VCP6 Study Guide

SECTION I – Configure & Administer vSphere Security

1.1 – Configure & Administer Role-Based Access Control

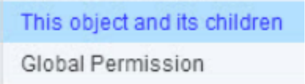
a. Compare & contrast propagated & explicit permission assignments

1) Privileges – rights to perform actions on an object
2) Role – set of privileges granting access to perform action on an object
3) Permissions – role(s) assigned to a user or group to perform actions on objects
4) Propagated permissions – selecting the option for permissions to be assigned to a vSphere object and objects below it in the vSphere hierarchy
5) Explicit permissions – permission added to an object without propagation
6) Notes about permissions and propagation in general:

- a) Propagation must be set manually; it's not 'universally' (automatically) applied
- b) Child permissions override any permissions inherited by the parent
- c) If vSphere objects inherit permissions from multiple parents, all permissions from both parents are applied
- d) If a user is assigned to a group, and both the user & the group has permissions assigned to a vSphere object, user permissions override group permissions

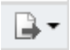
b. View/Sort/Export User & Group Lists

1) View: select a vSphere object > Manage tab > Permissions, then view '**Defined In**' column



This object and its children

Global Permission

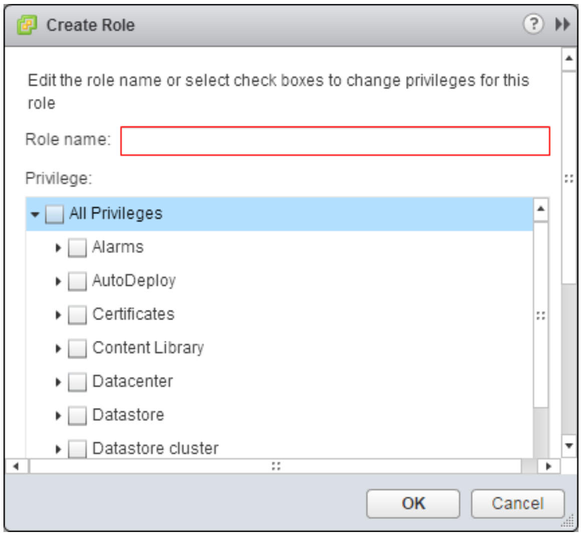
2) Export list – from the lower right of the Permissions tab, click: 

3) Sorting is as simple as clicking on a column from the Permissions tab

c. Add/Modify/Remove permissions for users & groups on vCenter Server inventory objects

1) From Navigation pane on left > Administration > Access Control > Roles

2) Click green "**+**" to **add** a Role by entering a Role Name & assigning desired Privileges for the Role wanting to grant to a user/group

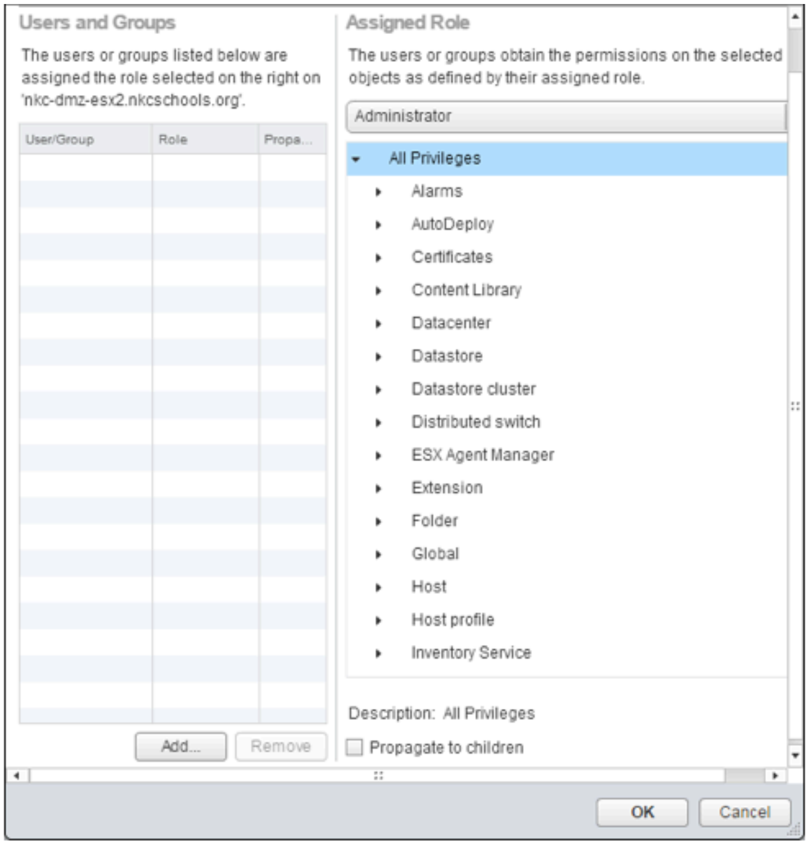


Edit the role name or select check boxes to change privileges for this role

Role name:

Figure 1, Create Role

3) To assign the Role to a user/group, click on a vSphere object on the left > Manage tab on the right > Permissions tab
4) Click the green "+" to add the created Role in Step 2 to a user/group; for ease of management, and if deemed appropriate, check the 'Propagate to children' option for the added permission to be applied not only on the current object, but sub-objects (child) in the vSphere hierarchy



The users or groups listed below are assigned the role selected on the right on 'nkc-dmz-esx2.nkcschools.org'.

The users or groups obtain the permissions on the selected objects as defined by their assigned role.

Administrator

Description: All Privileges

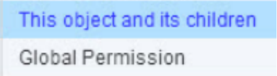
□ Propagate to children

Figure 2, Add Permission

5) To edit or remove a permission, click the pencil (Edit) or red '**x**' icon respectively in the permissions tab for a given vSphere object ✎ ✖ **NOTE:** If the "**x**" is greyed out after clicking on a permission, the permission is set at a higher level & thus needs removed at that level

d. Determine how permissions are applied & inherited in vCenter Server

1) Select a vSphere object > Manage tab > Permissions, then view the 'Defined In' column



This object and its children
Global Permission

The permission will show where it's defined ("This object", "This object and children", "Global"); also, see further 'notes' in a. above regarding inheritance, propagation, and overrides

2) If an object inherits permissions from more than 1 place (i.e. 2 parent objects), privileges from both are propagated to that (child) object

3) User permissions override Group permissions; child permissions override parent permissions

e. Create/Clone/Edit vCenter Server Roles

1) From Roles, select a Role, then click the Clone or Edit buttons ⧉ ✎ (Create – see 'c.' above)

2) Can't Edit System Roles, only Clone

f. Configure VMware Directory Service

1) Web Client (administrator@vsphere.local) > Administration > Single Sign-On > Configuration

2) Select Identity Sources tab, then click the green "**+**" to add the AD Identity Source

a) AD-Integrated/AD-LDAP format: Domain = FQDN of domain; Alias = NetBIOS name; SPN = STS/domain.com; UPN = joe@domain.com or domain.com\joe; DN = cn=x,ou=x,dc=domain,dc=com

3) If adding AD-Integrated Authenticaion, first join vCenter to Active Directory: Administration > Deployment > System Configuration > click Nodes, then select the vCenter node > Manage tab > Settings tab, select Active Directory under Advanced & click the Join button

a) For simpler process, use machine acct or add a machine to AD and use that 'system'

g. Apply a Role to a User/Group & to an object or group of objects

1) See 'b.' above

h. Change permission validation settings

1) This is for how often vCenter queries AD for user permissions

2) To change: select vCenter > Manage tab > Settings tab > General > Edit button, then select User Directory & Enable (checkbox) Validation; set Validation Period (default = 1440 mins, or 24hrs)

i. Determine the appropriate set of privileges for common tasks in vCenter Server

1) Privileges are determined by deciding what object(s) are needing actions to be performed on, then create a Role & selecting the appropriate Privileges for the action to be performed

2) See pp 128-129, Security Guide for common task and applicable role, but some takeways:

TASK	PRIVILEGES	MINIMUM DEFAULT USER
Create VM	Destination Folder or Datacenter: (several priv's) Destination Host/Cluster/RP: **resource.AssignVMtoResourcePool** Destination DS: **datastore.AllocateSpace** Assigning Network to VM: **network.AssignNetwork**	Folder/DC: Administrator On Host, etc: RP Admin Dest DS: Datastore Consumer To Assign Net: Network Admin
Deploy VM from Template	Several priv's for Destination Folder or DC, on Template, on Destinatoin Host/Cluster/RP, Destination DS, and Network	Administrator (except Datastore and Network)
Take Snapshot	Source VM/Folder: **virtualMachine.SnapshotMgmt.CreateSnap** Destination DS or DS Folder: **datastore.AllocateSpace**	On VM: VM Power User Destination DS: Datastore Consumer
Move VM into Resource Pool	Source VM/Folder: **resource.AssignVMtoResourcePool** **VirtualMachine.Inventory.move** Destination RP: **resource.AssignVMtoResourcePool**	On VM: Administrator Dest RP: Administrator
Install Guest OS	Source VM: (several priv's) Datastore with ISO: **datastore.BrowseDatastore**	On VM: VM Power User On Datastore with ISO: VM Power User
Migrate VM with VMotion	Source VM or Folder: **resource.migratePoweredOffVM** Destination Host/Cluster/RP (if different than Source): **resource.AssignVMtoResourcePool**	On VM: Resource Pool Admin Destination: Resource Pool Admin
Cold Migrate VM	Source VM or Folder: **resource.migratePoweredOffVM** Destination Host/Cluster/RP (if different than Source): **resource.AssignVMtoResourcePool** Destination Datastore (if different than Source): **datastore.AllocateSpace**	On VM: Resource Pool Admin Destination: Resource Pool Admin Destination DS: Datastore Consumer
Migrate VM with sVMotion	Source VM or Folder: **resource.migratePoweredOnVM** Destination Datastore: **datastore.AllocateSpace**	On VM: Resource Pool Admin Destination: Datastore Consumer

Move Host into Cluster	Source Host: **host.inventory.addHostToCluster** Destination Host: **host.inventory.addHostToCluster**	On Host: Administrator Destination Cluster: Administrator

3) Summary of above table - minimum permissions for a task

a) Create VM/VMotion/Cold Migrate/Migrate with sVMotion – Resource Pool Admin

b) Deploy VM from Template/Move VM in Resource Pool /Move Host in Cluster – Administrator

c) Take Snapshot & Install Guest OS – VM Power User

j. Compare & contrast default System/Sample Roles

1) System Roles are permanent Privileges & are *not editable* – **Administrator**, **No Access**, **Read Only**

2) Sample Roles are provided by VMware for frequently performed tasks; *can be edited*, cloned, or removed:

a) Virtual Machine Power User

b) Virtual Machine User

c) Resource Pool Administrator

d) VMware Consolidated Backup User

e) Datastore Consumer

f) Network Administrator

g) Content Library Administrator

k. Determine the correct permissions needed to integrate vCenter Server with other VMware products

1) Global permissions are applied to a global root object that spans multiple VMware solutions; as such, use Global permissions to give users/groups access for all objects in all solution hierarchies (pg. 122); global root -> Content Library; vCenter; Tags

2) Be aware of high-level privileges needed for VMware services such as VDP, SRM, vRep, VSAN, etc.

1.2 – Secure ESXi, vCenter Server, & Virtual Machines

a. Harden VM Access

1) Control VMware Tools Installation – limit **VM.Interaction.VMware Tools Install** privilege

2) Control VM data access – disable copy/paste capability via console

a) From vCenter Inventory > VM > Manage tab > Settings tab > Edit button > VM Options tab > Advanced > Edit Configuration button; 'Add Row' to add the desired security setting & value (parameter: **`isolation.tools.copy/paste.disable`** ; value: **true**)

b) Prevent VM sending config info to Hosts: **`isolation.tools.setInfo.disable = true`**

3) Configure VM security policies

a) Common security configuration parameters (Review online VM Security doc for other items: http://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.security.doc/GUID-6BFA8CA7-610F-4E6B-9FC6-D656917B7E7A.html):

1. Disable copy/paste in Console: see above

2. Set VMX file size (default = 1MB): **`tools.setInfo.sizeLimit=1234567`**

3. Set VM log amount #: **`vmx.log.KeepOld = 10`**

4. Disable VM -> configuration: **`isolation.tools.setinfo.disable = true`**

b. Harden VMs against Denial of Service Attacks

1) Control VM-VM communication – VMCI is no longer a supported VM config; set Shares

2) Control VM-device communication – limit **VM.Interaction** & limit **VM.Configuration** privileges

3) Configure network security policies – VLANs, Promiscuous Mode, Forged Transmit, & MAC Address options on vSwitch or PG

c. Harden ESXi Hosts

1) Enable/Configure/Disable services in ESXi firewall – Select a Host > Manage tab > Settings tab > System > Security Profile > Edit button under 'Firewall'; disable ESXi & Shell (are by default)

2) Change default account access – limit root access & use 'least privilege' concept

a) Modify password setting character length, or use passphrases

b) Format to change Security.PasswordQualityControl advanced parameter on Hosts: retry=# min=N0,N1,N2,N3,N4 passphrase=# (this is optional, if N2 is used)

c) Review Security Guide, pg. 135 and the pam_passwdqc "man page" (http://linux.die.net/man/8/pam_passwdqc)for further explanation of format meaning

3) Add an ESXi Host to a directory service – Select a Host > Manage tab > Settings tab > System > Authentication Services > 'Join Domain' button (verify time is sync'd with Dir Svcs)

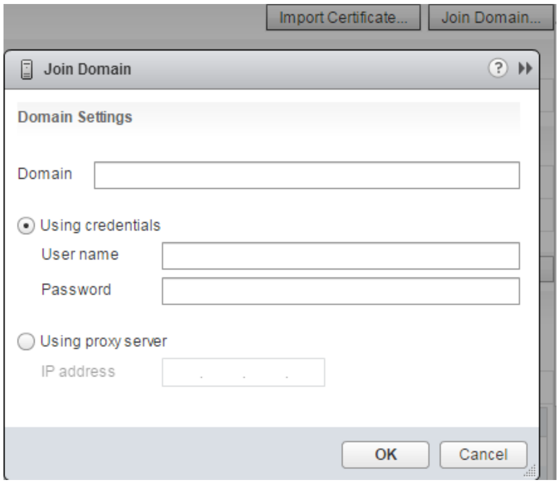


Figure 3, Host Add Directory Service

4) Enable Lockdown Mode – Select a Host > Manage tab > Settings tab > System > Security Profile > Edit button under 'Lockdown Mode'

a) Choose Normal or Strict; **NOTE:** in 'Strict', DCUI service is stopped

b) Adding users to DCUI.Access Advanced Host option or Exception Users list enables ability to disable lockdown in Normal Mode only in case of catastrophe

c) In Strict Mode, if the Host loses vCenter connection, the onl way to connect is if SSH is enabled & Exception Users are defined

d) When Strict or Normal is enabled, those in Exception Users list & who are Admins, or those in the DCUI.Access advanced option list, can use the DCUI; all other users get terminated

5) Control access to hosts (DCUI/Shell/SSH/MOB) – see Step 4 ir: access; disable services in Host > Manage tab, Settings tab > System > Services, then click Edit button & "Start"/"Stop" the service

a) MOB access – Select a Host > Manage tab > Settings tab > System > Advanced, search for `Config.HostAgent.plugins.solo.enableMob` and verify it's set to **false**

d. Harden vCenter Server

1) Control datastore browser access – limit **Datastore.Browse Datastore** privilege
2) Create/Manage vCenter Server Security Certificates – 4 options:
   a) VMCA (Root) – **default**, if nothing further is done after installing vCenter/ESXi
   b) VMCA Intermediate – make VMCA (PSC) an Intermediate CA to org Enterprise CA & replace all PSC certs; for cert replacment order, review Security Guide, pg. 80
   c) Custom – do not use VMCA, but rather a well-trusted/known CA (Entrust, Verisign, etc)
   d) Hybrid – a combination of using VMCA & Custom certs
   e) **ESXi** – Hosts use VMCA by default; this can be changed to use the Custom method, or even legacy 'thumbprint', customizable in vCenter Advanced "certmgmt" parameters in Web Client
3) Control MOB access – this was discussed in Host Security above (5a); MOB is only for Hosts
4) Change default account access – default Role = No Access; grant different Roles to users/groups
5) Restrict administrative privileges – don't add users/groups to Administrator Role (least priv's)

e. Understand implications of securing a vSphere environment

1) When modifying any items discussed to this point (i.e. Lockdown, permissions, enabling & disabling advanced options), understand how those changes affect access vs enhancing security

1.3 – Enable SSO & Active Directory Integration

a. Describe SSO architecture & components

1) Security Token Service (STS) – issues SAML tokens to represent identity of human/solution user
2) Administration server – allows configuration of SSO server
3) VMware Directory Service – associated with domain specified during SSO install & included with each PSC deployment; also stores certificate info
4) Identity Management Service – handles identity sources & STS authentication requests

b. Differentiate available authentication methods with VMware vCenter

1) Human user
   a) User logs in with Web Client
   b) Web Client passes login info to SSO & SSO checks if Web Client has a valid token & if user is in a valid Identity Source
   c) If all passes, SSO sends back a token to Web Client that represents the user
   d) The Web Client then passes the token on to vCenter
   e) vCenter checks with SSO for token validity
   f) SSO returns token to vCenter & authentication occurs
2) Solution user – set of services used in vCenter Server
   a) Machine – used by Component Mgr, License Server, & Logging Service
   b) vpxd – used by vCenter service daemon
   c) vpxd-extensions – Auto Deploy, Inventory Service
   d) vsphere-webclient
   e) Authentication -> solution user attempts to connect to vCenter; solution user redirected to SSO; if solution user has valid cert, SSO assigns a token back to solution user; solution user then connects to vCenter & performs tasks

c. Perform a Multi-Site SSO (PSC) installation

1) See: http://kb.vmware.com/kb/2034074 & http://kb.vmware.com/kb/2108548 for details

2) Overall, there isn’t anything special about this; from a high-level standpoint, the thing to keep in mind is order: install Platform Services Controller (PSC) 1st then vCenter’s attached to the PSC (can be either Windows or VCSA); repeat for additional PSCs/vCenters

d. Configure/Manage Active Directory Authentication
1) Use Web Client or vmdir CLI to manage

e. Configure/Manage Platform Services Controller (PSC)
1) PSC consists of: SSO, License Server, and VMCA; it’s all installed together..nothing to manage
2) Cannot change deployment type after install (i.e. Embedded PSC to External PSC or vice versa)
3) About the only thing to be done with PSC is to use VMCA via CLI or replace STS cert (see Security Guide, pg. 36)

f. Configure/Manage VMware Certificate Authority (VMCA)
1) Installed when PSC is installed; nothing needs configured

g. Enable/Disable Single Sign-On (SSO) users
1) Log on with ‘vsphere.local’ Admin accout, then Administration > Single Sign-On > Users and Groups; select the user and click the checkmark (Enable) or ⊘ (Disable)

h. Upgrade Single/Multi-Site SSO install
1) Upgrade from pre-v6 requires installing to the new Platform Services Controller (PSC), which now incorporates SSO, License Server, & the new VMware Cert Authority (VMCA)
2) Upgrade process will be dependent on several factors, including having embedded vs external install & whether on Windows vs appliance
3) If embedded, just perform the install on the single machine, which will upgrade everything
4) If external, upgrade SSO to a external PSC machine (VM or phys); after upgrading SSO to PSC, upgrade all vCenter instances previously connected to the SSO machine; see VMware KB: http://kb.vmware.com/kb/2108548

i. Configure SSO policies
1) Administration > Single Sign-On > Configuration > Policies tab (Password, Lockout, Token Policy)

j. Add/Edit/Remove SSO Identity Resources
1) Administration > Single Sign-On > Configuration > Identity Resources tab

k. Add an ESXi Host to an AD domain
1) Host > Manage tab > Settings tab > System > Authentication Services > Join Domain button

SECTION II – Configure and Administer vSphere Networking

2.1 – Configure Advanced Policies/Features and Verify Network Virtualization Implementation

a. Create/Delete a vDS
1) Create: Networking > rt-click DC object > Distributed Switch > **New Distributed Switch…**

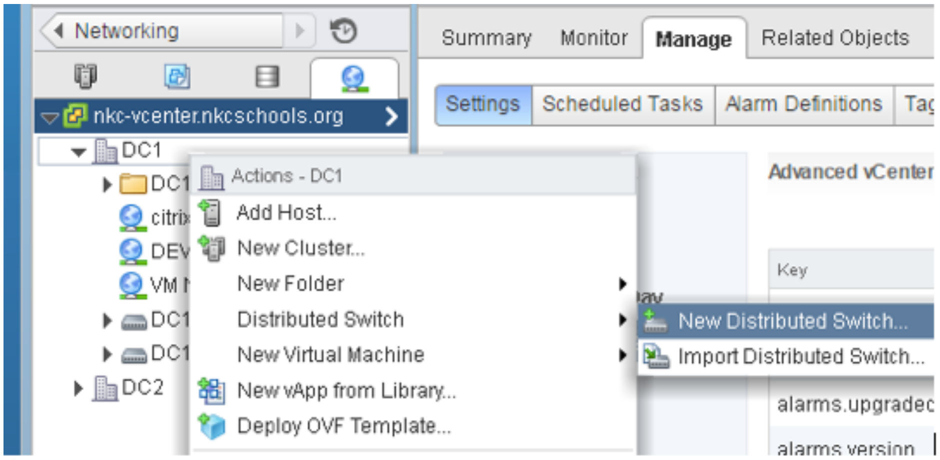
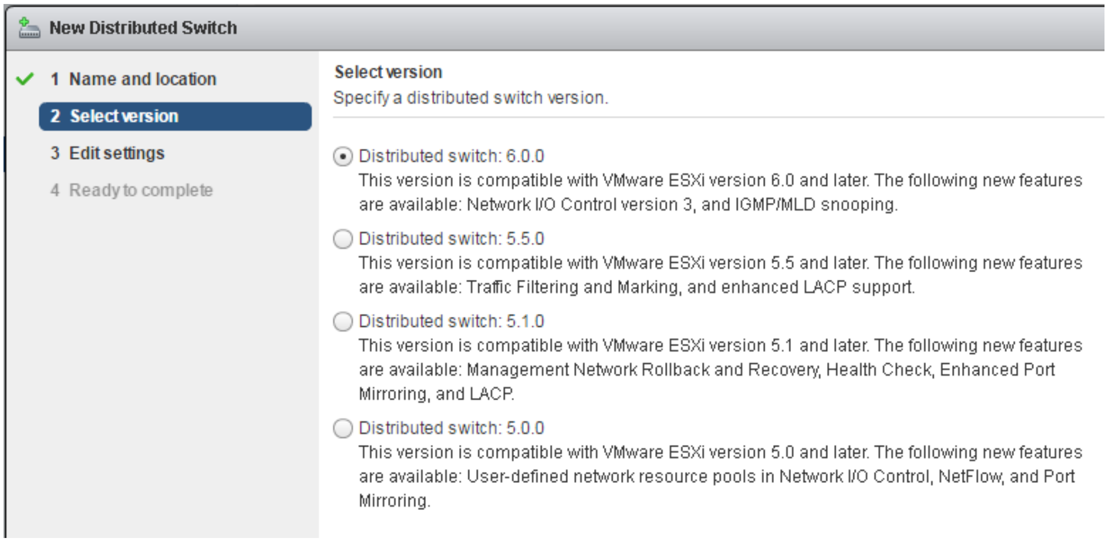


Figure 4, Create New vDS

2) Choose vDS Name (Next), then Version



New Distributed Switch

✓ 1 Name and location
2 Select version
3 Edit settings
4 Ready to complete

Select version
Specify a distributed switch version.

● Distributed switch: 6.0.0
This version is compatible with VMware ESXi version 6.0 and later. The following new features are available: Network I/O Control version 3, and IGMP/MLD snooping.

○ Distributed switch: 5.5.0
This version is compatible with VMware ESXi version 5.5 and later. The following new features are available: Traffic Filtering and Marking, and enhanced LACP support.

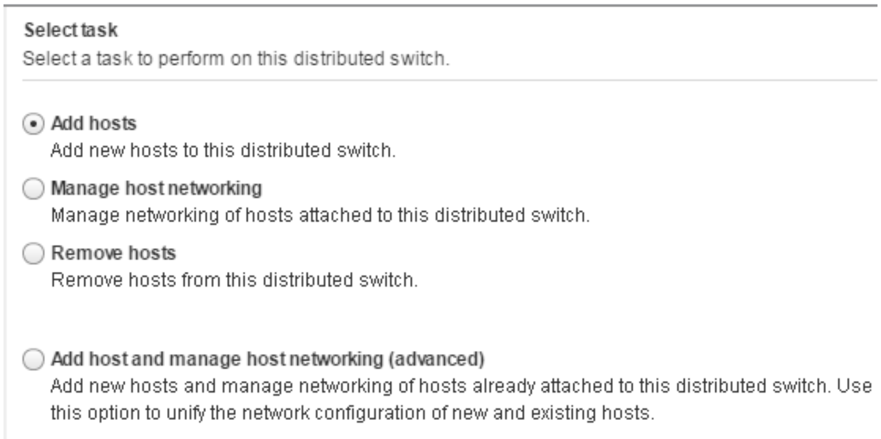
○ Distributed switch: 5.1.0
This version is compatible with VMware ESXi version 5.1 and later. The following new features are available: Management Network Rollback and Recovery, Health Check, Enhanced Port Mirroring, and LACP.

○ Distributed switch: 5.0.0
This version is compatible with VMware ESXi version 5.0 and later. The following new features are available: User-defined network resource pools in Network I/O Control, NetFlow, and Port Mirroring.

Figure 5, Select vDS Version

3) Lastly, modify Uplinks, eanble Network I/O, & choose whether to create a Port Group
4) After creation, add Hosts & desired Host adapters
5) Delete: before deleting a vDS, remove all Hosts & associated adapters (Uplinks); rt-click Distributed Switch > **Delete**

c. Add/Remove ESXi Hosts to/from a vDS
1) Add: rt-click vDS > **Add and Manage Hosts…** , select “Add hosts” & follow wizard
2) Remove: rt-click vDS > **Add and Manage Hosts…** select “Remove hosts” & follow wizard



Select task
Select a task to perform on this distributed switch.

● Add hosts
Add new hosts to this distributed switch.

○ Manage host networking
Manage networking of hosts attached to this distributed switch.

○ Remove hosts
Remove hosts from this distributed switch.

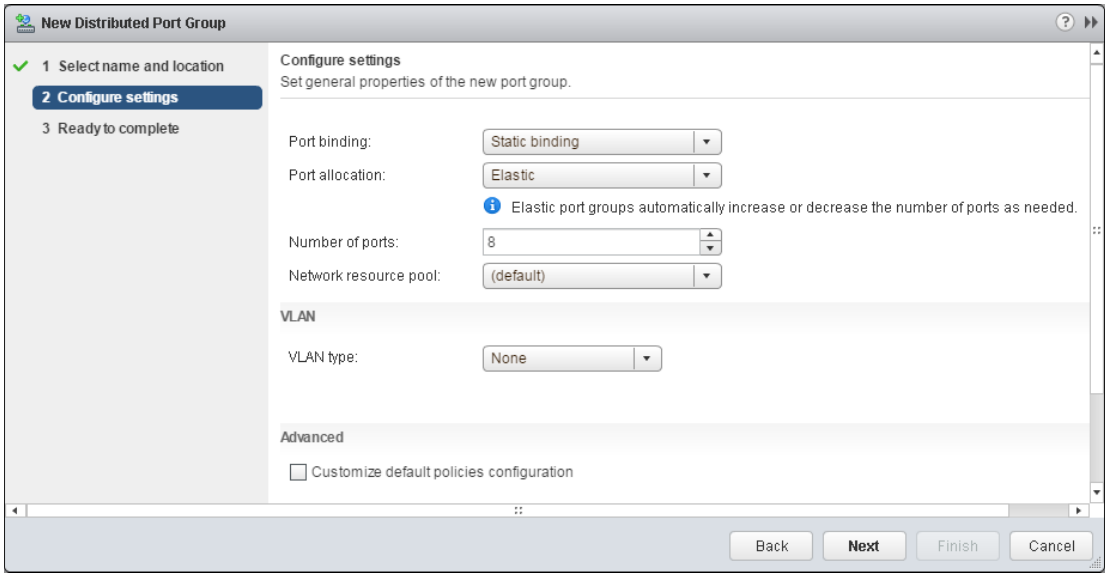
○ Add host and manage host networking (advanced)
Add new hosts and manage networking of hosts already attached to this distributed switch. Use this option to unify the network configuration of new and existing hosts.

Figure 6, Add Hosts to vDS

3) **NOTE:** if a Host's VMkernel or VM ports are still assigned to the vDS, the Host can't be removed

d. Add/Configure/Remove dvPort Groups

1) Add: Rt-click vDS > Distributed Port Group > **New Distributed PG**; modify Settings as needed



New Distributed Port Group

✓ 1 Select name and location
2 Configure settings
3 Ready to complete

Configure settings
Set general properties of the new port group.

Port binding: Static binding
Port allocation: Elastic
Elastic port groups automatically increase or decrease the number of ports as needed.
Number of ports: 8
Network resource pool: (default)

VLAN
VLAN type: None

Advanced
□ Customize default policies configuration

Figure 7, Configure dvPG Settings

2) Configure/Remove: Rt-click dvPG > Settings > Edit Settings or Delete; **NOTE:** unassign dvPorts from Hosts before deleting as you can't delete a dvPG with dvPorts still assigned

e. Add/Remove Uplink adapters to dvUplink Groups

1) Add: Rt-click dvPG > Edit Settings > Teaming & Failover & add 'Unused' Uplinks by clicking up arrow

2) To Remove, simply move the Uplink to 'Unused' section by clicking the down arrow

f. Configure vDS general & dvPG settings

1) Rt-click vDS > Settings > Edit Settings to change vDS <u>Name</u>, <u>number of Uplinks</u>, & <u>Network I/O</u>

2) Rt-click dvPG > Edit Settings and edit settings as needed (i.e. Teaming, VLAN, Advanced,

Monitoring, Misc, etc)

g. Create/Configure/Remove virtual adapters

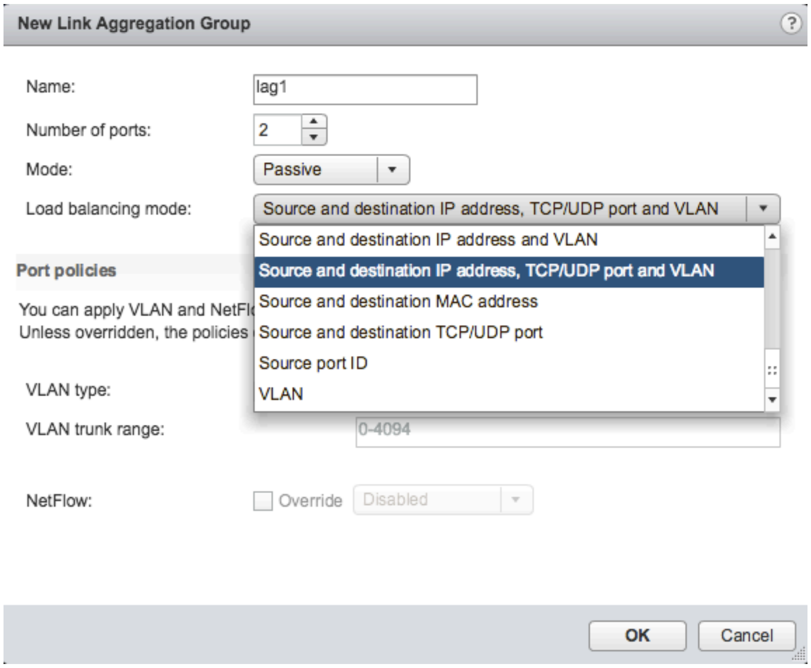
1) Create: Select a Host > Manage tab > Networking > VMkernel Adapters > click Add icon
2) Select VMkernel Network Adapter option, choose a dvPG, IP settings, services (VMotion, etc)
3) Configure/Delete: select the “vmk” from list > Edit (pencil) button or the Delete (“x”) button

h. Migrate VMs to/from a vDS

1) Rt-click a vDS > Migrate VM to Another Network…
2) Select the Source & a Destination vDS to migrate VMs from and to
3) Select VMs wanting to migrate and Finish

i. Configure LACP on Uplink PGs

1) Pre-req’s: minimum of 2 ports per LAG; Uplinks in LAG must match pSwitch Ports; LAG & Switch Hash must match; max of 64 LAGs per vDS; speed/duplex match pSwitch ports; 1 ‘Active’ LAG in Teaming/Failover; vDS 5.5 or 6.0; not able to deploy via Host Profiles; review all LACP support & limitations on pg. 56-57, Networking Guide
2) Create a Link Aggregation Group (LAG): Networking > vDS > Manage tab > Settings tab > LACP, then click ✚ ; set LAG to Standby in dvPG Team/Failover; assign pNICs to LAG Ports; set LAG to Active in dvPG


New Link Aggregation Group

Name: lag1

Number of ports: 2

Mode: Passive

Load balancing mode: Source and destination IP address, TCP/UDP port and VLAN

Port policies

You can apply VLAN and NetFl

Unless overridden, the policies

VLAN type:

VLAN trunk range: 0-4094

NetFlow: □ Override Disabled

?
Source and destination IP address and VLAN
Source and destination IP address, TCP/UDP port and VLAN
Source and destination MAC address
Source and destination TCP/UDP port
Source port ID
VLAN
OK
Cancel

Figure 8, Create LACP

j. Describe vDS Security policies/settings – on vSS/vDS Port Groups; all are set to *Reject* by default

1) These were discussed in Section 1.2 above (MAC Address Chg, Forged Transmit, Promiscuous)
   a) MAC Address Changes – affects incoming traffic to a VM to either change (Accept) or not change (Reject) the VM Effective MAC address
   b) Forged Transmits – affects outgoing traffic from a VM such that an ESXi Host compares the source MAC address with a VM’s Effective MAC (Reject), or not compare (Accept)

c) Promiscuous Mode – eliminates reception packet filtering such that a VM Guest OS receives all traffic (Accept), or traffic is filtered (Reject)

k. Configure dvPG Blocking Policies

1) Blocking can be done on either dvPG or dvUplinks in Settings > Miscellaneous; select 'Yes' or 'No' from drop-down

l. Configure Load Balancing/Failover Policies

1) Networking > rt-click dvPG > Edit Settings > Teaming & Failover

2) Load Balancing options:

a) Route based on originating virtual port – **default**

b) Route based on IP hash – etherchannel (Port Channel) needs to be configured on pSwitch

c) Route based on source MAC hash

d) Use explicit failover – by order of Uplinks under 'Active'

e) Route based on physical load – requires Ent+, and <u>on vDS only</u>

3) Failover – move Uplinks up down by up/down arrow to determine order as Active/Standby

m. Configure VLAN/PVLAN settings for VMs given communication requirements

1) Networking > rt-click dvPG > Edit Settings > VLAN and select VLAN options from drop-down

2) PVLAN: Networking > select vDS > Manage tab > Settings tab > PVLAN > Edit button > Add button; once this is set, go into dvPG & add PVLAN(s) as needed

3) VLAN & PVLAN notes:

a) VLAN tagging types – EGT (VLAN tagging done on pSwitch); VST (tagging done on ESXi Host); VGT (tagging done within the Guest OS)

b) PVLAN types – Promiscous = Primary PVLAN; Isolated = comm's only with Promiscous; Community = communicates with Promiscuous ports & ports on same secondary PVLANs

c) When PVLAN is created & assigned a VLAN ID, that same ID is assigned to the Promiscuous & cannot be changed

d) Only 1 Promiscuous and 1 Secondary Isolated VLANs per PVLAN allowed

4) Review KB: http://kb.vmware.com/kb/1010691

n. Configure Traffic Shaping Policies

1) Networking >rt-click dvPG > Edit Settings > Traffic Shaping, and modify Ingress/Egress options:

2) Avg bandwidth (kbits/s), Peak bandwidth (kbits/s), Burst size (KB)

o. Enable TCP Segmentation Offload support (TSO) for a VM

1) Enabled by default on on ESXi Hosts (**`net.UseHwTSO`**) & on vmxnet2/vmxnet3 adapters; in Windows adapter properties: Config tab > Adv'd, set 'Large Send Offload v2 (IPv4)' to Enabled

2) Linux: **`ethtool -K ethY tso on`**

p. Enable Jumbo Frames support on components

1) Enable on Physical Switch; vDS (Manage tab > Settings tab > Properties option > Edit button > Advanced option > MTU size to 9000); virtual adapter (Host > Manage tab > Networking tab > VMkernel option, select a VMkernel then the Edit (pencil) icon > NIC Settings & set to 9000); within the Guest OS adapter settings (Advanced > Configure)

q. Recognize behavior of vDS Auto-Rollback

1) Pg. 85-86 of Networking Guide

2) Rollback for vCenter is enabled by default: `config.vpxd.network.rollback` Advanced setting
3) Or, log into a Host DCUI > Network Restore Options > Restore vDS
4) Is done by deafult, or if disabled, can be done via DCUI; review Troubleshooting Guide for rollback behavior when issues encountered

r. Configure vDS across multiple vCenter Servers to support Long Distance VMotion
1) Requirements – vSphere6, Ent+, Web Client, vCenters in Enh Link Mode & in same SSO domain, vCenters time sync'd, and vCenters connected to same shared storage

s. Compare/Contrast vDS capabilities
1) http://kb.vmware.com/kb/1010555 – describes differences between vSS and vDS
2) vDS – Inbound traffic shaping, central mgmt, PVLAN, customize data plan, LLDP, Netflow, NIOC
3) If this means differences between vDS 5.0/5.1/5.5/6.0, not sure where that is documented

2.2 – Configure Network I/O Control (NIOC)

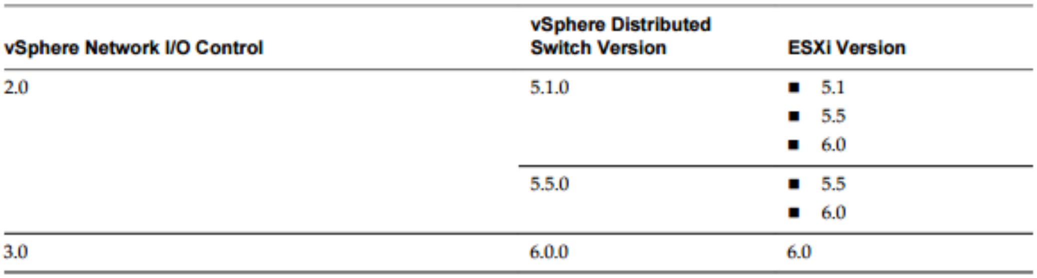
a. Define NIOC
1) vDS feature that allows bandwidth prioritization for different network resource pools

b. Explain NIOC capabilities
1) IEEE 802.1p outbound tagging
2) Load-based uplink teaming policy
3) Enforces traffic bandwidth traffic limits across vDS uplinks
4) Utilizes DRS & HA admission control
5) Separates system traffic into pools: FT, iSCSI, VM, VMotion, Mgmt, vRep, NFS
6) Configurable (in v3) on either vDS or VM (v2 was on phys adapter)

c. Configure NIOC Shares/Limits based on VM requirements (Low, Normal, High)
1) Select a vDS > Manage tab > Resource Allocation tab, select System Traffic
2) In the Traffic Type list at the bottom, select a type, then the Edit (pencil) icon; enter info
3) Shares can only be config'd 1-100; no more than 75% of an adapter bandwidth can be Reserv'd

d. Explain the behavior of a given NIOC setting
1) NIOC is based on Shares, Limits, Reservations so know what each are &, given resources, configure based off biz requirements & implications of what was implemented/config'd
2) Read through Network Guide & know requirements & implications of creating Network Pools, assigning NPs to dvPGs, & setting Share & Reservation bandwidth on VM adapters

e. Determine NIOC requirements
1) ESXi and vDS v.6 for NIOC v3; ESXi 5.1+ and vDS 5.1 for NIOC v2; Ent+



vSphere Network I/O Control	vSphere Distributed Switch Version	ESXi Version
2.0	5.1.0	■ 5.1 ■ 5.5 ■ 6.0
	5.5.0	■ 5.5 ■ 6.0
3.0	6.0.0	6.0

Figure 9, Network I/O Control Version Support

f. Differentiate NIOC capabilities
1) Main difference between NIOCv2 and v3 is SR-IOV isn’t available in v3 & user-defined settings in v2 are not retained when upgrading to v3
2) v2 bandwidth allocations are set at the physical adapter level; v3 on the vDS or VM level

g. Enable/Disable NIOC
1) Enable: Networking > rt-click vDS > Settings > Edit Settings > General , and Enable NIOC
2) Disable: same as above, but select Disable

h. Monitor NIOC
1) Networking > select vDS > Manage tab > Resource Allocation tab > System Traffic

SECTION III –Configure & Administer Advanced vSphere Storage

3.1 – Manage vSphere Storage Virtualization

a. Discover new storage LUNs
1) Adapter typess:
a) SCSI
b) iSCSI
c) RAID
d) FC
e) FCoE
f) Ethernet
2) Devices
a) Storage Adapter drivers are part of the VMkernel; as such, ESXi sees each device as a SCSI volume
3) Discovering new LUNs generally happens when an adapter rescan operation is performed
4) Auto rescans: creating/deleting/increasing a VMFS DS or RDM; adding an Extent
5) Manual rescans: Zone a new disk array; create new LUN on SAN; change Host Path Masking; reconnect a cable; change CHAP; add/remove iSCSI discovery/static addresses

b. Configure FC/iSCSI/FCoE LUNs as ESXi boot devices
1) FC – create a boot LUN for each Host; mask each LUN to its respective Host; get WWPN for SAN front-end port; configure storage adapter on each Host to boot from SAN (vendor-specific)
2) ISCSI – same as above, but determine iSCSI name/IP for targets assigned per Host; software or dependent iSCSI adapters must support iBFT (iSCSI Boot Firmware Table)

3) FCoE – enable Spanning Tree on pSwitch, dedicate whole boot LUN solely to FCoE Adapter; review remaining concepts in Storage Guide, pg. 55

c. Create NFS share for use with vSphere

1) Create a storage volume
2) Create folder on the volume
3) Share a folder on volume allowing Host(s) IP R/W access to share
4) Add NFS Storage in vSphere

d. Enable/Configure/Disable vCenter Server storage filters (all are configured by default)

1) **`config.vpxd.filter.vmfsFilter`** – filters LUNs already used by VMFS Datastore on any Host used by vCenter
2) **`config.vpxd.filter.rdmFilter`** – filters LUNs already referenced as RDM
3) **`config.vpxd.filter.SameHostAndTransportsFilter`** – filters LUNs unable to be used as Extent
4) **`config.vpxd.filter.hostRescanFilter`** – auto rescan enabled after performing certain storage functions (see Scan/Rescan section above)

e. Configure/Edit Independent/Dependent hardware initiators

1) Dependent HW – just need to make sure device is on VMware's HCL; vmk's needed
2) Independent HW – completely offloads to the adapter; vmk's not needed
3) Host > Manage tab > Storage tab > Storage Adapters, select new adapter in the list then click Edit button
4) FCoE – disable STP on pSwitch (prevent possible APD), turn on Priority-Based Flow Control (PFC) & set to AUTO

f. Enable/Disable software iSCSI initiator

1) Host > Manage tab > Storage tab > Storage Adapters, & click "**+**" (Add) > Software iSCSI Adapter
2) After added, select it & in the bottom Adapter Details section, click the Enable (Disable) button

g. Configure/Edit software iSCSI initiator

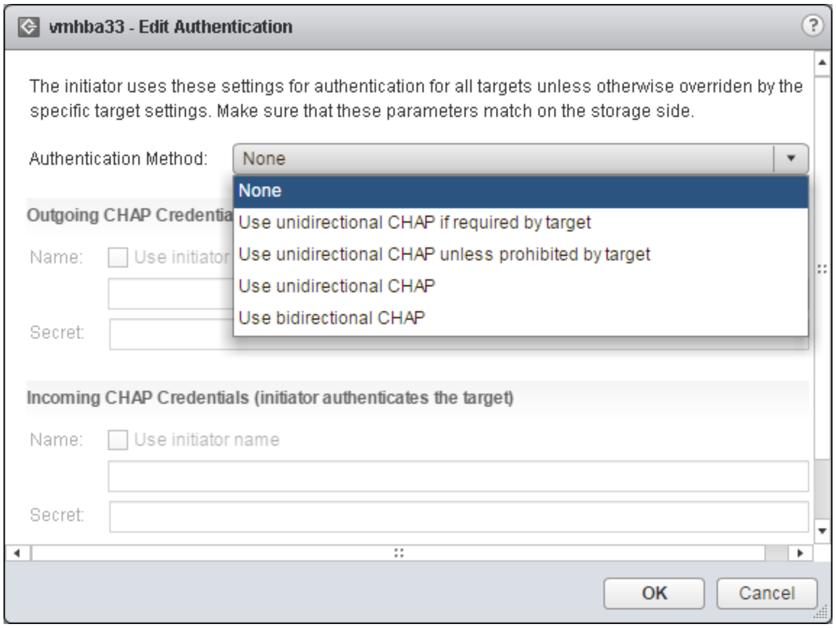
1) In the Host Storage Adapters, select the software adapter then choose tab options at bottom under Adapter Details; click the Edit button to modify settings

h. Configure iSCSI port binding

1) Host Storage Adapters, select the software adapter, then Network Port Binding tab at bottom and click "**+**" to add vmk's

i. Enable/Configure/Disable iSCSI CHAP

1) Host Storage Adapter, select the software adapter, then Properties tab at bottom > Authentication > Edit button; configure CHAP options (see below)



vmhba33 - Edit Authentication

The initiator uses these settings for authentication for all targets unless otherwise overriden by the specific target settings. Make sure that these parameters match on the storage side.

Authentication Method: None

None
Use unidirectional CHAP if required by target
Use unidirectional CHAP unless prohibited by target
Use unidirectional CHAP
Use bidirectional CHAP
Outgoing CHAP Credentia
Name:
Use initiator
Secret:
Incoming CHAP Credentials (initiator authenticates the target)
Name:
Use initiator name
Secret:
OK
Cancel

Figure 10, Enable iSCSI CHAP

j. Determine use case for FC Zoning

1) Security and segregation; done on the SAN/array side

k. Compare/Contrast array thin provisioning and virtual disk thin provisioning

1) Array – at the SAN (LUN) level; ESXi Host is not aware UNLESS array is VAAI capable; disk grows as data added even if a VMDK is thick-provisioned

2) VMDK – at VM level; disk grows as data written to disk only

3) Both can lead to over-provisioning storage

3.2 – Configure Software-Defined Storage

a. Explain VSAN and VVOL architectural components

1) VSAN:

a) vCenter 5.5U1, minimum of 3 ESXi 5.5 Hosts, & Web Client

b) Uses **Disk Groups** containing only 1 Flash & up to 7 HDDs (min 1 HDD required); each ESXi Host can have up to 5 Disk Groups (DGs)

c) **VSAN Storage** = (# of HDDs in a DG x # of DG x # of Hosts) – Overhead (1% per HDD x # of DGs x # of Hosts)

d) **Witnesses** – component containing only metadata

e) **VM Storage Policies/Storage Policy Based Management (SPBM)**

f) **VSAN Storage Objects** – VMDKs, VM Home, VM Swap, Snapshot Delta

g) Aggregates storage across ESXi Hosts in a Cluster to create a single DS; can later be expanded by adding HDDs to VSAN DGs, or simply adding Hosts with devices

h) **Fault Domains** – used as a redundancy mechanism in VSAN dispersing objects across racks (i.e. other fault domains)

2) VVOL:

a) **Virtual Volumes** – encapsulations of VM files, virtual disks (VMDKs), & their derivatives stored natively on the storage system

1. Identified by a unique GUID

2. Created automatically when performing a VM operation (creation, cloning, snapshotting)
3. Two VVOL types – data VVOL (VMDKs); configuration VVOL (vmx, logs, deltas, etc); **VMFS**

b) **Storage Provider** – VASA provider; software component acting as a vSphere storage awareness service, mediating out-of-band communication between vC/ESXi & storage system
1. Implemented with VMware APIs for Storage Awareness (VASA) & integrates with vSphere Storage Monitoring Service (SMS)
2. Delivers information from storage system (storage container) to vCenter & ESXi

c) **Storage Containers** – pool of raw storage capacity/aggregation of storage capabilities
1. Minimum of one Container is required; Container cannot span multiple arrays
2. Single Container can export multiple capability profiles thus VMs with diverse needs & differing storage policy settings can be a part of same Container
3. Must be mapped to vSphere as Virtual Datastores

d) **Protocol Endpoints** – logical I/O proxy for ESXi Hosts to communicate with VVOLs/VMDKs
1. Establishes a data path on demand from VMs to the VMs respective VVOL
2. Discovered by ESXi Hosts once Containers are mapped via Virtual Datastore creation

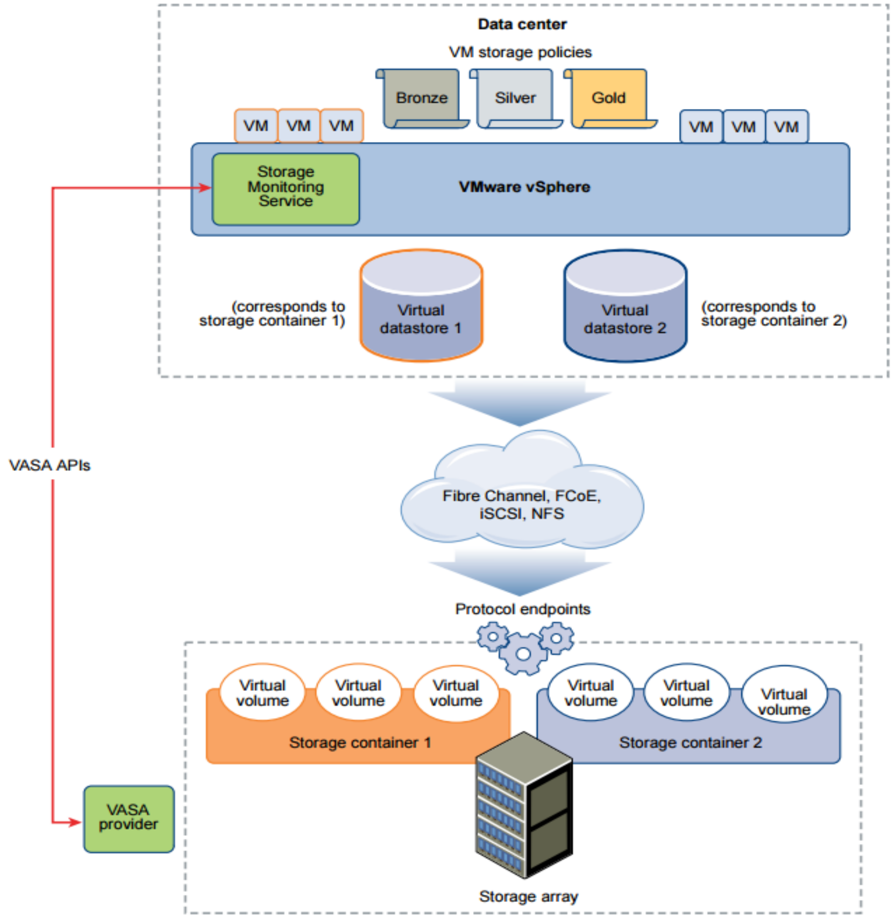


Figure 11, VVOL Architecture Diagram

b. Determine the role of storage providers in VSAN
1) Report underlying storage capabilities to vCenter; communicates VM storage req's with VSAN
2) View providers by selecting vCenter > Manage tab > Storage Providers; all Hosts have SP but only 1 is active

c. Determine the role of storage providers in VVOLs

1) VMware API for Storage Awaremess (VASA) provider; a software component acting as a storage awareness service, mediating out-of-band communication between vC/ESXi & storage system

d. Explain VSAN failure domains (FD) functionality

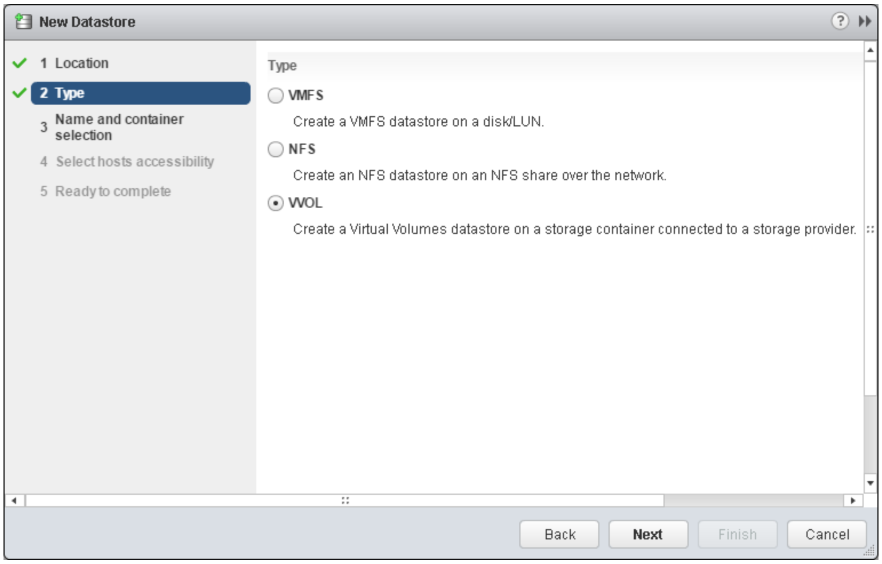
1) FDs instructs VSAN to distribute redundant components across servers in separate racks (FDs)
2) In simplest terms, a FD consists of 1 or more Hosts in a single server rack; minimum FD = 3
3) If a Host in a 3-Host FD fails, other Hosts are still operational and can receive data from the failed Host; VMs can be restarted via HA on the other 2 FD Hosts or Hosts in other FDs

e. Configure/Manage VSAN

1) Add a VSAN Network (VMkernel or vmk) to each Host participating in VSAN Cluster
2) Enable VSAN on a vSphere Cluster (select Cluster > Manage tab > Settings tab > Edit button and click to select 'Turn On VSAN'; **NOTE:** HA must be turned off first; and, VSAN Datastores canNOT be used for HA DS Heartbeating
3) Create a DG (in Cluster settings), of 1 SSD & at least 1 HD (but up to 7 HDs) for each ESXi Host in VSAN Cluster; **NOTE:** Not all participating Hosts need to have a DG
4) Add min of 3 Hosts to the VSAN Cluster; VSAN DS will display total of all Host DG's HD storage
5) If not already done, add a VSAN license to the Cluster: select the Cluster > Manage tab > Settings tab > Configuration section & select Licensing and click the Assign License button

f. Create/Modify VVOLs

1) Verify time sync among ESXi Hosts participating in VVOLs
2) Register vendor Storage Provider – vCenter > Manage tab > Storage Providers tab > click Register storage provider icon ("+"), then OK
3) Create a Virtual Datastore – Inventory > Datastores > Add DS icon > select VVOL type > select appropriate Storage Container in list & Hosts requiring access, then FINISH



Type

○ VMFS
Create a VMFS datastore on a disk/LUN.

○ NFS
Create an NFS datastore on an NFS share over the network.

● VVOL
Create a Virtual Volumes datastore on a storage container connected to a storage provider.

Figure 12, Create Virtual Datastore Wizard

4) Review Protocol Endpoint Multipathing Policy & change if needed: Host > Manage tab >

Storage tab > Protocol Endpoints

5) Create VM Storage Policy – Home > Policies/Profiles > VM Storage Policies > Create new VM Storage Policy
6) Create VMs and assign Policies to VM VMDKs (VM > Edit Settings > Virtual Hardware > expand Hard Disk #, and assign 'VM Storage Policy' from drop-down menu)

g. Configure Storage Policies

1) Home > Policies/Profiles > VM Storage Policies > Create new VM Storage Policy
2) Assign policy to VM disk(s)

h. Enable/Disable VSAN Fault Domains

1) Select VSAN Cluster > Manage tab > Settings tab, VSAN section and select Fault Domains
2) Click "+" to add a Host(s) to FDs

i. Create VVOLs given the workload and availability requirements

1) Pre-req's: verify SAN is VASA compliant; verify NTP config'd; SAN Storage Containers config'd
2) Register Storage Providers: vCenter > Manage tab > Storage Providers & click 'Register New Storage Provider' icon
3) Create a VVOL Datastore: Datastores > Create DS icon and select VVOL as DS 'Type'; add listed Storage Containers, then Finish
4) Review/change any Protocol Endpoints: Host > Manage tab > Storage tab > Protocol Endpoints

j. Collect VSAN Observer output

1) Launch via Ruby vSphere Console (RVC) ESXi Host CLI: **`vsan.observer --<parameter>`**
2) Once launched, go to a web browser & enter vCenter IP with port 8010 to view info/graphs
3) To collect Observer logs: **`vsan.observer <cluster> --run-webserver --force --generate-html-bundle /tmp --interval ## --max-runtime 1`**

k. Create Storage Policies appropriate for given workloads and availability requirements

1) Creating Storage Policies is discussed above. Create policies based on performance, SLAs, etc, then just assign a given SP to a VM VMDK as required

l. Configure VVOLs Protocol Endpoints

1) Host > Manage tab > Storage tab > Protocol Endpoints > select the Endpoint > Properties tab > Edit Multipathing button under 'Policies'

3.3 – Configure vSphere Storage Multi-pathing and Failover

a. Explain common multi-pathing components

1) The adapter (FC, iSCSI, physical NIC)
2) SAN or Network Switch
3) SAN Storage Processors (SPs)
4) PSA – Pluggable Storage Architecture
5) NMP – Native Multipathing Plug-in; generic VMware mutlipathing module
6) PSP – Path Selection Plug-in (Policy); handles path selection for a given device
7) SATP – Storage Array Type Plug-in (Policy); handles path failover for a given device

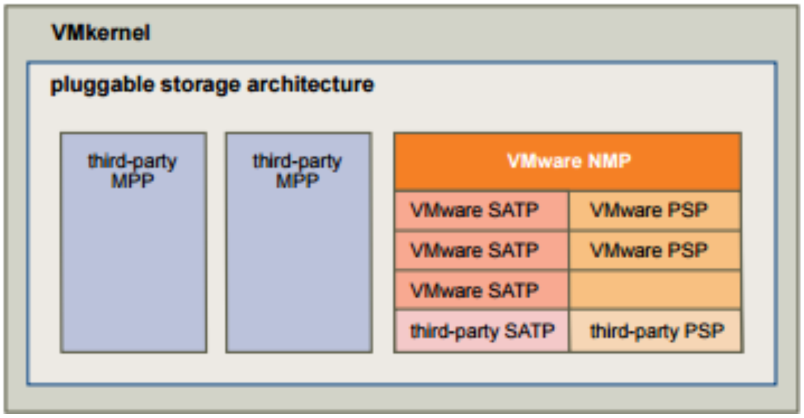


Figure 13, PSP/Multi-pathing Architecture

b. Differentiate APD and PDL states

1) APD – All Paths Down; condition when a storage device becomes inaccessible to the Host & no paths to device are available; transient condition, meaning it's **temporary**; APD timer = 140 secs

2) PDL – Permanent Device Loss; condtion when a storage device **permanently** fails or is administratively removed/excluded

c. Given a scenario, compare/contrast Active Optimized vs Active non-Optimized PG states

1) The default PSP for devices claimed by VMW_SATP_ALUA is VMW_PSP_MRU, which selects an "active/optimized" path reported by VMW_SATP_ALUA, or an "active/unoptimized" path if there's no "active/optimized" path; will revert to active/optimized when available

d. Explain features of the Pluggable Storage Architecture (PSA)

1) See Figure 12 above

2) PSP – responsible for choosing physical path I/O

a) MRU: selects a path upon boot; when path unavailable selects alternate, & does **not** revert (active/passive)

b) FIXED: selects preferred path upon boot; when unavailable selects alternate, & **does** revert (active/active)

c) RR: I/O rotates through active paths

3) SATP – responsible for array-specific operations, monitoring path health, changes in path state, & failover operations

e. Understand the effects of a given claim rule on multipathing & failover

1) Claim rules indicate which multipathing plug-in NMP or 3rd party MPP manages a given path

2) When a Host is started or rescan performed, it discovers all physical paths to storage devices, and based on claim rules determines which MPP claims the path to a device

3) The system searches SATP rules to assign to devices first by driver rules, then vendor or model rules, and lastly by transport rules

a) If no SATP match is found, the default SATP for FC and iSCSI is VMW_SATP_DEFAULT_AA and the default PSP for that SATP is VMW_PSP_FIXED

b) If a device is claimed by VMW_SATP_DEFAULT_ALUA, the default PSP is VMW_PSP_MRU

f. Explain the function of claim rule elements

1) Vendor

2) Model
3) Device ID
4) SATP
5) PSP
* Not sure what is really required here. The Storage Guide mentions Claim Rule elements (vendor, etc), but doesn't state 'function' per se. SATP & PSP were discussed above

g. Change the Path Selection Policy (PSP) using the UI
1) Host > Storage tab > Storage Devices > Properties tab > Mutipathing Policies section, click Edit Multipathing button, and select a PSP from drop-down, then click OK

h. Determine required claim rule elements to change the default PSP
1) PSA plugin to use (-P); Type (-t; values = vendor,location,driver,transport,device,target)
2) See pg. 194-195 esxcli claimrule parameters (note 'required' by each parameter description)

i. Determine the effect of changing PSP on Multipathing and Failover
1) Use Web UI or esxcli cmd, then a Host reboot is required
2) Paths must 1st be unclaimed, then reclaimed to be able to make the change

j. Determine the effects of changing SATP on relevant device behavior
1) VMware provides a SATP for every array VMware supports on the HCL
2) SATP monitors path health, , responds to errors from array, and handles failover
3) Changing the SATP may change the PSP which may create unexpected failover results

k. Configure/Manage Storage Load Balancing
1) Datastores > select a DS > Manage tab > Settings tab > Connectivity & Multipathing > select Host from the list and view MP details and change if needed

l. Differentiate available Storage Load Balancing options
1) This was discussed earlier (MRU, FIXED, RR) in d. above

m. Differentiate available Storage Multi-Pathing Policies
1) RR, MRU, FIXED were discussed in d.2) above

n. Configure Storage Policies
1) Home > VM Storage Policies, then assign to a VM Hard Disk

o. Locate failover events in the UI
1) select the vCenter Server > Monitor tab > Events tab

3.4 – Perform Advanced VMFS & NFS Configuration & Updates

a. Describe VAAI primitives for block devices and NAS
1) Block primitives: ATS (VMFS lock); Thin Provisioning; Full Copy (Cloning); Block Zero
2) NAS primitives: Full File Clone (Cloning); Reserve Space (VMDK thick prov); Native Snap Support; Extended Statistics
3) For example, to reclaim 'free' space on a Thin LUN/DS, use the esxcli cmd with UNMAP (see: http://kb.vmware.com/kb/2057513)

b. Differentiate VMware file system technologies

1) VMFS – block-based
2) NFS – file system-based

c. Upgrade VMFS3 to VMFS5

1) Datastores > select a DS on left > Manage tab > Settings tab > click Upgrade to VMFS5 link, OK
2) Perform DS rescan for all Hosts connected to the upgraded DS

d. Compare functionality of newly created vs upgraded VMFS5 datastores

1) New – 64TB datastores; 1MB block; VM = 62TB disks; small file suppt; storage reclamation; GPT
2) Upgraded – 1/2/4/8MB block; MBR; ATS+SCSI; 64KB subblock size; VM = 2TB VMDKs

e. Differentiate Physical Mode RDMs & Virtual Mode RDMs

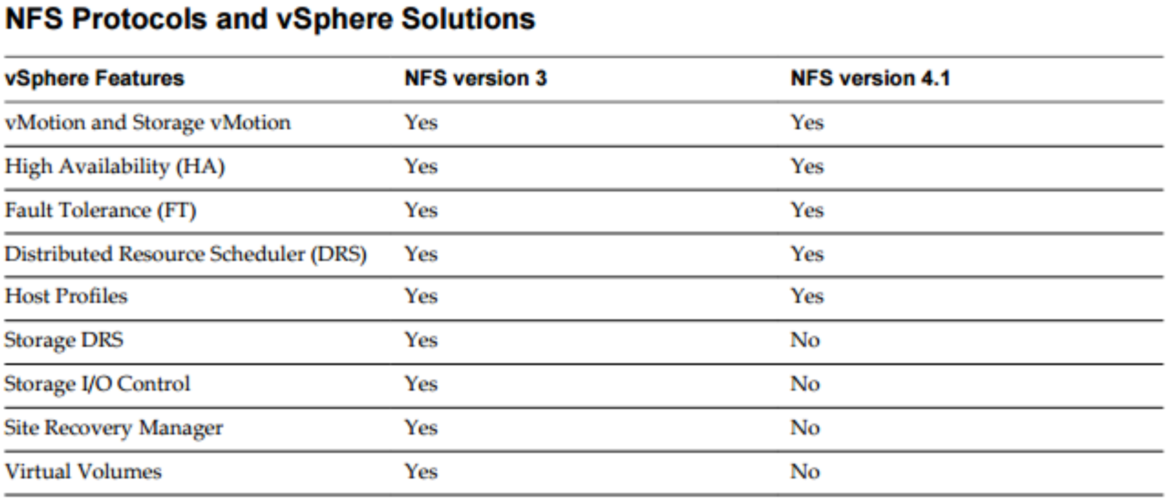
1) Physical – passes all SCSI cmds, except REPORT LUNs to mapping device; used for NPVI & MSCS; No snapshotting
2) Virtual – passes all READ & WRITE cmds to mapping device, not SCSI cmds
3) Pay note to what features/functions can be used with each RDM type when reviewing the Guides

f. Create Virtual/Physical Mode RDM

1) New VM wizard > on Customize Hardware window > New device drop-down, and select RDM > select a device/LUN > expand New Hard Disk & select RDM mode (disk mode), then OK

g. Differentiate NFS 3.x and 4.1 capabilities

1) NFS 4.1 does not support legacy FT or hardware acceleration (i.e. can't create thick disks); multipathing that supports session trunking; kerberos; share reservations; file locking; nonroot users; non-Kerberos mounts; simultaneous AUHT_SYS not supported
2) NFS 3 doesn't encrypt; no delegate user function; supports h/w acceleration



NFS Protocols and vSphere Solutions

vSphere Features	NFS version 3	NFS version 4.1
vMotion and Storage vMotion	Yes	Yes
High Availability (HA)	Yes	Yes
Fault Tolerance (FT)	Yes	Yes
Distributed Resource Scheduler (DRS)	Yes	Yes
Host Profiles	Yes	Yes
Storage DRS	Yes	No
Storage I/O Control	Yes	No
Site Recovery Manager	Yes	No
Virtual Volumes	Yes	No

Figure 14, NFS Protocol Feature Support

h. Compare/Contrast VMFS & NFS datastore properties

1) Shared already a bit above

i. Configure Bus Sharing

1) Rt-click VM > Edit Settings > Virtual Hardware tab > expand SCSI Controller, select SCSI Bus Sharing type from drop-down (None, Virtual [disk shared by VMs on same Host], Physical [disk shared by VMs on diff Hosts])

j. Configure Multi-Writer Locking

1) Rt-click VM > Edit Settings > VM Options tab > expand Advanced, click Edit Configuration > Add Rows > add Parameter for each HD with name of disk (i.e. scsi:0:sharing ; scsi:1:sharing) and set each SCSI parameter's value to **multi-writer**
2) Or, in Virtual H/W tab > expand Hard Disk # > configure the "Sharing" option drop-down to multi-writer

k. Connect an NFS 4.1 datastore using kerberos

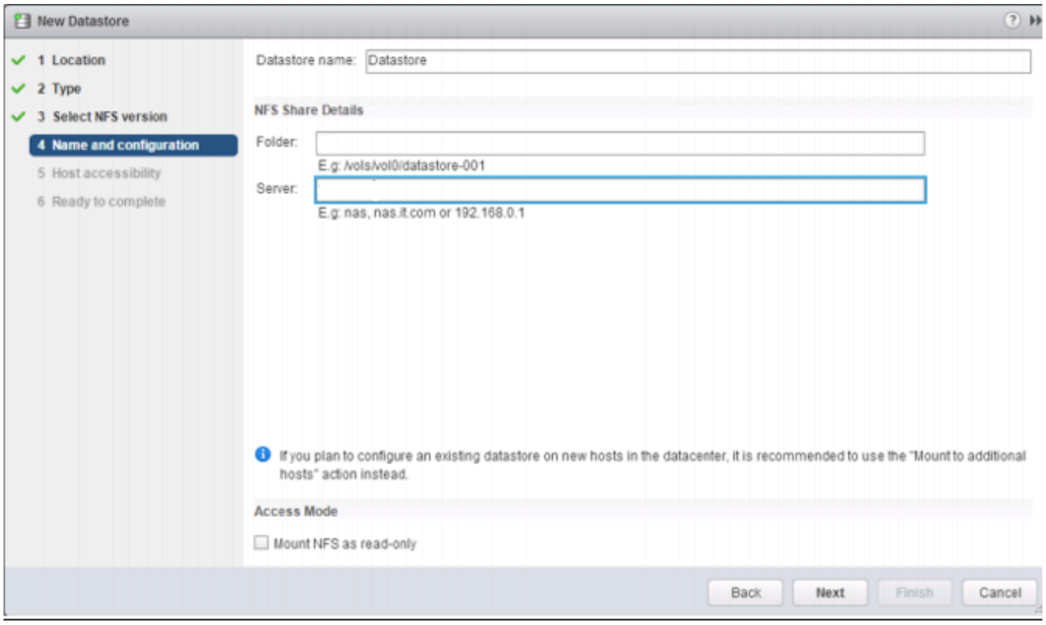
1) Per Host, and set DNS, time, and add each Host to an AD Domain (Settings tab)

l. Create/Rename/Delete/Unmount VMFS datastore

1) Create: Host/Clusters > Related Objects tab > Datastores tab > Add DS icon & follow wizard
2) From same area, rt-click DS & Rename, or Delete, or Unmount; Delete/Unmount pre-req's = no VMs; not in SDRS Cluster; SIOC is disabled; not used for HA DS Heartbeat

m. Mount/Unmount NFS datastore

1) Datastores > Add DS wizard > specify location > select NFS as type > select NFS version > enter DS Name > enter NFS share details (server, folder)



Datastore name: Datastore

NFS Share Details

Folder:

E.g: /vols/vol0/datastore-001

Server:

E.g: nas, nas.it.com or 192.168.0.1

If you plan to configure an existing datastore on new hosts in the datacenter, it is recommended to use the "Mount to additional hosts" action instead.

Access Mode

□ Mount NFS as read-only

Figure 15, Add NFS (Mount) Wizard

2) Unmount – rt-click DS > Unmount; **NOTE:** an Unmounted NFS (or VVOL) disappears from Inventory; DS unmount checks/pre-req's: no VMs, not in SDRS, SIOC disabled, not used in HA heartbeating

n. Extend/Expand VMFS datastore

1) Datastores > click Increase DS Capacity icon

o. Place a VMFS datastore in Maintenance Mode

1) Rt-click a DS > Maintenance Mode > Enter Maintenance Mode

2) Pre-req's for DS to be in MM: Storage DRS enabled; no CD Image Files stored on DS

p. Select the Preferred Path/Disable a Path to VMFS datastore

1) Preferred path can only be set on devices with FIXED PSP set

2) Host > Manage tab > Storage Devices > Properties tab (below) > MP Policies > Edit Multipathing button > click to select the Pref Path, then click OK (nothing definitively shows verifying the path as Pref)

q. Enable/Disable vStorage API for Array Integration (VAAI)

1) **Enable**: Per Host > Manage tab > Settings tab > Advanced > search for `datamover` options and verify value is set to **1** ; set to **0** **to disable**

r. Given a scenario, determine a proper use case for multiple VMFS/NFS datastores

1) HA – DS heartbeating

2) Storage Policies with different service levels (i.e. performance)

3) Prevent disk contention

3.5 – Setup and Configure Storage I/O Control (SIOC)

a. Describe benefits of SIOC

1) Cluster-wide storage I/O prioritization allowing better workload consolidation & reduces overprovisioning costs; extends constructs of Shares/Limits per VM during I/O contention

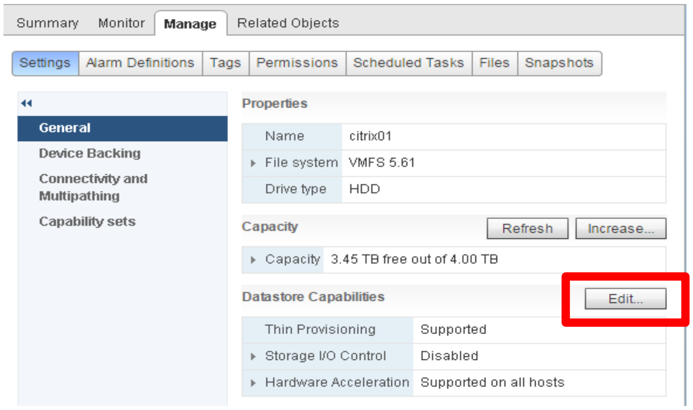
b. Enable/Configure SIOC

1) Already enabled by default on SDRS Cluster DS's

2) Req's: vCenter; RDM not supported; multiple DS extents not supported, Ent+, ESXi 4.1+

c. Configure/Manage SIOC

1) Go to Datastores > select it > Manage tab > Settings > General, and select Edit button, then check the box to enable SIOC; configure settings as needed



Properties

Name	citrix01
File system	VMFS 5.61
Drive type	HDD

Capacity

Capacity	3.45 TB free out of 4.00 TB

Datastore Capabilities

Thin Provisioning	Supported
Storage I/O Control	Disabled
Hardware Acceleration	Supported on all hosts

Figure 16, Enable SIOC

2) Set Share/Limit settings on VM disk(s)

d. Monitor SIOC
1) Storage > select a DS > Monitor tab > Performance tab, click Overview and set to Realtime

e. Differentiate between SIOC and Dynamic Queue Depth Throttling features
1) SIOC is a mechanism in the hypervisor that controls I/O via Shares/Limits
2) Queue Depth Throttling is an algorithm that adjusts LUN queue depth in the VMkernel I/O stack that reduces queue depth when there's contention (i.e. queue is full)

f. Given a scenario, determine a proper use case for SIOC
1) Any time disk latency averages 15+ms of latency
2) A lower ms threshold = less latency (i.e. higher performance), but also less throughput; higher ms = potential for more latency (degraded performance), but has higher throughput; default latency thresholds based on storage media/protocols: **FC = 20-30ms**; **SAS = 20-30ms**; **SSD = 10-15ms**; **SATA = 30-50ms**

g. Compare/contrast the effects of I/O contention in environments with/without SIOC
1) Without SIOC, a 'noisy neighbor' VM could attain more storage I/O than its allotment

SECTION IV – Upgrade a vSphere Deployment to 6.x

4.1 – Perform ESXi Host and Virtual Machine Upgrades

a.Configure download sources
1) Using C# Client > Home > Solutions and Applications > Update Manager > Configuration tab > Settings > Download Settings
3) In Download Sources pane, select 'Direct connection to Internet' > click **Add Download Source**
4) Enter the download source URL, (optional) description, then click 'Validate' > OK, then Apply

b. Setup a UMDS download repository
1) Using C# Client > Home > Solutions and Applications > Update Manager > Patch Repository tab

c. Import ESXi images
1) Update Manager > ESXi Images tab > Import ESXi Image, browse to the ISO & select Finish

d. Create Baselines and Baseline Groups
1) Update Manager > Baselines & Groups tab > click button for Host or VM, then the Create link
2) In same area, in the bottom Baseline Groups pane, click the Create link

e. Attach Baselines to vSphere objects
1) Select a vSphere object > Update Manager tab on right, then click the Attach link
2) You can do object solely, or via Cluster, Datacenter, folder, etc. for multiple objects

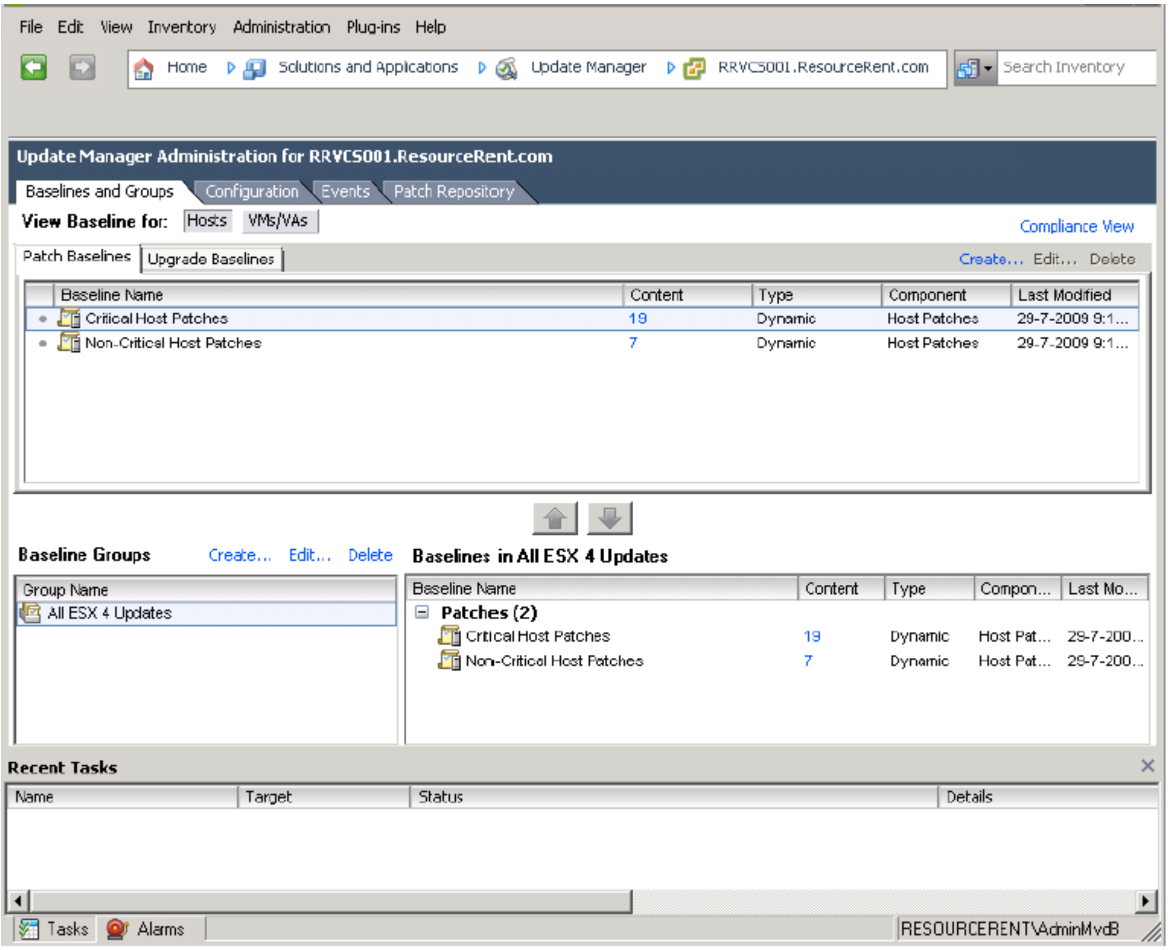
f. Scan vSphere objects
1) Select a vSphere object to scan > Update Manager tab on right, then click Scan & follow wizard

g. Stage patches and extensions

1) Select a vSphere Host to stage > Update Manager tab on right, then click Stage & follow wizard

h. Remediate an object

1) Select a vSphere object to remediate > Update Manager tab on right, then click Remediate



Update Manager Administration for RRVCS001.ResourceRent.com

View Baseline for: Hosts VMs/VAs

Baseline Name	Content	Type	Component	Last Modified
Critical Host Patches	19	Dynamic	Host Patches	29-7-2009 9:1...
Non-Critical Host Patches	7	Dynamic	Host Patches	29-7-2009 9:1...

Baseline Groups Create... Edit... Delete

Group Name
All ESX 4 Updates

Baselines in All ESX 4 Updates

Baseline Name	Content	Type	Compon...	Last Mo...
Patches (2)				
Crtical Host Patches	19	Dynamic	Host Pat...	29-7-200...
Non-Critical Host Patches	7	Dynamic	Host Pat...	29-7-200...

Recent Tasks

Name	Target	Status	Details

Figure 17, Update Manager Window

i. Upgrade a vDS

1) Networking > rt-click a vDS > Upgrade > Upgrade a Distributed Switch

j. Upgrade VMware Tools (several methods)

1) Select to automatically ‘Check and upgrade VMware Tools before power on’ in VM Options tab

2) Use VUM

3) List VMs > select several (with same OS) > Guest OS > Upgrade VMware Tools

4) Silent install (see: http://kb.vmware.com/kb/1018377)

k. Upgrade VM hardware

1) Power down VM(s) > rt-click and select Upgrade VM Compatibiltiy (or choose from Actions)

l. Upgrade an ESXi Host using vCenter Update Manager (VUM)

1) Configure UM Settings in Configuration tab (Maint Mode, Cluster, etc.)
2) Configure Baseline/Baseline Group if not already done
3) Attach BL/BLG to inventory object (explicit Host, or DC/Folder objects)
4) Manually perform UM Scan & review results of inventory objects' compliance
5) Select Host or vSphere object > UM tab > Remediate

m. Stage multiple ESXi Host upgrades

1) Same as l. above, but perform on a Host 'container' object (Cluster, DC, or folder)

n. Assign appropriate Baselines with target inventory objects

1) Discussed above

4.2 – Perform vCenter Upgrades

a. Compare methods of upgrading vCenter Server

1) Windows or appliance install with embedded or external Platform Services Controller (PSC)

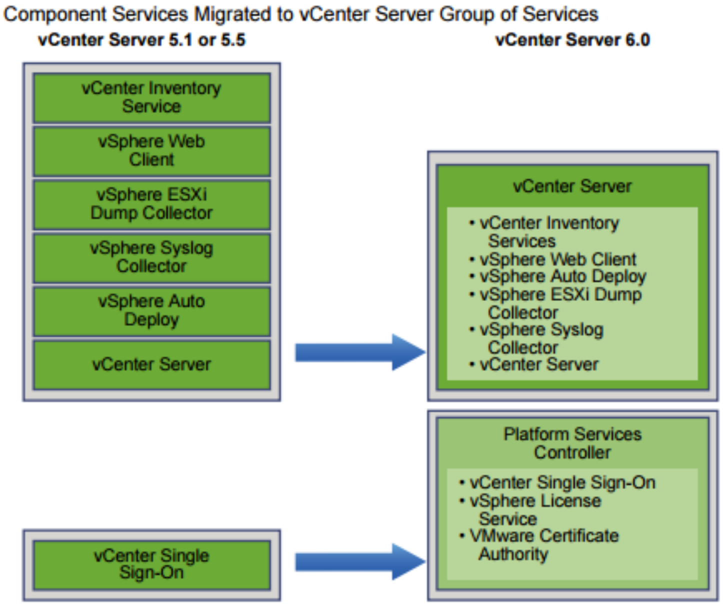

Component Services Migrated to vCenter Server Group of Services
vCenter Server 5.1 or 5.5
vCenter Server 6.0
vCenter Inventory Service
vSphere Web Client
vSphere ESXi Dump Collector
vSphere Syslog Collector
vSphere Auto Deploy
vCenter Server
vCenter Single Sign-On
vCenter Server
• vCenter Inventory Services
• vSphere Web Client
• vSphere Auto Deploy
• vSphere ESXi Dump Collector
• vSphere Syslog Collector
• vCenter Server
Platform Services Controller
• vCenter Single Sign-On
• vSphere License Service
• VMware Certificate Authority

Figure 18, vCenter Upgrade Path

b. Backup vCenter Server database, configuration, and certificate datastore

1) DB backup: dependent on DB type (SQL, Oracle, PostgreSQL)
2) Config backup: didn't see any documentation on this, but think there is an option for Win install
3) Cert store backup: same as 2; or, if using VCSA, just snap the VM appliance

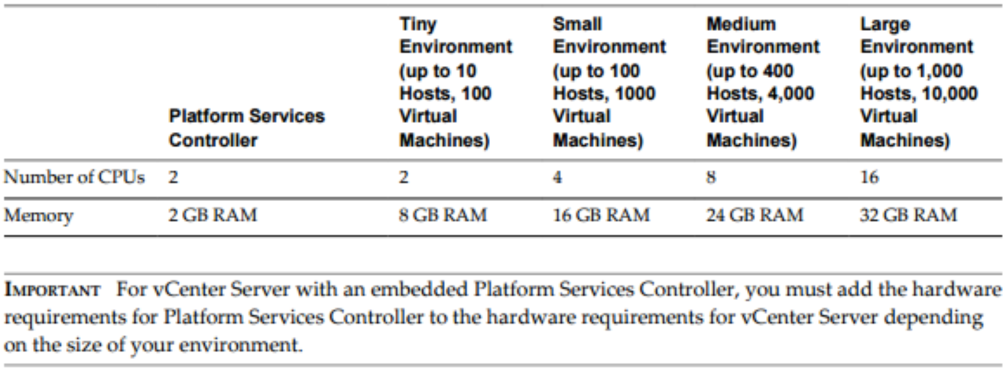
c. Perform update as prescribed for Appliance or Installable

1) Installable: upgrade SSO to PSC first, then vCenter (which now houses Inv, Web, & vC svcs , etc); if your install is already 'Embedded' (everything on 1 server), just run installer on vCenter
2) Appliance: always upgraded to an Embedded install; if wanting to use external PSC, a new VCSA must be deployed
3) **DB info:** Windows embedded can use bundled PostgreSQL for up to 20 Hosts/200 VMs; VCSA

bundled PostgreSQL supports up to 1000 Hosts/10000 VMs, or external Oracle

d. Upgrade VCSA
1) VCSA must be minimum of VCSA 5.1U3 to upgrade to v6; VCSA min ESXi Host version = 5.0
2) Download VCSA ISO and install the Client Integration Plugin
a) On Win 2012 server, just double-click the ISO to 'extract' the ISO contents > go into the **vcsa** folder and double-click 'ClientIntegrationPlugin-6.0.0.exe'
3) Export current VCSA configuration – didn't find how this is done; just snapshot the VCSA
4) After plug-in install, run **vcsa-setup.html**; **NOTE:** if plug-in isn't installed, you won't be able to view the web page correctly to perform the VCSA upgrade/install; min browser > FF 30+, Chrome 35+, IE10/11
5) Fill in appropriate info when requested

e. Given a scenario, determine the upgrade compatibility of an environment
1) Windows install is compatible to upgrade to v6 directly from 5,.x; VCSA min 5.1U3
2) VCSA upgrade is always embedded; to have external PSC, a new VCSA must be installed
3) vCenter sizing; **NOTE:** add the PSC requirement to the vCenter requirement for total min resources needed for install:



	Platform Services Controller	Tiny Environment (up to 10 Hosts, 100 Virtual Machines)	Small Environment (up to 100 Hosts, 1000 Virtual Machines)	Medium Environment (up to 400 Hosts, 4,000 Virtual Machines)	Large Environment (up to 1,000 Hosts, 10,000 Virtual Machines)
Number of CPUs	2	2	4	8	16
Memory	2 GB RAM	8 GB RAM	16 GB RAM	24 GB RAM	32 GB RAM

IMPORTANT For vCenter Server with an embedded Platform Services Controller, you must add the hardware requirements for Platform Services Controller to the hardware requirements for vCenter Server depending on the size of your environment.

Figure 19, vCenter Resource Requirements

4) vCenter for Windows – OS requirement = Win2K8 SP2; local DB can support 20 Hosts/200 VMs

f. Determine correct order of steps to upgrade a vSphere implementation
1) SSO → Platform Services Controller (PSC); PSC consolidates License Svr, SSO, & VMCA
2) vCenter → consolidates Web Client, Inventory Svc, Dump Collector, Syslog, Auto Dep, vCenter
2) VUM (if used)
3) ESXi Hosts
4) vSphere Client (only needed if VUM is used; or vCloud Connector)
5) VMware Tools
6) Virtual hardware (optional; only needed if h/w upgrade provides features org needs)

SECTION V – Administer and Manage vSphere 6.x Resources

5.1 – Configure Advanced/Multilevel Resource Pools

a. Understand/Apply (Resource Pools)

1) Parent – top-level
2) Child – sub to a Parent
3) Sibling – in same level
4) Root – top most level for standalone Host or Cluster (not viewable in vCenter)

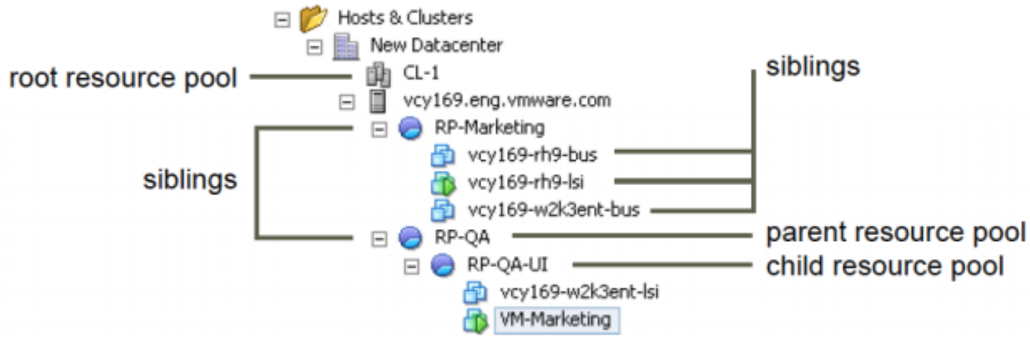


Figure 20, Resource Pool Hierarchy

b. Determine effect of Expandable Reservation parameter on resource allocatoin

1) Allows a child RP to ask its direct parent RP to borrow resources when the child runs out
2) Recursive – if direct parent has no available resources, the parent RP can ask its parent RP

c. Create a Resource Pool (RP) hierarchical structure

1) Inventory > rt-click a DRS-enabled Cluster or standalone Host > New Resource Pool
2) Enter info – Name, Shares/Limits/Reservation, Expandability
3) For a Sibling RP, repeat steps; for a child RP, rt-click newly created (parent) RP and create

d. Configure custom RP attributes

1) Rt-click a RP > Edit Resource Settings and change options as needed (Name, CPU, Memory)

e. Determine how RPs apply to vApps

1) vApps are containers like RPs; as such, vApps act like RPs as they also have resources allocated in the same manner as RPs (Shares/Limits/Reserv, Expandable Reserv, etc.)

f. Describe vFlash architecture

1) Read Cache; enables pooling of multiple local Flash-based devices into a single consumable vSphere construct called a Virtual Flash Resource (VFR)
2) VFR is consumed and managed in the same way CPU/memory are in vSphere; consumable by Virtual Host Swap Cache for vSphere Hypervisor and Virtual Flash Read Cache for VMs
3) Good candidates of vFlash – VDI, DB Warehouse, & read-intensive Web or Monitoring servers
4) Requires Ent+ 5.5+; max 16TB; max 8 SSDs per VFR; works with VMotion, HA, DRS; allows write-through (read cache) mode

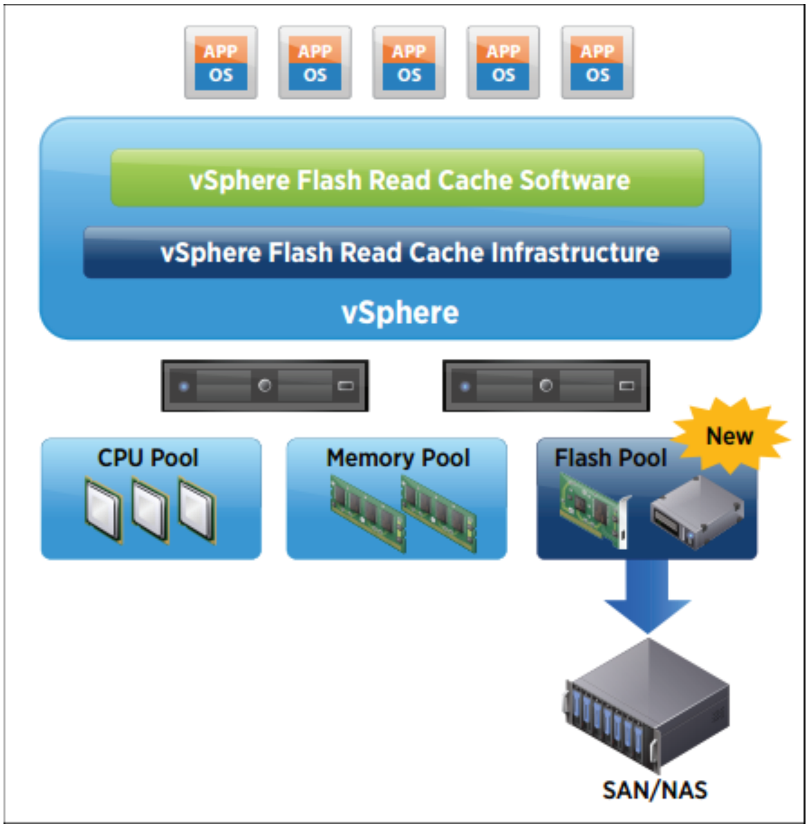

APP
OS
APP
OS
APP
OS
APP
OS
APP
OS
vSphere Flash Read Cache Software
vSphere Flash Read Cache Infrastructure
vSphere
CPU Pool
Memory Pool
Flash Pool
New
SAN/NAS

Figure 21, vFlash Architecture

g. Create/Remove a RP

1) See “c” above; to Remove, simply rt-click and Delete (remove any VMs in RP)

h. Add/Remove VMs from a RP

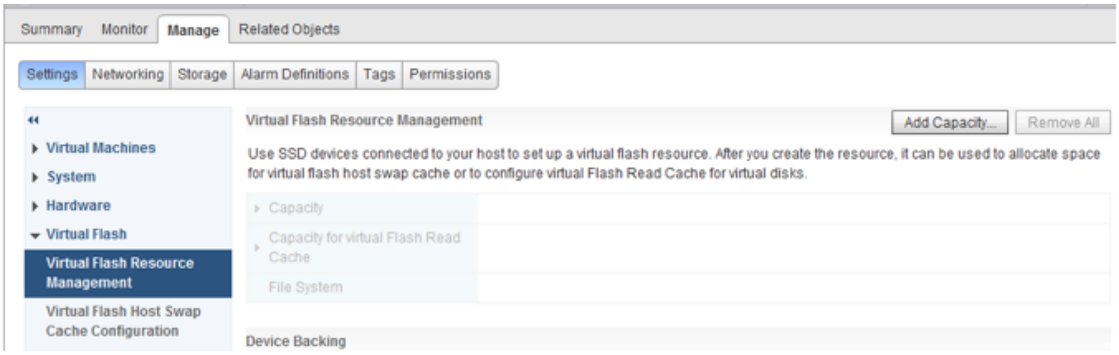
1) Add: rt-click VM(s) > Move To.. > expand Inventory until RP is shown, then click OK; drag/drop

2) Remove: same process as above

i. Create/Delete vFlash RP

1) Host > Manage tab > Settings tab > Virtual Flash Resource Management, ‘Add Capacity’ button

2) Select Virtual Flash Host Swap Cache Configuration, ‘Edit’ button



Virtual Flash Resource Management

Use SSD devices connected to your host to set up a virtual flash resource. After you create the resource, it can be used to allocate space for virtual flash host swap cache or to configure virtual Flash Read Cache for virtual disks.

Figure 22, Enable vFlash per Host

j. Assign vFlash resources to VMDKs

1) Rt-click VM > Edit Settings > VM Hardware, expand Hard Disk wanting to assign vFlash and configure amount (in GB by default) next to **Virtual Flash Read Cache**

k. Given a scenario, determine appropriate Shares, Reservations, Limits, for hierarchical RPs

1) This is usually a 'depends' situation
2) Know what each are → Limits = upper bound; Reservation = guaranteed/min; Share = allocation when contention (default CPU Share = 2000 [High], 1000 [Normal], 500 [Low])
3) To calculate & allocate Shares for objects:
   a) Total all Share amount for all VMs
   b) (High Share value x # of VMs with High value) / (Total Shares) = % of resource (CPU or RAM) needed to be allocated to high Share VMs; this % will then need to be divided by # of VMs with high Share value
   c) Repeat b) for medium (Normal) and low Share values
4) Understand how Shares and resources work in RPs with Expandable Reservation

SECTION VI – Backup & Recover a vSphere Deployment

6.1 – Configure and Administer a vSphere Backups/Restore/Replication Solution

a. Compare/contrast vSphere Replication (vR) compression methods

1) vRep utilizes FastLZ open source compression library, providing balance of speed, minimal CPU overheard, & compression efficiency
2) This bullet may refer to how compression is handled depending on source/target Host version:

SOURCE ESXi HOST	TARGET ESXi HOST	COMPRESSION SUPPORT
Pre-ESXi 6	Any vR supported version	No compression support
ESXi 6	Pre-ESXi6	Source compression/ vR appliance decompression
ESXi 6	ESXi 6	Source compression / target Host decompression

b. Differentiate VMware Data Protection (VDP) capabilities

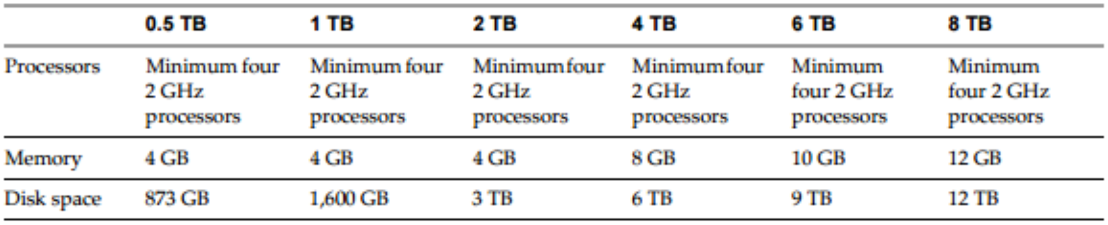
1) Virtual appliance
2) Web client managed (FlashPlayer 16+); IE 10.0.19, FF 34, Chrome 39 & Client Plug-in
3) Dedup capability; whole image or file level restore; uses VADP
4) vSphere Essentials Plus 5.0 (vCenter 5.5) and higher editions
5) No Phys/Indep Virt RDM or VVOL support
6) VM Hardware 7+ to support CBT

c. Configure recovery point objective (RPO) for a protected VM

1) This is self-explanatory; configure in vRep based on RPO req's for a VM
2) The key here is you can have only a max of 24 restore points, so config will be based on biz requirements coupled with max restore points allowed

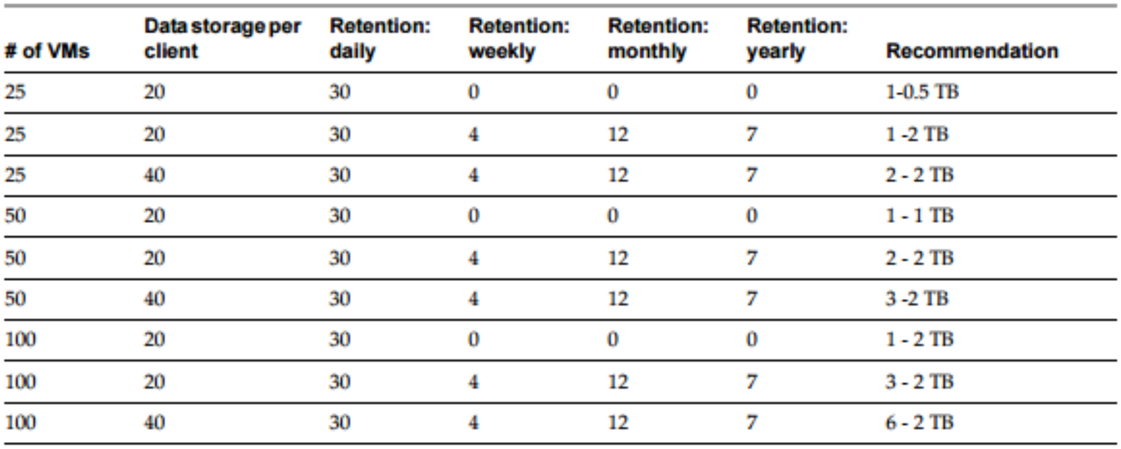
d. Explain VDP sizing guidelines

1) 400 VMs per VDP appliance (about 25 VMs per VDP capacity type)
2) 20 VDP appliances per vCenter
3) up to 8TB storage (.5TB, 1TB, 2TB, 4TB, 6TB, 8TB)



	0.5 TB	1 TB	2 TB	4 TB	6 TB	8 TB
Processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors
Memory	4 GB	4 GB	4 GB	8 GB	10 GB	12 GB
Disk space	873 GB	1,600 GB	3 TB	6 TB	9 TB	12 TB

Figure 23, VDP Capacity & Resources



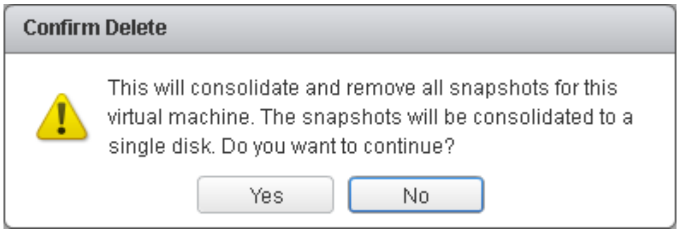
# of VMs	Data storage per client	Retention: daily	Retention: weekly	Retention: monthly	Retention: yearly	Recommendation
25	20	30	0	0	0	1-0.5 TB
25	20	30	4	12	7	1 -2 TB
25	40	30	4	12	7	2 - 2 TB
50	20	30	0	0	0	1 - 1 TB
50	20	30	4	12	7	2 - 2 TB
50	40	30	4	12	7	3 -2 TB
100	20	30	0	0	0	1 - 2 TB
100	20	30	4	12	7	3 - 2 TB
100	40	30	4	12	7	6 - 2 TB

Figure 24, VDP Sizing Guideline

4) Basically, **sizing** will depend upon Number & Type of VMs, amt of data, retention, & chg rate

e. Create/Delete/Consolidate VM snapshots

1) Create: rt-click VM > Snapshots > Take Snapshot..
2) Delete: rt-click VM > Snapshots Manage Snapshot > select snap & delete/delete all; doing so retains all data acquired since snap was taken & removes the snap



Confirm Delete

This will consolidate and remove all snapshots for this virtual machine. The snapshots will be consolidated to a single disk. Do you want to continue?

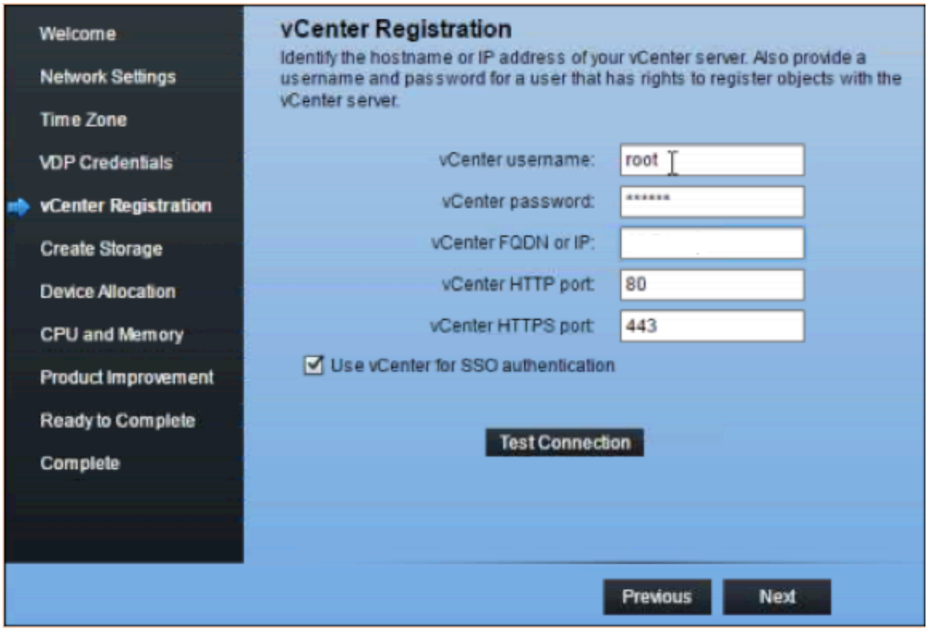
Figure 25, Delete Snapshot

3) Consolidate: rt-click VM > Snapshots > Consolidate

f. Install and configure VDP

1) Rt-click DC, Cluster, Host > Deploy OVF Template…

2) After deployment go to URL http://VDP-IP:8543/vdp-configure & login with root/changeme
3) Configure static IP settings, DNS, Hostname, Domain, Timezone, etc



vCenter Registration

Identify the hostname or IP address of your vCenter server. Also provide a username and password for a user that has rights to register objects with the vCenter server.

vCenter username: root
vCenter password: ******
vCenter FQDN or IP:
vCenter HTTP port: 80
vCenter HTTPS port: 443
☑ Use vCenter for SSO authentication

Figure 26, VDP Appliance Configuration

g. Create a backup job with VDP
1) Select vSphere Data Protection on left pane in Web Client > Backup tab > Backup Job Actions, then select New
2) Options:
a) Job Type = Guest Images (Applications is for Exchange, SQL, Sharepoint)
b) Data Type = Full Image (all disks) or Individual Disks
c) Backup Sources → select individual VM(s) or containers (DC, Cluster, Folder)
d) Select a Schedule (Next), then Retention Policy

h. Backup/Restore a VM with VDP
1) See g. above for Backup
2) From VDP Restore tab, select a VM > Restore icon and set restore options
a) Restore to orig location not allowed if VMDK not present… only 'new location' allowed

i. Install/Configure/Upgrade vRep
1) Virtual appliance OVF install & Web Client configuration via plug-in; vSphere Replication will be a Web Client Home left pane option; use the VAMI (https://vR-IP:5480) to register with SSO
2) First vR OVF is the vR Mgmt Server; additional vR OVFs are vR Servers (no mgmt)
3) 10 total OVFs can be deployed per vCenter (1 vR Mgmt & 9 vR Srvrs)
4) vRep network traffic can be isolated utilizing vmk for Replication service
5) Components that transmit replication data – vR agent & vSCSI filter; are built into vSphere
6) RPO range is 15mins to 24hrs on a per-VM basis; **NOTE: VSAN > VSAN replic RPO can be 5min**, and maximum restore points retained allowed is 24
7) Upgrade vRep Appliances by mounting an ISO; for vR 6 appliances, you can use the VAMI (https://vR-IP:5480)

j. Configure VMware Certificate Authority (VMCA) integration with vR

1) VAMI (https://vR-IP:5480) > vRep tab > Security > Configuration, select 'Accept only SSL certificates signed by a trusted Certificate Authority'
2) Save & Restart Service to apply changes

k. Configure vRep for single/multiple VMs

1) Browse to list of VMs in Web Client
2) Select **single** or **multiple** VMs > rt-click VM(s) > All vSphere Replication Actions > Configure Replication
3) Acknowledge VM number, select Target Site & Datastore, configure RPO & Quiesce, Finish

l. Recover a VM using vRep

1) Can only recover 1 VM at a time manually; SRM can be used for multiple-VM recovery; source VM must be powered off
2) From vR in Web Client > Incoming Replication tab, rt-click a VM > Recover
3) Two recovery options:
   a) Synchronize Recent Changes – source VM is off/accessible & vR replicates latest chgs to target before recovery; increased recovery time but ensures no data loss
   b) Use Latest Data Available – basically, no final sync before recovery; source VM not accessible
4) Select a folder & resource to recover the VM
5) Network must be manually configured, & choose whether to power on recovered VM or not
6) All restore points are recovered for VMs, so to revert to a specific RP, use Snapshot Manager to 'revert'

m. Perform a failback operation using vRep

1) Manual
2) After vR Recovery to a target, from that target site, configure a new replication in reverse back to the source site
3) The source VM must be unregistered from inventory before configuring reverse failover

n. Deploy a pair of vRep virtual appliances

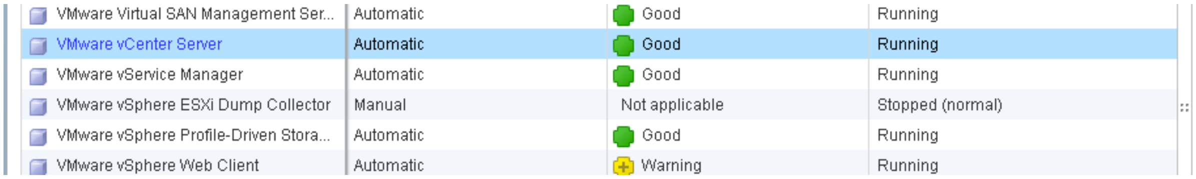
1) As noted above, the 1st vR appliance is the Mgmt server & subsequent ones are vR servers
2) All are OVFs so there's no difference in install
3) Configure 'sites' in the vRep plugin in the Web Client; review vRep Admin Guide for steps & privileges needed to do so

SECTION VII – Troubleshoot a vSphere Deployment

7.1 – Troubleshoot vCenter Server , ESXi, & VMs

a. Monitor status of vCenter service

1) From Web Client Home > Administration > System Configuration > Service, then select VMware vCenter Server from list and view Summary tab on right
2) Or, from System Configuration > Nodes > Related Objects tab



VMware Virtual SAN Management Ser...	Automatic	Good	Running
VMware vCenter Server	Automatic	Good	Running
VMware vService Manager	Automatic	Good	Running
VMware vSphere ESXi Dump Collector	Manual	Not applicable	Stopped (normal)
VMware vSphere Profile-Driven Stora...	Automatic	Good	Running
VMware vSphere Web Client	Automatic	Warning	Running

Figure 27, Monitor vCenter Server Service

b. Perform basic maintenance of vCenter Server database

1) If vCenter Server Service is stopped, could be issues with DB connectivity authentication
2) Check DB disk space usage; perform Log file Shrink operation (SQL) if needed

c. Monitor status of ESXi management agents

1) SSH into Host > **`/etc/init.d/hostd status`**
2) For the vCenter Server agent: **`/etc/init.d/vpxa status`**
3) Restart ESXi Management Agents from DCUI if needed (or replace **`status`** above with **`restart`**)

d. Determine ESXi Host stability issues & gather diagnostic information

1) Probably best way to determine Host stability is look at Events or Log Browser (Host > Monitor tab), Performance tab, and/or **`esxtop`** info
2) To gather logs, click on vCenter in Web Client > Monitor tab > System Logs tab, then Export System Logs button
3) Also, if Host doesn't meet h/w requirements, issues arise – 4GB RAM, 64bit, NX/XD enabled, Intel-VD/AMD-RVI enabled, Gb NICs

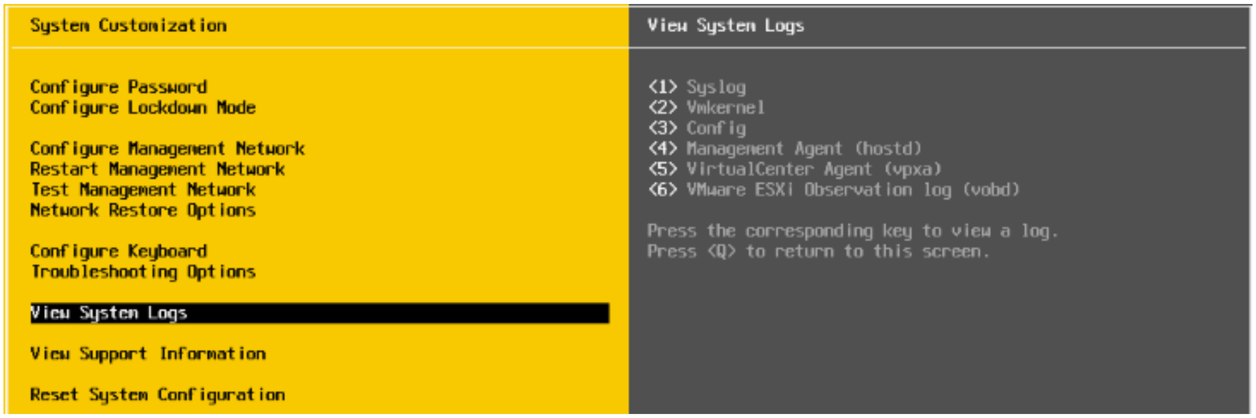
e. Monitor ESXi system health

1) From a Host > Monitor tab > Health Status tab
2) Check power consumption settings
   a) High – don't disable any power resources (increased host performance)
   b) Balanced – some power reduction without hindering performance
   c) Low – enable power savings settings with potential of hindering performance
   d) Custom

f. Locate & analyze vCenter Server & ESXi Logs

1) **Mgmt/vCenter Node** Logs are located in: **`/var/log/vmware/`** (VCSA) or **`C:\Program Data\VMware\vCenterServer\Logs`** (see KB: http://kb.vmware.com/kb/2110014)
   a) vpxd.log – main vCenter log
   b) vpxd-profiler.log – profile metrics for vCenter operations performed
   c) eam.log – ESX Agent Manager
   d) stats.log – performance charts
   e) vsphere-client.log – Web Client
   f) vws – system & h/w health manager
   g) Other **Mgmt Node** logs**:** vpostgres (DB log), workflow (workfl mgr), vapi, netdump, invsvc, vmware-sps (Profile driven storage), vmdird (Dir Svc Daemon)
   h) **PSC Node:** SSO (STS log), cis-license (Lic Svc), VMCA (Cert Svc), vmdir (Dir Svc)
2) **ESXi Logs** can be viewed in DCUI & are located in: **`/var/run/log`**
   a) hostd.log – hostd/management services
   b) vpxa.log – vCenter Server interaction

c) fdm.log – HA
d) syslog.log – default 'catch-all'
e) usb.log
f) hostprofiletrace.log
g) sdrsinjector.log – Storge DRS
h) vmkernel.log – VMkernel, device discovery, storage/network driver events, VM startup
i) DCUI logs – Syslog, VMkernel, Config, Mgmt Agent (hostd), vCenter (vpxa), Observation (vobd)



```
System Customization                          View System Logs

Configure Password                            <1> Syslog
Configure Lockdown Mode                       <2> Vmkernel
                                              <3> Config
Configure Management Network                  <4> Management Agent (hostd)
Restart Management Network                    <5> VirtualCenter Agent (vpxa)
Test Management Network                       <6> VMware ESXi Observation log (vobd)
Network Restore Options
                                              Press the corresponding key to view a log.
Configure Keyboard                            Press <Q> to return to this screen.
Troubleshooting Options

View System Logs

View Support Information

Reset System Configuration
```

Figure 28, View ESXi System Logs

g. Determine appropriate CLI command for a given troubleshooting task

1) Diverse topic; anywhere from esxcli cmds, to esxtop, to restarting agents; vimtop = VCSA esxtop
2) This KB references common VM tasks: http://kb.vmware.com/kb/2012964
3) What I recommend is SSH into a Host and just run esxcli, press ENTER, & view cmds; then, view what each sub-cmd does by only running 'get' and 'list' esxcli cmds; be familiar with what cmd displays what output

h. Troubleshoot common tasks

1) vCenter Server service – restart service; may be needed after Certs replaced
2) SSO – verify Identity Sources config (domain info/credentials); SSO user permissions; are services or firewalls disrupting communication (Windows version; port 7444)
3) vCenter Server connectivity – check vpxa.log on Hosts; valid permissions
4) VM resource contention, config, & operation – VM > Performance tab; check Shares/Res/Limits
5) PSC – see #2 (any issues with SSO, VMCA, & License)
6) Install problems – ESXi → along with install req's shared in d. above, is Host on HCL?..install on correct disk?... not having at least 4GB RAM fails install too; change BIOS boot to UEFI – "vmware boot bank" error; VMDirectory Service or DB errors?
7) VMware Tools install – either do a repair or uninstall/reinstall Tools
8) FT network latency – main cause here is either on latency saturated network or insufficient bandwidth on FT logging vmk; use a dedicated 10Gb NIC; also, Host resources could be low, so manual VMotion may be required (VM performance degragation noticed); or, if any VM is on a resource-constrained Host.. use VMotion to rectify and/or configure resource reservations
9) Review the scenarios in the Troubleshooting Guide for common issues in relation to each above item

7.2 – Troubleshoot vSphere Storage & Networking Issues

a. Identify & isolate network and storage resource contention & latency issues
   1) Network metrics to be aware of:
      a) %DRPTX/%DRPRX - % of transmitted or received packets dropped; threshold = **1**
      b) SPEED/UP/FDUPLX – self-explanatory; different config than switch port can cause issues
      c) MbTX/s (or MbRX/s) – Megabits transmitted (or received) per second
   2) Storage metrics to be aware of:
      a) DAVG – time in ms per cmd being sent to device (HBA); threshold = **15ms**
      b) KAVG – time in ms cmd spends in VMkernel; threshold = **4ms**
      c) GAVG – response time as perceived by guest (DAVG + KAVG); threshold = **20ms**
   3) To resolve SCSI Reservation issues: increase LUNs, reduce snapshots, update Host BIOS, less VMs on LUN

b. Monitor networking and storage resources using VROps alerts and all badges
   1) "Major" Badges, along with their subsequent "Minor" Badges
      a) **Health** → (score = 0[bad]-100[good]) Workload, Anomaly, Fault
      b) **Risk** → Time Remaining, Capacity Remaining, Stress
      c) **Efficiency** → (score = 0[bad]-100[good]) Reclaimable Waste (resources), Density (consolidation ratios)

c. Verify network and storage configuration
   1) Think this is self-explanatory. View info in appropriate areas – vDS, iSCSI configs, vmk configs, Jumbo Frames config'd end-to-end, IP settings, VLAN, etc. Just know where to look
   2) What is needed to configure FC? pg. 39, Storage Guide; to configure iSCSI? pg. 69, Storage Guide; to configure FCoE? pg. 45, Storage Guide; NFS? pg. 152, Storage Guide

d. Verify a given VM is configured with correct network resources
   1) Rt-click VM > Edit Settings > Virtual Hardware tab > expand Network Adapter #
   2) Look at connected PG/Network; is IP config'd; is vmnic connected; connect to diff vport

e. Monitor/Troubleshoot Storage Distributed Resource Scheduler (SDRS) issues
   1) SDRS disabled disk causes: VM is template, VM is FT enabled, VM config'd for bus sharing, manual SDRS config'd, VM has independent or hidden disks, disk is a CD ROM/ISOs
   2) Maint Mode failure: SDRS disabled on disk due to reasons above or affinity rules set/violation

f. Recognize impact of network & storage I/O control configurations
   1) Both can be based on config'd Shares, meaning nothing is impacted until there is contention
   2) If Reservations are set, then resources are already used for the object config'd and may affect sibling objects (proportionally)
   3) Know requirements – Ent+ license & at least vSphere 4.1 (SIOC) to Enable; is IOC enabled on vDS or DS (Perf chart won't show)

g. Recognize a connectivity issue caused by VLAN/PVLAN
   1) A VLAN isolates networks, so a few basic issues here could be mistyped VLAN # in the VMkernel adapter, no VLAN configured, or trunking not config'd on pSwitch port; review Section 2.1

h. Troubleshoot common issues with:

1) Storage & network – see items above
2) Virtual Switch and PG configuration – spelling match among Hosts (vSS); Security Policies similar
3) Physical network adapter configuration – not assigned to PG or dvPG; mis-config'd Load Balance (i.e. IP Hash > phys Link Ag); phys switch Trunking enabled; VLAN config; Security Pol's
4) VMFS metadata consistency (VMware On-Disk MetaData Analyzer [VOMA]) – via CLI & used for VMFS DSs only (`voma -m vmfs -d /vmfs/path/naa.###`)

7.3 – Troubleshoot vSphere Upgrades

a. Collect upgrade diagnostic information

1) Log directory may be displayed on screen, or simply in log location (see Section 7.1)

b. Recognize common upgrade issues with vCenter Server/VCSA

1) DB not configured properly (Windows install); pwd reset: `vpxd –P <pwd)`
2) DNS or NTP not configured properly
3) Compatibility (vSphere versions; min 5.x for Win & 5.1U3 for VCSA) and DB version
4) SSO – Identity Sources not configured properly; unable to speak with vCenter (Lookup Service).. firewall or port conflict issues, etc.
5) Sizing not compatible (tiny, small, etc.) with Host/VMs
6) As stated already above, review scenarios/examples in the Troubleshooting Guide for specific problem instances

c. Create/Locate/Analyze VMware log bundles

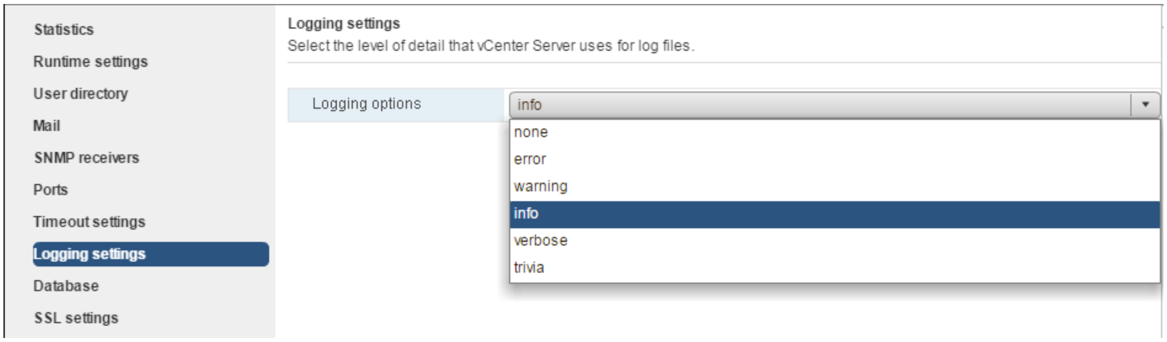
1) This was discussed in Section 7.1

d. Determine alternative methods to upgrade ESXi Hosts in event of failure

1) Methods to install – Interactive (directly on Host via USB/CD), scripted, Auto-Deploy, PXE-BOOT, Image Builder, VUM
2) Review the Install & Setup Guide for each setup method requirements

e. Configure vCenter Server Logging options

1) Select vCenter node in Web Client > Manage tab > Settings tab > General, then Edit Button



Logging settings

Select the level of detail that vCenter Server uses for log files.

Logging options: info

Figure 29, vCenter Logging Options Configuration

7.4 – Troubleshoot & Monitor vSphere Performance

a. Monitor CPU & memory usage including vROps badges and alerts

1) Badges were discussed briefly in Section 7.2
2) For metrics & their thresholds, see below (d.)

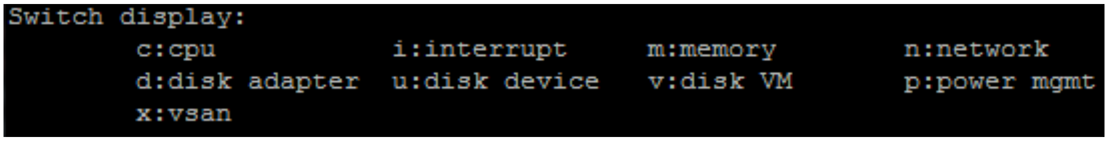
b. Identify & isolate CPU and memory contention issues
1) As mentioned with other resources, look at Host/VM Monitor tab > Performance tab and look at counters values to verify under threshold; or via `esxtop`

c. Recognize impact of using CPU/memory limits, reservations, & shares
1) Reservations – minimal amount of phys RAM reserved for VMs (guaranteed)
2) Limit – upper level (max)
3) Shares – amount of resources proportionally given **when under contention**

d. Describe and differentiate critical performance metrics
1) CPU
a) %USED – % phys CPU time used by worlds
b) %RDY – % time vCPU was ready to run but unable due to contention; threshold = **10%**
c) %CSTP – % time vCPUs in SMP VM stopped from executing; threshold = **3%**
d) %SYS – % time spent in VMkernel on behalf of world or RP; threshold = **20%**
2) Memory
a) MCTLSZ (Balloon size) – amt of guest phys memory reclaimed by balloon; threshold = **1**
b) SWCUR – amt of guest phys memory swapped out to VM swap file; threshold = **1**
c) SWR/s – rate which machine memory swapped in from disk; threshold = **1**
d) SWW/s – rate which machine memory swapped out from disk; threshold = **1**
3) Disk – covered in 7.2 above (DAVG, KAVG, GAVG)
a) VMDK Latency – (physcial read/write latency) threshold < **20ms**
4) Network – covered in Section 7.2

e. Describe and differentiate common metrics including:
1) Memory, CPU, Network, Disk – See d. above

f. Monitor performance through esxtop
1) SSH into a Host and type `esxtop`
2) View different resource views by typing letter corresponding to the resource



```
Switch display:
        c:cpu           i:interrupt     m:memory        n:network
        d:disk adapter  u:disk device   v:disk VM       p:power mgmt
        x:vsan
```

Figure 30, ESXTOP Resource Options List

g. Troubleshoot Enhanced vMotion Compatibility (EVC) issues
1) EVC is a Cluster setting allowing for VM vMotion between different CPU generations; CPUs must have same instruction set
2) Issues can be caused by:
a) Different CPU vendor-Hosts in Cluster
b) Verify CPU EVC compatible modes against VMware Compatibility Guide
c) If changing EVC mode (raise) VMs need to be powered off/on to get new CPU feature set
d) Are Hosts at least ESX/i 3.5U2

h. Troubleshoot VM performance with vROps

1) Same as previously discussed; guess I didn't mention what to do in vROps, but basically all that is needed is to view color-coded icons (orange/red = bad) & click on them to drill down to view the problem details

i. Compare/Contrast Overview & Advanced charts

1) Overview – displays several resource charts
2) Advanced – displays single resource chart & are configurable and exportable

7.5 – Troubleshoot HA & DRS Configurations and Fault Tolerance

a. Troubleshoot issues with:

1) DRS workload balancing – Host failure; vCenter off; affinity rules set; connected devices
2) HA failover/redundancy, capacity, & network config
   a) Cluster have resources based on Admission Control Policy – Host Failures Cluster Tolerates, Percentage of Cluster Resources Reserved as Failover Spare Capacity, Specify Failover Hosts
   b) Look for oversized VMs or failed Hosts
3) HA/DRS Cluster configuration
   a) Both require shared storage & proper licensing (Std for HA; Ent for DRS)
   b) DRS requires VMotion network – IP settings in same subnet; vmk naming match among Hosts
   c) VMware Tools installed for VM Monitoring
   d) Minimum of 2-Host Cluster
   e) HA config: uninitialized state, unreachable state, initialize error => reconfigure HA on Hosts and/or check if port 8182 is used; network partition => check VLANs, pNIC/pSwitch failure; for config timout set vCenter advanced setting to **240** (secs): **`config.vpxd.das.electionWaitTimeSec`**
   f) HA errors – unable to power on VMs, HA warnings, etc -> check VM reservations & migrate VMs to other Clusters that have high resources that distort slot size
   g) VM restart failure: verify HA enabled for the VM; sufficient Host resources for VM restart; VM file(s) inaccessible on VSAN during restart
4) vMotion/sVMotion configuration and migration
   a) Check vmk subnet, naming, IP, & service set; correct license; shared storage
   b) If VM migration with attached USB fails validation, re-add USB & enable it for VMotion, as well as make sure data isn't being transferred to USB at time of migration
5) FT configuration & failover issues – verify FT req's met -> thick disk; 2 vCPUs for Std/Ent & 4 for Ent+ ; FT & VMotion vmk's config'd; H/W Virt in Host BIOS on; features below are off for FT VM:
   a) VSAN, sVMotion, VMCP, VVOLs, SBPM, SIOC, pRDM, USB, & snapshots are not supported
   b) Latency -> VMotion secondary VM; verify dedicated 10Gb NIC; manually load balance (FT not supported by DRS); verify memory available on Host turning FT VM on (req'd = reserv + o/h)

b. Explain DRS Resource Distribution Graph & Target/Current Host Load Deviation

1) DRS Resource Distr Graph – displays memory & CPU metrics for each Host in a Cluster as % or size (MB/MHz), with each chart representing a VM on the Host
2) Target/Current Host Load Deviation – representation of balance of resources across all Hosts in DRS Clusters; runs every 5mins; <u>Target</u> = DRS value set, <u>Current</u> = Host calculation
   a) (VM Entitlements)/(Host Capacity) = Current Std Deviation; if Current Deviation is higher than Target Deviation, the Cluster is unbalanced & DRS recommneds VM migrations

c. Explain vMotion Resource Maps

1) A visual representation of Hosts, Datastores, & Networks associated with a VM and also indicate which Host are compatible VMotion targets

SECTION VIII – Deploy and Consolidate a vSphere Data Center

8.1 – Deploy ESXi Hosts Using Auto Deploy

a. Describe components & architecture of Auto Deploy environment

1) Auto Deploy server – serves images & host profiles to ESXi Hosts (part of vCenter)

2) Auto Deploy rules engine – send info to Auto Deploy server for which image/profile to serve which Host; maps software & config to Host based on the Host attributes

a) Rules – identifies target Hosts by root **MAC, SMBIOS, BIOS UUID, Vendor, Model, fixed DHCP IP** and assigns image profiles & host profiles to Hosts

b) Active Rule Set – has added Rules & applied to newly started Hosts

c) Working Rule Set – allows for Rule testing before making changes active

3) Image profile – defines set of VIBs to boot ESXi Hosts with

4) Host profiles – define machine-specific configs such as networking & storage setup

5) Host customization – stores info the user provides when host profiles are applied to a Host (IP info [previously called 'answer file'])

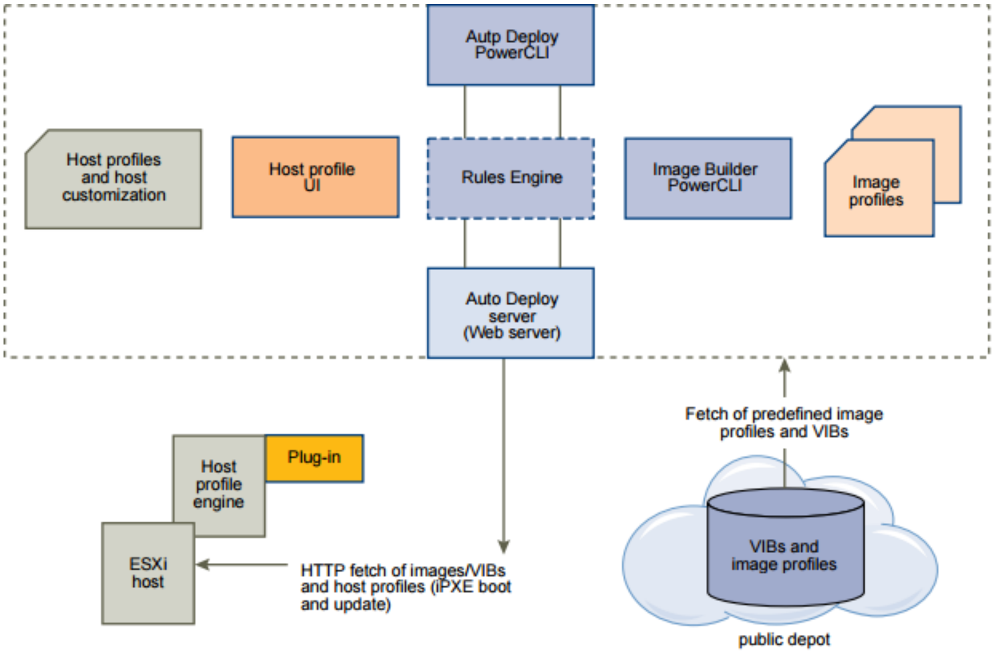

Autp Deploy PowerCLI
Host profiles and host customization
Host profile UI
Rules Engine
Image Builder PowerCLI
Image profiles
Auto Deploy server (Web server)
Fetch of predefined image profiles and VIBs
Host profile engine
Plug-in
ESXi host
HTTP fetch of images/VIBs and host profiles (iPXE boot and update)
VIBs and image profiles
public depot

Figure 31, Auto Deploy Architecture

b. Use Auto Deploy Image Builder & PowerCLI scripts

1) Image Builder is part of PowerCLI & used to create custom image profiles (see cmds below)

c. Implement Host Profiles with an Auto Deploy'd ESXi Host

1) Create a Host Profile from the 1st provisioned Auto Deploy'd Host

2) To implement with Auto Deploy, create a Rule with the Profile and 'activate' it (Active Rule Set)

d. Install & configure Auto Deploy

1) Auto Deploy is installed automatically with vCenter (mgmt node; not on PSC)
2) Change the Auto Deploy vCenter service startup type as needed & start it
3) Download the TFTP Boot Zip file from vCenter > Manage tab > Settings tab > Auto Deploy, download the **undionly.kpxe.vmw-hardwired** file & place on TFTP server
4) Configure DHCP to point to TFTP server (option 66; next-server) & file (option 67; boot-filename: **undionly.kpxe.vmw-hardwired**)
5) Set Hosts to PXE boot in BIOS
6) Write a PowerCLI Rule that assigns an image profile to Hosts
7) Write a PowerCLI Rule that assigns a host profile to Hosts (optional)
8) Write a PowerCLI Rule that assigns a Host to a vCenter location (Cluster, folder, [optional])

e. Understand PowerCLI cmdlets for Auto Deploy (see: https://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.install.doc/GUID-2D4D27BB-727F-4706-9DBE-49C41A108A8F.html)

1) **`New-DeployRule`** – cmdlet to write a rule that assigns an image profile & host profile to Hosts
2) **`Add-DeployRule`** – adds newly created Rule to Working and Active Set; use **`NoActivate`** parameter to only add to Working Set
3) **`Remove-DeployRule`** – use with **`-Delete`** parameter to completely remove Rule
4) **`Copy-DeployRule`** – basically recreates a previous Rule; used when updating image profile, and use **`-ReplaceItem`** parameter with it
5) **`Add-EsxSoftwareDepot`** – add the software depot containing image profiles
6) **`Get-EsxImageProfile`** – used to find desired image profile (**`standard`** has VMware Tools)
7) **`New-EsxImageProfile`** – used to create new Host image to install (use -**`cloneprofile`**)
8) **`Export-EsxImageProfile`** – preserve current profile for subsequent PowerCLI sessions
8) **`Test-DeployRuleSetCompliance`** – test new Rule against a Host without deploying it
9) **`Repair-DeployRuleSetCompliance`** – Remediate a Host to use new Rule set

f. Deploy multiple ESXi Hosts using Auto Deploy (Overview of process for First & Subsequent Boot)

1) First Boot:
   a) Host is powered on & starts a PXE boot process (configured in Host BIOS)
   b) DHCP server assigns an IP to the Host & instructs the Host to contact the TFTP server
   c) The Host contacts the TFTP server & downloads the iPXE file (boot loader) & iPXE config file
   d) The iPXE config file instructs the Host to make a HTTP boot request (which includes Host h/w and network info) to the Auto Deploy server
   e) Auto Deploy server queries rules engine for host information & streams components specified in the image profile, host profile, and vCenter location
   f) The Host boots with the image profile, & the host profile is applied (if one is provided)
   g) Auto Deploy adds the Host to vCenter registered with it and places the Host in a target folder or Cluster if specified by a Rule; if no Rule, will add to first DC displayed in Web Client UI
   h) If user imput is req'd, the Host is placed in Maint Mode; reapply host profile & update host customization to exit Main Mode; answer questions when prompted by host customization
   i) VMs may be migrated to Host if placed in DRS Cluster
   j) Each subsequent Host reboot, the Host gets reprovisioned by vCenter
2) Subsequent Boot:
   a) Host is powered on and Host gets reprovisioned by vCenter

g. Given a scenario, explain the Auto Deploy deployment model needed to meet a biz requirement
1) I think what this means is, based on # of Hosts to deploy, is Auto Deploy a viable solution to install vSphere. To deploy many Hosts, yes; for small & even medium environments, not really

8.2 – Customize Host Profile Settings

a. Edit answer file (Host customization) to customize ESXi Host settings
1) Place Host in Maint Mode
2) Attach the host profile that requires user input and provide different settings

b. Modify and apply a storage Path Select Plugin (PSP) to a device using Host Profiles
1) In Host Profile tree > Storage Configuration > Native Multi-Pathing (NMP) > PSP and SATP Configuration for NMP Devices > PSP Configuration For…
2) Enter the PSP name/value on the right, then Next > Finish
3) Apply profile to desired Host(s)

c. Modify and apply switch configurations across multiple Hosts using a Host Profile
1) In Host Profile tree > Network Configuration > vSwitch or vSphere Distributed Switch > make changes to sub-components as needed, then Next > Finish
2) Apply profile to desired Host(s)

d. Create/Edit/Remove a Host Profile from an ESXi Host
1) Create – Home > Monitor section > Host Profiles, then click green "+" to create a new profile
2) Edit – from same area as in 1. above, select a profile, click Actions > Edit Settings
3) Delete – from same area as in 1. above, select a profile, click Actions > Delete

e. Import/Export a Host Profile
1) Import – from Host Profiles section, select a profile & click icon
2) Export – from Host Profiles section, select a profile, click Actions > Export

f. Attach and apply a Host Profile to ESXi Hosts in a Cluster
1) Attach - from Host Profiles section, select a profile & click icon
2) Select the Host(s), Cluster(s), or DC(s) to attach the profile to
3) Click Attach button to move objects to the right pane
4) Enter additional customization if required, then Finish

g. Perform compliance scanning & remediation of ESXi Hosts and Clusters using Host Profiles
1) Compliance scan – from Host Profiles section, select a profile & click icon
2) Remediate – place Host in Maint Mode; from Host Profiles, select profile in left pane > Monitor tab > Compliance tab/button, then rt-click the Host(s) > Host Profile > Remediate; exit M Mode

h. Enable or disable Host Profile components
1) To enable items in Host Profiles, place a checkmark in the component box; to disable, remove the checkmark

8.3 – Consolidate Physical Workloads Using VMware Converter

a. Install vCenter Converter standalone instance
   1) Download .exe from VMware & install on Windows
   2) Be aware of software install requirements for Converter (a few 'main' ones below):
      a) Min. OS's – WinXP Pro SP3 & Win2K3 R2 SP2; RHEL 3.x; SUSE Ent 9.x; Ubuntu 10.04 LTS
      b) Thin/Thick disk types; Basic/Dynamic volumes; MBR & GPT partitions (no RAID or hybrid)
      c) IPv4 and IPv6 supported

b. Convert physical workloads using vCenter Converter
   1) Install Converter on device to be converted or a central Windows machine
   2) Open application & click Convert Machine button just below the File Menu; select Local (if currently on machine to be converted) or Remote to browse the network for the machine
   3) For machine destination, select VMware Infrastructure VM, and proivde the IP/Hostname of the ESXi Host or vCenter Server
   4) Name the VM
   5) Configure options: Data to Copy (typically all disks); disk controller; network settings; etc
   6) Choose optional settings: sysprep, install VMware Tools, startup mode, sync, or modify h/w

c. Modify server resources during conversion
   1) In the conversion wizard, you have ability to modify resources & storage

d. Interpret & correct errors during conversion
   1) Failure at 2% (hangs) is typical of a communication error, typical of Windows Firewall
   2) VM fails to boot – check disk controller (in converter wizard, change any IDE to SCSI)
   3) Logs: C:\ProgramData\Application Data\VMware\VMware Converter Enterprise\Logs

e. Deploy a physical host as a VM using vCenter Converter
   1) See as b. above

f. Collect diagnostic information during convesion operation
   1) Log location is in d. above
   2) Or, you can export logs via Task Menu > Export Logs…

g. Resize partitions during conversion process
   1) Self-explanatory; during conversion wizard, resize disks → maintain size, min size (copies only used space), type size in GB or MB (custom size); a hot-clone process chg'ing from block to file

h. Given a scenario, determine which virtual disk format to use
   1) I think this is referring to Thick or Thin; the larger the disk/volume, it's best to use Thin

SECTION IX – Configure and Administer vSphere Availability Solutions

9.1 – Configure Advanced vSphere HA Features

a. Modify vSphere HA advanced Cluster settings
   1) I don't think this is what some may think… i.e. Advanced OPTIONS (i.e. parameters), but rather

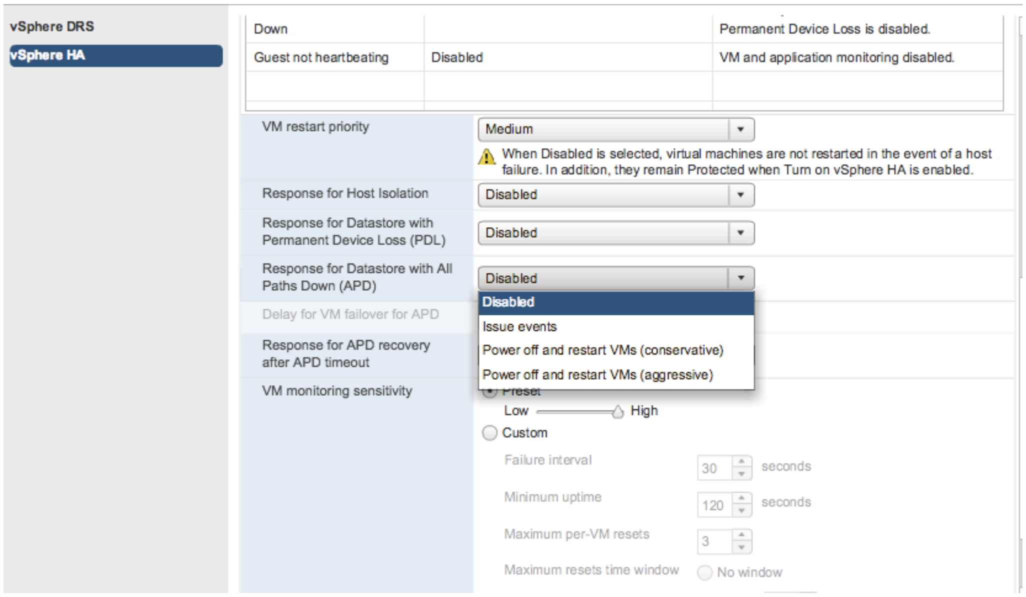
just settings that are a bit deeper than 'normal' HA settings; I'll share a few what I believe are Advanced below:

a) VM Restart Priority – although this is what I consider a 'basic' setting, a more advanced setting would be to set individual VM(s) Restart Priority in the Cluster > Manage tab > Settings tab > VM Overrides section

b) VM (& App) Monitoring – restarting a VM if VMware Tools heartbeats are no longer received

c) VM Component Protection (VMCP) – protects VMs against 'split-brain' situation when a Host is isolated or partitioned & master can't communicate with failed Host's datastore heartbeats

1. If Host Monitoring or VM Restart Priority is 'Disabled', VMCP won't perform restarts
2. Protects VMs against datastore accessibility failures (PDL or APD)



vSphere DRS
vSphere HA

Down		Permanent Device Loss is disabled.
Guest not heartbeating	Disabled	VM and application monitoring disabled.

VM restart priority: Medium
When Disabled is selected, virtual machines are not restarted in the event of a host failure. In addition, they remain Protected when Turn on vSphere HA is enabled.

Response for Host Isolation: Disabled

Response for Datastore with Permanent Device Loss (PDL): Disabled

Response for Datastore with All Paths Down (APD): Disabled

Disabled
Issue events
Power off and restart VMs (conservative)
Power off and restart VMs (aggressive)

Delay for VM failover for APD

Response for APD recovery after APD timeout

VM monitoring sensitivity: ● Preset

○ Custom

Failure interval: 30 seconds

Minimum uptime: 120 seconds

Maximum per-VM resets: 3

Maximum resets time window: ○ No window

Figure 32, Advanced HA Settings (VMCP)

d) Application Monitoring – requires obtaining SDK to set up app heartbeating

b. Configure a network for use with HA heartbeats

1) 3 Host Failure Types

a) Failure – Host doesn't respond to ICMP & doesn't send network/datastore heartbeats

b) Isolated – mgmt network heartbeat not seen by master, but datastore heartbeats are; can't ping gateway isolation address

c) Partitioned – a subset of Hosts unable to communicate via mgmt network; DS heartbeats are seen

2) HA uses the management network for agent heartbeating, or VSAN ntwk when used with VSAN

3) Both mgmt & VSAN networks require a vmk to be created & appropriate service (mgmt or VSAN) selected

4) When performing network maintenance in HA Clusters, disable Host Monitoring, make network change, rt-click Host(s) > reconfigure HA, then turn Host Monitoring back on

c. Apply an Admission Control Policy (ACP) for HA

1) Host Failures Cluster Tolerates – calculates 'slot size' for CPU (reservation or 32MHz) & Mem (largest config'd value + overhead); determines max # of slots per Host based on <u>max of either</u> CPU or Mem; 'current failover capacity' of cluster determined by taking out Host with largest

slot, add remaining Cluster Host slots, and if slots >= # of total Cluster VMs, you're set

2) Percentage of Cluster Resources Reserved – based on CPU & Mem reservation (or 32MHz/0MB +overhead, if none); failover capacity is calculated by [(Total Host CPU-VM CPU req)/Total Host CPU], then doing same for Mem; set a % (e.g. 25%) and subtract this from the capacity calc to determine how much Cluster resources are available for addt'l VMs (non Host-failed VMs.. i.e. prod); **NOTE:** if you set 25%, but need 30% to cover all VMs, some VMs may not get restarted
3) Specify Failover Hosts – self-explanatory; a Host in a Cluster is not used for prod, but is instead completely 'set aside' to be used for VMs to be restarted on in the event of a Host failure; VM-VM affinitiy rules will not apply with this policy
4) Deciding which Policy to use – resource fragmentation → when a VM needs more than 1 'slot' or Host to satisfy its resource req's. The only Policy that addresses this is Failover Hosts; Cluster heterogeneity → Percentage and Failover address this..Tolerates is too conservative a approach

d. Enable/Disable advanced vSphere HA settings (see: http://kb.vmware.com/kb/2033250)

1) HA Settings (Edit button) > Advanced options, and Add button; some commond parameters:
2) **`das.isolationaddressX`** – sets the IP address to ping if a host is isolated from the network
3) **`das.iostatsinterval`** – I/O stats interval for VM Monitoring (default = 120 secs)
4) **`das.slotcpuinmhz`** – (or **`slotmeminmb`**) defines CPU slot size maximum
5) **`das.ignoreRedundantNetWarning`** – set to ignore 'no HA network redundancy' warning
6) **`das.usedefaultisolationaddress`** – use Default Gateway as the isolation address or not
7) **`das.heartbeatDsPerHost`** – configure if wanting more than default of 2
8) **`das.ignoreInsufficientHbDatastore`** – if, for example, not enough DS's for the 2 min

e. Configure different heartbeat datastores for an HA Cluster

1) Usually it's best to have HA determine datastores automatically, determined by maximum # of Cluster Hosts having access to a heartbeating datastore; **NOTE:** VSAN not supported
2) Default # selected is 2 (value can be chg'd with **`das.heartbeatdsperhost`** & max value is 5)
3) Cluster > Manage tab > Settings tab > vSphere HA, Edit button then expand 'Datastore for Heartbeating' and select appropriate option (Auto, Only From List, or List & Complement Auto)

f. Apply VM monitoring for a Cluster

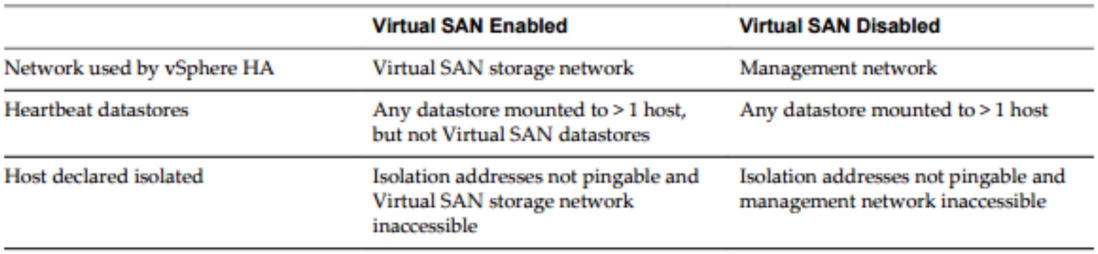
1) Cluster > Manage tab > Settings tab > vSphere HA, Edit button then select VM Monitoring Only from drop-down in 'Virtual Machine Monitoring' section
2) Requires VMware Tools to be installed

g. Configure VM Component Protection (VMCP) settings

1) Cluster > Manage tab > Settings tab > vSphere HA, Edit button then expand 'Failure Conditions…' section and choose from Response for Datastore with PDL and APD drop-downs
2) Not supported with FT VMs, or VMs on VSAN or VVols, or RDMs; supports only vSphere 6
3) Understand PDL and APD settings/responses (reference Fig. 32 above)

h. Implement vSphere HA on a VSAN Cluster

1) Requirements – minimum of 3 Host Cluster and vSphere 5.5
2) Network traffic uses VSAN network, not management (used only if VSAN is disabled)
3) VSAN datastores cannot be used for HA datastore heartbeating



	Virtual SAN Enabled	Virtual SAN Disabled
Network used by vSphere HA	Virtual SAN storage network	Management network
Heartbeat datastores	Any datastore mounted to > 1 host, but not Virtual SAN datastores	Any datastore mounted to > 1 host
Host declared isolated	Isolation addresses not pingable and Virtual SAN storage network inaccessible	Isolation addresses not pingable and management network inaccessible

Figure 33, HA Networking Differences

4) To implement/enable simply configure Cluster settings & turn HA on

i. Explain how HA communicates with DRS and DPM

1) DRS – DRS load-balances VMs after HA performs VM restarts (Host failover); DRS affinity rules can be set to be enforced, or enforced if possible ("must" or "should" settings); VMs may not auto-VMotion off a Host being placed in Main Mode due to resources reserved for failure
2) DPM – if enabled & HA admission control disabled, VMs may not failover

9.2 – Configure Advanced DRS Features

a. Configure VM-Host affinity/anti-affinity rules

1) Affinity – selected VMs must run on selected Hosts
2) Anti-Affinity – selected VMs cannot run on selected Hosts
3) To create this rule, a Host Group & VM Group must 1st be created (Cluster > Manage tab > Settings tab, select VM/Host Groups and add a Host Group (with Hosts) & VM Group (with VMs)
4) Cluster > Manage tab > Settings tab, select VM/Host Rules, and in the 'Type' drop-down select Virtual Machine to Hosts; finalize remaining bottom options (groups assigned & must/should)

b. Configure VM-VM affinity/anti-affinity rules

1) Affinity – selected VMs must be on the same Host
2) Anti-Affinity – selected VMs cannot run on the same Host
3) No groups needed; just go to Cluster > Manage tab > Settings tab, select VM/Host Rules, and in the 'Type' drop-down select "Keep Virtual Machines Together" (affinity) or "Separate…" (anti)

c. Add/Remove Host DRS Group

1) already covered in a. above

d. Add/Remove VM DRS Group

1) already covered in a. above

e. Enable/Disable DRS affinity rules

1) After you create a Rule, there is a check box in the Rule settings to Enable; either check (Enable) or uncheck (Disable) this box

f. Configure proper DRS automation level based on business requirements

1) Manual – vCenter suggests migration recommendation but admin must manually perform task
2) Partially Automated – VMs auto-placed on Hosts at power-on; vCenter suggests recommendation afterward
3) Fully Automated – VMs auto-placed on Hosts at power-on & auto-migrated afterward

a) Fully auto has 5 levels (1-5) to set; 1 is Highest priority & means would make most difference in Cluster balance, while 5 is lowest & migration would make little difference

g. Explain how DRS affinity rules effect VM placement
1) Discussed in a. & b. above

SECTION X – Administer and Manage vSphere Virtual Machines

10.1 – Configure Advanced vSphere Virtual Machine (VM) Settings

a. Determine how using a shared USB device impacts the environment
1) USB devices attached to a ESXi Host can be "passed through" to VMs such that the VM has direct access to the device; not supported with DPM & FT
2) To configure pass through of Host-attached USB devices to a VM:
a) VM > Edit Settings > Virtual Hardware tab > New Device, then select USB Controller; **NOTE:** USB 2.0 is for Windows OS's and 3.0 is currently only for Linux OS's
b) Add another device > Host USB Device, then select from the drop-down the Host-attached device wanting to add to the VM; enable VMotion support as well
3) If the VM with an attached USB is migrated & powered down, the VM will need to be migrated back to the Host with the USB device attached & re-added before turning the VM back on (best to configure an DRS Affinity Rule)

b. Configure VMs for vGPUs, DirectPath I/O & SR-IOV
1) vGPU – install graphics card in Host(s); install VIB on the ESXi Host(s), as well as graphics driver in Guest OS; power down the VM > Edit Settings > Virtual Hardware tab > Add New Shared PCI Device, select the PCI device to add from drop-down
2) DirectPath I/O – having direct access to a PCI device; power down a VM > Edit Settings > Add a PCI Device in the Virtual Hardware tab
a) Features not available with DirectPath I/O – VMotion, suspend/resume, snapshots
3) SR-IOV – for ESXi5.5+ ; representation of a VF on a pNIC with SR-IOV such that the VM & pNIC exchange data without VMkernel as an intermediary where latency may cause failure
a) Host > Manage tab > Networking tab, select Physical Adapters > Edit Adapter icon (pencil) and select Enabled from Status drop-down
b) Edit a VM > Virtual Hardware & add a Network device; expand the new section and from Adapter Type drop-down choose SR-IOV passthrough

c. Configure VMs for multicore vCPUs
1) Rt-click VM > Edit Settings > Virtual Hardware, expand CPU and select Cores from drop-down; **NOTE:** VM must be powered off to change Cores, even if Hot Add enabled
2) If vCPU Hot Plug is enabled, vNUMA support is disabled and instead VM uses UMA with interleaved memory access (see: http://kb.vmware.com/kb/2040375)

d. Differentiate VM configuration settings
1) Virtual Hardware, Guest OS, vCPU, Virtual Memory, Swap location, Hot Add, Bus Sharing, HDs
2) Note the security configurations from Section 1

e. Interpret VM configuration file (.vmx) settings

1) The settings in the .vmx file are basically the same items you have configured for the VM; below are some sample entries, most are obvious what they are/do:

```
virtualHW.version = "11"
floppy0.present = "true"
scsi0.present = "true"
scsi0.sharedBus = "none"
sched.cpu.units = "mhz"
sched.cpu.shares = "normal"
ethernet0.present = "true”
ethernet0.virtualDev = "vmxnet3”
guestOS = "windows7srv-64"
```

f. Enable/Disable advanced VM settings
   1) Power off VM, rt-click > Edit Settings > VM Options tab, expand Advanced section and click Edit Configuration button
   2) Click to Add a row with a parameter and its associated value; typically, a “1” value enables and “0” disables; review security options discussed in Section 1

10.2 – Create & Manage a Multi-Site Content Library

a. Publish a content catalog
   1) Content Libraries are containers for VM & vApp Templates or other files (i.e. ISOs, txt, etc.)
   2) Requirements
      a) Can be shared across vCenter Server instances, but all vC’s must be in same SSO domain
      b) Users in other vCenter SSO domains cannot subscribe to the Library
      c) Although only a single file (i.e. OVF) is shown in the Web Client, multiple files are actually loaded; each type of file (e.g. VM/vApp Template) are library items
   3) Two Library types:
      a) Local Library – used to store items in a single vCenter instance where created (not Published)
      b) Subscribed Library – create a Subscribed Library to subscribe to a Published Library
   4) Publish a content catalog:
      a) Create a Local Library (see h. below) & check the ‘Publish content library externally’ box
      b) Optionally enable authentication by checking the ‘Enable authentication’ box

b. Subscribe to a published catalog
   1) Create a Subscribed Library (see h. below) & select ‘Subscribed Content Library’ option
   2) Enter the Subscription URL & choose the download option (immediately or when needed)

c. Determine which privileges are required to globally manage a content catalog
   1) This depends on business requirements for a given Content Library admin, power user, or user
   2) Note that CL’s are not hierarchical from vCenter, but rather from the global root
   3) When privileges are decided upon (list of are under the Content Library area when creating a Role); create a Role with the desired CL priv’s
   4) Add a user or group to the Role at the global level
   5) Because of the heirarchy ‘issue’, if someone has appropriate privileges at the vCenter level, to be able to manage CLs, they need at least Read-Only global permission

d. Compare the functionality of Automatic Sync & On-Demand Sync

1) On-Demand/Manual Sync downloads only metadata of the Published Library subscribed to

2) Automatic Sync downloads full copies of all Published Library items locally

e. Configure Content Library to work across sites

1) This is nothing more than Publishing a configured/created Library; just select the Library in the list > Action Items > Edit Settings and check the box ‘Publish This Library Externally’

2) Optional – enabled authentication by checking the box & adding a password

f. Configure Content Library authentication

1) See e. above

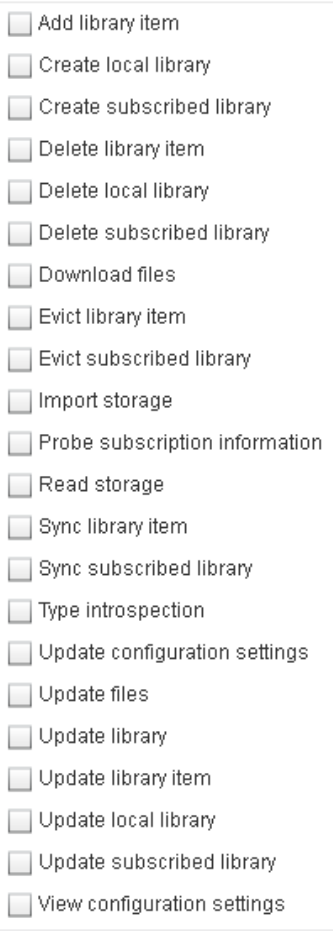
g. Set/Configure Content Library roles

1) Content Libraries are not ‘children’ of the vCenter they are created, but rather the Global root

2) Log in vCenter SSO > Administration > Global Permissions > Add icon (“+”); Add button to add a user, then assign ‘Content Library Administrator (sample)’ Role from drop-down

3) Or, create a custom role from Administration > Roles, and assign privileges from the Content Library “tree”; assign user to custom role as described in ‘2)’ above

4) There are 22 items you can select when configuring a custom Content Library role:

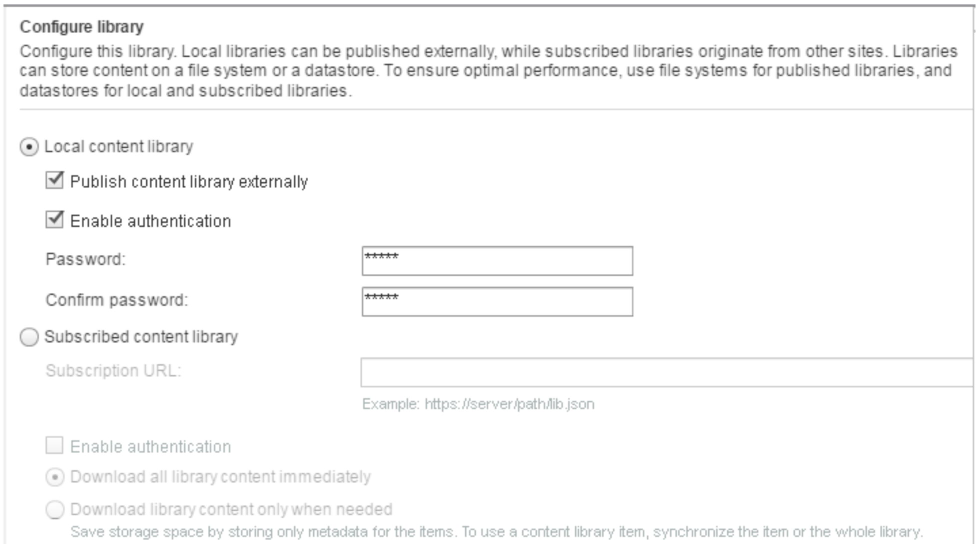


□ Add library item
□ Create local library
□ Create subscribed library
□ Delete library item
□ Delete local library
□ Delete subscribed library
□ Download files
□ Evict library item
□ Evict subscribed library
□ Import storage
□ Probe subscription information
□ Read storage
□ Sync library item
□ Sync subscribed library
□ Type introspection
□ Update configuration settings
□ Update files
□ Update library
□ Update library item
□ Update local library
□ Update subscribed library
□ View configuration settings

Figure 34, Content Library Privilege Options

h. Add/Remove Content Libraries

1) Create: Home > Inventories > Content Libraries > Create a New Library icon
2) Configure Library items – Name, Local or Subscribed, and Storage (File Sys or Datastore)



Configure library

Configure this library. Local libraries can be published externally, while subscribed libraries originate from other sites. Libraries can store content on a file system or a datastore. To ensure optimal performance, use file systems for published libraries, and datastores for local and subscribed libraries.

● Local content library

☑ Publish content library externally

☑ Enable authentication

Password: *****

Confirm password: *****

○ Subscribed content library

Subscription URL:

Example: https://server/path/lib.json

□ Enable authentication

● Download all library content immediately

○ Download library content only when needed

Save storage space by storing only metadata for the items. To use a content library item, synchronize the item or the whole library.

Figure 35, Create Content Library

3) To Remove a Library, select it in the Inventory > Content Libraries list > click Actions > Delete

10.3 – Configure & Maintain a vCloud Air Connection

a. Create a VPN connection between vCloud Air & an on-premise site (http://vcloud.vmware.com/using-vcloud-air/tutorials/creating-an-ipsec-vpn)

1) Created using the vCloud Director > Edge Gateways tab, rt-click the Gateway listed > Gateway Services
2) Firewall tab to verify required ports are open (50, 51, 500, 4500)
3) VPN tab > Add button and enter appropriate info; **NOTE:** local here means vCloud Air site
4) From on-premise vCD > Edge Gateways tab, rt-click Gateway > Gateway services & repeat 3.

b. Deploy a VM using vCloud Air (http://vcloud.vmware.com/using-vcloud-air/tutorials/deploying-a-virtual-machine-from-a-catalog)

1) From vCD in vCAir > select a VDC, and in Dashboard click Virtual Machines tab > Add One

c. Migrate a VM using vCloud Air

1) From vCC (open with C# > Home > Solutions & Applications > vCC) > Cloud tab & add both local vCenter/vSphere "Cloud" & remote Cloud (vCloud Air)
2) Select Virtual Machines tab > Actions > Copy and follow wizard; **NOTE:** Virtual H/W 11 currently not supported on vCloud Air

d. Verify VPN connection configuration to vCloud Air

1) From the VPN tab in Edge Gateway Services (see a. above), there should be a green checkmark

e. Configure vCenter Server connection to vCloud Air

1) Do so using vCloud Connector (vCC); some vCC requirements:
   a) vSphere 4U3
   b) IE 8-11 or Chrome 22/23
   c) Ports 80, 443, 5480, 8190
2) Install vCC Server OVF via C# client; **NOTE:** vCC UI not supported with Web Client
3) Install vCC Node OVF
4) Go to Node UI (https://IPorFQDN:5480) and configure
   a) Register Node with vCenter: Node tab > Cloud tab > Cloud Type and enter 'vSphere'; then enter vCenter https URL (IP or FQDN)
   b) Configure Proxy if needed
   c) Configure other settings as needed (Name, NTP, Time Zone, admin pwd, etc)
5) Go to Server UI (https://IPorFQDN:5480) & configure
   a) Register vCC Node(s) with vCC Server: Nodes tab > Register Node, & provide Node info/URL
   b) Enter "Cloud" info, which is local vSphere (just Cloud Type of 'vSphere' then user/pwd)
   c) Click Register, then repeat for additional vCC Nodes if needed
   d) Register vCloud Air vCC Node – same as above but when registering, select 'Public' (don't select Public for on-premise Node registering)
   e) Enter vCloud Air "Cloud" info & for Type enter 'vCloud Director'
   f) Register vCC Server with vSphere C# Client: Server tab > vSphere Client tab and add info
   g) Configure other settings as needed (ntp, DHCP, etc)

f. Configure replicated objects in vCloud Air Disaster Recovery service (http://vcloud.vmware.com/using-vcloud-air/tutorials/disaster-recovery-configuring-virtual-machine-replication)
1) Install vSphere Replication (vR)
2) Add vCloud Air site to vR: Manage tab, select Cloud Connection icon & enter vCAir info
3) Web Client > rt-click a VM > All vSphere Replication Actions > Configure Replication
4) Enter info in Replication wizard: 'Replicate to a Cloud Provider' (target site, VDC, etc)
5) Select vApp & RPO settings, then Finish the wizard
6) Repeat for other VMs as needed

g. Given a scenario, determine the required settings for VMs deployed in vCloud Air
1) Self-explanatory I think; based of biz requirements, configure VM settings needed when deploying to vCloud Air (network, cpu, memory, etc)

CONFIG MAXIMUMS – General Maximums (not inclusive; review actual Guide for full max's)

VMs

vCPUs – 128; RAM – 4TB; VMDK – 62TB
SCSI Controllers – 4
   Targets per Controller – 15 (60 total SCSI devices)
AHCI (SATA) Controllers – 4
   Targets per Controller – 30 (120 total SATA devices)
vNICs – 10
Floppy, USB Controller, IDE – 1
Concurrent Console connections – 40

HOST

CPUs – 480
RAM – 6TB
VMs – 1024
Total VM vCPUs – 4096
FT – 4 VMs; 4 vCPU; 16 VMDKs; 64GB RAM
VMDKs – 2048
iSCSI/FC/NFS LUNs & VMFS Volumes – 256
  HBAs/FCoE Adapters – 4
  pNICs associated with Software iSCSI – 8
File Size/Virtual RDM – 62TB
Physical RDM & LUN/Volume Size – 64TB
VMDirectPath PCI Limit – 8
NICs – 24 (e1000 1Gb); 16 (bnx2 1Gb); 8 for most 10Gb; 4 for 40Gb
vSS or vDS ports – 4096; 4088 creation ports; Active ports – 1016

CLUSTER

Hosts – 64
VMs – 8000 (VMs per Host in a Cluster is same as above: 1024)
Resource Pools per Host & Cluster – 1600 with a depth of 8

VCENTER

Hosts – 1000
Powered-on VMs – 10000 (Registered VMs – 15000)
Linked VCs – 10
  Hosts in Linked VCs – 4000
  Powered on VMs in Linked VCs – 30000 (Registered VMs – 50000)
Concurrent vSphere Client Connections – 100
Concurrent Web Client Connections – 180
Hosts per DC – 500
Concurrent vMotions: 1Gb – 4; 10Gb – 8
Concurrent svMotions: Host – 2; Datastore – 8
Appliance – Hosts: 1000; VMs: 15000

VUM

VMware Tools & Hardware Scans/Host – 90
VMware Tools & HW Upgrades/Host – 24
Host Scans/VUM Server – 75
Host Remediation & Upgrades/VUM Server – 71 (NOTE: 1 Host Upgrade per Cluster)

vSPHERE FLASH READ CACHE

Flash Resource per Host – 1; Virtual disk size – 16TB; Host swap cache – 4TB
Flash devices per Flash Resource - 8
Maximum cache per virtual disk – 400GB
Cumulative cached per Host – 2TB

Created by Shane Williford July 2016. If you reference this Study Guide, please give credit to the author