# VMware Certified Advanced Professional

Datacenter Administration Exam Study Guide

VDCA410 Exam

Based on Exam Blueprint Version 1.6

Version 1.6

3/27/2011

Sean Crookston (sean@seancrookston.com)

Damian Karlson (damiankarlson.com)

This guide was originally compiled and updated by Sean Crookston. As of February 2011, the study guide is now being maintained and updated by Damian Karlson, with Sean Crookston's permission.

## About this Guide

This is a collection of my notes and studying for the VCAP-DCA. This guide is a compilation of my comments and many other VMware and independent resources related to topics on the exam. Some topics I will put much detail into and some I will simply have a few links.

This guide is provided to aid in studying for and passing the VCAP-DCA.

You can find an archive of Sean Crookston's notes at http://www.vfail.net/vcap-dca/. Damian Karlson's notes can be found at http://damiankarlson.com/vcap-dca4-exam/.

# Contents

# VDCA410 Section 1 – Implement and Manage Storage

## Objective 1.1 – Implement and Manage Complex Storage Solutions

### Knowledge

- Identify RAID levels
- Identify supported HBA types
- Identify virtual disk format types

### Skills and Abilities

- Determine use cases for and configure VMware DirectPath I/O
- Determine requirements for and configure NPIV
- Determine appropriate RAID level for various Virtual Machine workloads
- Apply VMware storage best practices
- Understand use cases for Raw Device Mapping
- Configure vCenter Server storage filters
- Understand and apply VMFS resignaturing
- Understand and apply LUN masking using PSA-related commands
- Analyze I/O workloads to determine storage performance requirements

### Tools

- Fibre Channel SAN Configuration Guide
- iSCSI SAN Configuration Guide
- ESX Configuration Guide
- ESXi Configuration Guide
- vSphere Command-Line Interface Installation and Scripting Guide
- Product Documentation
- vSphere Client
- vscsiStats
- vSphere CLI
    - vicfg-*
    - vifs
    - vmkfstools
    - esxtop/resxtop

### Notes

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

VMware DirectPath I/O allows a guest VM to directly access an I/O device via bypassing the virtualization layer. This can result in improved performance and a good use case would be 10 Gigabit Ethernet for guests requiring a lot of network throughput.

Requirements from VMware's Direct Path I/O documentation:

- *VMDirectPath supports a direct device connection for virtual machines running on Intel Xeon 5500 systems, which feature an implementation of the I/O memory management unit (IOMMU) called Virtual*

*Technology for Directed I/O (VT-d). VMDirectPath can work on AMD platforms with I/O Virtualization Technology (AMDIOMMU), but this configuration is offered as experimental support.*

- Some machines might not have this technology enabled in the BIOS by default
- Each guest can support up to two pass through devices.
- A good guide to setup DirectPath I/O can be found at Petri It Knowledgebase

**Determine requirements for and configure NPIV**
So far the best resource I've found for how to configure NPIV is Simon Long's blog which also references a great article from Jason Boche's blog. NPIV allows a single N_PORT to have multiple WWPNs and multiple N_PORT IDs. This requires a supported set of hardware, includes HBAs and Switches. With NPIV you could present a LUN to a specific virtual machine, something which is not possible without NPIV.

Also it is good to bring up NPV, or N_Port Virtualization in which we talk about NP_Ports. The NP_Port will look like an NPIV host to the F_Port. This requires support from the upstream switch. Ultimately NPV allows you to add switches and ports to the fabric without requiring more domain ids.

Another good read on NPIV is this blog from Scott Lowe
There are some specific requirements to using NPIV

- It can only be used with Raw Device Mappings.
- You must have NPIV aware FC switches
- ESX(i) hosts must have HBAs that support NPIV. This is currently limited to QLogic and Emulex with NPIV compatible firmware. I suspect this may have been expanded since some of the information I've read may be a little older.

**Determine appropriate RAID level for various Virtual Machine workloads**
Similar to sizing physical servers, you will want to ensure your virtual machine workloads are evenly distributed (remember SCSI reservations) and on appropriately given storage for performance purposes. The determination of the RAID level of the storage will be made on a per virtual machine basis. I recommend reading the below to start thinking about how to best go about sizing virtual machine workloads.

Duncan Epping has a discussion over on his blog which highlights the write penalty and overall performance of different RAID levels, showing the differences in writes. For the test reads were consistent across the board, but writes suffered differently. Check out this chart which shows a real life example.

**Apply VMware storage best practices**
Read these two to help gain a better understanding of best practices for storage.

- http://www.vmware.com/technical-resources/virtual-storage/best-practices.html
- http://www.vmware.com/pdf/Perf_Best_Practices_vSphere4.1.pdf
- By default, Active/Passive storage arrays use Most Recently Used path policy.
- Do not use Fixed Path policy for Active/Passive storage arrays to avoid LUN thrashing.

**Understand use cases for Raw Device Mapping**

Raw device mappings allow management and access of raw SCSI disks or LUNs as VMFS files. An RDM file exists on a VMFS volume acting as a proxy for the device, which contains metadata used for managing and redirecting access to the physical disk.

A good read is the blog here which discusses why RDMs should probably not be used for performance purposes. Its main source of information comes from VMware's write-up for Performance Characterization of VMFS and RDM Using a SAN.

According to VMware:

- The main conclusions that can be drawn from the tests described in this study are: for random reads and writes, VMFS and RDM yield a similar number of I/O operations per second.
- For sequential reads and writes, performance of VMFS is very close to that of RDM (except on sequential reads with an I/O block size of 4K). Both RDM and VMFS yield a very high throughput in excess of 300megabytes per second depending on the I/O block size.
- For random reads and writes, VMFS requires 5 percent more CPU cycles per I/O operation compared to RDM.
- For sequential reads and writes, VMFS requires about 8 percent more CPU cycles per I/O operation compared to RDM.

You can configure RDM in two ways:

- Virtual compatibility mode—this mode fully virtualizes the mapped device, which appears to the guest operating system as a virtual disk file on a VMFS volume. Virtual mode provides such benefits of VMFS as advanced file locking for data protection and use of snapshots.

- Physical compatibility mode—this mode provides access to most hardware characteristics of the mapped device. VMkernel passes all SCSI commands to the device, with one exception, thereby exposing all the physical characteristics of the underlying hardware.

VMFS is the preferred option for most enterprise applications such as databases, ERP, CRM, VMware Consolidated Backup, Web servers, and file servers. Some of the common uses of RDM are in cluster data and quorum disks for configurations using clustering between virtual machines or between physical and virtual machines or for running SAN snapshot or other layered applications in a virtual machine.

When using RDMs you are limited in some of the actions you can perform:

- No migrating VMs with physical mode RDMs if the migration involves copying the disk (Storage vMotion)
- No VMware snapshots with physical mode RDMs
- No VCB support with physical mode RDMs, because VCB requires VMware snapshots
- No cloning VMs that use physical mode RDMs
- No converting VMs that use physical mode RDMs into templates

**Configure vCenter Server storage filters**

A couple of good blogs can be found here and here for some background on the topic.
To turn off vCenter Server Storage Filters (from the ESX configuration guide):

When you perform VMFS datastore management operations, vCenter Server uses default storage filters. The filters help you to avoid storage corruption by retrieving only the storage devices, or LUNs, that can be used for a particular operation. Unsuitable LUNs are not displayed for selection. You can turn off the filters to view all LUNs. Before making any changes to the LUN filters, consult with the VMware support team. You can turn off the filters only if you have other methods to prevent LUN corruption.

**Procedure**

1. In the vSphere Client, select Administration > vCenter Server Settings.
2. In the settings list, select Advanced Settings.
3. In the Key text box, type a key.
    a. config.vpxd.filter.vmfsFilter
    b. config.vpxd.filter.rdmFilter
    c. config.vpxd.filter.SameHostAndTransportsFilter
    d. config.vpxd.filter.hostRescanFilter
    e. NOTE: If you turn off the Host Rescan Filter, your hosts continue to perform a rescan each time you present a new LUN to a host or a cluster.
4. In the Value text box, type False for the specified key.
5. Click Add.
6. Click OK.
7. You are not required to restart the vCenter Server system.

**Understand and apply VMFS resignaturing**

Check out this KB article from VMware that will explain further VMFS resignaturing and how to do it from the GUI or command line. Prior to vSphere 4 enabling resignaturing was done server wide and applied to all volumes of the host. Now, with the use of the esxcfg-volume/vicfg-volume commands this can be done per volume.

The vicfg-volume command supports resignaturing a snapshot volume and mounting and unmounting the volume. You can also make the mounted volume persistent across reboots and query a list of snapshot volumes and original volumes. Remember, this command is for volumes with snapshots only and as such will only list those volumes.

See the vSphere CLI Reference for full syntax and usage of the vicfg-volume command.

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

Check out Masking a LUN from ESX and ESXi 4.0 using the MASK_PATH plug-in
Refer to my previous study topic on troubleshooting storage performance
See the vSphere CLI Reference for full syntax and usage of the vicfg-mpath and esxcli commands.

**Analyze I/O workloads to determine storage performance requirements**

Refer to my previous study topic on troubleshooting storage performance and checkout this great technical paper that goes in depth on the topic.

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

### Knowledge

- Identify storage provisioning methods
- Identify available storage monitoring tools, metrics and alarms

### Skills and Abilities

- Apply space utilization data to manage storage resources
- Provision and manage storage resources according to Virtual Machine requirements
- Understand interactions between virtual storage provisioning and physical storage provisioning
- Apply VMware storage best practices
- Configure datastore alarms
- Analyze datastore alarms and errors to determine space availability

### Tools

- vSphere Datacenter Administration Guide
- Fibre Channel SAN Configuration Guide
- iSCSI SAN Configuration Guide
- vSphere Command-Line Interface Installation and Scripting Guide
- Product Documentation
- vSphere Client
- vSphere CLI
    - vmkfstools

## Notes

This section in a lot of ways was partially delved into from Objective 1.1 and Objective 6.4. Additionally this topic delves into alarms and events pertaining to storage.

**Apply space utilization data to manage storage resources**

In general, you never want to have less than 20% space free. Other than that studying should be focused around on how to check these statistics out.

**Provision and manage storage resources according to Virtual Machine requirements**

- I think a lot of this was already covered in the previous section. I will add the following link for and in depth look at Windows counters that will assist in determining virtual machine requirements.

- Additionally this blog from simple-talk.com contains a good overview of best practices when it comes to provisioning virtual machine storage.

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

A couple of things to realize with this one. When you thin provision virtual machines you must account for the possibility of these virtual machines growing. It is often common nowadays to overprovision storage with thin provisioning and the risk is there that you could run out of physical storage as result. This is a very good use case for alarms in vCenter.

Additionally the physical storage provisioned will affect the performance of the guest. Read the other topics on storage already covered to understand the different raid levels and how they can affect performance.

**Apply VMware storage best practices**

VMware Virtual Storage Best Practices

**Configure datastore alarms**

vSphere has added a lot of alarms with its recent release. A blog from Jeremy Waldrop does a good job of focusing specifically on datastore alarms.

**Analyze datastore alarms and errors to determine space availability**

I'd recommend roaming the VMware community for this one.

http://communities.vmware.com/thread/257031

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

### Knowledge

- Explain the Pluggable Storage Architecture (PSA) layout

### Skills and Abilities

- Install and Configure PSA plug-ins
- Understand different multipathing policy functionalities
- Perform command line configuration of multipathing options
- Change a multipath policy
- Configure Software iSCSI port binding

### Tools

- vSphere Command-Line Interface Installation and Scripting Guide
- ESX Configuration Guide
- ESXi Configuration Guide
- Fibre Channel SAN Configuration Guide
- iSCSI SAN Configuration Guide
- Product Documentation
- vSphere Client
- vSphere CLI
    - esxcli

## Notes

**Explain the Pluggable Storage Architecture (PSA) layout**

What is Pluggable Storage Architecture (PSA) and Native Multipathing(NMP)?

Understanding VMware vSphere 4.1 PSA

Know the acronyms and understand the PSA. From Duncan Epping's blog: the acronyms below and a more in-depth information on each.

- PSA = Pluggable Storage Architecture
- NMP = Native Multipathing
- MPP = Multipathing Plugin (associates physical path with logical device)
- PSP = Path Selection Plugin (load-balancing)
- SATP = Storage Array Type Plugin (for failover)i.e. powerpath
- NMP "associates" a SATP with the set of paths from a given type of array.
- NMP "associates" a PSP with a logical device.
- NMP specifies a default PSP for every logical device based on the SATP associated with the physical paths for that device.
- NMP allows the default PSP for a device to be overridden.

**Install and Configure PSA plug-ins**

vSphere4 ESX4: How to configure iSCSI Software initiator on ESX4 against a HP MSA iSCSI Storage system

**Understand different multipathing policy functionalities**

Check out vStorage Multi Paths Options in vSphere

- Fixed will use the designate preferred path if configured and otherwise will use the first path discovered that works at system boot. A path is randomly selected when a failure occurs and the original path is selected when it comes back.
- Most recently uses the first working path at system boot. If this is unavailable, an alternative path is switched to and is used until the new path fails.
- Round Robin uses an automatic path selection that rotates and uses all available paths. It includes the ability to load balance across paths using active paths and is of most use on active/active array. In Active/passive arrays it will load between ports to the same storage processor. Not supported in MSCS environments.
- Fixed with array preference extends to fixed functionality to active/passive and ALUA mode arrays. VMW_PSP_FIXED_AP will select the preferred path according to array path preference and current path state.

**Perform command line configuration of multipathing options**

See the vSphere CLI Reference for full syntax and usage of the vicfg-mpath command.

**Change a multipath policy**

See the vSphere CLI Reference for full syntax and usage of the vicfg-mpath and esxcli commands.

Reminder, you must add –server <servername> as a connection option, otherwise the esxcli command will assume localhost, which will not work when running inside the vMA.

You use the esxcli command to set path policy like below, where VMW_PSP_xxx will either be Fixed, Fixed_AP, MRU, or RR

- *esxcli <connection options> nmp device setpolicy –device naa.xxx –psp VMW_PSP_xxx*

For more usage of this command check out Objective 6.4

**Configure Software iSCSI port binding (also referred to as multipathing)**
See the vSphere CLI Reference for full syntax and usage of the esxcli command.

List available uplinks for use with iSCSI adapters

- *esxcli swiscsi vmnic list –d <vmhba>*

Connect iSCSI initiator to the VMkernel ports

- *esxcli swiscsi nic add –n <port_name> –d <vmhba>*

To disconnect iSCSI initiator from VMkernel ports

- *esxcli swiscsi nic remove –n <port_name> –d <vmhba>*

To list all sw iSCSI sessions at the adapter level or target level

- *esxcli swisci session list –d <iscsi_adapter>*
- *esxcli swiscsi session list –d vmhba36*

Remove iSCSI sw sessions

- *esxcli swiscsi session remove –d*

# VDCA410 Section 2 – Implement and Manage Networking

## Objective 2.1 – Implement and Manage Complex Virtual Networks

### Knowledge

- Identify common virtual switch configurations

### Skills and Abilities

- Determine use cases for and apply IPv6
- Configure NetQueue
- Configure SNMP
- Determine use cases for and apply VMware DirectPath I/O
- Migrate a vSS network to a Hybrid or Full vDS solution
- Configure vSS and vDS settings using command line tools
- Analyze command line output to identify vSS and vDS configuration details

### Tools

- vSphere Command-Line Interface Installation and Scripting Guide
- vNetwork Distributed Switch: Migration and Configuration
- ESX Configuration Guide
- ESXi Configuration Guide
- Product Documentation
- vSphere Client
- vSphere CLI
    - vicfg-*

## Notes

**Determine use cases for and apply IPv6**

To enable IPv6 using a command line:

1. To enable IPv6 for the VMkernel, run the command:
   vicfg/esxcfg-vmknic -6 true
2. To enable IPv6 for the Service Console, run the command:
   esxcfg-vswif -6 true
3. To verify that IPv6 has been enabled, run the command:
   –vicfg-vmknic --list

Note the below:

- ESX 3.5 supports virtual machines configured for IPv6.
- ESX 4.0 supports IPv6 with the following restrictions:
  - IPv6 Storage (software iSCSI and NFS) is experimental in ESX 4.0.
  - ESX does not support TCP Segmentation Offload (TSO) with IPv6.
  - VMware High Availability and Fault Tolerance do not support IPv6.

**Configure NetQueue**

NetQueue is disabled by default and can be configured from the GUI or the command line

Enable NetQueue in VMkernel using VMware Infrastructure (VI) Client.

1. Choose **Configuration > Advanced Settings > VMkernel**.
2. Select the checkbox for **VMkernel.Boot.netNetqueueEnabled**.

At the command line, you can also add a line to /etc/vmware/esx.conf

*/vmkernel/NetQueueEnabled=True*

After you enable NetQueue by either of the above methods, you must enable NetQueue on the adapter module itself using the vicfg-module command.

Configure a supported NIC to use NetQueue:

```
vicfg-module <conn_options> -s "intr_type=2 rx_ring_num=8" s2io
```

Verify that NetQueue has been configured:

```
vicfg-module <conn_options> -g s2io
```

List the set of modules on the host:

```
vicfg-module <conn_options> -l
```

Changes require a reboot to take effect.

**Configure SNMP**

For ESX(i)

1 Configure SNMP Communities

> vicfg-snmp.pl –server <hostname> –username <username> –password <password> -c <community1>

Each time you specify a community with this command, the settings you specify overwrite the previous configuration. To specify multiple communities, separate the community names with a comma.

2 Configure SNMP Agent to Send Traps

> vicfg-snmp.pl –server <hostname> –username <username> –password <password> -t target address>@<port>/<community>.

You can then enable the SNMP agent by typing

> vicfg-snmp.pl –server <hostname> –username <username> –password <password> –enable.

And then send a test by typing

> vicfg-snmp.pl –server <hostname> –username <username> –password <password>–test.

3 Configure SNMP Agent for Polling

> vicfg-snmp.pl –server <hostname> –username <username> –password <password> -p <port>

For vCenter server

1 Select Administration—>vCenter Server Settings

2 If the vCenter Server is part of a connected group, in Current vCenter Server, select the appropriate server.

3 Click SNMP in the navigation list.

4 Enter primary Receiver  info, note if the port value is empty vCenter Server uses the default of 162.

5 Optionally enable additional receivers

6 Click OK.

**Determine use cases for and apply VMware DirectPath I/O**

- VMware DirectPath I/O allows a guest VM to directly access an I/O device via bypassing the virtualization layer. This can result in improved performance and a good use case would be 10 Gigabit Ethernet for guests requiring a lot of network throughput. Each guest can support up to two pass through devices.
- Requirements from VMware's Direct Path I/O documentation.
- *VMDirectPath supports a direct device connection for virtual machines running on Intel Xeon 5500 systems, which feature an implementation of the I/O memory management unit (IOMMU) called Virtual Technology for Directed I/O (VT-d). VMDirectPath can work on AMD platforms with I/O Virtualization Technology (AMDIOMMU), but this configuration is offered as experimental support.*

- Some machines might not have this technology enabled in the BIOS by default
- A good guide to setup DirectPath I/O can be found at Petri It Knowledgebase

**Migrate a vSS network to a Hybrid or Full vDS solution**
This document from VMware covers this topic in its entirety. Read it to gain a better understanding of vDS and reasoning on why a Hybrid solution may or may not work. This is a good excerpt from the document below:

*In a hybrid environment featuring a mixture of vNetwork Standard Switches and vNetwork Distributed Switches, VM networking should be migrated to vDS in order to take advantage of Network vMotion. As Service Consoles and VMkernel ports do not migrate from host to host, these can remain on a vSS. However, if you wish to use some of the advanced capabilities of the vDS for these ports, such as Private VLANs or bi-directional traffic shaping, or, team with the same NICs as the VMs (for example, in a two port 10GbE environment), then you will need to migrate all ports to the vDS.*

**Configure vSS and vDS settings using command line tools**
http://blog.scottlowe.org/2009/05/21/vmware-vSphere-vds-vmkernel-ports-and-jumbo-frames/

**Analyze command line output to identify vSS and vDS configuration details**
vicfg-vswitch -l (to get DVSwitch, DVPort, and vmnic names)

esxcfg-vswif -l (get vswif IP address, netmask, dvPort id, etc. ESX Only)

## Objective 2.2 – Configure and Maintain VLANs, PVLANs and VLAN Settings

### Knowledge

- Identify types of VLANs and PVLANs

### Skills and Abilities

- Determine use cases for and configure VLAN Trunking
- Determine use cases for and configure PVLANs
- Use command line tools to troubleshoot and identify VLAN configurations

### Tools

- vSphere Command-Line Interface Installation and Scripting Guide
- ESX Configuration Guide
- ESXi Configuration Guide
- Product Documentation
- vSphere Client
- vSphere CLI
    - vicfg-*

## Notes

**Determine use cases for and configure VLAN Trunking**
Several good blog articles that describe configuring VLAN Trunking on both the VMware and switch side can be found below.

- http://searchnetworking.techtarget.com/tip/0,289483,sid7_gci1515418,00.html
- http://searchnetworking.techtarget.com/tip/0,289483,sid7_gci1515654,00.html
- http://blog.scottlowe.org/2010/04/23/configuring-inter-vlan-routing/
- http://blog.scottlowe.org/2008/09/05/vmware-esx-nic-teaming-and-vlan-trunking-with-hp-procurve/

**Determine use cases for and configure PVLANs**
I would recommend checking out Eric Sloof's video training session on PVLANs.

- A private VLAN is an extension of the VLAN standard.
- It allows further segmentation to create private groups.
- This means others cannot see hosts in the same PVLAN, with the exception of those in the promiscuous PVLAN.

VMware has a good knowledge base article on configuring PVLANs on vNetwork Distributed Switches. The procedures below, from the article, explain how to create a PVLAN table and set the PVLAN in the dvPortGroup.

To create the PVLAN table in the dvSwitch:

1. In vCenter, go to **Home > Inventory > Networking**.
2. Click **Edit Setting** for the 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. Enter a VLAN ID in the VLAN ID field.
6. Select the Type for the Secondary VLANID. Choose one of the options from the dropdown menu.
   - Isolated
   - Community
     **Note**: There can be only one Promiscuous PVLAN and is created automatically for you.
     **Beware**: Before deleting any primary/secondary PVLANs, make sure that they are not in use or the operation is not be performed.

   Click **OK**.

To set 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.
   **Note**: The VLANs created in step 1 are listed here.

**Use command line tools to troubleshoot and identify VLAN configurations**
Reference the vSphere Command Line reference.
Show VLAN of port groups *vicfg-vswitch –l*

## Objective 2.3 – Deploy and Maintain Scalable Virtual Networking

### Knowledge

- Identify VMware NIC Teaming policies
- Identify common network protocols

### Skills and Abilities

- Understand the NIC Teaming failover types and related physical network settings
- Determine and apply Failover settings
- Configure explicit failover to conform with VMware best practices
- Configure port groups to properly isolate network traffic

### Tools

- ESX Configuration Guide
- ESXi Configuration Guide
- vSphere Command-Line Interface Installation and Scripting Guide
- Product Documentation
- vSphere Client
- vSphere CLI
    - vicfg-*

## Notes

**Understand the NIC Teaming failover types and related physical network settings**

A great blog post that goes over this in detail: http://vteardown.com/2009/08/07/vSphere-over-hyper-v-built-in-nic-teaming-support-for-any-nic-with-easy-set-up-directly-from-vSphere-client/

**Determine and apply Failover settings**
Configurable from the NIC teaming tab of the vSwitch

From the ESX(i) server configuration guide:

Load Balancing Settings

- Route based on the originating port ID (Default) — Choose an uplink based on the virtual port where the traffic entered the virtual switch.
- 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.
- Route based on source MAC hash — Choose an uplink based on a hash of the source Ethernet.
- Use explicit failover order — always use the highest order uplink from the list of Active adapters, which passes failover detection criteria. This is a best practice but is not the default.
- NOTE: IP-based teaming requires that the physical switch be configured with EtherChannel. For all other options, EtherChannel should be disabled.

Network Failover Detection

- Link Status only (Default) – 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.
- 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 status alone. When there are at least three NIC's, use beacon probing.
- "What is beacon probing?" – VMware KB1005577

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 NIC in the team because of a failover event, a notification is sent out over the 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. Source – VMware KB1556

Failback

- Select Yes or No to disable or enable 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 workload 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.

**Configure explicit failover to conform to VMware best practices**

Recognizing this is a best practice is probably all that needs to be stated here. To configure explicit failover, just go to the NIC teaming tab of the vSwitch properties to configure this. Set Load balancing to 'Use explicit failover order' and configure the appropriate order for NIC's in your environment.

**Configure port groups to properly isolate network traffic**

Not much to this section, use VLAN tagging and port groups to isolate network traffic on the same vSwitch. Additionally I may add not to forget to isolate traffic for storage and management, separate from virtual machine traffic. It is recommended to separate out your vMotion traffic and it can be on an isolated and non-routed network segment if needed.

## Objective 2.4 – Administer vNetwork Distributed Switch Settings

### Knowledge

- Explain relationship between vDS and logical vSSes

### Skills and Abilities

- Understand the use of command line tools to configure appropriate vDS settings on an ESX/ESXi host
- Determine use cases for and apply Port Binding settings
- Configure Live Port Moving
- Given a set of network requirements, identify the appropriate distributed switch technology to use
- Use command line tools to troubleshoot and identify configuration items from an existing vDS

### Tools

- ESX Configuration Guide
- ESXi Configuration Guide
- vSphere Command-Line Interface Installation and Scripting Guide
- Product Documentation
- vSphere Client
- vSphere CLI
    - vicfg-*

## Notes

**Understand the use of command line tools to configure appropriate vDS settings on an ESX/ESXi host**
Explore and be familiar with the usage of the vicfg-vswitch command.

From the vSphere Command Line Reference, the three options below are specific to the distributed virtual switch.

Add an uplink adapter to a distributed virtual port

*–add-dvp-uplink | –P*

Deletes an uplink adapter from a port on the distributed virtual switch.

*–del-dvp-uplink | –Q <adapter_name> –dvp <DVPort_id><dvswitchname>*

Name of a distributed virtual port

*–dvp | -V*

**Determine use cases for and apply Port Binding settings**
Three different types of port binding exist. A good read on the topic is a VMware KB here

Static Binding

- When you connect a VM to a dvPort group a port is reserved and is immediately assigned.
- This port is freed up only when the VM is removed from the dvPort group.
- No command line option and can only be done through vCenter.
- This is the **default setting** and is recommended for general use.

Dynamic Binding

- dvPort is assigned to a VM only when the VM is powered on and the NIC is connected.
- The dvPort is freed up when the VM is powered off or the NIC is disconnected.
- VMs connected to a dvPort group configured with dynamic binding MUST be powered on and off through vCenter.
- A use case for this would be an environment where you have more VMs than available ports.

Ephemeral binding

- dvPort is created and assigned to the VM when the VM is powered on and NIC is connected. This is just like the vSS
- dvPort is deleted when the VM is powered off of VM NIC is disconnected.
- Ephemeral dvPort assignments can be made through ESX(i) or vCenter.
- This is the only method that will allow you to manage ports when vCenter is down, although network traffic will be unaffected using the other binding methods when vCenter is down.
- Best use case is for emergency and recovery situations
- With this option set, the number of ports is set to 0 automatically at first and will grow.

**Configure Live Port Moving**
Live port migration means that a standalone dvPort can be moved to a dvPortGroup and acquire all the configuration of the dvPortGroup. Likewise, a dvPort which is a part of a dvPortGroup can be moved out from a dvPortGroup; the subsequent config changes to the dvPortGroup does not apply to this dvPort.

**Given a set of network requirements, identify the appropriate distributed switch technology to use**
Learn the differences between using the Nexus 1KV vs. VMware's distributed virtual switch.

There is certainly a price difference and then there is also a management difference. The 1KV is administered like a standard switch, so the Cisco guys in the organization can manage the virtual switching environment consistently with the physical switching environment.

This article here is a good read on the discussion of what option to approach and why.

**Use command line tools to troubleshoot and identify configuration items from an existing vDS**
This topic is covered in other sections of Objective 2 and the network troubleshooting section in Objective 6.

# VDCA410 Section 3 – Deploy DRS Clusters and Manage Performance

## Objective 3.1 – Tune and Optimize vSphere Performance

### Knowledge

- Identify appropriate BIOS and firmware setting requirements for optimal ESX/ESXi Host performance
- Identify appropriate ESX driver revisions required for optimal ESX/ESXi Host performance
- Recall where to locate information resources to verify compliance with VMware and third party vendor best practices

### Skills and Abilities

- Tune ESX/ESXi Host and Virtual Machine memory configurations
- Tune ESX/ESXi Host and Virtual Machine networking configurations
- Tune ESX/ESXi Host and Virtual Machine CPU configurations
- Tune ESX/ESXi Host and Virtual Machine storage configurations
- Configure and apply advanced ESX/ESXi Host attributes
- Configure and apply advanced Virtual Machine attributes
- Tune and optimize NUMA controls

### Tools

- vSphere Resource Management Guide
- vSphere Command-Line Interface Installation and Scripting Guide
- Performance Troubleshooting for VMware vSphere 4
- Product Documentation
- vSphere Client
    - Performance Graphs
- vSphere CLI
    - vicfg-*
    - resxtop/esxtop
    - vscsiStats

## Notes

**Identify appropriate BIOS and firmware setting requirements for optimal ESX/ESXi Host performance**
Some of this will vary system to system so this is going to be one where you play around a bit and get outside of your comfort zone and using the type of system you usually do.

Hyperthreading

- ESX(i) will use hyperthreading by default, but it may need to be enabled in the bios.
- Cannot enable hyperthreading on a system with great then 32 physical cores because of the logical limit of 64 CPUs
- http://www.dabcc.com/article.aspx?id=9482

Enable Power Management

- Enable power management or Demand-Based Switching (DBS) in the bios.
- You can then configure the CPU power management policy in the advanced host attribute, Power.CpuPolicy
- You will set this to either static (default) or dynamic. In dynamic the VMkernel optimizes each CPU's frequency to match demand. When CPU demands increase the policy ensures that CPU frequencies also increase.
- With static the VMkernel can detect power management feature available on the host but doesn't actively use them unless requested to do so by the BIOS.

**Identify appropriate ESX driver revisions required for optimal ESX/ESXi Host performance**

- Same as the above, this will vary implementation to implementation. Be aware of the memory requirements for drivers.
- Some drivers need 40MB, which almost doubles base system memory.
- An ESXi host uses additional system memory for management agents that run in the service console of an ESX host.

**Recall where to locate information resources to verify compliance with VMware and third party vendor best practices**
http://www.vmware.com/resources/compatibility/search.php?ie=UTF-8&q=vmware%20hcl

**Tune ESX/ESXi Host and Virtual Machine memory configurations**
For these tuning sections I am going to recommend referring to the troubleshooting sections I've previously covered as well as the links at the bottom of these notes.
http://www.vfail.net/?p=191

**Tune ESX/ESXi Host and Virtual Machine networking configurations**
For these tuning sections I am going to recommend referring to the troubleshooting sections I've previously covered as well as the links at the bottom of these notes.
http://www.vfail.net/2010/08/14/vcap-dca-objective-6-3-troubleshoot-network-performance-and-connectivity/

**Tune ESX/ESXi Host and Virtual Machine CPU configurations**
For these tuning sections I am going to recommend referring to the troubleshooting sections I've previously covered as well as the links at the bottom of these notes.
http://www.vfail.net/?p=191

**Tune ESX/ESXi Host and Virtual Machine storage configurations**
For these tuning sections I am going to recommend referring to the troubleshooting sections I've previously covered as well as the links at the bottom of these notes.
http://www.vfail.net/2010/08/18/objective-6-4-troubleshoot-storage-performance-and-connectivity/

**Configure and apply advanced ESX/ESXi Host attributes**
From pg. 97-99 of the vSphere Resource Management Guide

The process is easy but you will need to be familiar with a lot of different advanced settings and the pages above contain those settings.

- In the vSphere Client inventory panel, select the host to customize.
- Click the Configuration tab.
- In the Software menu, click Advanced Settings.
- In the Advanced Settings dialog box select the appropriate item (for example, CPU or Memory), and scroll in the right panel to find and change the attribute.

**Configure and apply advanced Virtual Machine attributes**
pg. 99 of the vSphere Resource Management Guide

- Select the virtual machine in the vSphere Client inventory panel, &select Edit Settings from right click menu.
- Click Options and click Advanced > General.
- Click the Configuration Parameters button.
- In the dialog box that appears, click Add Row to enter a new parameter and its value.

Advanced Virtual Machine Attributes

- sched.mem.maxmemctl Maximum amount of memory reclaimed from the selected virtual machine by ballooning, in megabytes (MB). If the ESX/ESXi host needs to reclaim additional memory, it is forced to swap. Swapping is less desirable than ballooning.
- sched.mem.pshare.enable Enables memory sharing for a selected virtual machine. This boolean value defaults to True. If you set it to False for a virtual machine, this turns off memory sharing.
- sched.swap.persist Specifies whether the virtual machine's swap files should persist or be deleted when the virtual machine is powered off. By default, the system creates the swap file for a virtual machine when the virtual machine is powered on, and deletes the swap file when the virtual machine is powered off.
- sched.swap.dir VMFS directory location of the virtual machine's swap file. Defaults to the virtual machine's working directory, that is, the VMFS directory that contains its configuration file. This directory must remain on a host that is accessible to the virtual machine. If you move the virtual machine (or any clones created from it), you might need to reset this attribute.

**Tune and optimize NUMA controls**
Pg. 73-77 of the vSphere Resource Management Guide

- The VMkernel.Boot.sharePerNode option controls whether memory pages can be shared (de-duplicated) only within a single NUMA node or across multiple NUMA nodes.
- VMkernel.Boot.sharePerNode is turned on by default, and identical pages are shared only within the same NUMA node. This improves memory locality, because all accesses to shared pages use local memory.
- In most situations the ESX(i) host's automatic NUMA optimizations will result in good performance, however you may need to tune this.
- You can do this through controlling memory and processor placement via CPU and Memory Affinity.

**Other Relevant Reading Related To This Section**

- http://www.virtualinsanity.com/index.php/2010/03/29/performance-troubleshooting-vmware-vSphere-network/
- http://www.virtualinsanity.com/index.php/2010/03/16/performance-troubleshooting-vmware-vSphere-storage/

- http://www.virtualinsanity.com/index.php/2010/02/19/performance-troubleshooting-vmware-vSphere-memory/
- http://www.virtualinsanity.com/index.php/2010/02/15/performance-troubleshooting-vmware-vSphere-cpu/

## Objective 3.2 – Optimize Virtual Machine Resources

### Knowledge

- Compare and contrast virtual and physical hardware resources
- Identify VMware memory management techniques
- Identify VMware CPU load balancing techniques
- Identify pre-requisites for Hot Add features

### Skills and Abilities

- Calculate available resources
- Properly size a Virtual Machine based on application workload
- Configure large memory pages
- Understand appropriate use cases for CPU affinity

### Tools

- vSphere Resource Management Guide
- vSphere Command-Line Interface Installation and Scripting Guide
- Understanding Memory Resource Management in VMware® ESX™ Server 4.1
- VMware vSphere™ : The CPU Scheduler in VMware® ESX™ 4.1
- vSphere Client
    - Performance Charts
- vSphere CLI
    - resxtop/esxtop

## Notes

**Identify VMware memory management techniques**
http://www.vmware.com/files/pdf/perf-vSphere-memory_management.pdf

**Identify VMware CPU load balancing techniques**
See the vSphere 4: The CPU Scheduler in VMware ESX4 Whitepaper and PG 73 of the vSphere 4 Resource Management Guide. From the Guide:

> ***NUMA Systems***
>
> *In a NUMA (Non-Uniform Memory Access) system, there are multiple NUMA nodes that consist of a set of processors and the memory.*
>
> *The NUMA load-balancer in ESX assigns a home node to a virtual machine. For the virtual machine, the memory is allocated from the home node. Since the virtual machine rarely migrates away from the home node, the memory access from the virtual machine is mostly local. Note that all vCPUs of the virtual machine are scheduled within the home node.*
>
> *If a virtual machine's home node is more heavily loaded than others, migrating to a less loaded node generally improves performance, although it suffers from remote memory accesses. The memory migration may also happen to increase the memory-locality. Note that the memory is moved gradually because copying memory has high overhead.*
>
> ***Hyperthreaded Systems***
>
> *Hyperthreading enables concurrently executing instructions from two hardware contexts in one processor. Although it may achieve higher performance from thread-level parallelism, the improvement is limited as the total computational resource is still capped by a single physical processor. Also, the benefit is heavily workload dependent.*
>
> *It is clear that a whole idle processor, that has both hardware threads idle, provides more CPU resource than only one idle hardware thread with a busy sibling thread. Therefore, the ESX CPU scheduler makes sure the former is preferred as the destination of a migration.*

**Identify pre-requisites for Hot Add features**
A couple of good blogs by David Davis and Jason Boche outline what and how to use Hot-Add/Hot-Plug. The ability to use this without having to reboot the guest virtual machine is extremely limited. ON the Microsoft side Windows 2008 Server Datacenter is necessary to support both features without a reboot while Windows 2008 Server Enterprise edition does not require a reboot for Hot Adding memory. When it comes to removing either hot added memory or hot plugged CPUs a reboot is required for all Windows guest operation systems.

**Properly size a Virtual Machine based on application workload**
Most physical machines do not need the 8 cores and 16 GB of memory or so they have assigned to them. When bringing a physical system over take note of what is assigned and properly allocate and plan for what is actually needed.

For memory, make sure you have enough to run the applications needed on the server. Avoid memory swapping, but also avoid allocating more memory then is needed. When this is done, the virtual machine's memory overhead is increased, taking away from the resources that other virtual machines could potentially use.

When sizing the number of processors the same concept applies. If the application(s) can't utilize more than 2 CPUs then there really is not much good in giving more than two CPUs.

**Configure large memory pages**
http://www.vmware.com/pdf/Perf_Best_Practices_vSphere4.1.pdf

**Large Memory Pages for Hypervisor and Guest Operating System**
In addition to the usual 4KB memory pages, ESX also makes 2MB memory pages available (commonly referred to as "large pages"). By default ESX assigns these 2MB machine memory pages to guest operating systems that request them, giving the guest operating system the full advantage of using large pages. The use of large pages results in reduced memory management overhead and can therefore increase hypervisor performance.

If an operating system or application can benefit from large pages on a native system, that operating system or application can potentially achieve a similar performance improvement on a virtual machine backed with 2MB machine memory pages. Consult the documentation for your operating system and application to determine how to configure them each to use large memory pages.
More information about large page support can be found in the performance study entitled Large Page Performance (available at http://www.vmware.com/files/pdf/large_pg_performance.pdf).

**Enabling Large Page Support in Windows Server 2003**:
http://www.vmware.com/files/pdf/large_pg_performance.pdf

To enable large page support in Windows Server 2003, the system administrator must grant appropriate users the privilege to "Lock pages in memory." This privilege is not enabled by default when Windows is installed. To grant this privilege, take the following steps:

1. Choose Start > Control Panel > Administrative Tools > Local Security Policy.
2. In the left pane of the Local Security Settings window, expand Local Policies and choose User Rights Assignment.
3. In the right pane of the Local Security Settings window, choose Lock pages in memory and choose Action > Properties. The Local Security Setting dialog box opens.
4. In the Local Security Setting dialog box, click Add User or Group.
5. Enter the appropriate user name, then click OK to close the Select Users or Groups dialog box.

**Understand appropriate use cases for CPU affinity**

- CPU intensive app, move away from core 0
- A good example that requires this is Cisco's Unity
- No HA if one of the VMs has CPU affinity set.

A must read on this topic is this article from Duncan Epping

## Objective 3.3 – Implement and Maintain Complex DRS Solutions

### Knowledge

- Explain DRS affinity and anti-affinity rules
- Identify required hardware components to support DPM
- Identify EVC requirements, baselines and components
- Understand the DRS slot-size algorithm and its impact on migration recommendations

### Skills and Abilities

- Properly configure BIOS and management settings to support DPM
- Test DPM to verify proper configuration
- Configure appropriate DPM Threshold to meet business requirements
- Configure EVC using appropriate baseline
- Change the EVC mode on an existing DRS cluster
- Create DRS and DPM alarms
- Configure applicable power management settings for ESX Hosts
- Properly size virtual machines and clusters for optimal DRS efficiency
- Properly apply virtual machine automation levels based upon application requirements

### Tools

- vSphere Resource Management Guide
- Product Documentation
- vSphere Client
    - DRS Resource Distribution Chart

## Notes

**Explain DRS affinity and anti-affinity rules**

- Specifies that two or more virtual machines are placed on the same host or on different hosts.
- When a conflict in rules occurs, the older rule takes precedence and the new rule is disabled.
- Disabled rules are then ignored.
- Higher precedence is given to preventing violations of anti-affinity rules then violations of affinity rules.

**To check on affinity rule violations**

1. Select the cluster in the inventory panel of the vSphere Client
2. Select the DRS tab, and click Faults
3. Any rule currently being violated has a corresponding fault on this page. Read the fault to determine why DRS is not able to satisfy the particular rule.

**Identify required hardware components to support DPM**

- Uses IPMI, iLO or WOL
- If one of those three is not supported, DPM can put the host in standby mode.
- If a host supports multiple protocols, the order of precedence is IPMI, iLO, WOL.
- For WOL make sure WOL is supported for physical NICs

**Identify EVC requirements, baselines and components**

- Configured at Cluster Level
- Helps to ensure vMotion compatibility for the hosts in a cluster by presenting the same CPU feature set to virtual machines.
- Must use same CPU vendors in cluster
- Verify CPU compatibility here VMware KB1003212
- Intel VT or AMD-V
- XD (Execute Disable) or NX (No Execute)

**Properly configure BIOS and management settings to support DPM**

- See some of the information above. You will want to make sure you properly configure IPMI/iLO as well as WOL if used. WOL will need to be configured and supported for the NIC.

**Test DPM to verify proper configuration**

- Manually put a host into standby
- Power off VM resources to let DPM take action based on the configured DPM Threshold

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

- Similar to DRS, the DPM power on/off recommendations are assigned priorities ranging from 1 to 5 stars.
- Priority 1 is mandatory while priority five will bring just a slight improvement.
- Configured per cluster under Power Management.
- You can override DPM on a host level, specifying particular hosts you would like to only manually involve or disable involvement entirely.

**Configure EVC using appropriate baseline**

This VMware KB1003212 covers this topic in depth. In it you can find what version of vSphere/ESX support what baselines and what CPUs support what baselines.

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

- Cluster Settings—>VMware EVC

**Create DRS and DPM alarms**

Check out this spreadsheet for a complete list of DRS alarms.

http://communities.vmware.com/servlet/JiveServlet/download/12145-1-35516/vSphere%20Alarms%20v2.xlsx;jsessionid=B696F778AA032D9AE6E36FBA38F1D98D

Specifically related to DPM, your most common event to monitor for will be a failure to bring a server back online when it is needed again.

Exit Standby Error alarm: *DrsExitStandbyModeFailedEvent*

Additionally these other events exist:

Entering Standby mode (about to power off host): *DrsEnteringStandbyModeEvent*
Successfully entered Standby mode (host power off succeeded): *DrsEnteredStandbyModeEvent*
Exiting Standby mode (about to power on the host): *DrsExitingStandbyModeEvent*
Successfully exited Standby mode (power on succeeded): *DrsExitedStandbyModeEvent*

**Configure applicable power management settings for ESX Hosts**

You can set advanced host attributes to manage power settings.

*Power.CpuPolicy*: When you set this attribute to the default value of static, VMkernel does not directly set CPU power management states and only responds to requests from the BIOS. When you enable this policy (set to dynamic), VMkernel dynamically selects appropriate power management states based on current usage. This can save power without degrading performance. Enabling this option on systems that do not support power management results in an error message.

**Properly size virtual machines and clusters for optimal DRS efficiency**

Realize that not properly sizing your virtual machines will affect the efficiency of DRS. If you give a system too much memory, then less memory available to other systems. Additionally, the overhead for the system will be higher with a higher amount of configured memory. Ultimately this can result in an increased slot size. One big mistake you can make is simply porting systems over with the same specs they had when they were physical, when they don't need it. If you bring enough multi-core systems over you may see performance issues quickly.

**Properly apply virtual machine automation levels based upon application requirements**

This will override the cluster settings for that virtual machine.
Under Cluster Settings—> VMware DRS—>Virtual machine Options

- Fully Automated(default)
- Partially Automated
- Manual
- Disabled

**Other Links**

- http://frankdenneman.nl/2010/03/drs-resource-distribution-chart/
- http://www.virtualizationteam.com/uncategorized/vmware-evc-enhanced-vmotion-compatibility-enable-vmware-vmotion-across-cpu-generations.html
- http://www.yellow-bricks.com/2010/03/09/vm-powered-on-alarm/

## Objective 3.4 – Perform Capacity Planning in a vSphere Environment

### Knowledge

- Understand the DRS slot-size algorithm and its impact on migration recommendations
- Identify tools needed for monitoring capacity planning
- Identify performance metrics related to resource contention and saturation

### Skills and Abilities

- Predict when additional ESX/ESXi Host, network or storage resources will be required by observing an existing environment
- Determine when to expand or contract provisioned Virtual Machine resources based upon observed Virtual Machine utilization
- Interpret performance metrics from vCenter to properly size the environment

### Tools

- vSphere Resource Management Guide
- Overview Performance Charts Help
- Product Documentation
- vSphere Client

## Notes

**Predict when additional ESX/ESXi Host, network or storage resources will be required by observing an existing environment**

Properly planning for capacity can help avoid this, but sometimes you just outgrow your environment. vCenter now has many more charts and resources that will give you a visual representation of performance and other metrics. Using these metrics you can see where you are at today and the trends on utilization, targeting the need to increase storage, network, or host requirements for your environment.

**Determine when to expand or contract provisioned Virtual Machine resources based upon observed Virtual Machine utilization**

After you have provisioned a virtual machine you may find it is not performing as well. The first question to ask is if this virtual machine has lesser resources then its physical counterpart did before. If so you will want to increase the CPU, memory, or storage requirements to get closer towards the original configuration.

Often times though the physical host will be way more powerful than the virtual machine needs to be. Giving a virtual machine more than enough resources will ensure it runs smoothly, but it will also waste expensive resources and prevent or hinder those resources from being utilized by other virtual machines. One big an mid-sized virtual machine with any customization to the slot size settings can heavily affect the slot size of your environment.

Refer to the other sections for VCAP-DCA troubleshooting to go through ESXTOP and other performance monitoring metrics.

**Interpret performance metrics from vCenter to properly size the environment**

Depending on your experience level it may not be completely straight forward what you are looking for here. Check out this document from VMware to gain a better understanding of performance charts in vCenter and what you are looking for.

## Objective 3.5 – Utilize Advanced vSphere Performance Monitoring Tools

### Knowledge

- Identify hot keys and fields used with resxtop/esxtop
- Identify fields used with vscsiStats

### Skills and Abilities

- Configure esxtop/resxtop custom profiles
- Determine use cases for and apply esxtop/resxtop Interactive, Batch and Replay modes
- Use vscsiStats to gather storage performance data
- Use esxtop/resxtop to collect performance data
- Given esxtop/resxtop output, identify relative performance data for capacity planning purposes

### Tools

- vSphere Resource Management Guide
- vSphere Command-Line Interface Installation and Scripting Guide
- Product Documentation
- vSphere Client
- vSphere CLI
    - esxtop/resxtop
    - vscsiStats

## Notes

Reading through the following three links will give you a great insight into using esxtop and vscsiStats.

- http://communities.vmware.com/docs/DOC-11812.pdf
- http://www.yellow-bricks.com/esxtop/
- http://www.yellow-bricks.com/2009/12/17/vscsistats/

**Identify hot keys and fields used with resxtop/esxtop**
See vSphere CLI Reference section for esxtop

**Identify fields used with vscsiStats**
See vSphere CLI Reference section for vscsiStats.

**Configure esxtop/resxtop custom profiles**

1. Load esxtop
2. Use hot keys to configure how you would like.
   - 'f' will add and remove fields
   - 'o' will change the order
   - other hot keys will give you settings specific to that view.
3. 'W' will save the settings to a new config file
4. Next time you load esxtop use the '-c' option to specify a configuration file

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

Batch

- Batch mode allows collection that will be captured to a file.
  - *esxtop –b > file.csv*

Replay

- Esxtop will replay resource utilization stats that were collected using the vm-support command
- The capture from the vm-support command would have been generated by the following command
  - *vm-support –s –d duration –I interval*
- You would then unzip/untar this for esxtop to use it.
  - *esxtop –R <path to dir>*

**Use vscsiStats to gather storage performance data**
http://communities.vmware.com/docs/DOC-10095
http://www.gabesvirtualworld.com/converting-vscsistats-data-into-excel-charts/

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

Again check out the links mentioned above in this section. They are a must read and will be a great guide in helping to identify performance related issues.

# VDCA410 Section 4 – Manage Business Continuity and Protect Data

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

### Knowledge

- Identify the three admission control policies for HA
- Identify heartbeat options and dependencies

### Skills and Abilities

- Calculate host failure requirements
- Configure customized isolation response settings
- Configure HA redundancy in a mixed ESX/ESXi environment
- Configure HA related alarms and monitor an HA cluster
- Create a custom slot size configuration
- Understand interactions between DRS and HA
- Create an HA solution that ensures primary node distribution across sites
- Analyze vSphere environment to determine appropriate HA admission control policy
- Analyze performance metrics to calculate host failure requirements
- Analyze Virtual Machine workload to determine optimum slot size
- Analyze HA cluster capacity to determine optimum cluster size

### Tools

- vSphere Availability Guide
- Product Documentation
- vSphere Client

## Notes

**Configure customized isolation response settings**

- The isolation response is the action HA will take when the heartbeat network is isolated. The response is either power off, leave powered on (default), or shut down.
- HA will try to restart the affected Virtual Machines and by default will try up to five times. This is configurable with the parameter das.maxvmrestartcount
- The default value for isolation failure detection is 15 seconds. This is configurable with the parameter das.failuredetectiontime
- At this point a restart is initiated by one of the primary hosts. The isolation response is actually initiated 1 second before the failure detection time.

Read the below excerpt from Duncan Epping's blog on why it is important to understand these different parameters and what affect configuring isolation response settings can have on your environment.

> *The default value for isolation/failure detection is 15 seconds. In other words the failed or isolated host will be declared dead by the other hosts in the HA cluster on the fifteenth second and a restart will be initiated by one of the primary hosts.*
>
> *For now let's assume the isolation response is "power off". The "power off" (isolation response) will be initiated by the isolated host 1 second before the das.failuredetectiontime. A "power off" will be initiated on the fourteenth second and a restart will be initiated on the fifteenth second.*
>
> *Does this mean that you can end up with your VMs being down and HA not restarting them?*
> *Yes, when the heartbeat returns between the 14th and 15th second the "power off" could already have been initiated. The restart however will not be initiated because the heartbeat indicates that the host is not isolated anymore.*
>
> *How can you avoid this?*
> *Pick "Leave VM powered on" as an isolation response. Increasing the das.failuredetectiontime will also decrease the chances of running in to issues like these.*
>
> *Basic design principle: Increase "das.failuredetectiontime" to 30 seconds (30000) to decrease the likely-hood of a false positive.*
>
> *A couple of additional parameters I've found necessary*
>
> *das.isolationaddressx Used to configure multiple isolation addresses.*
>
> *das.usedefaultisolationaddress Set to true/false and used in the cse where a default gateway is not pingable, in which case this set to false in conjunction with configuring another address for das.isolationaddress*

**Configure HA redundancy in a mixed ESX/ESXi environment**

- Redundant management networks are recommended for HA and there are two options to choose from, Network Redundancy Using NIC Teaming or Network Redundancy Using a Secondary Network.

**Create a custom slot size configuration**

A slot refers to a logical representation to power on a virtual machine in the cluster, taking into account memory and CPU resources that will satisfy this request.

Slot size is calculated using the highest CPU and memory reservation of any given VM, with a default of 256mhz for CPU and 0MB + memory overhead if no reservations are specified.

Set das.slotCpuInMHz or das.slotMemInMB to manually lower the slot size in cases where one VM causes a really large slot size.

**Understand interactions between DRS and HA**

4.1 has brought a lot of changes to this topic and until I know with certainty that 4.1 will not be included any time soon I will shy away from speaking of those changes.

In terms of functionality today, DRS and HA while separate pieces do work together to provide availability and performance. When a host goes down and HA performs a failover and restarts a virtual machine it is looking for to provide availability. It is then DRS's job to balance these machines across the cluster.

**Create an HA solution that ensures primary node distribution across sites**

The first 5 hosts that join the HA cluster are automatically selected as primary nodes.

You can manually view which nodes are primary with this command

*cat /var/log/vmware/aam/aam_config_util_listnodes.log*

Re-election of a primary will only occur when a primary is placed in maintenance mode, disconnected or removed from the cluster, or when a cluster is reconfigured for HA.

If all fail simultaneously, there is no HA initiated restart of VMs that occur.

In order to design an HA solution that ensures a primary is always available, the placement of your hosts is crucial. For each cluster, never put more than four hosts in a place where it could be a single point of failure, for example a chassis of blades. If you have 10 blades and two chassis, look to separate the blades amongst two chassis, and additionally make sure that no more than four blades are from one cluster in each chassis.

Read more about this concept here: http://www.yellow-bricks.com/2009/02/09/blades-and-ha-cluster-design/

**Analyze vSphere environment to determine appropriate HA admission control policy**

You have three choices for HA admission control policies

Host failures cluster tolerates

- Host with most slots is taken out of the equation, and then the next most if more than one 1 is set.
- Your percentage of resources should be equal or larger than your largest host so that all VMs on that host can be restarted.
- Tends to be very conservative as largest reservation dictates the slot size.

Percentage of cluster resources reserved as failover spare capacity

- Instead of using slot sizes, sets a percentage of resources to be left unused for HA purposes
- Tends to be a more realistic view of reservations as it uses actual reservations vs. slot size.
- More flexible.

Specify a failover host

- Specifies a single host specifically for failover purposes. You may end up with a lot of reserved capacity for failover, but you also will only get a single host for use as a failover server.

**Analyze Virtual Machine workload to determine optimum slot size**

If you are manually specifying the memory and CPU values for the slot size, make sure the slot size is representative of typical workloads.

**Analyze HA cluster capacity to determine optimum cluster size**

How many hosts in your cluster?

How many host failures can you tolerate?

What is the resource utilization of your virtual machines?

Other Relevant Articles and Links Related to this Section

- http://searchsystemschannel.techtarget.com/generic/0,295582,sid99_gci1515486,00.html
- http://www.dailyhypervisor.com/2009/03/31/vmware-ha-cluster-sizing-considerations/
- http://www.yellow-bricks.com/vmware-high-availability-deepdiv/
- http://www.b3rg.nl/vcdx/section-4-business-continuity-and-data-protection/objective-4.2-configure-advanced-ha-deployments.html
- http://geeksilver.wordpress.com/2010/10/04/vcap-dca-section-4-%E2%80%93-manage-business-continuity-and-protect-data-objective-4-1/

## Objective 4.2 – Deploy and Test VMware FT

### Knowledge

- Identify VMware FT hardware requirements
- Identify VMware FT compatibility requirements

### Skills and Abilities

- Modify VM and ESX/ESXi Host settings to allow for FT compatibility
- Use VMware best practices to prepare a vSphere environment for FT
- Configure FT logging
- Prepare the infrastructure for FT compliance
- Test FT failover, secondary restart and application fault tolerance in a FT Virtual Machine

### Tools

- vSphere Availability Guide
- Product Documentation
- vSphere Client

## Notes

This is a fairly quick objective to run through. I recommend giving Eric Siebert's blog article a good read if you are not familiar with the requirements and concepts behind fault tolerance. Additionally Vladan Seget has a great blog on troubleshooting FT.

**Identify VMware FT hardware requirements**

Requires a Fault Tolerance capable processor and both hosts but have the same processor family. While the speeds don't have to match remember that FT relies on close synchronization so the closer they are the better.

**Identify VMware FT compatibility requirements**

- Same Build number for ESX(i) hosts
- Gigabit NIC's
- Common Shared Storage
- Single Proc machine
- Thin Provisioned disks not supported (automatically converted)
- No snapshots

**Use VMware best practices to prepare a vSphere environment for FT**

Use the VMware Site Survey utility to check configuration compatibility with advanced features such as Fault Tolerance.

**Configure FT logging**

- Check the box on the virtual NIC for "Use this virtual adapter for Fault Tolerance logging"
- Separate NIC for FT Logging and vMotion recommended.

**Prepare the infrastructure for FT compliance**

On the Summary page of each host you will see the status of Fault Tolerance and can view the requirements you will need to take action on there.

**Other relevant blogs and websites related to this section**

- http://itknowledgeexchange.techtarget.com/virtualization-pro/masters-guide-to-vmware-fault-tolerance/
- http://www.vmware.com/files/pdf/resources/ft_virtualization_wp.pdf
- http://www.vladan.fr/troubleshooting-fault-tolerance-in-vSphere/

## Objective 4.3 – Configure a vSphere Environment to support MSCS Clustering

### Knowledge

- Identify MSCS clustering solution requirements
- Identify the three supported MSCS configurations

### Skills and Abilities

- Configure Virtual Machine hardware to support cluster type and guest OS
- Configure a MSCS cluster on a single ESX/ESXi Host
- Configure a MSCS cluster across ESX/ESXi Hosts
- Configure standby host clustering

### Tools

- Setup for Failover Clustering and Microsoft Cluster Service
- Product Documentation
- vSphere Client

## Notes

Your biggest resource for this section will be the Setup for Failover Clustering and Microsoft Cluster Service document from VMware.

**Knowledge**

**Identify MSCS clustering solution requirements**

**Identify the three supported MSCS configurations**

- Clustering virtual machines on a single host
- Storage can be local or on a SAN.
- Clustering virtual machines across physical hosts
- Clustering physical machines with virtual machines

**Configure Virtual Machine hardware to support cluster type and guest OS**

- See requirements above.

**Configure a MSCS cluster on a single ESX/ESXi Host**

- Refer to the Setup for Failover Clustering and Microsoft Cluster Service document for complete guidance on the process. Note that with a cluster on a single box you could use local storage or shared storage.
- A cluster on a single ESX(i) host requires A separate physical network adapter for clustered virtual machines to connect with external hosts.

**Configure a MSCS cluster across ESX/ESXi Hosts**

A cluster across ESX(i) hosts requires

- Two physical network adapters dedicated to the MSCS cluster and to the public and private networks.
- One physical network adapter dedicated to the service console (ESX hosts) or the VMkernel (ESXihosts).
- Fibre Channel (FC) SAN. Shared storage must be on an FC SAN.
- RDM in physical compatibility (pass-through) or virtual compatibility (non-pass-through) mode. VMware recommends physical compatibility mode. The cluster cannot use virtual disks for shared storage.
- Note-Failover clustering with Windows Server 2008 is not supported with virtual compatibility mode (nonpass-through) RDMs.
- Refer to the Setup for Failover Clustering and Microsoft Cluster Service document for complete guidance on the process.

**Configure standby host clustering (Cluster physical and virtual machines)**

Standby host clustering requires:

- Two physical network adapters dedicated to the MSCS cluster and to the public and private networks.
- One physical network adapter dedicated to the service console (ESX hosts) or the VMkernel (ESXi hosts).
- Use RDMs in physical compatibility mode (pass-through RDM). You cannot use virtual disks or RDMs in virtual compatibility mode (non-pass-through RDM) for shared storage.
- Use the STORport Miniport driver for the Fibre Channel (FC) HBA (QLogic or Emulex) in the physicalWindows machine.
- Do not run multipathing software in the physical or virtual machines.
- Use only a single physical path from the host to the storage arrays in standby host configurations.
- Refer to the Setup for Failover Clustering and Microsoft Cluster Service document for complete guidance on the process.

**The following limitations also exist to using MSCS clustering(not supported)**

- Clustering on iSCSI, FCoE, and NFS disks.
- Mixed environments, such as configurations where one cluster node is running a different version of ESX/ESXi than another cluster node.

- Clustered virtual machines as part of VMware clusters (DRS or HA).
- Use of MSCS in conjunction with VMware Fault Tolerance.
- Migration with vMotion of clustered virtual machines.
- N-Port ID Virtualization (NPIV)
- With native multipathing (NMP), clustering is not supported when the path policy is set to round robin.
- You must use hardware version 7 with ESX/ESXi 4.0.

**Other Relevant Reading related to this Section**

- http://www.infortrend.com/doc/appNote/APP_Note_MSCS%20in%20vSphere4.pdf
- http://kb.vmware.com/kb/1004617
- http://www.yellow-bricks.com/2009/06/03/mscs-vms-in-a-hadrs-cluster/
- http://www.boche.net/blog/index.php/2009/04/01/setup-for-microsoft-cluster-service/
- http://blog.vmote.net/?p=248

## Objective 4.4 – Deploy and Maintain vCenter Server Heartbeat

### Knowledge

- Identify the five protection levels for vCenter Server Heartbeat
- Identify the three server protection options for vCenter Server Heartbeat
- Identify supported cloning options

### Skills and Abilities

- Install and configure vCenter Server Heartbeat
- Determine use cases for and execute a manual switchover
- Recover from a failover
- Monitor vCenter Server Heartbeat and communication status
- Configure heartbeat settings
- Configure shutdown options
- Configure application protection
- Add/Edit Services
- Add/Edit Tasks
- Edit/Test Rules
- Install/Edit Plug-ins
- Add/Remove Inclusion/Exclusion Filters
- Perform Full System and Full Registry checks
- Configure/Test Alerts
- Troubleshoot common vCenter Server Heartbeat error conditions

### Tools

- vCenter Server Heartbeat QuickStart Guide
- vCenter Server Heartbeat Reference Guide
- Product Documentation
- vSphere Client

## Notes

Your main resource for this section will be the vCenter Server Heartbeat and Reference Guide and most of the following notes are directly from that document.

**Identify the five protection levels for vCenter Server Heartbeat**

- Server Protection- Provides continuous availability to end users through hardware failures or operating system crashes.
- Network Protection- Polls up to three nodes and ensures that the active server is visible on the network.
- Application Protection- Ensures applications and services stay alive on the network.
- Performance Protection- Monitors specific application attributes to ensure they remain within normal operating ranges.
- Data Protection- Intercepts data and maintains a copy of the data on the passive server for use in the event of a failure.

**Identify the three server protection options for vCenter Server Heartbeat**

- vCenter Server with SQL on same host
- vCenter Server with SQL Server on separate host
- vCenter Server only

**Identify supported cloning options**

- For creating supported pre-cloned images for use as a secondary server you can either use VMware Converter for a P2V or VMware vCenter to clone a VM for a V2V.
- At the time of installation you may also select "Not a clone of the Primary Server". This option will run a clone process for the specified secondary (physical or vm) and clone the servers for you.

**Install and configure vCenter Server Heartbeat**

RTFM on this one and even literally if you take a look at the recent blogs from Mike Laverick, the first 2 of a four part series.

**Determine use cases for and execute a manual switchover**

You can click Make Active on the vCenter Server Heartbeat Console Server: Summary page to manually initiate a managed switchover. When a managed switchover is triggered, the running of protected applications is transferred from the active machine to the passive machine in the server pair. The server roles are reversed.

**Recover from a failover**

1. Correct the conditions that caused the failover.
2. Verify the integrity of the disk data on the failed server.
3. Restart the failed, now passive, server after all issues are resolved.
4. Start vCenter Server Heartbeat on the passive server.
   At this point, the instances of vCenter Server Heartbeat running on the servers connect and begin to re-synchronize the data on the Primary server.
5. Wait until vCenter Server Heartbeat is fully synchronized. When the re-synchronization is complete, you can continue operating with this configuration (for example, the Secondary server is the active server and the Primary server is the passive server), or initiate a managed switchover.
6. Optionally, perform a managed switchover to return the Primary and Secondary servers to the same roles they had before the failover.

**Monitor vCenter Server Heartbeat and communication status**

The server monitoring page provides information about the status of communications between the pair of vCenter servers. In addition to a heartbeat a ping is also sent to ensure the servers can see each other.

**Configure heartbeat settings**

On the server monitoring page you can configure pings, configure failover, and configure response times.
To configure pings

1. Click Configure Pings to open the Server Monitoring: Ping Configuration dialog.
2. Click on the Ping Settings tab to configure the Ping Interval.
3. Click on the Ping Routing tab to add additional IP address for redundant NICs.

To configure failover(default 60 seconds)

1. Click Configure Failover to open the Server Monitoring: Failover Configuration dialog.
2. Type a new numeric value (seconds) in the Failover timeout text box or use the arrow buttons to set a new value.
3. Mark or clear the check boxes to select the actions to take if the specified Failover timeout is exceeded.
4. Click OK.

To configure response times

1. Click Configure Response Times to open the Server Monitoring: Response Times dialog.
2. Type new numeric values (seconds) into the text boxes or use the arrow buttons to select new values.
3. Click OK.

**Configure shutdown options**
Shutdown — Prompts you to select the server(s) to shut down. If you select the active server, additional options to stop or not stop protected applications appear in the dialog. Click OK.

**Configure application protection**
To configure applications

1. Click Configure on the Applications page.
   You can protect services and start monitoring applications or unprotect services and stop monitoring applications. You can also enable Verbose Plugin logging, Discover protected data at startup, Discover protected services at startup, and set the rule trigger count.
2. After making modifications to the configuration, click OK.

**Add/Edit Services**
To protect a service

1. Right-click on a service and select Add from the menu or click Add on Applications: Services page to invoke the Add Service dialog. The Name drop-down list contains a list of all currently running services.
2. Select the service and set the values for Target State on Active and Target State on Passive. Normally the Target State on Active is set to Running and the Target State on Passive is set to Stopped.
3. If vCenter Server Heartbeat is to manage the start and stop of the service, select Manage Starting and Stopping. If vCenter Server Heartbeat is to monitor the state of the service, select Monitor State. vCenter Server Heartbeat also assigns three sequential tasks to perform in the event of failure. Task options include Recover Service, Application Restart, Log Warning, Switchover, and any additional user-defined tasks previously created.
4. Assign a task to each of the three failure options and click OK.

Editing a Service

1. Select the service and click Edit. The Edit Service dialog opens to provide a subset of same options available when adding a new service.
2. Make the modifications and click OK.

**Add/Edit Tasks**
To add a task

1. Click Add to invoke the Add Task dialog. Assign a name to the task.

2. Select the task type from the drop-down list.
3. Select the identity of the server the task runs on (Primary or Secondary).
4. In the Command text box, type in the path or browse to the script, .bat file, or command for the task to perform.
5. Click OK.

Editing a Task

1. Right-click on an existing task and select Edit from the menu or select the task and click Edit at the top of the pane to invoke the Edit Task dialog.
2. Edit the parameters of the task.
3. Click OK.

**Edit/Test Rules**

To edit a rule

1. Right-click on the rule and select Edit from the menu or click Edit at the top of the pane.
2. Edit the parameters of the rule and click OK.

To check a rule condition

1. Right-click on the rule and select Check Now from the menu or click Check Now at the top of the pane. The rule condition is displayed in the pane.

**Install/Edit Plug-ins**

To install a new plug-in

1. Click Applications: Plugin to open the Plugins page.
2. Right-click an existing plug-in and select Install from the menu or click Install at the top of the pane to invoke the Install Plugins dialog.
3. Type a path to the plug-in location or click Browse to navigate to the plug-in location. The path statement is case-sensitive.
4. Click OK.

To edit the plug-in configuration

1. Right-click on an existing plug-in from the Plugins list and select Edit from the menu or select the plug-in and click Edit at the top of the pane to invoke the Edit Plugin dialog.
2. Review the configuration options before making modifications as they are specific to each plug-in.
3. Click OK.

**Add/Remove Inclusion/Exclusion Filters**

To define filters that include files and folders for protection and replication

1. In the Data: File Filters pane, click Add Inclusion Filter to open the Add Inclusion Filter dialog.
2. Type the complete path and pattern, specify a pattern containing wildcards, or use Browse to locate the file or folder.
3. Click OK. The two forms of wildcards available are *, which matches all files in the folder, and **, which matches all files, subfolders and the files in the subfolders of the folder. After defining the filter, you can add additional Inclusion Filters.
4. Inclusion and exclusion filters can be edited by selecting the filter and clicking Edit at the top of the File Filters pane or right-clicking the filter and selecting Edit from the menu. Edit the value in the Pattern: text box by typing over the current file filter definition.

**Perform Full System and Full Registry checks**

1. To initiate a full registry check Click Full Registry Check in the Registry Synchronization pane.

2. When you click Full System Check, a dialog asks you to confirm the request and warns you that depending on the amount of data under protection, this task can take a long time to complete (for example, a number of hours). Click Yes to perform the check.

**Configure/Test Alerts**
You can configure alerts in by clicking Configure Alerts on the Logs page

1. Click Test Alert Reporting to run a test alert email. This way you can avoid triggering an actual alert during the operation of the active server

**Troubleshoot common vCenter Server Heartbeat error conditions**
Refer to the troubleshooting section of the guide of the vCenter Server Heartbeat and Reference Guide for common scenarios and troubleshooting.

**Other relevant blogs and websites related to this section**

- http://www.vmware.com/support/pubs/heartbeat_pubs.html
- https://www.vmware.com/tryvmware/p/activate.php?p=vmware-vSphere&lp=1#tab_install
- http://searchvirtualdatacentre.techtarget.co.uk/news/column/0,294698,sid203_gci1518928,00.html
- http://searchvirtualdatacentre.techtarget.co.uk/news/column/0,294698,sid203_gci1518932,00.html
- vCenter Server Heartbeat and Reference Guide

# VDCA410 Section 5 – Perform Operational Maintenance

## Objective 5.1 – Implement and Maintain Host Profiles

### Skills and Abilities

- Use Profile Editor to edit and/or disable policies
- Create sub-profiles
- Use Host Profiles to deploy vDS

### Tools

- vSphere Datacenter Administration Guide
- VMware vSphere™ 4: Deployment Methods for the VMware® vNetwork Distributed Switch
- Product Documentation
- vSphere Client

## Notes

**Create sub-profiles**

http://www.vmware.com/files/pdf/techpaper/VMW-Host-Profiles-Tech-Overview.pdf
http://blogs.vmware.com/management/2010/08/vmware-host-profiles.html
http://www.vadapt.com/2010/03/232/
http://jasonnash.wordpress.com/2009/05/04/video-demo-of-vSpheres-host-profiles/

**Use Host Profiles to deploy vDS**

http://www.vmware.com/resources/techresources/10050
http://www.virtualinsanity.com/wp-content/uploads/vDS-Implementation-Cheat-Sheet-b.pdf

**Other relevant blogs and websites related to this section**

http://www.yellow-bricks.com/2009/01/19/compare-your-hosts/
http://kb.vmware.com/kb/1017477

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

### Knowledge

- Identify firewall access rules for Update Manager

### Skills and Abilities

- Determine use case for, install and configure Update Manager Download Service
- Configure a shared repository
- Configure smart rebooting
- Manually download updates to a repository
- Perform orchestrated vSphere upgrades
- Create and modify baseline groups
- Troubleshoot Update Manager problem areas and issues
- Generate database reports using MS Excel or MS SQL
- Upgrade vApps using Update Manager

### Tools

- VMware vCenter Update Manager Installation and Administration Guide
- Product Documentation
- vSphere Client
- VMware-umds

## Notes

For the most part all of the content you are going to find for this objective can be found in the vCenter Update Manager Installation and Administration Guide.

**Identify firewall access rules for Update Manager**
Network port requirements for Update Manager are outlined in VMware KB1004543.

**Troubleshoot Update Manager problem areas and issues**
There is not a great deal of information available on the Internet specific to troubleshooting Update Manager, but installing it and playing around with it will go a long way.

You can also check out the following links for a little more information. There is also a troubleshooting section within the vCenter Update Manager Installation and Administration Guide

- http://blog.michaelburger.de/Virtuozity.php/2009/02/25/troubleshooting-vmware-update-manager
- http://www.yellow-bricks.com/2009/02/02/vmware-update-manager-sql/

**Generate database reports using MS Excel or MS SQL**
Pg 159 and 160 of the vCenter Update Manager Installation and Administration Guide

**Upgrade vApps using Update Manager**
Attach an upgrade baseline to the vApp just as you would a folder, cluster, or datacenter.

**Tools: vmware-umds**
Be sure to review the syntax of the vmware-umds command line tool on the Update Manager server. Be familiar with what it can do.

# VDCA410 Section 6 – Perform Advanced Troubleshooting

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

### Knowledge

- Identify vCenter Server log file names and locations
- Identify ESX/ESXi log files names and locations
- Identify tools used to view vSphere log files

### Skills and Abilities

- Generate vCenter Server and ESX/ESXi log bundles
- Use vicfg-syslog to configure centralized logging on ESX/ESXi Hosts
- Test centralized logging configuration
- Configure the vMA appliance as a log host
- Use vilogger to enable/disable log collection on the vMA appliance
- Use vilogger to configure log rotation and retention
- Analyze log entries to obtain configuration information
- Analyze log entries to identify and resolve issues

### Tools

- vSphere Management Assistant Guide
- vSphere Command-Line Interface Installation and Scripting Guide
- vSphere Datacenter Administration Guide
- Product Documentation
- vSphere Client
- vicfg-syslog
- vilogger

## Notes

**Identify vCenter Server log file names and locations**

- http://www.vmwarewolf.com/which-virtual-center-log-file/

**Generate vCenter Server and ESX/ESXi log bundles**

- vCenter Server http://kb.vmware.com/kb/1011641
- ESX/ESXi http://kb.vmware.com/kb/1010705

**Use vicfg-syslog to configure centralized logging on ESX/ESXi Host**

- vicfg-syslog <conn_options> -i
  Displays the syslog server configuration.
- vicfg-syslog <conn_options> -s mysyslogserver
  Makes mysyslogserver the syslog server for the server specified in <conn_options>.
- vicfg-syslog <conn_options> -p <port>
  Sets the port number used by the syslog server.
- From the GUI http://kb.vmware.com/kb/1016621

**Configure the vMA appliance as a log host**

- Great blog on setting up for AD authentication and connecting
  http://geeksilver.wordpress.com/2010/07/22/how-to-use-vma-4-1-installation-configuration/
- Great blog on setting up your vMA appliance as a log host
  http://www.simonlong.co.uk/blog/2010/05/28/using-vma-as-your-esxi-syslog-server/

**Use vilogger to enable/disable log collection on the vMA appliance**
**Use vilogger to configure log rotation and retention**

- See the vSphere Management Assistant Guide

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

- Very good blog entry on logs here http://www.simonlong.co.uk/blog/2010/06/03/vmware-esxi-4-log-files/

ESX logs

- under /var/log
  - vmkernel - VMKernel Messages
  - vmkwarning - VMKernel Warnings
  - messages - Service Console Log
- Under /var/log/vmware
  - hostd - ESX Service Log
  - aam - HA Log
- Under /var/log/vpx

    - vpxa - vCenter Agent log

ESXi logs

- under /var/log
    - hostd - ESXi Service log
    - messages - Syslog (vmkernel/hostd)
    - vxpa - vCenter Agent Log

## Objective 6.2 – Troubleshoot CPU and Memory Performance

### Knowledge

- Identify resxtop/esxtop metrics related to memory and CPU
- Identify vCenter Server Performance Chart metrics related to memory and CPU

### Skills and Abilities

- Troubleshoot ESX/ESXi Host and Virtual Machine CPU performance issues using appropriate metrics
- Troubleshoot ESX/ESXi Host and Virtual Machine memory performance issues using appropriate metrics
- Use Hot-Add functionality to resolve identified Virtual Machine CPU and memory performance issues

### Tools

- vSphere Resource Management Guide
- vSphere Command-Line Interface Installation and Scripting Guide
- Product Documentation
- vSphere Client
- vSphere CLI
    - resxtop/esxtop

## Notes

**Identify resxtop/esxtop metrics related to memory and CPU**

- Esxtop does not exist in vMA, you must use resxtop
- One limitation of resxtop is the lack of replay mode.
- You must specify the remote server –server=

**Identify vCenter Server Performance Chart metrics related to memory and CPU**
This can be checked at the cluster or server level and you will have more granular options to check at the server level.

**Memory**

You must first have a firm understanding of terminology when it comes to memory in the VMware world. This blog from Scott Sauer is a must read if you are not familiar with the below terms.

- Transparent Page Sharing
- Memory Over commitment
- Memory Overhead
- Memory Balloon Driver

With the ability to overcommit memory you will want to make sure excessive swapping is not occurring at both the host and virtual machine level.

Use memory reservations cautiously. Memory that is reserved cannot be used by another virtual machine that may need it.

Memory ballooning relies on drivers installed in the guest with VMware Tools. No VMware Tools mean potential performance impacts to your server.

**CPU**

There are many counters that can be added and checked including core usage and reservations. Again reservations should be used cautiously.

Watch out for virtual machines that are consistently using a large percentage of CPU resources. A typical server is idle most of the time so check and see if something out of the ordinary is occurring. If in fact the server is using these resources then allocate another vCPU.

High CPU ready times are a dead giveaway for other issues that may be going on.

Virtual machines that have multiple CPU's installed but the incorrect HAL will not help the virtual guest out.

**Troubleshoot ESX/ESXi Host and Virtual Machine CPU performance issues using appropriate metrics**

From the blog of Duncan Epping, these are four commonly needed values to look at when taking into account CPU performance issues. His blog entry is one that is updated over time based on the community so read the comments there and checks if any of these thresholds are changed over time. Ultimately performance is relative to the environment so some of this may not always apply.

| | | | |
|---|---|---|---|
| CPU | %RDY | 10 | Overprovisioning of vCPUs, excessive usage of vSMP or a limit (check |

| | | | |
|---|---|---|---|
| | | | %MLMTD) has been set. See Jason's explanation for vSMP VMs |
| CPU | %CSTP | 3 | Excessive usage of vSMP. Decrease amount of vCPUs for this particular VM. This should lead to increased scheduling opportunities. |
| CPU | %MLMTD | 0 | If larger than 0 the world is being throttled. Possible cause: Limit on CPU. |
| CPU | %SWPWT | 5 | VM waiting on swapped pages to be read from disk. Possible cause: Memory overcommitment. |

If you want to move historical data over to a gui based format you can use esxplot or Windows' Perfmon to interpret the data. To gather this data you would use batch mode as shown below.

*esxtop -b -d delay in seconds -n iterations > capturefile.csv*

**Troubleshoot ESX/ESXi Host and Virtual Machine memory performance issues using appropriate metrics**

Again from the blog of Duncan Epping, five commonly needed values to look at when troubleshooting memory performance. Same applies as above.

| | | | |
|---|---|---|---|
| MEM | MCTLSZ (I) | 1 | If larger than 0 host is forcing VMs to inflate balloon driver to reclaim memory as host is overcommited. |
| MEM | SWCUR (J) | 1 | If larger than 0 host has swapped memory pages in the past. Possible cause: Overcommitment. |
| MEM | SWR/s (J) | 1 | If larger than 0 host is actively reading from swap (vswp). Possible cause: Excessive memory overcommitment. |
| MEM | SWW/s (J) | 1 | If larger than 0 host is actively writing to swap (vswp). Possible cause: Excessive memory overcommitment. |
| MEM | N%L (F) | 80 | If less than 80 VM experiences poor NUMA locality. If a VM has a memory size greater than the amount of memory local to each processor, the ESX scheduler does not attempt to use NUMA optimizations for that VM and "remotely" uses memory via "interconnect". |

**Use Hot-Add functionality to resolve identified Virtual Machine CPU and memory performance issues**

A couple of good blogs by David Davis and Jason Boche outline what and how to use Hot-Add/Hot-Plug. The ability to use this without having to reboot the guest virtual machine is extremely limited. On the Microsoft side Windows 2008 Server Datacenter is necessary to support both features without a reboot while Windows 2008 Server

Enterprise edition does not require a reboot for Hot Adding memory. When it comes to removing either hot added memory or hot plugged CPU's a reboot is required for all Windows guest operation systems.

***Other relevant blogs and websites related to this section***

- http://communities.vmware.com/docs/DOC-10352
- http://communities.vmware.com/docs/DOC-11812
- http://www.boche.net/blog/index.php/2009/01/28/esxtop-drilldown/
- http://www.vreference.com/public/vReference-esxtop1.2.pdf
- http://labs.vmware.com/flings/esxplot
- http://www.simonlong.co.uk/blog/2010/03/24/using-esxtop-with-vmware-esxi/
- http://pubs.vmware.com/vsp40u1_i/resmgmt/c_using_the_esxtop_utility.html#1_7_6_22_1
- http://www.boche.net/blog/index.php/2009/05/10/vSphere-memory-hot-add-cpu-hot-plug/
- http://searchvmware.techtarget.com/tip/0,289483,sid179_gci1367631_mem1,00.html
- http://www.virtualizationadmin.com/articles-tutorials/vmware-esx-articles/general/understanding-and-customizing-vmware-esx-server-performance-charts.html
- http://www.virtualinsanity.com/index.php/2010/02/19/performance-troubleshooting-vmware-vSphere-memory/
- http://www.virtualinsanity.com/index.php/2010/02/15/performance-troubleshooting-vmware-vSphere-cpu/
- http://www.yellow-bricks.com/esxtop/

## z

### Knowledge

- Identify virtual switch entries in a Virtual Machine's configuration file
- Identify virtual switch entries in the ESX/ESXi Host configuration file
- Identify CLI commands and tools used to troubleshoot vSphere networking configurations
- Identify logs used to troubleshoot network issues

### Skills and Abilities

- Utilize net-dvs to troubleshoot vNetwork Distributed Switch configurations
- Utilize vicfg-* commands to troubleshoot ESX/ESXi network configurations
- Configure a network packet analyzer in a vSphere environment
- Troubleshoot Private VLANs
- Troubleshoot Service Console and VMkernel network configuration issues
- Troubleshoot DNS and routing related issues
- Use esxtop/resxtop to identify network performance problems
- Use CDP and/or network hints to identify connectivity issues
- Analyze troubleshooting data to determine if the root cause for a given network problem originates in the physical infrastructure or vSphere environment

### Tools

- ESX Configuration Guide
- ESXi Configuration Guide
- vSphere Command-Line Interface Installation and Scripting Guide
- Product Documentation
- vSphere Client
- vSphere CLI
    - vicfg-*
    - net-dvs
    - resxtop/esxtop

## Notes

**Identify virtual switch entries in a Virtual Machine's configuration file**

- Best thing to do here is open up a vmx file and learn what is configured. Below is a trimmed down vmx from my lab with just the network setting showing.

  *virtualHW.version = "7"*

  *ethernet0.present = "true"*
  *ethernet0.wakeOnPcktRcv = "true"*
  *ethernet0.networkName = "VM Network"*
  *ethernet0.addressType = "vpx"*
  *ethernet0.generatedAddress = "00:50:56:a4:52:92"*
  *ethernet1.present = "true"*
  *ethernet1.virtualDev = "e1000"*
  *ethernet1.networkName = "VM Network"*
  *ethernet1.addressType = "vpx"*
  *ethernet1.generatedAddress = "00:50:56:a4:34:04"*
  *ethernet2.present = "true"*
  *ethernet2.virtualDev = "e1000"*
  *ethernet2.networkName = "VM Network"*
  *ethernet2.addressType = "vpx"*
  *ethernet2.generatedAddress = "00:50:56:a4:74:e9"*
  *ethernet0.startConnected = "true"*
  *ethernet2.startConnected = "false"*
  *ethernet0.pciSlotNumber = "32"*
  *ethernet1.pciSlotNumber = "33"*
  *ethernet2.pciSlotNumber = "35"*
  *ethernet0.virtualDev = "e1000"*

  *ethernet1.startConnected = "false"*

**Identify virtual switch entries in the ESX/ESXi Host configuration file**

- load up /etc/vmware/esx.conf and check it out

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

- There is not a ton of information out there on using the net-dvs command. One blog that contains some relevant information can be found at http://geeksilver.wordpress.com/2010/05/21/vds-vnetwork-distributed-switch-my-understanding-part-2/

- Something I did not know, this command is listed as an unsupported command. It will not run (to my knowledge) from the vMA and I ran it when locally logged into the host. The syntax of the command can be found below

  Warning: This is an unsupported command. Use at your own risk.
  net-dvs -a [ -P maxPorts] switch_name
  net-dvs -d switch_name
  net-dvs [ -A | -D ] -p port switch_name
  net-dvs [ -s name=value | -u name ] -p port switch_name
  net-dvs -l [ switch_name ]
  net-dvs -i (init database)
  net-dvs [-S | -R | -G ]
  net-dvs -T
  net-dvs -v "vlanID[;t|p[0-7][;min-max,min-max...]]

net-dvs -V “primaryVID,secondaryVID,i|c|p;primaryVID,secondaryVID,i|c|p…”
net-dvs -m
“sid;dname;snaplen;[oiveId];encapvlan;wildcardsIn,wildcardsOut;dstPort1,dstPort2,…;srcInPort1,srcInport2,…;srcOutPort1,srcOutPort2,…;:sid2;dname2…”
net-dvs dvswitch -k “respool1_id;respool2_id;…”
net-dvs dvswitch -p dvport -K “respool1_id:shares:limit;respool2_id:shares:limit;…”
net-dvs dvswitch -p dvport -z “respool_id”
net-dvs dvswitch -j [activate|deactivate]
net-dvs -L uplink_name1[,uplink_name2,...] -t team_policy_type -p port switch_name
net-dvs dvswitch -H “red|yellow|green:some message” switch_name
net-dvs -o “depth,param|classname;depth,param|classname;… -p port|globalPropList switch_name
net-dvs –mtu mtu_value [-p dvport] switch_name
net-dvs –x 0|1 -p dvport switch_name
net-dvs –vlan vlanID -p dvport switch_name
net-dvs –reset -p dvport switch_name
net-dvs –cap cap_value -p dvport switch_name
net-dvs –states -p dvport switch_name
net-dvs –miscInfo ;# Dumps cpu/meminfo
net-dvs –vmknicIp <vmknic> ;# Displays IPv4 address on <vmknic>

**Utilize vicfg-* commands to troubleshoot ESX/ESXi network configurations**

- Below are the commands I’d consider relevant for troubleshooting in this section. You can use the vSphere Command Line Reference to gain more information on each of these commands and others.

  - vicfg-authconfig(4.1 only) Manages Active Directory authentication.
  - vicfg-dns.pl Specifies an ESX/ESXi host’s DNS (Domain Name Server) configuration.
  - vicfg-ipsec Supports setup of IPSec.
  - vicfg-nics Manages the ESX/ESXi host’s NICs (uplink adapters).
  - vicfg-ntp Specifies the NTP (Network Time Protocol) server.
  - vicfg-route Lists or changes the ESX/ESXi host’s route entry (IP gateway).
  - vicfg-snmp Manages the Simple Network Management Protocol (SNMP) agent.
  - vicfg-vmknic Adds, deletes, and modifies virtual network adapters (VMkernel NICs).
  - vicfg-vswitch Adds or removes virtual switches or vNetwork Distributed Switches, or modifies switch settings.

**Configure a network packet analyzer in a vSphere environment**

- Too much to put in words on this one. Check out the blog below for assistance. I’d recommend using Wireshark as this is what was used in the troubleshooting course offered by VMware.
- http://itknowledgeexchange.techtarget.com/it-consultant/packet-sniffing-is-your-best-friend/
- http://www.petri.co.il/wireshark-ethereal.htm

**Troubleshoot Private VLANs**

- Great source of PVLAN information at http://professionalvmware.com/2010/04/private-vlan-resources/
- Free video (nearly 40 minutes!) detailing PVLAN’s from Eric Sloof at http://www.ntpro.nl/blog/archives/1465-Online-Training-Configure-Private-VLAN-IDs.html
- Complete definition of what is a PVLAN from VMware KB1010691
- How to configure PVLAN’s from VMware KB1010703

**Troubleshoot Service Console and vmkernel network configuration issues**

- Using VMware’s Resolution Paths a good starting point is the VMware KB1007986 for troubleshooting service console issues.

**Troubleshoot DNS and routing related issues**

- VMware KB4309499 is probably a good start for troubleshooting DNS/routing.
- To change/update DNS use the vicfg-dns command

**Use esxtop/resxtop to identify network performance problems**

- Run esxtop and hit 'n' to enter the networking view
- Again the best resource I've found so far on troubleshooting using esxtop as a whole is Duncan Epping's Blog and I've included the two counters for networking in the table below.
- Two key performance counters you will need to know when troubleshooting network issues are below for both received and transmitted dropped packets. This goes without saying, but you are looking for no dropped packets here.
- The default view for networking will also show current and peak transmission stats to assist in your troubleshooting.

| | | | |
|---|---|---|---|
| NETWORK | %DRPTX | 1 | Dropped packages transmitted, hardware overworked. Possible cause: very high network utilization |
| NETWORK | %DRPRX | 1 | Dropped packages received, hardware overworked. Possible cause: very high network utilization |

**Use CDP and/or network hints to identify connectivity issues**

- Cisco Discovery Protocol CDP Information via the ESX Command Line and Virtual Center (note replace vmware-vim-cmd with vim-cmd)
- The command *vim-cmd hostsvc/net/query_networkhint* will query and show network hints

## Objective 6.4 – Troubleshoot Storage Performance and Connectivity

### Knowledge

- Recall vicfg-* commands related to listing storage configuration
- Recall vSphere 4 storage maximums
- Identify logs used to troubleshoot storage issues
- Describe the VMFS file system

### Skills and Abilities

- Use vicfg-* and esxcli to troubleshoot multipathing and PSA-related issues
- Use vicfg-module to troubleshoot VMkernel storage module configurations
- Use vicfg-* and esxcli to troubleshoot iSCSI related issues
- Troubleshoot NFS mounting and permission issues
- Use esxtop/resxtop and vscsiStats to identify storage performance issues
- Configure and troubleshoot VMFS datastores using vmkfstools
- Troubleshoot snapshot and resignaturing issues
- Analyze log files to identify storage and multipathing problems

### Tools

- ESX Configuration Guide
- ESXi Configuration Guide
- vSphere Command-Line Interface Installation and Scripting Guide
- Product Documentation
- vSphere Client
- vSphere CLI
    - vicfg-*
    - esxcli
    - resxtop/esxtop
    - vscsiStats
    - vmkfstools

## Notes

**Recall vicfg-* commands related to listing storage configuration**

Refer to the vSphere Command-Line Interface Reference for more information on the below commands.

| | |
|---|---|
| vicfg-iscsi | vicfg-iscsi supports configuration and property retrieval for software or hardware iSCSI initiators. |
| vicfg-mpath | The vicfg-mpath command supports listing information about Fibre Channel or iSCSI LUNs and changing a path's state. |
| vicfg-mpath35 | vicfg-mpath35 provides an interface to configure multipath settings for Fibre Channel or iSCSI LUNs on ESX/ESXi version 3.5 hosts. |
| vicfg-nas | The vicfg-nas command manipulates NAS file systems associated with ESX/ESXi hosts. |
| vicfg-rescan | Perform a rescan operation each time you reconfigure your storage setup |
| vicfg-scsidevs | The vicfg-scsidevs command displays information about available LUNs on ESX/ESXi 4.x hosts. |
| vicfg-volume | The vicfg-volume command supports resignaturing a snapshot volume and mounting and unmounting the volume. |
| vicfg-module | The vicfg-module command supports setting and retrieving VMkernel module options. |

**Recall vSphere 4 storage maximums**

- Refer to the storage section of the vSphere Configuration Maximums guide.

**Use vicfg-* and esxcli to troubleshoot multipathing and PSA-related issues**

- Use the vicfg-mpath command to list information about FC or iSCSI luns. Refer to vSphere Command-Line Interface Reference for further detail and description of the command syntax.
- You use the esxcli command to set path policy, such as Fixed, Fixed_AP, MRU, or RR
- You can use the Mask_Path plugin to mask paths. Refer to VMware KB1009449 on masking a LUN from ESX and ESXi 4.0.

**Use vicfg-module to troubleshoot VMkernel storage module configurations**

- The vicfg-module command supports setting and retrieving VMkernel module options. Refer to vSphere Command-Line Interface Reference for further detail and description of the command syntax.

**Use vicfg-* and esxcli to troubleshoot iSCSI related issues**

- Refer to vSphere Command-Line Interface Reference for further detail and description of vicfg-isci syntax.

**Troubleshoot NFS mounting and permission issues**

- Refer to vSphere Command-Line Interface Reference for further detail and description of the vicfg-nas syntax.

**Use esxtop/resxtop and vscsiStats to identify storage performance issues**

- 'd' for disk adapter view
- 'u' for disk device view
- 'v' for disk VM view

From Duncan Epping's ESXTOP section on his blog, the following counters are critical to troubleshooting performance specifically related to storage.

| | | | |
|---|---|---|---|
| DISK | GAVG (H) | 25 | Look at "DAVG" and "KAVG" as the sum of both is GAVG. |
| DISK | DAVG (H) | 25 | Disk latency most likely to be caused by array. |
| DISK | KAVG (H) | 2 | Disk latency caused by the VMkernel, high KAVG usually means queuing. Check "QUED". |
| DISK | QUED (F) | 1 | Queue maxed out. Possibly queue depth set to low. Check with array vendor for optimal queue depth value. |
| DISK | ABRTS/s (K) | 1 | Aborts issued by guest (VM) because storage is not responding. For Windows VMs this happens after 60 seconds by default. Can be caused for instance when paths failed or array is not accepting any IO for whatever reason. |
| DISK | RESETS/s (K) | 1 | The number of commands reset per second. |

**Configure and troubleshoot VMFS datastores using vmkfstools**

- You can do a lot with this command so refer to vSphere Command-Line Interface Reference for further detail and description of the command syntax.

**Troubleshoot snapshot and resignaturing issues**

- The vicfg-volume command supports resignaturing a snapshot volume and mounting and unmounting the volume. Refer to vSphere Command-Line Interface Reference for further detail and description of the command syntax. Check out this blog for more information and a discussion on using the vicfg-volume command.

**Other relevant blogs and websites related to this section**

- VMware Storage Resolution Paths
- http://www.virtualinsanity.com/index.php/2010/03/16/performance-troubleshooting-vmware-vSphere-storage/

Additional troubleshooting links

- http://vSphere-land.com/tag/troubleshooting
- http://www.vcritical.com/2009/10/easy-recovery-from-a-full-vmware-esx-datastore/
- http://www.virtuallyghetto.com/2010/06/esxcli-part1-what-is-esxcli.html
- http://www.yellow-bricks.com/2009/03/18/iscsi-multipathing-with-esxcliexploring-the-next-version-of-esx/
- http://www.punchingclouds.com/?p=965

- http://professionalvmware.com/2010/02/manage-vmfs-file-systems-using-the-cli-vcdx-prep/

## Objective 6.5 – Troubleshoot vCenter Server and ESX/ESXi Host Management

### Knowledge

- Identify CLI commands and tools used to troubleshoot management issues

### Skills and Abilities

- Troubleshoot vCenter Server service and database connection issues
- Troubleshoot the ESX Service Console firewall
- Troubleshoot ESX/ESXi server management and connectivity issues
- Determine the root cause of vSphere management or connectivity issue

### Tools

- ESX Configuration Guide
- ESXi Configuration Guide
- vSphere Command-Line Interface Installation and Scripting Guide
- Product Documentation
- vSphere Client
- vSphere CLI
    - vicfg-*

## Notes

**Troubleshoot vCenter Server service and database connection issues**

- Troubleshooting vCenter server and database issues can be at times frustrating, but it is important to note as this blog entry did that your vCenter issue may not be like all the others you are reading about. Be cautious and check all the little things including the database server backend.
- A good KB on this is for VMware KB1003926.

**Troubleshoot the ESX Service Console firewall**

See the man pages for esxcfg-firewall, or vSphere Command-Line Interface Installation and Scripting Guide

**Troubleshoot ESX/ESXi server management and connectivity issues**

- This VMworld presentation from last year goes through some good vCenter troubleshooting http://www.vmworld.com/docs/DOC-3969

**Determine the root cause of vSphere management or connectivity issue**

- Again you may see many issues that appear the same but are different than others. Refer to the resolution paths for some great information and troubleshooting steps on this.

**Other relevant blogs and websites related to this section**

- VMware System Management Resolution Paths
- http://myvirtualcloud.net/?p=163

Lots of good links for vCenter server here:

- http://vSphere-land.com/tag/vcenter-server
- http://vmware-land.com/esxcfg-help.html
- http://www.yellow-bricks.com/2010/03/10/changing-the-directory-of-your-vSphere-vcenter-log-files/
- http://answers.oreilly.com/topic/1627-how-to-open-and-close-a-firewall-port-via-the-console-on-a-vmware-server/

# VDCA410 Section 7 – Secure a vSphere Environment

## Objective 7.1 – Secure ESX/ESXi Hosts

### Knowledge

- Identify configuration files related to network security
- Identify virtual switch security characteristics

### Skills and Abilities

- Add/Edit Remove users/groups on an ESX Host
- Customize SSH settings for increased security
- Enable/Disable certificate checking
- Generate ESX Host certificates
- Enable ESXi lockdown mode
- Replace default certificate with CA-signed certificate
- Configure SSL timeouts
- Secure ESX Web Proxy
- Enable strong passwords and configure password policies
- Identify methods for hardening virtual machines
- Analyze logs for security-related messages

### Tools

- ESX Configuration Guide
- ESXi Configuration Guide
- vSphere Command-Line Interface Installation and Scripting Guide
- Product Documentation
- vSphere Client
- vSphere CLI
    - vicfg-user
    - vifs

## Notes

**Add/Edit Remove users/groups on an ESX Host**

- You can manage this through the GUI as shown here or using the vicfg-user command.

**Customize SSH settings for increased security**

- Disabled by default for root. You can use SU to elevate to root privileges and should never allow root access via SSH.
- If needed you can enable root access as shown in VMware KB8375637.

**Enable/Disable certificate checking**

- You can follow the guide from VMware KB4646606 for enabling/disabling certificate checking.

**Generate ESX Host certificates**

- Read the below section on replacing the default certificate to get guidance on generating a host certificate.

**Enable ESXi lockdown mode**

- Can be enabled during host addition to vCenter
- Can be set by going to Configuration—>Software—Security Profile
- A good read on the topic of ESXi lockdown can be found here.

**Replace default certificate with CA-signed certificate**

- Check out this article from vm-help.com for an in depth instruction on replacing the default certificate with a CA signed one.

**Configure SSL timeouts**

From the ESX Configuration Guide

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 ESX.
- The Handshake Timeout setting applies to connections that have not completed the SSL handshake process with port 443 of ESX.
- Both connection timeouts are set in milliseconds. Idle connections are disconnected after the timeout period. By default, fully established SSL connections have a timeout of infinity.

1. Log in to the service console and acquire root privileges.
2. Change to the directory /etc/vmware/hostd/.
3. Use a text editor to open the config.xml file.
4. Enter the <readTimeoutMs> value in milliseconds. For example, to set the Read Timeout to 20 seconds, enter the following command.
    a. <readTimeoutMs>20000</readTimeoutMs>

5. Enter the <handshakeTimeoutMs> value in milliseconds. For example, to set the Handshake Timeout to 20 seconds, enter the following command.

    a. <handshakeTimeoutMs>20000</handshakeTimeoutMs>

6. Save your changes and close the file.
7. Enter the following command to restart the vmware-hostd process.
    a. service mgmt-vmware restart

From ESXi config guide

1. Use the vifs command to get a copy of the config.xml file to edit.
    - For Linux systems, use this command.
        - vifs --server <hostname> --username <username> --get /host/config.xml <directory>/config.xml
    - For Windows systems, use this command.
        - vifs --server <hostname> --username <username> --get /host/config.xml <directory>\config.xml
2. Use a text editor to open the config.xml file.
3. Enter the <readTimeoutMs> value in milliseconds. For example, to set the Read Timeout to 20 seconds, enter the following command.

    a. <readTimeoutMs>20000</readTimeoutMs>

4. Enter the <handshakeTimeoutMs> value in milliseconds. For example, to set the Handshake Timeout to 20 seconds, enter the following command.

    b. <handshakeTimeoutMs>20000</handshakeTimeoutMs>

5. Save your changes and close the file.
6. Use the vifs command to put a copy of the config.xml file on the ESXi host.
    - For Linux systems, use this command.
        - vifs --server <hostname> --username <username> --put <directory>/config.xml /host/config.xml
    - For Windows systems, use this command.
        - vifs --server <hostname> --username <username> --put <directory>\config.xml /host/config.xml
7. Use the Restart Management Agents operation through the direct console to have the settings take effect.

**Secure ESX Web Proxy**

- Check the sections for both the ESX(i) config guides for configuring the web proxy.

**Enable strong passwords and configure password policies**

- For ESX you will issue the command like shown below.

  esxcfg-auth –maxpassdays=90 –minpassdays=30 –passwarnage=75

- This blog article is also another good read on the topic of password complexity
  http://www.vm-help.com/esx40i/password_complexity.php

**Identify methods for hardening virtual machines**

The vSphere security hardening guide is a great resource for this section. It is very detailed and has many options. Here are just a few from the document below.

- Prevent Virtual Disk Shrinking-Rapidly inducing this from within the guest could cause a DOS attack.
- Prevent other users from viewing remote console session(multiple at a time)
- *RemoteDisplay.maxConnections=1*
- Disable VM to VM communication through VMCI

**Analyze logs for security-related messages**

Some log file description here.

http://www.vadapt.com/2010/03/vSphere-securitylog-files/

## Objective 7.2 – Configure and Maintain the ESX Firewall

### Knowledge

- Identify vicfg-firewall commands
- Explain the three firewall security levels
- Identify ESX firewall architecture with/without vCenter Server

### Skills and Abilities

- Enable/Disable pre-configured services
- Configure service behavior automation
- Open/Close ports in the firewall
- Create a custom service
- Set firewall security level

### Tools

- ESX Configuration Guide
- ESXi Configuration Guide
- vSphere Command-Line Interface Installation and Scripting Guide
- Product Documentation
- vSphere Client
- vSphere CLI
    - vicfg-firewall

## Notes

**Enable/Disable pre-configured services**

- esxcfg –e *service*
- esxcfg –d *service*

**Configure service behavior automation**

**Open/Close ports in the firewall**

- Allow syslog outgoing traffic:
    - *esxcfg-firewall -o 514,udp,out,syslog*
- Close a port
    - *esxcfg-firewall –c 514,udp,out,syslog*

**Create a custom service**

http://kb.vmware.com/kb/1001081
http://www.yellow-bricks.com/2007/12/31/howto-adding-a-firewall-service-on-esx/

**Set firewall security level**

- View security level
    - *esxcfg-firewall –q incoming*
    - *esxcfg-firewall –q outgoing*
- Set medium security
    - *esxcfg-firewall –-allowOutgoing –-blockIncoming*
- Set low security
    - *esxcfg-firewall -–allowIncoming –allowOutgoing*
- Set high security (default)
    - *esxcfg-firewall -–blockIncoming –blockOutgoing*
- Setting the level requires a restart of vmware-hostd
    - *service mgmt-vmware restart*

## Objective 7.3 – Deploy and Administer vShield Zones

### Knowledge

- Identify vShield Zones components
- Identify the four CLI command modes

### Skills and Abilities

- Configure vShield Zones
- Backup and restore vShield Manager Data
- Backup CLI Configuration
- Create/Delete Layer 2/3/4 firewall rules using VM Wall
- Install/Uninstall a vShield manually and from template
- Configure vShield Manager plug-in capability
- Configure VM Flow charts
- Update vShield Zones
- Add/Edit/Delete User Accounts
- Assign rights to a user
- Add/Delete Application-Port Pair mapping
- Execute/Schedule Execution of virtual machine discovery
- Utilize vShield Zones CLI commands to configure and monitor vShield Zones
- Analyze traffic using VM Flow to determine root cause of network related issues

### Tools

- vShield Zones QuickStart Guide
- vShield Zones Administration Guide
- Introduction to vShield Zones
- Product Documentation
- vShield Manager
- vShield CLI
- vSphere Client

## Notes

**Identify vShield Zones components**
VShield Zones consist of two main components

- vShield manager-management center for all distributed vShield instances. Provides monitoring, configuration, and software updating for your vShields.
- vShield-The active security component of vShield zones. A vShield is installed on each ESX host you want to protect. It will monitor traffic between hosts as well as between virtual machines on the host.

**Identify the four CLI command modes**
From the vShield Zones Administration Guide

- Basic: Basic mode is a read-only mode. To have access to all commands, you must enter Privileged mode.
- Privileged: Privileged mode commands allow support-level options such as debugging and system diagnostics. Privileged mode configurations are not saved upon reboot. You must run the write memory command to save Privileged mode configurations.
- Configuration: Configuration mode commands allow you to change the current configuration of utilities on a vShield Zones virtual machine. You can access Configuration mode from Privileged mode. From Configuration mode, you can enter Interface configuration mode.
- Interface Configuration: Interface Configuration mode commands allow you to change the configuration of virtual machine interfaces. For example, you can change the IP address and IP route for the management port of the vShield Manager.

**Backup and restore vShield Manager Data**
pg 19-21

**Backup CLI Configuration**
pg 43-44

**Create/Delete Layer 2/3/4 firewall rules using VM Wall**
pg 48-50

**Install/Uninstall a vShield manually and from template**
pg 41

**Configure vShield Manager plug-in capability**
page 18

**Configure VM Flow charts**
pg 52-54

**Update vShield Zones**
pg 21-22

**Add/Edit/Delete User Accounts**
pg 23-25

**Assign rights to a user**
pg 24

**Add/Delete Application-Port Pair mapping**
pg 54-56

**Execute/Schedule Execution of virtual machine discovery**
pg 58-59

**Utilize vShield Zones CLI commands to configure and monitor vShield Zones**
pg 65

**Analyze traffic using VM Flow to determine root cause of network related issues**
pg 51

**Other Relevant Reading Related To This Section**

- http://kendrickcoleman.com/index.php?/Tech-Blog/testing-out-vshield-zones.html
- http://searchvmware.techtarget.com/tip/0,289483,sid179_gci1363051_mem1,00.html
- http://kb.vmware.com/kb/1022536
- VCAP-DCA Objective 3.5 – Utilize Advanced vSphere Performance Monitoring Tools
- VCAP-DCA Objective 3.4 – Perform Capacity Planning in a vSphere Environment

# VDCA410 Section 8 – Perform Scripting and Automation

## Objective 8.1 – Execute VMware Cmdlets and Customize Scripts Using PowerCLI

### Knowledge

- Identify vSphere PowerCLI requirements
- Identify Cmdlet concepts
- Identify environment variables usage

### Skills and Abilities

- Use VMRun to execute commands in a guest OS
- Install vSphere PowerCLI
- Install Update Manager PowerShell Library
- Use basic and advanced Cmdlets to manage VMs and ESX Hosts
- Use Web Service Access Cmdlets
- Use Datastore and Inventory Providers
- Given a sample script, modify the script to perform a given action

### Tools

- vSphere PowerCLI Installation Guide
- vSphere PowerCLI Administration Guide
- Product Documentation
- vSphere PowerCLI commands
- vSphere PowerCLI Cmdlets

## Notes

PowerCLI Resources:

- http://www.vfail.net/powercli/
- Trainsignal's PowerShell training (Sean Crookston's affiliate link)

**Use VMRun to execute commands in a guest OS**

- Install VMware VIX (Windows or Linux)
- VMware Tools must be installed in Guest OS
- C:\Program Files (x86)\VMware\VMware VIX\vmrun.exe
- http://www.vmware.com/pdf/vix160_vmrun_command.pdf
- http://www.virtuatopia.com/index.php/Controlling_VMware_Virtual_Machines_from_the_Command_Line_with_vmrun#The_Basics_and_Syntax_of_vmrun
- http://blogs.vmware.com/vix/2008/12/managing-vm-guests-using-vmrun.html
- http://www.virtuallyghetto.com/p/vmware-vix_29.html

**Install vSphere PowerCLI**

- Both the download and documentation can be found at http://communities.vmware.com/community/vmtn/vsphere/automationtools/powercli

**Install Update Manager PowerShell Library**

- http://communities.vmware.com/community/vmtn/vsphere/automationtools/powercli/updatemanager

**Use basic and advanced Cmdlets to manage VMs and ESX Hosts**

- Use the resources above to learn more about PowerShell and PowerCLI

**Use Web Service Access Cmdlets**

- vSphere PowerCLI Administration Guide
- The vSphere PowerCLI 4.1 list of cmdlets includes two Web Service Access cmdlets Get-View & Get-VIObjectByVIView

**Use Datastore and Inventory Providers**

- From pg 24-26: The Datastore Provider (VimDatastore) is designed to provide access to the contents of one or more datastores. The items in a datastore are files that contain configuration, virtual disk, and the other data associated with a virtual machine. All file operations are case-sensitive.

## Objective 8.2 – Administer vCenter Orchestrator

### Knowledge

- Identify vCenter Orchestrator requirements
- Identify default Orchestrator plug-ins

### Skills and Abilities

- Install and Configure vCenter Orchestrator
- Configure vCenter Orchestrator database
- Configure vCenter Orchestrator LDAP connection
- Configure vCenter Orchestrator vCenter server connections
- Run a Workflow
- Administer Actions, Tasks, Workflows and Policies
- Administer Packages
- Identify appropriate Workflow for a given management activity

### Tools

- vCenter Orchestrator Installation and Configuration Guide
- vCenter Orchestrator Administration Guide
- Product Documentation
- vCenter Orchestrator Web Configuration
- vCenter Orchestrator Client
- vSphere Client

## Notes

I recommend you check out the vCenter Orchestrator team's blog at http://www.vcoteam.info/. Other than that, you will want to pop open the installation and configuration guide and play around from there.

**Identify vCenter Orchestrator requirements**

- Hardware
- 4 GB RAM, 2GB Disk, Static IP, 2.0 GHz+ CPU
- Software
- Working LDAP server in your infrastructure
- Web browser (Firefox 3.0, 3.5 IE 7)
- DB recommended on separate machine from server

**Identify default Orchestrator plug-ins**

- Mail Plug-in
- SSH plug-in
- vCenter 4.x plugin
- vCO Library
- WebOperator
- Enumeration
- NET
- XML
- Database
- Non-Default(Microsoft,VI3,Perspectives)

**Install and Configure vCenter Orchestrator**

- You can install Orchestrator with vCenter Server or as a standalone installation.
- Pg 19 of the vCenter Orchestrator Installation and Configuration Guide

**Configure vCenter Orchestrator database**

- pg 46 of the vCenter Orchestrator Installation and Configuration Guide

**Configure vCenter Orchestrator LDAP connection**

- Pg 39-45 of vCenter Orchestrator Installation and Configuration Guide

**Run a Workflow**

- pg 31-32 of the vCenter Orchestrator Administration Guide

**Administer Actions, Tasks, Workflows and Policies**

- Chapter 6, pg 51 of the vCenter Orchestrator Administration Guide

**Administer Packages**

- Pg 55, Chapter 7 of the vCenter Orchestrator Administration Guide

**Identify appropriate Workflow for a given management activity**

- Chapter 3 of the vCenter Orchestrator Administration Guide

## Objective 8.3 – Administer vSphere using the vSphere Management Assistant

### Knowledge

- Identify vMA prerequisites
- Identify vMA specific commands
- Determine when vMA is needed

### Skills and Abilities

- Install and Configure vMA
- Add/Remove target servers
- Perform updates to the vMA
- Use vmkfstools to manage VMFS datastores
- Use vmware-cmd to manage VMs
- Use esxcli to manage Storage Multipathing
- Troubleshoot common vMA errors and conditions

### Tools

- vSphere Management Assistant Guide
- vSphere Command-Line Interface Installation and Scripting Guide
- Product Documentation
- vSphere Management Appliance
- vifp (vifpinit has been replaced by vifptarget)
- vima-update
- vSphere CLI
    - vicfg-*
    - vmkfstools
    - esxcli
    - vmware-cmd
- vSphere Client

## Notes

It is no secret as noted here that the service console is on its way out, so knowledge of command-line based administration and the vMA has become even more important.

The vMA is a CentOS based virtual machine packaged with the vSphere CLI and vSphere SDK for Perl. It allows the ability to run scripts against ESX/ESXi as well as vCenter and now includes Active Directory authentication with the 4.1 release. The vMA can also be used as a syslog server, which is a necessity when using ESXi as the logs are not retained after a reboot.

Before reading through any of the blueprint outline below I would recommend giving the vMA 4.1 guide a quick read. It details all the steps to setup a working vMA appliance. You can download the appliance here**.** You should also check out these two blog posts:

- Blog on setting up for AD authentication
- Blog on setting up your vMA appliance as a log host (not necessarily relevant to this section of the blueprint but important nonetheless)

**Install and Configure vMA**

- Pretty straightforward, import the .OVF and follow the prompts.
- Read the blogs mentioned above for setting up AD authentication, which can also be found in the admin guide. AD authentication is new to 4.1 so it is not currently on the blueprint but I imagine it will be added soon.

**Add/Remove target servers**

- Sudo vifp addserver <FQDN ESX host>
- Sudo vifp remove <FQDN ESX host>
- Sudo vifp reconfigure <FQDN ESX host>

**Perform updates to the vMA**

- sudo vma-update info
- sudo vma-update scan
- sudo vma-update

**Use vmkfstools to manage VMFS datastores**

From the vSphere Command-Line Interface Reference:
*You use the vmkfstools vSphere CLI to create and manipulate virtual disks, file systems, logical volumes, and physical storage devices on an ESX/ESXi host. You can use vmkfstools to create and manage a virtual machine file system (VMFS) on a physical partition of a disk and to manipulate files, such as virtual disks, stored on VMFS-3 and NFS. You can also use vmkfstools to set up and manage raw device mappings (RDMs).*

You will want to use this command extensively and go through all of its options.

**Use vmware-cmd to manage VMs**

- From the vSphere Command-Line Interface Reference:
- *vmware-cmd provides an interface to perform operations on a virtual machine. You can retrieve information such as the power state, register and unregister the virtual machine, set configuration variables, and manage snapshots.*
- Again you will need to go through this command and the options extensively. A good example that every VMware admin has encountered at some point, resolving a stuck virtual machine, can be found here.

**Use esxcli to manage Storage Multipathing**

- Use the vicfg-mpath and vicfg-mpath35 (for esx 3.5 hosts) to configure and manage storage multipathing.
- This blog entry shows off a little PowerShell for setting a preferred path. Most of the reference for storage multipathing will be from the below. Additionally the vSphere Troubleshooting course is a good target for this type of exercise.

From the vSphere Command-Line Interface Reference:
*The vicfg-mpath command supports listing information about Fibre Channel or iSCSI LUNs and changing a path's state.*

**Troubleshoot common vMA errors and conditions**

- Refer to the Troubleshooting vMA section of the vMA Administration Guide
- By far the best resource for vMA information can be found at the blog virtuallyGhetto

***Other relevant blogs and websites related to this section***

**vMA Setup**

- http://communities.vmware.com/community/vmtn/vSphere/automationtools/vima
- http://www.vmware.com/support/developer/vima/vma41/doc/vma_41_guide.pdf
- http://geeksilver.wordpress.com/2010/07/22/how-to-use-vma-4-1-installation-configuration/
- http://www.simonlong.co.uk/blog/2010/05/28/using-vma-as-your-esxi-syslog-server/
- http://www.virtuallyghetto.com/2010/05/getting-started-with-vma.html

**vmkfstools**

- http://pubs.vmware.com/vi35/wwhelp/wwhimpl/common/html/wwhelp.htm?context=server_config&file=sc_appb.21.1.html
- http://www.vmware.com/support/developer/vcli/vcli41/doc/reference/vmkfstools.html

**vmware-cmd**

- http://www.vmware.com/support/developer/vcli/vcli41/doc/reference/vmware-cmd.html
- http://www.vmware.com/support/esx2/doc/vmware-cmd.html
- http://www.yellow-bricks.com/2009/04/15/the-basics-how-to-kill-a-vm-thats-stuck-during-shutdown/

**vicfg-mpath**

- http://www.vmware.com/support/developer/vcli/vcli41/doc/reference/vicfg-mpath.html
- http://virtuallynil.com/2010/02/12/setting-preferred-paths-in-esxi/
- http://photomission.co.uk/2010/10/04/vcap-dca-8-3/

# VDCA410 Section 9 – Perform Advanced vSphere Installations and Configurations

## Objective 9.1 – Install ESX Server with custom settings

### Knowledge

- Identify Service Console memory defaults and maximums
- Identify default and optional ESX partitions

### Skills and Abilities

- Configure optional ESX partitions during installation
- Install/uninstall custom drivers
- Configure advanced bootloader options
- Configure kernel options
- Given a scenario, determine when to customize a configuration

### Tools

- ESX and vCenter Server Installation Guide
- Product Documentation
- vSphere CLI
  - vicfg-advcfg
  - vicfg-module
- vSphere Client

## Notes

**Identify Service Console memory defaults and maximums**

With vSphere 4.x the default is not exactly cut and dry. The default is 300 MB, however with amounts of RAM 16GB or larger the default will actually be more. The maximum is 800 MB regardless. As for answering this question in a lab I'm not sure it will really matter. Just be aware of these things and check out this excellent blog article by Duncan Epping on the topic.

**Identify default and optional ESX partitions**

A default ESX installation will leave you with the below configuration. Note this was with a 40 GB disk so you will have more space on your VMFS volume with a bigger drive.

```
Service Console Partitions:   vmkcore      110 MB
                              vmfs3      39.75 GB
                              swap         600 MB
                              ext3        5.00 GB  /
                              ext3        1.10 GB  /boot
                              ext3        2.00 GB  /var/log
```

Additionally you may create other partitions.

**/opt** Some of the logging occurs here for HA and hardware agents so it may be best to move this partition out to it's own to prevent root from filling up. Read Jason Boche's blog to read more about this.

**/tmp** Another good one to move outside of root to prevent it from taking up space?

**/home** not necessarily needed anymore but again if it's used you risk filling up root by not having a separate mount point.

**/var** You may want to create the mount point here to dedicate more space to /var/log and /var/core and to prevent filling up your root directory.

**Install/uninstall custom drivers**

- Can be done during ESX installation or post installation using vCenter Update manager or the vSphere CLI.
- Cannot be done using PXE

**Configure advanced bootloader options**

- If you deselect the Configure boot loader automatically check box, the Bootloader Options page will appear.
- Enter bootloader kernel arguments. These arguments will be written to the grub.conf file and they will be passed to the ESX kernel every time ESX boots.
- An optional bootloader password of up to 30 characters can be entered.
- By default the GRUB bootloader is installed in the MBR. For legacy hardware that stores BIOS info in the MBR, click Install GRUB on the first partition of the disk instead.

**Configure kernel options**

- In the advanced setup you can specify kernel arguments to be written to the grub.conf file and passed to the kernel every time ESX boots.
- http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esx_vc_installation_guide.pdf

**Given a scenario, determine when to customize a configuration**

**vicfg-advcfg**

- The vicfg-advcfg command offers a number of low-level advanced options.
- Most options are not intended for customer use. You might use this command when VMware Technical Support or a VMware Knowledge Base article instructs you to do so.
- You can use the vicfg-advcfg -s option to enable and disable CIM providers.

Set a VMkernel option:

```
vicfg-advcfg <conn_options> --set-kernel 1 assumeCommonBusClock
```

Set the value of a specific configuration item given its identifying path and the value to set:

```
vicfg-advcfg <conn_options> -s 1 VMkernel.Boot.xapicForce
```

**vicfg-module**

- The vicfg-module command supports setting and retrieving VMkernel module options. This command is a vSphere CLI implementation of the esxcfg-module service console command, but it supports only some of the options esxcfg-module supports. The command is commonly used when VMware Technical Support, a Knowledge Base article, or VMware documentation instruct you to do so.

Configure a supported NIC to use NetQueue:

```
vicfg-module <conn_options> -s "intr_type=2 rx_ring_num=8" s2io
```

Verify that NetQueue has been configured:

```
vicfg-module <conn_options> -g s2io
```

List the set of modules on the host:

```
vicfg-module <conn_options> -l
```

***Other relevant blogs and websites related to this section***

- http://vmetc.com/2009/07/22/best-practices-for-vSphere-esx-4-service-console-partitions/
- http://www.yellow-bricks.com/2009/05/27/partitioning-your-esx-host-part-ii/

## Objective 9.2 – Plan and Execute Scripted Installations

### Knowledge

- Identify default installation scripts
- Identify boot options for scripted installation

### Skills and Abilities

- Perform a scripted ESX Host installation
- Perform a scripted ESXi Host installation
- Configure media repository
- Edit installation script parameters
- Configure pre/post script tasks
- Evaluate use cases for scripted installation

### Tools

- ESX and vCenter Server Installation Guide
- Product Documentation
- ks-first-safe.cfg
- ks-first.cfg

## Notes

Something on topic and cool is the ultimate deployment appliance mentioned by Jeremy Waldrop and Mike Laverick. This appliance lets you install all types of base operating systems, now including VMware.

**Identify default installation scripts**

- When you install using a default installation script, the default root password is mypassword.
- The installation media contains the following default installation scripts:
    - ESXi: ks.cfg Installs ESXi on the first detected disk
    - ESX: ks-first-safe.cfg -Installs ESX on the first detected disk and preserves the VMFS datastores on the disk. ks-first.cfg- Installs ESX on the first detected disk.
    - Additionally, after your first interactive installation of ESX, the installer creates a /root/ks.cfg script in the ESX filesystem. This script reflects the choices you made in the interactive installation.

**Identify boot options for scripted installation**

- See the ESX Installation Guide

**Perform a scripted ESX Host installation**

- Use the ESX Installation Guide to learn more about the syntax involved in creating scripted installation scripts.
- The installation script can reside in one of the following locations:
    - Default installation script
    - FTP
    - HTTP/HTTPS
    - NFS
    - USB flash drive
    - Local disk

**Perform a scripted ESXi Host installation**

Check out VMware's guide for Deploying ESXi 4.1 using the Scripted Install feature.

Some important things to note from it:

- You can boot the scripted installation with a CD-ROM drive or over the network using PXE booting
- It supports scripted installations of ESXi to local and remote disks
- All configuration directives initiated by the installation script are logged in the /var/log/weasel.log file of the ESXi host
- Scripted Install is available only with the Installer version of ESXi and is not available in the Embedded version of ESXi
- You cannot use Scripted Install to install ESXi Installable to a USB device

Additionally you will want to check out the ESXi installable and vCenter Server Setup Guide.

Scripted installations include the following steps:

- Create a script using the supported commands.
- Edit the installation script as needed to change settings that are unique for each host.
- Run the scripted installation.

The installation script can reside in one of the following locations:

- Default installation script
- FTP
- HTTP/HTTPS
- NFS

When creating the script there are two main approaches you can take

- Create multiple scripts, each containing unique network identification information. The unique network information includes the static IP address and host name of each ESXi host.
- Create one script (or use a default script) that uses DHCP to set up multiple ESXi hosts. After you complete a scripted installation, you can configure each ESXi host separately to assign a unique host name and IP address. VMware recommends that you use static IP addresses.

**Configure media repository**

This blog from Virtual Kenneth goes through a lot of the above but additionally will give a good guide on setting up an ESXi source repository on a Windows box.

Another good set of blogs on the topic are from Simon Long. The link is to the first of a three part series on rapid deployment of ESXi.

**Configure pre/post script tasks**

For the above topics read the guides to learn the proper configuration options if you do not already know them. Additionally you can use the output of a ESX installation to give you a good example of what a scripted installation file will look like based on the configuration options you are choosing. This file will be found at /root/ks.cfg

**Evaluate use cases for scripted installation**

Automating deployment which will save time and eliminate human error on the setup part.

**Other relevant blogs and websites related to this section**

- http://kb.vmware.com/kb/1022308
- http://vinternals.com/2009/07/unattended-esxi-installation/

## Objective 9.3 – Configure vCenter Server Linked Mode

### Knowledge

- Identify Linked Mode Prerequisites
- Identify differences between Linked and non-linked vCenter Server Configurations
- Identify when a role requires reconciliation

### Skills and Abilities

- Reconcile Roles in a Linked Mode Configuration
- Create and Join a Linked Mode Group
- Determine use cases for vCenter Server Linked Mode
- Troubleshoot Linked Mode Configurations

### Tools

- ESX and vCenter Server Installation Guide
- vSphere Datacenter Administration Guide
- Product Documentation
- vSphere Client

## Notes

- Available with Standard licensing and above.
- Uses ADAM DB
- Supported amount of hosts/VMs is 3000/10,000

**Identify Linked Mode Prerequisites**
Refer to VMware's online documentation for more information about Linked Mode.

Linked Mode vCenter Servers must meet all the requirements of a standard build plus:

- Operational DNS for Linked Mode Replication
- Two way trust relationship if in different domain or the same domain for vCenter servers that are linked
- An account with admin privileges on both the existing and to be linked vCenter server system.
- Network time must be synchronized amongst servers

**Identify differences between Linked and non-linked vCenter Server Configurations**

**Identify when a role requires reconciliation**
Reconciliation will happen automatically when configuring linked mode if any differences exist that you have not yet resolved. If conflicts occur the role on the joining system is renamed.

**Reconcile Roles in a Linked Mode Configuration**
Refer to VMware's online documentation for reconciling roles in a linked mode config.

**Create and Join a Linked Mode Group**
Refer to VMware's online documentation for direction on creating and joining a linked mode group.
Note that the first vCenter server will be configured as a standalone while the others can join a Linked Mode group.

**Determine use cases for vCenter Server Linked Mode**
Linked mode is geared towards larger environments where administration may become more difficult. Linked mode helps with this by providing a scalable architecture that allows visibility across multiple instances of vCenter server. Roles, permissions, and license are replicated.

**Troubleshoot Linked Mode Configurations**
Refer to VMware's online documentation for direction on how to troubleshoot Linked Mode config. A lot of the setup is going to rely on your DNS and AD infrastructure so keeping in mind that those two pieces are crucial to this running is your first step in troubleshooting issues.