PVLANS, & VLAN Settings .....	65
VCAP-DCA 5 Objective 2.3 – Deploy & Maintain Scalable Virtual Networking.....	69
VCAP-DCA 5 Objective 2.4–Administer vNetwork Distributed Switch Settings .....	72
VCAP5-DCA-Objective 3.1–Tune and Optimize vSphere Performance .....	76
VCAP5-DCA-Objective 3.2–Optimize Virtual Machine Resources .....	88
VCAP5-DCA–Objective 3.3 – Implement and Maintain Complex DRS Solution.....	100
VCAP5-DCA – Objective 3.4 – Utilize Advanced vSphere Performance Monitoring Tools .....	122
VCAP5-DCA Objective 4.1–Implement and Maintain Complex VMware HA Solutions.....	133
VCAP5-DCA Objective 4.2-Deploy and Test VMware FT.....	151
VCAP-DCA 5 Objective 5.1–Implement and Maintain Host Profiles.....	161
VCAP-DCA 5 Objective 5.2 – Deploy and Manage Complex Update Manager Environments .....	167
VCAP5-DCA – Objective 6.1 – Configure, Manage, and Analyze vSphere Log Files.....	175
VCAP5-DCA – Objective 6.2 – Troubleshoot CPU and Memory Performance.....	188
VCAP5-DCA – Objective 6.3 – Troubleshoot Network Performance and Connectivity .....	192
VCAP5-DCA – Objective 6.4 – Troubleshoot Storage Performance and Connectivity.....	196
VCAP5-DCA – Objective 6.5 – Troubleshoot vCenter Server and ESXi Host Managemen.....	200
VCAP-DCA 5 Objective 7.1– Secure ESXi Hosts .....	204
VCAP-DCA 5 Objective 7.2–Configure and Maintain the ESXi Firewall.....	213
VCAP-DCA5 Objective 8.1 – Execute VMware Cmdlets and Customize Scripts Using PowerCLI.....	218
VCAP-DCA 5 Objective 8.2–Administer vSphere Using the vSphere Management Assistant .....	224
VCAP-DCA 5 Objective 9.1–Install ESXi Server with Custom Settings.....	233
VCAP-DCA 5 Objective 9.2 – Install ESXi Hosts Using Auto Deploy .....	237

# VCAP5-DCA Objective 1.1 – Implement and Manage Complex Storage Solutions

For this objective I used the following documents:

- [Best Practices for NFS on vSphere White Paper](#)
- Documents listed in the Tools section

## ***Objective 1.1 – Implement and Manage Complex Storage Solutions***

### Knowledge

**\*\*ITEMS IN BOLD ARE TOPICS PULLED FROM THE BLUEPRINT\*\***

- **Identify RAID Levels**
  - If you are looking at this blueprint and contemplating taking this exam I'm going to assume that you know what RAID is. If you don't, then you are possibly in for a LONG VCAP5-DCA preparation. I'm not going to list out every single RAID level, but I will go over the most commonly used ones; RAID 0, 1, 5, 6 and 1+0
    - RAID 0: Striping only, no redundancy. Data is striped over all disks in a RAID 0 set. Minimum of 2 disks.
      - Pros:
        - Very good performance
        - Allows for the maximum use of disk space
      - Cons
        - No redundancy
        - Any drive failure will destroy the entire dataset
    - RAID 1: Mirroring only, no striping. Data is mirrored across disks. If you have a two disk RAID 1 set then the same data is on both disks. Minimum of 2 disks.
      - Pros:
        - Redundant
        - Write performance degradation is minima
      - Cons:
        - You lose half of your disk capacity (two 1TB disks, 2TB total only nets you 1TB)
    - RAID 5: Striping with parity. Data is striped across the all disks in the RAID 5 set and parity bits are distributed across the disks. Minimum of 3 disks
      - Pros:

- Can sustain a loss of 1 drive in the set
    - Very good read performance
  - Cons:
    - Write performance not as good as RAID 1 due to parity calculation
    - Throughput is degraded when a disk does fail
- RAID 6: Striping with double parity. Data is striped across all disks in the RAID 6 set along with double parity. Minimum of 4 disks
  - Pros:
    - Can sustain a loss of 2 drives in the set
    - Useful in large RAID sets
    - Very good read performance
  - Cons:
    - Requires 4 disks
    - More disk space is utilized for the extra parity
    - Write performance not as good as RAID 1 or 5 due to double parity calculation
- RAID 1+0 (RAID 10): Mirroring and Striping. Disks in a RAID 10 set are mirrored and then striped across more disks. Minimum of 4 drives and total drives must be an even number
  - Pros:
    - Great read/write performance
    - Can survive many drive failures as long as all drives in a mirror don't fail
  - Cons:
    - Only 50% of disk capacity is available due to mirroring
    - Complex compared to RAID 0 and RAID 1

- **Identify Supported HBA types**

- The three types of Host Bus Adapters (HBA) that you can use on an ESXi host are Ethernet (iSCSI), Fibre Channel or Fibre Channel over Ethernet (FCoE). In addition to the hardware adapters there is software versions of the iSCSI and FCoE adapters (software FCoE is new with version 5) are available.
- There are far too many adapters to list, but the usual suspects make them:
  - Broadcom

- Brocade
- Cisco
- Emulex
- QLogic
- To see all the results search [VMware's compatibility guide](#)

- **Identify virtual disk format types**

- There are three types of virtual disk formats:
  1. Thick Provision Lazy Zeroed – a thick disk is created and all space on the underlying storage is allocated upon creation. The blocks within the allocated space are zeroed out on demand (not at the time of virtual disk creation)
  2. Thick Provision Eager Zeroed – a thick disk is created and all space on the underlying storage is allocated upon creation. The blocks within the allocated space are zeroed out up front – it will take some time (considerable amount of time depending on disk size) to create this type of virtual disk
  3. Thin Provisioned – Only space that is needed is allocated to these types of disks. As the need for more physical space grows a thin provisioned disk will grow to meet that demand, but only up to its configured size
- Using a Raw Device Mapping (RDM) may also be considered a virtual disk format type. While I don't consider it a virtual disk format, I wanted to include it anyway. A RDM is a pointer to a physical LUN on a SAN. When you create a RDM a .vmdk file is created, but only contains pointer to the physical LUN

#### Skills and Abilities

- **Determine use cases for and configure VMware DirectPath I/O**

- DirectPath I/O allows a VM to access a device on the physical server without intervention from the hypervisor
- The CPUs must have Intel Virtualization Technology for Directed I/O (Intel VT-d) feature or if using AMD processors, have AMD I/O Virtualization Technology (IOMMU). Once you verify your CPUs are capable, ensure the feature is enabled within the BIOS
- According to test results done by VMware in a recent performance whitepaper, [Network I/O Latency in vSphere 5](#), using DirectPath I/O lowered the round trip time by 10 microseconds.

While 10 microseconds may seem miniscule, it can be the difference with very low latency applications

- A few use cases:
  - Stock Market applications (an example used in the aforementioned white paper)
  - A legacy application that may be bound to the physical device
  - Can improve CPU performance for applications with a high packet rate
- Configuring DirectPath I/O on the ESXi host (from [VMware KB 1010789](#))
  - In the vSphere client select a host from the inventory > click the *Configuration* tab > click *Advanced Settings* under the *Hardware* pane
  - Click *Edit* and select the device(s) you want to use > click *OK*
  - Reboot the host (once the reboot is complete the devices should now appear with a green icon)
- Configuring a PCI Device (Direct Path I/O) on a Virtual Machine (from [VMware KB 1010789](#))
  - In the vSphere client right-click the virtual machine you want to add the PCI device to and click *Edit Settings...*
  - Click the *Hardware* tab > click *Add*
  - Choose the PCI device > click *Next*
- **Determine requirements for and configure NPIV**
  - N-Port ID Virtualization (NPIV) is used to present multiple World Wide Names (WWN) to a SAN network (fabric) through one physical adapter. NPIV is an extension of the Fibre Channel protocol and is used extensively on converged platforms (think Cisco UCS)
  - Here are a list of requirements you must meet in order to use NPIV
    - The Fibre Channel switches must support NPIV
    - The physical HBAs in your hosts must support NPIV
      - vMotioning a virtual machine configured with NPIV to a host whose physical HBA does not support NPIV will revert to using the WWN of the physical HBA
    - Heterogeneous HBAs across physical hosts is not supported
    - The physical HBAs must have access to the LUNs that will be accessed by the NPIV-enabled virtual machines

- Ensure that the NPIV LUN ID at the storage layer is the same as the NPIV target ID
  - Guest NPIV only works with Fibre Channel switches
  - NPIV does not support Storage vMotion
  - Unfortunately I don't have an environment that I can go through and document for you the step-by-step process. The steps below are from the vSphere 5 Storage Guide
  - Configuring NPIV
    - Open the New Virtual Machine wizard.
    - Select Custom, and click Next.
    - Follow all steps required to create a custom virtual machine.
    - On the Select a Disk page, select Raw Device Mapping, and click Next.
    - From a list of SAN disks or LUNs, select a raw LUN you want your virtual machine to access directly.
    - Select a datastore for the RDM mapping file
    - Follow the steps required to create a virtual machine with the RDM.
    - On the Ready to Complete page, select the Edit the virtual machine settings before completion check box and click Continue. The Virtual Machine Properties dialog box opens.
    - Assign WWNs to the virtual machine.
      - Click the Options tab, and select Fibre Channel NPIV.
      - Select Generate new WWNs.
      - Specify the number of WWNNs and WWPNS.
        - A minimum of 2 WWPNS are needed to support failover with NPIV. Typically only 1 WWNN is created for each virtual machine.
    - Click Finish.
- **Determine appropriate RAID level for various Virtual Machine workloads**
  - Earlier in this objective I covered different RAID levels and their respective advantages/disadvantages. Now lets discuss where these RAID levels fit in best with different workloads
  - Typically when your workloads are read intensive it is best to use RAID 5 or RAID 6. When the workload is write intensive you want to use RAID 1 or RAID 1+0. Hopefully the

application owner can give you the read/write percentages so that you can determine which RAID level is best.

- Here's an example:
  - Formula:  $(\text{total required IOPs} * \text{read}\%) + (\text{total required IOPs} * \text{write}\% * \text{RAID penalty}) = \text{total IOPs required}$
  - 400 IOPs required
  - 35% read
  - 65% write
  - RAID1 =  $(400 * 0.35) + (400 * 0.65 * 2) = 660$  IOPs
    - 15K disks required = 4
    - 10K disks required = 5
    - 7.2 disks required = 9
  - RAID5 =  $(400 * 0.35) + (400 * 0.65 * 4) = 1180$  IOPs
    - 15K disks required = 7
    - 10K disks required = 9
    - 7.2 disks required = 16
  - RAID6 =  $(400 * 0.35) + (400 * 0.65 * 6) = 1700$  IOPs
    - 15K disks required = 10
    - 10K disks required = 14
    - 7.2 disks required = 23
- As you can see, the number of disks required depends on the RAID level you choose. So when determining which RAID level to choose, you need to factor in the number of disks you have against the level of protection you will provide. Each of the above RAID levels can meet the IOPs required for the workload, but some require more disks dependent upon the RAID level and type of disks.
- In the above example I would go with RAID 5 on 15K disks. While RAID 1 would only require 4 disks to meet the IOPs requirement, it may actually require more disks because you lose 50% capacity in any give RAID 1 set.
- A tool built-in to ESXi that can be VERY useful in determining the I/O characteristics of a virtual machine workload is **vscsiStats**. I'm not going to go into real detail here as to how exactly to interpret the statistics is pulls, but will provide you with the basics and a super AWESOME blog that really goes into detail and even provides some templates



- you can run **vscsiStats** from anywhere within the shell (console or SSH), but keep in mind that the first “S” in “Stats” is capitalized
- To get going, here is the commands you will run to start, along with an explanation of each paramter

```

1
2 # find the world ID for the VM you want to collect statistics on
3 vscsiStats -l
4
5 # this will start the collection. -s tells it to start and -w specifies the world ID
6 vscsiStats -s -w 466937
7
8 # here is what should be returned after entering the command above
9 # "vscsiStats: Starting Vscsi stats collection for worldGroup 466937, handleID 8207 (
10 # "Success."
11
12 # after this runs for a period of time you need to pull what's been collected using t
13 # for the world ID and -p <stat> for the stat you want to pull (-p can be ioLength, s
14 # latency, interarrival and all. Use the -c parameter to specify a csv format
15 vscsiStats -w 466937 -p all -c
16
17 # once you're done you want to stop the collection
18 vscsiStats -x
19

```

- If you want to learn how to interpret these results check out Erik Zandboer's [three-part series](#), it is definitely a useful resource

- **Apply VMware storage best practices**

- Best practices for storage and vSphere will always require a look at your storage vendor's documentation as it will differ across platforms. However, from the vSphere side we can apply general best practices regardless of the underlying storage platform
- Best Practices for Fibre Channel Storage
  - First and foremost you should document the environment
    - includes software versions, zoning LUN masking, etc...
  - Only one VMFS datastore per LUN
  - Disable automatic host registration
    - GUI – Modify *Advanced Settings* > *Disk* > *Disk.EnableNaviReg* = 0



- the **esxcli** way

```
1 esxcli system settings advanced set -i=0 -o "/Disk/EnableNaviReg"
```

- Use read/write caching on the array
  - ensure non-ESXi hosts are not accessing the same LUNs or physical disks as your ESXi hosts
  - Ensure you have paths to all storage processors for proper load balancing and redundancy
  - Enable Storage I/O Control (SIOC)
  - Ensure you design your storage with proper IOPs in mind (see above section on identifying proper RAID levels)
  - use a dual redundant switching fabric
  - match all queue depths across the application, guest OS, ESXi host, HBA and storage array
- Best Practices for iSCSI
    - Document the environment
    - Use on one VMFS datastore per LUN
    - Enable read/write cache on the array
    - only ESXi hosts should be accessing the LUN(s) and underlying physical disks
    - Ensure each ESXi hosts has the appropriate number of network adapters to handle throughput for iSCSI traffic
    - Bind multiple network adapters to the iSCSI software adapter for redundancy
    - match all queue depths across the application, guest OS, ESXi host and storage array
    - separate uplinks on the physical switch so they are not using the same buffers
    - Ensure you don't have Ethernet bottle necks going to your storage (or anywhere for that matter)
    - Isolate storage traffic to its own VLAN if possible
    - Enable Storage I/O Control (SIOC)
  - Best Practices for NFS
    - Isolate storage traffic to its own VLAN if possible

- Enable Storage I/O Control (SIOC)
- Mount all NFS exports the same across all hosts
- If you increase the max number of NFS mounts for a hosts, be sure to also increase the heap size accordingly
  - Increase Max NFS volumes through the GUI
    - Modify *Advanced Settings > NFS > NFS.MaxVolumes*
  - The **esxcli** way

```
1 esxcli system settings advanced set -i=32 -o "/NFS/MaxVolumes"
```

- Increase the TCP Heap Size through the GUI (**changing the heap size requires a reboot of the ESXi host**)
  - Modify *Advanced Settings > Net > Net.TcpipHeapSize*
- The **esxcli** way

```
1 esxcli system settings advanced set -i=16 -o "/Net/TcpipHeapSize"
```

- **Understand the use cases for Raw Device Mapping**

- In order to understand why you would use a Raw Device Mapping (RDM), we need to define it. “An RDM is a mapping file in a separate VMFS volume that acts as a proxy for a raw physical storage device” – *vSphere Storage Guide*
- RDMs come in two flavors; physical compatibility mode and virtual compatibility mode
  - Physical compatibility mode:
    - The VMkernel passes all SCSI commands to the mapped device with the exception of the REPORT LUNs command. This command is virtualized so that the VMkernel can isolate the mapped device to whichever virtual machine owns it
    - Can be greater than 2TB in size (assumes VMFS5)
  - Virtual compatibility mode:
    - Unlike physical compatibility mode, virtual mode will only pass the READ and WRITE command to the mapped device, all other SCSI commands are handled by the VMkernel
    - Cannot be greater than 2TB
- There are certain scenarios in which you don't have a choice but to use RDMs:
  - When using Microsoft Clustering Services across physical hosts. Any cluster data disks and quorum disks should be configured as a RDM

- If at any point you want to use N-Port ID Virtualization (NPIV) within the guest you will need to use a RDM
- If you need to run SAN management agents inside a virtual machine
- To fully understand the use cases for RDMs you must also know their limitations
  - Virtual machine snapshots are only available when using a RDM in virtual compatibility mode
  - You can't map to a certain partition on a device, you must map to the entire LUN
  - You cannot use direct attached storage devices to create a RDM (direct attached devices do not export the SCSI serial number, which is required for a RDM)
- Now that you have read what a RDM is, the available modes, when you MUST use them and what some of their limiting factors are you can start to narrow down the use cases. To further assist you here is a table from the vSphere Storage Guide that outlines the feature sets when using VMFS, virtual RDM and physical RDM

ESXi Features	Virtual Disk File	Virtual Mode RDM	Physical Mode RDM
SCSI Commands Passed Through	No	No	Yes REPORT LUNs is not passed through
vCenter Server Support	Yes	Yes	Yes
Snapshots	Yes	Yes	No
Distributed Locking	Yes	Yes	Yes
Clustering	Cluster-in-a-box only	Cluster-in-a-box cluster-across-boxes	Physical-to-virtual clustering cluster-across-boxes
SCSI Target-Based Software	No	No	Yes

- **Configure vCenter Server storage filters**

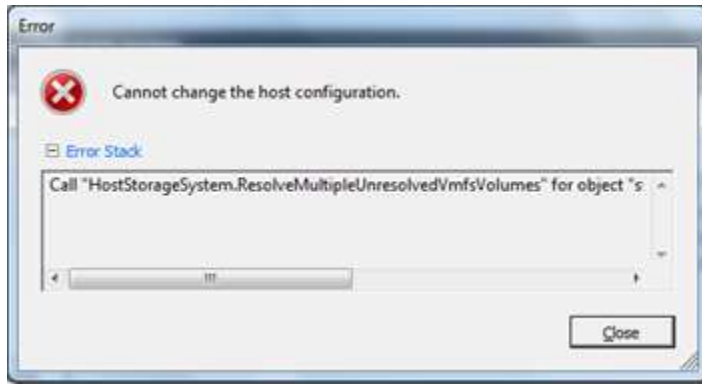
- There are four different storage filters that can be configured; VMFS Filter, RDM Filter, Same Host and Transports Filter and the Host Rescan Filter. If you don't know what these are, here is a quick explanation:
  - **VMFS Filter:** filters out storage devices or LUNs that are already used by a VMFS datastore

- **RDM Filter:** filters out LUNs that are already mapped as a RDM
- **Same Host and Transports Filter:** filters out LUNs that can't be used as a VMFS datastore extend.
  - Prevents you from adding LUNs as an extent not exposed to all hosts that share the original VMFS datastore.
  - Prevents you from adding LUNs as an extent that use a storage type different from the original VMFS datastore
- **Host Rescan Filter:** Automatically rescans and updates VMFS datastores after you perform datastore management operations
- You create these filters from vCenter through *Administration > vCenter Server Settings... > Advanced Settings*. From here you enter in a new *Key/Value* pair and click the *Add* button
- Once those settings are added there are a few different places you can view them:
  - within the *Advanced Settings* window of where you added them
  - The *vpxd.cfg* file on your vCenter server (C:\ProgramData\VMware\VMware VirtualCenter)
    - located between the `<filter></filter>` tags
  - you can also view the *vpxd.cfg* file from the ESXi host itself (*/etc/vmware/vpxa*)
- All storage filters are enabled by default. To disable them set the following keys to *false*

VMFS Filter	config.vpxd.filter.vmfsFilter
RDM Filter	config.vpxd.filter.rdmFilter
Same Hosts and Transports Filter	config.vpxd.filter.SameHostAndTransportsFilter
Host Rescan Filter	config.vpxd.filter.hostRescanFilter

- Here is a short video of Configuring vCenter Server Storage Filters
- **Understand and apply VMFS resignaturing**
  - VMFS resignaturing occurs when you you are trying to mount a new LUN to a host that already has a VMFS datastore on it. You have three options when mounting a LUN to an ESXi host with an existing VMFS partition; *Keep the existing signature*, *Assign a new signature* and *Format the disk*. Here is a brief description of each of those options

- *Keep the existing signature*: Choosing this option will leave the VMFS partition unchanged. If you want to preserve the VMFS volume (keep the existing UUID), choose this option. This is useful when you are doing LUN replication to a DR site and need to mount the cloned LUN – MUST BE WRITABLE
  - *Assign a new signature*: Choosing this option will delete the existing disk signature and replace it with a new one. You MUST use this option (or the format option) if the original VMFS volume is still mounted (you can't have two separate volumes with the same UUID mounted simultaneously). During resignaturing a new UUID and volume label are assigned, which consequently means that any virtual machines that are registered on this VMFS volume must have their configuration files updated to point to the new name/UUID or the virtual machines must be removed/re-added back to the inventory
  - *Format the disk*: Nothing much new here; choosing this option is the same as creating a new VMFS volume on a blank LUN – - ALL EXISTING DATA WILL BE LOST
- There are two way that you can add an LUN with an existing VMFS volume to a host; through the GUI and through the command line. The following assumes your host has access to the LUN on the array side:
  - Adding a LUN with an Existing VMFS Volume using the GUI
    1. From within the vSphere client, either connect to vCenter or directly to a host, navigate to the Hosts and Clusters view: *Home > Hosts and Clusters* (or *Ctrl + Shift + H*)
    2. Select the host you want to add the LUN to on the right > select the *Configuration* tab
    3. Click on the *Storage Hyperlink*
    4. Click the *Add Storage...* hyperlink in the upper right
    5. Select *Disk/LUN* > click *Next*
    6. Select the appropriate LUN > click *Next*
    7. Select one of the aforementioned options (*Keep the existing signature*, *Assign a new signature* or *Format the disk*)
    8. Click *Finish*
    9. If you are connected to vCenter you may receive the following error during this process



- i. Check out VMware [KB1015986](https://kb.vmware.com/kb/1015986) for a workaround (connect directly to the host and add the LUN)

- o Adding a LUN with an Existing VMFS Volume using **esxcli**
  1. SSH or direct console to the ESXi host that you want to add the LUN with the existing VMFS volume to — You can also connect to a vMA instance and run these commands
  2. Once connected you need to identify the ‘snapshots’ (which volumes have an existing VMFS volume on it)

01  
02  
03  
04  
05  
06  
07  
08  
09  
10

```
# This will list the snapshots that are available
esxcli storage vmfs snapshot list

# Mount a snapshot named 'replicated_lun' and keep the existing signature (find the s
# to mount using the output from the previous command
esxcli storage vmfs snapshot mount -l 'replicated_lun'

# Mount a snapshot named 'replicated_lun' and assign a new signature (find the snapsh
# to mount using the output from the first command
esxcli storage vmfs snapshot resignature -l 'replicated_lun'
```

- o Here is a video showing you how to mount a VMFS volumes that has an identical UUID as another volume. It will show you how to mount a volume while keeping the existing signature and by applying a new signature; all using **esxcli** – Enjoy!

- **Understand and apply LUN masking using PSA-related commands**

- o LUN masking gives you control over which hosts see which LUNs. This allows multiple hosts to be connected to a SAN with multiple LUNs while allowing only hosts that you specify to see a particular LUN(s). The most common place to do LUN masking is on the back-end storage array. For example, an EMC Clariion or VNX provides LUN masking by way of

Storage Groups. You add hosts and LUNs to a storage group and you have then essentially “masked” that host to only seeing those LUNs.

- Now that we have a better idea of what LUN masking is, let’s go into an example of how you would actually do this on an ESXi host.
- The first thing we need to do is identify which LUN we want to mask. To do this:
  - **esxcfg-scsidevs -m** — the -m will display only LUNs with VMFS volumes, along with the volume label. In this example we are using the “vmfs\_vcap\_masking” volume”

```
/sbin #  
/sbin # esxcfg-scsidevs -m  
t10.ATA_____TOSHIBA_MK3252GSX_____  
0 vlabs-vmhost04_vmfs01  
naa.5000144ff548121b:1  
0 vlabs-px300_iscsi_vmfs02  
naa.5000144fd4b74168:1  
0 vmfs_vcap_masking  
/sbin #
```

- Now that we see the volume we want, we need to find the device ID and copy it (starts with “naa.” In this example our device ID is **naa.5000144fd4b74168**
- We have the device ID and now we have to find the path(s) to that LUN
  - **esxcfg-mpath -L | grep naa.5000144fd4b74168** — the -L parameter gives a compact list of paths

```
/sbin # esxcfg-mpath -L | grep naa.5000144fd4b7416  
vmhba35:C0:T1:L0 state:active naa.5000144fd4b74168 vmhba35  
vmhba35:C2:T1:L0 state:active naa.5000144fd4b74168 vmhba35  
/sbin #
```

- We now see there are two paths to my LUN, which are **C0:T1:L0** and **C2:T1:L0**
- Knowing what are paths are we can now create a new claim rule, but first we need to see what claim rules exist in order to not use an existing claim rule number
  - **esxcli storage core claimrule list**



```

/sbin # esxcli storage core claimrule list
Rule Class      Rule  Class  Type      Plugin
-----
MP           0  runtime  transport  NMP
MP           1  runtime  transport  NMP
MP           2  runtime  transport  NMP
MP           3  runtime  transport  NMP
MP           4  runtime  transport  NMP
MP          101  runtime  vendor     MASK_PATH
MP          101  file     vendor     MASK_PATH
MP          65535  runtime  vendor     NMP
/sbin # █

```

- We can use any rule numbers for our new claim rule that isn't in the list above. We'll use **500**. Now let's create the new claim rule for the first path; **C0:T1:L0** which is on adapter **vmhba35**
  - **esxcli storage core claimrule add -r 500 -t location -A vmhba35 -C 0 -T 1 -L 0 -P MASK\_PATH** — you know the command succeeded if you don't get any errors.
- Masking one path to a LUN that has two paths will still allow the LUN to be seen on the second path, so we need to mask the second path as well. This time we'll use **501** for the rule number and **C2:T1:L0** as the path. The adapter will still be **vmhba35**
  - **esxcli storage core claimrule add -r 501 -t location -A vmhba35 -C 2 -T 1 -L 0 -P MASK\_PATH** — you know the command succeeded if you don't get any errors.
- Now if you run **esxcli storage core claimrule list** again you will see the new rules, **500** and **501** but you will notice the *Class* for those rules show as **file** which means that it is loaded in **/etc/vmware/esx.conf** but it isn't yet loaded into runtime. Let's load our new rules into runtime
  - **esxcli storage core claimrule load**
  - Now run **esxcli storage core claimrule list** and this time you will see those rules displayed twice, once as the **file Class** and once as the **runtime Class**

```

MP          500  runtime  location  MASK_PATH
MP          500  file     location  MASK_PATH
MP          501  runtime  location  MASK_PATH
MP          501  file     location  MASK_PATH

```

- Only one more step left. Before those paths can be associated with the new plugin (MASK\_PATH), they need to be disassociated from the plugin they are currently using. In this case those paths are claimed by the NMP plugin (rule 65535). This next command will unclaim all paths for that device and then reclaim them based on the claimrules in runtime. Again we'll use **naa.5000144fd4b74168** to specify the device
  - **esxcli storage core claiming reclaim -d naa.5000144fd4b74168**
  - After about 30 seconds, if you are watching the storage area on your host within the vSphere client you will see that datastore disappear from the list
  - Running **esxcfg-mpath -L | grep naa.5000144fd4b74168** again will now show 0 paths (before it showed 2)
- Here is a quick list of commands you would need to run if you wanted to unmask those two paths to that LUN and get it to show up again in the vSphere client

```

1  esxcli storage core claimrule remove -r 500
2  esxcli storage core claimrule remove -r 501
3  esxcli storage core claimrule load
4  esxcli storage core claiming unclaim -t location -A vmhba35 -C 0 -T 1 -L 0
5  esxcli storage core claiming unclaim -t location -A vmhba35 -C 2 -T 1 -L 0
6  esxcli storage core adapter rescan -A vmhba35

```

- Here is a pretty awesome video of performing LUN masking using the all powerful **esxcli**
- **Identify and tag SSD devices**
  - There are a few ways that you can identify an SSD device. The easiest way is to look in the storage area (select host > click *Configuration* > click the *Storage* hyperlink) and look at the *Drive Type* column of your existing datastores. This will either say *Non-SSD* or *SSD*

Identification	Status	Device	Drive Type
vlabs-px300_iscsi...	✓ Normal	EMC iSCSI Disk (...)	Non-SSD
vlabs-vmhost04_...	✓ Normal	Local ATA Disk (t...	Non-SSD
vm_backups	✓ Normal	10.90.190.130:/n...	Unknown
vmfs_vcap_maski...	✓ Normal	EMC iSCSI Disk (...)	Non-SSD

- o Now you can only use the previous method if you already have a datastore mounted on that LUN. If you don't, SSH into your host and let's use **esxcli** to figure out which devices are SSDs

- **esxcli storage core device list**

```

- # esxcli storage core device list
naa.5000144f60f4627a
  Display Name: EMC iSCSI Disk (naa.
  Has Settable Display Name: true
  Size: 10240
  Device Type: Direct-Access
  Multipath Plugin: NMP
  Devfs Path: /vmfs/devices/disks/na
  Vendor: EMC
  Model: LIFELINE-DISK
  Revision: 2
  SCSI Level: 5
  Is Pseudo: false
  Status: on
  Is RDM Capable: true
  Is Local: false
  Is Removable: false
  Is SSD: true

```

- The *Is SSD* will show *True* or *False*

- o The PowerCLI Way

```

01 $esxcli = Get-EsxCli
02 $esxcli.storage.core.device.list()
03
04 #Here is the output (truncated)
05
06 #AttachedFilters      :
07 #DevfsPath            : /vmfs/devices/disks/na
08 #Device               : naa.5000144f60f4627a
09 #DeviceType          : Direct-Access
10 #DisplayName          : EMC iSCSI Disk (naa.50
11 #IsPseudo             : false
12 #IsRDMCapable        : true
13 #IsRemovable         : false
14 #IsSSD                : true
15 #Model                : LIFELINE-DISK

```

15

- Identifying a SSD device is easy when they are detected automatically, but what if your SSD device isn't tagged as a SSD by default? The answer is you can manually tag them. This has to be done with our good friend **esxcli**
  - First you need to identify which device is not being tagged automatically (there are multiple ways of tagging the device, in this example we will use the device name) Run the following command so you can get the *Device Display Name* and the *Path Selection Policy*
    - **esxcli storage nmp device list**

```
~ # esxcli storage nmp device list
naa.5000144f60f4627a
Device Display Name: EMC iSCSI Disk (naa.5000144f60f4627a)
Storage Array Type: VMW SATP DEFAULT AA
Storage Array Type Device Config: SATP VMW_SATP_DEFAULT_AA
Path Selection Policy: VMW_PSP_FIXED
Path Selection Policy Device Config: {preferred=vmhba35:C1
Path Selection Policy Device Custom Config:
Working Paths: vmhba35:C1:T3:L0
```

- In this example the device name will be **naa.5000144f60f4627a** and the PSP will be **VMW\_SATP\_DEFAULT\_AA**— now we must add a PSA claim rule specifying the device, the PSP and the option to enable SSD
  - **esxcli storage nmp satp rule add -s VMW\_SATP\_DEFAULT\_AA -d naa.5000144f60f4627a -o enable\_ssd** — no result should be displayed
- Just like our claimrules in the previous section, we need to unclaim the device and load the claimrules into runtime. An additional step is also needed to execute the claimrules (this step was not required when creating LUN Masking claim rules). Again, you will need the device ID for the next command (**naa.5000144f60f4627a**)

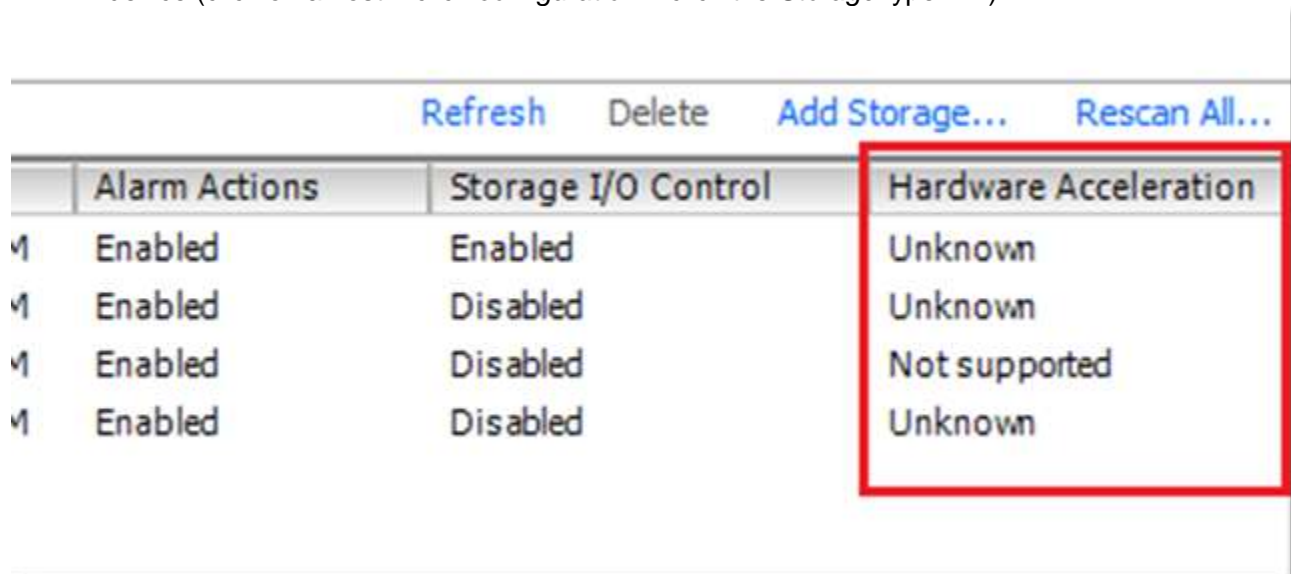
```
1 # unclaim the device
2 esxcli storage core claiming unclaim -t device -d naa.5000144f60f4627a
3
4 # load the claim rules into runtime
5 esxcli storage core claimrule load
6
7 # execute the claim rules
8 esxcli storage core claimrule run
```

```
9 # if the device is already mounted you will see it disappear from the Datast
10 # and then reappear with a Drive Type of SSD
11
```

- While I was writing this up I figured out you can tag drives as a SSD drive even if they aren't actually SSDs. I was excited about being able to document it and then realized that [William Lam](#) of [virtuallyGhetto](#) fame had already [documented this 10 months ago](#)

- **Administer hardware acceleration for VAAI**

- Since I only have block storage in my lab I will not be showing examples hardware acceleration for NFS, but will list procedures and capabilities for it
- Within the vSphere client you can see whether Hardware Acceleration is supported for your device (click on a host > click *configuration* > click the *Storage* hyperlink)



The screenshot shows a table with four columns: Alarm Actions, Storage I/O Control, Hardware Acceleration, and an unlabeled column. The Hardware Acceleration column is highlighted with a red border. The table contains four rows of data.

	Alarm Actions	Storage I/O Control	Hardware Acceleration	
✓	Enabled	Enabled	Unknown	Refresh Delete Add Storage... Rescan All...
✓	Enabled	Disabled	Unknown	
✓	Enabled	Disabled	Not supported	
✓	Enabled	Disabled	Unknown	

- The hardware acceleration available for block devices are:
  - Full Copy
  - Block Zeroing
  - Hardware Assisted Locking (ATS)
  - Unmap
- If your device is T10 compliant, it uses the the T10 based SCSI commands, therefore enabling hardware acceleration support without the use of the VAAI plugin. If your device is not T10 compliant (or is partially) the VAAI plugin is used to bridge the gap and enable hardware acceleration

- Display Hardware Acceleration Plug-Ins and Filter
  - **esxcli storage core plugin list -N VAAI** — displays plugins for VAAI
  - **esxcli storage core plugin list -N Filter** – displays VAAI filter

```
~ # esxcli storage core plugin list -N VAAI
Plugin name      Plugin class
-----
VMW_VAAIP_CX    VAAI
~ #
~ #
~ #
~ # esxcli storage core plugin list -N Filter
Plugin name      Plugin class
-----
VAAI_FILTER     Filter
~ #
```

- Displaying whether the device supports VAAI and any attached filters (for this example I'm using **naa.6006016014422a00683427125a61e011** as the device)
  - **esxcli storage core device list -d naa.6006016014422a00683427125a61e011**

```

~ # esxcli storage core device list -d naa.6006016014422a00683427125a61e011
naa.6006016014422a00683427125a61e011
  Display Name: AFCENT_Enterprise_Cluster_vm_vmfs1
  Has Settable Display Name: true
  Size: 1638400
  Device Type: Direct-Access
  Multipath Plugin: NMP
  Devfs Path: /vmfs/devices/disks/naa.6006016014422a00683427125a61e011
  Vendor: DGC
  Model: RAID 5
  Revision: 0430
  SCSI Level: 4
  Is Pseudo: false
  Status: on
  Is RDM Capable: true
  Is Local: false
  Is Removable: false
  Is SSD: false
  Is Offline: false
  Is Perennially Reserved: false
  Thin Provisioning Status: unknown
  Attached Filters: VAAI_FILTER
  VAAI Status: supported
  Other UIDs: vml.02000000006006016014422a00683427125a61e011524149442035
~ #

```

- Display VAAI status of each primitive on a device (again using `naa.6006016014422a00683427125a61e011`)
  - `esxcli storage core device vaai status get -d naa.6006016014422a00683427125a61e011`

```

~ # esxcli storage core device vaai status get -d naa.6006016014422a00683427125a61e011
naa.6006016014422a00683427125a61e011
  VAAI Plugin Name: VMW_VAAIP_CX
  ATS Status: supported
  Clone Status: supported
  Zero Status: supported
  Delete Status: unsupported
~ #

```

- Before we move on to adding hardware acceleration claim rules, lets check out how to display the current claim rules for filters and for VAAI
  - Filter — `esxcli storage core claimrule list -c Filter`
  - VAAI – `esxcli storage core claimrule list -c VAAI`
- Adding hardware acceleration claim rules is a 5 step process. The first two steps are creating two claim rules, one for the VAAI filter and another for the VAAI plugin. The third and fourth steps are loading the claim rules into runtime. The last step is executing the claim rules.

Since you are doing this manually you would need to know the *Type* information, in our case is *Vendor* and the *Vendor information* which in this case will be *vlabs*. Let's get to it:

```
1
2 # this will create a new claim rule for the VAAI_Filter with a type of "Vendor" and t
3 # the -u parameter automatically assigns the rule number
4 esxcli storage core claimrule add -c Filter -P VAAI_FILTER -t vendor -V vlabs -u
5
6 # this will create a new claim rule for the VAAI Plugin with a plugin name of "VMW_VA
7 # the -f parameter is being used to force the command as the aforementioned plugin name
8 esxcli storage core claimrule add -c VAAI -P VMW_VAAI_VLABS -t vendor -V vlabs -u -f
9
10 # load the filter plugin claim rule into runtime
11 esxcli storage core claimrule load -c Filter
12
13 # load the VAAI plugin claim rule into runtime
14 esxcli storage core claimrule load -c VAAI
15
16 # execute the new claim rules
17 esxcli storage core claimrule run -c Filter
```

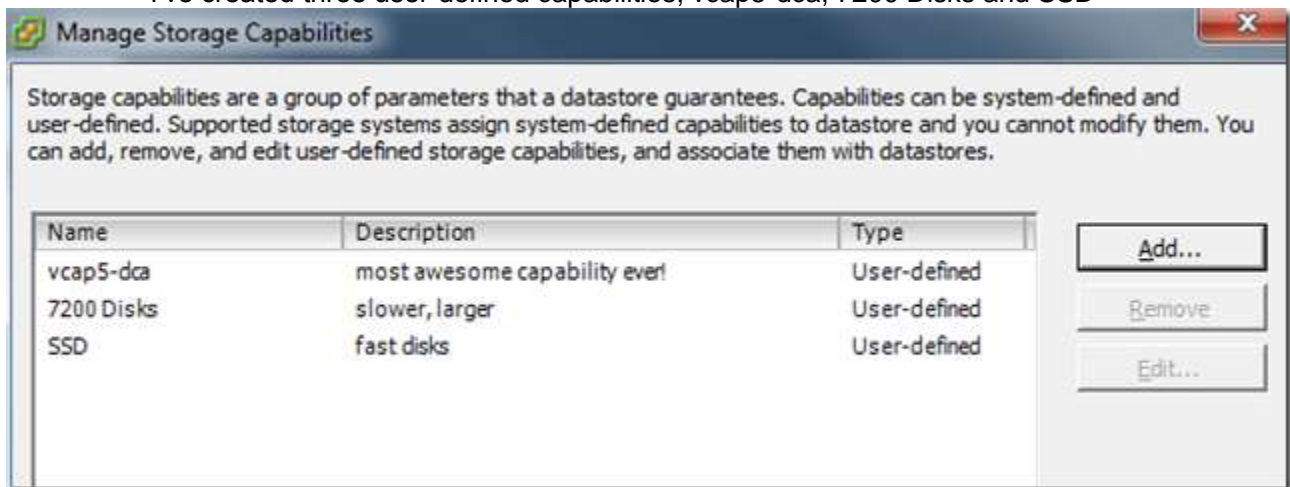
- For NFS you will need to install the plug-in provided by your array vendor and then verify the hardware acceleration (use **esxcli storage nfs list**). To see the full procedure for installing and updating NAS plugins see pages 177-180 of the [vSphere Storage Guide](#)

- **Configure and administer profile-based storage**

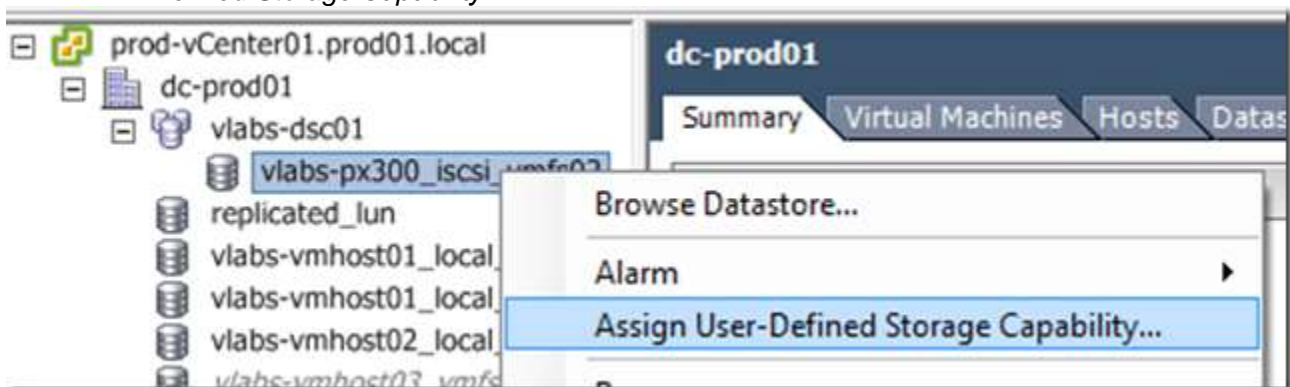
- Before we can administer profile-based storage we first must configure it (I know "DUH"). Of course, before we can configure it we must have a basic understanding of the elements of profile-based storage. Profile-based storage are profiles of certain storage features an array might have. Those features are added as a capability (if they are not already defined by the array). There are system-defined capabilities and user-defined capabilities. Here are a list of basic steps on the road to profile-based storage
  - Create user-defined capabilities (optional) to go along with any system-defined capabilities
  - Associate those capabilities with datastores that coincide with said capability
  - Enable virtual machine storage profiles (host or cluster level)
  - Create virtual machine storage profiles
  - Associate a virtual machine storage profile with virtual disks or virtual machine files
  - Check for compliance of the associated storage profile on the virtual machine



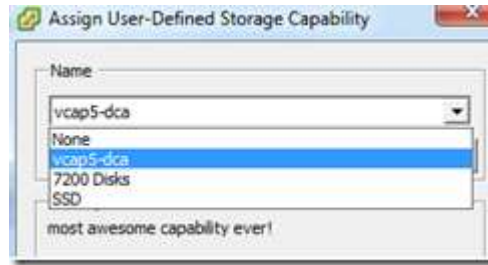
- Let's create some user-defined storage capabilities.
  - Log into vCenter using the vSphere client and click the *Home* button in the navigation bar
  - Under *Management* click the *VM Storage Profiles* button
  - Just under the navigation bar, click *Manage Storage Capabilities*
  - You're now presented with a dialog box where you can add your own. Click the *Add...* button
  - Type the *Name* of the capability > give it a *Description* > click *OK*
  - I've created three user-defined capabilities; vcap5-dca, 7200 Disks and SSD



- When you're finished adding capabilities, click the *Close* button
- We've created the capabilities, but now we need to associate them with a datastore(s)
  - Navigate to the *Datastores and Datastore Cluster* view (*Home > Inventory > Datastores and Datastore Clusters* or use the hot keys *Ctrl + Shift + D*)
  - Right-click on the datastore that you want to assign a capability to > click *Assign User-Defined Storage Capability...*



- From the drop-down menu select an existing storage capability (you can also create a new capability from here should you need to by clicking the *New...* button)

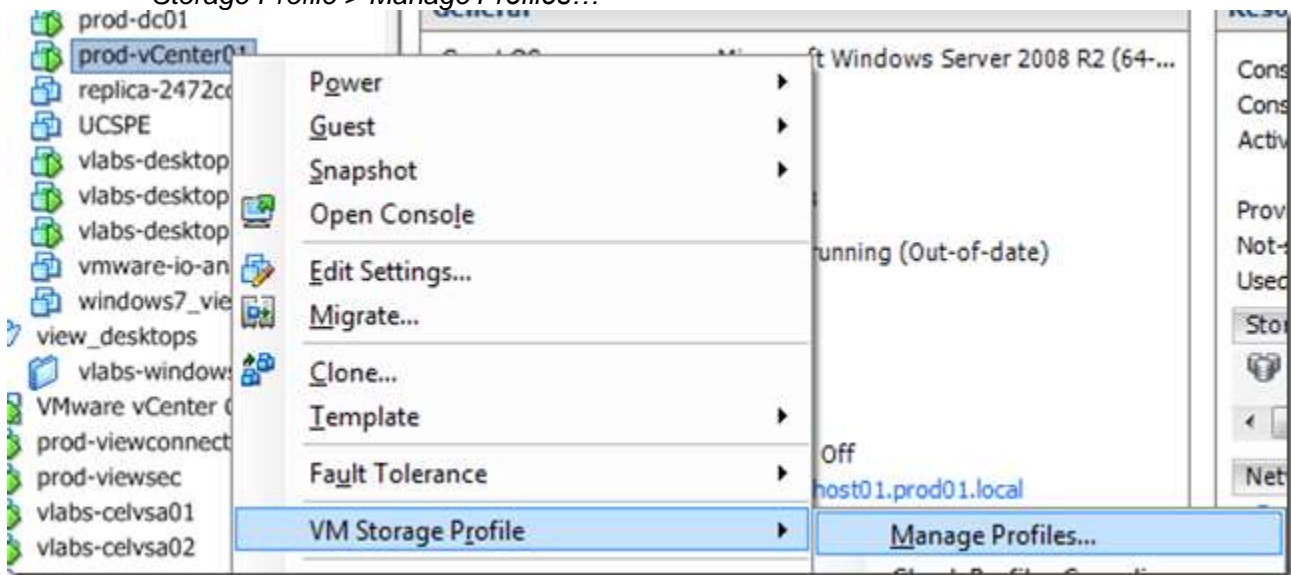


- Click *OK*
- Repeat on all datastores in which you need to assign a user-defined storage capability. If you are assigning the same storage capability to multiple datastores you can select them all at once and then assign the capability
- **NOTE: You can only assign one storage capability per datastore**
- We need to create virtual machine storage profiles, but first we must enable this on either a host or a cluster
  - In the vSphere client and click the *Home* button in the navigation bar
  - Under *Management* click the *VM Storage Profiles* button
  - Under the navigation bar click *Enable VM Storage Profiles*
  - From here you can select a particular cluster
    - ALL hosts within the cluster must have a *Licensing Status* of **Licensed**. Any other status, such as *Unknown* and you will not be able to enable it
  - Once you've selected which cluster you want click the *Enable* hyperlink in the top right

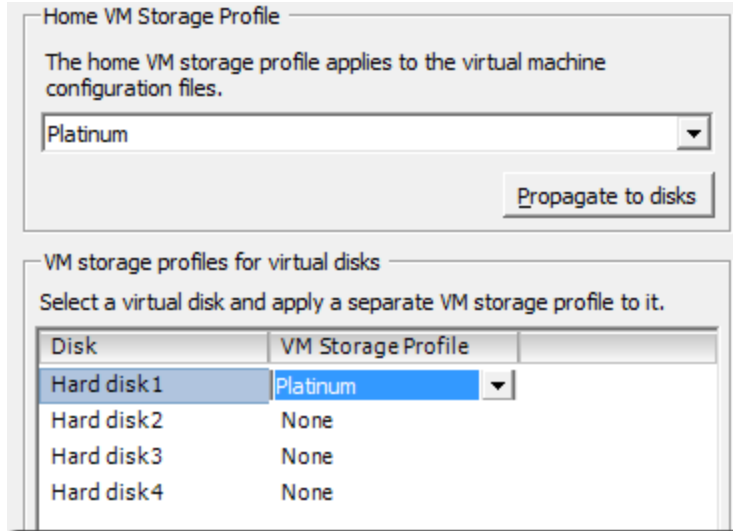


- Click the *Close* button once the *VM Storage Profile Status* changes to **Enabled**
- Creating a new VM Storage Profile
  - In the vSphere client and click the *Home* button in the navigation bar
  - Under *Management* click the *VM Storage Profiles* button
  - Under the navigation bar click *Create VM Storage Profile*
  - Enter in a descriptive name (such as a defined SLA, e.g. **Platinum**)
  - Enter in a description for the new profile > click *Next*
  - Select which storage capabilities should be a part of this profile. For this example I'm selecting the **vcap5-dca** capability)

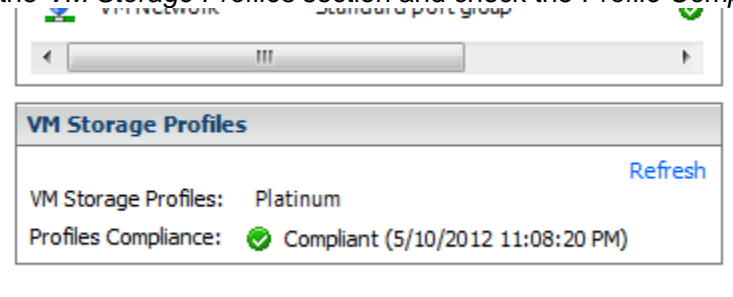
- BE CAREFUL HERE. If you select more capabilities than exist on a single datastore then a VM that has this particular storage profile applied to it will never show up as compliant
- Click *Next* > click *Finish*
- We have successfully created a VM Storage Profile, but it won't do us any good until we associate it with a virtual machine
  - In the vSphere client navigate to the *VMs and Templates* view (*Home > Inventory > VMs and Templates* or press *Ctrl + Shift + V*)
  - Right-click on a virtual machine that you want to apply a VM Storage Profile to > click *VM Storage Profile > Manage Profiles...*



- From the drop-down menu choose a profile. In our case it's the *Platinum* profile
- From here you have two options. You can click *Propagate to disks*, which will associate all virtual disks for that VM to the *Platinum* profile. If you don't want to propagate to all the disks you can manually set which disks you want to be associated with that profile
- In this example I am forgoing the propagate option and only setting this on Hard disk 1

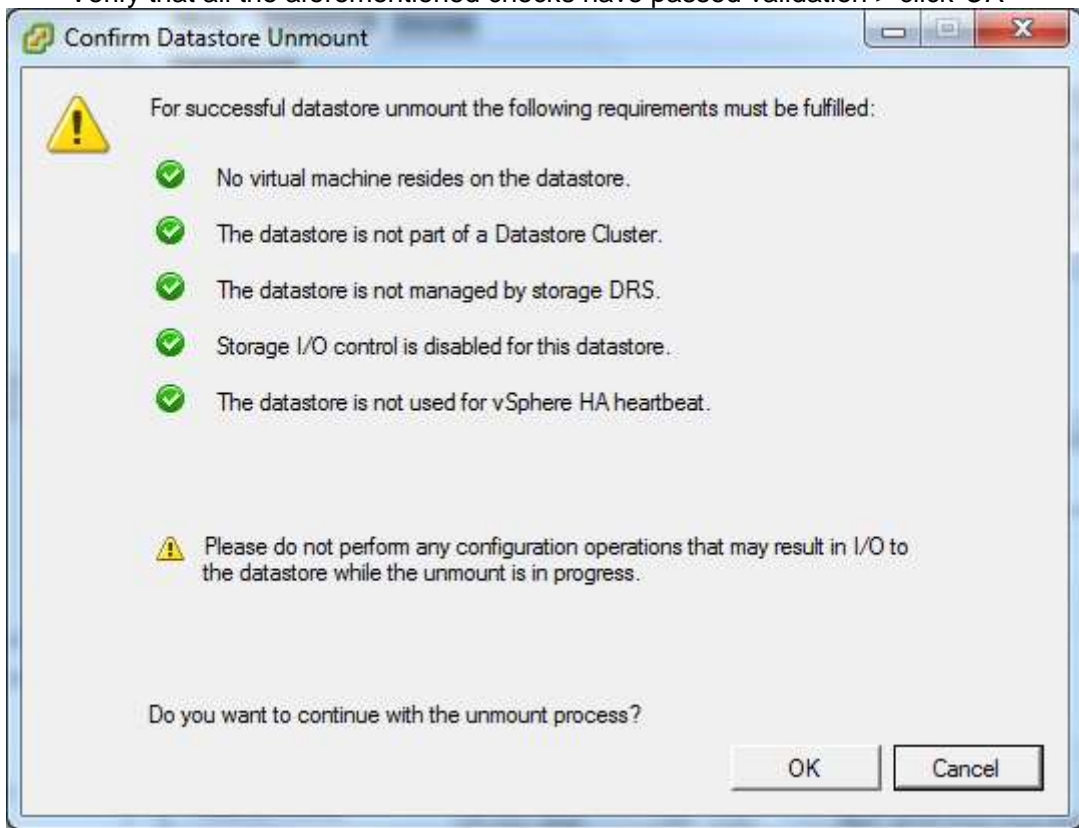


- Click *OK* when you are finished
- Lastly, we need to check the compliance of the VM Storage Profile as it relates to that particular VM
  - In the vSphere client navigate to the *VMs and Templates* view (*Home > Inventory > VMs and Templates* or press *Ctrl + Shift + V*)
  - Click on the virtual machine that you just associated the VM Storage Profile with and click the *Summary* tab (should be default)
  - Look at the *VM Storage Profiles* section and check the *Profile Compliance*



- Here it will list whether it is compliant or not and the last time it checked (if you need to check it again for compliance you can initiate that by right-clicking the VM > click *VM Storage Profile > Check Profiles Compliance*)
- **Prepare storage for maintenance (mounting/un-mounting)**
  - Should you need to perform storage maintenance on disks that make up a VMFS volume you will want to unmount it from vSphere. Here are a list of prerequisites for a VMFS datastore before it can be unmounted

- No virtual machine resides on the datastore
- The datastore is not part of a Datastore Cluster
- The datastore is not managed by storage DRS
- Storage I/O control is disabled for this datastore
- The datastore is not used for vSphere HA heartbeating
- To un-mount a datastore perform the following steps:
  - In the vSphere client, navigate to the *Hosts and Clusters* view
  - Select a host on the left and click the *Configuration* tab on the right > click the *Storage* hyperlink
  - Right-click on the datastore you want to un-mount and click *Unmount*
  - Verify that all the aforementioned checks have passed validation > click *OK*



- If any of the requirements fail to validate then you will not be able to unmount the datastore
- Using **esxcli** (I'm using the `vmfs_vcap_masking` datastore)
  - **esxcli storage filesystem unmount -l vmfs\_vcap\_masking**
    - There are scenarios where the GUI won't let you un-mount a volume, say for example the datastore has a virtual machine on it. In this instance, even if the VM is

powered off the GUI won't let you unmount the datastore. Using the **esxcli** command above however will let you unmount the datastore IF the VM is powered off

- If you try to unmount a datastore via **esxcli** while a powered on VM resides on that datastore you will receive the following error

```
~ # esxcli storage filesystem unmount -l vlabs-vmhost04_vmfs01
Sysinfo error on operation returned status : Busy. Please see the VMkernel log
~ #
```

- Here is more information from the vmkernel log (screenshot is broken up)

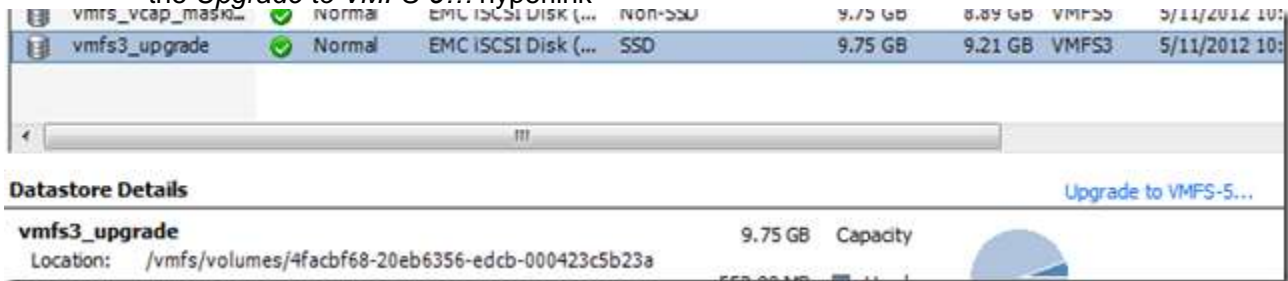
```
iscsi_vmk: iscsivmk_ConnCommandResponse: Conn [CID: 0 L: 10.90.190.7:60
VC: 637: unmounting opened volume ('4f61a871-1ff6a6a7-c602-002522dd8c78
Unmount VMFS volume f530 28 2 4f61a871 1ff6a6a7 2500c602 788cdd22 4 1 0
664 R: 10.90.190.131:3260]
'vlabs-vmhost04_vmfs01') is not allowed.
0 0 0 0 : Busy
```

- Once you're complete with your maintenance you want to mount the volume
  - In the vSphere client, navigate to the *Hosts and Clusters* view
  - Select a host on the left and click the *Configuration* tab on the right > click the *Storage* hyperlink
  - Right-click on the datastore you want to mount and click *Mount*
  - Monitor the *Recent Tasks* pane to see when the operation is complete. Once complete the datastore will be available
  - Using **esxcli** (I'm using the `vmfs_vcap_masking` datastore)
    - **esxcli storage filesystem mount -l vmfs\_vcap\_masking**

- **Upgrade VMware storage infrastructure**

- As with unmounting/mounting datastores, upgrading your VMware storage infrastructure, particularly upgrading to VMFS5, can be done through the GUI or using **esxcli**. Here are a few facts about upgrading from VMFS3 to VMFS5
  - VMFS5 has a 1MB block size regardless of disk file size
  - VMFS5 sub-blocks are now 8KB (VMFS3 is 64KB)
  - Block size you used on your VMFS3 partition will carry-over to the VMFS5 partition
  - The disk type of your newly upgraded VMFS5 partition will remain MBR until it exceeds the 2TB limit, at which it will automatically be converted to a GPT disk

- The upgrade can be done online without disruption to running virtual machines
- If you have any VMFS2 partitions you will need to first upgrade them to VMFS3 and then you can upgrade to VMFS5
- If you prefer to build new VMFS5 partitions instead of upgrading, but don't have space to create a new volume you can use the VM shuffle methodology to move VMs off one datastore to another, wipe the partition and create a new one and then continue with the shuffle until all VMFS datastores are complete. [Conrad Ramos](#) wrote a PowerCLI script to automate this, check it out [here](#)
- Upgrade VMFS3 to VMFS5 via the vSphere Client
  - In the vSphere client, navigate to the *Hosts and Clusters* view
  - Select a host on the left and click the *Configuration* tab on the right > click the *Storage* hyperlink
  - Click on the datastore you want to upgrade > below the *Datastore* pane on the right, click the *Upgrade to VMFS-5...* hyperlink



- Click *OK* to perform the upgrade
- Upgrade VMFS3 to VMFS5 via **esxcli** (upgrading a volume with the name of **vmfs3\_upgrade**)
  - **esxcli storage vmfs upgrade -l vmfs3\_upgrade**
  - once the command completes you will see that volume reflected as *VMFS5* under the *Type* column of the *Datastore Views* section within the vSphere client

## Tools

- [vSphere Installation and Setup Guide](#)
- [vSphere Storage Guide](#)
- [vSphere Command-Line Interface Concepts and Examples](#)

## Command-line Tools

- vscsistats
- esxcli
- vif

# VCAP5-DCA Objective 1.2 – Manage Storage Capacity in a vSphere Environment

For this objective I used the following documents:

- Documents listed in the Tools section

## ***Objective 1.2 – Manage Storage Capacity in a vSphere Environment***

### Knowledge

**\*\*ITEMS IN BOLD ARE TOPICS PULLED FROM THE BLUEPRINT\*\***

- **Identify storage provisioning methods**
  - There are two types of storage that can be provisioned through vSphere; block storage and NAS.
    - Block Storage
      - Local – any local storage attached to the host; uses VMFS
      - iSCSI – IP storage using a hardware or software iSCSI initiator; uses VMFS
      - FCoE – Fibre Channel over Ethernet using a hardware or software HBA; uses VMFS
      - FC – Fibre Channel using a hardware HBA; uses VMFNAS Storage
    - NAS Storage
      - NFS – currently using NFSv3 to mount NFS shares as datastores; uses NFS instead of VMFS
  - GUI Provisioning Method
    - The easiest way to provision storage is using the vSphere client. From the vSphere client you can create VMFS 3 or VMFS 5 datastores, you can create Raw Device Mappings or create a Network File System. You can do all this through the *Add Storage* wizard from within the client
      - Log into the vSphere client
      - Select a host > click the *Configuration Tab*
      - Click the *Storage* hyperlink
      - Click the *Add Storage. . .* hyperlink to launch the *Add Storage* wizard
    - From the *Add Storage* wizard you can provision block or NAS storage into the vSphere environment
  - Command-line Provisioning Methods
    - To provision storage through the command-line you can use **vmkfstools**



- There aren't a WHOLE lot of options for this command as it relates to creating file systems (you can also use **vmkfstools** to provision virtual disks. Here are the options:
  - You can specify whether it will be VMFS 3 or VMFS 5
  - You can set a block size (VMFS 3 ONLY)
  - You can set the volume name
- You can also choose to span or grow an existing file system
- Check out this example for creating a new VMFS 5 volume with a name of *vmkfstools\_vcap5\_volume* (a partition must exist on the LUN prior to creating a file system, which is what **partedUtil** is used for) — [VMware KB1009829](#) details this out as well

```

01
02 # you'll need the device ID (esxcli storage core device list)
03
04 # this command will get the current partition information, you need to see the last us
05 partedUtil get /vmfs/devices/disks/naa.5000144f60f4627a
06
07 # sample results "1305 255 63 20971520"
08
09 # in this case 20971520 is the last usable sector. To create the partition we'll use 2
10 # this command creates partition number 1, starting at 128, ending at 20971500 with a
11 partedUtil set /vmfs/devices/disks/naa.5000144f60f4627a "1 128 20971500 251 0"
12
13 # this command creates the VMFS 5 volume with a label of "vmkfstools_vcap5_volume"
14 vmkfstools -C vmfs5 -S vmkfstools_vcap5_volume /vmfs/devices/disks/naa.5000144f60f4627a
15
16 # if you want to remove this volume via the command line you can delete the underlying
17 partedUtil delete /vmfs/devices/disks/naa.5000144f60f4627a 1
18
19 # perform a rescan of the adapter and the volume will no longer be present
20 esxcli storage core adapter rescan -A vmhba35

```

- You can also add and remove new NAS volumes in the command-line using **esxcli**

```

1 # list any mounted NAS volumes
2 esxcli storage nfs list
3
4 # add a new NAS volume named "vm_backups"
5 esxcli storage nfs add -H 10.90.190.130 -s /nfs/vm_backups -v vm_backups
6
7 # remove a NAS volume named "vm_backups"
8 esxcli storage nfs remove -v "vm_backups"

```

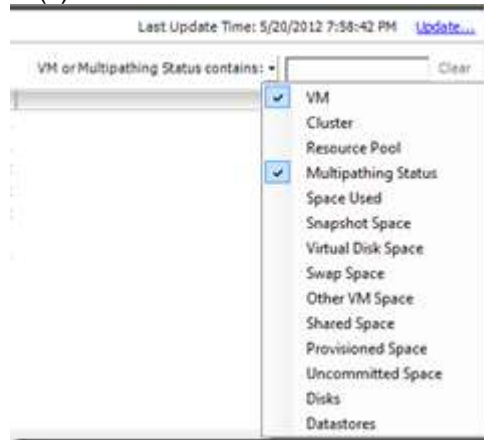
- **Identify available storage monitoring tools, metrics and alarms**

- Two built-in monitoring tools that come with vSphere are *Storage Reports* and *Storage Maps*. Both of these can be found in the *Storage Views* tab within the vSphere client (this pertains to looking at host inventory objects)
  - In the hosts and clusters view click on a host
  - Click the *Storage Views* tab on the right
- Different metrics exist to monitor storage performance and utilization. These metrics can be viewed within the vSphere client or by using **esxtop/resxtop**
- There are also a number of pre-defined alarms that will assist your monitoring efforts, such as *Datastore usage on disk* and *Thin-provisioned LUN capacity exceeded*.
- Storage Reports
  - Storage reports will show you information on how different objects within your inventory map to storage entities. By default a storage report for a host inventory object includes:
    - VM Name
    - Multipathing Status
    - Space Used
    - Snapshot Space
    - Number of disks
  - Here is a screen shot detailing out the defaults (the items checked) as well as all available fields that can be displayed within storage reports (for host inventory objects)

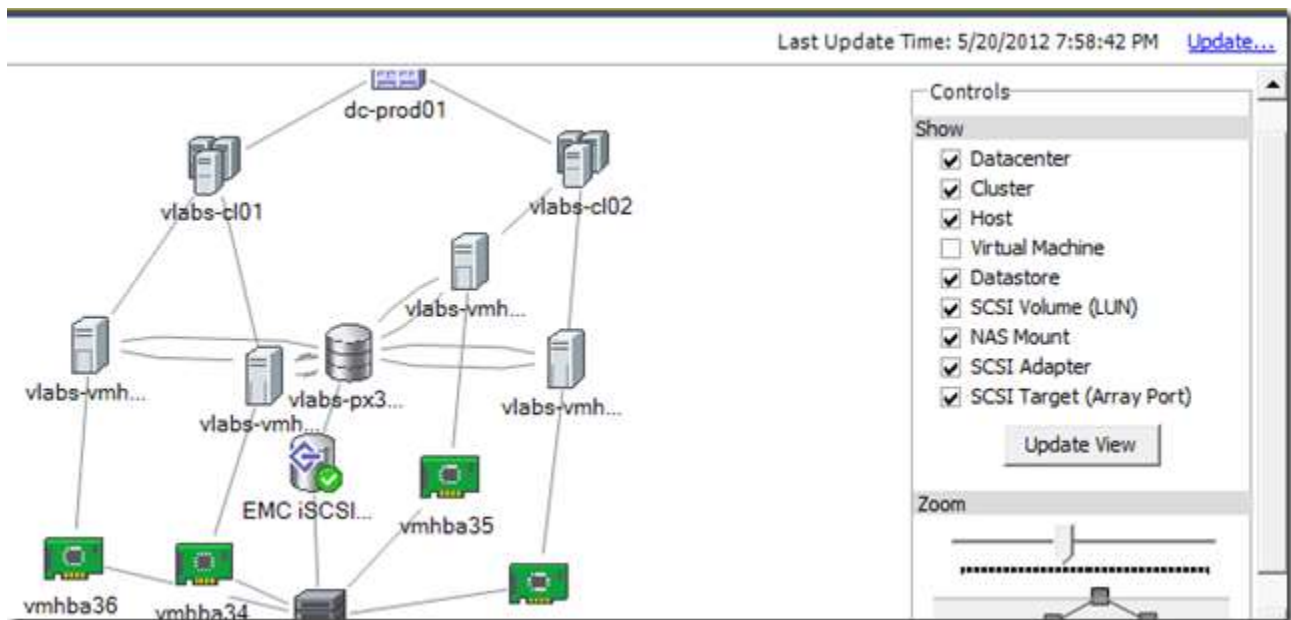


- The columns and information displayed will be dependent upon which inventory object you have selected. I'll let you go through each one and see how these reports vary

- Reports are updated every 30 minutes by default. You can manually update them by clicking the *Update...* hyperlink from within *Storage Views > Reports* located on the upper right of the screen
- You can filter these reports by selecting which columns you want to search on, and then typing in the keyword(s)



- You can export reports in the following formats
  - HTML
  - XLS
  - CSV
  - XML
  - Export Reports
    - Choose an inventory object
    - Click the *Storage Views* tab and select *Reports*
    - Choose which columns you want to view and any filtering
    - Right-click below the table and select *Export List...*
    - Enter in a name and choose the file format > click *Save*
- Storage Maps
  - Storage maps give you a nice representation of storage resources (physical and virtual) as they pertain to a specific inventory object. Storage maps are also updated automatically every 30 minutes and you can manually update them by clicking the *Update...* hyperlink located near the top right of the inventory object > *Storage Views > Maps* screen
  - Just as with Storage reports, Storage maps have default views for each type of inventory object. Using the different checkbox within the *Maps* area you can filter out object relationships that you do not wish to see



- By left-clicking on an object you can drag it to different parts of the screen
- Storage maps can also be exported in the same fashion as Storage reports, although, as you can imagine, your file type selection will be different
  - .jpeg
  - .bmp
  - .png
  - .tiff
  - .gif
  - .emf
- Storage Metrics (vSphere Client)
  - As with storage reports and storage maps, the types of metrics you will see as they relate to storage will vary depending upon which inventory object you select. For example, if you select a datastore inventory object you will by default be show space utilization views in a graph format (graphs based on file type and the top 5 virtual machines)
  - You can then change that default view from *Space* and change it to *Performance*, which will show you a slew of performance charts for that particular datastore
  - To see the real “meat and potatoes” of metrics as they relate to storage within the vSphere client you need to look at advanced performance charts
    - Select a host from the inventory
    - Click the *Performance* tab > click the *Advanced* button

- From the drop down there are four related storage items
  - *Datastore*
  - *Disk*
  - *Storage Adapter*
  - *Storage Path*
- If I went into every counter that you could see for the objects above you will be reading this post for the next 6 weeks. So know where these metrics are and at the very least familiarize yourself with defaults
- Storage Metrics (**esxtop/resxtop**)
  - I decided not to go into a lot of detail for this section as there are already some great resources out there. For a good review of this tool check out Duncan Eppings [blog post on esxtop](#). For a detailed review of all statistics for esxtop check out this [VMware community post](#)
  - For storage monitoring there are three panels within **esxtop** that you will want to be intimately familiar with (the letters at the end correspond to the **esxtop** hotkey for those panels)
    - Storage Adapter Panel (d)
    - Storage Device Panel (u)
    - Virtual Machine Storage Panel (v)
  - Some key metrics you want to look at for the panels above
    - *MBREAD/s* — megabytes read per second
    - *MBWRTN/s* — megabytes written per second
    - *KAVG* — latency generated by the ESXi kernel
    - *DAVG* — latency generated by the device driver
    - *QAVG* — latency generated from the queue
    - *GAVG* — latency as it appears to the guest VM (*KAVG* + *DAVG*)
    - *AQLEN* – storage adapter queue length (amount of I/Os the storage adapter can queue)
    - *LQLEN* – LUN queue depth (amount of I/Os the LUN can queue)
    - *%USD* – percentage of the queue depth being actively used by the ESXi kernel ( $ACTV / QLEN * 100\%$ )
- Alarms

- There are a number of different pre-configured alarms related to storage that can be leveraged to alert you of impending storage doom. As with a lot of functions within vSphere, different alarms are pre-defined based on the inventory object that you select. Which means there are different storage related alarms for different inventory objects
  - If you are in the vSphere client and you select the top-most inventory object (the vCenter object) and you go to the *Alarms* tab, you can select *Definitions* and view ALL pre-configured alarms for all objects
- Again, I won't go into every single alarm and what they do, but here are a list of some I think are important to know, along with their default triggers
  - *Cannot connect to storage* – this alarm will alert you when a host has an issue connecting to a storage device The three default triggers are:
    - *Lost Storage Connectivity*
    - *Lost Storage Path Redundancy*
    - *Degraded Storage Path Redundancy*
  - *Datastore cluster is out of space* – this alarm monitors disk space on datastore clusters. The default triggers are:
    - Send a Warning when utilization is above 75%
    - Send an Alert when utilization is above 85%
  - *Datastore usage on disk* – this alarm monitors disk space on a datastore. The default triggers are:
    - Send a Warning when utilization is above 75%
    - Send an Alert when utilization is above 85%
  - *Thin-provisioned LUN capacity exceeded* – this alarm monitors thin-provisioned LUNs using the vSphere Storage APIs. Triggers for these alarms must be modified through the vSphere API (VASA) and is implemented by your storage vendor

### Skills and Abilities

- **Apply space utilization data to manage storage resources**
  - I'm not 100% what VMware is looking for on this, but my best guess is to use some of the techniques above to determine current space utilization, and then manage your storage resources appropriately

- Since we've already gone through the different metrics and alarms to monitor, let's use the ESXi shell to determine VMFS disk usage. The command **df**, which in Linux speak stands for *disk filesystem*, is used to display the the filesystems that are mounted to that particular host.

```

1 # the -h parameter will make the disk space for the filesystem appear
2 # as human readable (in this case in GB) you can use the -m or -k
3 # parameters for megabytes and kilobytes respectively
4
5 df -h
6
7 # if you want to return only VMFS and NFS paritions run this command
8
9 df -h | awk '/VMFS*/ || /NFS/'

```

Since I filtered the results you don't see an explanation of each column. From left to right:

Filesystem	Size	Used	Available	Use%	Mounted on
NFS	829.0G	52.6G	776.4G	6%	/vmfs/volumes/vm_backups
VMFS-5	9.8G	881.0M	8.9G	9%	/vmfs/volumes/vmfs_vcap_masking
VMFS-5	293.0G	6.0G	287.0G	2%	/vmfs/volumes/vlabs-vmhost04_vmfs01
VMFS-5	799.8G	397.6G	402.1G	50%	/vmfs/volumes/vlabs-px300_iscsi_vmfs02

- At the moment we are focused on space utilization, so we want to focus on the *Use%*. As you can see, none of my partitions are over 50%. If I had a highly used partition you would most likely get an alarm from the *Datastore Usage* alarm, and you could use **df** to see a summary of all your partitions
  - There are lots of way to rectify this, add more space/extents, delete unneeded virtual machines or remove unneeded virtual disks (you could accomplish this through the vSphere client or by using the **vmkfstools -U** command)
  - The bottom line is that you need to be aware of, not only how you can determine space utilization, but then to apply that data in an intelligent way in order to manage your storage resources effectively
- **Provision and manage storage resources according to Virtual Machine requirements**

- I've covered some of this in [Objective 1.1 – Implement and Manage Complex Storage Solutions](#). Before you can provision, or manage, storage resources for a virtual machine, you first must know the virtual machine requirements, which includes, but is not limited to:
  - Space – how much space is needed
  - I/O workload – how many spindles are needed to satisfy the workload
  - Resiliency — how protected does the data need to be
- Looking at the above list you can look at the application requirements for the recommended amount of disk space. You can use tools such as **vscsiStats** or *IOMeter* to determine the workload characteristics and how many spindles you'll need. Depending upon availability and resiliency requirements will determine RAID level, whether snapshots (array level) will be used, what level of backup and how often to backup and how long the data needs to remain in an off-site location
- Once you've determined the virtual machine requirements you can start to provision and manage your storage based on those requirements. If you have a virtual machine that requires a certain level of service or, say it needs to be on super fast storage, you can leverage a few vSphere features to help you accomplish that goal
  - *Profile Driven Storage* – again, I covered this in Objective 1.1 on how to configure and implement profile driven storage. You can create a profile based on a virtual machine(s) requirement, such as fast disks, and assign that storage capability to one or more datastores. You can then create a storage profile and apply it to the virtual machine. Whenever that particular virtual machine is on a datastore that doesn't meet that storage profile, it will be marked non-compliant
  - *Datastore Cluster* – you can group similar datastores into a construct known as a datastore cluster. This allows you to assign virtual machines to that datastore cluster, and, in conjunction with Storage DRS, the virtual machine will be placed on the least used datastore (in terms of I/O and space utilization)
- You can provision storage for a virtual machine in a few different ways:
  - Adding a new disk through the vSphere Client
  - **vmkfstools**
- Adding storage to a virtual machine through the vSphere client is pretty straight forward so lets go through how you would create an empty virtual disk using **vmkfstools**

```

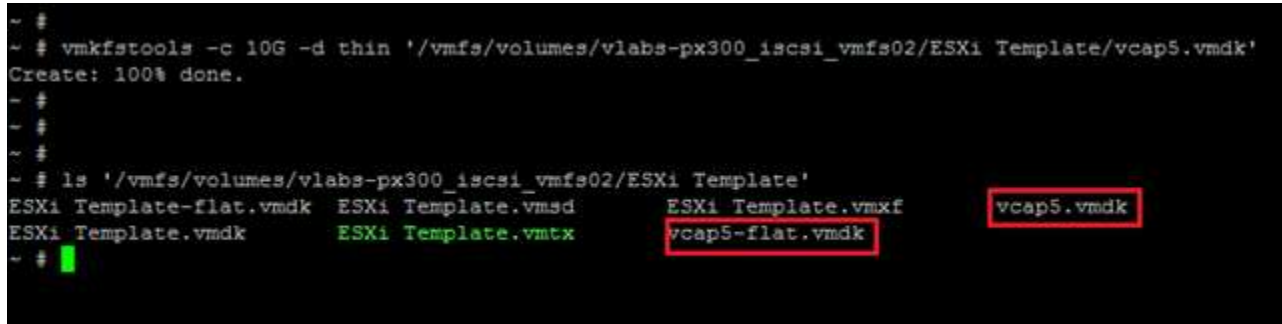
1 # the -c parameter specifies you want to create a new virtual disk and then you specif
2 # the -d parameter specifies the disk format; zeroedthick, thin and eagerzeroedthick (
3 # the -a specifies the adapter type; buslogic, lsilogic, ide (default is buslogic)

```



4  
5  
6  
7  
8

```
# here we will create a 10GB thin disk named vcap5.vmdk with the default buslogic adap  
# in a virtual machine folder named ESXi Template  
vmkfstools -c 10G -d thin '/vmfs/volumes/vlabs-px300_iscsi_vmfs02/ESXi Template/vcap5.
```



```
~ #  
~ # vmkfstools -c 10G -d thin '/vmfs/volumes/vlabs-px300_iscsi_vmfs02/ESXi Template/vcap5.vmdk'  
Create: 100% done.  
~ #  
~ #  
~ #  
~ # ls '/vmfs/volumes/vlabs-px300_iscsi_vmfs02/ESXi Template'  
ESXi Template-flat.vmdk  ESXi Template.vmsd  ESXi Template.vmx  vcap5.vmdk  
ESXi Template.vmdk      ESXi Template.vmtx  vcap5-flat.vmdk
```

- Above you can see that the command was successful and that the *vcap5-flat.vmdk* and *vcap5.vmdk* files were created

- **Understand the interactions between virtual storage provisioning and physical storage provisioning**

- The virtual provisioning of physical storage can add benefit to your organization as long as you understand the implications of what you are doing. Virtual storage provisioning allows you to over-commit your storage resources as needed
- If I had to pick one construct to understand when it comes to the interaction between virtual storage provisioning and physical storage provisioning it would be with *Thin Provisioning*. Thin provisioning allows you to create a virtual disk that is, for example, 40GB in size, but you're actually only using 5GB. The guest operating system thinks its hard disk is physically 40GB, while the physical storage has only allocated 5GB
  - The biggest thing that you need to understand here is that by thin provisioning the actual size on the disk is less than what you've provisioned, which can get you into trouble if you aren't paying attention to the physical storage
  - If you have a 100GB datastore, you can put 40 VMs with 5GB virtual hard disks that are thin provisioned. Even those those 40 VMs may only be using 2GB each, they have the potential to grow up to 5GBs, which at a certain point would cause you to physically run out of storage space; NOT GOOD!

- In the section above we went over created an empty virtual disk, and we created it as a thin disk. Since it is a thin disk, the provisioned size will be different from the actual size. Here is what you'll see when looking in the datastore browser

Name	Size	Provisioned Size	Type
New Virtual Machine.vmx	1.53 KB		Virtual Machine
New Virtual Machine.vmx.f	0.27 KB		File
New Virtual Machine.vmsd	0.00 KB		File
New Virtual Machine.vmdk	0.00 KB	5,242,880.00 KB	Virtual Disk
vcap5.vmdk	0.00 KB	10,485,760.00 KB	Virtual Disk

- As you can see the *Size* and *Provisioned Size* are much different.
- The same exists when you have a datastore full of thin disks, the *Capacity* and *Provisioned Space* will differ. Let's have a look (Go to the *Datastores and Datastore Cluster* view > click on a datastore on the left > click the *Summary* tab on the right)

Capacity	
Capacity:	<b>1.56 TB</b>
Provisioned Space:	<b>2.64 TB</b>
Free Space:	<b>605.57 GB</b>
Last updated on:	<b>5/23/2012 6:17:00 AM</b>





- The *Capacity* is 1.56 TB while the provisioned space is more than 1TB over the physical capacity. However, my physical free space is still ~600GB
- The point I'm trying to get across is that you need to be intimately familiar with what your virtual storage environment is, and what it is doing, while keeping the physical storage in mind
- If you have a thinly provisioned virtual disk that you want/need to physically consume all of its provisioned space AFTER you have created it then you can *Inflate* the disk. This can be done within the datastore browser by right-clicking on the VMDK file and selecting *Inflate*. You can also do this from the command line; here is how

```

1 # this command will inflate a thin disk, thereby forcing it to consume its fully provi
2 # on the physical storage array. Again we're using the vcap5.vmdk
3
4 vmkfstools -j '/vmfs/volumes/vlabs-px300_iscsi_vmfs02/New Virtual Machine/vcap5.vmdk'
```

- This operation can take quite a long time to complete depending on how much physical space needs to be zeroed out

- Now as you can see the *Size* shows what the *Provisioned Size* used to show, and now the *Provisioned Size* column is blank (which is expected as that field isn't populated unless the virtual disk is thin)






Name	Size	Provisioned Size	Type
 New Virtual Machine.vmx	1.53 KB		Virtual Machine
 New Virtual Machine.vmx	0.27 KB		File
 New Virtual Machine.vmsd	0.00 KB		File
 New Virtual Machine.vmdk	0.00 KB	5,242,880.00 KB	Virtual Disk
 vcap5.vmdk	10,485,760.00 K		Virtual Disk

- **Apply VMware storage best practices**

- This seems redundant as [Objective 1.1 – Implement and Manage Complex Storage Solutions](#) has a section called **Apply VMware storage best practices**, See the details in that post under the same heading

- **Configure Datastore Alarms**

- There are five pre-configured datastore alarms that ship with vSphere 5, see the below screen shot for their names and descriptions

Name	Description
 Datastore usage on disk	Default alarm to monitor datastore disk usage
 Unmanaged workload detected on SIOC-enabled datas...	Default alarm that triggers if an unmanaged I/O wo
 Pre-4.1 host connected to SIOC-enabled datastore	Default alarm that triggers if a pre-4.1 host is conne
 Datastore capability alarm	Alarm that triggers if storage array detects that the
 Thin-provisioned LUN capacity exceeded	Alarm that triggers if storage array detects that thi

- Aside from the five datastore alarms you see above, there are a lot more triggers we can use to create alarms for the *Datastore* monitor and whether you choose to monitor for a specific condition/state or for a specific event
  - Log into the vSphere client and navigate to the *Datastores and Datastore Cluster* view
  - Click on a datastore from the listing on the left > click the *Alarms* tab > click the *Definitions* button
  - Right-click anywhere under the pre-configured alarms and select *New Alarm...*
  - Enter in the following details:
    - *Alarm Name:* Datastore Over Provisiong Alarm

- *Description:* Alarm to monitor the provisioned space on the datastore
- *Alarm Type:* Datastore
- Choose *Monitor for specific conditions or state...*
- *Enable this alarm:* Check this box

- Click on the *Triggers* tab > click *Add* to add a new trigger
- Enter in the following details:
  - *Trigger Type:* Datastore Disk Provisioned (%)
  - *Condition:* Is above
  - *Warning:* 100
  - *Alert:* 200
  - Select the *Trigger if any of the conditions are satisfied* radial button

Trigger Type	Condition	Warning	Condition Length	Alert
Datastore Disk Provisioned (%)	Is above	100	200	

- Click the *Reporting* tab

- Choose if you want the alarm to repeat when the condition exceeds a certain range
- Choose the frequency

General | Triggers | Reporting | Actions |

Range  
Repeat triggered alarm when condition exceeds this range:  
0 percent (above or below limit)

Frequency  
Repeat triggered alarm every:  
0 minutes

- Click the *Actions* tab > click *Add* to add an action
- Enter in the following details
  - *Action:* Send a notification email
  - *Configuration:* [josh.coen@valcolabs.com](mailto:josh.coen@valcolabs.com)
  - You can choose when to perform this action based on the alarm transition state. By default this will perform the action one time when the alarm goes from warning to alert. Just leave the default
- Click *OK* (you will get a warning message if your vCenter SMTP settings are not configured)

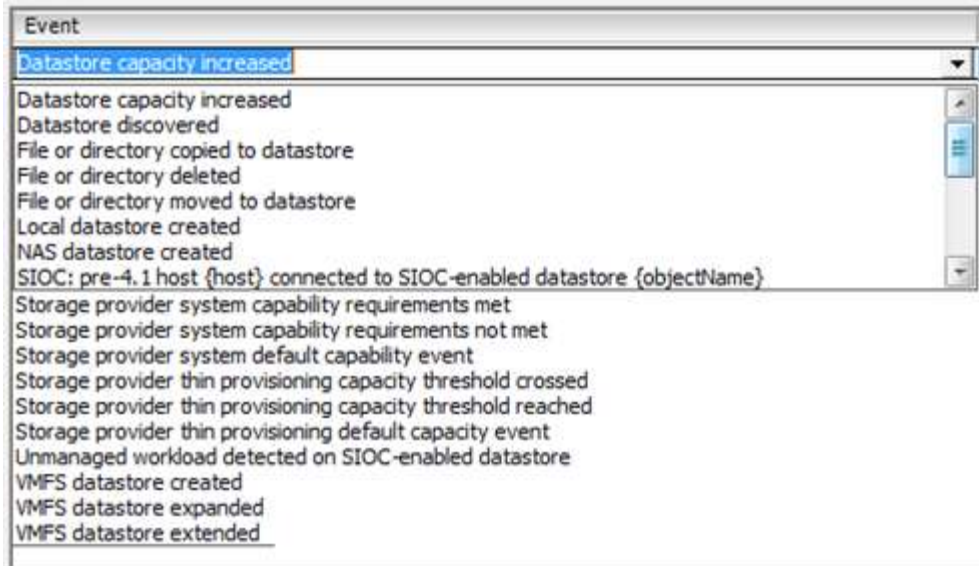
General | Triggers | Reporting | Actions |

Specify the actions to take when a type of alarm changes.  
Select whether the action should be repeated.  
Specify how often actions should be repeated.

Action	Configuration
Send a notification email	josh.coen@valcolabs.com;

Once

- There are A LOT more triggers that relate to the *Datastore* monitor when you select the *Monitor for specific events occurring...* radial button. Here is a list:



- As you can see you have A LOT of options to choose from and you can use the instructions in the previous steps to create new alarms that can help you effectively monitor your datastores

- **Analyze Datastore Alarms and errors to determine space availability**

- Using datastore alarms and errors to determine your available space is pretty straight forward. The default alarm *Datastore usage on disk* is the perfect alarm to use, and it's enabled by default
- The *Datastore usage on disk* alarm is pre-configured to trigger a warning when its disk usage is over 75%. It will trigger an alert if it gets above 85%. Now again, these are the defaults for this alarm, you may want to edit the thresholds based on your organizations best practices as it relates to %free for storage
- You can only edit alarms in the scope in which they are defined in. In this case, the *Datastore usage on disk* alarm is defined at the top level object, which is the vCenter object
- I created an 8.6GB eagerzeroedthick virtual disk using vmkfstools on a datastore that had only 8.89GB free.

```

1 # for those interested, here is the command I used to create the virtual disk
2
3 vmkfstools -c 8600mb -d eagerzeroedthick /vmfs/volumes/vmfs_vcap_masking/vcap5.vmdk

```

- Once my view was updated (these are updated every 30 minutes) an alert was triggered

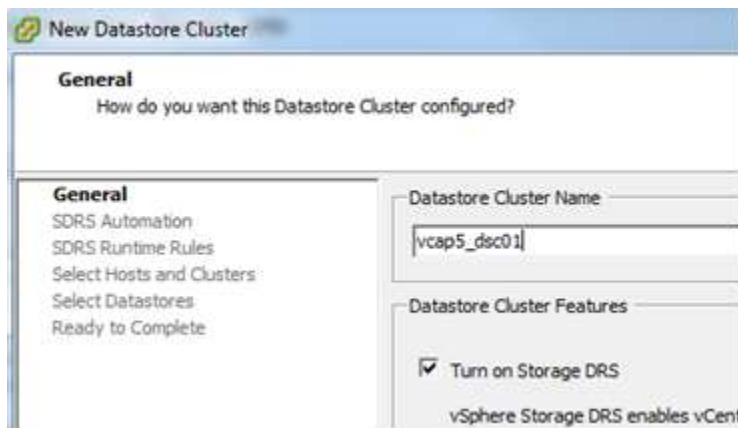
The screenshot shows the vSphere Storage Configuration interface. On the left, a tree view lists storage objects, with 'vmfs\_vcap\_masking' selected. The main pane displays the 'General' tab for this volume, showing its location as 'ds:///vmfs/volumes/4fa41a21-878f4a...', its type as 'VMFS', and that it is connected to 4 hosts. To the right, a 'Capacity' section shows 'Capacity: Provisioned Space' and 'Free Space: Last updated'. Below the main pane, a 'Triggered Alarms' section contains a table with the following data:

Object	Status	Name	Triggered	Acknowledged
vmfs_vcap_masking	Alert	Datastore usage on disk	5/23/2012 9:44:32 PM	

- Now if I was seeing this alert for the first time the first thing I would do is check the space availability of my datastore. If it was in fact close to being at capacity I would either allocate more space, delete unneeded virtual disks/files or perform a storage vMotion to another datastore that had more capacity

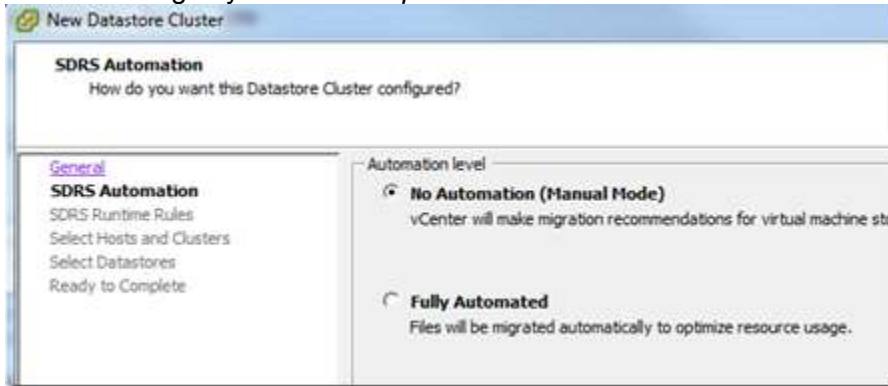
- **Configure Datastore Clusters**

- Configuring datastore clusters is an easy enough process, but it is a process and can only be created from the vSphere client (can't create in vSphere Web Client)
  - Log into the vSphere client and navigate to the *Datastores and Datastore Clusters* view
  - Right-click on your datacenter object and select *New Datastore Cluster...*
  - Enter in a name for the datastore cluster and choose whether or not to enable Storage DRS

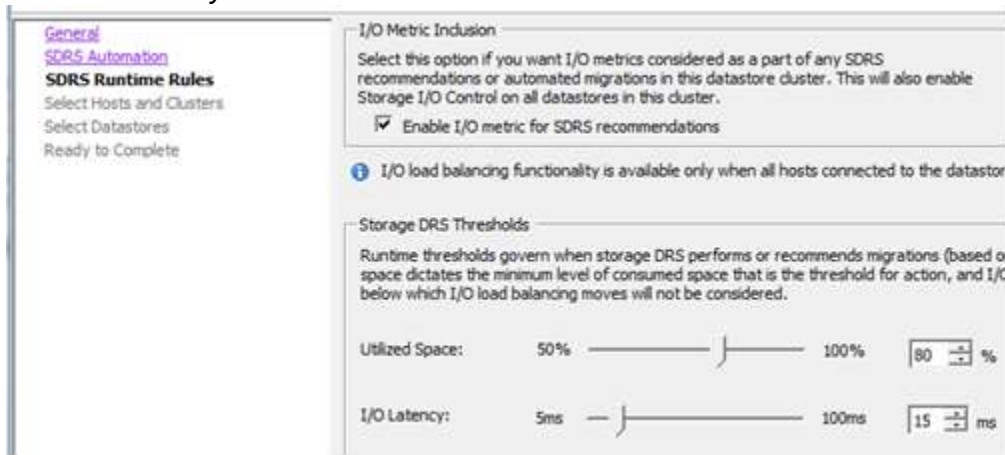


- Click *Next*

- Choose either *No Automation (Manual Mode)* or *Fully Automated*
- We aren't adding any *Advanced Options* so click *Next*

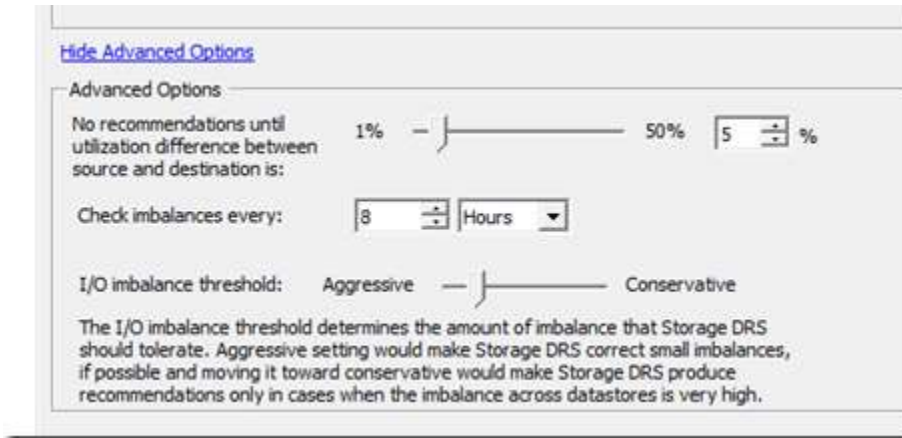


- Decide whether you want to enable the I/O metric for SDRS recommendations
- Choose the thresholds you want SDRS recommendations to be triggered on
  - *Utilized Space* — default is 80%
  - *I/O Latency* — default is 15ms



- Click the *Show Advanced Options* hyperlink to set the advanced options
  - Set the percentage for the minimum utilization difference between the source and destination datastore before SDRS will make a recommendation
    - Here is an example: If leave this at the default (5%), SDRS will not make a recommendation for a move unless the there is *at least* a 5% difference between the source datastore and the destination datastore in terms of utilization. So, the datastore first needs to exceed the utilization space threshold and then there needs to be at least 5% difference in terms of utilization before SDRS will make a recommendation
  - Set the frequency that SDRS should check for imbalances — default is 8 hours
  - Set the I/O imbalance threshold

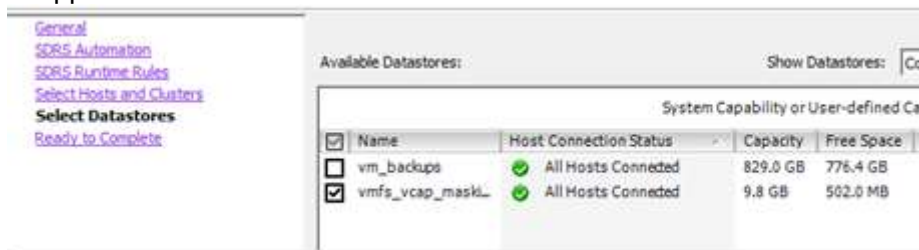




- Click *Next*
- Select which cluster(s) you want to use > click *Next*



- Select which datastores you want as part of the datastore cluster
  - Best practice is to use datastores that have similar capabilities, that way application owners and users should never experience a degradation of service due to an applied SDRS recommendation



- Click *Next* > click *Finish*

## Tools

- [vSphere Storage Guide](#)
- [vSphere Command-Line Interface Concepts and Examples](#)
- [vCenter Server and Host Management Guide](#)
- [Product Documentation](#)
- vSphere Client / Web Client
- vSphere CLI

# VCAP5-DCA Objective 1.3 – Configure and Manage Complex Multipathing and PSA Plug-ins

For this objective I used the following documents:

- Documents listed in the Tools section

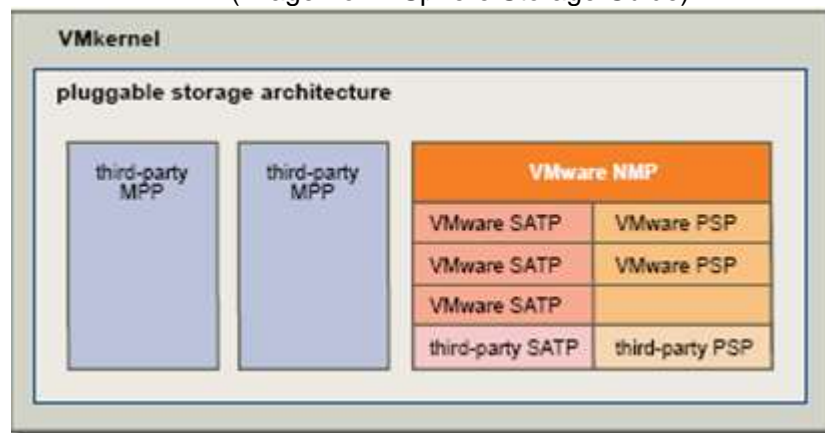
## **Objective 1.3 – Configure and Manage Complex Multipathing and PSA Plugin-ins**

### Knowledge

**\*\*ITEMS IN BOLD ARE TOPICS PULLED FROM THE BLUEPRINT\*\***

- **Explain the Pluggable Storage Architecture (PSA) layout**
  - The Pluggable Storage Architecture (PSA) is a framework that is use for handling multipathing in a VMware environment. The framework is modular so it allows third-party vendors to build their own multipathing plugins and put them directly inline with storage I/O. The PSA is a collection sits at the vmkernel layer and is essentially a collection of vmkernel APIs

(image from vSphere Storage Guide)



- The PSA consists of plug-ins and sub plug-ins and perform different functions
  - Multipathing Plug-in (MPP)
    - These are provided by third-party vendors. An example of of a MPP is EMCs PowerPath/VE. VMware's Native Multipathing Plug-in is also a MPP
  - Native Multipathing Plug-in (NMP)
    - Path Selection Plug-in (PSP)
      - Determines which active path to use when issuing an I/O request to a storage device

- If the active path to a particular storage device fails, PSP will determine which path to use next to issue the I/O request
- Third-party vendors can create and integrate PSPs that run alongside VMware's PSPs
- Storage Array Type Plug-ins (SATP)
  - Determines and monitors the physical path states to the storage array
  - Determines when a physical path has failed
  - Activates new physical paths when the active path(s) has failed
  - Perform any other necessary array specific actions required during a storage fail-over
  - Third-party vendors can create and integrate SATPs that run alongside VMware's SATPs

### Skills and Abilities

- **Install and Configure PSA plug-ins**

- Third-party vendors can supply their own MPP, such as EMC PowerPath/VE, or they can supply sub-plugins for PSP or SATP that supplements VMware's NMP. These plug-ins will come in the form of a bundle and can be installed the following ways:

- VMware vSphere Update Manager
- Connected directly to the host via SSH console (use the **esxcli software vib install** command)
- Using the vSphere Management Assistant (vMA) using the **esxcli software vib install** command
- If the new plugin is not automatically registered you can do so manually

```

1 # check to see if the new plug-in is registered
2
3 esxcli storage core plugin registration list
4
5 # if it isn't register the new plugin. In this example the module name is 'vcap_satp_v
6 # the plug-in class is SATP and the plug-in name is 'VCAP_SATP_VA'
7
8 esxcli storage core plugin registration add -m vcap_satp_va -N SATP -P VCAP_SATP_VA

```

- If you need to set a new default PSP for a SATP use the following commands:

```
1 # this commnad lists out the current SATPs and their associated default PSP
2
3 esxcli storage nmp satp list
4
5 # this command will change the default PSP. Here i'm changing the VMW_SATP_CX
6 # default PSP from VMW_PSP_MRU to VMW_PSP_RR
7
8 esxcli storage nmp satp set -s VMW_SATP_CX -P VMW_PSP_RR
```

- Any devices that are currently using the SATP that you just changed will need to have all of their paths unclaimed and reclaimed. If you want to perform these operations via **esxcli** you will have to stop all I/O going to these devices, which usually isn't a possibility. In this case you must reboot the host(s) in order for the new PSP to take effect
- When you load a third-party SATP into NMP you are doing so in order to use the new SATP with a particular device. Here are the commands to run in order to claim a device under a different SATP – in this example I'm going to change the default SATP for a particular device to another SATP. When you install a third-party SATP the claim rule will most likely be specific to a class of devices and not a device ID, which is what I'm doing here.

```
1 # create a new claim rule for a device using the VMW_SATP_CX plugin
2
3 esxcli storage nmp satp rule add -s VMW_SATP_CX -d naa.5000144f60f4627a
4
5 # list the SATP claim rules to ensure it was added
6
7 esxcli storage nmp satp rule list -s VMW_SATP_CX
```

- **Understand different multipathing policy functionalities**

- I understand “multipathing policy functionalities” to be the Path Selection Plug-ins, or PSP. If someone has any comments what else this might be referring to, please let me know! [VMware KB 1011340](#) also refers to PSPs as multipathing policies
- By default there are three PSP's that ship with vSphere
  - VMW\_PSP\_MRU

- The host will use the pat that is most recently used (MRU). When a path fails and another one is activated, the host will continue to use this new active path even when the original path comes back up.
    - Default for active/passive arrays
    - Default for ALUA devices
  - VMW\_PSP\_FIXED
    - The host will use a fixed path that is either, set as the *preferred* path by the administrator, or is the first path discovered by the host during the boot process
    - Default for active/active arrays
  - VMW\_PSP\_RR
    - The host will use all active paths in a round robin (RR) fashion. It uses an algorithm to iterate through all active paths. The default number of I/Os that are issued to a particular path is 1000 before moving on to the next active/available path
    - No default array types are listed for this PSP
- **Perform command line configuration of multipathing options**
    - There are a multitude of multipathing options that can be changed using the command line. Some can be changed in the GUI as well, but other settings must be changed via command line
    - In the **Install and Configuring PSA Plug-ins** I covered how to change the default PSP for a particular SATP, so I won't go over that again here
    - Changing the PSP on a particular device

```

1 # list details of the device you want to change, including the PSP
2
3 esxcli storage nmp device list -d naa.5000144fd4b74168
4
5 # this command will change the PSP for a particular device
6 # in this example I'm changing the PSP to VMW_PSP_FIXED
7
8 esxcli storage nmp device set -d naa.5000144fd4b74168 -P VMW_PSP_FIXED

```

- You can view device configurations for individual devices based on their assigned PSP. The following commands will view the device configurations for devices assigned the RR and Fixed PSPs. There will also be a command that lists the generic device configuration regardless of its assigned PSP

```
1 # list device configuration details for a device configured for VMW_PSP_FIXED
2
3 esxcli storage nmp psp fixed deviceconfig get -d naa.5000144ff548121b
4
5 # list the generic device configuration details for any device
6
7 esxcli storage nmp psp generic deviceconfig get -d naa.5000144fd4b74168
8
9 # list the device configuration details for a device configured for VMW_PSP_RR
10
11 esxcli storage nmp psp roundrobin deviceconfig get -d naa.5000144fd4b74168
```

- You can also set different parameters for PSP with **esxcli**. The following commands will set the preferred path on a device using VMW\_PSP\_FIXED and customize different parameters for a device using VMW\_PSP\_RR

```
1 # this command will set the preferred path on a device using the VMW_PSP_FIXED plug-in
2 # use -E will set it back to the default
3 # use -d to specify the device
4 # use -p to specify the path
5
6 esxcli storage nmp psp fixed deviceconfig set -d naa.5000144ff548121b -p vmhba35:C1:T
7
8 # run this command to see the preferred path has changed
9
10 esxcli storage nmp psp fixed deviceconfig get -d naa.5000144ff548121b
11
```

12

13 # these commands allow you to customize a device using the VMW\_PSP\_RR plug-in

14 # use -d to specify the device

15 # use -B to set the byte limit. This will only change if you specify the 'type' as 'b

16 # use -I to set the iops limit. This will only change if you specify the 'type' as 'i

17 # use -t to set the type of round robin path switching. Accepted values are 'bytes',

18 # use -U to allow round robin to use an active non-optimized path

19 # in this command we are changing the IOPs limit from its default of 1000

20 # to 2500. Remember you must use the -t parameter to specify 'iops' or the value will

21

22 esxcli storage nmp psp roundrobin deviceconfig set -d naa.5000144fd4b74168 -I 2500 -t

23

24 # run this command to see that the IOOperation Limit has changed to 2500

25

26 esxcli storage nmp psp roundrobin deviceconfig get -d naa.5000144fd4b74168

27

28 # run this command to set the device back to the VMW\_PSP\_RR default

29

30 esxcli storage nmp psp roundrobin deviceconfig set -d naa.5000144fd4b74168 -t default

31

32

- o You can also make changes to a device configuration using the *generic* option. Here is an example of changing a device that is using the VMW\_PSP\_RR plug-in

1 # use this command to list the current device configuration

2

3 esxcli storage nmp psp generic deviceconfig get -d naa.5000144fd4b74168

4

5 # here is what was returned

6 # '{policy=rr,iops=1000,bytes=10485760,useANO=0;lastPathIndex=0: NumIOsPending=0,numB

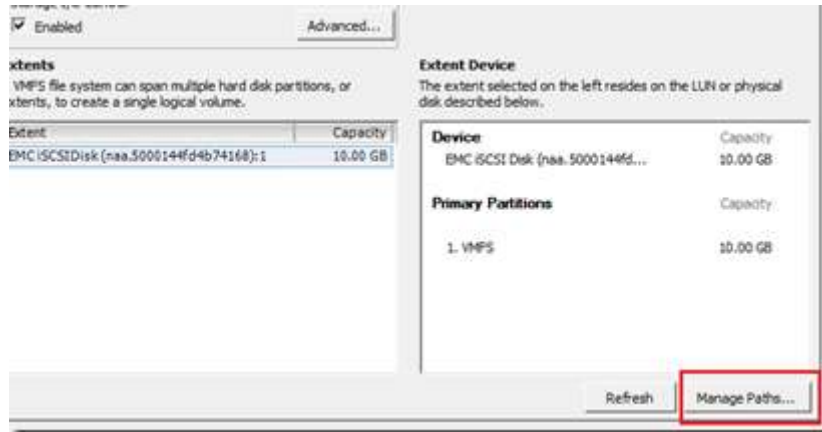
```
7
8 # use -d to specify the device
9 # use -c for the configuration
10 # you can make changes to the individual parameters by name. If you want to change th
11 # then use the '-P iops=#'
12 # unlike the previous command where you had to specify a 'type' in order to get the '
13 # to change, you do NOT have to specify that here
14
15 # changing the 'iops' to 5000
16
17 esxcli storage nmp psp generic deviceconfig set -d naa.5000144fd4b74168 -c 'iops=5000
18
```

- As you can see there are a lot of different things you can change with **esxcli** and multipathing configuration. Here is a video of performing some of these configurations

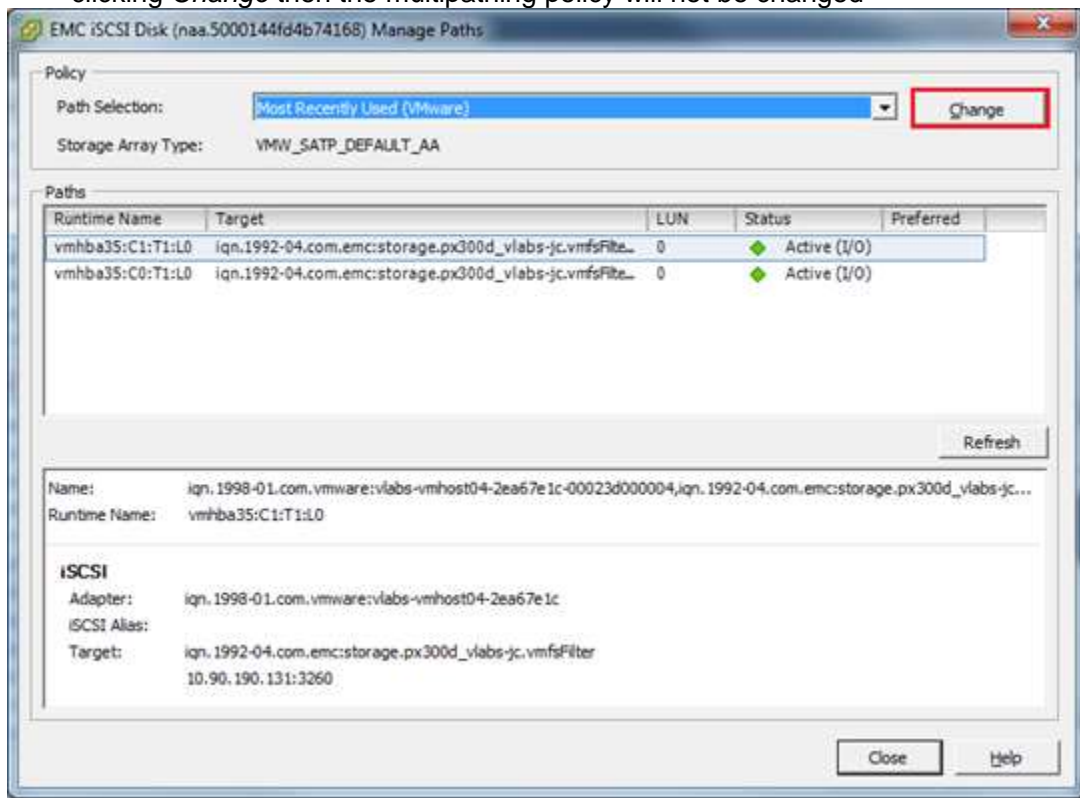
- **Change a multipath policy**

- You can change the multipathing policy a either in the GUI or via the command-line. I covered the command-line method in the previous section, **Perform command line configuration of multipathing options**, so I won't go over here again. Here is how you change the multipath policy in the GUI
  - Log into the vSphere client > select a host that is connected to the device you want to change the multipathing policy for
  - Click the *Configuration* tab > click the *Storage* hyperlink
  - Right-click the datastore you in which you want to modify the multipathing policy for > click *Properties...*
  - Click the *Manage Paths...* button





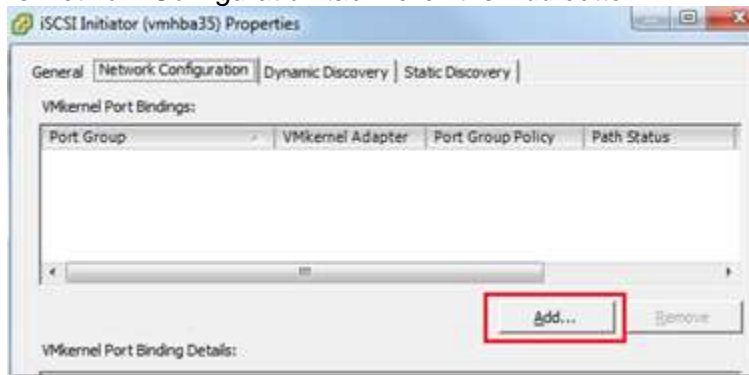
- From the *Path Selection*: drop-down select the multipathing policy you want to change it to
- Click *Change* << this is important, if you click the *Close* button without first clicking *Change* then the multipathing policy will not be changed



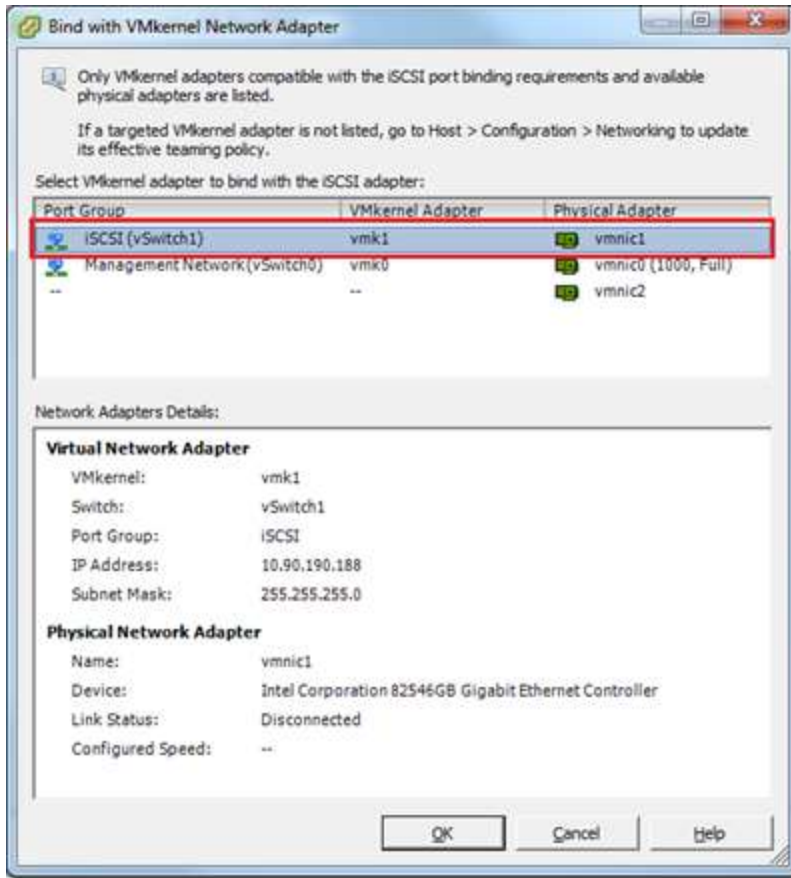
- Click *Close* (MAKE SURE YOU CLICKED CHANGE FIRST)
- Click *Close* to exit the datastore properties

- **Configure Software iSCSI port binding**

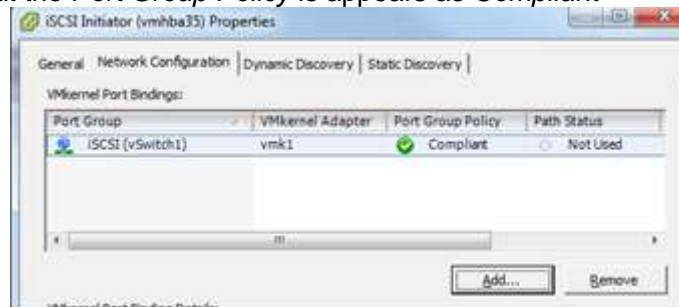
- Prior to vSphere 5 software iSCSI port binding could only be configured via the CLI. With the release of vSphere 5, VMware has made all of our lives easier and added this to the GUI (in the properties of the iSCSI software initiator)
- Before you begin the port binding process you need to have created 1:1 mappings of vmkernel adapters:physical adapters. This way, we can bind a single vmkernel adapter to a single physical adapter, enabling multipathing. Ensure these steps have been completed:
  - Created as many virtual switches or port groups as the number of physical adapters you will be using for iSCSI
  - You've created a vmkernel adapter for each vswitch or port group
  - You changed the *NIC Teaming* on each vswitch or port group to reflect on one active adapter and no standbys
  - the iSCSI software adapter is enabled and has its targets configured
- Once you have this done you need to configure port binding. Let's go through how to do it in the GUI first
  - Log into the vSphere client > select the host for which you are configuring iSCSI port binding on
  - Click the *Configuration* tab on the right > click the *Storage Adapters* hyperlink
  - Select the iSCSI software initiator > click the *Properties...* hyperlink
  - Select the *Network Configuration* tab > click the *Add* button



- Select the vswitch or port group that corresponds with the vmkernel adapter and physical adapter that you have setup for iSCSI



- Click OK
- Ensure that the *Port Group Policy* is appears as *Compliant*



- Click *Close* > click *Yes* to perform a rescan
- Now lets do the iSCSI port binding using **esxcli**

```

1 # we are binding the iscsi adapter (vmhba35) with vmk1, which has a 1:1 mapping with v
2
3 esxcli iscsi networkportal add -A vmhba35 -n vmk1
4
5 # run this command to verify the binding

```

6

7 `esxcli iscsi networkportal list`

- Here is the result of the list command, as you can see, vmhba35 and vmk1 are bound

```
/sbin # esxcli iscsi networkportal list
vmhba35
Adapter: vmhba35
Vmknic: vmk1
MAC Address: 00:04:23:c5:b2:3a
MAC Address Valid: true
IPv4: 10.90.190.188
IPv4 Subnet Mask: 255.255.255.0
IPv6:
MTU: 1500
```

## Tools

- [vSphere Installation and Setup Guide](#)
- [vSphere Storage Guide](#)
- [vSphere Command-Line Interface Concepts and Examples](#)
- [Product Documentation](#)
- vSphere Client
- vSphere CLI

# VCAP-DCA 5 Objective 2.1–Implement & Manage Complex Virtual Networks

## Objective 2.1 – Implement & Manage Complex Virtual Networks

For this objective I used the following resources:

- vCenter Server and Host Management guide
- vSphere Networking guide
- VMware White Paper – VMware vNetwork Distributed Switch: Migration and Configuration
- VMware KB Article 1008065
- VMware VROOM! Blog
- Eric Sloof's blog
- Jason Boche's blog

### Knowledge

#### Identify Common Virtual Switch Configurations

Focus around VMware best practices for virtual switches

- Use multiple physical uplinks per vSwitch
- Separate network traffic from VMkernel ports and VM traffic (VLANs, dedicated pNICs)
- Select the appropriate Load Balancing policy for your configuration
- Dedicated vSwitch for IP based storage (iSCSI, NFS)
- Secure network for Management Network traffic

### Skills and Abilities

#### Configure SNMP

- Configuring SNMP on vCenter Server
  1. Select *Administration* -> *vCenter Server Settings* to display the vCenter Server Settings dialog box
  2. In the settings list, select *SNMP*
  3. In Receiver URL, enter the host name or IP address of the SNMP receiver
  4. In the field next to the Receiver URL field, enter the port number of the receiver

Note – The port number must be a value between 1 and 65535

5. In Community, enter the community identifier

6. Click *OK*

For further information see page 37 of the *vCenter Server and Host Management* guide

- Configuring SNMP on an ESXi host

SNMP can be configured either via vSphere CLI or using the VMware vMA with the `vicfg-snmp` command. I will be outlining the process via the `vicfg-snmp` command.

- Specify the communities and trap targets

```
# vicfg-snmp -t <target hostname>@<port>/<community>
```

- Enable the SNMP service

```
# vicfg-snmp -E
```

- Send a test trap to verify that the agent is configured correctly

```
# vicfg-snmp -T
```

Eric Sloof ([blog](#) / [twitter](#)) has put together a great video going into greater detail of the above steps. Video located [HERE](#).

### Determine Use Cases For and Apply VMware DirectPath I/O

Josh Coen ([blog](#) / [twitter](#)) has already covered this top in Objective 1.1 located [HERE](#).

### Migrate a vSS Network to a Hybrid or Full vDS Solution

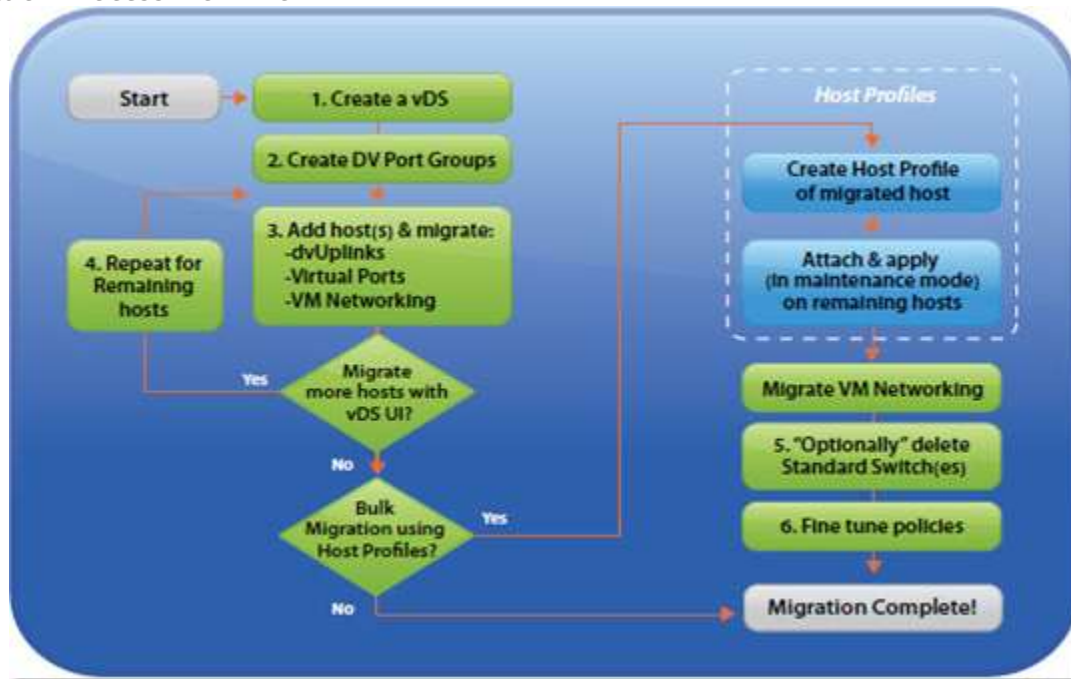
Migration from a vNetwork standard Switch only environment to one featuring one or more vNetwork Distributed Switches can be accomplished in either of two ways:

- Using only the vDS User Interface (vDS UI)
- Using a combination of the vDS UI and Host Profiles

*Table of Migration Methods*

Deployment Situation	Suggested Method	Details
New servers, same vmnic config, no active VMs	vDS UI + HP	Migrate first host with vDS UI. Take host profile and apply to remaining hosts
<5 Existing Servers, no active VMs	vDS UI	Small number of servers. Can use host profiles, but possibly easier to continue with vDS UI
>5 Existing servers, same vmnic configs, no active VMs	vDS UI + HP	Larger number of servers with similar vmnic configuration. No active VMs so can enter maintenance mode and use Host Profiles
Existing Servers, active/operational VMs	vDS UI	Cannot use Maintenance Mode as VMs active. Phased vmnic migration suggested to ensure continuity of VM communications
Existing Servers, dissimilar vmnic configurations	vDS UI	Enables per host tailoring of vmnic to dvUplink PortGroup mapping
Ongoing Compliance Checking	HP	Non-disruptively check network settings are compliant with approved "golden" configuration

## Migration Process Work Flow



*Host Migration with some Disruption to VMs* – The process outlined in Step 3 above includes two sub-steps:

- Migration of vmnics and virtual ports (VMkernel ports and Service Consoles) can be migrated in a single step from vCenter Server
- Migration of VM Networking where the VMs are migrated from vSS Port Groups to vDS DV Port Groups

If all vmnics are migrated in the first step above then all VMs will lose network connectivity until the following step is completed.

*Host Migration without Disruption to VMs*– If you need completely non-disruptive migration for VMs while deploying vDS, then a phased vmnic migration is required. The objective of a phased migration of vmnics is to maintain concurrent network connectivity over both vSS and vDS switches so that VM migration from vSS Port Groups to vDS DV Port Groups can proceed without interruption to network sessions.

Step 3 of the non-disruptive process based on the above flow chart is as follows

- Add host to vDS
- Migrate one vmnic from the NIC team supporting VM networking from vSS to vDS dvUplink
- Migrate VM networking from vSS Port Groups to vDS DV Port Groups
- Migrate remaining vmnics and virtual ports (vmkernel and Service Consoles) to vDS

*Source: VMware White Paper – VMware vNetwork Distributed Switch: Migration and Configuration*

### ***Configure vSS and vDS Settings Using Command Line Tools***

#### ***Analyze Command Line Output to Identify vSS and vDS Configuration Details***

I am grouping both of these topics together as you will utilize most of the same commands to either configure or gain insight on how a vSS or vDS is configured. Also of note, the `esxcfg-*` commands are still available however learn and study the new `esxcli` commands as well.

Several commands can be used to configure vSwitches

- `esxcfg-vswitch` – Examine and configure virtual switches
- `esxcfg-vswif` – Examine and configure service console ports
- `esxcfg-vmknic` – Examine and configure VMkernel ports
- `esxcfg-route` – Examine and configure routing
- `esxcli network namespace`
  - `ip namespace` – Commands to create/configure vmk nics
  - `vswitch namespace` – Command to manipulate virtual switches
  - `nic namespace` – Configuration of physical interfaces

#### **Configure Netflow**

1. Log in to the vSphere Client and select the *Networking* inventory view
2. Right-click the vSphere distributed switch in the inventory pane, and select *Edit Settings*
3. Navigate to the *NetFlow* tab
4. Type the *IP address* and *Port* of the NetFlow collector
5. Type the *VDS IP address*
6. (Optional) Use the up and down menu arrow to set the *Sampling rate*.
7. (Optional) Select *Process internal flows only* to collect data only on network activity between virtual machines on the same host
8. Click *OK*

For further reading see page 70 of the *vSphere Networking* guide as well as [THIS](#) post on the VMware Networking blog

Eric Sloof again has a great video to guide you through the above steps located [HERE](#).

#### **Determine Appropriate Discovery Protocol**

Switch discovery protocols allows vSphere administrators to determine which switch port is connected to a given vSphere standard switch (CDP only) or vSphere distributed switch (both CDP and LLDP).



- Enable Cisco Discovery Protocol on a vDS

1. Log in to the vSphere Client and select the *Networking* inventory view
2. Right-click the vSphere distributed switch in the inventory pane, and select *Edit Settings*
3. On the *Properties* tab, select *Advanced*
4. Select *Enabled* from the Status drop-down menu
5. Select *Cisco Discovery Protocol* from the *Type* drop-down menu
6. Select the CDP mode from the *Operation drop-down menu*

Option	Description
--------	-------------

Listen	ESXi detects and displays information about the associated Cisco switch port, but information about the vSphere distributed switch is not available to the Cisco switch administrator
--------	---

Advertise	ESXi makes information about the vSphere distributed switch available to the Cisco switch administrator, but does not detect and display information about the Cisco switch
-----------	---

Both	ESXi detects and displays information about the associated Cisco switch and makes information about the vSphere distributed switch available to the Cisco switch administrator
------	--

7. Click *OK*

- Enable Link Layer Discovery Protocol on a vDS

1. Log in to the vSphere Client and select the *Networking* inventory view
2. Right-click the vSphere distributed switch in the inventory pane, and select *Edit Settings*
3. On the *Properties* tab, select *Advanced*
4. Select *Enabled* from the Status drop-down menu
5. Select *Link Layer Protocol* from the *Type* drop-down menu
6. Select the LLDP mode from the *Operation drop-down menu*

Option	Description
--------	-------------

Listen	ESXi detects and displays information about the associated physical switch port, but information about the vSphere distributed switch is not available to the switch administrator
--------	--

Advertise	ESXi makes information about the vSphere distributed switch available to the physical switch administrator, but does not detect and display information about the physical switch
-----------	---

Both	ESXi detects and displays information about the associated physical switch and makes information about the vSphere distributed switch available to the switch administrator
------	---

7. Click *OK*

For further reading see page 70 of the *vSphere Networking* guide.

Jason Boche ([blog](#) / [twitter](#)) has also written two blog posts covering the use of CDP and LLDP. They can be found [HERE](#) and [HERE](#).

# VCAP-DCA 5 Objective 2.2 – Configure & Maintain VLANs, PVLANS, & VLAN Settings

## Objective 2.2 – Configure & Maintain VLANs, PVLANS, & VLAN Settings

For this objective I used the following resources

- VMware KB Article 1010691
- VMware KB Article 1004048
- VMware KB Article 1010703
- Chris Wahl's blog
- IT Cookbook blog

### Knowledge

#### **Identify types of VLANs and PVLANS**

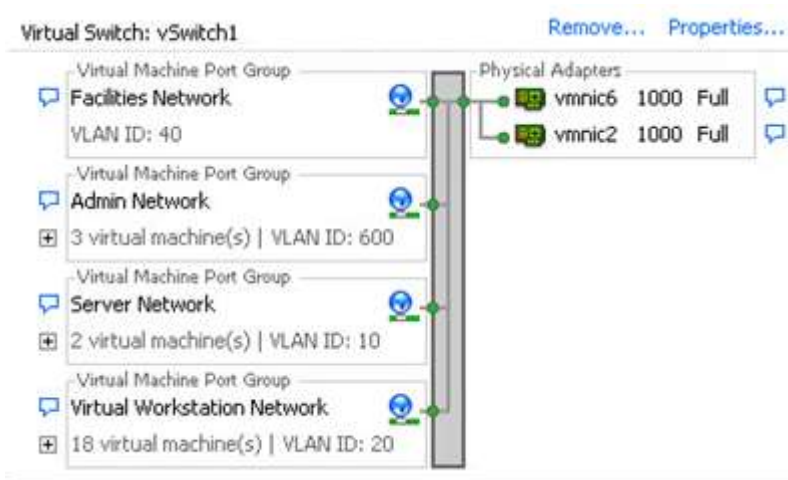
- A VLAN (virtual lan) is a grouping of hosts that are able to communicate in the same broadcast domain even though they may not be physically plugged into the same network device
- VLAN Trunking is the ability to pass multiple VLAN traffic (thus sharing) through a singular physical network connection
- Private VLANs allow you to isolate traffic between virtual machines in the same isolated VLAN. These isolated PVLANS are referred to as the primary VLAN divided into secondary VLANs. PVLANS are only configurable in ESX on vDS. There are three types of secondary PVLAN:
  1. Promiscuous – VM's are reachable by and can reach any machine in the same primary VLAN
  2. Isolated – Vm's can talk to no virtual machines except those in the promiscuous PVLAN
  3. Community – VM's can talk to each other and to the VMs in the promiscuous PVLAN, but not to any other VM

See [VMware KB Article 1010691](#) "Private VLAN (PVLAN) on vNetwork Distributed Switch – Concept Overview" for additional reading.

### Skills and Abilities

#### **Determine use cases for and configure VLAN Trunking**

Use case for using VLAN trunking would be if you have multiple VLANs in place for logical separation or to isolate your VM traffic but you have a limited amount of physical uplink ports dedicated for your ESXi hosts. For example:



In the above example four port groups are created and are “tagged” with the required VLAN id’s that are used. Each of the vmnics is bonded together in an EtherChannel(completed on the physical Cisco switch) and is configured to “trunk” the various VLANs. On the ESXi switch side the NIC Teaming Load Balancing Policy will need to be set to Route based on IP hash. Note – this is just an example, you do not have to/need to use EtherChannel/Link aggregation to use VLAN trunking.

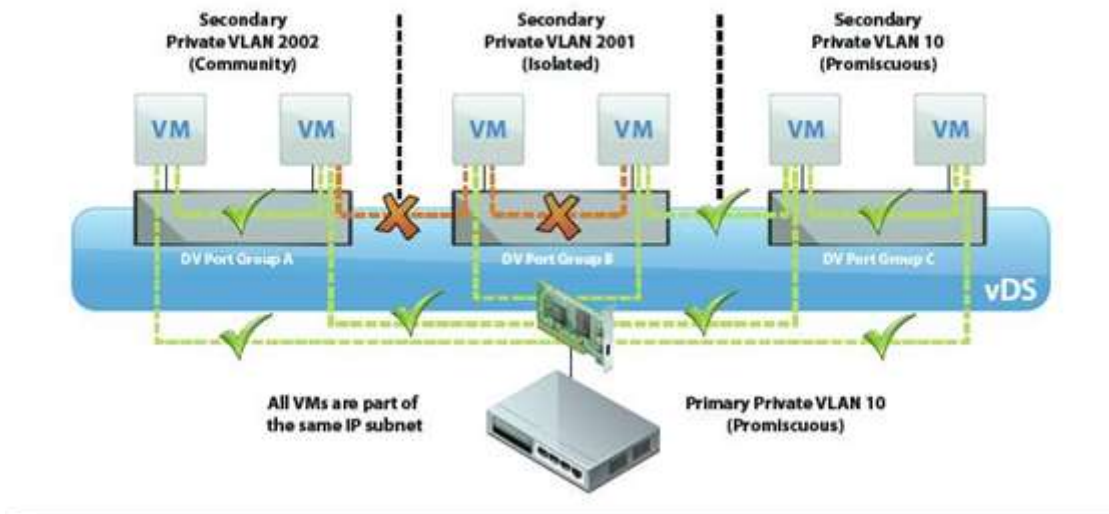
For additional reading on configuring and using EtherChannel or Link Aggregation see [VMware KB Article 1004048](#) “Sample Configuration of EtherChannel/Link aggregation with ESX/ESXi and Cisco/HP switches”

Chris Wahl ([blog](#) / [twitter](#)) has also has an excellent blog article outlining the use of Trunks and Portgroups with vSphere. Article found [HERE](#).

### Determine use cases for and configure PVLANS

Private VLANs provide additional security between virtual machines on the same subnet without exhausting VLAN number space. PVLANS are particularly useful on a DMZ where the server needs to be available to external connections and possibly internal connections, but rarely needs to communicate with other servers on the DMZ. This may be more easily explained with a picture:

Figure 4 - Private VLANs provide a simple way of selectively isolating VMs without exhausting IP subnets.



(Graphic supplied by [IT Cookbook - real world experience](#))

Configuring a PVLAN is completed as follows

1. In vCenter, go to Home -> Inventory -> Networking
2. Click Edit Settings on the desired dvSwitch
3. Choose the Private VLAN tab
4. On the Primary tab, add the VLAN that is used outside the PVLAN domain. Enter a private VLAN ID and/or choose one from the list
5. On the Secondary Tab, create the PVLANS of the desired type (see definitions above). Enter a VLAN ID in the VLAN ID field
6. Select the Type for the Secondary VLAN ID
7. Click Ok

To set the PVLAN in the dvPortGroup

1. Highlight dvPortGroup and click Edit Settings
2. Click General -> VLAN -> Policies
3. Using the dropdown, set the VLAN type to Private
4. Select VLAN from the Private VLAN Entry dropdown

Above procedure was taken from [VMware KB Article 1010703](#) "Configuration of Private VLAN (PVLAN) on vNetwork Distributed Switch"

Again, Chris Wahl has a great article covering the use of Private VLANs (PVLANS) in vSphere. Article is located [HERE](#).

**Use command line tools to troubleshoot and identify VLAN configurations**

See section "Configure vSS and vDS Settings Using Command Line Tools" in Objective 2.1 located [HERE](#).

### **Additional Resources**

To further “pimp out” Chris Wahl, he recently covered all of Section 2 objectives on the ProfessionalVMware Brownbag series. Available [HERE](#) on iTunes (release date is 9 5 12).

# VCAP-DCA 5 Objective 2.3 – Deploy & Maintain Scalable Virtual Networking

## Objective 2.3 – Deploy & Maintain Scalable Virtual Networking

For this objective I used the following resources:

- vSphere Networking Documentation
- VMware Virtual Networking Concepts Whitepaper
- VMware KB Article 1006558
- VMware KB Article 1006778
- VMware KB Article 1005577
- VMware KB Article 1002722
- VMware KB Article 1004088
- VMware KB Article 1004048
- VMware KB Article 1001938

### Knowledge

#### **Identify VMware NIC Teaming Policies**

- Load Balancing – Determines how OUTGOING traffic is distributed among the network adapters assigned to a vSwitch. Four options are available:
  1. *Route based on the originating port ID (Default)* – Choose an uplink based on the virtual port where the traffic entered the virtual switch
  2. *Route based on IP Hash* – Choose an uplink based on a hash of the source and destination IP addresses of each packet. For non-IP packets, whatever is at those offsets is used to compute the hash (See [VMware KB Article 1001938](#) “ESX/ESXi host requirements for link aggregation” for further reading)
  3. *Route based on source MAC Hash* – Choose an uplink based on a hash of the source Ethernet
  4. *Use explicit failover order* – Always use the highest order uplink from the list of Active adapters which passes failover detection criteria
- Network Failover Detection – Controls the link status and beacon probing. Beaconing is not supported with guest VLAN tagging. Two options for use:
  1. *Link Status Only* – Relies solely on the link status that the network adapter provides. This option detects failures, such as cable pulls and physical switch power failures, but not configuration errors, such as a physical switch port being blocked by spanning tree or that is misconfigured to the wrong VLAN or cable pulls on the other side of a physical switch.

2. *Beacon Probing* – Sends out and listens for beacon probes on all NICs in the team and uses this information, in addition to link status, to determine link failure. This detects many of the failures previously mentioned that are not detected by link stats alone (See [VMware KB Article 1005577](#) “What is beacon probing?” on how beacon probing works and how to properly implement).

- *Notify Switches* – Select Yes or No to notify switches in the case of failover. If you select Yes, whenever a virtual NIC is connected to the vSwitch or whenever that virtual NIC’s traffic would be routed over a different physical network to update the lookup tables on physical switches. In almost all cases, this process is desirable for the lowest latency of failover occurrences and migrations with vMotion

*Note – Do not use this option when the virtual machines using the port group are using Microsoft Network Load Balancing in unicast mode. No such issue exists with NLB running in multicast mode. For proper implementation of MS NLB have a look at [VMware KB Article 1006558](#) “Sample Configuration – Network Load Balancing (NLB) Multicast Mode Configuration” or [VMware KB Article 1006778](#) “Sample Configuration – Network Load Balancing (NLB) UNICAST Mode Configuration”.*

- *Failback* – Select Yes or No to disable or enabled failback. This option determines how a physical adapter is returned to active duty after recovering from a failure. If failback is set to Yes (default), the adapter is returned to active duty immediately upon recovery, displacing the standby adapter that took over its slot, if any. If failback is set to No, a failed adapter is left inactive even after recovery until another currently active adapter fails, requiring its replacement.
- *Failover Order* – Specify how to distribute the work load for uplinks, If you want to use some uplinks but reserve others for emergencies in case the uplinks in use fail, set this condition by moving them into different groups:
  - *Active Uplinks* – Continue to use the uplink when the network adapter connectivity is up and active
  - *Standby Uplinks* – Use this uplink if one of the active adapter’s connectivity is down
  - *Unused Uplinks* – Do not use this uplink

Information above taken from the *vSphere Networking* documentation and the *VMware Virtual Networking Concepts* whitepaper. For a brief video on configuring NIC teaming see [VMware KB Article 1004088](#) “NIC teaming in ESXi and ESX”.

### **Identify Common Network Protocols**

A brief list of what I think are “common” protocols:

- HTTP – TCP Port 80

- HTTPS – TCP Port 443
- Telnet – TCP Port 23
- SSH – TCP Port 22
- SNMP – UDP Port 161
- DNS – TCP/UDP Port 53

### Skills and Abilities

#### **Understand the NIC Teaming Failover Types and Related Physical Network Settings**

Review information under “Identify VMware NIC Teaming Policies”. For information on physical network settings to use the IP Hash load balancing policy review the following VMware KB Articles:

- [VMware KB Article 1001938](#) “ESX/ESXi host requirements for link aggregation”
- [VMware KB Article 1004048](#) “Sample configuration of EtherChannel / Link aggregation with ESX/ESXi and Cisco/HP switches”

#### **Determine and Apply Failover Settings**

Review information under “Identify VMware NIC Teaming Policies”

#### **Configure Explicit Failover to Conform with VMware Best Practices**

See [VMware KB Article 1002722](#) “Dedicating specific NICs to portgroups while maintaining NIC teaming and failover for the vSwitch” for an example of this configuration

#### **Configure Portgroups to Properly Isolate Network Traffic**

Review the VMware KB Article listed above as well as leverage the use of VLAN tagging on a vSwitch/portgroups to further isolate network traffic



# VCAP-DCA 5 Objective 2.4—Administer vNetwork Distributed Switch Settings

## **Objective 2.4 – Administer vNetwork Distributed Switch Settings**

For this objective I used the following resources:

- VMware KB Article 1022312
- VMware KB Article 1010555
- VMware YouTube Channel
- VMware Network I/O Control: Architecture, Performance and Best Practices White Paper
- VMware & Cisco Virtual Networking Features of the VMware vNetwork Distributed Switch and Cisco Nexus 1000V Switches
- VMware & Cisco DMZ Virtualization Using VMware vSphere 4 and the Cisco Nexus 1000V Virtual Switch
- VMware Networking Blog
- Geeksilver's Blog
- Trainsignal Blog

### Knowledge

#### **Describe the Relationship Between vDS and the VSS**

vDS is short for “vNetwork Distributed Switch” and VSS is short for “Virtual Standard Switch”. VSS configuration and data is maintained on an individual host level where vDS configuration is saved in the vCenter database and a cached copy is maintained on each host. This cache is updated every 5 minutes. An ESXi 5 host can use both switch technologies at the same time for a “hybrid” implementation.

Check out two great articles over at GeekSilver's Blog on vDS:

- [vDS \(vNetwork Distributed Switch\) My Understanding Part 1](#)
- [vDS \(vNetwork Distributed Switch\) My Understanding Part 2](#)

Also have a look at [VMware KB Article 1010555](#) “*Overview of vNetwork Distributed Switch Concepts*”

### Skills and Abilities

#### **Understand the Use of Command Line Tools to Configure Appropriate vDS Settings on an ESXi Host**

Will most configuration of a vDS is done via the vCenter Client there are a few commands that can be used from the CLI:

To list and view all switches (vSS and vDS) on a host

```
# esxcfg-vswitch -l
```

Add an uplink to a DVPort on a DVSwitch

```
# esxcfg-vswitch -add-dvp-uplink=<vmnic> (or -P)
```

Delete an uplink from a DVPort on a DVSwitch (Must specify DVPort ID)

```
#esxcfg-vswitch -del-dvp-uplink=<vmnic> (or -Q)
```

Specify a DVPort Id for the operation

```
#esxcfg-vswitch -dvp=<dvport> (or -V)
```

### Determine Use Cases For and Apply Port Binding Settings

Port binding determines when and how a virtual machine's virtual NIC is assigned to a virtual switch port. There are three port binding options that are configurable at the port group level:

- *Static Binding*- The default setting, a virtual switch port is permanently assigned to the VM's NIC when the NIC is configured. No further VM connections are possible once all current virtual switch ports are assigned
- *Dynamic Port Binding (Deprecated in ESXi 5.x)*- The virtual switch port is assigned to the VM's NIC at the moment the virtual machine is powered on. This option allows for virtual switch port over commitment
- *Ephemeral Port Binding (None)* - Resembles the behavior of standard virtual switch port assignment, the number of ports will be automatically set to unlimited. You can continue to connect virtual machines up to the maximum number of ports available for a distributed switch

Review [VMware KB Article 1022312](#) "Choosing a port binding type" for more details

### Configure Live Port Moving

From the Trainsignal.com Blog article ["VMware Networking: Configuring and Troubleshooting a vNetwork Part 2"](#) Live Port Moving is described as:

*Transfer stand-alone port groups to distributed port groups, assigning settings associated with distributed port group to the stand-alone group*

As there is no mention that I could find in the VMware core document set for Live Port Moving that will have to do. 😊

To configure follow the below steps:

1. In the vSphere Client, display the Networking inventory view and select the dvPort group
2. From the Inventory menu, select Network -> Edit Settings
3. Select Advanced to edit the dvPort group properties
4. Choose whether to allow live port moving
5. Click OK

### **Given a Set of Network Requirements, Identify the Appropriate Distributed Switch Technology to Use**

Besides offering the vDS, VMware also allows for a 3rd party switch to be installed and used on ESXi hosts (rides over the top of the vDS technology). Currently the only vendor supplied switch on the market is the Cisco Nexus 1000v. Listed below is various information about both:

- vDS and Cisco 1000v require Enterprise Plus licensing
  - 1KV requires additional licensing from Cisco (per CPU)
  - vDS is managed via vSphere Gui/1KV is managed via Cisco IOS
  - 1KV uses a virtual supervisor module and virtual Ethernet module
- VMware and Cisco have put together to papers outlining the use of the Nexus 1KV (still relevant though base on vSphere 4.x)
- [\*Virtual Networking Features of the VMware vNetwork Distributed Switch and Cisco Nexus 1000V Switches\*](#)
  - [\*DMZ Virtualization Using VMware vSphere 4 and the Cisco Nexus 1000V Virtual Switch\*](#)

### **Configure and Administer vSphere Network I/O Control**

Enabling Network I/O Control is a easy a checking a checkbox. The configuration is the far more trickier part. Review the following links for further information and “Best Practices” for NIOC:

- VMware YouTube video, [\*“vSphere Network IO Control”\*](#)
  - [\*VMware Network I/O Control: Architecture, Performance, and Best Practices\*](#)(based on vSphere 4.1)
  - VMware Networking Blog [\*“vSphere 5 New Networking Features – Enhanced NIOC”\*](#)
- ### **Use Command Line Tools to Troubleshoot and Identify Configuration Items from an Existing vDS**

Other than commands covered in above you can use the `net-dvs` command on an ESXi host. The command is located in the `/usr/lib/vmware/bin` directory. To see the use of the command refer to the link above to GeekSilver's Blog for "vDS, My Understanding Part 1"

# VCAP5-DCA-Objective 3.1–Tune and Optimize vSphere Performance

---

For this objective I used the following documents:

- [Performance Best Practices for VMware vSphere 5.0](#)
- [vSphere Resource Management Guide](#)
- Documents listed in the Tools section

## ***Objective 3.1 – Tune and Optimize vSphere Performance***

### Knowledge

**\*\*ITEMS IN BOLD ARE TOPICS PULLED FROM THE BLUEPRINT\*\***

- **Identify appropriate BIOS and firmware setting requirements for optimal ESXi host performance**
  - BIOS settings on your hosts is an important thing to take into consideration when optimizing your environment. Here are some general guidelines (pulled from the aforementioned whitepaper) you can follow that will assist you in your optimization efforts
    - Ensure you are using the most up-to-date firmware for your host
    - Ensure all populated sockets are enabled
    - Enable “Turbo Boost” if your processor supports it (is this like the turbo button on my x486?)
    - If your processor(s) support hyper-threading, make sure it is enabled
    - Disable node interleaving (enable this will essentially disable NUMA)
    - Disable any hardware devices that you won’t be using
    - Depending on your workload characteristics you may, or may not, want to disable cache prefetching features. Workloads that randomly access memory may get a performance boost if these features are disabled
    - Set the CPU power-saving features to “OS Controlled”
      - this will allow the hypervisor to control and manage these features
    - Last, but certainly not least, enable Hardware Virtualization (VT). You will know right away if this is NOT enabled if you try and boot a 64-bit virtual machine and get a ‘longmode’ error

- **Identify appropriate driver revisions required for optimal ESXi host performance**
  - I don't know exactly what it is they are looking for here, and I can't find it in any of their product documentation. A few things that come to mind though:
    - Check the [VMware HCL](#)
      - From the dropdown you can select a category of what you are looking for



- In this example I chose *IO Devices*
- You can then select which VMware product and version and then select which vendor and I/O Device type
- Click *Update and View Results*
- Scroll through the list until you find the device you are looking for. The model of the device should be a hyperlink, click the hyperlink
- Here you will see pertinent information for the release and the device driver to use

Model Detail		
Model:	Emulex OneConnect OCe10102-FX 10GbE FCoE, NIC, iSCSI CNA	VID: 19a2
Device Type:	FCoE CNAs	DID: 0704
Partner Name:	Emulex	SVID: 10DF
Number of Ports:	0	SSID: E602
Notes:		
Model Release Details		
Release	Device Driver(s)	Firmware Version
<input checked="" type="checkbox"/> ESXi 5.0 U1	lpfc820 version 8.2.2.105.34	N/A
ESXi 5.0 U1	lpfc820 version 8.2.2.1-18vmw	N/A

- I have no idea if this is the 'optimized' driver, but logically you would think it's the best device driver for that device, based on the product version
- The next best place to look would be to check the vendor's website and see if they have made a separate driver to use with your version of vSphere

## Skills and Abilities

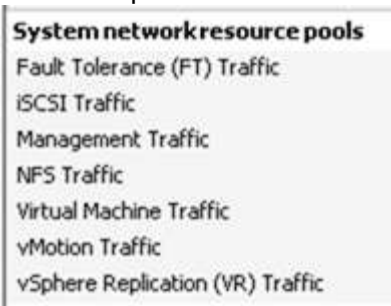
- **Tune ESXi host memory configuration**

- In this section (and the rest of the “tuning” sections) I will not go over how to identify bottlenecks or misconfigurations (such as using ESXTOP to diagnose). I will simply be listing some recommended practices that should optimize and make your hosts more efficient. Troubleshooting will be covered in section 6
- One thing that you will see a lot of are blanket memory configurations for virtual machines, such as all Windows Server 2K8 R2 VMs will get a base of 4GBs of RAM and will only be increased if needed. On the surface this seems like a good practice, but what if that VM only needs 3GB?
  - Virtual machine memory overhead is dependent on the configured memory size of a virtual machine, the more you configure, the more overhead it takes, the less memory is available for your other virtual machines.
    - Don't under-configure the memory where the working set can't keep up because of too little memory (thrashing)
    - Don't over-configure the memory where the working set doesn't use all the configured memory and now you have wasted more memory than needed on memory overhead
- The same concept above applies to the number of vCPUs you configure for a virtual machine. The more vCPUs you configure increases the amount of memory overhead.
  - Don't give you virtual machines more vCPUs than what is needed. Doing so increases memory overhead
- Memory over-commitment is a feature of vSphere, and VMware has 5 different mechanisms to deal with over-commitment. There are a few things to keep in mind when talking about over-commitment, and tuning our hosts to use it effectively
  - The biggest degradation of performance to a virtual machine is when the host starts swapping to disk. There are four other memory over-commitment techniques that are used before swapping to disk
    - Don't disable these other memory over-commitment techniques; ballooning, page sharing and memory compression
- Use the new swap to host cache feature

- This is a new memory over-commitment technique that allows the host to swap to cache instead of to disk. The 'cache' it is referring to is a SSD disk
  - Configure a SSD as host cache, which will get much better performance than swapping to traditional disk
- Virtual machine swap files are created in the VM working directory by default (typically where the .vmx file is located)
  - Ensure that location of those swap files have enough free disk space. The swap file is created dynamically during a power on operation and is the same size as the configured memory for that VM
  - Don't place swap files on thin-provisioned disks
- The biggest take away here should be, its OK to overcommit memory, but not to the point where you are swapping out to disk.

- **Tune ESXi host networking configuration**

- One thing that you want to monitor when thinking about virtual networking and how to make it perform as efficient as possible is your CPU utilization. Virtual networking relays heavily on the CPU to process the network queues. The higher CPU utilization you have, the less throughput you make get
- DirectPath I/O may provide you a bump in network performance, but you really need to look at the use case. You can lose a lot of core functionality when using this feature, such as vMotion and FT (some special exceptions when running on UCS for vMotion) so you really need to look at the cost:benefit ratio and determine if it's worth the tradeoffs
- You can control your bandwidth and how it is allocated by using Network I/O Control (NIOC). You allocate bandwidth to resource pools and use shares/limits to establish priority. There are seven pre-defined network resource pools:

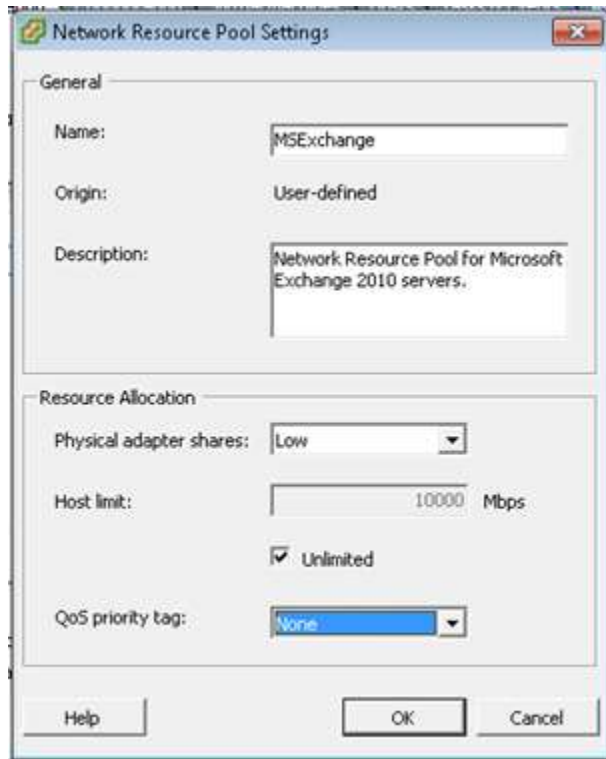




- There is also something called a user-defined resource pool in which you can create your own resource pool in order to prioritize other traffic not covered by the pre-defined pools
- User-defined pools are pretty archaic, all you can do is assign shares and a QoS priority tag. Let's go through an example of creating a user-define network resource pool:
  - Log into the vSphere client
  - Switch to the *Networking* view by selecting the *View* menu > select *Inventory* > select *Networking* (*Ctrl + Shift + N*)
  - Select a vDistributed Switch from the inventory on the left (remember that NIOC requires an enterprise+ license) > click the *Resource Allocation* tab
  - Click the *New Network Resource Pool...* hyperlink



- Enter in a *Name* and *Description*
- Set the *Physical Adapter Shares* value (*Low, Normal, High or Custom*)
- If you *Uncheck* the *Unlimited* option be sure to enter in what amount, in *Mbps* that you want to set it to
- Set a *QoS Priority Tag* if desired and select a tag from the dropdown (1-7)
- Click *OK*



- Use separate vSwitches with different physical adapters. Doing so should help avoid unnecessary contention between the VMkernel and virtual machines
- The use of the VMXNET3 paravirtualized adapter should be used as the standard, not the exception. When creating new virtual machines you should be asking yourself “Why shouldn’t I use VMXNET3?”, not “Why should I use VMXNET3?”
- If you have network latency sensitive applications you want to adjust the ESXi host power management settings to the maximum performance. You do this so resources aren’t asleep for some reason when your application needs them
  - Log into the vSphere client and navigate to the *Hosts and Clusters* view
  - Select a host from the inventory > click the *Configuration* tab
  - In the *Hardware* pane click the *Power Management* hyperlink
  - Click the *Properties* hyperlink in the upper right
  - Select the *High Performance* option
  - Click *OK*
- Also for applications that are sensitive to network latency you want to disable *C1E* and other *C-states* in the BIOS of the host(s) that the application may run on
- When using the VMXNET3 networking adapter, there is a feature called virtual interrupt coalescing. Disabling this feature can improve performance for certain network latency-

sensitive applications. However, be careful when enabling this as it may reduce performance for other types of workloads. This is enabled per-VM with the *ethernetX.coalescing.Scheme* advanced configuration option, which we'll go over configuring in a later section

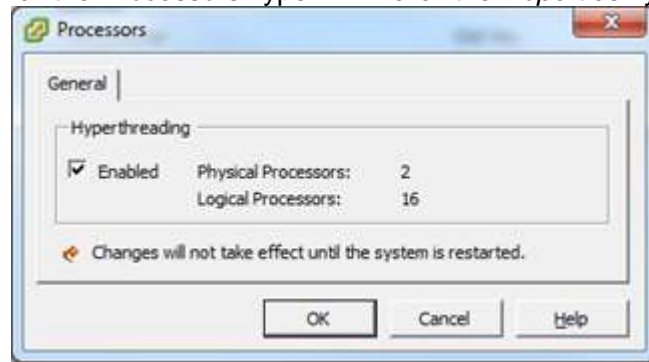
- SplitRx Mode is a new feature that was introduced with vSphere 5.0 and it can improve performance for virtual machines in certain circumstances. Typically, networking traffic comes into a network queue and is processed by a single physical CPU. SplitRx Mode is a per-VM setting that allows network traffic coming into a single network queue to be processed by multiple physical CPUs
  - If the VM is a network appliance that is traversing traffic between virtual machines on the same host using the API, then throughput may be increased with the use of SplitRx
  - If you have more than one virtual machine on the same host receiving multicast traffic from the same location then SplitRx can improve throughput and CPU efficiency
  - Enable SplitRx mode using the *ethernetX.emuRxMode* advanced configuration setting

- **Tune ESXi host CPU configuration**

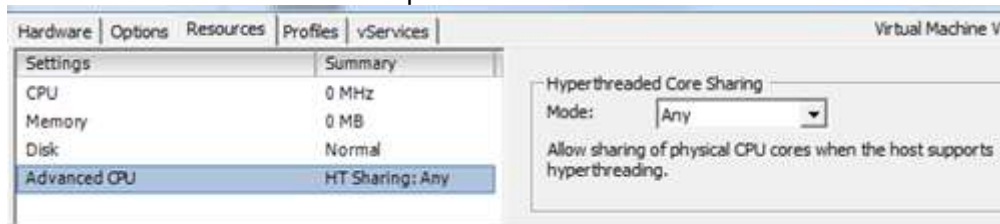
- This may be a given, but turn on DRS. You don't want a host getting overloaded with VMs and maxing out the CPU when there are other hosts in your cluster that have idle CPU cycles
- Don't configure your VMs for more vCPUs than their workloads require. Configuring a VM with more vCPUs than it needs will cause additional, unnecessary CPU utilization due to the increased overhead relating to multiple vCPUs
- If your hardware supports Hyper-threading (the hardware itself and BIOS) then the hypervisor should automatically take advantage of it. If your hardware does support hyper-threading but it doesn't show enabled in vCenter, ensure that you enable it in your hardware BIOS
  - Here you can see that hyper-threading is enabled

Processors			
General			
Model	Intel(R) Xeon(R) CPU	E5520	@ 2.27GHz
Processor Speed	2.3 GHz		
Processor Sockets	2		
Processor Cores per Socket	4		
Logical Processors	16		
Hyperthreading	Enabled		

- In vCenter you can enable/disable hyper-threading by going to the *Configuration* tab of the host > click the *Processors* hyperlink > click the *Properties* hyperlink



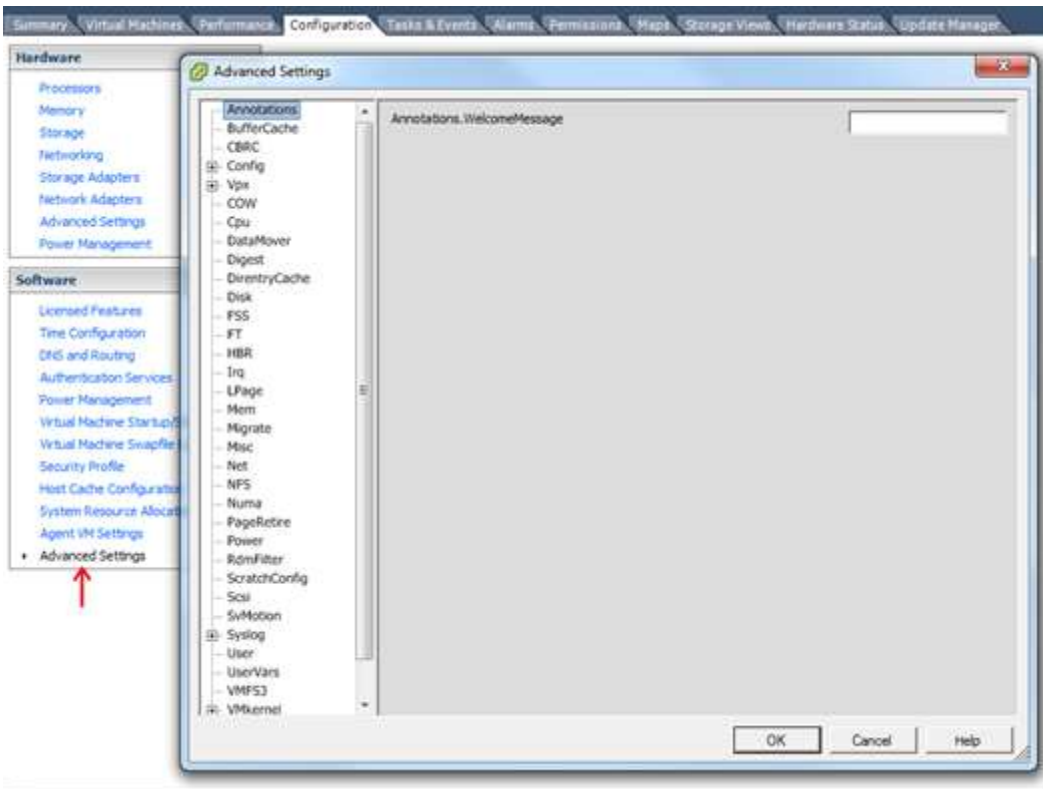
- When using hyper-threading ensure that you leave the per-VM advanced CPU setting to *Any*. Changing this setting to *None* will essentially disable hyper-threading for that particular virtual machine as it will place the other 'core' in a halted state



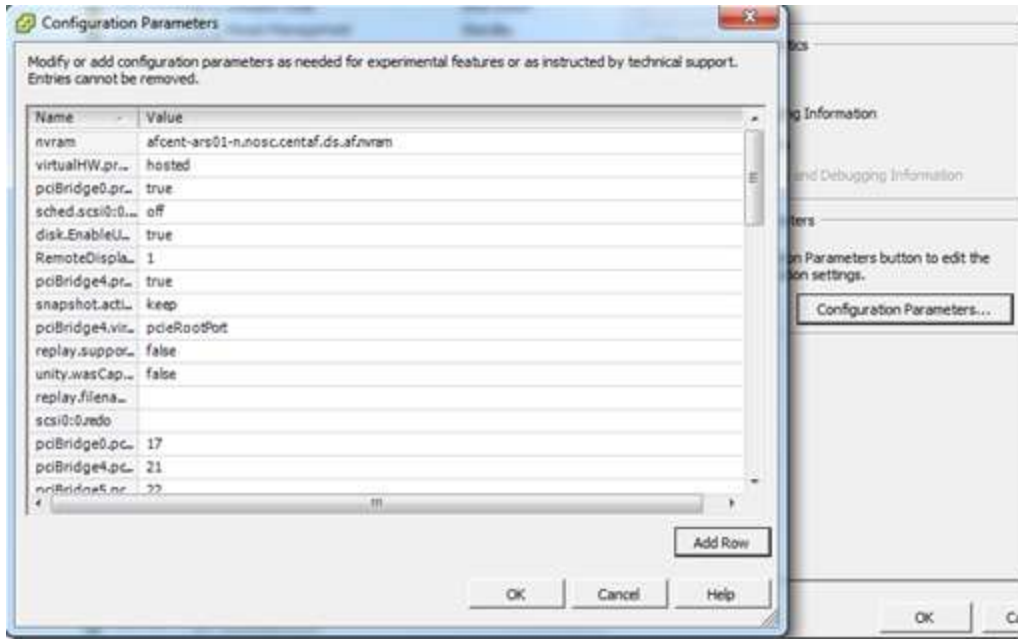
- When dealing with NUMA systems, ensure that node interleaving is disabled in the BIOS. If node interleaving is set to enabled it essentially disables NUMA capability on that host
- When possible configure the number of vCPUs to equal or less than the number of physical cores on a single NUMA node
  - When you configure equal or less vCPUs:physical cores the VM will get all its memory from that single NUMA node, resulting in lower memory access and latency times

- **Tune ESXi host storage configuration**

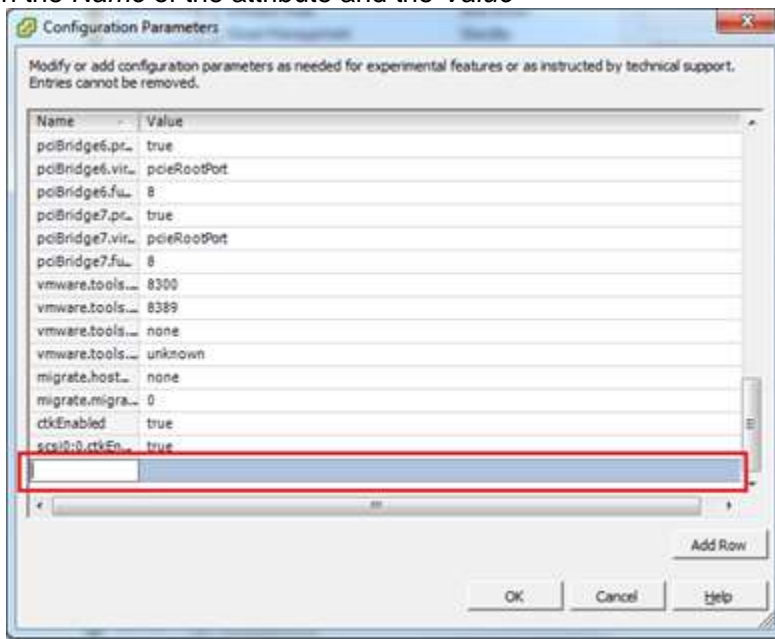
- Enable Storage DRS. Even if you set it to manual, enable Storage DRS in order to get the initial placement recommendations. Storage DRS is enabled by creating a *Datastore Cluster*. This has been covered in [Objective 1.2 – Manage Storage Capacity in a vSphere Environment](#) so I won't go over it again, but just know that you should enable this when possible
  - Turn on Storage I/O Control (SIOC) to split up disk shares globally across all hosts accessing that datastore. SIOC will proportionally assign disk shares per-host based on the sum of VM disks shares and total disk shares for that datastore
  - Ensure that the storage configuration setup has enough IOPs to support the virtual machine workloads running on said storage
  - One of the key metrics you want to monitor in *r/esxtop* are GAVG counters, these are the “guest average” counters and they indicate what the guest VM is seeing. For example, the GAVG/cmd counter will show what latency the guest VM is seeing when accessing that particular storage device. Again, this will be covered more in-depth in Section 6
  - Ensure that your multi-pathing policies are set in accordance with the best practices from VMware and your storage vendor. Even if the multi-pathing policy you are currently using might be working, it doesn't mean that there isn't a better one out there that is more efficient
- 
- **Configure and apply advanced ESXi host attributes**
    - There are many advanced host attributes that can be set, such as for memory or CPU
    - Configure Advanced ESXi Host Attributes
      - Log into the vSphere client
      - Click on a host from the inventory > click the *Configuration* tab
      - On the right, in the *Software* pane click the *Advanced Settings* hyperlink



- Choose the item on the left where the attribute is located, such as *Cpu*
  - On the right, locate the proper attribute and make the required change
  - A list of Memory and CPU advanced attributes can be found in the [vSphere Resource Management](#) guide on pages 104-106
- **Configure and apply advanced Virtual Machine attributes**
    - Advanced virtual machine attributes are changed per VM and typically the VM will need to be powered off in order to make the change
      - I have successfully made advanced VM changes with VMs powered on using PowerCLI and then either powering the VM off/on or performing a vMotion. The vMotion is registering the VM on a new host, which means it goes through the .VMX file again
    - Configuring Advanced Virtual Machine Attributes
      - Log into the vSphere client
      - From the inventory, right-click a VM and select *Edit Settings...*
      - Click the *Options* tab > click *General* > click the *Configuration Parameters* button



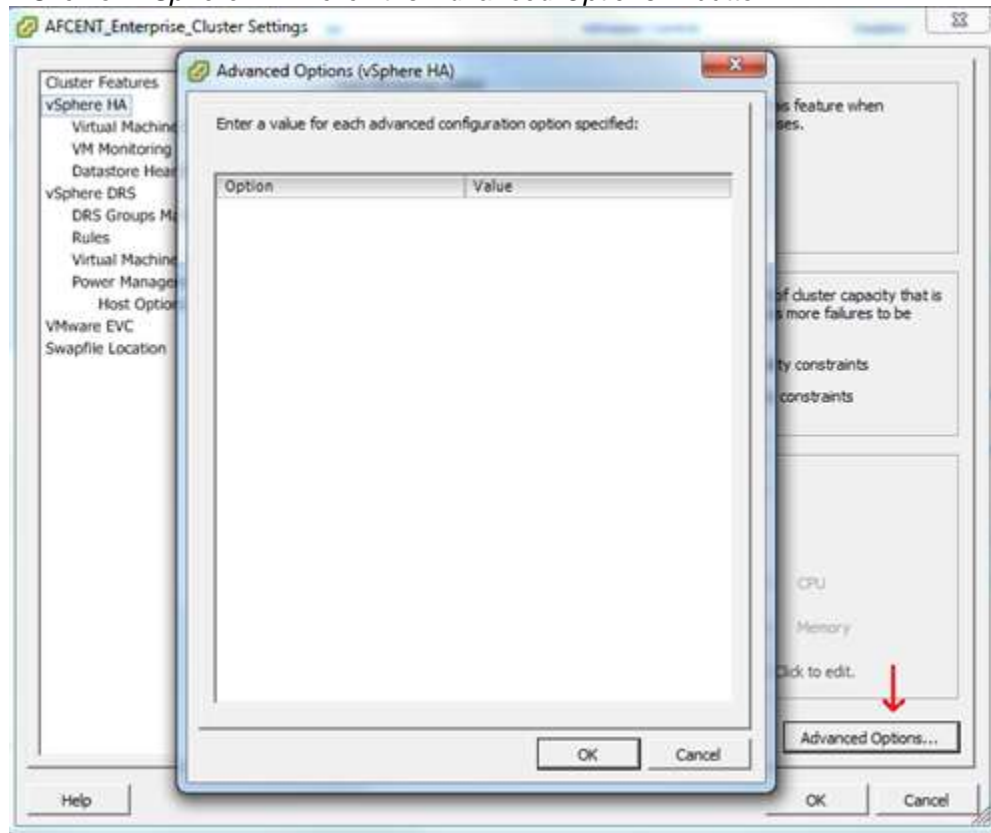
- Click the *Add Row* button
- Enter in the *Name* of the attribute and the *Value*



- Click *OK*
- Some of the advanced virtual machine attributes can be found in the [vSphere Resource Management](#) guide on page 107

- **Configure advanced cluster attributes**

- The only advanced cluster attributes that I know of are for vSphere HA. If there are others that can be configured for the cluster please let me know!
- Configure Advanced Cluster Attributes
  - Log into the vSphere client
  - From the inventory, right-click on a cluster and click *Edit Settings...*
  - Click on *vSphere HA* > click the *Advanced Options...* button



- Here you can add different options and values. A list and explanation of advanced HA options can be found on Ducan Epping's ([blog](#) / [twitter](#)) [HA Deepdive](#) post
- Click *OK* when finished

## Tools

- [vSphere Command-Line Interface Concepts and Examples](#)
- [vSphere Monitoring and Performance Guide](#)
- [Product Documentation](#)
- vSphere Client / Web Client
  - Performance Graphs



# VCAP5-DCA-Objective 3.2–Optimize Virtual Machine Resources

---

For this objective I used the following documents:

- Documents listed in the Tools section

## **Objective 3.2 – Optimize Virtual Machine Resources**

### Knowledge

**\*\*ITEMS IN BOLD ARE TOPICS PULLED FROM THE BLUEPRINT\*\***

- **Compare and contrast virtual and physical hardware resources**
  - At its most basic form, virtual resources allow you to overcommit your virtual machines. Virtual resources are the makeup of physical resources and allow flexibility
  - Over commitment of virtual resources is a good idea as long as its managed well. Configuring X amount of virtual resources on a virtual machine does not meant the commensurate physical resources will be used, which is where the flexibility of virtual resources comes in
  - While virtual hardware resources add overhead that physical resources do not, using virtual resources you can get the most out of the physical resources
    - I don't have a lot more to say about this. I didn't see any reference to this topic in the documentation and I believe the basic comparisons of physical vs. virtual still apply. Please, if anyone has a reference from the documentation please let me know in the comments
- **Identify VMware memory management techniques**
  - With the introduction of vSphere 5 new management techniques were introduced to further optimize memory management
  - Hosts allocate memory to virtual machines based on their most recent working set size and relative shares to the resource pool. The working set size is monitored for 60 seconds (default period). This interval can be changed by modifying the advanced setting *Mem.SamplePeriod*
  - A cool new feature introduced with vSphere 5 is *VMX Swap*. I've explained this in previous objectives, but I'll go through it real quick. Every VM has memory overhead, and that memory is reserved during power on. A chunk of that memory is reserved for the VMX process. Instead of using physical memory for the VMX process, VMX swap files are created

during power on and memory needed for the VMX process is swapped to the VMX swap files instead of using memory. This feature is enabled by default and is invoked when the host memory is overcommitted

- ESXi memory sharing allows virtual machines running the same operating systems and/or applications to, when possible, share the memory pages. This technique is called Transparent Page Sharing (TPS). You can set advanced settings per-host to specify a custom interval of how often the host scans for memory and host much CPU resources to consume doing it. Those two settings are *Mem.ShareScanTime* and *Mem.ShareScanGHZ*. The defaults are 60 (minutes) and 4 respectively
- Memory Compression is a technique that is used right before pages start getting swapped to disk. Memory pages that can be condensed into 2KB or less are stored in what's called the virtual machine's compression cache. You can set the maximum size of the compression cache with the *Mem.MemZipMaxPct* advanced setting. The default is 10%. If you want to enable/disable memory compression use the *Mem.MemZipEnable* advanced setting. Use the value 0 to disable and 1 to enable
- Before getting into the memory reclamation techniques lets talk about the idle memory tax. The idle memory tax is a construct that, during a time of contention, will reclaim idle memory that is held by a virtual machine. Jason Boche ([blog](#) / [twitter](#)) has an older, but still excellent and relevant [blog post on the Idle Memory Tax \(IMT\)](#). The more idle memory a virtual machine has, the more the tax goes up, effectively reclaiming more memory. There are two advanced settings associated with the idle memory tax; *Mem.IdleTax* and *Mem.IdleTaxType*. *Mem.IdleTax* is the maximum percentage of total guest memory that can be reclaimed by the idle memory tax, with a default of 75%. *Mem.IdleTaxType* specifies whether the tax increases/decreases based on the amount idle memory (this is called variable and is the default). For this setting, 1 is the default (variable) and 0 is for a flat rate
- There are two memory reclamation techniques that are used when memory contention exists amongst virtual machines; memory ballooning and memory swapping
- Memory ballooning uses the memory balloon driver, known as *vmmemctl* which is loaded into the guest operating system as part of the VMware tools installation. Obviously, if the virtual machine doesn't have VMware tools installed, it won't have the balloon driver, which means the ballooning technique will be skipped and swapping may occur (this is bad!). When memory pressure exists the balloon driver determines the least valuable pages and swaps them to the virtual disk of the virtual machine (this is not host swapping). Once the memory is

swapped to virtual disk, the hypervisor can reclaim that physical memory that was backing those pages and allocate it elsewhere. Since ballooning is performing swap to virtual disk, there must be sufficient swap space within the guest operating system. You can limit the amount of memory that gets reclaimed on a per-virtual machine basis by adding `sched.mem.maxmemctl` line to the virtual machine configuration file. The value is specified in MB

- There are two types of swap to disk mechanism; swap to disk and swap to host cache. Swapping to disk is the same as it's been in previous versions; a swap file is created (by default in the same location as the virtual machine's configuration file) during power-on and during times of memory contention, if ballooning doesn't slow/stop contention or the balloon driver isn't working or available, swapping to disk occurs. Alternatively, for swap file location, you can change this per-VM, per-host, or specify a datastore for an entire cluster
- Host cache is new in vSphere 5. If you have a datastore that lives on a SSD, you can designate space on that datastore as host cache. Host cache acts as a cache for all virtual machines on that particular host as a write-back storage for virtual machine swap files. What this means is that pages that need to be swapped to disk will swap to host cache first, and the written back to the particular swap file for that virtual machine
- **Identify VMware CPU load balancing techniques**
  - CPU affinity is a technique that doesn't necessarily imply load balancing, but it can be used to restrict a virtual machine to a particular set of processors. Affinity may not apply after a vMotion and it can disrupt ESXi's ability to apply and meet shares and reservations
  - ESXi hosts can take advantage of multicore processors and use them to produce the most optimized performance for your virtual machines. The ESXi CPU scheduler is aware of the processor topology within the system and can see how the sockets, cores and logical processors are related to each other
    - By default, the CPU scheduler will spread the workload across all sockets in the system in undercommitted systems
    - You can override the default behavior by adding `sched.cpu.vsmcConsolidate = True` to the virtual machine configuration file. This setting will prevent the workload from being spread across all sockets it and limited it to the same socket
  - Hyperthreading is a feature that only exists in certain Intel processor families. Hyperthreading breaks up a single core on into two logical threads. This allows vCPU1 to execute instructions on thread1 while vCPU2 can execute instructions on thread2

- Be careful when setting manual CPU affinity when hosts have hyperthreading enabled. The scenario exists where two virtual machines get bound to the same core (one on thread1 and one on thread2) which could be detrimental to the performance of those workloads
- Hyperthreading is needs to be enabled in the Host BIOS and once that is done, should automatically be enabled in vSphere
- NUMA (Non-Uniformed Memory Access) nodes work differently then your standard x86 system, and therefore, ESXi has a separate CPU scheduler; the NUMA scheduler. At a very high level, NUMA is an architecture that provides more than one memory bus. Each socket has its own bus to memory and the physical processors have the option to access memory that isn't located on its dedicated bus (that's the non-uniform part)
  - When a virtual machine is allocated memory, it takes memory locality into mind, meaning it will provide best effort in assigning memory that is from the home node (the home node is a term used to describe a processor and memory local to that processor)
  - If there is an imbalance in the load, the NUMA scheduler can change a virtual machines home node on-the-fly (CPU DRS for NUMA?). Even though the home node moves to a new home node, it does not automatically mean that the memory is relocated to its new home node, however the scheduler has the ability to relocate remote memory to once again make it local
  - The dynamic load balancing algorithm will exam the load and decide whether a rebalance is needed, this happens every two seconds by default
- **Identify pre-requisites for Hot Add features**
  - There are a lot of different virtual hardware items that can be hot added to a virtual machine. Even though the topic doesn't specifically refer to CPU and memory, that is what I'm going to focus on
  - Hot add cannot be abled for all virtual machines, here are some of the prerequisites:
    - Only certain guest operating systems are supported for hot add, so ensure the guest operating system you are using supports it
    - Hot add must be enabled per virtual machine and the virtual machine must be powered off in order to enable it

- If you are hot-adding multicores vCPUs then the virtual machine must be using hardware version 8
- If you are hot-adding a vCPU to a virtual machine using virtual hardware 7, the number of cores per socket must be set to 1
- The virtual machine MUST have at least hardware version 7 or later
- Install VMware tools
- You can perform hot-add operations through the standard vSphere client or the vSphere web client

### Skills and Abilities

#### • **Tune Virtual Machine memory configurations**

- In this section (and the rest of the “tuning” sections) I will not go over how to identify bottlenecks or misconfigurations (such as using ESXTOP to diagnose). I will simply be listing some recommended practices that should optimize and make your virtual machines more efficient. ESXTOP and vscsiStats will be covered in section 3.4 and in section 6
- Pay attention to your virtual machine memory allocation. You don’t want to overcommit to the point where the VM starts swapping to host cache, or worse, disk. You can use the built-in performance charts and **esxtop** / **resxtop** to determine whether the VM is swapping pages to virtual disk or the host is swapping to disk (these items are covered in detail in section 3.4 and section 6)
- Don’t oversize memory on your virtual machines
  - Even if you have the available physical memory, don’t allocate any more than what’s needed. Over-allocating memory will waste physical memory as the more memory you allocate to a virtual machine, the more memory the vmkernel takes for overhead
- Proceed cautiously when setting memory reservations and limits. Setting these too low or too high can cause unnecessary memory ballooning and swapping
- Ensure VMware tools is installed and up-to-date
- If you need to control priority over memory, use memory shares to determine relative priority
- Use an SSD disk to configure Host cache

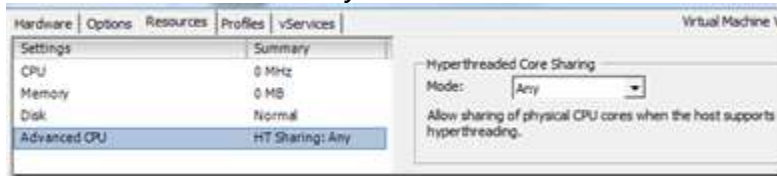
#### • **Tune Virtual Machine networking configurations**

- Here’s an easy one – use the paravirtualized network adapter, also known as the VMXNET3 adapter
  - Requires VMware tools to be installed
  - Requires virtual machine hardware version 7 or later

- Ensure the guest operating system is supported
- Enable jumbo frames for the VM if the rest of the infrastructure is using jumbo frames
  - Is set in the guest OS driver

- **Tune Virtual Machine CPU configurations**

- If hyperthreading is enabled for the host, ensure that the Hyperthreaded Core Sharing Mode for your virtual machines are set to *Any*



- If you need to disable hyperthreading for a particular virtual machine, set the Hyperthreaded Core Sharing Mode to *None*
- Select the proper hardware abstraction layer (HAL) for the guest operating system you are using
  - This only applies for the guest operating systems that have different kernels for single processor (UP) and multiple processors (SMP). Single vCPU would use UP and all others will use SMP
- If your application or guest OS can't leverage multiple processors then configure them with only 1 vCPU
- If your physical hosts are using NUMA, ensure the virtual machines are hardware version 8 as this exposes the NUMA architecture to the guest operating systems allowing NUMA aware applications to take advantage of it. This is known as Virtual NUMA

- **Tune Virtual Machine storage configurations**

- Logical disks you create inside the guest OS should be separated into separate VMDK files. In other words, have a 1:1 for logical disks and VMDKs for your OS disk and data disks
- Ensure the guest operating system disks are aligned with the VMFS volumes they reside on
  - Some guest operating systems (such as Windows Server 2008) do this automatically
- Consider using the paravirtualized SCSI (PVSCSI) adapter
  - The PVSCSI adapter can provide higher throughput and lower CPU utilization
  - Requires virtual machine hardware version 7 or later

- Large I/O requests have the potential to be broken up into smaller requests by the device driver within the guest OS. Modify the registry to increase the block size as fragmented I/O requests can reduce performance

- **Calculate available resources**

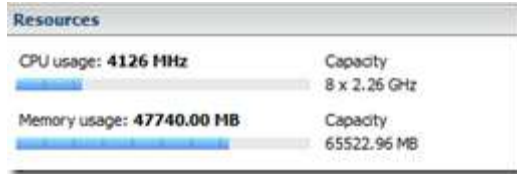
- In vSphere 5 there are many visualizations within the GUI that will show you what the available resources are for a cluster, host or a virtual machine. You can also determine available resources for a host using **esxtop**

- Determining available resources for a cluster can be done by viewing the *Resource Distribution Chart*

- Log into the vSphere client
- Navigate to the *Hosts and Clusters* view > select a cluster from the inventory tree
- In the *vSphere DRS* pane on the right, click the *View Resource Distribution Chart* hyperlink
- Here you can see CPU and Memory usages in MHz or MB or the percentage of each



- Viewing available host memory in the GUI
  - Log into the vSphere client
  - Navigate to the *Hosts and Clusters* view > select a host from the inventory tree
  - You can view the current host resource utilization, as well as available resources by taking the total capacity and subtracting the current usage > located in the *Resources* pane



- You can also calculate available host resources using **esxxtop**
  - SSH into a host and type **esxxtop** at the command line
  - On the CPU screen (default screen when running esxxtop, press **C** to get to it) you'll see two lines at the top called *PCPU USED (%)* and *PCPU UTIL (%)*

```

1:14:26pm up 37 days 16:21, 431 worlds, 10 VMs, 16 vCPUs: CPU load average: 0.31, 0.32, 0.34
PCPU USED(%): 13 16 19 14 18 12 13 24 12 35 20 7.6 24 18 16 48 AVG: 19
PCPU UTIL(%): 15 17 19 14 17 11 14 24 13 35 19 8.2 24 19 17 47 AVG: 20
CORE UTIL(%): 29 33 28 36 46 27 41 62 AVG: 38

  ID  GID NAME      NWLD  %USED  %RUN  %SYS  %WAIT  %VMWAIT  %RDY  %IDLE  %OVRLE
  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---
    1     1 idle      16 543.93 1600.00 0.00 0.00 - 19.54 0.00 5.19
  
```

- There is some difference between *PCPU USED* and *PCPU UTIL*, but for calculating available CPU resources, let's focus on *PCPU USED (%)*. You'll see each physical CPU represented on this line and its corresponding *USED* percentage
- *PCPU USED (%)* represents the effective work of that particular VCPU, thus, allowing you to calculate the available resources per PCPU
- You can also look at *AVG*, which is the last field in the *PCPU USED (%)* line and that averages all PCPUs. This would tell you the overall CPU resources used for the host (thus enabling you to calculate the available resources)
- To calculate the available memory for a host in esxxtop press the **M** button to navigate to the memory screen. This time we'll focus on the second and third lines, which are *PMEM /MB* and *VMKMEM /MB*, respectively. This is physical memory represented in megabytes and vmkernel memory represented in megabytes

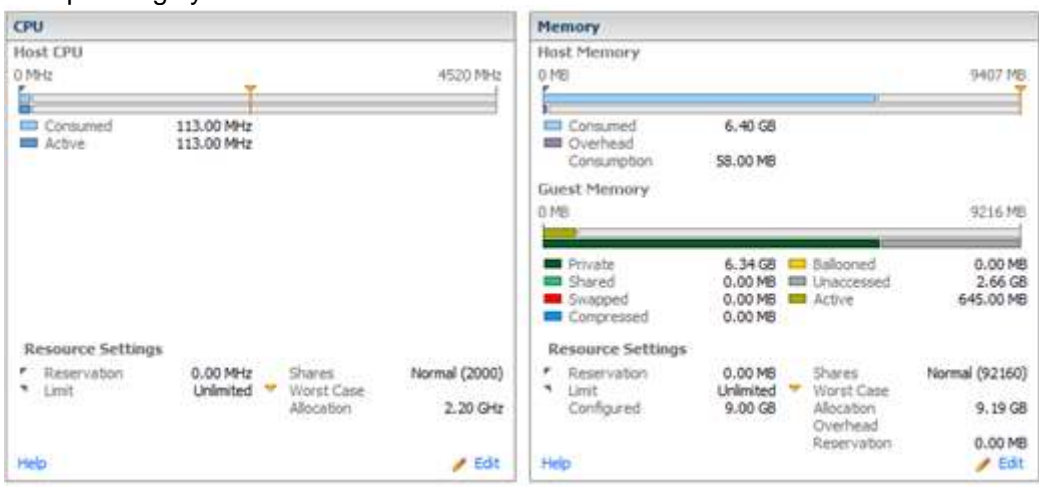
```

1:33:51pm up 37 days 16:41, 426 worlds, 9 VMs, 15 vCPUs: MEM overcommit avg: 0.00, 0.00, 0.00
PMEM /MB: 65522 total: 1458 vmk, 41251 other, 22812 free
VMKMEM/MB: 65199 managed: 1266 minfree, 4616 rsvd, 60583 ursvd, high state
NUMA /MB: 32768 (10722), 32754 (11545)
PSHARE/MB: 613 shared, 244 common: 369 saving
SWAP /MB: 0 curr, 0 rclmtgt: 0.00 r/s, 0.00 w/s
ZIP /MB: 0 zipped, 0 saved
MEMCTL/MB: 0 curr, 0 target, 26621 max
  
```

- *PMEM /MB* will show you your total amount of physical memory, how much is being used by the vmkernel and how much memory is free on the host
- *VMKMEM /MB* important items are the *rsvd* and *ursvd* fields. These represent, in MB how much memory is reserved and unreserved for the host. Here is why these are important:



- If your *PMEM* is showing 20GB of memory available, but the *VMKMEM* only shows 15GB *ursvd* (unreserved) then your virtual machines only have 15GB available to them
- You can view the available virtual machine resources through the GUI as well
  - Log into the vSphere client
  - Navigate to the *Hosts and Clusters* view > select a virtual machine from the inventory tree
  - On the right, click on the *Resource Allocation* tab
  - Here you can see the physical CPU and Memory that is allocated to the virtual machine. You can also see what is being consumed (CPU) or is active (MEM ) within the guest operating system

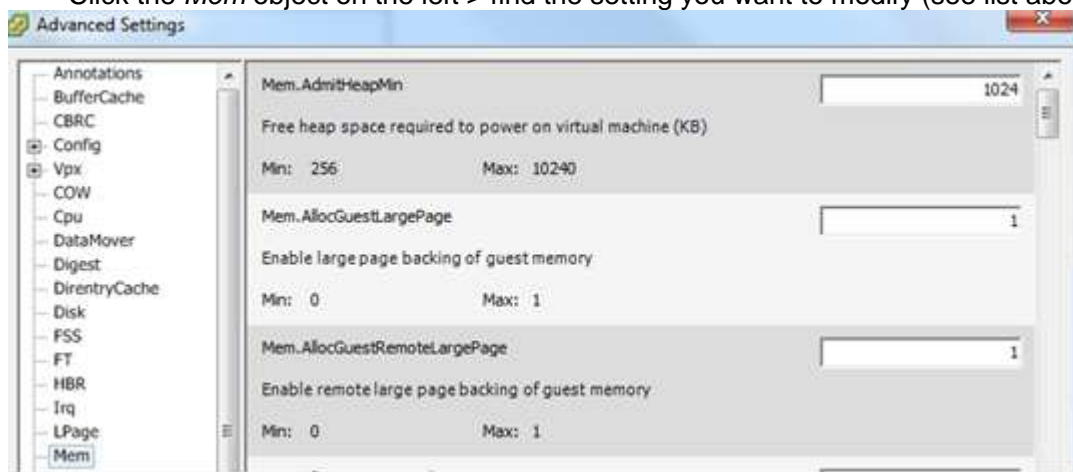


- Above you can see that this particular virtual machine could consume up to ~4.5Ghz of CPU, but is only consuming 113MHz. You can also see that the VM has the potential to use ~9GB of memory, and it has consumed 6.4GB, but there is only 645MB active
- **Properly size a Virtual Machine based on application workload**
  - Sizing a virtual machine based on application workload has already been covered in [Objective 1.1 – Implement and Manage Complex Storage Solutions](#) (Determine appropriate RAID levels for various virtual machine workloads). **vscsiStats** is briefly gone over and will be covered more in section 3.4
- **Modify large memory page settings**

- Large memory page settings are configured per-host. Here are a list of existing large page settings:

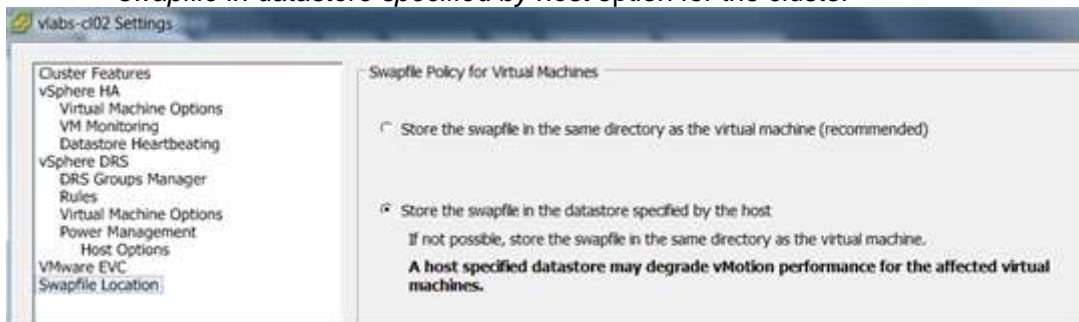
Mem.AllocGuestLargePage	Enables backing of guest large pages with host large pages. Reduces TLB misses and improves performance in server workloads that use guest large pages. 0=disable.	1
Mem.AllocUsePSharePool and Mem.AllocUseGuestPool	Reduces memory fragmentation by improving the probability of backing guest large pages with host large pages. If host memory is fragmented, the availability of host large pages is reduced. 0 = disable.	15
LPage.LPageDefragEnable	Enables large page defragmentation. 0 = disable.	1
LPage.LPageDefragRateVM	Maximum number of large page defragmentation attempts per second per virtual machine. Accepted values range from 1 to 1024.	32
LPage.LPageDefragRateTotal	Maximum number of large page defragmentation attempts per second. Accepted values range from 1 to 10240.	256
LPage.LPageAlwaysTryForNPT	Try to allocate large pages for nested page tables (called 'RVT' by AMD or 'EPT' by Intel). If you enable this option, all guest memory is backed with large pages in machines that use nested page tables (for example, AMD Barcelona). If NPT is not available, only some portion of guest memory is backed with large pages. 0= disable.	1

- You can modify any of the settings above by doing the following
  - Log into the vSphere client
  - Navigate to the *Hosts and Clusters* view > select a host from the inventory tree
  - On the right, click the *Configuration* tab
  - In the *Software* pane click the *Advanced Settings* hyperlink
  - Click the *Mem* object on the left > find the setting you want to modify (see list above)

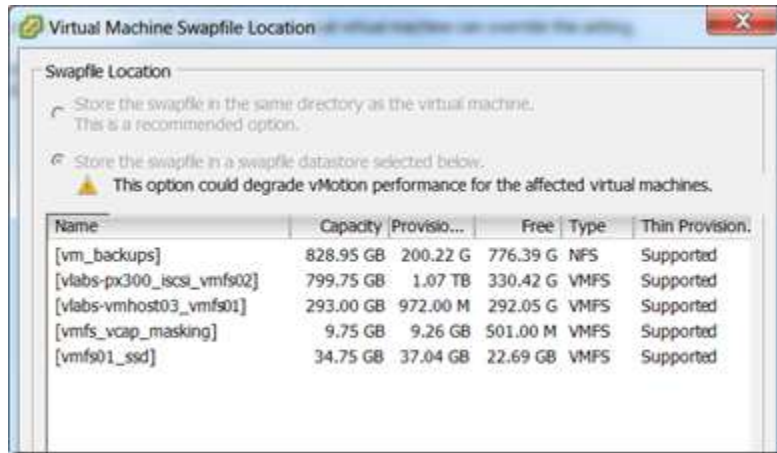


- **Understand appropriate use cases for CPU affinity**
  - CPU affinity is a tricky thing, and as a general practice, shouldn't be used.
  - Some use cases (there are very few) that you want to use CPU affinity:
    - Simulating a workload
    - Load testing for an application
    - Certain workloads can also benefit from this

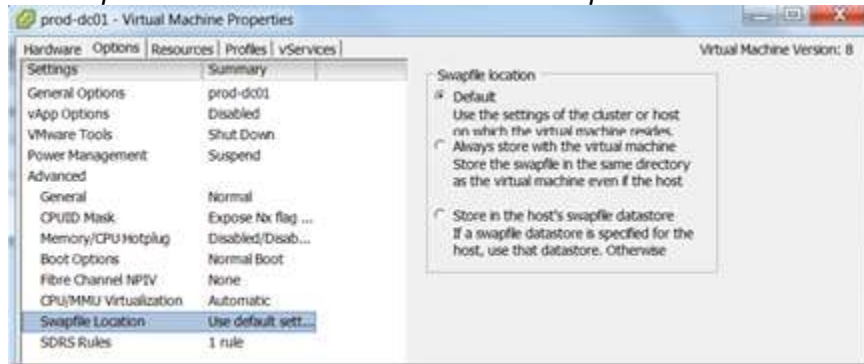
- From a [blog post](#) by Frank Denneman: “When the virtual machine workload is cache bound and has a larger cache footprint than the available cache of on CPU, it can profit from aggregated caches”
  - Along with understanding the use cases for CPU affinity, it is important to understand some potential issues that are associated with it:
    - If you are using NUMA hardware, the NUMA scheduler may not be able to manage virtual machine with CPU affinity, essentially disabling NUMA for that virtual machine
    - Hyperthreaded enabled hosts may not be able to fully leverage hyperthreading on a virtual machine with CPU affinity
    - Reservations and shares may not fully be respected for a virtual machine configured for CPU affinity
    - CPU affinity might not exist for a virtual machine across all hosts in a cluster during a migration
- **Configure alternate virtual machine swap locations**
  - Configuring an alternate location for virtual machine swap files is a simple task, but can be mundane if you have to do it for a lot of virtual machines
    - Alternatively you could configure an alternate swap location for the host
      - Select host from inventory tree
      - Choose *Configuration* > click *Virtual Machine Swapfile Location* hyperlink
      - Click the *Edit...* hyperlink (if this is disabled then you have to choose the *Store the swapfile in datastore specified by host* option for the cluster



- Select the datastore where you want to store the swapfile for all virtual machines on that host



- Click OK
- To configure the alternate swapfile location for a particular virtual machine
  - Log into the vSphere client
  - Navigate to the *Hosts and Clusters* view
  - Right-click a virtual machine from the inventory > click *Edit Settings...*
  - Click the *Options* tab > at the bottom click the *Swapfile Location*



- Select one of the following options (as you can see in the screenshot above)
  - Default – which is either the cluster default or host default
  - Always store with the virtual machine – swapfile is stored in the same directory as the host
  - Store swap file in the host's swapfile directory

## Tools

- [vSphere Resource Management Guide](#)
- [vSphere Virtual Machine Administration](#)
- [Product Documentation](#)
- *vscsiStats*
- vSphere Client / Web Client

## VCAP5-DCA–Objective 3.3 – Implement and Maintain Complex DRS Solutions

---

For this objective I used the following documents:

- [VMware vSphere 5 Clustering Technical Deepdive](#) by Duncan Epping and Frank Denneman
- Documents listed in the Tools section

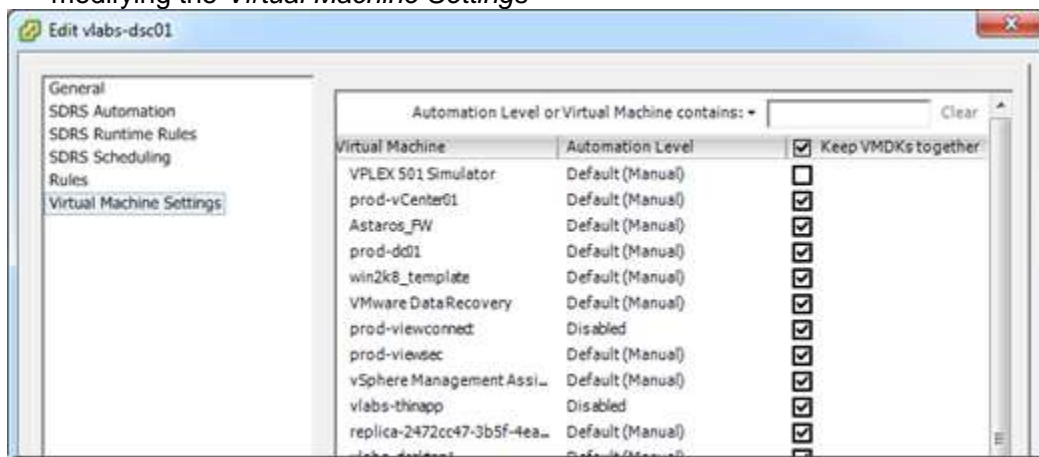
### **Objective 3.3– Implement and Maintain Complex DRS Solutions**

#### Knowledge

**\*\*ITEMS IN BOLD ARE TOPICS PULLED FROM THE BLUEPRINT\*\***

- **Explain DRS / storage DRS affinity and anti-affinity rules**
  - DRS affinity and anti-affinity rules
    - Two types of rules exist; *VM-Host affinity* rules and *VM-VM affinity* rules
    - VM-Host affinity rules
      - Allows you to tie a virtual machine or group of virtual machines to a particular host or particular set of hosts. Also allows anti-affinity for said objects
      - Before creating a VM-Host affinity rule you need to create a DRS group and a host group
      - Decide whether it is a “must” rule or a “should” rule
        - “Must” rules will never be violated by DRS, DPM, or HA
        - “Should” rules are best effort and can be violated
    - VM-VM affinity rules
      - Used to keep virtual machines on the same host or ensure they do NOT run on the same host. If you had two servers that provide load-balancing for an application, it’s a good idea to ensure they aren’t running on the same host
      - VM-VM affinity rules shouldn’t conflict with each other. Meaning, you shouldn’t have one rule that separates virtual machines and another rule that keeps them together. If you have conflicting rules then the older rule wins and the new rule is disabled
  - Storage DRS affinity and anti-affinity rules
    - Storage DRS affinity rules are similar to DRS affinity rules, but instead of being applied to virtual machines and hosts they are applied on virtual disks and virtual machines when using datastore clusters

- The three different storage DRS affinity/anti-affinity rules are *Inter-VM Anti-Affinity*, *Intra-VM Anti-Affinity* and *Intra-VM Affinity*(The “intra” rules are also known as VMDK anti-affinity and VMDK affinity)
  - Inter-VM ant-affinity allows you to specify which virtual machines should not be kept on the same datastore within a datastore cluster
  - Intra-VM anti-affinity lets you specify the virtual disks that belong to a particular virtual machine are stored on separate datastores within a datastore cluster
  - Intra-VM affinity will store all of your virtual disks on the same datastore within the datastore cluster (this is the default)
- Storage DRS affinity rules are invoked during initial placement of the virtual machine and when storage DRS makes its recommendations. A migration initiated by a user will not cause storage DRS to be invoked
- You can change the default behavior for all virtual machines in a datastore cluster by modifying the *Virtual Machine Settings*



- This allows you to specify VMDK affinity or VMDK ant-affinity
- **Identify required hardware components to support DPM**
    - DPM uses one of the following methods to bring hosts out of standby:
      - Intelligent Platform Management Interface (IPMI)
      - HP Integrated Lights-Out (HP iLO)
      - Wake on LAN (WOL)
    - IPMI and HP iLO both require a base management controller (BMC) – this allows access to hardware functions via a remote computer over LAN

- THE BMC is always on whether the host is or not, enabling it to listen for power-on commands
- IPMI that uses MD2 for authentication is not supported (use plaintext or MD5)
- To use the WOL feature instead of IPMI or HP iLO the NIC(s) you are using must support WOL. More importantly, the physical NIC that corresponds to the vMotion vmkernel portgroup must be capable of WOL
  - In this case you can see that my vMotion vmkernel is located on vSwitch0, which has vmnic0 as its uplink
  - If you look at the *Network Adapters* section (host > configuration > network adapters) you can see that vmnic0 has WOL support

Device	Speed	Wake on LAN Supported
<b>Realtek Realtek 8168 Gigabit Ethernet</b>		
vmnic0	1000 Full	Yes

- **Identify EVC requirements, baselines and components**
  - Enhanced vMotion Compatibility (EVC) is used to mask certain CPU features to virtual machines when a host(s) in a cluster have a slightly different processor than other hosts in the cluster
  - An AWESOME knowledge base article answers a lot of questions about EVC; [VMware KB1005764](#)
  - There are multiple EVC modes so check out the [VMware Compatibility Guide](#) to see which mode(s) your CPU can run
  - Enable Intel VT or AMD-V on your hosts
  - Enable the execute disable bit (XD)
  - CPUs must be of the same vendor
  
- **Understand the DRS / storage DRS migration algorithms, the Load Imbalance Metrics, and their impact on migration recommendations**
  - DRS and Storage DRS use different metrics and algorithms, so I'll talk about each of them separately

- DRS
  - By default DRS is invoked every 5 minutes (300 seconds). This can be changed by modifying the vpxd configuration file, but it is highly discouraged and may or may not be supported
  - Prior to DRS performing load-balancing it will first try and correct any constraints that exists, such as DRS rules violations
  - One constraints have been corrected, DRS moves on to load-balancing using the following process:
    - Calculates the Current Host Load Standard Deviation (CHLSD)
    - If the CHLSD is less than the Target Host Load Standard Deviation (THLSD) then DRS has no further actions to execute
    - If CHLSD is greater than the THLSD then:
      - DRS executes a “bestmove” calculation which determines which VMs are candidates to be vMotioned in order to balance the cluster. The CHLSD is then calculated again
      - The costs, benefits and risks are then weighed based on that move
      - If the migration does not exceed the costs, benefits, and risks threshold, the migration will get added to the recommended migration list
    - Once all migration recommendations have been added to the list, the CHLSD is then calculated based on simulating those migrations on the list
  - The tolerance for imbalance is based on the user-defined migration thresholds (five total). The more aggressive the threshold, the lower the tolerance is for cluster imbalance
  - For a much deeper dive into DRS calculations, check out chapter 14 of the vSphere 5 Technical Deepdive mentioned at the top of this post
- Imbalance Calculation and metrics
  - As mentioned earlier, load imbalance is when the CHLSD is greater than the THLSD.
  - Some things that will cause the DRS imbalance calculation to trigger are:
    - Resource settings change in a virtual machine or resource pool
    - When a host is added/removed from a DRS cluster
    - When a host enters/exits maintenance mode
    - Moving a virtual machine in/out of a resource pool
- Storage DRS

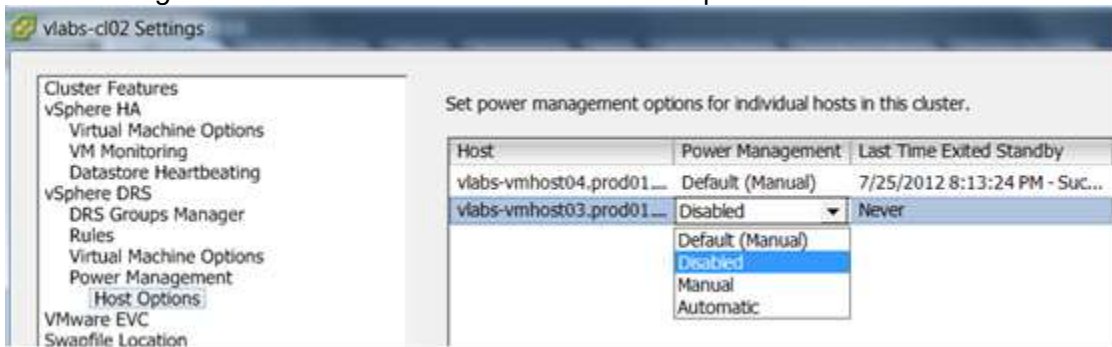


- There are two types of calculations performed by Storage DRS; initial placement and load-balancing
- As with DRS, Storage DRS has a default invocation period, however it is much longer – 8 hours is the default interval. Again, it is not recommended that you change the default interval
- Initial placement takes datastore space and I/O metrics into consideration prior to placing a virtual machine on a datastore. It also prefers to use a datastore that is connected to all hosts in the cluster instead of one that is not
- Storage DRS Load imbalance
  - Before load-balancing is taken into consideration, corrections to constraints are processed first. Examples of constraints are VMDK affinity and anti-affinity rule violations
  - Once constraint violations have been corrected, load-balancing calculations are processed and recommendations are generated
    - There are Storage DRS rules that are taken into account when the load-balancing algorithms run; Utilized Space and I/O Latency. Recommendations for Storage DRS migrations will not be made unless these thresholds are exceeded
    - Additionally, you can set advanced options that specify your tolerance for I/O imbalance and the percentage differential of space between source and destination datastores
      - Example: destination datastore must have more than a 10% utilization difference compared to the source datastore before that destination will be considered
  - Storage DRS also calculates a cost vs. benefits analysis (like DRS) prior to making a recommendation
- Besides the standard invocation interval, the following will invoke Storage DRS:
  - If you manually click the Run Storage DRS hyperlink
  - When you place a datastore into datastore maintenance mode (the I/O latency metric is ignored during this calculation)
  - When you move a datastore into the datastore cluster
  - If the space threshold for a datastore is exceeded
- There are a lot more technical details involved, such as workload and device modeling, but these facets of Storage DRS are complex and would make this post extremely long, If you

care to review these, check out chapter 24 of the vSphere 5 Technical Deepdive mentioned at the top of this post

### Skills and Abilities

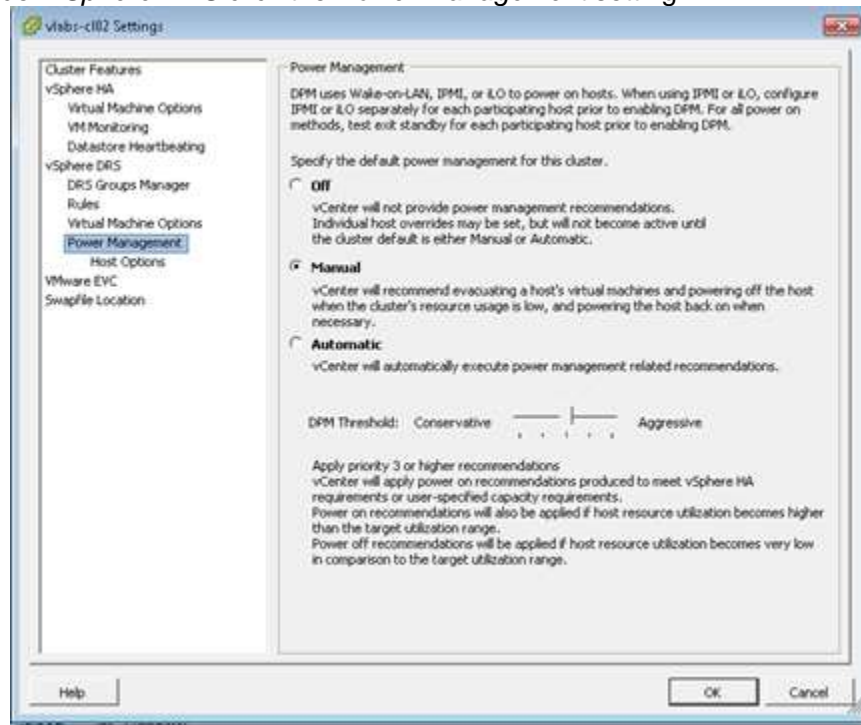
- **Properly configure BIOS and management settings to support DPM**
  - This will be slightly different for each system depending on the BIOS that it's running. You will also need to configure your IPMI or iLO settings if you are using either of those technologies to support DPM. Most IPMI controllers (BMCs) will have their own configuration screen that can be accessed when booting the host
  - Some BIOS may require you to enable to WOL feature (if it's an onboard NIC)
- **Test DPM to verify proper configuration**
  - Before you can use the WOL option for DPM and enable it on a DRS cluster you must first successfully enter *Standby* mode and power the host back on successfully, If you aren't able to successfully power the host back on after entering standby mode then you can need to disable the power management setting for that host
    - Log into the vSphere client
    - From the inventory tree right-click the cluster and select *Edit Settings...*
    - Under *Power Management* click on *Host Options*
    - In the right, find the host(s) that failed to exit standby and under the *Power Management* column select *Disabled* from the dropdown box



- Click *OK*

- **Configure appropriate DPM Threshold to meet business requirements**

- As a business, all resources consumed cost money and being efficient as possible while still meeting business requirements is important. Using DPM can save you on unneeded power consumption, but you don't want to use it to the point of negative returns. Setting the DPM threshold for your cluster(s) is an important consideration. You set the DPM threshold by:
  - Log into the vSphere client
  - From the inventory tree, right-click on your DRS cluster > click *Edit Settings...*
  - Under *vSphere DRS* click the *Power Management* setting



- Here you can see that there are three different options you can choose; *Off*, *Manual* and *Automatic*
  - Off – power management is turned off
  - Manual – vCenter will give you recommendations during low resource utilization for hosts that can be put into standby mode
  - Automatic – vCenter will automatically place hosts in standby mode based on the DPM threshold that is set
- Setting the *Automatic* option and figuring out the DPM threshold to use is where business requirements are factored in. Before we can make the correlation, let's talk about different migration thresholds. Like the DRS migration threshold, the DPM threshold is based on

priority recommendations. The further to the right you move the slider, the more aggressive DPM becomes, the higher priority recommendations start to be included

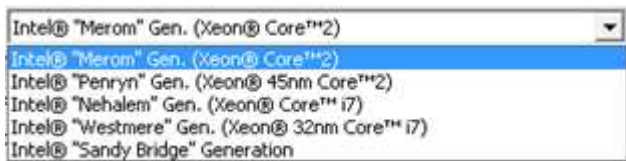
- There are five priority recommendations from 1-5
- With the slider all the way to the left, only priority one recommendations are generated. When you move the slider to the right one notch, only priority one and two recommendations are generated. Each notch to the right will include a new priority level

- Consider your hard requirements regarding resource availability. Determine if your workloads are capable of operating under resource contention should they need to wait for a host to be brought out of standby mode. Workloads can fluctuate, and while DPM will always keep enough resources powered on to satisfy admission control, it may not be able to react fast enough to meet resource demand

- **Configure EVC using appropriate baseline**

- EVC allows you to present the same CPU instruction sets to your virtual machines across a DRS cluster, even if the instruction sets of your physical CPUs across hosts are different. A few EVC requirements:
  - All hosts must have CPUs from the same vendor (Intel or AMD)
  - Hardware virtualization for each host should be enabled (Intel-VT or AMD-V)
  - Execute Disabled bit (Intel) or the No Execute bit (AMD) should be enabled in the BIOS
  - Any virtual machine that is running on a host with a higher CPU feature set than what is presented via the configured EVC baseline must be powered off prior to configuring EVC
    - If those virtual machines are not powered off then you will not be able to enable EVC
- Unless you are using applications that take advantage of certain advanced CPU features that can potentially be masked by EVC you want to use the highest baseline compatible with your hosts. To configure EVC on a new cluster:
  - Log into the vSphere client
  - Right-click a datacenter from the inventory tree and click *New Cluster...*
  - Enter in a *Name* for the cluster (you will most likely want to enable DRS and HA, but for these purposes we'll skip those steps and go straight to EVC)
  - Click *Next*
  - Choose *Enable EVC for AMD Hosts* for AMD processors or *Enable EVC for Intel Hosts* if using Intel processors
  - Choose an EVC mode

- Intel



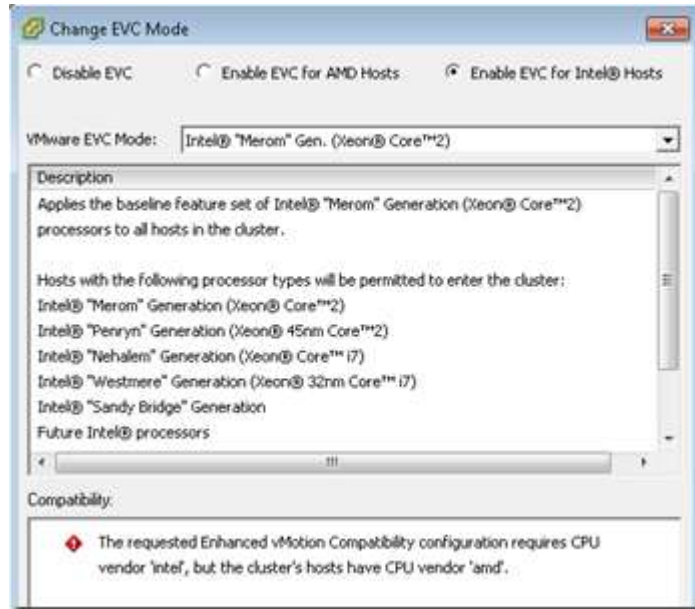
- AMD



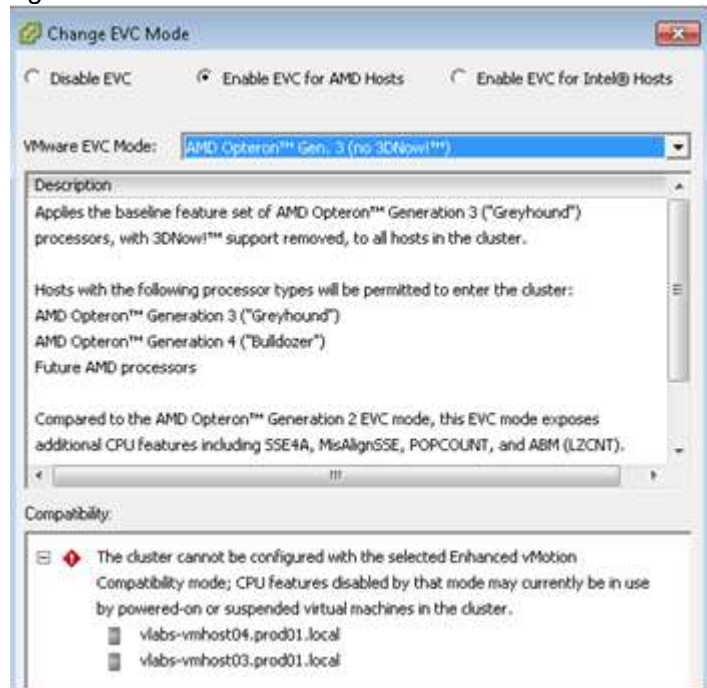
- Each mode you select will give you a description of that mode, as well as the knowledge base article to look at ([VMware KB1003212](#))
- Complete the cluster configuration

- **Change the EVC mode on an existing DRS cluster**

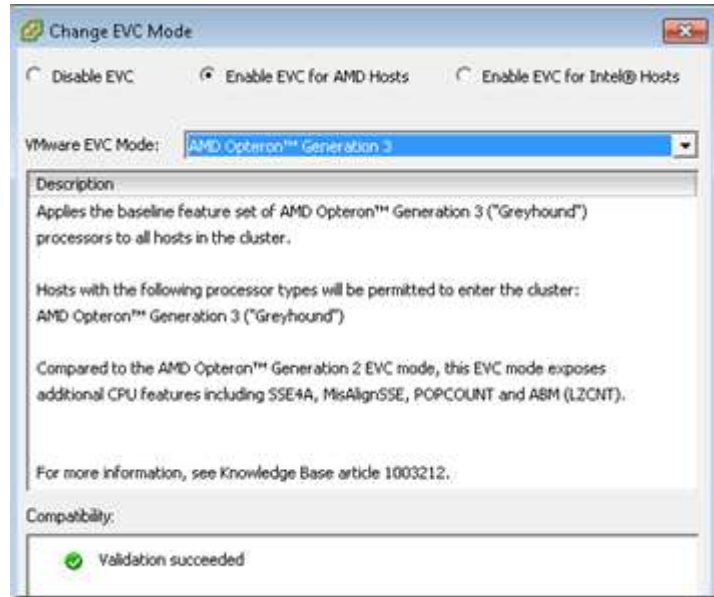
- Changing the EVC mode or enabling EVC mode for the first time on an existing cluster can potentially be disruptive. As stated earlier, if you have virtual machines that are running on hosts that expose a higher level of advanced CPU features than are presented with the EVC baseline you want to configure, then those virtual machines must be powered off. To enable EVC mode or change the EVC mode on an existing DRS cluster:
  - Log into the vSphere client
  - Right-click the DRS cluster you want to modify from the inventory tree > click *Edit Settings...*
  - Select the *VMware EVC* option > click the *Change EVC Mode...* button
  - Select *Enable EVC for AMD Hosts* or *Enable EVC for Intel Hosts*
  - Select the desired mode from the dropdown
    - If the mode you select is not compatible with the processors running in your hosts you will get errors



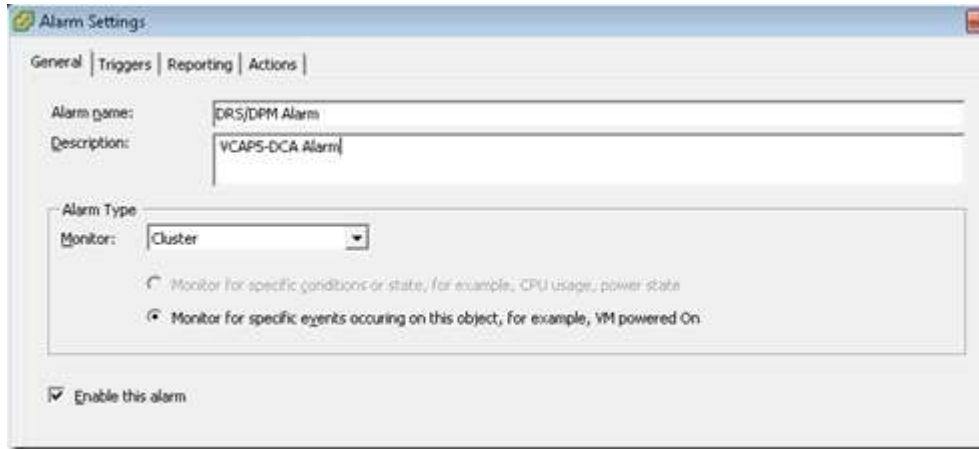
- If the mode you select is not compatible, possibly due to having powered on virtual machines running on hosts with greater CPU features than the selected EVC mode, or possibly due to a misconfigured BIOS setting on a host(s) you will see the following error



- When you choose a mode that is compatible, it will show as *Validation Succeeded*



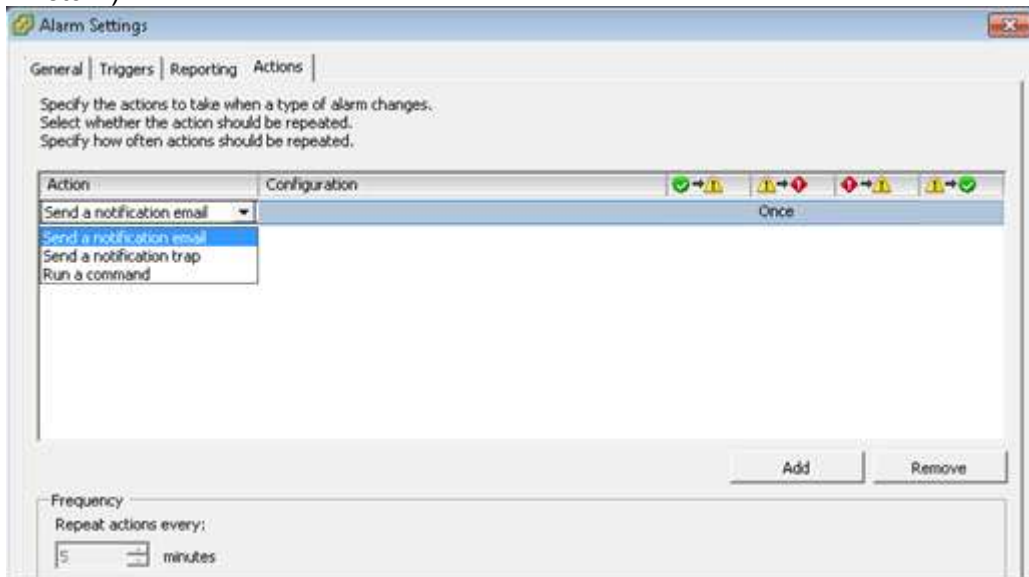
- Click *OK* when finished
  
- **Create DRS and DPM alarms**
  - Since DPM is a facet of DRS, I'll cover creating DRS and DPM alarms together
  - One of the best pre-configured alarms for DRS/DPM is the *Exit Standby Error*. This is an event based alarm, so it will only trigger when the host/cluster reports an event of a host not able to exit standby mode
  - To create a new DRS/DPM alarm for a cluster:
    - Log into the vSphere client
    - Select a cluster from the inventory tree > on the right, click the *Alarms* tab
    - Click the *Definitions* button > here you will see a list of pre-defined alarms
    - Right-click a white area of that pane > click *New Alarm...*
    - Enter in an *Alarm name* and *Description* > from the alarm type dropdown select *Cluster*



- Click the *Triggers* tab > click the *Add* button > click the event in the event column to get a drop down
- Select which event you want. Here are a few DRS/DPM alarm events



- Click on the *Actions* tab > click *Add* > select a desired action from the dropdown and when the action should be initiated (when alarm goes from green to red, red to green, etc...)

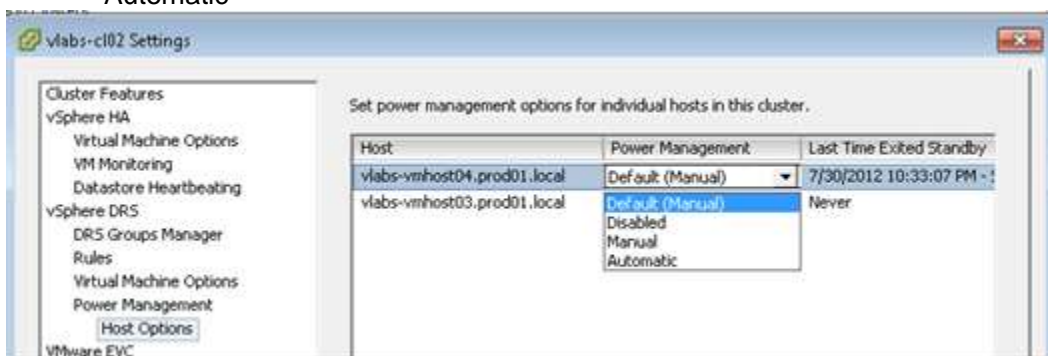


- Click *OK* when finished



- **Configure applicable power management settings for ESXi hosts**

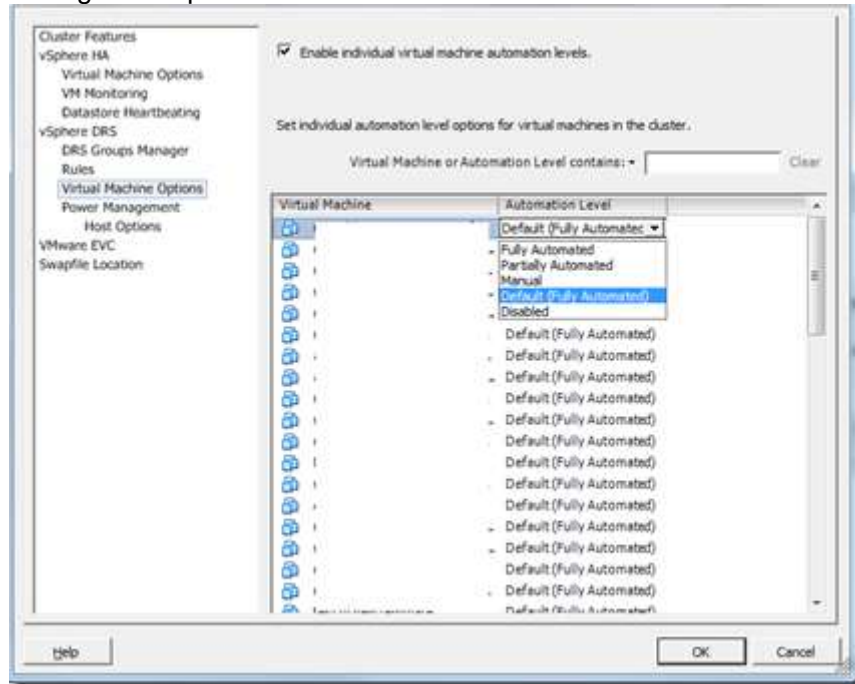
- Power management settings can be set on the hosts themselves (the active policy) or within the DRS cluster settings for DPM purposes
- Set the *Active Policy* power management for an ESXi host
  - Log into the vSphere client
  - Select a host from the inventory tree > click the *Configuration* tab on the right
  - In the *Hardware* pane click the *Power Management* hyperlink > click the *Properties* hyperlink
  - Choose from one of the following power management policies
    - High Performance
    - Balanced
    - Low power
    - Custom
- Set the Power management setting for DRS/DPM
  - Log into the vSphere client
  - Right-click a DRS cluster from the inventory tree > click *Edit Settings...*
  - Click *Host Options* under *vSphere DRS* > *Power Management*
  - Here you will see a list of hosts that are part of the DRS cluster, under the *Power Management* column choose from one of the following settings
    - Default
    - Disabled
    - Manual
    - Automatic



- Click OK

- **Properly size virtual machine and clusters for optimal DRS efficiency**
  - You don't want to size your virtual machines to the cluster, rather, you want to sized your clusters based on virtual machines
  - Properly sizing you virtual machine s and clusters can be tricky, especially if you don't have hard requirements. Virtual machine sizing is the most important, and cluster sizes will be based on how you size your virtual machines with a percentage added in for scale and redundancy
  - In order to get optimal DRS efficiency from your clusters you want to
    - Ensure each host has the same resource configuration (memory, CPU)
    - DRS Clusters support a maximum of 32 hosts and 3000 virtual machines
    - Put vMotion on a separate layer network and use 10Gb if possible, also multiple NIC vMotion
    - Don't set VM-HOST affinity rules (must rules) unless you absolutely have to
    - Don't change the default automation level per virtual machine if you don't have to
  - Don't oversize your virtual machines, wasted resources can cause cluster imbalance
  
- **Properly apply virtual machine automation levels based upon application requirements**
  - When creating a DRS cluster you set a virtual machine automation level for the cluster. There might be some use cases that require a virtual machine, or a set of virtual machines, that require a different level of automation then what the default for the cluster is. You can set automation levels for virtual machines individually
    - Do this sparingly. The more individual changes you make, the more management overhead you add, as well as potentially reducing the effectiveness of DRS
  - Why would you want to make changes to an individual virtual machine?
    - Applications might have to stay on a particular host due to licensing requirements
    - If you have an application that is constantly changing its memory contents, you may want not want it to move hosts as often as other virtual machines
  - Apply automation levels to individual virtual machines
    - Log into the vSphere client
    - Right-click on a DRS cluster from the inventory tree and click *Edit Settings...*
    - Under the *vSphere DRS* option choose *Virtual Machine Options*
    - Ensure that the *Enable individual virtual machine automation levels* checkbox is checked

- In the *Automation Level* column, change the virtual machine(s) to the desired automation level using the dropdown



- Click *OK*

- **Create and administer ESXi host and Datastore Clusters**

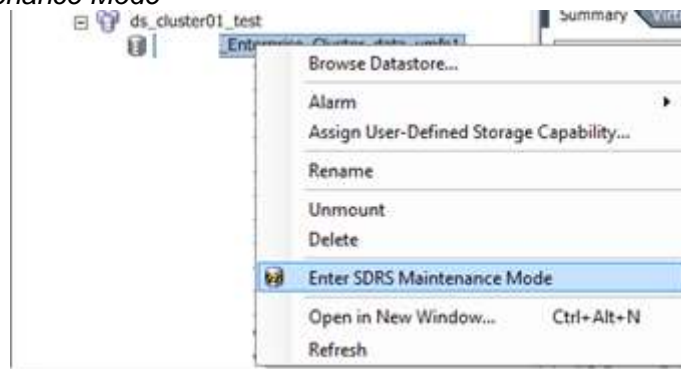
- I've already documented, in detail, the creation and administration of Datastore Clusters in [Objective 1.2 – Manage Storage Capacity in a vSphere Environment](#) (it's towards the bottom the the post). Please refer to that section.

- **Administer DRS / Storage DRS**

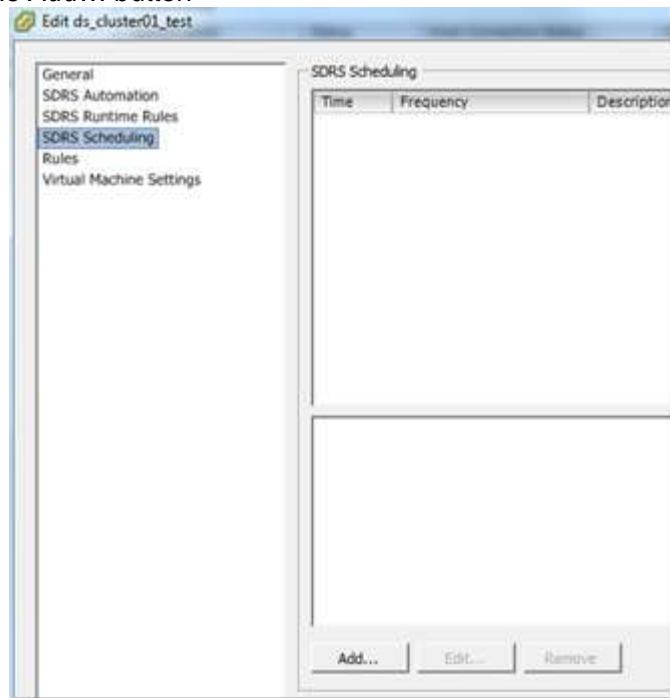
- Administering a DRS cluster involves creating and managing DRS affinity and anti-affinity rules, DRS virtual machine groups, DRS cluster validation and standard addition/removal of hosts from the DRS cluster
- All administration takes place within the GUI and almost all of it within the cluster settings
- Administering DRS
  - Adding and removing hosts
    - This is pretty straight forward; right-click on the cluster and click *Add Host* and go through the wizard

- To remove a host from the cluster the host must be in maintenance mode first
- Cluster Validation
  - A cluster can become overcommitted or invalid. The cluster object in the inventory tree will show yellow for overcommitted and red for invalid. A cluster can become invalid if you make changes directly to a host, and those changes aren't reflected in vCenter. When vCenter comes back into the mix, there is a mismatch, which causes it to become invalid
- Creating VM Anti Affinity/Affinity rules
  - There is some overlap between some of the VCAP-DCA objectives and the VCP5 objectives. While I hate referring you to another link to get information, I feel that it isn't very efficient to duplicate some of these items when I could be continuing with other objectives in the blueprint.
    - Check out [Objective 5.1 – Create and Configure VMware Clusters](#) from the VCP5 blueprint to read about DRS affinity rules
- Storage DRS can only be used with a new construct known as Datastore Clusters. With this new construct, come different points of administration, such as datastore maintenance mode, Storage DRS scheduled tasks, Storage DRS recommendations and, as with DRS, automation levels for individual virtual machines
- Administering Storage DRS
  - Storage DRS Maintenance Mode
    - Must be manually invoked and is only available to datastores within a datastore cluster
    - Log into the vSphere client
    - Navigate to the *Datastores and Datastore Clusters* view (*Ctrl+Shift+D*)
    - Right-click on the datastore within the datastore cluster and click *Enter SDRS Maintenance Mode*

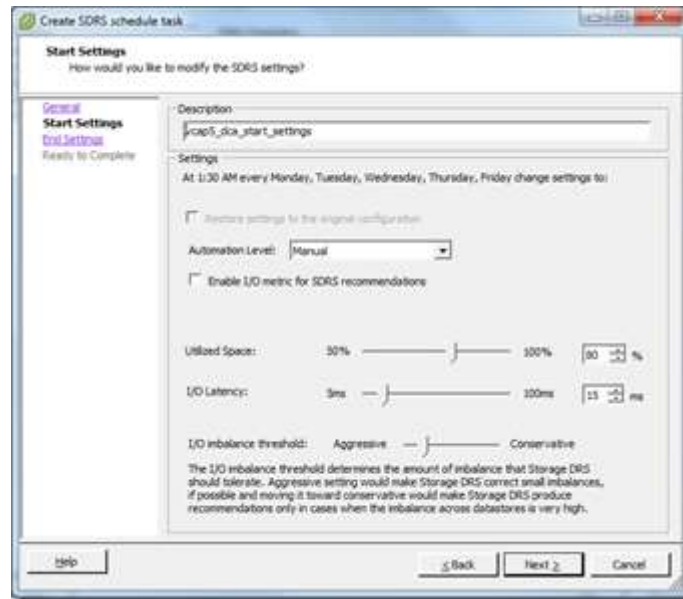
*Maintenance Mode*



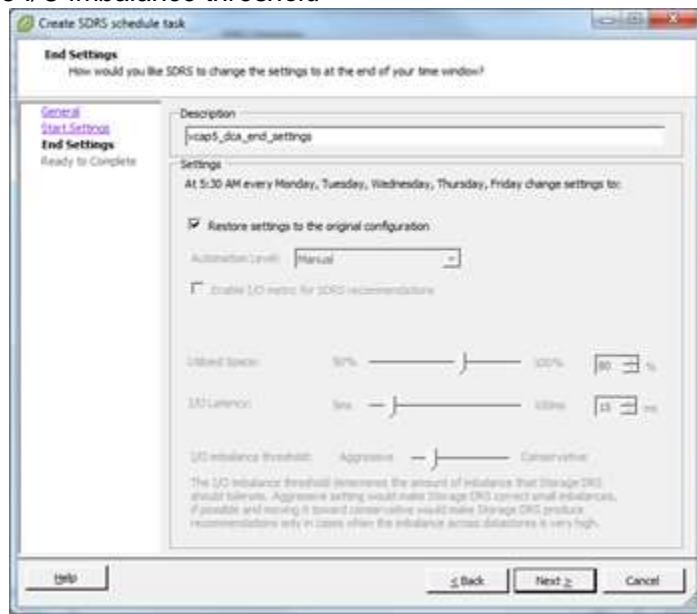
- SDRS Scheduling
  - You can schedule Storage DRS to run at certain time (such as when little/I/O users are at the office) in order to move vmdks to different datastores within the cluster. You then set the end settings which will revert SDRS back to its original configuration, or to a configuration you specify
  - Log into the vSphere client
  - Navigate to the *Datastores and Datastore Clusters* view (*Ctrl+Shift+D*)
  - Right-click a datastore cluster from the inventory tree > click *Edit Settings...*
  - Choose *SDRS Scheduling*
  - Click the *Add...* button



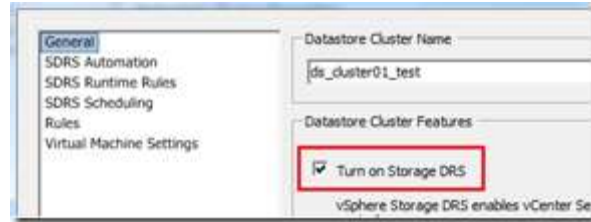
- Enter a Start and End time as well as the Frequency > click *Next*
- At the *Start Settings* page enter in a *Description*
- Choose the *Automation Level* (Manual or Fully Automated)
- Enable the *I/O metric* for SDRS recommendations (optional)
- Set the *Utilized Space (%)*
- Set the *I/O Latency (ms)*
- Decide and set your *I/O imbalance threshold* (see screenshot for description)



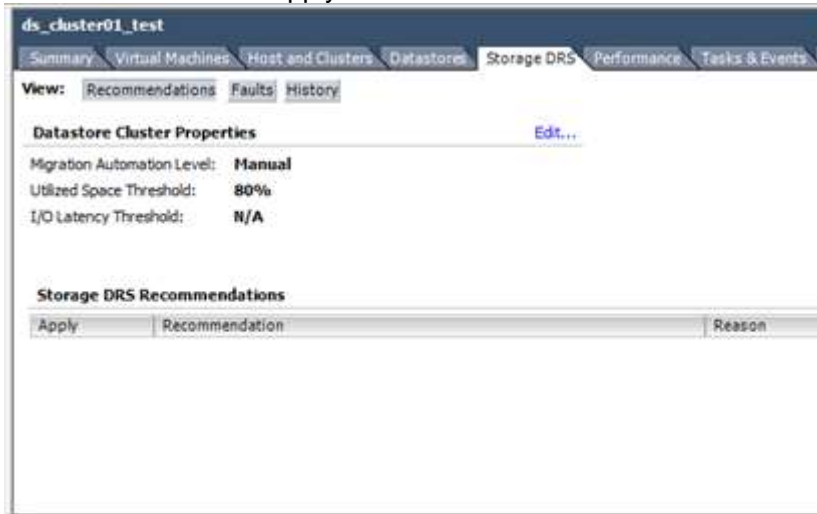
- Click *Next*
- At the *End Settings* page enter in a *Description*
- Leave the *Restore settings to the original configuration* checkbox checked
  - If you uncheck this option, set the *Utilized Space (%)*, *I/O Latency (ms)* and the *I/O imbalance threshold*



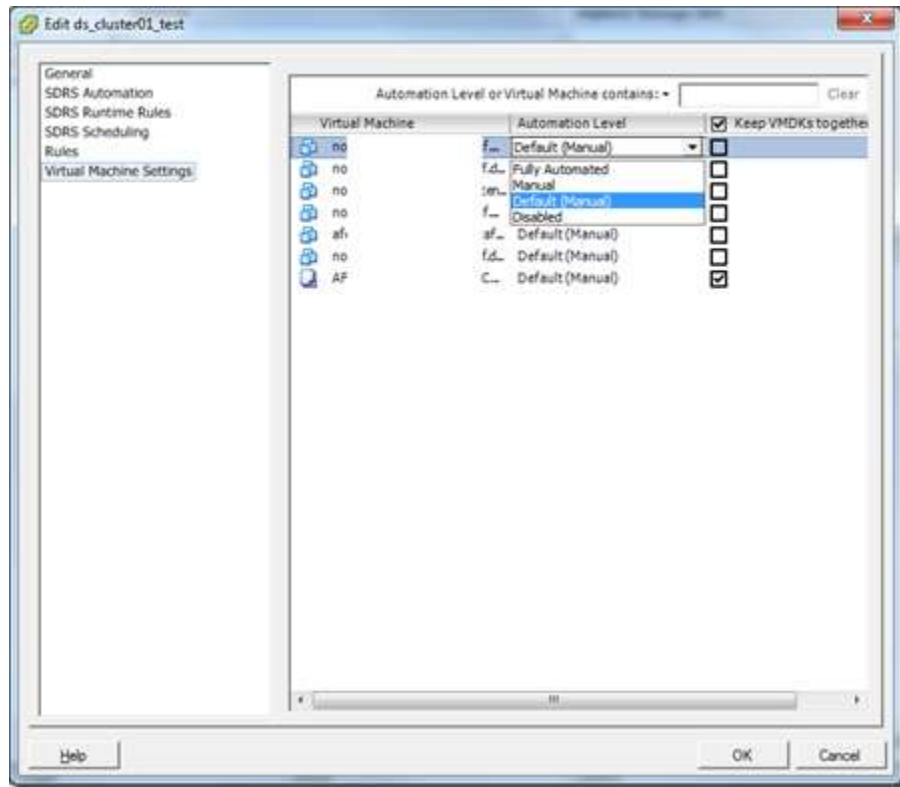
- Click *Next*
- Click *Finish*
- Storage DRS Recommendations
  - Before you can get Storage DRS recommendations, or use it period, you need to make sure it is enabled on



- Log into the vSphere client
- Navigate to the *Datastores and Datastore Clusters* view (*Ctrl+Shift+D*)
- Choose a datastore cluster from the inventory tree > click the *Storage DRS* tab on the right
- In the *Storage DRS Recommendations* pane you can choose any pending recommendations and apply them

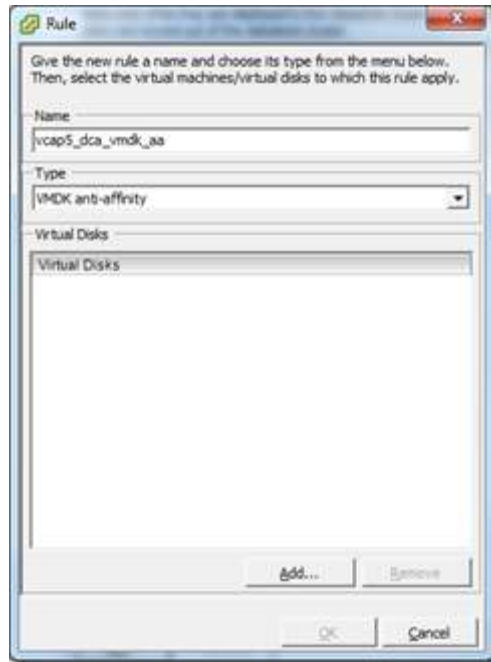


- Storage DRS Virtual Machine Settings
  - There are two parts that make up virtual machine settings; the automation level and the option to keep VMDKs (disk affinity) together
  - Log into the vSphere client
  - Navigate to the *Datastores and Datastore Clusters* view (*Ctrl+Shift+D*)
  - Right-click a datastore cluster from the inventory tree > click *Edit Settings...*
  - Choose *Virtual Machine Settings*
  - For each virtual machine you want to change, set the *Automation Level*(Fully Automated, Manual, Default or Disabled)
  - Check/uncheck the box to *Keep VMDKs together*

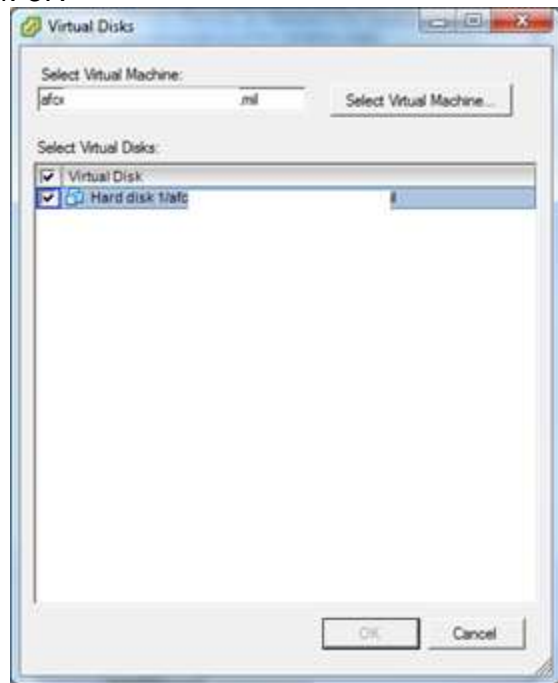


- Click *OK*
- Storage DRS Rules
  - Like DRS, Storage DRS has rules you can setup. Rules to keep VMs separate (VM anti-affinity), which means disks from those particular virtual machines will be kept on different datastores within the datastore cluster. The other option is the VMDK anti-affinity which separates virtual disks that belong to a particular virtual machine on different datastores within the datastore cluster
  - Log into the vSphere client
  - Navigate to the *Datastores and Datastore Clusters* view (*Ctrl+Shift+D*)
  - Right-click a datastore cluster from the inventory tree > click *Edit Settings...*
  - Choose *Rules* > click *Add...*
  - Enter in a *Name* for the new rule > choose the type of rule from the dropdown

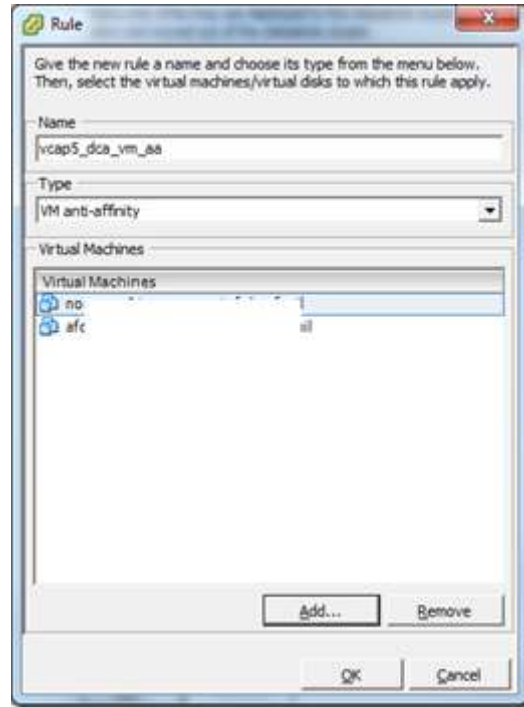




- *VMDK anti-affinity*
  - Click *Add*
  - Click the *Select Virtual Machine* button
  - Choose a virtual machine from the list > click *O*Choose the virtual disks you want to separate (in the screenshot below there is only one virtual disk, you need at least two before you can proceed)
  - Click *OK*



- *VM anti-affinity*
  - Click *Add*
  - Select two or more virtual machines from the list
  - Click *OK*



- Click *OK* when finished

## Tools

- [vSphere Resource Management Guide](#)
- [Product Documentation](#)
- vSphere Client
  - DRS / Storage DRS Resource Distribution Chart

# VCAP5-DCA – Objective 3.4 – Utilize Advanced vSphere Performance Monitoring Tools

---

For this objective I used the following documents:

- Documents listed in the Tools section

## **Objective 3.4 – Utilize Advanced vSphere Performance Monitoring Tools**

### Knowledge

**\*\*ITEMS IN BOLD ARE TOPICS PULLED FROM THE BLUEPRINT\*\***

- **Identify hot key fields used with *resxtop* / *esxtop***
  - There are some different hot keys that will get you to different views within ***resxtop*** / ***esxtop*** and some other hot keys that will perform different functions from within those screens. Let's start with the different screens (the sort by commands are listed underneath each display, and are case sensitive):
    - *resxtop* / *esxtop*Displays
      - **c:cpu**– used to display CPU statistics
        - **U** - will sort by the %USED metric
        - **R** - will sort by the %RDY metric
        - **N** – will sort by the GID (group ID)
      - **i:interrupt** - used to display the interrupt handler statistics (I really don't know what that even means)
      - **m:memory**– used to display memory statistics
        - **M**- will sort by the MEMSZ metric
        - **B**- will sort by the MCTLSZ metric
        - **N** – will sort by the GID (group ID)
      - **n:network**– used to display network statistics
        - **T**- will sort by MbTX/s
        - **t**- will sort by PKTTX/s
        - **N** – will restore the default sort order (which I believe is the **PORT-ID**field)
        - **R**- will sort by MbRX/s
        - **r** – will sort by PKTRX/s
      - **d:disk adapter** – used to display disk adapter statistics
        - **r**- will sort by READS/s

- **R**- will sort by MBREADS/s
- **N** – will restore the default sort order (which I believe is the **ADAPTR**field)
- **w**- will sort by WRITES/s
- **T** – will sort by MBWRTN/s
- **u:disk device**– used to display disk device statistics
  - **r**- will sort by READS/s
  - **R**- will sort by MBREADS/s
  - **N** – will restore the default sort order (which I believe is the **DEVICE**field)
  - **w**- will sort by WRITES/s
  - **T** – will sort by MBWRTN/s
- **v:disk VM**– used to display VM disk statistics
  - **r**- will sort by READS/s
  - **R**- will sort by MBREADS/s
  - **N** – will restore the default sort order (which I believe is the **GID**field)
  - **w**- will sort by WRITES/s
  - **T** – will sort by MBWRTN/s
- **p:power mgmt** – used to display power statistics
- Some other hot keys that might be useful:
  - **h** from any screen will display the help menu. The help menu will display hot keys for other screens, and other options
  - **f** from any screen will bring up a list of available fields for that particular statistic. To turn on/off a metric press the letter corresponding to the field name
  - **s** from any screen brings up a prompt that allows you to enter in the number of seconds you want the screen to refresh (the lowest is 2)
  - **q** from any screen will quit the *resxtop / esxtop* utility
- **Identify fields used with vscsiStats**
  - Fields are a bit difficult to identify with vscsiStats because the utility generates data that is best used when put into a histogram. Some of the different metrics it pulls:
    - **I/O Command Length**- overall commands, read commands and write commands
    - **Distance between successive commands (in LBNs)**– overall distance, read distance and write distance

- **Distance between each command from the 16 closest previous commands**— overall, read and write commands
  - **Latency** (in microseconds) – overall, read and write latency
  - **Number of outstanding I/Os**— when a new I/O is issued, new read I/O and new write I/O
  - **I/O Interarrival Time** – overall interarrival time, I/O read interarrival time and I/O write interarrival time
- I'll go over in a later section of how to run vscsiStats

## Skills and Abilities

- **Configure *esxtop* / *resxtop* custom profiles**
  - Creating a custom profile in *esxtop* / *resxtop* is pretty simple. This procedure is the same with both *esxtop* and *resxtop*. Just remember with *resxtop* that you need to either connect to a server first, or specify the server when running the utility
  - Configure *esxtop* / *resxtop* Custom Profiles
    - SSH to an ESXi host or the vMA (vSphere Management Assistant)
    - Type *esxtop* (use *resxtop* if you are connected to a vMA)
    - Go through each display and customize them to your liking. Examples of this would be which fields to display, field order, refresh interval, etc...
    - Once you have made all of your customizations, press **W**
    - The default location is **<current working directory>/.esxtop50rc**, You can use this or specify your own path and filename
    - When finished, press enter to save the file (for this example I've use **/tmp/.vcap5esxtopconf**

```

1:21:21am up 33 days 3:28, 317 worlds, 3 VMs, 6 vCPUs; CPU load average: 0.
Save config file to (Default to : // .esxtop50rc): /tmp/.vcap5esxtopconf
vmhba0 - 1 0.00 0.00 0.00 0.00 0.00
vmhba32 - 0 0.00 0.00 0.00 0.00 0.00
vmhba33 - 0 0.00 0.00 0.00 0.00 0.00
vmhba34 - 0 0.00 0.00 0.00 0.00 0.00
vmhba35 - 8 0.00 0.00 0.00 0.00 0.00

```

- You have saved the configuration successfully
- Now you can load *esxtop* / *resxtop* using the **-c** parameter
  - *esxtop -c /tmp/.vcap5esxtopconf*
  - Press enter
  - Now all of the customizations you made and saved previously should be set

- **Determine use cases for and apply *esxtop* / *resxtop* Interactive, Batch and Replay modes**

- Interactive Mode

- *esxtop* / *resxtop* interactive mode is for real-time analysis/troubleshooting of a particular host. For example, if you are trying to nail down a certain performance issue (Compute, Network or Storage) then interactive mode is for you
- Using Interactive mode is as simple as typing *esxtop* from the command line, either from the console of a host or SSH'd to the host. Use *resxtop* if you are connected to the vMA

- Batch Mode

- Batch mode can be useful if you want to track certain metrics over a period of time. Now you can do some of the same thing with history charts from vCenter, but with vCenter you are limited to >20 second intervals, *esxtop* / *resxtop* can go as low as 2 second intervals
- To use Batch mode use the following commands; applies to *esxtop* and *resxtop*

```
1 # -b stands for batch mode
2 # -d stands for delay (in seconds), which i've set to 2
3 # -n is the number of iterations that will be complete, which i've set to 400
4 # setting the iterations to 400 means that it will record all metrics over an 800 second
5 # the > means export and i'm exporting to a compressed csv file
6 # named vcap5esxtopbatch.csv.gz
7
8 esxtop -b -d 2 -n 400 > vcap5esxtopbatch.csv.gz
```

- Once batch mode is complete you can copy the CSV file over to another system and decompress it
- You can then load it into a utility called ***esxplot***, which is awesome BTW. *esxplot* is a VMware Labs Fling and can be found [here](#)
- You can also load the results into the Windows ***perfmon*** utility and analyze the capture

- Replay Mode

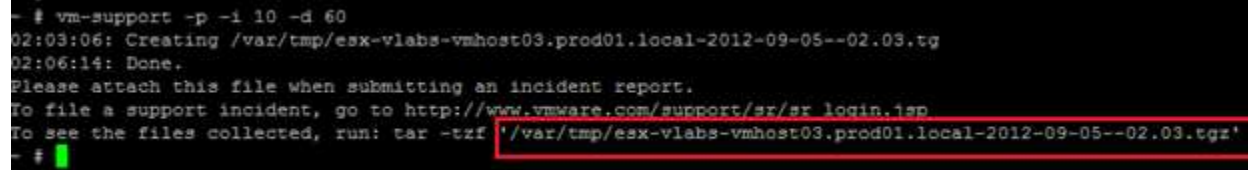
- Replay mode is a pretty cool feature of *esxtop* / *resxtop*. Replay mode allows you to use a *vm-support* generated bundle and run *esxtop* / *resxtop* in Replay mode against it, thus allowing you to look at snapshots of an environment
- A big use case for this is when you need someone else who does not have access to your host(s) analyze these metrics. Using Reply mode you can generate a support

bundle and send it to whomever you need. They can then extract that bundle and use *esxtop* / *resxtop*Replay mode against it to see what's been going on

- To generate a support bundle with performance snapshots run the following command directly from the host or using the vMA

```
1 # the -p parameter specifies you want to collect performance snapshots
2 # the -i parameter specifies the interval (in seconds) between collecting
3 # performance snapshots
4 # the -d parameter specifies the duration of which the performance snapshots
5 # should be taken
6
7 vm-support -p -i 10 -d 60
```

- Check out VMware [KB1967](#) for additional information
- Once complete the location of the support bundle will be displayed on the screen



```
- # vm-support -p -i 10 -d 60
02:03:06: Creating /var/tmp/esx-vlabs-vmhost03.prod01.local-2012-09-05--02.03.tgz
02:06:14: Done.
Please attach this file when submitting an incident report.
To file a support incident, go to http://www.vmware.com/support/sr/sr_login.jsp
To see the files collected, run: tar -tzf '/var/tmp/esx-vlabs-vmhost03.prod01.local-2012-09-05--02.03.tgz'
```

- Before you can use this newly generated bundle with Replay mode, you must first decompress it. Change directory to */var/tmp*

```
1 # the -x parameter means you want to extract the files
2 # the -z parameter filters it through gzip
3 # the -f parameter specifies the name of the TAR file
4
5 tar -xzf esx-vlabs-vmhost03.prod01.local-2012-09-05--02.03.tgz
6
7 # before continuing you may need to reconstruct files that were fragmented
8 # by running the following script from the support directory
9
10 #change to support directory
11 cd /var/tmp/esx-vlabs-vmhost03.prod01.local-2012-09-05--02.03
```

```
12 #run reconstruct script
13 ./reconstruct.sh
14
```

- Now enter in the following command to run Replay mode against the extracted bundle

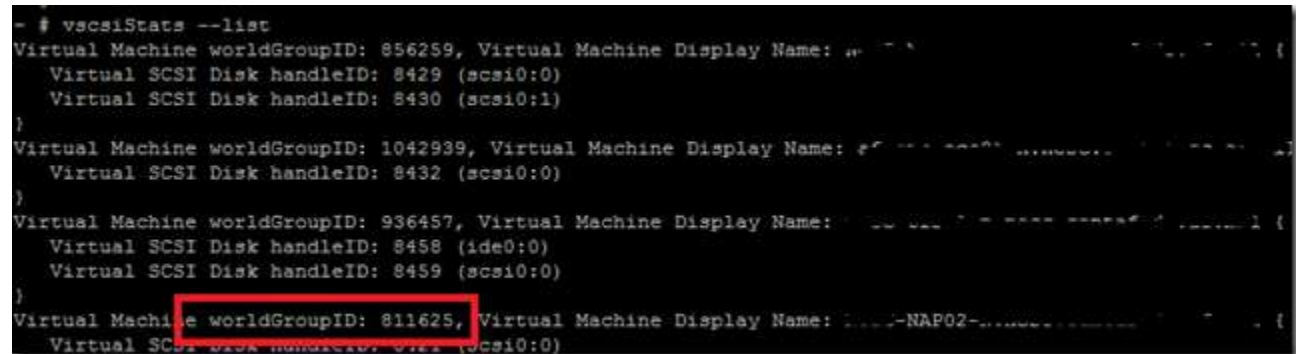
```
1 # -R specifies Replay mode
2 # the path is the location of your extracted support bundle
3
4 esxtop -R /var/tmp/esx-vlabs-vmhost03.prod01.local-2012-09-05--02.03
```

- **Use vscsiStats to gather storage performance data**

- To run vscsiStats you'll need to know the worldGroupID of the VM you want to gather performance data on. To get the worldGroupID of the VMs on a specific host run the following command

```
1 vscsiStats --list
```

- You'll be presented with a list of VMs for that host. Find the VM you want to gather data on and find the worldGroupID. In this example I'm getting the worldGroupID for the NAP02 VM, which is 811625



```
- # vscsiStats --list
Virtual Machine worldGroupID: 856259, Virtual Machine Display Name: ...
  Virtual SCSI Disk handleID: 8429 (scsi0:0)
  Virtual SCSI Disk handleID: 8430 (scsi0:1)
}
Virtual Machine worldGroupID: 1042939, Virtual Machine Display Name: ...
  Virtual SCSI Disk handleID: 8432 (scsi0:0)
}
Virtual Machine worldGroupID: 936457, Virtual Machine Display Name: ...
  Virtual SCSI Disk handleID: 8458 (ide0:0)
  Virtual SCSI Disk handleID: 8459 (scsi0:0)
}
Virtual Machine worldGroupID: 811625, Virtual Machine Display Name: ...-NAP02-...
  Virtual SCSI Disk handleID: 8459 (scsi0:0)
```

- Now that we have the worldGroupID we need to start the collection. If the VM you are gathering data for has multiple disks, you can specify a particular disk with the -i parameter. If you don't specify a handle ID then the collection will be for all disks attached to the VM

```
1 # run vscsiStats on all disks for a VM with the worldGroupID of 811625
2 # the -w parameter specifies the worldGroupID
3 # the -s parameter tells vscsiStats to start the collection
4
5 vscsiStats -w 811625 -s
```



```

6
7 # run vscsiStats on a specific disk on the VM. The worldGroupID for the VM is
8 # 811625 and the handleID for the specific disk is 8422
9 # the -i paramter is used to specify a specific disk (handleID)
10
11 vscsiStats -w 811625 -i 8422 -s

```

- In this example I'm starting a collection against the VM with a worldGroupID of 811625 and a handleID of 8422

```

~ # vscsiStats -w 811625 -i 8422 -s
vscsiStats: Starting Vscsi stats collection for worldGroup 811625, handleID 8422 (scsi0:1)
Success.
~ #

```

- Once you've started the collection you can look at the data it has collected via histograms. The `-p` option is used to specify a histogram. The following histogram types can be specified:
  - all
  - ioLength
  - seekDistance
  - outstandingIOs
  - latency
  - interarrival
- By default this will be displayed on the screen, but what you really want is to be able to import it into excel so you can analyze the data. To comma delimit the file use the `-c` option. Here's an example of exporting a histogram with a type of *all* using comma delimitation exported to a file named `vcap5vscsiStats.csv` for a VM with a worldGroupID of 811625 and a handleID of 8422

```

1 # the -w parameter specifies the worldGroupID
2 # the -i parameter specifies the handleID
3 # the -p parameter specifies the type of histogram you want
4 # the -c parameter specifies the output be comma delimited
5
6 vscsiStats -w 611825 -i 8422 -p all -c > /tmp/vcap5vscsiStats.csv

```

- To stop the vscsiStats collection execute the following command

```

1 # the -w parameter specifies the groupWorldID

```

```
2 # the -x parameter tells vscsiStats to stop collecting
3 # if you are collecting on multiple disks you can use the -i parameter
4 # to stop collection on only a specific disk
5
6 vscsiStats -w 625811 -x
```

- To view data collected in really cool 3-D surface charts check out [this site](#). It requires you to type up a small script (example provided) to get 21 thirty second samples. You can then take the output of that and import it into a template that will build all of the surface charts for you. Very cool stuff.

- **Use *esxtop* / *resxtop* to collect performance data**

- There are a few ways to view performance data within *esxtop* / *resxtop*; interactive mode, batch mode and replay mode. I covered these modes earlier so I won't go into them again here. To *collectdata* I would assume this means over a period of time. To do that you have to use batch mode
- Batch mode allows you to collect performance data with *esxtop* / *resxtop* over a period of time. You can specify a custom configuration file that contains only views and fields that are pertinent and you specify the delay between captures and number of iterations you want to capture
  - - For example, you want to collect data using *esxtop* / *resxtop* every 5 seconds for 10 minutes. To do this you will specify a delay of 5 seconds with the number of iterations to 120 ((minutes x 60) / delay). This example would be ((10 x 60) / 5) = 120
- Here is the command you need to execute

```
1 # the -b parameter tells esxtop /resxtop to run in batch mode
2 # the -d parameter specifies the delay between captures
3 # the -n parameter specifies the number of iterations to perform
4 # i'm outputting this to a CSV file for import into another tool
5
6 esxtop -b -d 5 -n 120 > /tmp/vcap5esxtop.csv
```

- Once this completes copy the CSV file to a system where you have [esxplot](#). Open **esxplot** and import the CSV file. Now you can analyze the performance data you just collected

- **Given *esxtop* / *resxtop* output, identify relative performance data for capacity planning purposes**

- When planning for future capacity, you need to see where you stand now. Are you oversubscribed? Do you currently have enough CPU, Memory, Disk? If so, what levels are you at? If not, how do you tell what is oversubscribed? Well, I am not going to go over every metric that exists within *esxtop* / *resxtop*, but I will go into a few metrics that can easily let you know if you have a problem

- CPU

- The CPU load average at the top of the screen can be a quick way to determine if your physical CPUs are being hammered on that particular host. The load average is represented in 1, 5 and 15 minutes from left to right based on 6 second samples. The CPU load takes into account the ready time and run time for all groups on the host
- Based on the below screenshot you'll see that the CPU load average for 1 minute is 0.23, for 5 minutes is 0.22 and 15 minutes is 0.23

```
7:38:18pm up 21 days 2:14, 418 worlds, 9 VMs, 15 vCPUs; CPU load average: 0.23, 0.22, 0.23
PCPU USED(%): 7.3 2.3 4.1 3.4 5.8 5.2 5.9 2.8 3.6 1.9 55 2.4 4.0 27 1.6 27 AVG: 10
PCPU UTIL(%): 7.6 2.6 4.4 3.5 6.1 5.1 5.7 2.7 3.9 1.8 51 2.8 4.3 27 2.0 28 AVG: 9.9
CORE UTIL(%): 10 7.8 11 8.6 5.5 52 30 29 AVG: 19
```

- The **PCPU UTIL(%)** statistic can also let you know if you are in an overcommitted state. If the **PCPU UTIL(%)** is high across all PCPUs then there is a good change you are overcommitting your CPU resources on that host
- You can see here each that the AVG across all is only 9.9%, so all is well

```
7:38:18pm up 21 days 2:14, 418 worlds, 9 VMs, 15 vCPUs; CPU load average: 0.23, 0.22, 0.23
PCPU USED(%): 7.3 2.3 4.1 3.4 5.8 5.2 5.9 2.8 3.6 1.9 55 2.4 4.0 27 1.6 27 AVG: 10
PCPU UTIL(%): 7.6 2.6 4.4 3.5 6.1 5.1 5.7 2.7 3.9 1.8 51 2.8 4.3 27 2.0 28 AVG: 9.9
CORE UTIL(%): 10 7.8 11 8.6 5.5 52 30 29 AVG: 19
```

- Memory

- The **state** metric is an easy one to look at and understand. The **state** metric has the following possible values
  - High – will be High if free memory is greater >6%
  - Soft – will be Soft if free memory is 4%-6%
  - Hard – will be Hard if free memory is 2% – 4%

- Low – will be Low if free memory is <2%
- If your host is in a **High State** then there isn't memory pressure. If your host is in any other **State** then you need to start monitoring closely and think about adding more capacity if it's in a **Hard** or **Low** state
- As you can see this particular host is in a **High State**

```
7:52:42pm up 21 days 2:28, 418 worlds, 9 VMs, 15 vCPUs; MEM overcommit avg: 0.
PMEM /MB: 65522 total: 1467 vmk, 44447 other, 19607 free
VMKMEM/MB: 65199 managed: 1266 minfree, 8749 rsvd, 56449 ursvd, high state
NUMA /MB: 32768 (10740), 32754 ( 7134)
PSHARE/MB: 1948 shared, 820 common: 1128 saving
SWAP /MB: 0 curr, 0 rclmtgt: 0.00 r/s, 0.00 w/s
ZIP /MB: 0 zipped, 0 saved
MEMCTL/MB: 0 curr, 0 target, 26621 max
```

- Another statistic to look at is **SWAP /MB**. This will tell you if there is memory swapping currently happening for the host, and what rate memory is swapping in from/out to disk. If the **r/s** or **w/s** is high then you have a problem. Most likely if these two are high your memory state is either Hard or Low
- As you can see from the screenshot below, the **r/s** and **w/s** are at 0.00, which is good

```
7:52:42pm up 21 days 2:28, 418 worlds, 9 VMs, 15 vCPUs; MEM overcommit avg: 0.
PMEM /MB: 65522 total: 1467 vmk, 44447 other, 19607 free
VMKMEM/MB: 65199 managed: 1266 minfree, 8749 rsvd, 56449 ursvd, high state
NUMA /MB: 32768 (10740), 32754 ( 7134)
PSHARE/MB: 1948 shared, 820 common: 1128 saving
SWAP /MB: 0 curr, 0 rclmtgt: 0.00 r/s, 0.00 w/s
ZIP /MB: 0 zipped, 0 saved
MEMCTL/MB: 0 curr, 0 target, 26621 max
```

o Disk

- Using *esxtop* / *resxtop* you can't really determine if you have enough disk in terms of capacity (GB), but you may be able to determine if you have enough capacity in terms of number of spindles as it relates to IOPs (I/Os per second). IOPs is an important metric for storage performance, and as a result, application performance for your VMs.
- These statistics are per-VM instead of per-host (as we've been focused on for CPU and memory), but you might need more capacity in terms of IOPs for only one VM, and it can be deciphered based on those per-VM statistics. If you have an application/workload that requires a certain amount of IOPs you can use *esxtop* / *resxtop* to see what IOPs you are currently getting to make sure you are where you need to be, or identify a deficiency. Here are the counters you can look at

-

- **READS/s**– shows the number of reads per second
- **WRITES/s** – shows the number of writes per seconds
- You can use the metrics identified above in concert with *esxtop* / *resxtop* Batch mode and see if you are getting the required amount of sustained IOPs over a certain period of time

## Tools

- [vSphere Resource Management Guide](#)
- [Product Documentation](#)
- vSphere Client
- vSphere CLI
  - *esxtop* / *resxtop*
  - *vscsiStats*

# VCAP5-DCA Objective 4.1–Implement and Maintain Complex VMware HA Solutions

---

For this objective I used the following documents:

- [VMware vSphere 5 Clustering Technical Deepdive](#) by Duncan Epping and Frank Denneman
- Documents listed in the Tools section

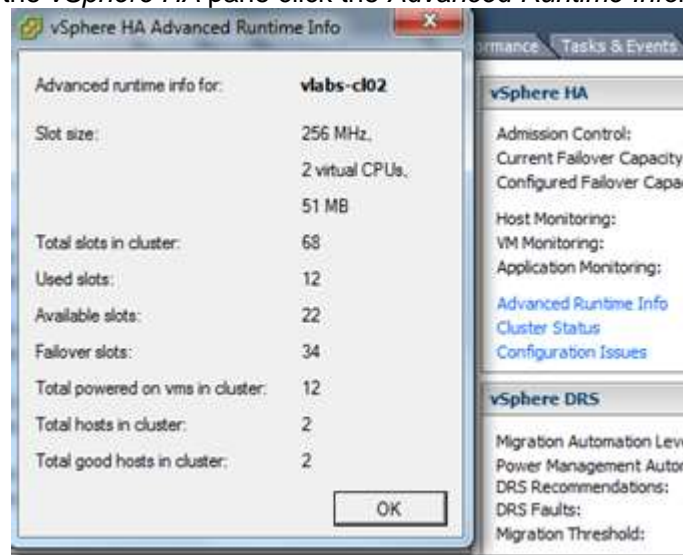
## **Objective 4.1 – Implement and Maintain Complex VMware HA Solutions**

### Knowledge

**\*\*ITEMS IN BOLD ARE TOPICS PULLED FROM THE BLUEPRINT\*\***

- **Identify the three admission control policies for HA**
  - There are actually three types of admission control mechanisms; host, resource and HA. As you may be aware, HA is the only one of the three that can be disabled. There are several operations within vSphere that will result in resource constraints being applied. Operations such as powering on a virtual machine, migrating a virtual machine or increasing CPU/memory reservations on a virtual machine
  - There are three three types of HA admission control policies:
    - **Host Failures Cluster Tolerates**
      - Using this policy you would specify a the number of host failures. Meaning, resources are kept available based on the number of hosts you specify in order to ensure resource capacity for failed over virtual machines
      - This is accomplished using a 'slot size' mechanism. Slot sizes are logical constructs of memory and CPU and represent a single virtual machine.
      - Slot sizes are calculated based on the largest CPU and memory reservation for a virtual machine. If no reservations are present, the defaults are:
        - 32MHz for CPU
          - this can be changed by modifying the advanced setting **das.vmcPuminMhz**
        - 0MB + overhead for memory
        - The most restrictive between memory slots and CPU slots will ultimately determine the slot count
      - Lets go through an example:
        - Host 1: 8GB memory, one 2.56GHz CPU
        - Host 2: 8GB memory, one 2.56GHz CPU

- VM1: 2GB memory reservation, 700Mhz CPU reservation
- VM2: 3GB memory reservation, 400MHz CPU reservation
- With the configuration above, The memory slot would be 3GB and the CPU slot would be 700MHz
- Since these hosts are the same size, the slot size per host is 2.5 for memory and 3 for CPU
- Since the number of memory slots is the most restrictive, it is used as number of slots per host
- Total number of cluster slots: 4
- Used Slots: 2
- Available Slots: 0
- Failover Slots: 2
- Total powerd on vms in cluster: 2
- Total hosts in cluster: 2
- Total good hosts in cluster: 2
- You can view slot information for the cluster using the *Advanced Runtime Info*
  - Log into the vSphere client > select a cluster
  - Click the *Summary* tab
  - In the *vSphere HA* pane click the *Advanced Runtime Info*hyperlink



- Percentage of Cluster Resources Reserved
  - This admission control policy implements resource constraints based upon a user-defined percentage of memory and CPU resource

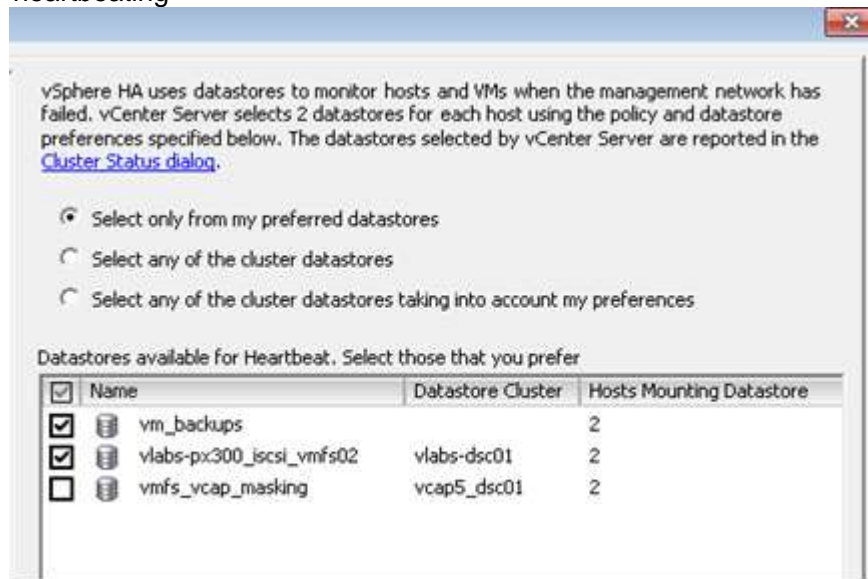
- Virtual Machine resource requirements:
  - If no CPU reservation exists a default of 32Mhz is used
  - If no memory reservation exists a default of 0MB + overhead is used
- Calculate failover capacity with the following formula
  - $\text{Total Host Resources} - \text{Total Resource requirement} / \text{Total Host Resources}$
  - Here's an example:
    - Total Host CPU Resources: 5000GHz
    - Total CPU resource requirements: 2400GHz
    - $5000 - 2400 = 2600 / 5000 = 52\%$  failover capacity
- When admissions control is invoked, it will check the current CPU and memory failover capacity. If the operation that invoked admission control will violate the percentages defined for the cluster, then admissions control will not allow the operation to complete. Here are the steps:
  - Total resources currently being used by powered-on virtual machines is calculated
  - Total host resources are calculated (excluding overhead)
  - CPU and memory failover capacity is calculated
  - The percentage of failover capacity for CPU and memory is compared to the user-defined percentages of the cluster
  - Prior to the operation being performed, a calculation is done to determine the new failover capacity if the operation is allowed. If the new failover capacity violates the user-defined percentages (CPU or memory), then the operation is not allowed
- If you log into the vSphere client and look at the *Summary* tab for a cluster you can see information related to this admission control policy in the *vSphere HA* pane

vSphere HA	
Admission Control:	Enabled
Current CPU Failover Capacity:	82 %
Current Memory Failover Capacity:	99 %
Configured CPU Failover Capacity:	25 %
Configured Memory Failover Capacity:	25 %
Host Monitoring:	Enabled
VM Monitoring:	Disabled
Application Monitoring:	Disabled



- Here you can easily see the current CPU failover and memory capacity as well as the user-defined percentages
  - Specify Failover Hosts
    - This is the most straight-forward policy of the three. Using this admission control policy will set aside whatever number of hosts you specify **ONLY** for failover purposes
    - If you have a 4-node HA cluster using the *Specify Failover Hosts* and configure it for 1, then whichever host you specify will never be used except in the event of an HA failover
- **Identify heartbeat options and dependencies**
  - vSphere HA has two heartbeating mechanisms; network and datastore heartbeating
  - Network Heartbeating
    - Network heartbeating is pretty straight-forward. Slave nodes will send a heartbeat to the master node and the master node will send a heartbeat to each of the slave nodes. The slaves do not send heartbeats to each other, but will communicate during the master node election process
    - Network heartbeats occur every 1 second by default
    - Networking heartbeating is dependent on the management address of the host
  - Datastore Heartbeating
    - Datastore heartbeating was introduced in vSphere 5 and adds another layer of resiliency for HA. Datastore heartbeating also helps in preventing unnecessary restarts of virtual machines
    - When a master node stops receiving network heartbeats it will then use datastore heartbeats to determine if the host is network partitioned, isolated or if it has complete failed
    - The datastore heartbeating mechanism is only used when:
      - The master node loses connectivity to slave nodes
      - Network heartbeating fails
    - HA will select two datastores to use for datastore heartbeating (by default, you can increase this with an advanced setting which is covered later). The criteria used for the datastore selection is:
      - Datastore that is connected to all hosts

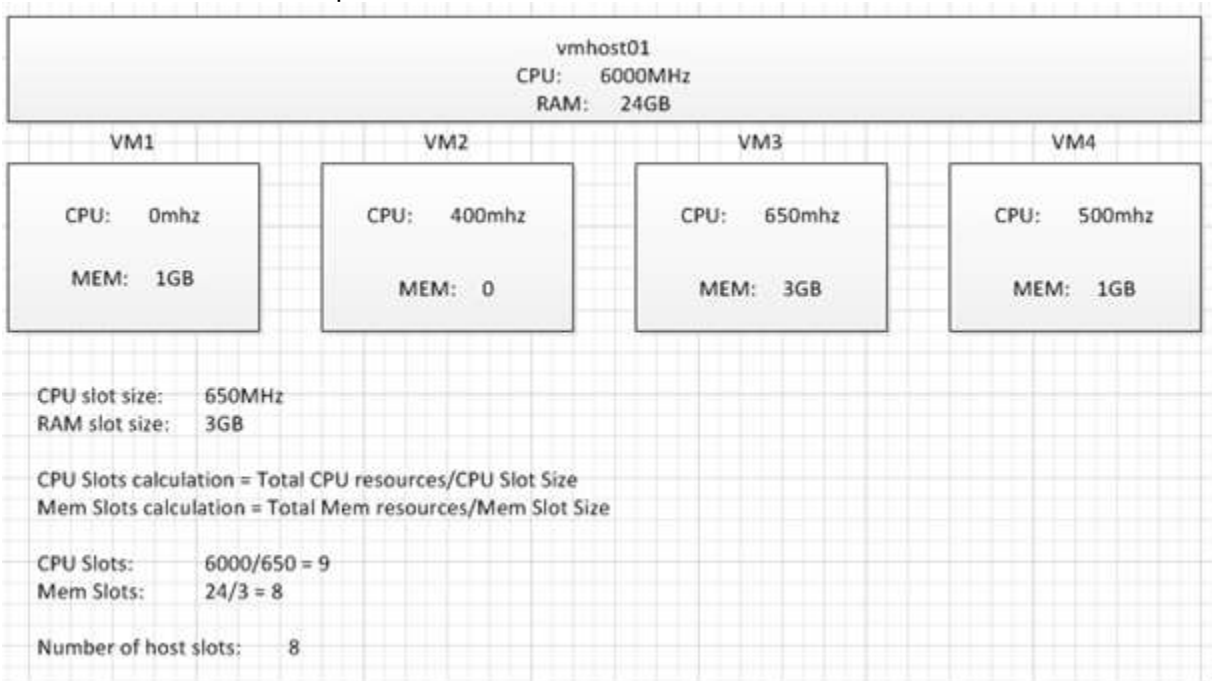
- this is best effort, if there aren't datastore connected to all hosts it will select a datastore that with the highest number of connected hosts
- When possible, VMFS datastores are chosen over NFS datastores
- When possible, the two datastores selected will be on different storage arrays
- Datastore heartbeating creates a file on the selected datastores for each host (**VMFS**) and the file remains in an up-to-date state as long as the host is connected to the datastore. If the host gets disconnected from the datastore, then the file for that host will no longer be up-to-date. (**NFS**) The host will write to the heartbeat file every 5 seconds
- If you so desire, you can manually select the datastores to be used for datastore heartbeating
  - Log into the vSphere client > right-click a cluster and select *Edit Settings...*
  - Under *vSphere HA* select *Datastore Heartbeating*
  - Choose the *Select only from my preferred datastores* radial button
  - Place a checkbox next to at least two datastores you want to use for datastore heartbeating



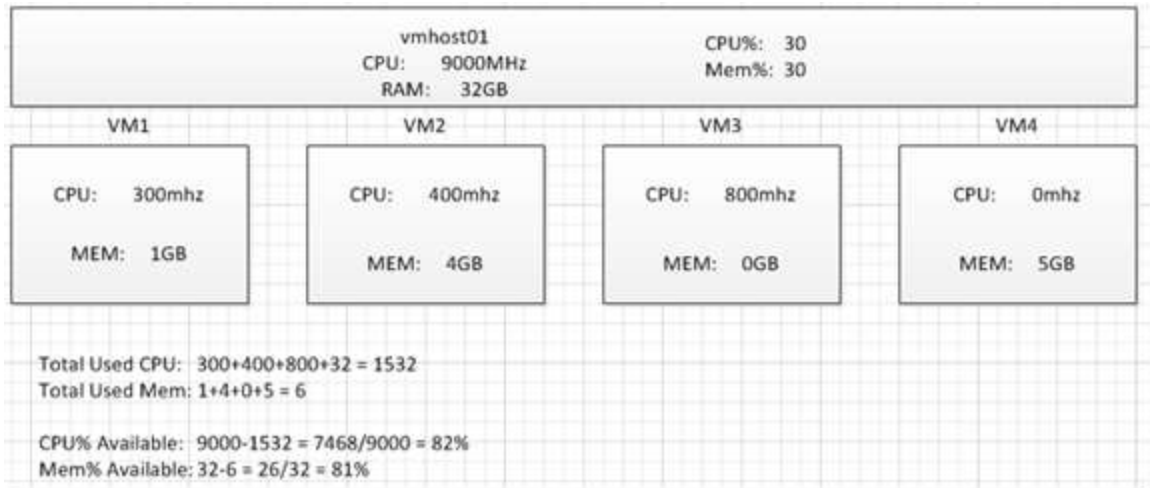
### Skills and Abilities

- **Calculate host failure requirements**
  - Earlier I covered how you can manually calculate host failover requirements depending on the admission control policy you're using, but I'll go over it again here
  - Host Failures Cluster Tolerates

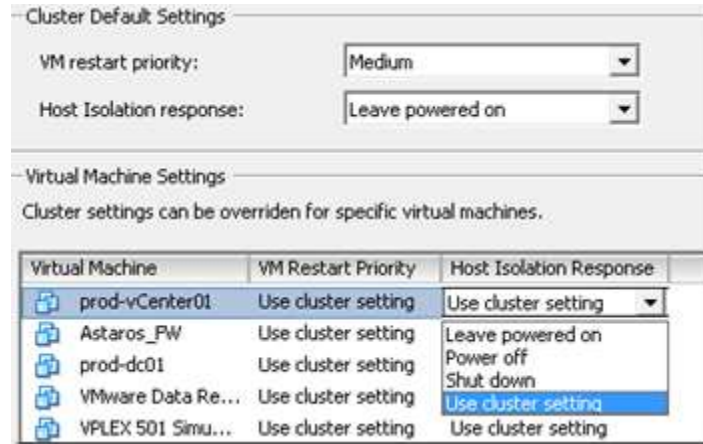
- This uses a logical object called a 'slot'. Depending on how many virtual machines are powered on, and what resources they are configured with, will determine the amount of slots are required for failover for any given host
- Once you determine the slot size for CPU and Memory you calculate the total number of slots for the host
  - CPU = Total CPU resources/CPU slot size
  - Mem = Total Mem resources/Mem slot size
- Here is an example of the slots calculation



- In the example above the host failover requirement could be up to 8 slots
- Percentage of Cluster Resources Reserved
  - You can configure separate percentages for CPU and memory.
  - If no CPU or memory reservations exist each VM will use 32MHz and 0 + overhead, respectively
  - Same scenario as before



- In this example the percentages for CPU and memory are both set to 30%. The current available percentage is 82% for CPU and 81% for memory. Operations such as powering on and migrating virtual machines will not have any issues as the available percentages are well above the user-defined 30%. Assuming other hosts have the same resource configuration you would need 18% CPU and 19% memory free on another host in order for all virtual machines to be successfully failed over
  - Specify failover hosts
    - There isn't much to calculate here, the specified hosts will stand idle unless a failover occurs
- **Configure customized isolation response settings**
  - You can set custom HA isolation responses for each individual virtual machine
    - Log into the vSphere client
    - Right-click on a cluster > click *Edit Settings...*
    - Under *vSphere HA* options click *Virtual Machine Options*
    - Here you can set the cluster default isolation response and the isolation response for individual virtual machines
    - Find the virtual machine you want to modify > choose an option under the *Host Isolation Response* column
      - *Leave Powered On*
      - *Power Off*
      - *Shut Down*
      - *Use cluster setting*



- There are a multitude of custom HA isolation response settings that you can configure on a HA cluster, These settings are configured at the cluster level, within the *vSphere HA > Advanced Options...*
  - **das.isolationaddress[#]** – by default the IP address used to check isolation is the default gateway of the host. You can add more IP addresses for the host to use during an isolation check. A total of 10 addresses can be used (0-9)
  - **das.usedefaultisolationaddress** – this option is either set to true or false. When set to false a host will NOT use the default gateway as an isolation address. This may be useful when the default gateway of your host is an unpingable address, or a virtual machine, such as a virtual firewall
  - **das.isolationShutdownTimeout** – use this option to specify the amount of time (in seconds) it will wait for a guest shutdown process that was initiating by invoking the isolation response, before HA will forcefully power off a virtual machine
- **Configure HA redundancy**
  - **Management Network**
    - Since HA uses the management network to send out network heartbeats, it is a good idea and best practice to make your management network redundant. There are two ways that you can accomplish this; use NIC teaming on the vSS or vDS where your management network resides or add an additional vmkernel port on a separate vSS or vDS and enable it for management
    - NIC Teaming
      - Add an additional NIC to the vSS or VDS that hosts the management network
        - Ideally this will be physically connected to a separate switch
      - Set the new NIC as a standby adapter

- If the active adapter fails, the standby will take over, thus allowing network heartbeats to be transmitted and received
- Add a new vmkernel port
  - Create a new vmkernel port on an existing or new vSS/vDS that currently is not being used for management
  - Enable the vmkernel port for management
  - Network heartbeats can now be sent/received on this new vSS/vDS which will allow network heartbeats to continue should your primary management network fail
- **Datastore Heartbeat**
  - The nature of datastore heartbeating is, by default, redundant. When HA is enabled it will select two datastores to use for datastore heartbeating. VMware states that two datastores are enough for all failure scenarios
  - If you have a need to configure more than two heartbeat datastores per host you can use this advanced setting
    - **das.heartbeatDsPerHost** – set this to the number heartbeat datastores you want to use
  - If possible, ensure you have two datastores that reside on two separate physical storage arrays
- **Network partitions**
  - A network partition is created when a host or a subset of hosts lose network communication with the master node, but can still communicate with each other. When this happens an election occurs and one of the hosts is elected as a master
  - The criteria for a network partition is
    - The host(s) cannot communicate with the master node using network heartbeats
    - The host(s) can communicate with the master using datastore heartbeats
    - The host(s) are receiving election traffic
  - I don't fully understand what network partitions has to do with "Configuring HA for redundancy", but I do know that network partitions are bad. Why are they bad?
    - vSphere can only connect to one master host, so if you have a subset of hosts in a network partition, they will not receive any configuration changes related to vSphere HA until the network partition is resolved
    - Hosts can only be added to the partitioned segment that communicates with vCenter

- When using FT, the primary and secondary VMs could end up being on a partition where the host is not responsible for the primary or secondary FT virtual machine. This scenario could prevent the secondary VM from restarting should the primary VM fail IF the primary VM lived on host that was not responsible for that VM
  - This is possible because a master host that has a lock on a datastore is responsible for all the VMs that live on that datastore. The master host of a network partition that the FT VMs are running on may not be the master that has a lock on that datastore, thereby it is not responsible for it from a HA perspective
- So I guess the lesson is, configure HA for redundancy in order to avoid network partitions
  - Ensure management network redundancy at the vmkernel layer, the hardware layer (think NICs on a separate bus) and the physical network layer
- **Configure HA related alarms and monitor an HA cluster**
  - There are seven default alarms that ship with vCenter related to HA
    - Insufficient vSphere HA failover resources
    - vSphere HA failover in progress
    - Cannot find a 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
  - There are plenty of additional alarms that you can create for clusters and virtual machines related to vSphere HA. Here are a list of available triggers for each
    - Clusters

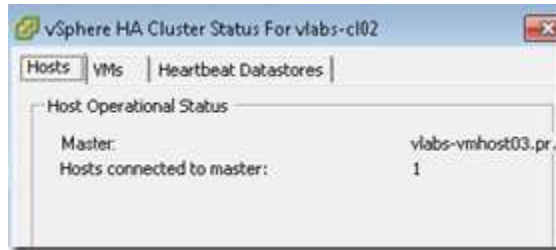
Event
Checked cluster for compliance
vCenter Server connected to a vSphere HA master agent
vCenter Server disconnected from a master vSphere HA agent
vCenter Server is unable to find a master vSphere HA agent
vSphere HA admission control disabled
vSphere HA admission control enabled
vSphere HA completed a failover action
vSphere HA detected an invalid master agent
vSphere HA disabled for cluster
vSphere HA enabled for cluster
vSphere HA failover resources are insufficient
vSphere HA failover resources are sufficient
vSphere HA host failed
vSphere HA host monitoring state changed
vSphere HA initiated a failover action
vSphere HA removed a datastore from preferred heartbeat datastores
vSphere HA VM monitoring state changed

- Virtual Machines

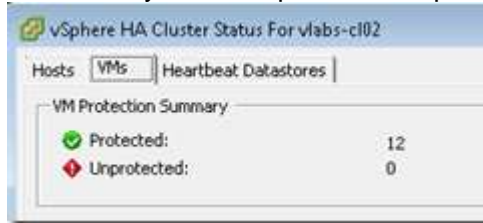
vSphere HA cannot reset VM
vSphere HA enabled VM reset with screenshot
vSphere HA failed to restart a network isolated virtual machine
vSphere HA failed to start a Fault Tolerance secondary VM.
vSphere HA is resetting VM
vSphere HA powered off VM on isolated host
vSphere HA reached maximum Secondary VM restart count.
vSphere HA restarted a virtual machine
vSphere HA shut down VM on isolated host
vSphere HA successfully started a Fault Tolerance secondary VM.
vSphere HA virtual machine failover unsuccessful
Virtual machine failed to become vSphere HA Protected
Virtual machine is not vSphere HA Protected
Virtual machine is vSphere HA protected
Not enough resources for vSphere HA to start VM

- o I'm not going to go over how to configure alarms as I did so in [Objective 1.2 – Manage Storage Capacity in a vSphere Environment](#).
- o Aside from the vSphere HA alarms you can monitor an HA cluster using the *Summary* tab of a given cluster. In the *vSphere HA* pane you can look at the *Cluster Status* and any *Configuration Issues* that may be related to HA
  - Log into the vSphere client > click a cluster from the inventory > select the *Summary* tab
  - Click the *Cluster Status* hyperlink located in the *vSphere HA* pane
  - There are three tabs in this dialog box
    - *Hosts*: allows you to see which host is the master and how many hosts are connected to the master

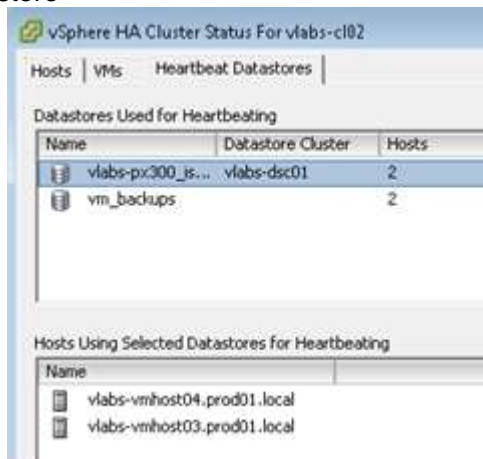




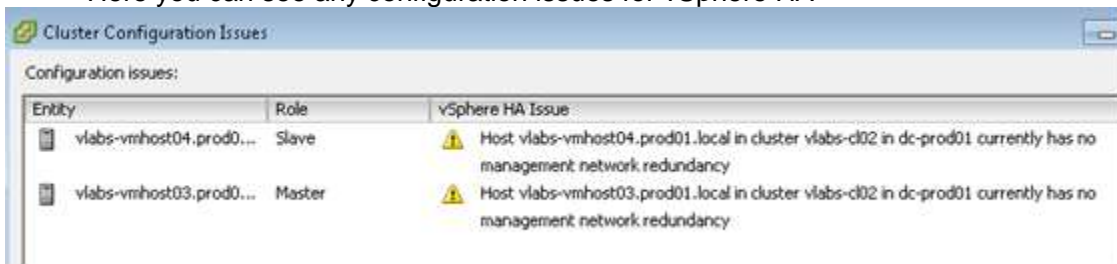
- *VMs*: shows you how many VMs are protected/unprotected



- *Heartbeat Datastores*: shows you which datastores are being used for datastore heartbeating. Clicking each datastore shows you which hosts are using that particular datastore



- Click on the *Configuration Issues* hyperlink
- Here you can see any configuration issues for vSphere HA

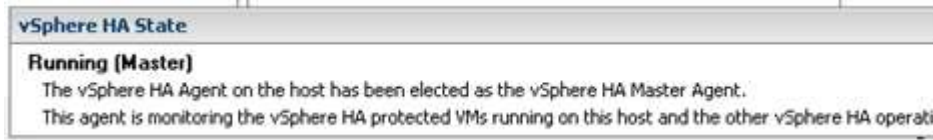


- As you can see in the example above, there is no management network redundancy for either host that is part of this HA cluster. Remember that having management network redundancy can be key in avoiding network partitions

- Looking at the summary tab of each host that is part of a HA cluster will show you the *vSphere HA State* for that host
  - Log into the vSphere client > select a host from the inventory > click the *Summary* tab



- Clicking on the small dialogue button will give you more information about the HA state

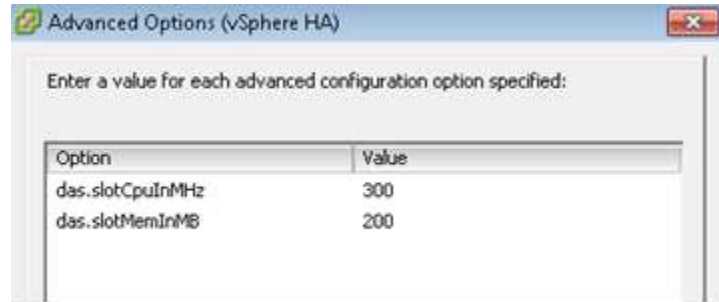


- When troubleshooting vSphere HA you can look at logs for a host that is giving you trouble. Here are some key logs and their locations
  - **fdm.log** – /etc/vmware
  - **hostd.log** – /etc/vmware

- **Create a custom slot size configuration**

- There are two advanced settings that you can configure in order to create a custom slot size; one for CPU and one for memory
  - **das.slotCpuInMHz**
  - **das.slotMemInMB**
- These two advanced settings allow you to specify the maximum slot size in your cluster
  - If a VM has reservations that exceed the maximum slot size then the VM will use multiple slots
- Customizing the slot size can have an unintended, and adverse effect during failover
  - You have a custom slot size of 1GB of memory. Let's say that nets you 20 slots for a host. If you have a virtual machine on that host with a 5GB memory reservation then 5 slots need to be available on that host in order for the VM to be powered on. Now, let's say across your cluster you have 15 free slots, but none of the hosts in the cluster have 5 free slots, then the VM with the 5GB memory reservation will not be able to power-on during a failover
- To set these advanced settings
  - Log into the vSphere client > right-click a cluster from the inventory > click *Edit Settings...*
  - Click *vSphere HA* > click the *Advanced Options...* button

- In the option column add a new option `das.slotCpuInMHz` > specify the maximum CPU slot size in the value column
- In the option column add a new option `das.slotMemInMB` > specify the maximum memory slot size in the value column



- Click *OK* when finished > click *OK* again to exit the cluster settings dialog
- **Understand interactions between DRS and HA**
    - vSphere DRS and vSphere HA can compliment each other when they are enabled on the same cluster. For example, after a HA failover DRS can help to load balance the cluster. Here are some other interactions
      - If DPM has put hosts in standby mode and HA admission control is disabled, this can cause insufficient resources to be available during a HA failover. When DRS is enabled it can work to bring those hosts out standby mode and allow HA to use them for failover
      - When entering maintenance mode DRS is used to evacuate virtual machines to other hosts. DRS is HA aware and will not migrate a virtual machine to a host, that in doing so, would violate HA admission control rules. When this happens you will have to manually migrate the virtual machine
      - If you are using required DRS VM-HOST affinity rules this may limit the ability to place VMs on certain hosts as HA will not violate required VM-HOST affinity rules
      - If you have a VM that needs to be powered on with enough available resources, but those resources are fragmented, HA will ask DRS to try and defragment those resources in order to allow the VM(s) to be powered on
  - **Analyze vSphere environment to determine appropriate HA admission control policy**
    - There are multiple factors to be considered when deciding which HA admission control policy should be chosen. Here are some things to consider
      - *Availability requirements* – across your cluster you need to determine what resources you have available for failover and how limiting you want to be with those available resources

- *Cluster configuration* – the size of your hosts, whether the hosts are sized the same or unbalanced with regards to total resources
- *Virtual Machine reservations* – if you are using virtual machine reservations you need to look at the largest reservation
- *Frequency of cluster configuration changes* – this refers to how often you are adding/removing hosts from your cluster
- All these things should be considered when choosing the HA admission control policy. Let's look at the different HA admission control policies and analyze them based on the factors listed above
  - *Specify Failover Hosts* – This policy is geared towards availability. If you HAVE to have available resources above all other factors to ensure HA failover and have the budget to let hosts stand idle then choose the Specify Failover Hosts admission control policy
    - Geared towards availability
    - Cluster configuration isn't an issue, specify the proper amount of failover hosts dependent upon your availability requirements
    - Virtual machine reservations don't matter at this point
    - Frequency of cluster configuration changes do play a small role here. If you are constantly adding new hosts to your cluster there may be a requirement to specify additional failover hosts to meet availability requirements
  - *Host Failures Cluster Tolerates*– This policy isn't as cut and dry as Specify Failover hosts. If you are worried about resource fragmentation, meaning you have enough resources spread across the hosts in the cluster, but not enough per host to meet availability requirements during a HA failover, then this policy is for you
    - Meets availability requirements by avoiding the resource fragmentation paradigm
    - Cluster configuration is a serious issue. If you have unbalanced hosts, meaning some hosts have more total resources than others, then this can lead to under utilized hosts. Using this policy the host with the highest amount of slots is NOT included in the slot size calculation, therefore limiting the amount of cluster slots. In other words, the number of powered on virtual machines that can be powered on
    - Virtual machine reservations is another serious issue. If you have some VMs with rather large CPU or memory reservations then the number of slots will be smaller. This leads to a conservative consolidation ratio and again, under utilized hosts

- You can use advanced settings to limit the size of the CPU and memory slots, but doing so directly undermines resource fragmentation avoidance and may not always meet availability requirements
- Frequency of cluster configuration changes can be an administrative overhead problem. If you have a 10 host cluster and specify the Host Failures Cluster Tolerates at 3 and then add 10 more hosts, the number of host failures that the cluster will tolerate is still 3. Therefore, if you are constantly adding hosts you will need to change the number of host failures appropriately to meet availability requirements
- *Percentage of Cluster Resources*– This policy is meant to be flexible and is the HA admission control policy recommended by VMware for most HA clusters. If you need flexibility and seamless scalability with regards to admission control then this is the policy you'll want to pick
  - This policy meets availability requirements based on CPU and memory percentages you define as needing to be available
  - Cluster configuration is a non-issue. Regardless of the size of your hosts, balanced or unbalanced, the percentages for CPU and memory that you define will stay the same. You will however need to do a bit more leg work upfront to calculate what percentages to define based on availability requirements. If your hosts are unbalanced it will take more time to do
  - Virtual machine reservations have no effect when using the Percentage of Cluster Resources admission control policy. Again, the user-defined percentages will remain the same regardless of virtual machine reservations
  - The frequency of cluster configuration changes have no impact when using this admission control policy. As you add or remove hosts the total number of cluster resources that need to be available will dynamically change based on resources being added or removed from the cluster
  - The big downside to using this admissions control policy is resource fragmentation. Just because your cluster meets the availability requirements based on the user-defined percentages does not mean that those available resources aren't fragmented across all the hosts in the cluster. As discussed earlier, if DRS is also enabled and resources are fragmented during a failover event, HA will ask DRS for best effort to

try and defragment the cluster in order to facilitate the best outcome of said failover event

- Again, VMware recommends using the Percentage of Cluster Resources admission control policy for most environments. Should you find this policy does not meet some of your business requirements, evaluate the other two policies based on the factors detailed above to determine the proper course of action
- **Analyze performance metrics to calculate host failure requirements**
  - Regardless of the HA admission control policy you choose you need to determine what your host failure requirements are. In order to do this you will need to look at the performance metrics of your virtual machines that will be part of the HA cluster
  - To look at the performance metrics of a virtual machine you can use the vSphere client performance tab to look at advanced metrics, such as CPU and memory utilization, and you can do so over a specified period of time
  - You can also use **esxtop/resxtop** to view performance metrics for virtual machines. I will not go into how to use these tools as they are well documented on other places
    - [Interpreting esxtop Statistics](#)
    - [Duncan Epping's ESXTOP deep dive](#)
  - You should look at the virtual machines performance over a period of time to determine the average utilization. You should also look at the hosts performance over a period of time to determine its resource consumption and resource availability
    - Determining the host's resource availability should give you a better handle on determining your available cluster resources compared to the average virtual machine resource consumption. When you compare those two metrics you can further determine what percentage of resources you need to always keep available in order to satisfy a HA failover. This really adds value when using the Percentage of Cluster Resource admission control policy
  - A big factor that must be considered are the size of your virtual machine reservations. HA will not power on a virtual machine if it violates the admission control policy. HA will also not power on a virtual machine if it can't meet the reservation. Now, this doesn't relate directly to performance metrics, I feel it is an important factor to consider when calculating host failure requirements
- **Analyze HA cluster capacity to determine optimum cluster size**

- Trying to right-size a HA cluster can be challenging, especially in a fluid environment. Above all it will come down to availability requirements
  - What VMs do you need available even when a failover occurs
    - What is their resource utilization
  - How many hosts are currently in your cluster
    - Does this meet your availability requirements
    - How does your availability requirements match-up in terms of scaling up within the cluster based on the number of hosts in the cluster. A better way of asking the question; how many more VMs can with my current cluster resources while still maintaining required resource availability
  - What is your current cluster utilization and availability and how does that matchup against availability requirements
  - What admission control policy are you using
- These are very basic questions, but answering each of them and taking into consideration your calculated host failure requirements should enable you to determine if you have right-sized your cluster, or if configuration changes need to be made to meet availability, and ultimately, business requirements

#### Tools

- [vSphere Availability Guide](#)
- [Product Documentation](#)
- vSphere Client

# VCAP5-DCA Objective 4.2-Deploy and Test VMware FT

---

For this objective I used the following documents:

- Documents listed in the Tools section

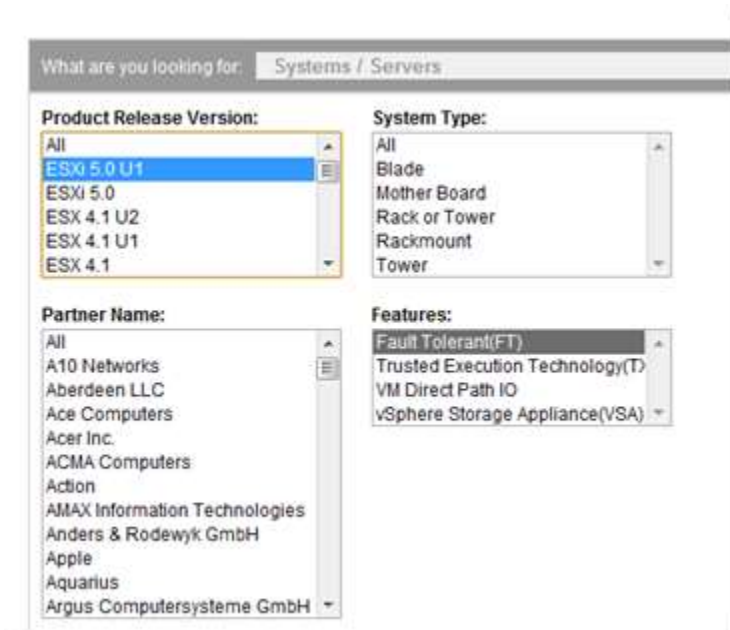
## ***Objective 4.2 – Deploy and Test VMware FT***

### Knowledge

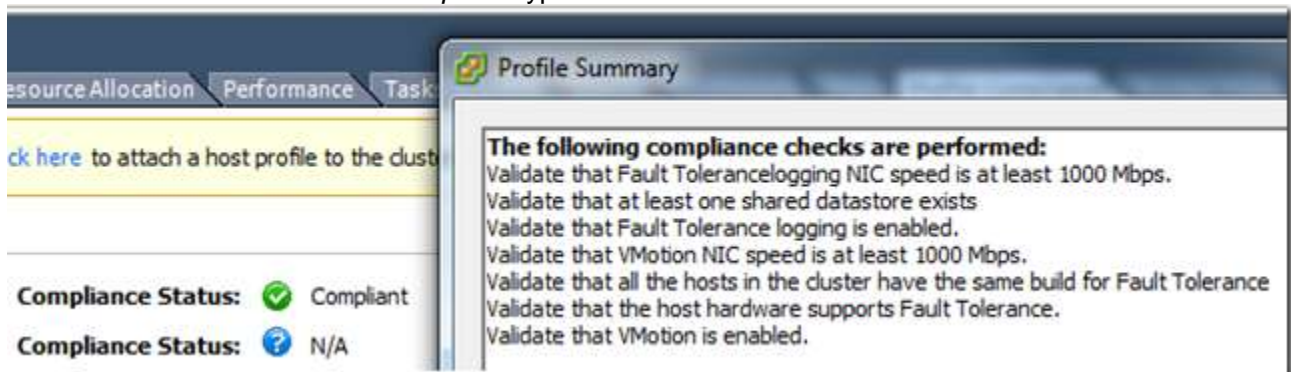
**\*\*ITEMS IN BOLD ARE TOPICS PULLED FROM THE BLUEPRINT\*\***

- **Identify VMware FT Hardware Requirements**
  - There are some pretty strict hardware requirements when it comes to VMware Fault Tolerance (FT). Only certain processors are compatible with VMware's vLockstep technology. What this means is the vLockstep technology requires certain extensions on the physical processor in order for it to work. VMware provides a nice utility called [VMware SiteSurvey](#) which will generate a report showing you your host's hardware compatibility with VMware technology, including Fault Tolerance (you need to have the vSphere client installed on the system you are loading SiteSurvey on)
  - There are too many processor combinations to list out here, but running SiteSurvey will tell you if your processors are compatible. Check out the [help page](#) for SiteSurvey which includes a list of FT capable processors
  - Here is a list of other hardware requirements
    - Both hosts that are hosting the FT virtual machines must have processors in the same family and be within +/- 400MHz of each other
    - The hosts must also be certified for FT use. Check out the [VMware Compatibility Guide](#) to ensure your hosts are supported
      - Open the VMware Compatibility Guide in a web browser
      - Choose the version of vSphere you are using
      - In the *Features* list box choose *Fault Tolerant(FT)*
      - Click *Update and View Results*

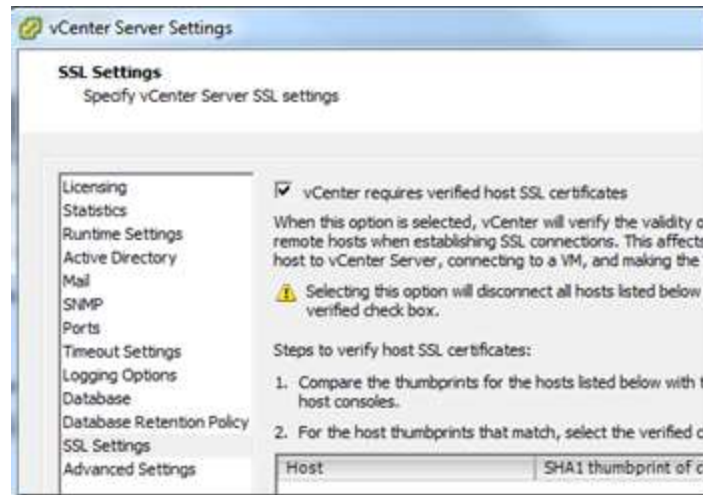




- Just searching on these two items will return a lot of results. Feel free to narrow down the search by selecting additional criteria
- The host(s) must support *Hardware Virtualization* and it must be enabled in the BIOS
- If your hosts are part of a vSphere cluster you can check the *Profile Compliance* tab to determine if they are compatible with FT
  - Log into the vSphere client
  - From the inventory select the cluster which contains that hosts you are checking FT compatibility on
  - Select the *Profile Compliance* tab on the right
  - Click the *Check Compliance Now* hyperlink
  - Check the *Compliance Status* to see whether it is compliant or not
    - Click the *Description* hyperlink to view the details



- As you can see from the screenshot above, my hosts meet the physical hardware requirements and compatibility requirements (which is covered in the next section) for FT. The *Profile Summary* is just a list of what items are checked, it does not indicate which checks have passed or failed
- **Identify VMware FT compatibility requirements**
  - There are a slew of compatibility requirements on your cluster and virtual machines for FT; lets start with the cluster requirements
  - Cluster Requirements
    - Both hosts participating in FT must have access to the same datastores that the FT virtual machine resides on
    - Host certificate checking must be enabled
      - Log into the vSphere client
      - Click the *Administration* menu > select *vCenter Server Settings...*
      - Click *SSL Settings* > ensure that the *vCenter required verified host SSL certificates* checkbox is checked



- FT logging and vMotion networks must be configured
    - The hosts must be part of a HA enabled cluster
  - Virtual Machine Requirements
    - Virtual machine files must be on storage that both hosts have access to
    - The FT virtual machine cannot have more than 1 vCPU
    - Ensure the virtual machine is running a supported guest operating system
      - see [VMware KB1008027](https://kb.vmware.com/s/article/1008027) for a list of supported guest operating systems
  - vSphere Compatibility Requirements
    - Virtual machines that are provisioned as a linked clone are not supported for FT

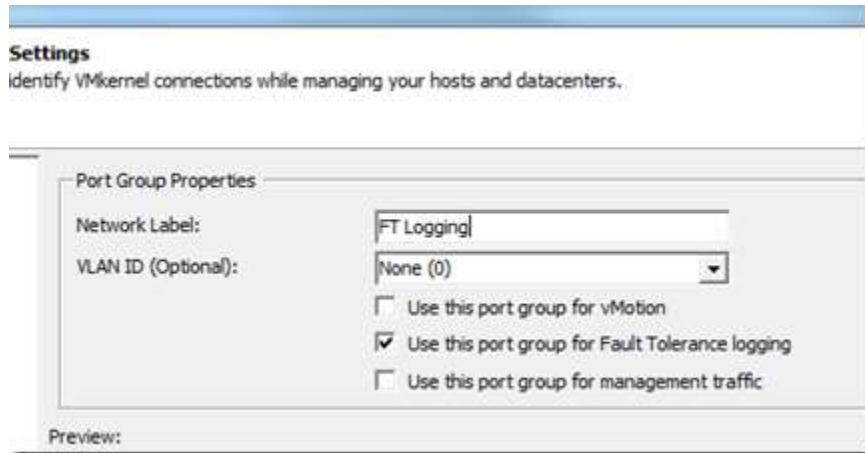
- Storage vMotion is not supported on FT virtual machines
  - Disable FT if you want to perform a storage vMotion and then re-enable
- If you are using an application that leverages VADP (API for data protection) to backup your virtual machines then you won't be able to enable FT on it
- You cannot snapshot a FT virtual machine
- Incompatible Features and Devices (list taken straight from the Availability Guide)
  - You can't use SMP, only 1 vCPU for a FT virtual machine
  - The FT virtual machine cannot have a physical raw device mapping
  - Virtual CD-ROM/floppy drives cannot be backed by a physical or remote device
  - Paravirtualization is not supported on FT virtual machines
  - USB and sound devices
  - NPIV is not supported
  - NIC passthrough or the use of the vance networking drivers
  - Thin-provisioned virtual disks
    - When enabling FT, thin-provisioned disks will try to be expanded automatically. However, the virtual machine must be powered off
  - Hot-pluggable devices are not supported
  - Extended Page Tables/Rapid Virtualization Indexing is disabled
  - Serial or parallel ports
  - IPv6 is not supported with the FT logging, so use IPv4
  - Video devices that have 3D enabled are not supported for FT

### Abilities

- **Modify VM and ESXi host settings to allow for FT compatibility**
  - As discussed earlier there are strict requirements that must be followed in order to run FT in your environment. Those requirements are for hosts and virtual machines (most if not all of this section I just covered in the preceding section, if you think something else should be a part of this section that I have not listed, please feel free to leave a comment)
  - Host Settings
    - Configure the proper networking on each host. You will need at least two physical 1Gb NICs. Configure one vSwitch or port group with on physical NIC for vMotion and create another vSwitch or port group with the other physical NIC for FT logging (more detail on how to configure FT logging is below)
    - Ensure that the hosts you are using for FT are at the same vSphere build

- Configure shared storage for the hosts. The hosts that will be hosting the FT VMs need to have access to the storage in which the FT virtual machine's files are located
  - Ensure that all of the requirements listed in the preceding section **Identify VMware FT compatibility requirements** have been met
- Virtual Machine Settings
  - No snapshots
  - Only 1 vCPU
  - No physical raw device mappings
  - Refer to the list in the preceding section, **Identify VMware FT compatibility requirements**, for all the of the virtual machine restrictions
- **Use VMware best practices to prepare a vSphere environment for FT**
  - Here are a list of some good best practices to use when preparing to implement FT
    - Your hosts should run +/- 400MHz as it relates to CPU frequency
    - Ensure your hosts are running the same CPU instruction sets. These setting are typically enabled/disabled in the systems BIOS
    - Use 10Gb NICs and enable jumbo frames for FT logging
    - Store any required ISO files on a datastore that both hosts have access to
  - Avoid Network Partitions
    - I discussed this in the first part of this objective. If you have a network partition and the master that owns the primary FT VM does not own the secondary FT VM then the secondary will not start if the primary fails
  - Best practices for performing host upgrades
    - Since FT requires that the FT virtual machines run on hosts with the same version and build, you'll need a methodical way of performing upgrades to those hosts
      - vMotion the primary and secondary FT virtual machines off of the two hosts that you will be upgrading
      - Upgrade both hosts
      - On the primary VM, turn off FT
      - vMotion the primary VM (which currently has FT disabled) to one of the new upgraded hosts
      - Turn FT back on
  - There are some other FT configuration recommendations that, in most cases, should be followed

- No more than four FT virtual machines on a single ESXi host. Total should include both primary and secondary VMs
- Allocate excess memory to the resource pool that contains the FT virtual machines. This allows for overhead memory
  - A reservation is automatically set to the configured memory amount when you enable FT. The excess memory will allow for overhead should the FT VM utilize the the configured amount of memory
- Do not use more than 16 virtual disks per FT virtual machine
- Have at least three hosts in a cluster (the third host should meet the same requirements for FT and match the physical and logical configurations of the other two hosts). This allows for n+1 should a host fail, another one in the cluster will be there to allow for the creation of a secondary FT virtual machine
- When using NFS, have at least one 1Gb NIC on the NAS hardware side
- **Configure FT logging**
  - Configuring FT logging is a pretty easier process. You'll need to do this on each host:
    - Log into the vSphere client
    - Select a host from the inventory that you will be using for FT > click the *Configuration* tab
    - Click the *Networking* hyperlink
      - If you don't have a vSwitch with a dedicated physical NIC for FT logging, create one now
    - Click the *Properties* hyperlink for the vSwitch you will be using for FT logging
    - Click the *Add* button > select *VMkernel* > click *Next*
    - Enter in a *Network Label* such as FT Logging
    - Choose a VLAN if necessary
    - Check the *Use this port group for Fault Tolerance logging* > click *Next*



- Enter in the *IP Address* and *Subnet Mask* (this should be on a different subnet than your vMotion VMkernel port group) > click *Next*
- Click *Finish* > click *Close* to close the vSwitch Properties dialog box
- **Prepare the infrastructure for FT compliance**
  - If you have followed all of the guidance and configuration in the preceding sections then your infrastructure should be ready for FT. Here are a few ways that you can check to make sure you're FT compliant
    - Use Profile Compliance on whichever cluster you will be using for FT (the cluster needs to be enabled for HA for this to work)
      - Log into the vSphere client > select a cluster object from the inventory
      - Click on the *Profile Compliance* tab
      - Click the *Check Compliance Now* hyperlink
      - Ensure the *Compliance Status* is marked as *Compliant*

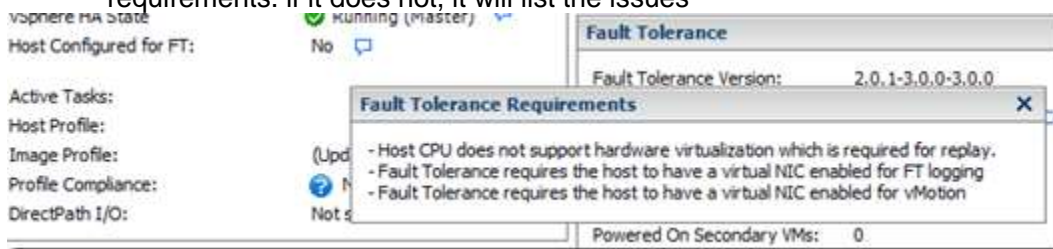


- The above screenshot is what you don't want to see
- Here you can see which host(s) are not compliant

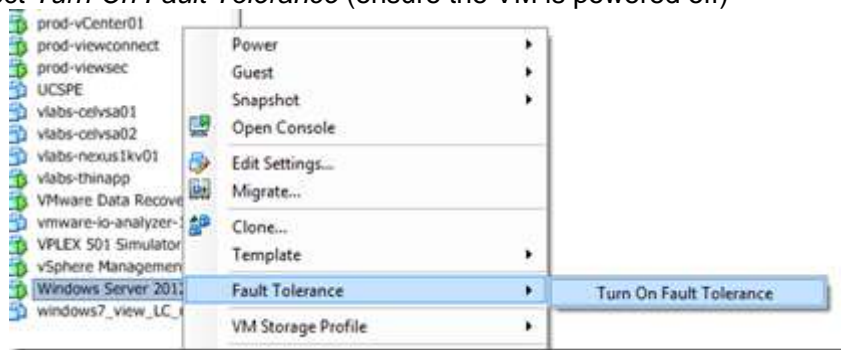
Select an entity below to view its compliance failures

Host Name	Cluster Requirements Compliance
vlabs-vmhost01.prod01Jo...	✖ Noncompliant
vlabs-vmhost02.prod01Jo...	✖ Noncompliant

- Profile Compliance will show you whether you are compliant or not for HA, but if you're not, it doesn't tell you which requirements haven't been met. To do so you need to look at the *Summary* tab for each host
  - Log into the vSphere client > select a host object from the inventory
  - Click the *Summary* tab
  - In the *General* pane you will see *Host Configured for FT:* and it will say either *Yes* or *No* and it has a small dialog icon next to it
  - Click the dialog icon. This will show you if the host does or does not meet FT requirements. if it does not, it will list the issues



- As you can see, the host I used for this screenshot is not configured for FT and has hardware and software configurations that must be changed in order for it to meet FT requirements
- **Test FT failover, secondary restart, and application fault tolerance in a FT Virtual Machine**
  - Before we can test FT failover we need to enable FT on a virtual machine. This process is easy once you've meet all of the requirements that have been discussed earlier in this post
  - Turn on Fault Tolerance
    - Log into the vSphere client
    - Navigate to the *Hosts and Clusters* view
    - Right-click on the virtual machine that you want to enable FT on > click *Fault Tolerance* > select *Turn On Fault Tolerance* (ensure the VM is powered off)



- Once you do this you will see a warning about a few operations that will occur once you turn FT on

- Thin-provisioned disks will be zeroed out and made thick
  - This can take quite some time depending on the amount of free space that needs to be zeroed
- DRS automation for the VM will be set to disabled
- clear
- 
- 
- A memory reservation is created; the reservation size is equal to the configured amount of memory



- Click Yes to continue
- Once complete the icon for the virtual machine will be blue
- Right-click the VM and select *Power* > click *Power On*
- Once it is powered on click on the VM itself in the inventory > on the right pane select the *Summary* tab
- In the *Fault Tolerance* pane ensure that the *Fault Tolerance Status* shows as *Protected*



- Test FT Failover
  - Log into the vSphere client
  - Right-click on the FT protected VM > select *Fault Tolerance*
  - Click *Test Failover*
- The task itself only takes a second to show completed in the *Recent Tasks* pane, but there is a lot more that still has to happen before the failover test is complete



- You'll notice during the failover test that the *Fault Tolerance Status* goes from *Protected* to *Not protected* and that it is *Starting*



- It will then go into a *Not protected* state and it will show *Need Secondary VM*
- At this point in the test, the primary has failed and the secondary has now completely taken over as the primary. In order for FT to be fully operational it now needs a new secondary



- You will see the status change again from *Not protected, Need Secondary VM* to *Not protected, Starting*
- Eventually the *Fault Tolerance Status* will show as *Protected* meaning a new secondary VM has been created and FT logging is now occurring between the new primary and secondary
- Test Secondary Restart
  - Log into the vSphere client
  - Right-click on the FT protected VM > select *Fault Tolerance*
  - Click *Test Restart Secondary*
- Like you saw previously the *Fault Tolerance Status* will go from *Protected* to *Not protected, Starting* while the secondary FT VM restarts. Once the restart is complete the *Fault Tolerance Status* will once again show *Protected*
- Unfortunately I don't have a way to show testing of application FT. I'm not 100% sure if that is referring to application monitoring or merely testing an application running in a FT VM while it is failing over or the secondary is restarting. If it is the latter, it is simple enough to monitor and see if you stay connected to that particular application, such as Microsoft Exchange
- There is a good VMware KB ([KB1020058](https://kb1020058.vmware.com)) that covers how to test a FT configuration. It also goes over different scenarios and what behavior to expect from FT. There are certain situations where a FT VM can become unavailable and the secondary will not take over (such as loss of network connectivity to the primary VM).

# VCAP-DCA 5 Objective 5.1–Implement and Maintain Host Profiles

## Objective 5.1 – Implement and Maintain Host Profiles

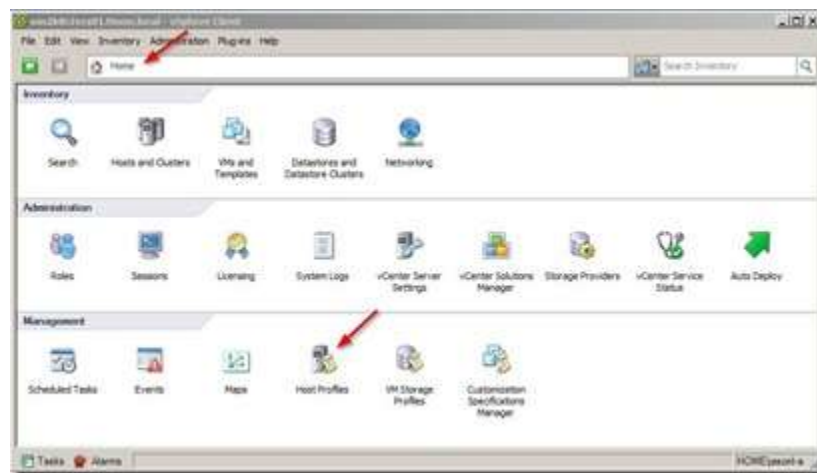
For this objective I used the following documentation:

- vSphere Host Profiles documentation
- VMware vNetwork Distributed Switch: Migration and Configuration white paper

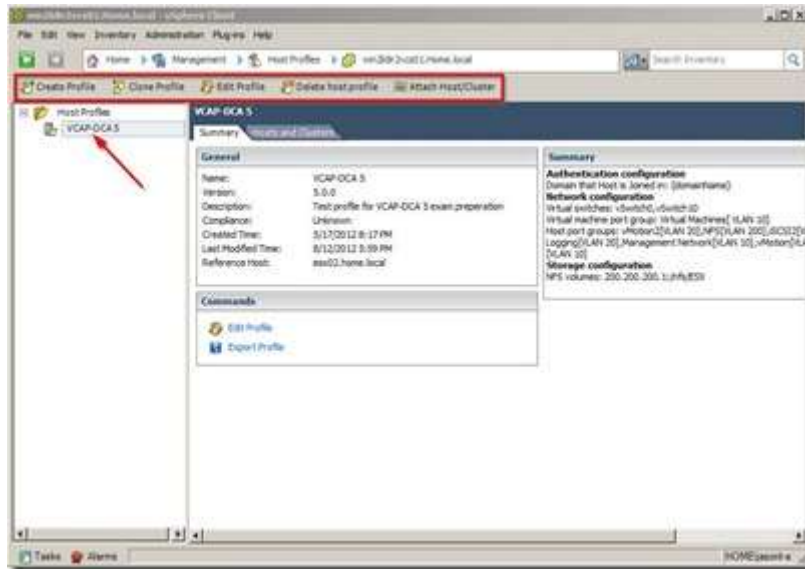
### Skills and Abilities

#### Use Profile Editor to edit and/or disable policies

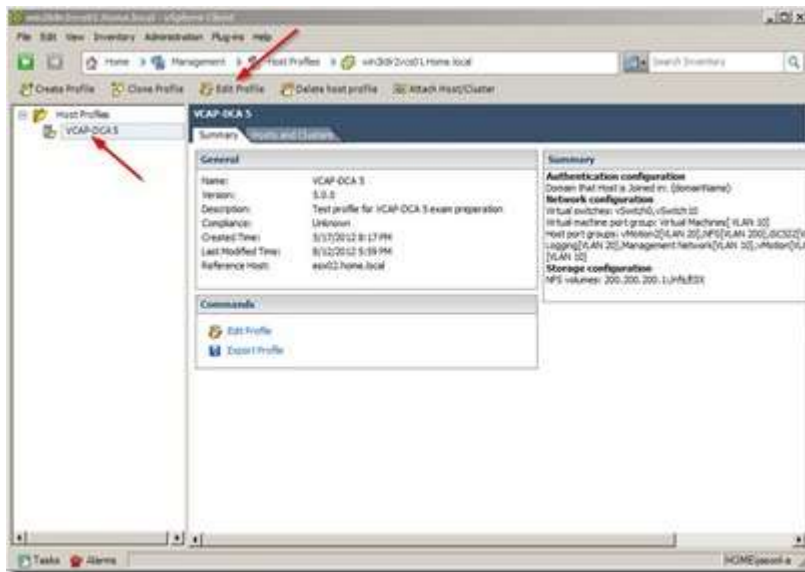
To access/manage Host Profiles from the “Home” menu screen select “Host Profiles” under the “Management” section:



If you have any existing host profiles they will be listed in the left side navigation window. In the example below the “VCAP–DCA 5” profile listed. When selecting the profile the menu options become available to Clone Profile, Edit Profile, Delete host profile, and Attach Host/Cluster. If no profile is listed your only option will be to Create Profile:

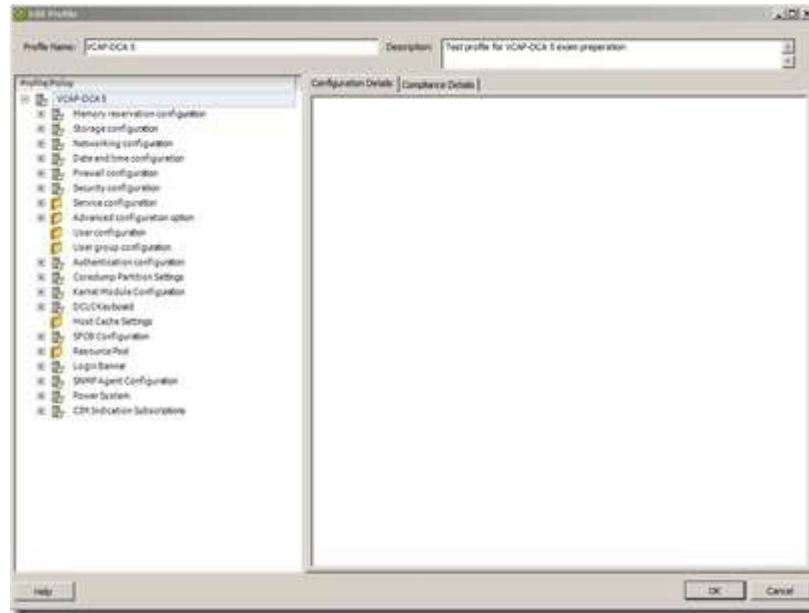


To edit a profile a select the profile and click “Edit Profile” from the menu:



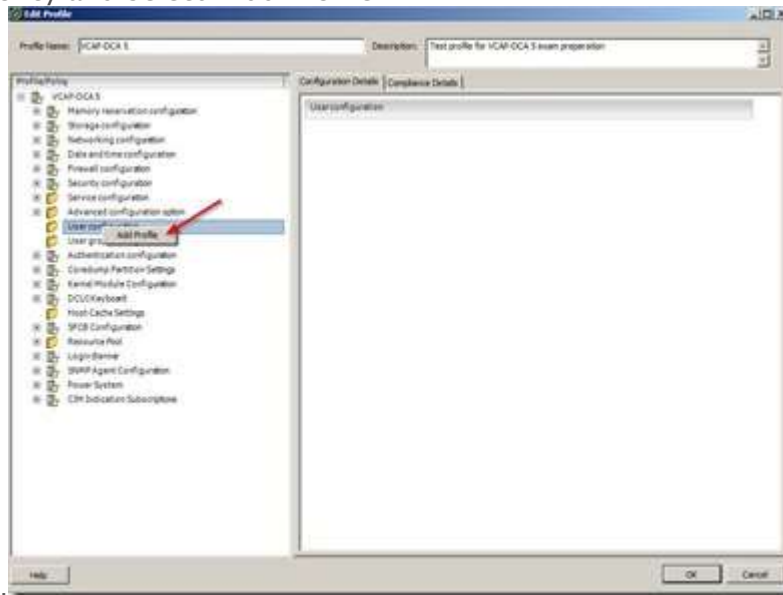
The “Edit Profile” screen will be displayed similar to the screenshot below. Each host profile is composed of several sub-profiles that are designated by functional group to represent configuration instances. Each sub-profile contains many policies and compliance checks that describe the configuration that is relevant to the profile.

Each policy consists of one or more options that contains one or more parameters. The parameters consist of a key and a value. The value can be one of a few basic types, for example integer, string, string array or integer array.

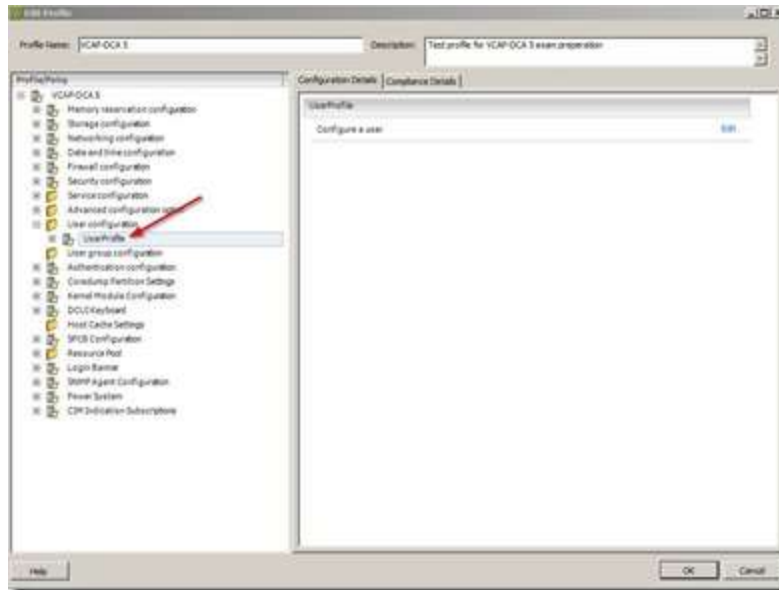


### Create sub-profiles

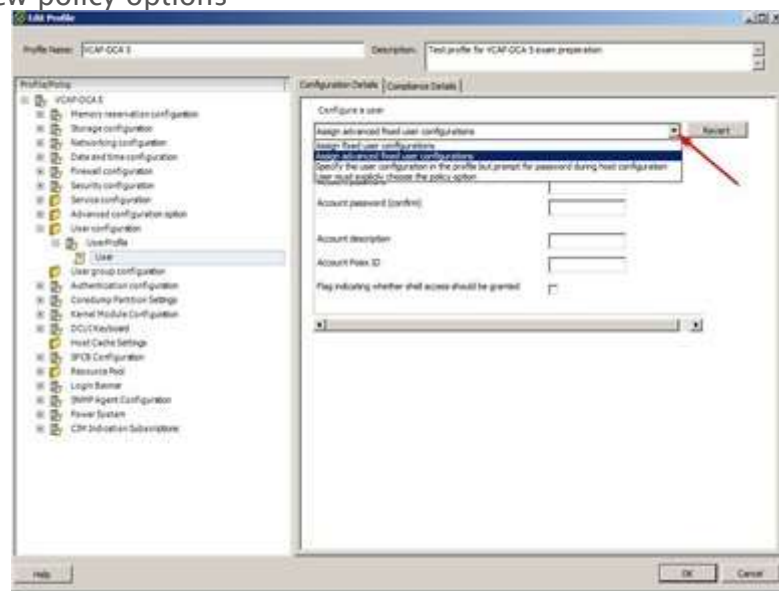
- Open the Profile Editor for the profile you wish to edit (as outlined above)
- On the left side of the Profile Editor, expand a sub-profile until you reach the policy you want to edit (noted with a “folder” icon)
- Right click the policy and select “Add Profile



- A new profile will be created under the given target



- Expand the new policy till you receive the “Configuration Details” tab in the right pane
- Configure the new policy options



- Click OK save and close the Host Profile

### Use Host Profiles to deploy vDS

Prior to deploying the host profile the target host must be in Maintenance Mode. The overview of deploying the vDS is as follows:

- Create vDS (without any associated hosts)
- Create Distributed Virtual Port Groups on vDS to match existing or required environment
- Add host to vDS and migrate vmins to dvUplinks and Virtual Ports DV Port Groups
- Delete Standard Switch from host

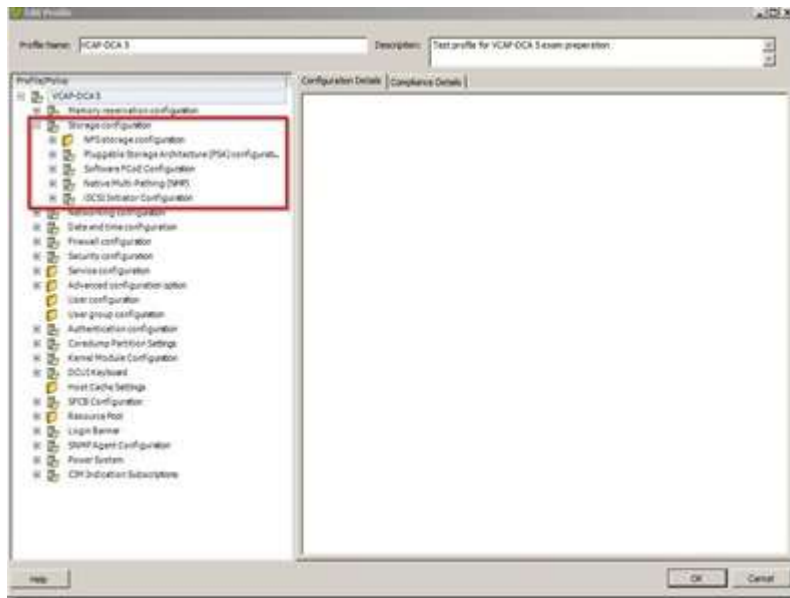
- Create Host Profile of Reference Host
- Attach and apply host profile to candidate hosts
- Migrate VM networking for VMs and take hosts out of Maintenance Mode

For a more detailed description of the above steps read pages 24 thru 28 of the *VMware vNetwork Distributed Switch: Migration and Configuration* white paper.

### Use Host Profiles to deploy vStorage Policies

This is a tricky section as I am not exactly sure what VMware means by a “vStorage Policy”. I am taking a guess and if I am wrong please let me know in the comments section below.

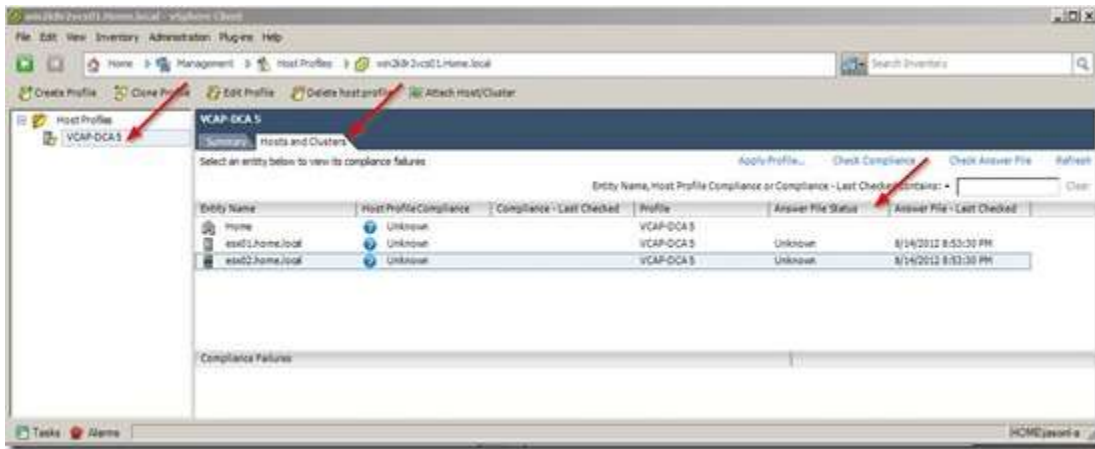
With that said, I believe VMware is talking about the “Storage configuration” node within the Host Profile:



Under this node there are several sub-categories covering everything from configuring the iSCSI initiator for a host to setting up the desired Path Selection Policy (PSP) and Storage Array Type Plugin (SATP). I would suggest creating a test policy and playing with these settings to get a feel for what they do and how they work.

### Manage Answer Files

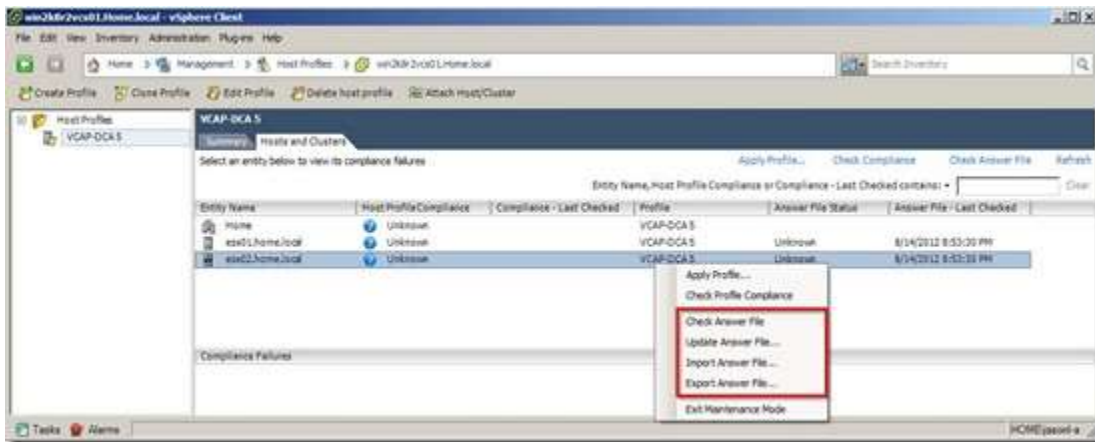
Answer files are used for ESXi hosts that are provisioned using VMware Auto Deploy, which is a new feature in vSphere 5. An answer file contains the ‘answers’ to settings in the Host Profile. For example what value to set the root password to. You access the answer file from the by select the Host Profile and then click on the “Hosts and Clusters” tab:



From the screenshot above you can see that answer file for each of my hosts is marked as “Unknown”. The other two status options are “Incomplete” and “Complete”. Each is defined as follows:

- Incomplete – The answer file is missing some of the required user input answers
- Complete – The answer file has all of the user input answers needed
- The host and associated profile exist but the status of the answer file is not known. This is the initial state of an answer file.

If you right click on the “Answer File Status” several options are available to work with for that hosts answer file:



- Check Answer File – This confirms the status of the answer file. See descriptions above
- Update Answer File – Allows you to enter or update the user input values for the host profile
- Import Answer File – Allows you to import and exported answer file
- Export Answer File – Allows you to export an answer file to be used with another host profile

# VCAP-DCA 5 Objective 5.2 – Deploy and Manage Complex Update Manager Environments

## Objective 5.2 – Deploy and Manage Complex Update Manager Environments

For this objective I used the following resources:

- Installing and Administering VMware vSphere Update Manager
- Reconfiguring VMware vSphere Update Manger
- VMware KB Article 1012382 “TCP and UDP Ports required to access vCenter Server, ESX/ESXi hosts, and other network components”
- VMware KB Article 1004543 “VMware Update Manager network port requirements”

### Knowledge

#### Identify Firewall Access Rules for Update Manager

Port	Source	Target	Purpose
80	Update Manager Server	VMware.com & xml.shavlik.com	To obtain metadata for the updates, Update Manager must be able to connect to the target sites
80	ESXi Host	Update Manager Server	ESXi Host to Update Manager Server. The reverse proxy forwards the required to port 9084
443	Update Manager Server	VMware.com & xml.shavlik.com	To obtain metadata for the updates, Update Manager must be able to connect to the target sites
443	ESXi Host	Update Manager Server	ESXi Host to Update Manager Server. The reverse proxy forwards the required to port 9084
443	vCenter Server	Update Manager Server	vCenter Server to Update Manager Server. The reverse proxy forwards the request to port 8084
902	Update Manager Server	ESXi Host	To push patches and updates from Update Manager to the ESX/ESXi Hosts to be updated
1433	Update Manager Server	Microsoft SQL Server	Update Manager to Microsoft SQL Server connectivity (for UM Database)
1521	Update Manager Server	Oracle Database Server	Update Manager to Oracle connectivity (for UM Database)



8084	Update Manager Server	vCenter Server	SOAP between components of Update Manger Server and the vCenter Update Manager client plug-in. Configurable at install
9084	Update Manager Server	ESXi Host	ESX/ESXi hosts connect to the VUM webservice listening for updates. Configurable at install
9087	Update Manager Server	vCenter Server	Port used for uploading host update files. Configurable at install
9000-9100	ESXi Host	Update Manager Server	This is the recommend port range from which to choose ports for Update Manager if ports 80 and 443 are already in use. Update Manager automatically opens these ports for ESX Host scanning and remediation

Network port information provided by VMware KB Article [1004543](#) and VMware KB Article [1012382](#).

### Skills and Abilities

#### **Install and Configure Update Manager Download Service**

In certain network environments your vCenter Server and Update Manager server may not have access to the internet directly or may have connectivity to a host who does. In these instances the use of Update Manager Download Service (UMDS) to download the patch binaries can be used.

- UMDS Prerequisites
  - Ensure that the machine on which you install UMDS has Internet access
  - Uninstall prior versions of UMDS if installed
  - Update Manager DB needs to be configured and a ODBC connection configured on the host
  - UMDS and Update Manager must be installed on different machines
- Installing UMDS
  - Insert the VMware vCenter Update Manager installation DVD in the DVD drive
  - Browse to the “umds” folder on the DVD and run “VMware-UMDS.exe”
  - Select the language for the installation and click OK
  - Review the Welcome page and click Next
  - Read the patent agreement and click Next
  - Accept the terms in the license agreement and click Next

- Select the database options and click Next
- Enter the Update Manager Download Service proxy settings and click Next
- Select the Update Manager Download Service installation and patch download directories and click Next
- Click Install to begin the installation
- Click Finish when complete
- Configuration Commands
- To download ESX/ESXi host updates and virtual appliance updates:  
*vmware-umds -S -enable-host -enable-va*
- To download ESX/ESXi host updates and disable virtual appliance updates:  
*vmware-umds -S -enable-host -disable-va*
- To download only ESXi 5.x patches  
*vmware-umds -S -disable-host*
- vmware-umds -S -e embeddedEsx-5.0.0*

### Configure a Shared Repository

You must create the shared repository using the UMDS and host it on a web server or a local disk. The UMDS you use must be of a version compatible with Update Manager. Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click Update Manager under Solutions and Applications on the Home page. Follow the below steps:

- On the Configuration tab, under Settings, click Patch Download Settings
- In the Patch Download Sources pane, select Use a shared repository
- Enter the path or the URL to the shared repository  
*NOTE - You cannot use folders located on a network drive as a shared repository. Update Manager does not download patch binaries, patch metadata, and notifications from folders on a network share*
- Click Validate URL to validate the path. Make sure that the validation is successful, if the validation fails Update Manager reports a reason for the failure. You can use the path to the shared repository only when the validation is successful
- Click Apply
- Click Download Now to run the VMware vCenter Update Manager Update Download task and to download the patches and notifications immediately

## Configure Smart Rebooting

Smart rebooting selectively restarts the virtual appliances and virtual machines in the vApp to maintain startup dependencies. You can enable and disable smart rebooting of virtual appliances and virtual machines in a vApp after remediation. Smart rebooting is enabled by default. If you disable smart rebooting, the virtual appliances and virtual machines are restarted according to their individual remediation requirements, disregarding existing startup dependencies.

Procedure:

- Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under **Solutions and Applications** on the Home Page
- On the **Configuration** tab, under **Settings**, click **vApp Settings**
- Deselect **Enable smart reboot after remediation** to disable smart rebooting

## Manually Download Updates to a Repository

Instead of using a shared repository or the Internet as a patch download source, you can import patches and extensions manually by using an offline bundle. You can import offline bundles only for hosts that are running ESX/ESXi 4.0 or later.

Prerequisites

- The patches and extensions you import must be in ZIP format
- To import patches and extensions, you must have the **Upload File** privilege

Procedure

- Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under **Solutions and Applications** on the Home Page
- On the **Configuration** tab, under **Settings**, click **Patch Download Settings**
- Click **Import Patches** at the bottom of the **Patch Download Sources** pane
- On the **Select Patches** page of the **Import Patches** wizard, browse to and select the .zip file containing the patches you want to import
- Click **Next** and wait until the file upload completes successfully
- Click **Next**
- On the **Confirm Import** page of the **Import Patches** wizard, review the patches that you import into the Update Manager repository
- Click **Finish**

You imported the patches into the Update Manager patch repository. You can view the imported patches on the Update Manager Patch Repository tab

### **Perform Orchestrated vSphere Upgrades**

Orchestrated upgrades allow you to upgrade the objects in your vSphere inventory in a two-step process: host upgrades followed by virtual machine upgrades. You can configure the process at the cluster level for higher automation, or at the individual host or virtual machine level for granular control.

You can upgrade clusters without powering the virtual machine off as long as VMware Distributed Resource Scheduler (DRS) is available for the cluster. To perform an orchestrated upgrade, you must first remediate a cluster against a host upgrade baseline, and then remediate the same cluster against a virtual machine upgrade baseline group containing the VM Hardware Upgrade to Match Host and VMware Tools Upgrade to Match Host baselines.

### **Create and Modify Baseline Groups**

Baselines contain a collection of one or more updates such as service packs, patches, extensions, upgrades, or bug fixes. Baseline groups are assembled from existing baselines. When you scan hosts, virtual machines, and virtual appliances, you evaluate them against baselines to determine their level of compliance.

Update Manager supports different types of baselines that you can use and apply when scanning and remediating objects in your inventory:

- Upgrade Baseline – Defines which version a particular host, virtual hardware, VMware Tools, or virtual appliance should be.
- Patch Baseline – Defines a number of patches that must be applied to a given host or virtual machine
- Extension Baseline – Contains extensions (additional software such as third-party device drivers) that must be applied to a given host. Extensions are installed on hosts that do not have such software installed on them and patched on hosts that already have the software installed. All third-party software for ESX/ESXi hosts is classified as a host extension, although host extensions are not restricted to just third-party software.

Update Manager includes default baselines that you can use to scan any virtual machine, virtual appliance, or host to determine whether they have all patches applied for the

different categories or are upgraded to the latest version. The default baselines cannot be modified or deleted:

- Critical Host Patches – Checks ESX/ESXi hosts for compliance with all critical patches
- Non-Critical Host Patches – Checks ESX/ESXi hosts for compliance with all optional patches
- VMware Tools Upgrade to Match Host – Checks virtual machines for compliance with the latest VMware Tools version on the host Update Manager supports upgrading of VMware Tools for virtual machines on hosts that are running ESX/ESXi 4.0 and later
- VM Hardware Upgrade to Match Host – Checks the virtual hardware of a virtual machine for compliance with the latest version supported by the host. Update Manager supports upgrading to virtual hardware version 8.0 on hosts that are running ESXi 5.x
- VA Upgrade to Latest – Checks virtual appliances compliance with the latest released virtual appliance version

#### Create a Fixed Patch Baseline

- Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click Update Manager under Solutions and Applications on the Home Page
- On the Baseline and Groups tab, click Create above the Baselines pane, this will launch the New Baseline wizard
- In the New Baseline wizard, under Baseline Type, select Host Patch and click Next
- Select Fixed for the type of baseline and click Next
- Select individual patches to include, and click the down arrow to add them to the Fixed Patches to Add list
- (Optional) Click Advanced to find specific patches to include in the baseline
- Click Next
- Review the Ready to Complete page and click Finish

The fixed patch baseline is displayed in the Baselines pane of the Baselines and Groups tab

#### Create a Dynamic Patch Baseline

- Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click Update Manager under Solutions and Applications on the Home Page
- On the Baseline and Groups tab, click Create above the Baselines pane
- In the New Baseline wizard, under Baseline Type, select either Host Patch and click Next
- Select Dynamic as the type of baseline, and click Next

- On the Dynamic Baseline Criteria page, enter criteria to define the patches to include, and then click Next
- (Optional) On the Patches to Exclude page, select one or more patches in the list and click the down arrow to permanently exclude them from the baseline
- (Optional) Click Advance to select specific patches to exclude from the baseline
- Click Next
- (Optional) On the Other Patches to Add page, select individual patches to include in the baseline and click the down arrow to move them into the Fixed Patches to Add list
- (Optional) Click Advanced to select specific patches to include in the baseline
- Review the Ready to Complete page and click Finish

The dynamic patch baseline is displayed in the Baselines pane of the Baselines and Groups tab

### **Troubleshoot Update Manager Problem Areas and Issues**

Refer to chapter 17 “Troubleshooting” of the Installing and Administering VMware vSphere Update Manager documentation for troubleshooting examples and solutions.

### **Generate Database Reports Using MS Excel or MS SQL**

Using Microsoft Excel, you can connect to the Update Manager database and query the database views to generate a common report:

- Log in to the computer on which the Update Manager database is setup
- From the Windows Start menu, select Programs > Microsoft Office > Microsoft Excel
- Click Data > Import External Data > New Database Query
- In the Choose Data Source window, select VMware Update Manager and click OK
- In the Query Wizard – Choose Columns window, select the columns of data to include in your query and click Next
- Click OK in the warning message that the query wizard cannot join the tables in your query
- In the Microsoft Query window, drag a column name from the first view to the other column to join the columns in the tables manually

Using a Microsoft SQL Server query, you can generate a common report from the Update Manager database. An example query is provided on page 179 of the VMware vCenter Update Manager Installation and Administration Guide.

### **Upgrade vApps Using Update Manager**

vApps are managed in the same ways as hosts or vm's. You will need to create a baseline and attach it to the vApp object. You then can perform scans and remediation's as documented for hosts and vm's.

### Utilize Update Manger PowerCLI to Export Baselines for Testing

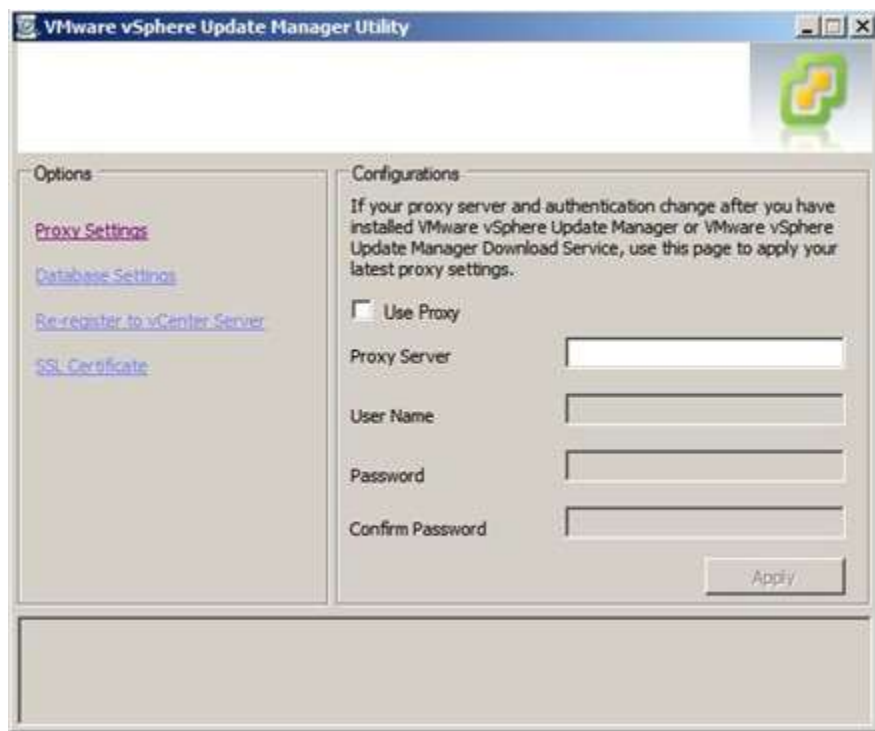
See pages 155 thru 158 of the Installing and Administering VMware vSphere Update Manager documentation for a full eight step workflow as well as the required PowerCLI script to complete this task

### Utilize the Update Manger Utility to Reconfigure VUM Settings

The Update Manager Utility is available by default when you install either Update Manager or UMDS. The tools allows for post installation configuration of the following settings:

- Proxy Settings
- Database Settings (user name and password)
- Re-register to vCenter Server
- SSL Certificate

To launch the application browse to the installation directory for Update Manager or UMDS (be default should be C:\Program Files (x86)\VMware Infrastructure\Update Manager) and look for the VMwareUpdateManagerUtility executable. Below is a screenshot after launching the application and logging in:



## VCAP5-DCA – Objective 6.1 – Configure, Manage, and Analyze vSphere Log Files

---

For this objective I used the following documents:

- Documents listed in the Tools section

### **Objective 6.1 – Configure, Manage, and Analyze vSphere Log Files**

Knowledge

**\*\*ITEMS IN BOLD ARE TOPICS PULLED FROM THE BLUEPRINT\*\***

- **Identify vCenter Server log file names and locations**
  - Below are a list of the log file names and their locations (I used VMware [KB1021804](#) to help me with this)
  - vCenter Server (Windows and Virtual Appliance)
    - **vpzd-###** – this is the main vCenter log and it will have a number at the end of it. The highest number is the most current log.
      - (Windows) `c:\programdata\VMware\VMware VirtualCenter\Logs`
      - (Virtual Appliance) `/var/log/vmware/vpx`
    - **vpzd-profiler-###** – this log stores some form of metrics. These metrics are viewable at the following URL: <https://<ip>or hostname of vcenter>/vod/index.html>
      - You will be challenged for credentials. Here is a screenshot



## VMware VirtualCenter Operational Dashboard

Home

**Host: prod-vCenter01**  
Started on: 2012-09-04 18:57:21.071  
Uptime: 1 day 2 hours 52 mins 2 secs  
Log to file: ON [toggle](#)

**Detail Pages**

[Pull Counters](#)   [Push Counters](#)   [Lock stats](#)   [Ho](#)

**Virtual Machine & Host Operations (invocations/min)**

NAME
Create VM
Register
Unregister
Reconfigure VM
Clone
Relocate
Migrate
Power Off
Power On
Group Power On
Add Host
Add Host (Cluster)
Reconnect Host
Enter Maintenance Mode
Enter Standby Mode

**Client Communication (invocations/min)**

NAME	LAST 5 MIN.
Incoming Calls	77.313431

- (Windows) *c:\programdata\VMware\VMware VirtualCenter\Logs*
  - (Virtual Appliance) */var/log/vmware/vpx*
  - **cim-diag** and **vws**– these logs hold CIM (Common Information Model) information, such as vCenter ↔ Host communications via CIM
    - (Windows) *c:\programdata\VMware\VMware VirtualCenter\Logs*
    - (Virtual Appliance) */var/log/vmware/vpx*
  - There are multiple folders located in the **drmdump** folder at the location below. These folders contain DRS proposed actions and actions taken. These logs are compressed
    - (Windows) *c:\programdata\VMware\VMware VirtualCenter\Logs\drmdump\cluster###*
    - I couldn't find these logs in the virtual appliance
- **Identify ESXi log file names and locations**

- Here is a list of ESXi log file names and their locations (I used VMware [KB2004201](#) to help me with this)
  - Log and configuration files can be found by going to the following URL:
    - <https://<ip or hostname of ESXi host>/host>

Configuration files		
Name	Last Modified	Size
<a href="#">auth.log</a>	18-Mar-2012 00:13	34865
<a href="#">configRP.log</a>	02-Aug-2012 21:54	6498
<a href="#">dhclient.log</a>	18-Mar-2012 00:13	2701
<a href="#">esx.conf</a>	06-Sep-2012 01:41	22978
<a href="#">esxupdate.log</a>	18-Mar-2012 00:13	395756
<a href="#">fdm.log</a>	18-Mar-2012 00:13	1538659
<a href="#">hostAgentConfig.xml</a>	29-Jun-2012 20:19	24273
<a href="#">hostd.log</a>	18-Mar-2012 00:13	564335
<a href="#">hostprofiletrace.log</a>	18-Mar-2012 00:13	0
<a href="#">hosts</a>	02-Aug-2012 21:54	238
<a href="#">license.cfg</a>	02-Aug-2012 21:54	310
<a href="#">motd</a>	29-Jun-2012 20:19	313
<a href="#">openwsman.conf</a>	06-Sep-2012 01:37	639
<a href="#">pam.d/passwd</a>	29-Jun-2012 20:19	236
<a href="#">proxy.xml</a>	02-Aug-2012 21:54	2576
<a href="#">sfcf.cfg</a>	02-Aug-2012 21:54	933
<a href="#">shell.log</a>	18-Mar-2012 00:13	32107
<a href="#">snmp.xml</a>	02-Aug-2012 21:54	114
<a href="#">ssh_host_dsa_key</a>	02-Aug-2012 21:54	672
<a href="#">ssh_host_dsa_key_pub</a>	02-Aug-2012 21:54	617
<a href="#">ssh_host_rsa_key</a>	02-Aug-2012 21:54	1675
<a href="#">ssh_host_rsa_key_pub</a>	02-Aug-2012 21:54	381
<a href="#">ssh_root_authorized_keys</a>	29-Jun-2012 20:19	0
<a href="#">ssl_cert</a>	02-Aug-2012 21:54	1996
<a href="#">ssl_key</a>	02-Aug-2012 21:54	1704

- You can access logs via the DCUI (Direct Console User Interface)
- You can access logs by SSH'ing into the host at the following location(s)
  - **auth.log**– ESXi shell authentication success/failures
    - `/var/log/auth.log`
  - **dhclient.log**– DHCP client service log
    - `/var/log/dhclient.log`
  - **esxupdate.log**– Update installation log
    - `/var/log/esxupdate.log`
  - **hostd.log**– Host management log–also for VM tasks and events
    - `/var/log/hostd.log`

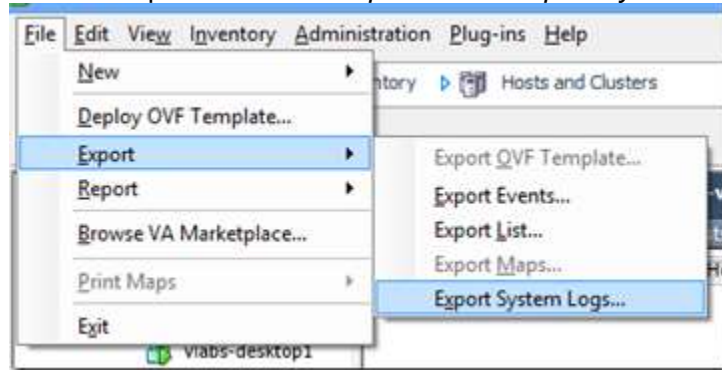
- **shell.log**– logs things that happen in the ESXi shell
  - */var/log/shell.log*
- **sysboot.log**– early VMkernel startup and module loading
  - */var/log/sysboot.log*
- **syslog.log**- scheduled tasks, DCUI use and watchdogs
  - */var/log/syslog.log*
- **usb.log**– USB arbitration events
  - */var/log/usb.log*
- **vob.log**– VMkernel observation events
  - */var/log/vob.log*
- **vmkernel.log**– core VMkernel logs, storage and networking device driver events and virtual machine startup
  - */var/log/vmkernel.log*
- **vmkwarning.log**– summary of warning and alert log messages from the VMkernel logs
  - */var/log/vmkwarning.log*
- **vmksummary.log**– summary of ESXi startup and shutdown, hourly heartbeat w/uptime, number of VMs running and service resource consumption
  - */var/log/vmksummary.log*
- **vpaxa.log**– vCenter server vpaxa agent logs, communication between vCenter and hostd
  - */var/log/vpaxa.log*
- **fdm.log**– vSphere HA (High Availability) events generated by the FDM service
  - */var/log/fdm.log*

- **Identify tools used to view vSphere log files**

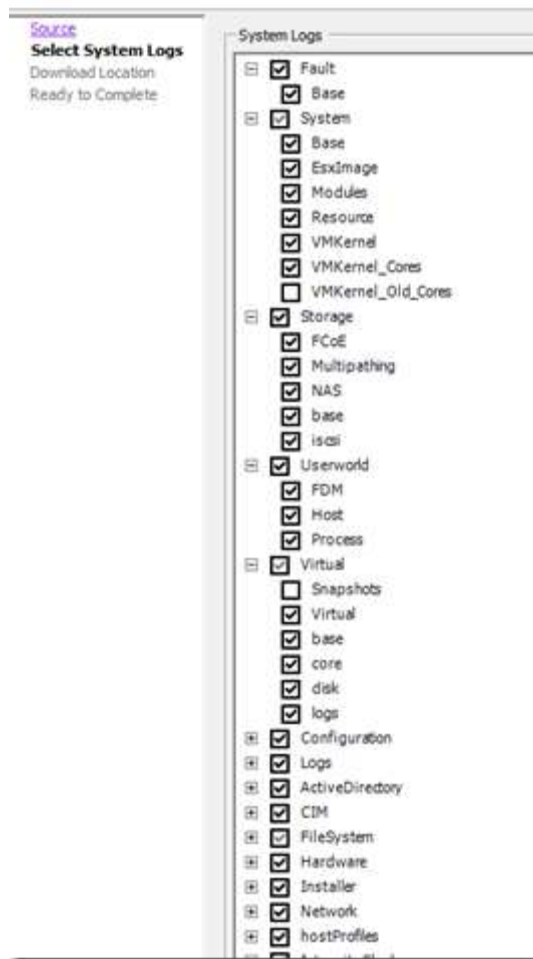
Skills and Abilities

- **Generate vCenter Server and ESXi log bundles**
  - You can generate log bundles from the GUI or via the command line. I'll cover both
  - Generate log bundles from the GUI
    - Log into the vSphere client

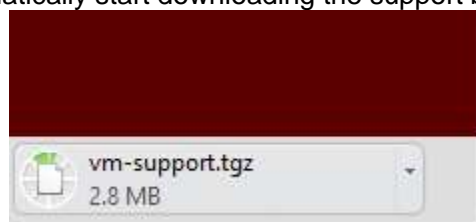
- Click *File* from the top menu > click *Export* > click *Export System Logs...*



- Select at which level you want to export logs from. Select the topmost object (the vCenter object) to export ALL logs > leave the checkbox *Include Information from vCenter and vSphere Client* checked if you want to also export those logs
- Click *Next*
- Select which logs you want to export; by default they are all checked. As you can see there are a TON of logs



- Click *Next*
- Click the *Browse* button to select a location to save the log bundle to > click *Next*
- Click *Finish*
- New in ESXi 5 you can invoke a the export log utility via http
  - From a web browser browse to <https://username:password@ESXHostnameOrIPAddress/cgi-bin/vm-support.cgi>
  - This will automatically start downloading the support bundle named *vm-support.tgz*



- Generate log bundles from the command line
  - SSH into an ESXi host

- To export logs you'll need to use the *vm-support* command. You can export information based on a list of groups or certain 'manifests' or you can export information on a particular virtual machine. You can also set a log level with the *-log/level* option; values are 0-50 with 0 being the most verbose
- Generate a generic bundle by executing *vm-support* and it will generate a log bundle in a .gz format and by default place it in the */var/tmp* directory
  - use the *-w* option to change the working directory of where the bundle will be saved

• **Use *esxcli system syslog* to configure centralized logging on ESXi hosts**

- Before you configure your hosts for syslog you can check the current configuration from the command line using the following command

1 `esxcli system syslog config get`

- Here is an example of what it will look like when nothing has been configured for syslog

```
# esxcli system syslog config get
Default Rotation Size: 1024
Default Rotations: 8
Log Output: /scratch/log
Log To Unique Subdirectory: false
Remote Host: <none>
#
```

- You can also use the following command to list out the same details seen in the previous command output, but for each individual log. This also will tell you what all of the log files are

1 `esxcli system syslog config logger list`

- Before you configure centralized logging you will need to know the location of the remote syslog server. I'm using the VMware syslog Collector in my lab, and these example. I'll go over how to set this up in the last objective of this section

- Here is a list of commands on how to change the different syslogging option on an ESXi host. Keep in mind that all of the commands in the following examples are being defined globally, so any sub-logs that have the same value as the default global will also be changed. . You don't have to execute all commands individually, you can group some into the same command

1 `# change the default rotation size by executing the following command`

2 `# in this example we are changing it to 3MB`

3 `# you shouldn't receive any output (no output is good output); this applies to all th`

4 `esxcli system syslog config set --default-size=3072`

5

6 # change the default rotations by executing the following command

7 # in this example we are changing them to 16

8

9 esxcli system syslog config set --default-rotate=16

10

11 # set the host to send logs to a remote syslog by executing the following command

12 # in this example we are sending them to a host with the IP of 10.90.90.10

13

14 esxcli system syslog config set --loghost 10.90.190.10

15

16 # to load the changes into runtime execute the following command

17

18 esxcli system syslog reload

19

20

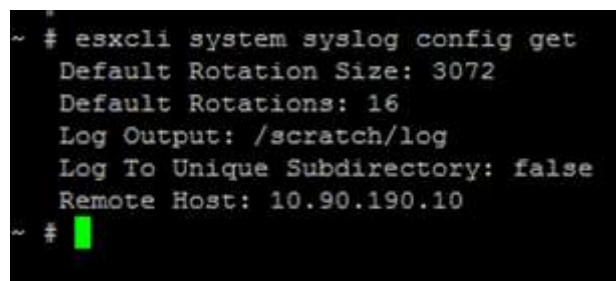
- Once you've changed your configuration and reloaded the syslog daemon, run the following command to ensure the proper changes

1 # view your configuration by running the following command

2

3 esxcli system syslog config get

- Now you should see the log rotations set to 16, the size set to 3072 and the loghost set to 10.90.190.10



```
~ # esxcli system syslog config get
Default Rotation Size: 3072
Default Rotations: 16
Log Output: /scratch/log
Log To Unique Subdirectory: false
Remote Host: 10.90.190.10
~ #
```

- If you still don't see the logs showing up on your remote syslog server after configuring the remote host, ensure that the ESXi firewall has the syslog ports open
  - Log into the vSphere client

- From the inventory tree, click the ESXi host that you configured the remote syslog server on > click the *Configuration* tab
- Under the *Software* pane click the *Security Profile* hyperlink
- In the right-pane click the *Properties...* hyperlink
- Find the *syslog* service located under the *Ungrouped services*
- If the checkbox next to the *syslog* service isn't checked, check it

Label	Incoming Ports	Outgoing Ports	Protocols
<b>Ungrouped</b>			
<input checked="" type="checkbox"/> DNS Client	53	53	UDP,TCP
<input type="checkbox"/> VM serial port connected to vSPC		0-65535	TCP
<input checked="" type="checkbox"/> NTP Client		123	UDP
<input checked="" type="checkbox"/> Fault Tolerance	8100,8200	80,8100,8200	TCP,UDP
<input type="checkbox"/> DVFilter	2222		TCP
<input checked="" type="checkbox"/> NFC	902	902	TCP
<input type="checkbox"/> CIM Secure Server	5989		TCP
<input checked="" type="checkbox"/> HBR		31031,44046	TCP
<input checked="" type="checkbox"/> WOL		9	UDP
<input checked="" type="checkbox"/> vSphere Web Access	80		TCP
<input checked="" type="checkbox"/> <b>syslog</b>		514,1514	UDP,TCP
<input type="checkbox"/> DVSSync	8301,8302	8302,8301	UDP

- Click *OK*

- **Test centralized logging configuration**

- Testing your logging configuration can be done pretty simply. There is a command in the *esxcli system syslog* namespace that allows you to send a message to all your logs at the same time. You can use this to send a message, and then check the log on your remote syslog system and see if it shows up. Here's the command

```

1 # this command will send the message "vcap5-test-configuration" to all your logs
2
3 esxcli system syslog mark --message="vcap5-test-configuration"

```

- Here you can see the message was logged, which means your centralized logging is configured properly

```

<166>2012-09-11T00:33:46.994Z vlabs-vmhost03.prod01.local Vpxa: [5EF46B90 verbose "Defa
<166>2012-09-11T00:33:46.994Z vlabs-vmhost03.prod01.local Vpxa: [5EF46B90 verbose "Vpxa
<166>2012-09-11T00:33:46.994Z vlabs-vmhost03.prod01.local Vpxa: [5EF46B90 verbose "Vpxa
<166>2012-09-11T00:33:47.049Z vlabs-vmhost03.prod01.local Hostd: [FFFC0AC0 error "Vmxan
<166>2012-09-11T00:33:47.049Z vlabs-vmhost03.prod01.local Hostd: [FFFC0AC0 info "Vmxan
<190>2012-09-11T00:33:47.164Z vlabs-vmhost03.prod01.local mark: vcap5-test-configuration
<166>2012-09-11T00:33:47.164Z vlabs-vmhost03.prod01.local Hostd: [FFFC0AC0 info "Vmxan
<166>2012-09-11T00:33:47.164Z vlabs-vmhost03.prod01.local Hostd: [FFFC0AC0 verbose "Vm
<166>2012-09-11T00:33:47.164Z vlabs-vmhost03.prod01.local Hostd: [5F6F1B90 verbose "Sys
<166>2012-09-11T00:33:47.165Z vlabs-vmhost03.prod01.local Hostd: [5F6F1B90 verbose "Sys

```

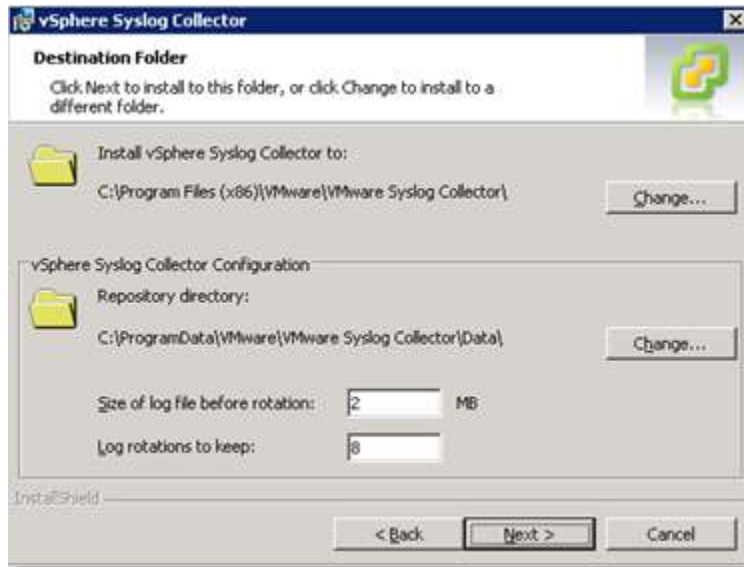
- **Analyze log entries to obtain configuration information**
- **Analyze log entries to identify and resolve issues**



- - Unfortunately I'm not to sure how to document these two sections. The list of logs that I detailed above tells you the type of information that you'll find in each one, which may help in deciphering the configuration or finding relevant entries within a log to help you narrow down a problem
- **Install and configure VMware syslog Collector and ESXi Dump Collector**
  - Before we begin you need to have the vCenter bits downloaded
  - Install and Configure VMware syslog Collector
    - Log onto the server you plan on installing syslog Collector
    - From the location of the vCenter bits, double click the *autorun.exe* file
    - Under *vCenter Support Tools* click *VMware Syslog Collector* > click the *Install* button



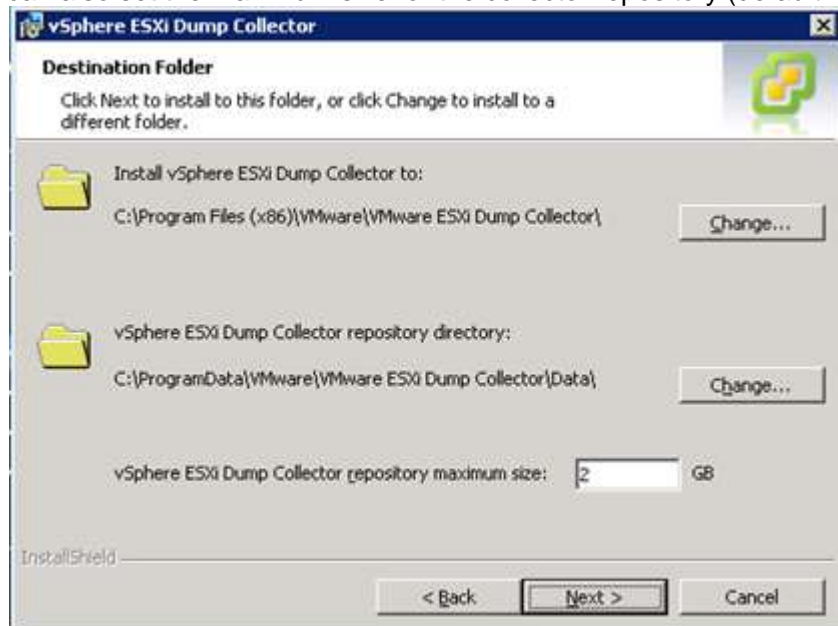
- Choose a language and click *OK*
- When the install dialog comes up, click *Next*
- Click *Next* > Click the *I accept the terms...* radial button > click *Next*
- Here you can change the default installation directory and the default log repository location
- You can also set the log rotation frequency and size (2MB and 8 by default, respectively)



- Make changes if desired, click *Next*
- Choose whether you want to perform a stand-alone installation or an installation that is integrated with vSphere. For these purposes I'm using the *VMware vCenter Server installation*
- Choose an option and click *Next*
- If you chose the *VMware vCenter Server installation* setup type, enter in the *IP Address/Name* of the vCenter server along with the username and password
- Click *Next*
- Unless you want to change the ports, leave the defaults at the *vSphere Syslog Collector Port Settings* page > click *Next*
- Click *Next* at the identification screen (choose to use the IP or name)
- Click *Install*
- Once the installation is complete, click *Finish*
- Install and Configure VMware syslog Collector
  - Log onto the server you plan on installing syslog Collector
  - From the location of the vCenter bits, double click the *autorun.exe* file
  - Under *vCenter Support Tools* click *VMware ESXi Dump Collector* > click the *Install* button



- Choose a language and click *OK*
- When the install dialog comes up, click *Next*
- Click *Next* > Click the *I accept the terms...* radial button > click *Next*
- Here you can change the default installation directory and the default log repository location
- You can also set the maximum size for the collector repository (default is 2GB)



- Click *Next*

- Choose whether you want to perform a stand-alone installation or an installation that is integrated with vSphere. For these purposes I'm using the *VMware vCenter Server installation*
- Choose an option and click *Next*
- If you chose the *VMware vCenter Server installation* setup type, enter in the *IP Address/Name* of the vCenter server along with the username and password
- Click *Next*
- Unless you want to change the collector server port, click *Next*
- Click *Next* at the identification screen (choose to use the IP or name)
- Click *Install*
- Once the installation is complete, click *Finish*

## Tools

- [vSphere Management Assistant Guide](#)
- [vSphere Command-Line Interface Concepts and Examples](#)
- [Product Documentation](#)
- VMware syslog Collector
- ESXi Dump Collector
- *esxcli*

# VCAP5-DCA – Objective 6.2 – Troubleshoot CPU and Memory Performance

---

For this objective I used the following documents:

- <http://communities.vmware.com/docs/DOC-11812> – Everything ESXTOP
- <http://www.yellow-bricks.com/esxtop/> – Good rollup from Duncan
- Documents listed in the Tools section

## **Objective 6.2 – Troubleshoot CPU and Memory Performance**

Knowledge

**\*\*ITEMS IN BOLD ARE TOPICS PULLED FROM THE BLUEPRINT\*\***

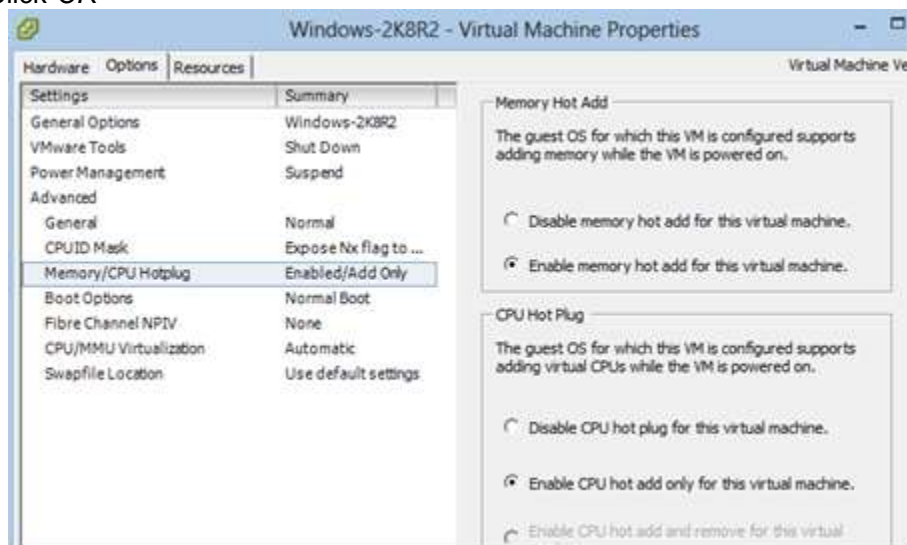
- **Identify *resxtop* / *esxtop* metrics related to memory and CPU**
  - Here are a list of some of the key CPU and memory related metrics *resxtop* / *esxtop*. A list of all metrics can be found in the link above (“Everything ESXTOP”)
  - CPU metrics
    - **%RDY** (higher than 5) – indicates the amount of time the world was ready to run, but the world is stuck in a run queue while it waits on the CPU scheduler to schedule time on a physical CPU
    - **%SYS** (higher than 15) – indicates that the VM may have a lot of I/O. Represents the percentage of time used by system services on behalf of the world
    - **%SWPWT** (higher than 3) – indicates the percentage of time the world spends waiting on vmkernel memory swapping
    - **%CTSP** (higher than 3) – indicates the percentage of time the world spends in a ready, co-deschedule state. Used for SMP virtual machines. The higher this metric the further ahead on vCPU is over another vCPU.
    - **%MLMTD** (higher than 0) – indicates a VM is being throttled by a CPU limit that has been set. Indicates that the world was ready to run, but wasn’t aloud to due to the limit
  - Memory metrics
    - **SWCUR** (higher than 0) – indicates the host is swapping memory <- THIS IS BAD!
    - **MCTLSZ** (higher than 0) – indicates that memory is being ballooned; if memory pressure continues, memory compression may occur

- **ZIP/s** (higher than 0) – indicates that memory is being compressed; if memory pressure continues, memory swapping may occur
- **Identify vCenter Server Performance Chart metrics related to memory and CPU**

#### Skills and Abilities

- **Troubleshoot ESXi host and Virtual Machine CPU performance issues using appropriate metrics**
  - Using some of the tools mentioned above you can troubleshoot ESXi host and virtual machine CPU performance, such as **esxtop / resxtop** and, if you're running Windows, you can use Windows **Perfmon**.
  - I won't go into perfmon here, but here are some key metrics to look at when troubleshooting host and virtual machine CPU performance problems
    - **%RDY** (higher than 5) – indicates the amount of time the world was ready to run, but the world is stuck in a run queue while it waits on the CPU scheduler to schedule time on a physical CPU
    - **%MLMTD** (higher than 0) – indicates a world is being throttled by a CPU limit that has been set. Indicates that the world was ready to run, but wasn't aloud to due to the limit
    - **PCPU UTIL(%)** (all over 90-95%) – percentage of unhalted CPU cycles per PCPU. Also the average across all PCPUs
    - **%SWPWT** (higher than 3) – indicates the percentage of time the world spends waiting on vmkernel memory swapping
    - **%CTSP** (higher than 3) – indicates the percentage of time the world spends in a ready, co-deschedule state. Used for SMP virtual machines. The higher this metric the further ahead on vCPU is over another vCPU.
  - **Troubleshoot ESXi host and Virtual Machine memory performance issues using appropriate metrics**
    - Again, here are metrics to focus on from **esxtop**; these are the same metrics listed above in the *Knowledgesection*.
      - **SWCUR** (higher than 0) – indicates the host is swapping memory <- THIS IS BAD!

- **MCTLSZ** (higher than 0) – indicates that memory is being ballooned; if memory pressure continues, memory compression may occur
- **ZIP/s** (higher than 0) – indicates that memory is being compressed; if memory pressure continues, memory swapping may occur
- **Use Hot-Add functionality to resolve identified Virtual Machine CPU and memory performance issues**
  - The concept behind hot-add is to be able to add/remove memory and CPU resources on a virtual machine that is powered-on. Not all guest operating systems support this, so make sure you are using one that is supported (I can't find a list for this, will post if I can find one)
  - One thing to keep in mind is that hot-plug/add functionality must first be enabled before it can be used, and to enable it the virtual machine must be powered off
  - Enable CPU/Memory Hot-Add
    - Log into vCenter or directly to the host using the vSphere client
    - From the *Hosts and Clusters* view or *VMs and Templates* view find the virtual machine you want to enable hot-add on
    - If the virtual machine is powered on, power it off
    - Right-click the VM and select *Edit Settings*
    - Click the *Options* tab at the top
    - Select *Memory/CPU Hotplug*
    - Set *Memory Hot Add* to *Enable memory hot add for this virtual machine*
    - Set *CPU Hot Plug* to *Enable CPU hot plug for this virtual machine*
    - Click *OK*



- The operation is now complete. You can power-on the virtual machine and hot/remove memory or vCPUs to this VM while it is powered-on

## Tools

- [vSphere Resource Management Guide](#)
- [Product Documentation](#)
- vSphere Client / Web Client
- vSphere CLI
  - *resxtp / esxtp*



# VCAP5-DCA – Objective 6.3 – Troubleshoot Network Performance and Connectivity

---

For this objective I used the following documents:

- Documents listed in the Tools section

## **Objective 6.3 – Troubleshoot Network Performance and Connectivity**

Knowledge

**\*\*ITEMS IN BOLD ARE TOPICS PULLED FROM THE BLUEPRINT\*\***

- **Identify vCLI commands and tools used to troubleshoot vSphere networking configurations**
  - There are a good amount of vCLI commands that you can use to troubleshoot your networking configurations. Most of which start with “**vicfg-**“. Here are some basic ones, but without their options listed. You can find a full reference in the command line concepts and examples document listed in the tools section
    - **vicfg-vswitch**
    - **vicfg-nics**
    - **vicfg-vmknics**
    - **vicfg-route**
    - **vicfg-dns**
- **Identify logs used to troubleshoot network issues**
  - There are a few different log files you can look at for networking related issues:
    - DHCP issues – /var/log/dhclient.log
    - Networking driver and device issues – /var/log/vmkernel.log
    - vCenter issues – /var/log/vpxa.log

Skills and Abilities

- **Utilize net-dvs to troubleshoot vNetwork Distributed Switch configurations**

- the ***net-dvs*** command will show you A LOT of information about your distributed switches. Probably a lot more than you want. By simply running ***net-dvs*** without any options or switches you'll see the following information:
  - maximum ports
  - the switch name
  - Number of uplinks and their names
  - MTU, Discovery protocol
  - Individual configuration for each uplink, and its port numbers
- This information can help you put together what the dvSwitch might look like, along with individual ports on the dvSwitch for their respective uplinks
- There is a **WHOLE** lot more to this command than what I just went over. If you execute ***net-dvs -help*** you will see all the things that you can do with this command. One thing to keep in mind is that this command is *unsupported* and shouldn't be used in a production network. To be quite honest, I have no idea why it's on the blueprint. Since the command is unsupported, I will leave it at what I've explained above. If you'd like to explore the command more than I encourage you to do so in your lab
- **Utilize vSphere CLI commands to troubleshoot ESXi network configurations**
  - I went over the list of basic commands in the preceding section, but I'll list them here again
    - ***vicfg-vswitch***
    - ***vicfg-nics***
    - ***vicfg-vmknic***
    - ***vicfg-route***
    - ***vicfg-dns***
  - Use the above commands to perform troubleshooting
- **Troubleshoot Private VLANs**
  - Andrew Scorsone over at [thefoglite](#) has a good write-up on this, check it out [here](#)
- **Troubleshoot vmkernel related network configuration issues**
  - First place to look here is the vmkernel log file, located on every host at `/var/log/vmkernel.log`. This will present any events related to networking configuration and the vmkernel.
  - Ensure you have at least one vmkernel interface enabled for management. You should have at least two vmkernel interfaces on different networks plugged into separate switches for redundancy

- Use ***vicfg-vmknic*** to assist in configuration validation as well as the vSphere Client/Web Client
- Use the DCUI to test management networking connectivity
- You can also use ***esxcli network diag ping*** to troubleshoot connectivity
- **Troubleshoot DNS and routing related issues**
  - Use the ***vicfg-dns*** and ***vicfg-route*** commands to troubleshooting DNS and routing
  - Use the DCUI or the vSphere client to set DNS servers and DNS domain names
  - Use esxcli commands to set/troubleshooting DNS related items
    - ***esxcli network ip dns server***
    - ***esxcli network ip dns search***
  - You can also use esxcli commands to troubleshooting routing issues
    - ***esxcli network ip route ipv4 list*** < this command will list the current routes on the host
    - explore the ***esxcli network ip route*** namespace for more options
- **Use esxtop / resxtop to identify network performance problems**
  - Again, [thefoglite](#) has put together a great article on identifying network performance problems with ***esxtop / resxtop*** [here](#), it is well worth the read
- **Analyze troubleshooting data to determine if the root cause for a give network problem originates in the physical infrastructure or vSphere environment**
- **Configure and administer Port Mirroring**
  - This process assumes you know the IP address of the source/destination VM
  - Log into the vSphere client and goto the networking view
  - If you don't already know the port you want to mirror:
    - Select the vDS you want to configure port mirroring on
    - Click the *Ports* tab
    - Find the virtual machine whose port you want to mirror, and record the port it is connected to
    - Also record the destination virtual machine port that you will be mirroring to (if you're mirroring to a VM)
  - Right-click the vDS you are configuring port mirroring on > click *Edit Settings*
  - Click the *Port Mirroring* tab > click *Add*
  - Enter in the *Name* and *Description*
  - Change the following options if you wish
    - *Allow normal IO on destination ports*

- *Encapsulation VLAN* (enter in the VLAN ID)
  - *Mirrored Packet Length* (enter in packet length, default is 60)
- Click *Next*
- Select one of the *Traffic Direction* options:
  - *Ingress / Egress*
  - *Ingress*
  - *Egress*
- Enter in a *source port ID* > click the double arrow to add > click *Next*
- Select either *Port* or *Uplink* for the *Destination Type*
  - If you selected *Port* then enter in the destination port ID and click the double arrow to add
  - If you selected *Uplink* then choose from the list of uplinks and click the double arrow to add
- Click *Next*
- If you want to enable the port mirroring session right away check the *Enable this port mirroring session* checkbox
- Click *Finish*
- **Utilize Direct Console User Interface (DCUI) and ESXi Shell to troubleshoot, configure, and monitor ESXi networking**
  - Once logged into the DCUI you can
    - Look at log files (specifically vmkernel.log)
    - Enable / disable physical adapters
    - Change the management IP settings
    - Revert your management network back to the standard switch (if it currently resides on a vDS)
    - Test management network connectivity
    - Restore all settings to default (you probably don't want to do this)

## Tools

- [vSphere Command-Line Interface Concepts and Examples](#)
- [vSphere Installation and Setup Guide](#)
- [vSphere Resource Management Guide](#)

# VCAP5-DCA – Objective 6.4 – Troubleshoot Storage Performance and Connectivity

---

For this objective I used the following documents:

- Documents listed in the Tools section

## **Objective 6.4 – Troubleshoot Storage Performance and Connectivity**

Knowledge

**\*\*ITEMS IN BOLD ARE TOPICS PULLED FROM THE BLUEPRINT\*\***

- **Identify logs used to troubleshoot storage issues**
  - Log files that can be used to troubleshoot storage issues on an ESXi host all reside in the **/var/log** folder on the host:
    - **vmkernel.log** — you could see the host disconnecting/reconnecting to devices
    - **storagem.log** — storage I/O control information
    - **vobd.log** — observations made by the vmkernel
- **Describe the attributes of the VMFS-5 file system**
  - - Can now be up to 64TB (VMFS-3 was 2TB)
    - Single 1MB block size (VMFS-3 had 4 different sizes)
    - Maximum file count is >100K
    - VMDK files up to 2TB (this has not changed from VMFS-3)
    - VMFS-5 uses GPT as its partition table (VMFS-3 used a MBR partition table)
    - RDMs can be up to 64TB (pass-through RDMs only)
    - The Sub-block size is 8KB (VMFS-3 used 64KB sub-block size)

Skills and Abilities

- **Use *esxcli* to troubleshoot multipathing and PSA-related issues**
  - There are a few different contexts within *esxcli* that can be used for multipathing and PSA-related issues. I will list those contexts below and denote where they apply
    - ***esxcli storage core path*** –this context allows you to look at pathing that exists for devices connected to the host. Use ***esxcli storage core path list -d*** option along with a given device ID (e.g. naa.60060160891227...) to list all paths to a particular device

- ***esxcli storage nmp psp*** — this context allows you to look at the various PSPs on the system and modify their properties
- ***esxcli storage nmp satp*** — this context allows you to look at the various SATPs installed on the system and modify their properties
- **Use *esxcli* to troubleshoot VMkernel storage module configurations**
  - ***esxcli storage core plugin registration list*** — this command lists out all registered modules for the host, to include SATPs and PSPs
  - ***esxcli storage core plugin <add><remove>*** — allows you to add or remove modules as needed
- **Use *esxcli* to troubleshoot iSCSI related issues**
  - The ***esxcli iscsi*** context allows you to perform most configuration aspects related to iSCSI, and lets you list all configurations, which can be useful when troubleshooting
  - Here are a few commands to get you started:
    - 
    - ***esxcli iscsi networkportal list*** — this will list the vmkernel ports you have configured
    - ***esxcli iscsi logicalportal list*** — this command gives you a summary of all vmkernel ports to include the MAC address
    - ***esxcli iscsi session list*** — this command will list all active iSCSI sessions
    - ***esxcli iscsi adapter target portal list*** — this command will list all iSCSI targets the host is connected to
    - ***esxcli iscsi adapter capabilities get -A <vmhba##>*** — this command will list the capabilities of the give iSCSI HBA
- **use *esxtop* / *resxtop* and *vscsiStats* to identify storage performance issues**
  - You can see a brief introduction to using ***vscsiStats*** in a previous VCAP5 blog post; [Objective 1.1 – Implement and Manage Complex Storage Solutions](#) – look about a quarter of the way down the page
  - Here is a list of storage metrics you can look at in ***esxtop* / *resxtop*** to troubleshoot storage performance issues
  - For storage monitoring there are three panels within ***esxtop*** that you will want to be intimately familiar with (the letters at the end correspond the the ***esxtop*** hotkey for those panels)
    - 
    - Storage Adapter Panel (d)

- Storage Device Panel (u)
- Virtual Machine Storage Panel (v)
- Some key metrics you want to look at for the panels above
  - *MBREAD/s* — megabytes read per second
  - *MBWRN/s* — megabytes written per second
  - *KAVG* — latency generated by the ESXi kernel
  - *DAVG* — latency generated by the device driver
  - *QAVG* — latency generated from the queue
  - *GAVG* — latency as it appears to the guest VM (*KAVG* + *DAVG*)
  - *AQLEN* – storage adapter queue length (amount of I/Os the storage adapter can queue)
  - *LQLEN* – LUN queue depth (amount of I/Os the LUN can queue)
  - *%USD* – percentage of the queue depth being actively used by the ESXi kernel ( $ACTV / QLEN * 100\%$ )

- **Configure and troubleshoot VMFS datastores using *vmkfstools***

- Here is an example of how to create a VMFS-5 datastore using *vmkfstools*

```

01 # you'll need the device ID (esxcli storage core device list)
02
03 # this command will get the current partition information, you need to see the last us
04 partedUtil get /vmfs/devices/disks/naa.5000144f60f4627a
05
06 # sample results "1305 255 63 20971520"
07
08 # in this case 20971520 is the last usable sector. To create the partition we'll use 2
09 # this command creates partition number 1, starting at 128, ending at 20971500 with a
10 partedUtil set /vmfs/devices/disks/naa.5000144f60f4627a "1 128 20971500 251 0"
11
12 # this command creates the VMFS 5 volume with a label of "vmkfstools_vcap5_volume"
13 vmkfstools -C vmfs5 -S vmkfstools_vcap5_volume /vmfs/devices/disks/naa.5000144f60f4627
14 # if you want to remove this volume via the command line you can delete the underlyin

```

```
15 partedUtil delete /vmfs/devices/disks/naa.5000144f60f4627a 1
16
17 # perform a rescan of the adapter and the volume will no longer be present
18 esxcli storage core adapter rescan -A vmhba35
19
```

- **Troubleshoot snapshot and re-signaturing issues**

- I already done an extensive write-up on VMFS resignaturing, you can find it here;[Objective 1.1 – Implement and Manage Complex Storage Solutions](#) – look about a half way down the page

- **Analyze log files to identify storage and multipathing problems**

- The log files you'll look at are the same log files I listed above. Here they are again
  - vmkernel.log — you could see the host disconnecting/reconnecting to devices
  - storagerm.log — storage I/O control information
  - vobd.log — observations made by the vmkernel
- You are going to want to look for any errors in each of these logs, and you'll want to try and do event correlation by looking at the timestamps contained within the log(s). Doing this should give you a better picture at what exactly was going on at a certain time and, hopefully, allow you to determine the root cause

## Tools

- [vSphere Command-Line Interface Concepts and Examples](#)
- [vSphere Installation and Setup Guide](#)
- [vSphere Resource Management Guide](#)
- [vSphere Troubleshooting Guide](#)
- [Product Documentation](#)
- vSphere Client / Web Client
- vSphere CLI
  - esxcli
  - resxtp / esxtp
  - vscsiStats
  - vmkfstools



# VCAP5-DCA – Objective 6.5 – Troubleshoot vCenter Server and ESXi Host Management

---

For this objective I used the following documents:

- Documents listed in the Tools section

## **Objective 6.5 – Troubleshoot vCenter Server and ESXi Host Management**

Knowledge

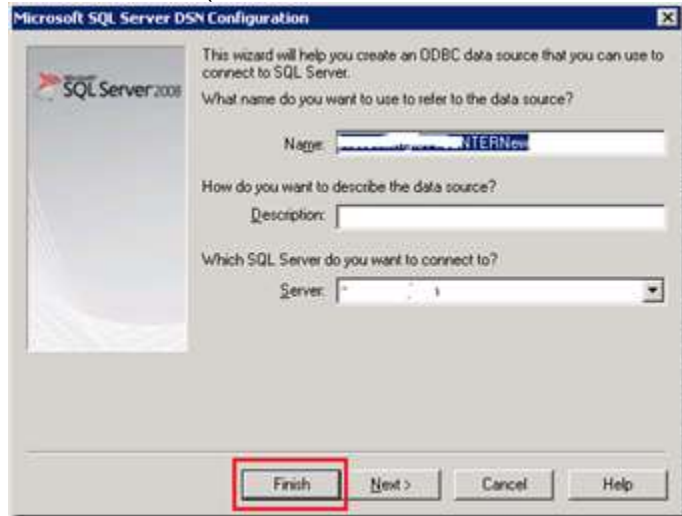
**\*\*ITEMS IN BOLD ARE TOPICS PULLED FROM THE BLUEPRINT\*\***

- **Identify CLI commands and tools used to troubleshoot management issues**
  - If you can get to the console of your ESXi hosts, you can try restarting the management agents by running the following command:
    - ***services.sh restart***

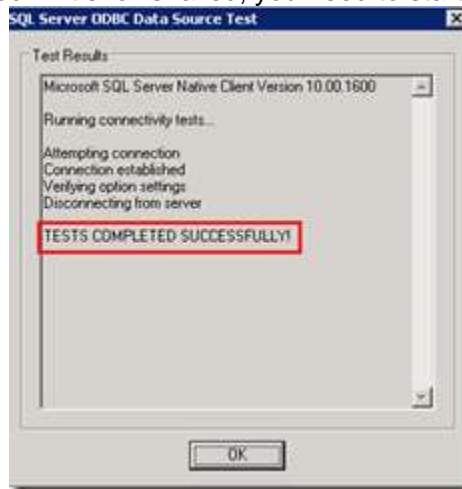
Skills and Abilities

- **Troubleshoot vCenter Server services and database connection issues**
  - The first area that I look at when troubleshooting vCenter is ensuring that the vCenter Server (assumes you are running vCenter on a Windows box and not the appliance) services are started:
    - VMware VirtualCenter Server
    - VMware VirtualCenter Management Webservices
    - vCenter Inventory Service
    - VMware vSphere Profile-Driven Storage Service
  - If the VMware VirtualCenter Server service won't start, you'll need to check a few items:
    - If you are running SQL Server Express on the vCenter server, ensure the SQL service is also started
    - If you are running the database on a separate server, ensure that server is up and the database application is up. Once you have verified this, check the ODBC connection on the vCenter Server
      - 
      - Click *Start* > select *Administrative Tools* > click *Data Sources (ODBC)*
      - Click the *System DSN* tab

- Ensure that a system data source exists. If it does exist, test the connection
- Select the data source > click *Configure...*
- Click the *Finish* button (I've taken out the name and server in the screenshot)



- Click the *Test Data Source...* button. If you see *TESTS COMPLETED SUCCESSFULLY!* then you know the connection from the vCenter server to the database is good. If it shows failed, you need to start investigating why it is failing



- **Troubleshoot ESXi Firewall**

- You can look at your firewall settings through the GUI or using **esxcli**
- Using the GUI
  - Log into the vSphere client and navigate to the *Hosts and Clusters* view
  - Select a host from the inventory tree and click on the *Configuration* tab on the right-hand side of the screen

- Under *Software*, click the *Security Profile* hyperlink
- Next to *Firewall* click the *Properties* hyperlink

The screenshot shows the 'Firewall' properties window in ESXi. It has a 'Refresh' button and a 'Properties...' button (highlighted with a red box). Below the buttons is a table titled 'Incoming Connections' with the following data:

Service	Port	Protocol	Access
CIM Server	5988	(TCP)	All
SSH Server	22	(TCP)	All
NFC	902	(TCP)	All
vMotion	8000	(TCP)	All
DHCP Client	88	(UDP)	All

- From here you can enable/disable different services
- Using **esxcli**
  - Use the following **esxcli** context for firewall related commands: **esxcli network firewall**
  - From here you can load and unload the firewall
    - **esxcli network firewall <load><unload>**
  - You can view the ruleset
    - **esxcli network firewall ruleset list**
  - You can set IP ACLs using this command
    - **esxcli network firewall ruleset allowedip <add><list><remove>**
  - You can see a full listing of all of the rules:
    - **esxcli network firewall ruleset rule list**
- **Troubleshoot ESXi host management and connectivity issues**
  - this one is pretty hard to try and write about. it is really going to depend on the symptoms you are seeing in order to even figure out where to start. However, here are a few things you can check:
    - Physical connectivity
    - IP/subnet mask
    - VLAN on the vSwitch
    - VLAN on the physical switch
    - Reported duplex settings
    - ICMP

- **Determine the root cause of a vSphere management or connectivity issue**
  - Again, this one is hard to put down on paper without knowing specific symptoms. Here are some things you can check:
    - Ensure all vCenter services are started
    - Ensure you have connectivity between your vCenter server and database (see some steps a previous section above)
    - Ensure the database is mounted and online
    - Ensure physical connectivity to the vCenter server
    - Ensure the proper VLANs are set
    - Ensure IP configuration on the vCenter server is correct
- **Utilize Direct Console User Interface (DCUI) and ESXi Shell to troubleshoot, configure, and monitor an environment**
  - From The DCUI you can:
    - Configure the management network (IP, subnet mask, default gateway)
    - Configure DNS and domain
    - If the management network exists on a virtual Distributed Switch, you can restore it to a standard switch
    - Test the management network, which does the following by default:
      - Pings the default gateway
      - Pings the primary DNS server
      - Pings the secondary DNS server
      - Tries to resolve the hostname
    - You can edit the IPs and use whatever you'd like to test the management network
    - You can view the status of the physical adapters and connect/disconnect them from the virtual Standard Switch where the management network resides
    - Restart the management network
    - restore network settings to default
    - Look at system logs in order to determine errors

# VCAP-DCA 5 Objective 7.1– Secure ESXi Hosts

## Objective 7.1 Secure ESXi Hosts

For this objective I used the following resources:

- vSphere Security Documentation
- vSphere Examples and Scenarios Documentation
- vSphere 5 Hardening Guide
- VMware KB Article 1002934 How promiscuous mode works at the virtual switch and portgroup levels
- VMware KB Article 1017910 Using Tech Support Mode in ESXi 4.1 and ESXi 5.0
- VMware KB Article 1012285 Failure to enable Fault Tolerance for a virtual machine
- VMware KB Article 1008077 Enabling or disabling Lockdown mode on an ESXi host
- VMware KB Article 2015499 Configuring CA signed certificates for ESXi 5.0 hosts
- VMware KB Article 2015383 Implementing CA signed SSL certificates with vSphere 5
- VMware KB Article 1029944 Generating custom or default SSL certificates
- VMware KB Article 2015387 Configuring OpenSSL for installation and configuration of CA signed certificates in the vSphere Environment
- VMware KB Article 1012033 ESX and ESXi 4.x and 5.x password requirements and restrictions
- VMware KB Article 2004201 Location of ESXi 5.0 log files

### Knowledge

#### **Identify virtual switch security characteristics**

MAC Address Changes – This setting affects traffic that a virtual machine receives. When the option is set to Accept (Default), ESX accepts requests to change the effective MAC address to other than the initial MAC address.

When the option is set to Reject, ESX does not honor requests to change the effective MAC address to anything other than the initial MAC address, which protects the host against MAC impersonation. The port that the virtual adapter used to send the request is disabled and the virtual adapter does not receive any more frames until it changes the effective MAC address to match the initial MAC address. The guest operating system does not detect that the MAC address change was not honored.

In some situation, you might have a legitimate need for more than one adapter to have the same MAC address on a network – for example, if you are using Microsoft Network Load

Balancing in unicast mode. When MS NLB is used in the standard multicast mode, adapters do not share MAC addresses.

*Forged Transmissions* – This setting affects traffic that is transmitted from a virtual machine. When the option is set to Accept (Default), ESX does not compare source and effective MAC addresses

To protect against MAC impersonation, you can set this option to Reject. If you do, the host compares the source MAC address being transmitted by the operating system with the effective MAC address for its adapter to see if they match. If the addresses do not match, ESX drops the packet.

The guest operating system does not detect that its virtual network adapter cannot send packets by using the impersonated MAC address. The ESX host intercepts any packets with impersonated addresses before they are delivered, and the guest operating system might assume that the packets are dropped.

*Promiscuous Mode Operation* – Promiscuous mode eliminates any reception filtering that the virtual network adapter would perform so that the guest operating system receives all traffic observed on the wire. By default, the virtual network adapter cannot operate in promiscuous mode.

Although promiscuous mode can be useful for tracking networking activity, it is an insecure mode of operation, because any adapter in promiscuous mode has access to the packets regardless of whether some of the packets are received only by a particular network adapter. This means that an administrator or root user within a virtual machine can potentially view traffic destined for other guest or host operating systems.

See page 51 of the *vSphere Networking* documentation for the procedure to how to configure these settings. For additional reading on how promiscuous mode works have a look at [VMware KB Article 1002934](#) “How promiscuous mode works at the virtual switch and portgroup levels”

### Skills and Abilities

#### **Add/Edit Remove users/groups on an ESXi host**

Adding a user to an ESXi host

- Connect directly to the ESXi host via the vSphere Client
- Click the *Users & Group* tab and click *Users*
- Right-click anywhere in the Users table and click *Add* to open the *Add New User* dialog box

- Enter a login, a user name, a numeric user ID (UID), and a password
- Specifying the user name and UID are optional. If you do not specify the UID, the vSphere Client assigns the next available UID
- Create a password that meets the length and complexity requirements. The host checks for password compliance using the default authentication plug-in, pam\_passwdqc.so. If the password is not compliant, the following error appears: A general system error occurred: passwd: Authentication token manipulation error.
- To allow a user access to access the ESX host through a command shell, select Grant shell access to this user
- To add the user to a group, select the group name from the Group drop-down menu and click Add
- Click *OK*

#### Edit a user account on an ESXi host

- Connect directly to the ESX host via the vSphere Client
- Click the Users & Groups tab and click Users
- Right-click the user and click Edit to open the Edit User dialog box
- To change the user ID, enter a numeric user UID in the UID text box
- Enter a new user name
- To change the user's password, select Change Password and enter the new password
- Create a password that meets the length and complexity requirements. The host checks for password compliance using the default authentication plug-in, pam\_passwdqc.so. If the password is not compliant, the following error appears: A general system error occurred: passwd: Authentication token manipulation error
- To change the user's ability to access the ESX host through a command shell, select or deselect Grant shell access to this user
- To add the user to a group, select the group name from the Group drop-down menu and click Add
- To remove the user from a group, select the group name from the Group membership box and click Remove
- Click *OK*

#### Remove a User or Group

- Connect directly to the ESX host via the vSphere Client
- Click the Users & Groups tab and click Users or Groups
- Right-click the user or group to remove and select Remove

## Adding a Group to an ESXi host

- Connect directly to the ESX host via the vSphere Client
- Click the Users & Groups tab and click Groups
- Right-click anywhere in the Group table and click Add to open the Create New Group dialog box
- Enter a group name and numeric group ID (GUI) in the Group ID text box
- For each user that you want to add as a group member, select the user name from the list and click Add
- Click OK

## Add or Remove Users from a Group

- Connect directly to the ESX host via the vSphere Client
- Click the Users & Groups tab and click Groups
- Right-click the group to modify and select Properties to open the Edit Group dialog box
- To add the user to a group, select the group name from the Group drop-down menu and click Add
- To remove the user from a group, select the group name from the Group membership box and click Remove
- Click OK

## Customize SSH settings for increased security

By default SSH access to an ESXi host is disabled by default and gone are the days of “ESX Classic” and manipulating the `sshd.config` file to allow the ‘root’ account SSH access. In ESXi you can enable SSH access either via the vSphere Client or at the Direct Console User Interface. See [VMware KB Article 1017910](#) “Using Tech Support Mode in ESXi 4.1 and ESXi 5.0” on how to enable SSH as well as set the SSH timeout values.

## Enable/Disable certificate checking

To prevent man-in-the-middle attacks and to fully use the security that certificates provide, certificate checking is enabled by default. Note that certificate checking is required to use VMware Fault Tolerance (see [VMware KB Article 1012285](#) “Failure to enable Fault Tolerance for a virtual machine”).

Procedure – Taken from page 72 of the *vSphere Security* documentation

- Log in to the vCenter Server system using the vSphere Client
- Select *Administration* -> *vCenter Server Settings*
- Click *SSL Settings* in the left pane and verify that *Check host certificates* is selected



- If there are hosts that require manual validation, compare the thumbprints listed for the hosts to the thumbprints in the host console (see below)
- If the thumbprint matches, select *Verify* check box next to the host
- Click *OK*

To obtain the host thumbprint using the Direct Console User Interface

- Log in to the direct console and press *F2* to access the *System Customization* menu
- Select *View Support Information*
- The host thumbprint appears in the column on the right

### **Generate ESXi host certificates**

Procedure – Taken from page 72 of the *vSphere Security* documentation

- Log in to the ESXi Shell and acquire root privileges
- In the directory */etc/vmware/ssl*, back up any existing certificates by renaming them using the following commands:
  - `mv rui.crt orig.rui.crt`
  - `mv rui.key orig.rui.key`
- Run the command `/sbin/generate-certificate` to generate new certificates
- Run the command `/etc/init.d/hostd restart` to restart the *hostd* process
- Confirm that the host successfully generated new certificates by using the following command and comparing the time stamps of the new certificate files with *orig.rui.crt* and *orig.rui.key*
- `ls -la`

### **Enable ESXi lockdown mode**

When you enable lockdown mode, no users other than *vpxuser* have authentication permissions, nor can they perform operations against the host directly. Lockdown mode forces all operations to be performed through vCenter Server. This includes running vCLI commands or using the vMA against the host. You can enable lockdown mode using the Add Host wizard to add an ESXi host to vCenter Server, using the vSphere Client to manage a host, or using the direct console user interface.

**Note** – *If you enable or disable lockdown mode using the direct console user interface, permissions for users and groups on the host are discarded. To preserve these permissions, you must enable and disable lockdown mode using the vSphere Client connect to vCenter Server*

Enabling lockdown mode affects which users are authorized to access host services. The chart below list which services can be used by different types of users when the host is running in lockdown mode, compared to when the host is running in normal mode:

Service	Normal Mode	Lockdown Mode
vSphere WebServices API	All users, based on ESXi permissions	vCenter only (vpxuser)
CIM Providers	Root users and Admin Users	vCenter only (ticket)
Direct Console User Interface	Root users and Admin Users	Root users
ESXi Shell	Root users and Admin users	No users
SSH	Root users and Admin users	No users

Procedure – Taken from page 82 and 83 of the *vSphere Security* documentation  
Using the vSphere Client

- Log in to a vCenter Server system using the vSphere Client
- Select the host in the inventory panel
- Click the *Configuration* tab and click *Security Profile*
- Click the *Edit* link next to lockdown mode
- Select *Enable Lockdown Mode*
- Click *Ok*

Using the Direct Console User Interface (DCUI)

- At the DCUI of the host, press *F2* and log in
- Scroll to the *Configure Lockdown Mode* setting and press *Enter*
- Press *ESC* until you return to the main menu of the DCUI

For further reading on Lockdown Mode see pages 81 thru 83 of the *vSphere Security* documentation. Also see [VMware KB Article 1008077](#) “Enabling or disabling Lockdown mode on an ESXi host” to enable/disable lock down mode using *vim-cmd* as well as PowerCLI.

### Replace default certificate with CA-signed certificate

This is one of those topics that goes far into great detail and has been well documented by others in the VMware community as well as several VMware KB articles. Below is the procedure outlined in the *vSphere Security* documentation as well several other resources I would strongly recommend reading as well.

Procedure – Taken from page 73 of the *vSphere Security* documentation

- Log in to the ESXi Shell and acquire root privileges
- In the directory */etc/vmware/ssl*, back up any existing certificates by renaming them using the following commands:
  - `mv rui.crt orig.rui.crt`
  - `mv rui.key orig.rui.key`
- Copy the new certificate and key to */etc/vmware/ssl*
- Rename the new certificate and key to *rui.crt* and *rui.key*
- Restart the *hostd* process
  - `/etc/init.d/hostd restart`

For additional reading/information on using CA–signed certificates take a look at the following:

- [VMware KB Article 2015499](#) “Configuring CA signed certificates for ESXi 5.0 hosts”
- [VMware KB Article 2015383](#) “Implementing CA signed SSL certificates with vSphere 5”
- [VMware KB Article 1029944](#) “Generating custom or default SSL certificates”
- [VMware KB Article 2015387](#) “Configuring OpenSSL for installation and configuration of CA signed certificates in the vSphere environment”

### **Configure SSL timeouts**

Timeout periods can be set for two types of idle connections:

- The Read Timeout setting applies to connections that have completed the SSL handshake process with port 443 of ESXi
- The Handshake Timeout setting applies to connections that have not completed the SSL handshake process with port 443 of ESXi

Procedure – Taken from page 75 of the *vSphere Security* documentation

- Log in to the ESXi Shell and acquire root privileges
- Change to the directory */etc/vmware/hostd*
- Use a text editor to open the *config.xml* file
- Enter the `<readTimeoutsMs>` value in milliseconds
- Enter the `<handshakeTimeoutMs>` value in milliseconds
- Save your changes and close the file
- Restart the *hostd* process:
  - `/etc.init.d/hostd restart`

### **Configure vSphere Authentication Proxy**

The *vSphere Authentication Proxy* allows for better security in environments that plan on leveraging either PXE booting hosts or utilizing VMware AutoDeploy. It does this by eliminating the need to store Active Directory credentials with the host configuration. The installation and configuration of the proxy is a multi-step process that has been outlined on pages 65 thru 69 of the “*vSphere Security*” documentation. Rather than re-type the steps I will refer you to that document.

### **Enable strong passwords and configure password policies**

Password strength and complexity – By default ESXi uses the *pam\_passwdqc.so* plugin to set the rules that users must observe when creating passwords and to check password strength. To configure password complexity, you can change the default value of the following parameters:

- *N0* –Is the number of characters required for a password that uses characters from only one character class. For example, the password contains only lowercase letters
- *N1* – Is the number of characters required for a password that uses characters from two character classes
- *N2* –Is used for passphrases. ESXi requires three words for a passphrase. Each word in the passphrase must be 8 to 40 characters long
- *N3* –Is the number of characters required for a password that uses characters from three character classes
- *N4* –Is the number of characters required for a password that uses characters from all four character classes
- *match* –Is the number of characters allowed in a string that is reused from the old password. If the *pam\_passwdqc.so* plugin finds a reused string of this length or longer, it disqualifies the string from the strength test and uses only the remaining characters
- *retry* – Is the number of times a user is prompted for a new password if the password candidate is not sufficiently strong

Procedure – Taken from page 93 of the *vSphere Security* documentation

- Log in to the ESXi Shell and acquire root privileges
- Open the *passwd* file with a text editor
- Edit the following line
  - *password requisite /lib/security/\$ISA/pam\_passwdqc.so retry=N min=N0,N1,N2,N3.N4*
- Save the file

[VMware KB Article 1012033](#) “ESX and ESXi 4.x and 5.x password requirements and restrictions” covers the same steps as well as provides an example.

### **Identify methods for hardening virtual machines**

Suggestions take from the *vSphere Security* documentation (as well as procedures to implement) starting on page 87:

- Install antivirus software
- Disable copy and past to the clipboard
- Remove unnecessary hardware devices
- Limiting guest operating system writes to host memory

For additional security settings covering VMs, ESXi hosts, networking, and vCenter I STRONGLY suggest taking a look at the VMware “vSphere 5 Hardening Guide” located [HERE](#).

### **Analyze logs for security-related messages**

Review [VMware KB Article 2004201](#) “*Location of ESXi 5.0 log files*”. The article covers each of the host log files and tools that can be used to view them.

### **Manage Active Directory integration**

Procedure – Taken from page 67 of the *vSphere Security* documentation

- Select a host in the vSphere Client inventory, and click the *Configuration* tab
- Click *Properties*
- In the Directory Services Configuration dialog box, select the directory service from the drop-down menu
- Enter a domain
- Click *Join Domain*
- Enter the user name and password of a directory service user who has permissions to join the host to the domain, and click *OK*
- Click *OK* to close the Directory Services Configuration dialog box

Jason Boche ([blog](#) / [twitter](#)) has put together a post outlining how to place a host in a specific AD OU when joining it to your domain. That post is located [HERE](#). If you are or planning on using VMware Host Profiles to manage your ESXi systems have a look at page 41 of the “VMware *vSphere Examples and Scenarios*” documentation. It will outline the proper configuration steps needed.

# VCAP-DCA 5 Objective 7.2–Configure and Maintain the ESXi Firewall

## Objective 7.2 – Configure and Maintain the ESXi Firewall

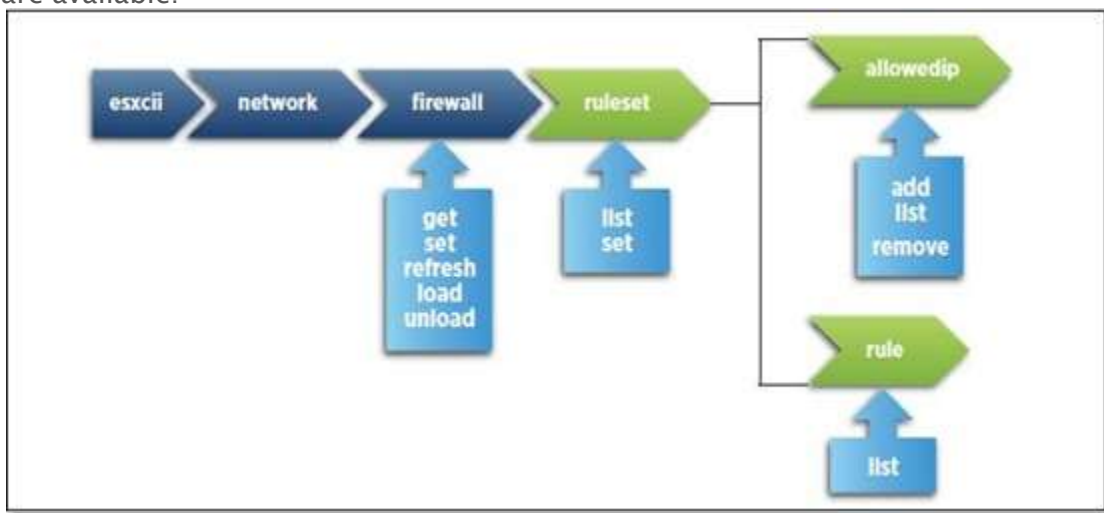
For this objective I used the following resources:

- VMware “What’s New in VMware vSphere 5.0 – Platform
- VMware KB Article 2005284 “About the ESXi 5.0 Firewall”
- Eric Sloof’s Blog
- William Lam’s Blog

### Knowledge

#### Identify esxcli firewall configuration commands

New in ESXi 5 is a *esxcli firewall* command namespace. The diagram below taken from VMware “What’s New in VMware vSphere 5.0 – Platform” outlines the new commands that are available:



For additional informational on the firewall namespaces see [VMware KB Article 2005284](https://kb.vmware.com/s/article/2005284) “About the ESXi 5.0 Firewall”

#### Explain the three firewall security levels

- High Security (Default) – Firewall is configured to block all incoming and outgoing traffic, except for ports 22,123,427,443,902,5989, and 5988. These are ports used for basic ESXi communication
- Medium Security – All incoming traffic is blocked, except on the default ports and any ports you specifically open. Outgoing traffic is not blocked

- Low Security – There are no ports blocked on either incoming or outgoing traffic. This setting is equivalent to removing the firewall

Skills and Abilities

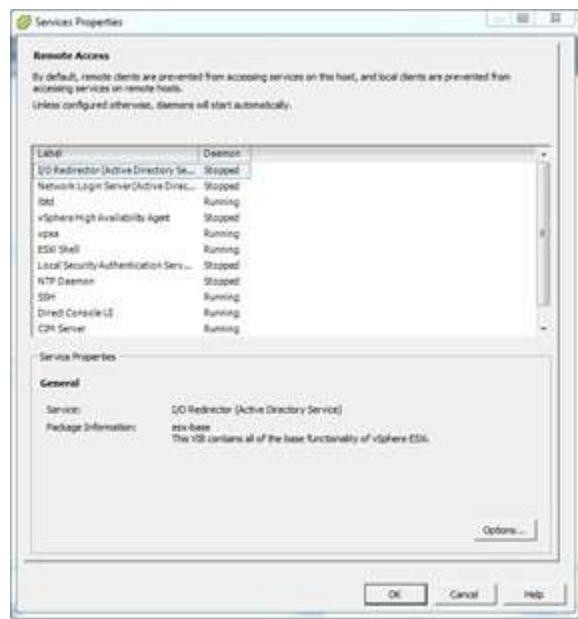
**Enable/Disable pre-configured services**

**Configure service behavior automation**

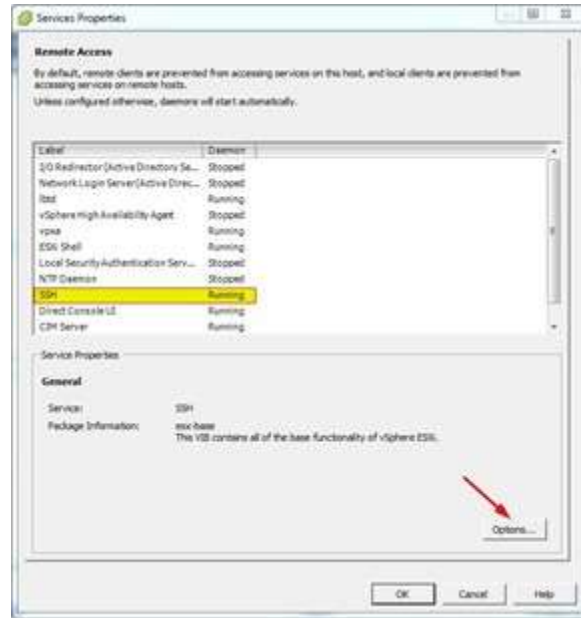
I am going to combine these two sections as you will end up in the same place to to accomplish both of these tasks.

Procedure

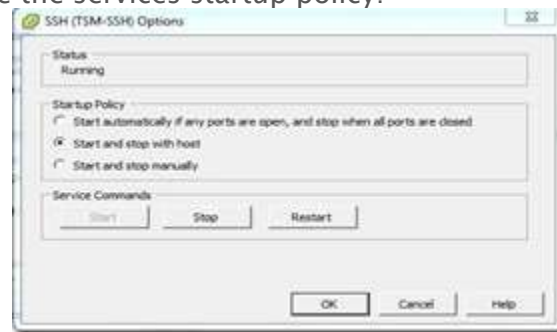
- Log into a vCenter Server system using the vSphere Client
- Select a host in the inventory panel
- Click the *Configuration* tab
- Under the *Software* section select *Security Profile*
- In the upper right hand corner of the *Services* section click *Properties* to see a list of services:



- Select the service you wish to edit and click *Options* in the lower right hand corner:



- The service options dialog will be displayed. From here you can select to start/stop/restart the service and configure the services startup policy:

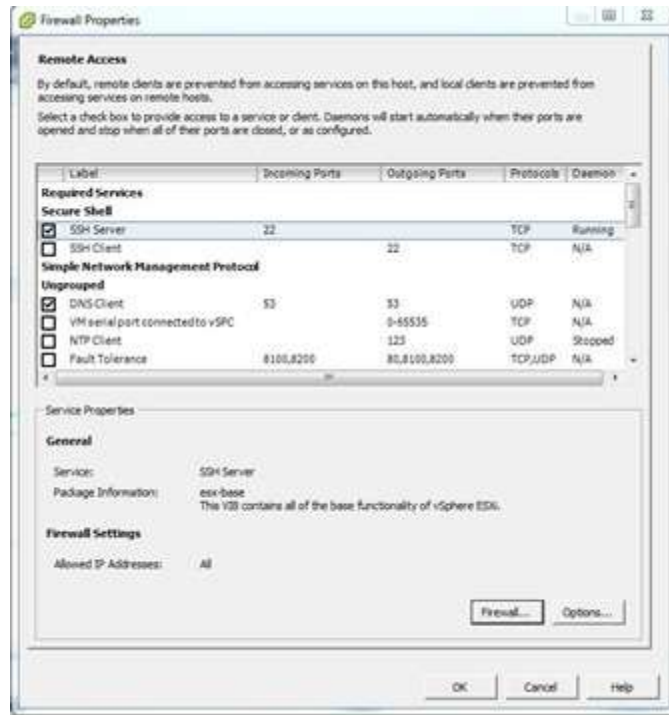


## Open/Close ports in the firewall

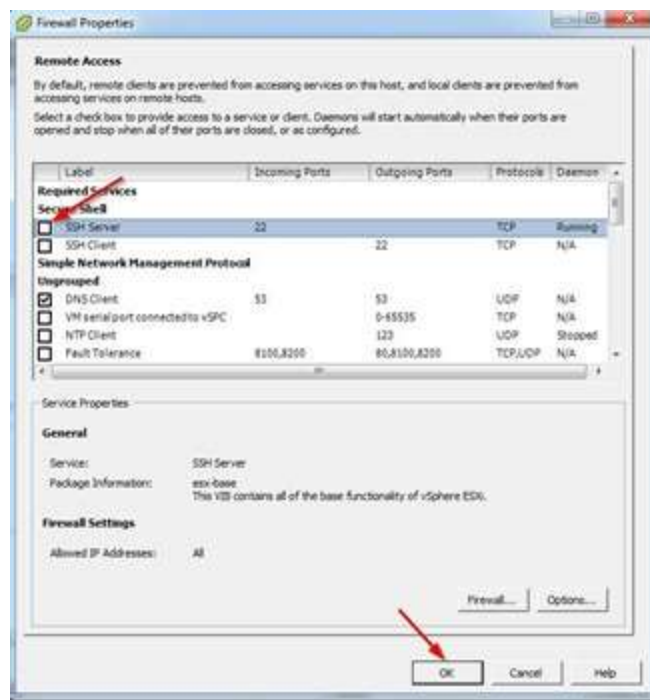
### Procedure

- Log into a vCenter Server system using the vSphere Client
- Select a host in the inventory panel
- Click the *Configuration* tab
- Under the *Software* section select *Security Profile*
- Towards the center of your screen in the *Firewall* section click *Properties*
- The *Firewall Properties* page will be displayed:





- Open or close a firewall port “check” the box next to the name of the service and click “OK” to apply the change. In the example below I am closing the firewall port for the “SSH Server”:



Eric Sloof ([blog](#) / [twitter](#)) has put together outline the above steps. That video is located [HERE](#).

Create a custom service

William Lam ([blog](#) / [twitter](#)) has a blog post outlining this procedure. Instead of reinventing the wheel (and probably not as good) have a look at William's post located [HERE](#).

# VCAP-DCA5 Objective 8.1 – Execute VMware Cmdlets and Customize Scripts Using PowerCLI

THIS SECTION WAS COMPLETED BY CONRAD RAMOS -- THANKS CONRAD FOR CONTRIBUTING!

Hey [vNoob](#) here; Helping out Jason and Josh by doing an objective for them. Hope it is helpful

**Objective 8.1 – Execute VMware Cmdlets and Customize Scripts Using PowerCLI**  
Knowledge

## **Identify vSphere PowerCLI requirements**

Directly from the vmware website for [PowerCLI 5.1 release notes](#):

To use VMware vSphere PowerCLI, you need to have installed the following software:

- Windows PowerShell 2.0
- A supported version of .NET Framework
  - .NET Framework 2.0 with Service Pack 2
  - .NET Framework 3.0 or .NET Framework 3.0 with Service Pack 1, or Service Pack 2
  - .NET Framework 3.5 or .NET Framework 3.5 with Service Pack 1

## **Identify Cmdlet concepts**

[http://msdn.microsoft.com/en-us/library/windows/desktop/ms714395\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms714395(v=vs.85).aspx)

- A cmdlet is a lightweight command that is used in the Windows PowerShell environment. The Windows PowerShell runtime invokes these cmdlets within the context of automation scripts that are provided at the command line. The Windows PowerShell runtime also invokes them programmatically through Windows PowerShell APIs.
- Windows PowerShell uses a verb-and-noun name pair to name cmdlets. For example, the Get-Command cmdlet included in Windows PowerShell is used to get all the cmdlets that are registered in the command shell. The verb identifies the action that the cmdlet performs, and the noun identifies the resource on which the cmdlet performs its action.

## **Identify environment variables usage**

- Environment Variables are usually used as shortcuts to common paths that are found on a computer. Environment Variables are stored in the [PSDrive](#) Env.

- To find which environment variables are available to use, at a powershell prompt type “Get-ChildItem Env:” To which the output will look similar to this:

Name	Value
----	-----
ALLUSERSPROFILE	C:\ProgramData
APPDATA	C:\Users\Username\AppData\Roaming
CommonProgramFiles	C:\Program Files\Common Files
CommonProgramFiles(x86)	C:\Program Files (x86)\Common Files
CommonProgramW6432	C:\Program Files\Common Files
COMPUTERNAME	W7D-Name
ComSpec	C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK	NO
HOMEDRIVE	C:
HOMEPATH	\Users\Username
LOCALAPPDATA	C:\Users\Username\AppData\Local
LOGONSERVER	\\MicrosoftAccount
NUMBER_OF_PROCESSORS	8
OS	Windows_NT
Path	C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common;C:\W
\WINDOWS...	
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.CPL
PROCESSOR_ARCHITECTURE	AMD64
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 42 Stepping 7, GenuineIntel
PROCESSOR_LEVEL	6
PROCESSOR_REVISION	2a07
ProgramData	C:\ProgramData
ProgramFiles	C:\Program Files
ProgramFiles(x86)	C:\Program Files (x86)
ProgramW6432	C:\Program Files
PSModulePath	C:\Users\Username\Documents\WindowsPowerShell\Modules;C:\W
\system32\WindowsPowerS...	
PUBLIC	C:\Users\Public
SESSIONNAME	Console
SystemDrive	C:
SystemRoot	C:\WINDOWS
TEMP	C:\Users\Username\AppData\Local\Temp
TMP	C:\Users\Username\AppData\Local\Temp
USERDOMAIN	W7D-Username
USERDOMAIN_ROAMINGPROFILE	W7D-Username
USERNAME	Username
USERPROFILE	C:\Users\Username
windir	C:\WINDOWS

- In order to use the listed Environment Variables “\$env:” should be place in the front

For example

```
PS T:\> cd $env:commonprogramfiles
PS C:\Program Files\Common Files>
```

## Skills and Abilities

### **Install and configure vSphere PowerCLI**

- Download the latest version of vSphere PowerCLI from the VMware Web site.
- Navigate to the folder that contains the vSphere PowerCLI installer file you downloaded and double-click
- the executable file.
- If the installation wizard detects an earlier version of vSphere PowerCLI on your system, it will attempt
- to upgrade your existing installation.
- On the Welcome page, click Next.
- On the VMware Patents page, click Next.
- Accept the license agreement terms and click Next.
- On the Custom Setup page, select the components that you want to install.
- Option Description
  - vSphere PowerCLI Installs a set of cmdlets for managing vSphere features. This vSphere PowerCLI component is mandatory and selected by default.
  - vCloud Director PowerCLI Installs a set of cmdlets for managing vCloud Director features.
- (Optional) On the Custom Setup page, click Change to select a different location to install
- vSphere PowerCLI.
- Click Next.
- On the Ready to Install the Program page, click Install to proceed with the installation.
- Click Finish to complete the installation process.

### **Install and configure Update Manager PowerShell Library**

You can download the Update Manager PowerCLI installer package from the [product landing page](#).

- To install the Update Manager PowerCLI
- Start the Update Manager PowerCLI installer.
- Click Next in the Welcome page to continue with the installation.
- Read and accept the license agreement terms.
- Click Install.
- Click Finish to complete the installation process.

### **Use basic and advanced Cmdlets to manage VMs and ESXi Hosts**

- For more examples please refer to the [PowerCLI User's Guide](#)
- After connecting to the vCenter Server with "connect-viserver \$vcenterservername", you can retrieve information about the vms and hosts by using the two basic commands "Get-VM and Get-VMHost".

- Directly from the Get-Help of set-vm and set-vmhost

*C:|PS>Get-VM -Location ResourcePool01 | Set-VM -MemoryGB 2 -NumCPU 2*

-Upgrades the memory and CPU count of the virtual machines in ResourcePool01.

*C:|PS>Set-VM \$vm -Name "Web Server" -GuestID winNetStandardGuest -Description "Company's web server"*

-Changes the name, description, and guest ID of the specified virtual machine.

*C:|PS>Set-VMHost -VMHost Host -State "Disconnected"*

-Resets the state of the Host virtual host to disconnected.

### Use Web Service Access Cmdlets

- The get-view and the get-viobjectbyviview are considered the Web Services Access Cmdlets
- Both of these cmdlets function to access/manipulate the underlying .Net objects or PowerCLI
- Get-View takes a Powershell VIOject and converts it to a vSphere .Net View Object. Get-VIOjectByVIView does just the opposite.
- "Using the Web Service Access cmdlets for low-level VMware vSphere management requires some knowledge of both PowerShell scripting and the VMware vSphere API."[quote](#)

*Get-View -viewtype "VirtualMachine"*

-Returns the vSphere .Net view objects of all the virtual machines

*\$view=Get-View -viewtype "VirtualMachine"*

*Get-VIOjectByVIView \$view*

-Stores the previous example's result in the variable \$view, then converts it back to the standard PowerShell VIOject

### Use Datastore and Inventory Providers

- The Datastore and Inventory Providers allow you to browse the the default datastore drives
- Using the cmdlet Get-PSDrive you should see two psdrives listed, vmstore and vmstores
- VMstore is the last connected vCenter Server, and VMStores is the currently connected vCenter Server
- PSDrives are great because they operate much like one would navigate an operating system via commandline.(Case-Sensitive)

```
PS C:\power> get-psdrive
```

Name	Used (GB)	Free (GB)	Provider	Root
A			FileSystem	A:\
AD			ActiveDire...	//RootDSE/
Alias			Alias	
C	39.31	.59	FileSystem	C:\
D			FileSystem	D:\
E			FileSystem	E:\
Env			Environment	
Function			Function	
HKCU			Registry	HKEY_CURRENT_USER
HKLM			Registry	HKEY_LOCAL_MACHINE
Variable			Variable	
vi			VimInventory	\LastConnectedVCenterServer
vis			VimInventory	\
vmstore			VimDatastore	\LastConnectedVCenterServer
vmstores			VimDatastore	\

```
PS C:\power> cd vmstore:
```

```
PS vmstore:\> dir
```

Name	Type	Id
Test	Datacenter	Datacenter-d...

```
PS vmstore:\> cd Test
```

```
PS vmstore:\Test> dir
```

Name	FreeSpaceGB	CapacityGB
Datastore1	118.977	134.750
Datastore2	124.710	134.750

Given a sample script, modify the script to perform a given action

Let's look at an example we used earlier

**Get-VM -Location ResourcePool01 | Set-VM -MemoryGB 2**

- This example is great if we only want to ever change the memory allocated to VMs in ResourcePool01, but if we know this will be something we are going to use over and over again to individual VMs, let make it a bit more usable.

- Put this into a txt file  
*Param(\$vm, [int]\$value)*  
*Get-VM \$vm | Set-VM -MemoryGB \$value*
- Name the text file something easy like “setvmgb.ps1” The ps1 extension denotes a powershell file. The param(\$vm) states that \$vm will be our parameter for the vm used, and [int]\$value will be the integer used. This makes the script much more usable and versatile. So let’s try it out

*./setvmgb.ps1 -vm myfirstvm -value 3*

-Will set the vm “MyFirstVM” to have 3GB

*./setvmgb.ps1 -vm “myfirstvm”, “mysecondvm” -value 2*

-Will set “MyFirstVM” and “MySecondVM” to have 2gb

*./setvmgb -vm (Get-vm -location ResourcePool01) -value 2*

-With “Get-vm -location ResourcePool01” we grab all the VMs in that resource pool, and set them to 2GB



# VCAP-DCA 5 Objective 8.2—Administer vSphere Using the vSphere Management Assistant

## Objective 8.2 – Administer vSphere Using the vSphere Management Assistant

For this objective I used the following resources:

- vSphere Management Assistant Guide  
Additional Resources
- ProfessionalVMware.com has covered this objective in the #vBrownBag VCAP-DCA5 series. Video is located [HERE](#).

### Knowledge

#### **Identify vMA prerequisites**

- Hardware Requirements
  - ESXi host supporting 64-bit guest OS
  - AMD Opteron, rev E or later processor
  - Intel processors with EM64T support with VT enabled
  - 3GB of storage space
- Software Requirements
  - vSphere 5.0
  - vSphere 4.1 or later
  - vSphere 4.0 Update 2 or later
  - vCenter Application 5.0

#### **Determine when vMA is needed**

- Used to remotely manage ESXi hosts
- Central location to execute system management scripts

### Skills and Abilities

#### **Install and configure vMA**

Install – Procedure taken from page 13 of the *VMware vSphere Management Assistant Guide*

- Use a vSphere Client to connect to a system that is running the supported version of ESXi or vCenter Server
- If connected to a vCenter Server system, select the host to which you want to deploy vMA in the inventory pane
- Select File -> Deploy OVF Template

- The Deploy OVF Template wizard appears
- Select Deploy from file if you have already downloaded and unzipped the vMA virtual appliance package
- Click Browse, select the OVF, and click Next
- Click Next when the download details are displayed
- Accept the license agreement
- (Optional) Specify a name for the virtual machine
- Select a location for the virtual machine when prompted
- If you are connected to a vCenter Server system, you can select a folder
- If connected to a vCenter Server system, select the resource pool for the virtual machine
- By default, the top-level root resource pool is selected
- If prompted, select the datastore to store the virtual machine on and click Next
- Select the network mapping and click Next
- Choose the IP Address Allocation (Fixed, Transient, or DHCP)
- If you choose Fixed, enter the IP address information on the following screen
- Review the information and click Finish

Configure – When the OVF has been deployed and the vMA powered on open the console for the VM to finish the base configuration. You will be prompted during first boot for the following:

- Network configuration – Allows you to set the vMA to use either DHCP or a static IP address
- Password – Set the password for the *vi-admin* account
- Timezone – After last two are configured and the vMA finishes booting from the console menu screen you can set the timezone.

#### **Add/Remove target servers**

Add a vCenter Server as a target server for AD Authentication:

- Log into vMA as vi-admin
- Add the vCenter target server using the following command:
  - *vifp addserver <FQDN of Host> -authpolicy adauth -username <Domain> | <UserName>*
- Verify that the target server has been added using the following command:
  - *vifp listservers -long*

Add a vCenter Server as a target server for Fastpass Authentication

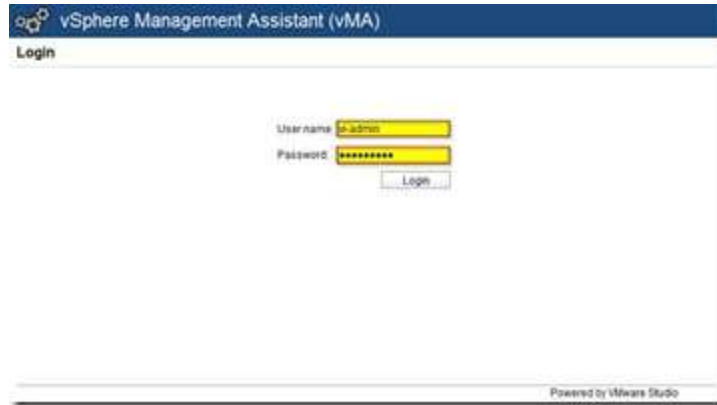
- Log in to vMA as vi-admin
- Add a server as a vMA target by running the following command:

- #vifp addserver <FQDN of Host> -authpolicy fpauth
- Specify the username when prompted
- Specify the password for that user when prompted
- Review and accept the security risk information
- Verify that the target server has been added
- #vifp listservers -long  
Add an ESXi host as a vMA target server
- Log in to vMA as vi-admin'
- Run addserver to add a server as a vMA target
- #vifp addserver <FQDN of Host>
- You are prompted for the target server's root user password
- #root@<servername>'s password
- Specify the root password for the ESX/ESXi host that you want to add
- Verify that that target server has been added:
- #vifp listservers
- Set the target as the default for the current session
- #vifptarget -set | -s <server>
- Verify that you can run a vSphere CLI command without authentication by running a command, for example
- vicfg-nics -l

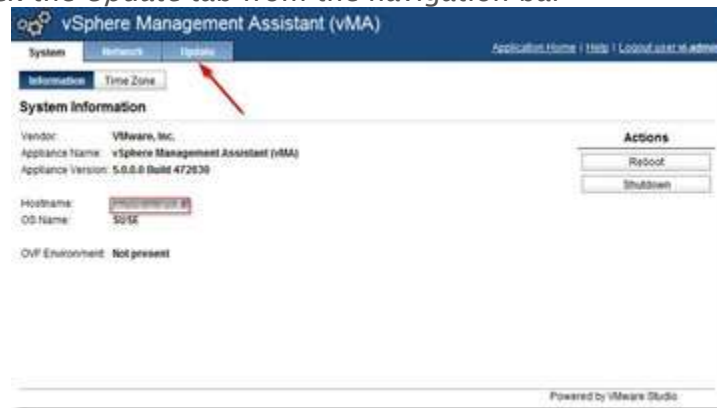
### **Perform updates to the vMA**

Unlike previous versions of the vMA, the update procedure is done using a Web UI as opposed to from the command line:

- Point your web browser to the FQDN or IP address of your vMA followed by a /5480:
- <http://myvma.company.local/5480>
- The Web UI login page will be displayed. Enter the *vi-admin* username and password and click *Login*



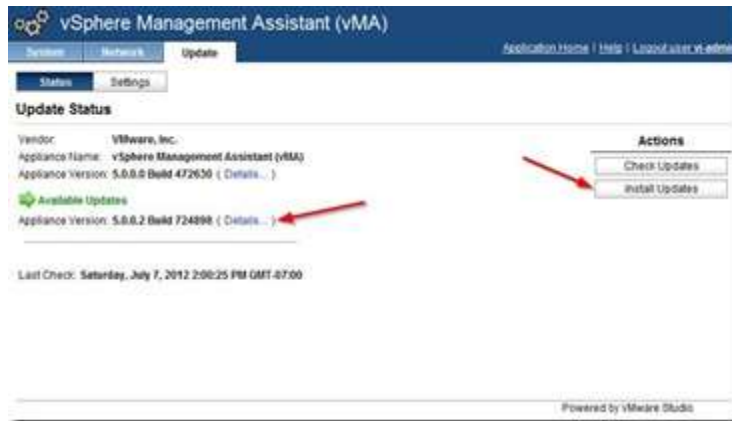
- Once logged in click the *Update* tab from the navigation bar



- In the right hand side of the screen under *Actions* click the *Check Updates* button:



- If any update are available they will be displayed and with the option to see details about them. To install the updates click *Install Updates* located under *Actions*



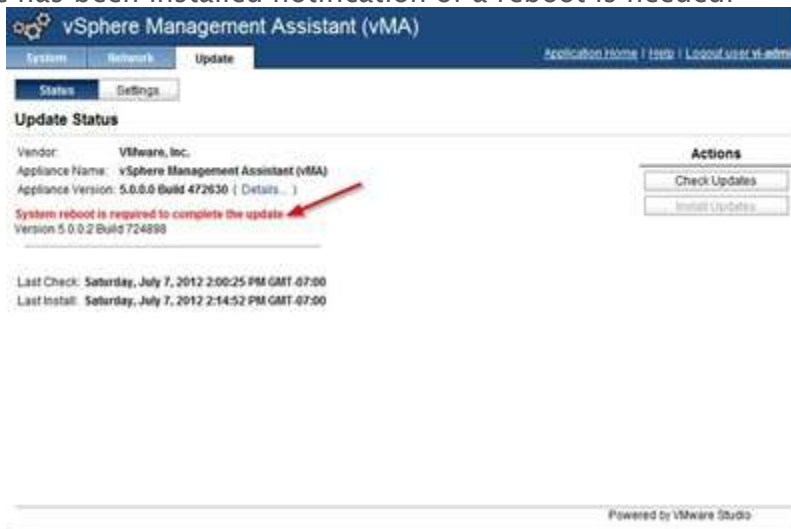
- Click yes on the *Install Update* dialog window:



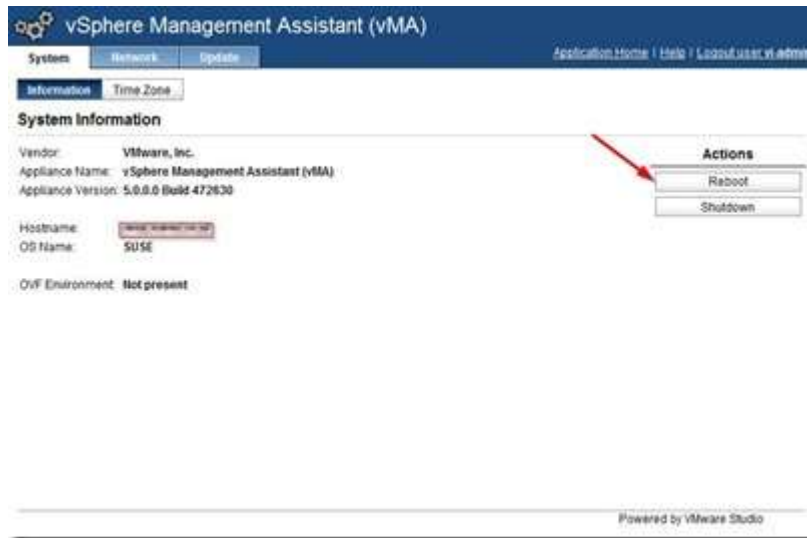
- The updates will begin installing



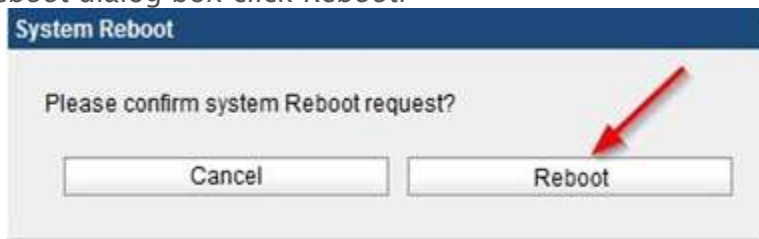
- Once the update has been installed notification of a reboot is needed:



- From the navigation menu select the *System* tab and under *Actions* click *Reboot*.



- On the *System Reboot* dialog box click *Reboot*.



## Use *vmkfstools* to manage VMFS datastores

### vmkfstools File system Command Options

Option	Description
-blocksize	Uses the specified size for the file system creation. Used with -createfs
-b	
-createfs	
-C	Creates a VMFS file system
-queryfs	
-P	Lists attributes of a file system
-setfsname	Sets the label for the file system. Used with -createfs
-S	
-spanfs	Extends the VMFS file system

-Z

## vmkfstools Virtual Disk Options

Option	Description
-adaptype -a	Uses the specified type for disk creation
-clonevirtualdisk -i	Clones the specified virtual disk
-createrdm -r	Maps a raw disk to a file on a VMFS files system
-createrdmpassthru -z	Maps a passthrough raw disk to a file on a VMFS file system
-createvirtualdisk -c	Creates a virtual disk
-deletevirtualdisk -U	Deletes the specified virtual disk
-diskformat -d	Uses the specified format for disk creation
-extendvirtualdisk -X	Extends the specified virtual disk
-geometry -X	Extends the specified virtual disk
-inflatedisk -j	Converts a thin virtual disk to eagerzeroedthick format, preserving all existing data

-renamevirtualdisk	Renames the specified virtual
-E	disk
-writezeros	Cleans the virtual disk by
-w	writing zeroes over all its
	data

Below is an example of using *vmkfstools*. In the screen shot I am creating a new VMDK named *vcap-dca* that is 5GB in size and is a thin provisioned disk. I have already navigated to the VM's directory on the datastore:

```

/vmfs/volumes/4f878fa9-2d0da0f4-be0a-bcaec54e97bd/vesx01 # vmkfstools -c 5G -d t
hin vcap-dca.vmdk
Create: 100% done.
/vmfs/volumes/4f878fa9-2d0da0f4-be0a-bcaec54e97bd/vesx01 # ls
vcap-dca-flat.vmdk  vesx01.vmd  vmware.log
vcap-dca.vmdk      vesx01.vmx
vesx01.nvram       vesx01.vmx
/vmfs/volumes/4f878fa9-2d0da0f4-be0a-bcaec54e97bd/vesx01 #

```

## Use *vmware-cmd* to manage VMs

Remote Connection String

```
#vmware-cmd -server <Host> -username root <command>
```

Server operations

```
vmware-cmd -l
```

```
vmware-cmd -s register <config_file_path> <datacenter> <resource pool>
```

```
vmware-cmd -s unregister <config_file_path>
```

VM Operations

```
vmware-cmd <cfg> getstate
```

```
vmware-cmd <cfg> start <powerop_mode>
```

```
vmware-cmd <cfg> stop <powerop_mode>
```

```
vmware-cmd <cfg> reset <powerop_mode>
```

```
vmware-cmd <cfg> suspend <powerop_mode>
```

```
vmware-cmd <cfg> setguestinfo <variable> <value>
```

```
vmware-cmd <cfg> getguestinfo <variable>
```

```
vmware-cmd <cfg> getproductinfo <prodinfo>
```

```
vmware-cmd <cfg> connectdevice <device_name>
```



```

vmware-cmd <cfg> disconnectdevice <device_name>
vmware-cmd <cfg> getconfigfile
vmware-cmd <cfg> getuptime
vmware-cmd <cfg> answer
vmware-cmd <cfg> gettoolslastactive
vmware-cmd <cfg> hassnapshot
vmware-cmd <cfg> createsnapshot <name> <description> <quiesce> <memory>
vmware-cmd <cfg> revertsnapshot
vmware-cmd <cfg> removesnapshots

```

## Use *esxcli* to manage ESXi Host configurations

See [Objective 1.3 - Configure and Manage Complex Multipathing and PSA Plugins](#) for *esxcli* command examples.

## Troubleshoot common vMA errors and conditions

Troubleshooting chart taken from page 24 of the *VMware vSphere Management Assistant Guide* documentation.

### Troubleshooting vMA

You can find troubleshooting information for all VMware products in VMware Knowledge Base articles and information about vMA known issues in the release notes. Table 2-3 explains a few commonly encountered issues that are easily resolved.

Table 2-3. Troubleshooting vMA

Issue	Resolution
You can deploy vMA but when you start up the virtual machine, an error occurs.	Check whether your setup meets the hardware and software requirements listed in "Hardware Requirements" on page 12.
You add a server but the vSphere CLI command or Perl script still prompts for authentication.	Run <code>viforget</code> for the target server.
You have added multiple servers. You do not know where vMA runs vSphere CLI commands if you do not specify <code>--server</code> .	After a call to <code>viforget</code> , your prompt changes to include the current target.
You want to enable DNS resolution in vMA.	You can configure the DNS resolution name server for vMA by updating the <code>/etc/resolv.conf</code> file. Add the following line for each DNS server in your network: <code>nameserver &lt;dns server ip address&gt;</code> Type <code>man resolv.conf</code> for details on that file. If vMA is set up for DHCP, and the network is restarted, changes you made to <code>/etc/resolv.conf</code> are lost.
Problems while adding Active Directory target or configuring vMA for Active Directory.	If you are unable to authenticate from vMA or cannot add vMA to the domain controller, check the following: <ul style="list-style-type: none"> <li>Your DNS server setup in vMA resolves the IP address or host name of the vCenter server to an FQDN and the FQDN contains the domain name to which vMA is added.</li> <li>The <code>vifp listserver</code> command shows the name of vCenter as the FQDN that contains the domain name to which vMA is added as the suffix.</li> <li>The date and time settings on vMA, the domain controller and vCenter Server are identical. Check the time zone as well. The time may not exactly be the same but may vary by an hour. However, a large skew in the time may cause authentication problems.</li> </ul>

This release of vMA provides the `vmo-support` script that enables you to collect various system configuration information and other logs. You can run this script by issuing the following command:

```
> sudo vmo-support
```

The script generates the information and log bundle and appends it to the `vmware_` log file on the ESXi host on which vMA is deployed.

# VCAP-DCA 5 Objective 9.1–Install ESXi Server with Custom Settings

## Objective 9.1 – Install ESXi Server with Custom Settings

For this objective I used the following resources:

- vSphere 5 Documentation Center –> [Understanding Image Builder](#)
- vSphere 5 Documentation Center –> [Image Builder Common Tasks](#)
- VMware “vSphere Installation and Setup” documentation

### Knowledge

#### Identify ESXi Image Builder Requirements

- Microsoft .NET 2.0
- Microsoft PowerShell 1.0 or 2.0
- vSphere PowerCLI (includes Image Builder cmdlets)

### Skills and Abilities

#### Create/Edit Image Profiles

#### Install/Uninstall Custom Drivers

Grouping these two skills together. An Image Profile is an ESXi image that has been created that contains VMware and thirty-party drivers packaged as VIBs. Using the Image Builder PowerCLI cmdlets you can export the images as either ZIP files or ISO files. To start you need to create a “Software Depot”. These depots can either be local or accessed via HTTP. For this example we will be leveraging a local software depot that contains the ESXi 5.0 zip file.

For additional reading on Image Builder, have a look at the following resources:

- vSphere 5 Documentation Center –> [Understanding Image Builder](#)
- vSphere 5 Documentation Center –> [Image Builder Common Tasks](#)

Step 1 – Using the “Add-EsxSoftwareDepot” cmdlet to import the base ESXi 5.0 image:



Step 2 – To see that the image has been imported run the “Get-EsxImageProfile” cmdlet. Note that there are two images listed, one with and one without VMware Tools:



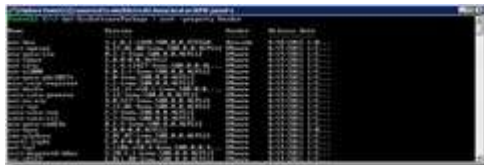
Step 3 – With the software depot imported, using the “New-ESXImageProfile” cmdlet we will make a “clone” of the ESXi image name “VCAP-DCA5”. Later we will modify this image by adding additional VIBs:



Step 4 – Now with our “VCAP-DCA5” base ESXi image lets add some additional VIBs. In this example I will be adding Brocade Ethernet and CAN drivers. As we did in Step 1 I will be adding a software depot containing the Brocade VIB files:



Step 5 – To confirm the VIB has been added and to get its name for the next step use the “Get-ESXSoftwarePackage” cmdlet. In the example I am using the “sort” function to list the “Vendor” column alphabetically, this way the Brocade package will be listed first:



Step 6 – Using the “Add-ESXSoftwarePackage” cmdlet and the package name retrieved in step 5 will add the newly imported Brocade VIB to our “VCAP-DCA5” image:



Step 7 – Now to verify that the Brocade VIB is indeed installed into our image:



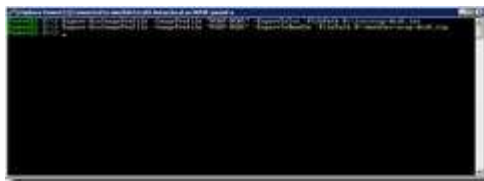
Step 8 – If you want to remove a VIB, say that Brocade driver we just installed, use the “Remove-EsxSoftwarePackage” cmdlet:



Step 9 – The Brocade package is no longer listed:



Step 10 – After your image is created and fine tuned to your liking use the “Export-EsxImageProfile” cmdlet to export the image either as an ISO or an offline bundle to be used with Update Manager to install your ESXi hosts:



### Configure Advanced Bootloader Options

ESXi supports installing or upgrading an existing installation using scripts. You can utilize either these by using supported commands from boot prompt. To access the prompt, during the installer process press “Shift+O”:



Enter your boot command:



Review page 49 of the VMware “vSphere Installation and Setup” documentation for a full listing of supported commands

## Configure Kernel Options

The boot loader configuration file `boot.cfg` specifies the kernel, the kernel options, and the boot modules that the `mboot.c32` boot loader uses in an ESXi installation. You can modify the `kernelopt` line of the `boot.cfg` file to specify the location of an installation script or to pass other boot options. Below are the available commands:

Command	Description
<code>title=STRING</code>	Sets the bootloader title to <code>STRING</code>
<code>kernel=FILEPATH</code>	Sets the kernel path to <code>FILEPATH</code>
<code>kernelopt=STRING</code>	Appends <code>STRING</code> to the kernel boot options
<code>modules=FILEPATH1—FILEPATH2</code>	Lists the modules to be loaded, separated by three hyphens

## Given a Scenario, Determine when to Customize a Configuration

The most common scenario would be to include storage/network drivers that are not included with the default ESXi installation. Other opportunities would include using a kickstart or a scripted installation to quickly deploy multiple ESXi hosts with a base configuration (vSwitches, storage, etc).

# VCAP-DCA 5 Objective 9.2 – Install ESXi Hosts Using Auto Deploy

## Objective 9.2 – Install ESXi Hosts Using Auto Deploy

For this objective I used the following resources:

- VMware “vSphere Installation and Setup” documentation  
[Knowledge](#)

### Identify Auto Deploy Requirements

Auto Deploy Environment Requirements

- Do not use VLAN tagged networks at the boot NIC
- 2GB of disk space (minimum) for Auto Deploy repository
- DHCP server in the environment
- TFTP server in the environment
- Set up a remote Syslog server (optional). Leverage vSphere Syslog Collector
- Set up ESXi Dump Collector and configure hosts to leverage  
[Software Requirements](#)

- Microsoft .NET 2.0
- Microsoft Powershell 2.0
- VMware vSphere PowerCLI
- Set up a remote Syslog server (optional but recommended). Leverage vSphere Syslog Collector
- Set up ESXi Dump Collector (optional but recommended) and configure hosts to leverage  
[Skills and Abilities](#)

### Install the Auto Deploy Server

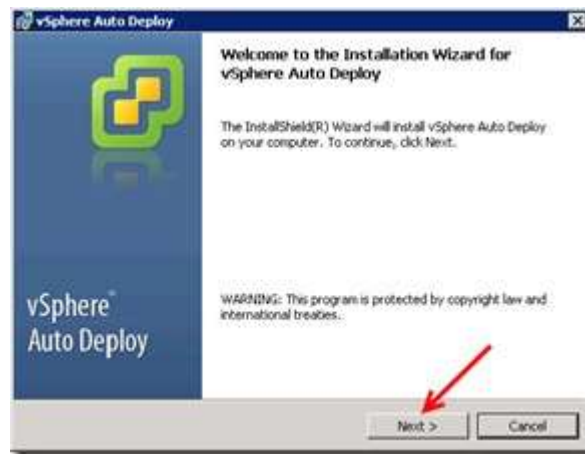
Auto Deploy is an installation option included on the vSphere vCenter media. Select “VMware Auto Deploy” from the selection list:



Select the "Setup Language"



Click "Next" on the "Welcome" dialog



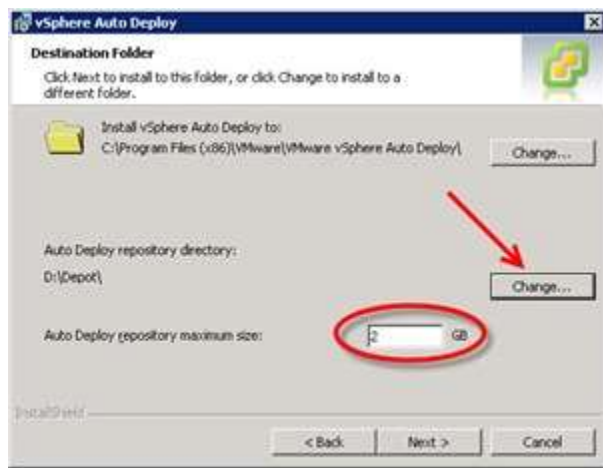
Click "Next" on the "End User Patent Agreement":



Accepted the “End User License Agreement”, click “Next”:

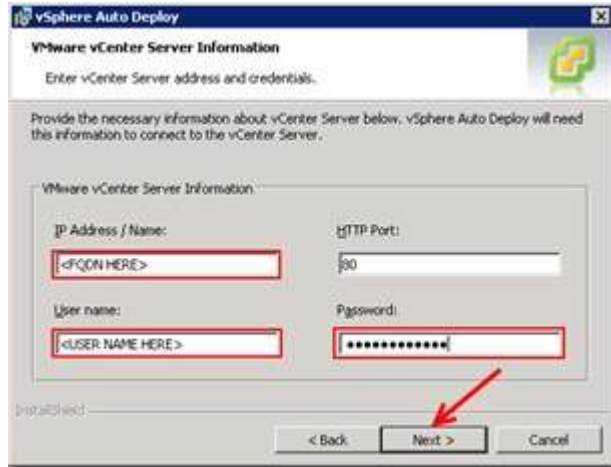


Don’t fall asleep on this screen! Be sure to change the “Auto Deploy repository directory” from the default. In the example I am using D:\Depot.

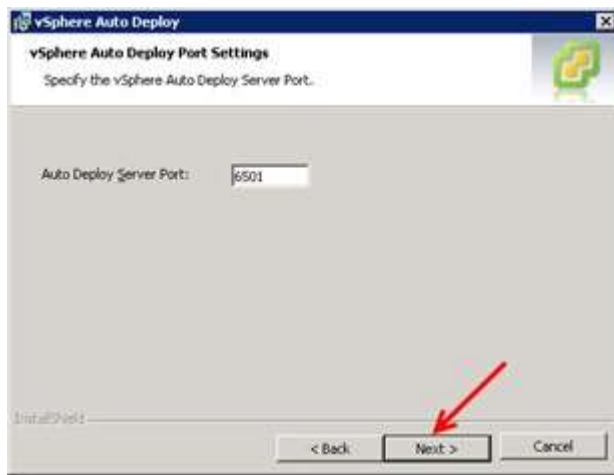


Provide the FQDN of your vCenter server along with administrative credentials:

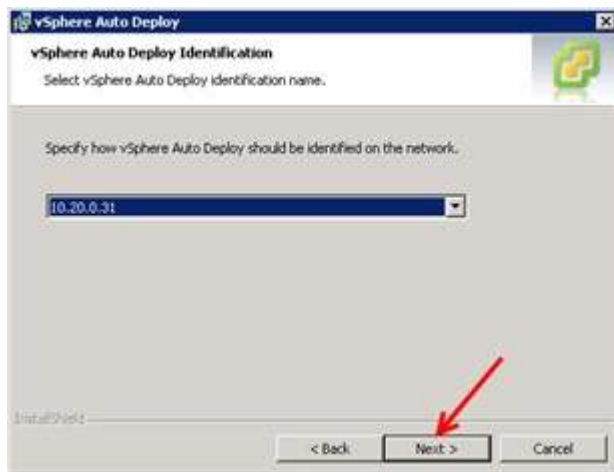




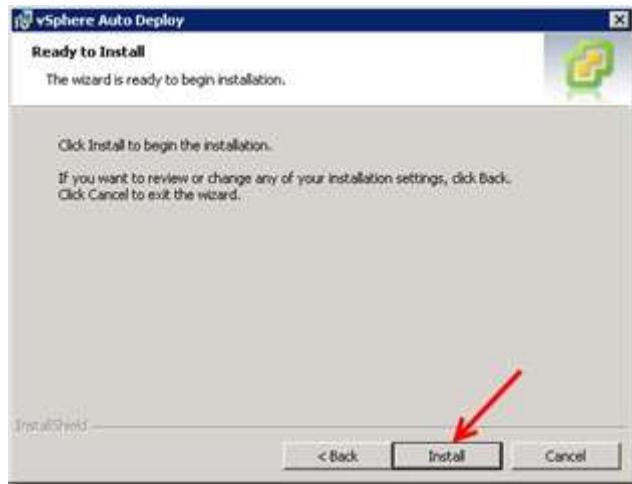
Leave the default server port and click "Next":



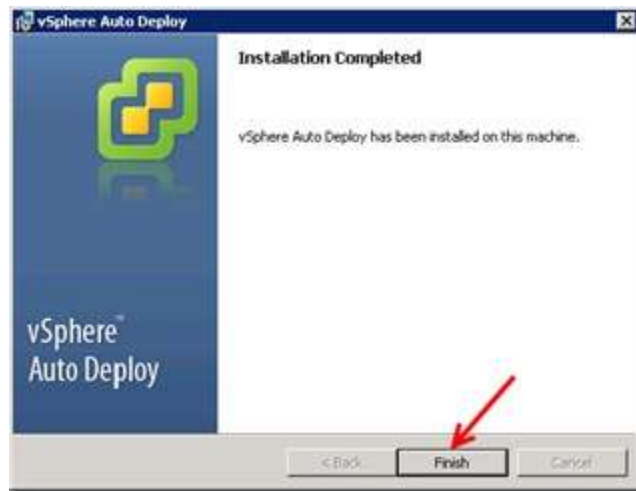
If you have multiple interfaces on your Auto Deploy server, choose the correct listening IP from the drop down:



Click "Install" to continue:



Select "Finish" to close out the installation:



Auto Deploy is now installed.

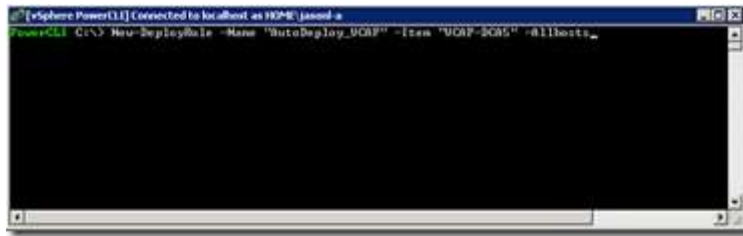
### Utilize Auto Deploy cmdlets to Deploy ESXi Hosts

At this time the use and configuration of Auto Deploy is completed using vSphere PowerCLI cmdlets. The commands and there uses are listed below:

Command	Description
Get-DeployCommand	Returns a list of Auto Deploy cmdlets
New-DeployRule	Creates a new rule with the specified items and patterns
Set-DeployRule	Updates an existing rule with the specified items and patterns. You cannot update a rule that is part of a rule set
Get-DeployRule	Retrieves the rules with the specified names

Copy-DeployRule	Clones and updates an existing rule
Add-DeployRule	Adds one or more rules to the working rule set and, by default, also to the active rule set. Use the <i>NoActivate</i> parameter to add a rule only to the working rule set
Remove-DeployRule	Removes one or more rules from the working rule set and from the active rule set. Run this command with the <i>-Delete</i> parameter to completely delete the rule.
Set-DeployRuleset	Explicitly sets the list of rules in the working rule set
Get-DeployRuleset	Retrieves the current working rule set or the current active rule set
Switch-ActiveDeployRuleset	Activates a rule set so that any new requests are evaluated through the rule set
Get-VMHostMatchingRules	Retrieves rules matching a pattern. For example, you can retrieve all rules that apply to a host or hosts. Use this cmdlet primarily for debugging.
Test-DeployRulesetCompliance	Checks whether the items associated with a specified host are in compliance with the active rule set
Repair-DeployRulesetCompliance	Given the output from <i>Test-DeployRulesetCompliance</i> , this cmdlet updates the image profile, host profile, and location for each host in the vCenter Server inventory. The cmdlet might apply image profiles, apply host profiles, or move hosts to prespecified folders or clusters on the vCenter Server system.
Apply-EsxImageProfile	Associates the specified image profile with the specified host
Get-VMHostImageProfile	Retrieves the image profile in use by a specified host. This cmdlet differs from the <i>Get-EsxImageProfile</i> cmdlet in the Image Builder PowerCLI
Repair-DeployImageCache	Use this cmdlet only if the Auto Deploy image cache is accidentally deleted
Get-VMHostAttributes	Retrieves the attributes for a host that are used when the Auto Deploy server evaluates the rules.

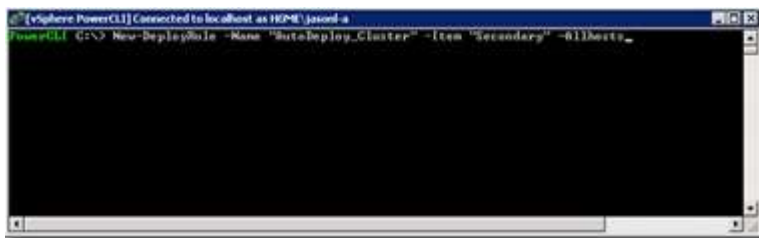
To deploy an ESXi host via Auto Deploy you need to first create a “Deployment Rule”. A deployment rule is created using the “New-DeployRule” cmdlet:



```
[vSphere PowerCLI] Connected to localhost as HDP@ [asoad-a]
PowerCLI C:\> New-DeployRule -Name "AutoDeploy_VCAP" -Item "UCBP-DCS5" -AllHosts_
```

The above command will create a deployment rule named “AutoDeploy\_VCAP” and will use the “VCAP-DCA5” image profile (created in Objective 9.1 [HERE](#)) and will apply the rule to “Allhosts” or any ESXi host boots from it.

Next we will create an additional deployment rule to specify a vSphere cluster location to add each host to join:



```
[vSphere PowerCLI] Connected to localhost as HDP@ [asoad-a]
PowerCLI C:\> New-DeployRule -Name "AutoDeploy_Cluster" -Item "Secondary" -AllHosts_
```

Using the “Get-DeployRule” cmdlet we can list the newly created deployment rules:



```
[vSphere PowerCLI] Connected to localhost as HDP@ [asoad-a]
PowerCLI C:\> Get-DeployRule

Name       : AutoDeploy_VCAP
PatternList :
ItemList   : (UCBP-DCS5)

Name       : AutoDeploy_Cluster
PatternList :
ItemList   : (Secondary)

PowerCLI C:\> _
```

Next, to make the deployment rules active we will create a “Deploy Rule Set”. Using the “Add-DeployRule” cmdlet we will add each of the two deploy rules:

```
PowerCLI C:\> Add-DeployRule "AutoDeploy_UCRP"

Name       : AutoDeploy_UCRP
PatternList : (UCRP-DC05)
ItemList   : (UCRP-DC05)

PowerCLI C:\> Add-DeployRule "AutoDeploy_Cluster"

Name       : AutoDeploy_UCRP
PatternList : (UCRP-DC05)
ItemList   : (UCRP-DC05)
Name       : AutoDeploy_Cluster
PatternList : (Secondary)
ItemList   : (Secondary)

PowerCLI C:\> _
```

To verify the configuration, issue the “Get-DeployRuleSet” cmdlet:

```
PowerCLI C:\> Get-DeployRuleSet

Name       : AutoDeploy_UCRP
PatternList : (UCRP-DC05)
ItemList   : (UCRP-DC05)
Name       : AutoDeploy_Cluster
PatternList : (Secondary)
ItemList   : (Secondary)

PowerCLI C:\> _
```

We are now ready to deploy some ESXi hosts!

### Configure Bulk Licensing

Procedure taken from pages 71 through 72 of the VMware *vSphere Installation and Setup* documentation:

Step 1 – Connect to the vCenter Server system you want to use and bind the associated license manager to a variable

```
Connect-VIServer -Server <Your Server> -User <Username> -Password <Password>  
$licenseDataManager = Get-LicenseDataManager
```

Step 2 – Run a cmdlet that retrieves the datacenter in which the hosts for which you want to use the bulk licensing feature are located.

```
$hostContainer = Get-DataCenter -Name Datacenter-X
```

Step 3 – Create a new *LicenseData* object and a *LicenseKeyEntry* object with associated type ID and license key.

```
$licenseData = New-Object VMware.Vim.Automation.License.Types.LicenseData  
$licenseKeyEntry = New-Object VMware.VimAutomation.License.Types.LicenseKeyEntry
```

*\$licenseKeyEntry.TypeId = "vmware-vmware"*

*\$licenseKeyEntry.LicenseKey = "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"*

Step 4 - Associate the *LicenseKeys* attribute of the *LicenseData* object you created in step 3 with the *LicenseKeyEntry* object

*\$licenseData.LicenseKeys += \$licenseKeyEntry*

Step 5 - Update the license data for the data center with the *LicenseData* object and verify that the license is associated with the host container.

*\$licenseDataManager.UpdateAssociatedLicenseData(\$hostContainer.Uid, \$licenseData)*

*\$licenseDataManager.QueryAssociatedLicenseData(\$hostContainer.Uid)*

Step 6 - Provision one or more hosts with Auto Deploy and assign them to the data center or cluster that you assigned the license data to.

Step 7 - Verify that the host is successfully assigned to the default license *XXXXX-XXXXX-XXXXX-XXXXX-XXXXX*

- Using a vSphere client, log in to the vCenter Server System
- Navigate to the *Configuration -> License Features* tab for the host and check that the correct license is displayed

All hosts that you assigned to the data center are now licensed automatically.

### **Provision/Reprovision ESXi Hosts Using Auto Deploy**

Thought not configured in this objective, prior to attempting to deploy ESXi hosts via Auto Deploy the proper infrastructure/components need to be in place. This includes the setup of DHCP services with reservations and a TFTP server. These concepts are not covered on the exam, but do know they are required to implement Auto Deploy.

To provision an ESXi host with Auto Deploy is pretty straight forward once the infrastructure and deployment rules/rulesets have been created. Be sure that in the BIOS of the server you have configured the boot order to list network first. From there it should go as follows:

Your system will PXE boot and via TFTP locate the boot image:

```
Network Boot from Intel E1000
Copyright (C) 2002-2000 VMware, Inc.
Copyright (C) 1997-2000 Intel Corporation

CLIENT MAC ADDR: 08 50 56 83 79 CE GUID: 42330F02-3096-8157-1FF0-61227F90E2F0
CLIENT IP: 10.20.0.200 MASK: 255.255.255.0 DHCP IP: 10.20.0.11
STANDARD IP: 10.20.0.1
PXE->ES: PXE at 0E95:0070, entry point at 0E95:0100
      UEFI code segment 0E95:0070, data segment 0E9F:5000 (011-63000)
      UEFI device is PCI 02:00:0, type 01X-002.3
      UEFI from boot memory after PXE unload
qPXE Initializing devices...

qPXE 1.0.0.0 -- Open Source Boot Firmware -- http://otherboot.org
Features: Boot HTTP HTTPS iSCSI DNS TFTP NetImage COMBOOT ELF Multiboot PXE PXOOT
Press Ctrl-R for the qPXE command line..._
```

The ESXi installation will begin:

```
Loading VMware ESXi
Loading /usr/sbin/EFI/Boot/efi/boot/efi/BootManager.efi
Loading /usr/sbin/EFI/Boot/efi/boot/efi/BootManager.efi
Loading /usr/sbin/EFI/Boot/efi/boot/efi/BootManager.efi
Loading /usr/sbin/EFI/Boot/efi/boot/efi/BootManager.efi
```

Once the installation has completed you will have a functioning base installation of ESXi:



### Configure an Auto Deploy Reference Host

After you have your initial host has been deployed you will want to use that as your “Reference Host”. Since Auto Deployed ESXi hosts run in memory per host setting are not maintained during reboots. In this case you want to leverage “Host Profiles” to save you both time and to have a standard base configuration. On the initial host you will want to

configure NTP, syslog, networking, and security settings. Then capture those settings in a Host Profile and create a deployment rule containing the profile.

For further information read pages 79 through 85 of the VMware *vSphere Installation and Setup* documentation.