Tips 8
Section 1 - Create and Deploy vSphere 6.x Infrastructure Components 12
Objective 1.1 - Perform Advanced ESXi Host Configuration 12
Configure and Manage Auto Deploy configurations 12
Determine use case for Stateless vs Stateful installs 13
Create / Modify rules and rule sets 14
Create and associate Host Profiles for an Auto Deploy reference host 14
Configure Kernel Boot Parameters for scripted install according to a deployment plan: 15
Modify scripted weasel install (ks.cfg) 15
Create / Modify scripted installation 15
Configure Advanced System Settings according to a deployment plan: 15
Edit System Swap / Scratch Configuration 15
Configure ESXi host to use a central Syslog Server 16
Manage/Edit the Core Dump configuration of an ESXi host 19
Objective 1.2 - Deploy and Configure Core Management Infrastructure Components 22
Deploy vCenter core components according to a deployment plan: 22
Deploy and Configure a Platform Services Controller (PSC): 22
Determine use case for embedded vs external PSC 24
Re-point a vCenter Server Appliance to another External PSC 24
Deploy and Configure Identity Sources for Single Sign-On: 25
Configure Single Sign-On users and groups 25
Change Default domain for Single Sign-On 26
List services registered with Single Sign-on 26
Deploy and configure vCenter Server 27
Deploy / Configure Enhanced Link Mode 31
Manage / Configure vCenter components according to a deployment plan: 32
Configure Global Permissions for vCenter services 32
Configure Dump Collector service 32
Configure the Syslog Collector / Syslog service 33
Managing vCenter Server advanced configurations 34
Objective 1.3 - Deploy and Configure Update Manager Components 35
Deploy / Configure Update Manager components according to a deployment plan: 35
Configure VUM Update Manager download service 35

Configure a VUM shared repository 36
Configure VUM smart rebooting 37
Manually download updates to a VUM repository 38
Create and modify VUM baseline groups 39
Perform VUM orchestrated vSphere upgrades 39
Troubleshoot Update Manager problem areas and issues 40
Utilize Update Manager to reconfigure VUM settings 40
Objective 1.4 - Perform Advanced Virtual Machine Configurations 40
Tune Virtual Machine disk controller configurations according to a deployment plan ... 40
Configure .vmx file for advanced configuration scenarios 40
Configure a virtual machine for Hot Add features 41
Upgrade virtual machine hardware and VMware Tools 41
Troubleshoot virtual machine deployment issues 42
Section 2 - Deploy and Manage a vSphere 6.x Storage Infrastructure 43
Objective 2.1 - Implement Complex Storage Solutions 43
Determine use cases for Raw Device Mapping 43
Apply storage presentation characteristics according to a deployment plan: 43
VMFS re-signaturing 43
LUN masking using PSA-related commands 44
Create / Configure multiple VMkernels for use with iSCSI port binding 44
Configure / Manage vSphere Flash Read Cache 45
Create / Configure Datastore Clusters 46
Upgrade VMware storage infrastructure 46
Deploy virtual volumes 46
Deploy and configure VMware Virtual SAN 50
Configure / View VMFS locking mechanisms 52
ATS-Only mechanism 52
ATS_SCSI mechanism 52
Configure Storage I/O Control to allow I/O prioritization 53
Configure Storage Multi-pathing according to a deployment plan 54
Objective 2.2 - Manage Complex Storage Solutions 55
Identify and tag (mark) SSD and local devices 55
Administer hardware acceleration for VAAI 56

Configure, administer, and apply storage policies 56
Prepare storage for maintenance 57
Apply space utilization data to manage storage resources 57
Provision and manage storage resources according to Virtual Machine requirements 57
Configure datastore alarms, including Virtual SAN alarms 58
Expand (Scale up / Scale Out) Virtual SAN hosts and diskgroups 58
Objective 2.3 - Troubleshoot Complex Storage Solutions 58
Analyze and resolve storage multi-pathing and failover issues 58
Troubleshoot storage device connectivity 59
Analyze and resolve Virtual SAN configuration issues 59
Troubleshoot iSCSI connectivity issues 59
Analyze and resolve NFS issues 60
Troubleshoot RDM issues 60
Section 3 - Deploy and Manage a vSphere 6.x Network Infrastructure 61
Objective 3.1 - Implement and Manage vSphere Standard Switch (vSS) Networks 61
Create and manage vSS components according to a deployment plan: 61
VMkernel ports on standard switches 61
Advanced vSS settings 61
Configure TCP/IP stack on a host 61
Create a custom TCP/IP stack 62
Configure and analyze vSS settings using command line tools 62
Objective 3.2 - Implement and Manage vSphere 6.x Distributed Switch (vDS) Networks 63
Deploy a LAG and migrate to LACP 63
Migrate a vSS network to a hybrid or full vDS solution 65
Analyze vDS settings using command line tools 65
Configure Advanced vDS settings (NetFlow, QOS, etc.) 66
Determine which appropriate discovery protocol to use for specific hardware vendors 68
Configure VLANs/PVLANs according to a deployment plan 69
Create / Apply traffic marking and filtering rules 69
Objective 3.3 - Scale a vSphere 6.x Network Implementation 70
Configure appropriate NIC teaming failover type and related physical network settings 70
Determine and apply failover settings according to a deployment plan 70
Configure and manage network I/O control 3 70

Determine and configure vDS port binding settings according a deployment plan 71
Objective 3.4 - Troubleshoot a vSphere 6.x Network Implementation 71
Perform a vDS Health Check for teaming, MTU, mismatches, etc. 72
Configure port groups to properly isolate network traffic 73
Use command line tools to troubleshoot and identify configuration issues 73
Use command line tools to troubleshoot and identify VLAN configurations 74
Use DCUI network tool to correct network connectivity issue 74
Section 4 - Configure a vSphere Deployment for Availability and Scalability 75
Objective 4.1 - Implement and Maintain Complex vSphere Availability Solutions 75
Configure a HA cluster to meet resource and availability requirements 75
Configure custom isolation response settings 76
Configure VM Component Protection (VMCP) 76
Configure HA redundancy settings: 77
Management network 77
Datastore heartbeat 77
Network partitions 77
Configure HA related alarms and analyze a HA cluster 78
Configure VMware Fault Tolerance for single and multi-vCPU virtual machines 78
Objective 4.2 - Implement and Manage Complex DRS solutions 79
Configure DPM, including appropriate DPM threshold 79
Configure / Modify EVC mode on an existing DRS cluster 80
Create DRS and DPM alarms 82
Configure applicable power management settings for ESXi hosts 82
Configure DRS cluster for efficient/optimal load distribution 85
Properly apply virtual machine automation levels based upon application requirements 86
Administer DRS / Storage DRS 86
Create DRS / Storage DRS affinity and anti-affinity rules 86
Configure advanced DRS / Storage DRS settings 87
Configure and Manage vMotion / Storage vMotion 88
Create and manage advanced resource pool configurations 89
Objective 4.3 - Troubleshoot vSphere clusters 89
Analyze and resolve DRS/HA faults 89

Troubleshoot DRS/HA configuration issues 90
Troubleshoot Virtual SAN/HA interoperability 91
Resolve vMotion and storage vMotion issues 91
Troubleshoot VMware Fault Tolerance 91
Section 5 - Configure a vSphere Deployment for Manageability 93
Objective 5.1 - Execute VMware Cmdlets and Customize Scripts Using PowerCLI 93
Install and configure vSphere PowerCLI 93
Use basic and advanced PowerCLI Cmdlets to manage a vSphere deployment 93
Analyze a sample script, then modify the script to perform a given action 95
Use PowerCLI to configure and administer Auto Deploy (including Image Builder) 95
Create a report from a PowerCLI script 96
Objective 5.2 - Implement and Maintain Host Profiles 96
Use Profile Editor to edit and / or disable policies 96
Create and apply host profiles 97
Use Host Profiles to deploy vDS 98
Use Host Profiles to deploy vStorage policies 99
Import / Export Host Profiles 99
Manage Answer Files 101
Configure stateful caching and installation for host deployment 102
Objective 5.3 - Manage and analyze vSphere log files 102
Generate vSphere log bundles 102
Configure and test centralized logging 103
Analyze log entries to obtain configuration information 103
Analyze log entries to identify and resolve issues 104
Configure logging levels for vSphere 104
Objective 5.4 - Configure and manage Content Library 106
Create a Global User 107
Create a Content Library 107
Subscribe to a Content Library 109
Configure a Content Library for space efficiency 110
Synchronize a subscribed Content Library 110
Section 6 - Configure a vSphere Deployment for Performance 111
Objective 6.1 - Utilize Advanced vSphere Performance Monitoring Tools 111

Configure esxtop / resxtop custom profiles 111
Evaluate use cases for and apply esxtop / resxtop Interactive, Batch and Replay modes 111
Use vScsiStats to gather storage performance data 112
Use esxtop / resxtop to collect performance data 113
Given esxtop / resxtop output, identify relative performance data for capacity planning purposes 114
Objective 6.2 - Optimize Virtual Machine resources 115
Adjust Virtual Machine properties according to a deployment plan: 115
Network configurations 115
CPU configurations 115
Storage configurations 116
Troubleshoot Virtual Machine performance issues based on application workload: 116
Modify Transparent Page Sharing and large memory page settings 116
Optimize a Virtual Machine for latency sensitive workloads 118
Configure Flash Read Cache reservations 119
Section 7 - Configure a vSphere 6.x Environment for Recoverability 120
Objective 7.1- Deploy and manage vSphere Replication 120
Configure and manage a vSphere Replication infrastructure: 120
Isolate vSphere Replication network traffic 120
Enable data compression of vSphere Replication traffic 120
Configure and manage vSphere Replication of virtual machines 121
Analyze and resolve vSphere Replication issues: 121
Storage configuration 121
Multiple point in time snapshots 121
Enabling vSphere Replication on VMs 121
Objective 7.2 - Deploy and Manage vSphere Data Protection 122
Create, edit and clone a vSphere Data Protection backup job 122
Modify a preconfigured backup job. 122
Backup and restore a Virtual Machine (file level restore, full VM backup) 122
Create a replication job according to a deployment plan 122
Configure a Backup Verification job to ensure integrity of restore points 122
Objective 7.3 - Backup and Recover vSphere Configurations 123

Backup and restore distributed switch configurations....123
Backup and restore resource pool configurations....124
Export Virtual Machines to OVA/OVF format....125
Use a Host profile to recover an ESXi host configuration....125
Section 8 - Configure a vSphere 6.x Environment for Security....126
Objective 8.1 - Manage authentication and end-user security....126
Add/Edit Remove users on an ESXi host....126
Configure vCenter Roles and Permissions according to a deployment plan....126
Configure and manage Active Directory integration....126
Analyze logs for security-related messages....128
Enable and configure an ESXI Pass Phrase....128
Disable the Managed Object Browser (MOB) to reduce attack surface....129
Objective 8.2 - Manage SSL certificates....129
Configure and manage VMware Certificate Authority....130
Configure and manage VMware Endpoint Certificate Store....130
Enable / Disable certificate checking....130
Generate ESXi host certificates....131
Replace default certificate with CA-signed certificate....131
Configure SSL timeouts according to a deployment plan....131
Objective 8.3 - Harden a vSphere 6.x Deployment....132
Enable and configure ESXi Lockdown mode (Strict / Normal)....132
Configure a user on the Lockdown Mode Exception Users list....132
Customize SSH settings for increased security....132
Enable strong passwords and configure password policies....133
Configure vSphere hardening of virtual machines according to a deployment plan....134

Tips

Review the VCAP6-DCV Deployment Exam details at:
https://mylearn.vmware.com/mgrReg/plan.cfm?plan=88753&ui=www_cert

Review the details on the VMware Certification Platform Interface – UI Guide
https://mylearn.vmware.com/lcms/web/portals/certification/VMware%20Certification%20Platform%20Interface.pdf

VCP6-DCV Official Cert Guide (VMware Press) – VMware Press does not yet have an official guide for the VCAP6-DCV Deploy Exam, but you can make could use of your VCP6-DCV Official Cert Guide. The coverage of the VCP6-DCV and VCAP6-DCV exams are very similar, but one exam is multiple choice and one is hands-on. This VCAP6-DCV Deploy Study Guide makes many references to specific items in the *VCP6-DCV Official Cert Guide*.
http://www.pearsonitcertification.com/store/vcp6-dcv-official-cert-guide-covering-exam-2vo-621-9780789756480

If you are preparing for VCP6-DCV, you should consider begin efficient by beginning your VCAP6-DCV Deploy exam preparation while preparing for VCP6-DCV. As you prepare for specific VCP6-DCV exam objectives, you can practice the corresponding VCAP6-DCV Deploy exam tasks hands-on. This will reinforce your skills and knowledge of the topic and better prepare you for the VCP6-DCV exam. It will shorten the amount of time you require to prepare for VCAP6-DCV Deploy exam after passing the VCP6-DCV exam.

VMware Hands on Labs: As an alternative to building your own lab environment, where many vSphere features such as vSAN and vVOLs may be difficult to implement, consider using the VMware Hands on Labs (HOL). For most of your preparation, you can use HOL-1710-2 or HOL-1721-SDC-6 (or any HOL in which vSphere 6.0 is deployed). In this case, just ignore the actual lab materials and just use the environment as you wish to practice your work. If you make a mistake, you know that you can end the lab and restart it again with a fresh environment. For major items in which you need a lot of work, consider using the associated HOL, such as:

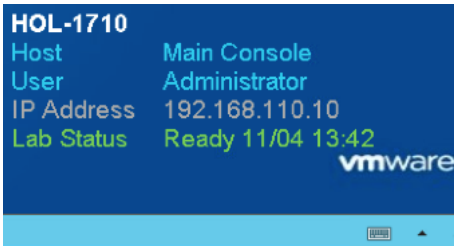
- VMware Virtual SAN: HOL-1708-SDC-1 – Virtual SAN 6.2 from A to Z
- Virtual Volumes: HOL-1708-SDC-2 Virtual Volumes and Storage Policy Based Management

Manage your time!!!
You will be given 27 tasks, each with multiple steps, and 190 minutes to complete. That is approximately 7 minutes per task.

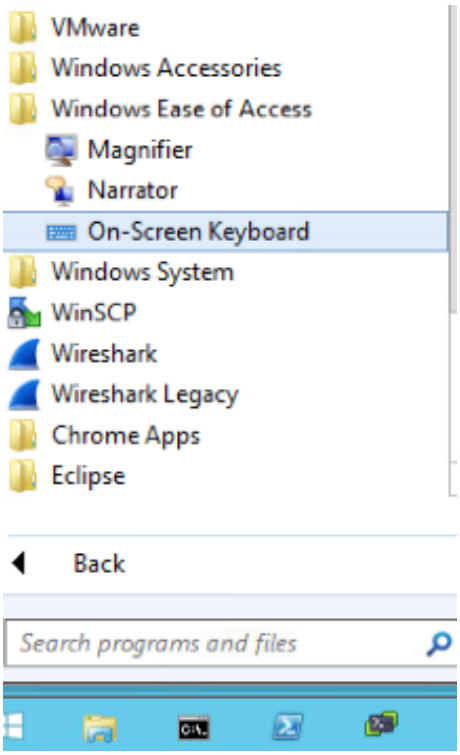
- Only a few tasks are dependent on another task. Consider reviewing the first question. If you are confident you can complete it in 4 or 5 minutes, then perform the task.

Otherwise make a note (on the provided scratch sheet) of the task number with just a single word or two to remind you what the task is. Then move on to the next task.

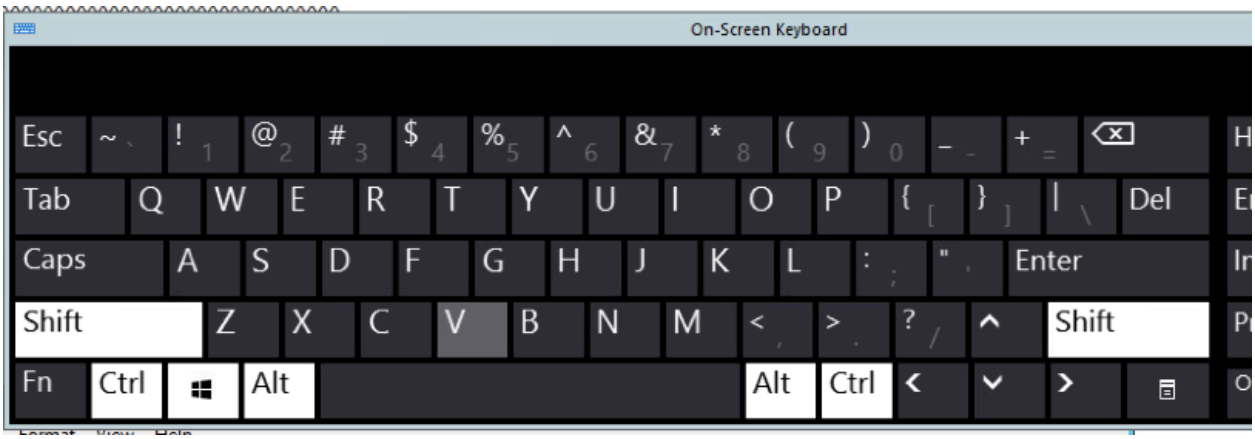
- You may not have sufficient time to complete all tasks. Although some tasks may be scored higher than others, you could assume that if you correctly and *completely* perform 22 of the 27 tasks, you will likely pass.
- Read the *VMware Certification Platform Interface – UI Guide* completely and practice its advice in Hands On Labs. For example, practice using left and right arrow keys plus the delete key when correcting typing mistakes, since the Backspace key will not work
- Also, practice using the Microsoft keyboard to perform copy / paste. Which is NOT the same keyboard that you may see in Hands on Labs in the lower right corner of the screen



You should use the keyboard at **Programs** > **Windows Ease of Access** > **On-Screen Keyboard**



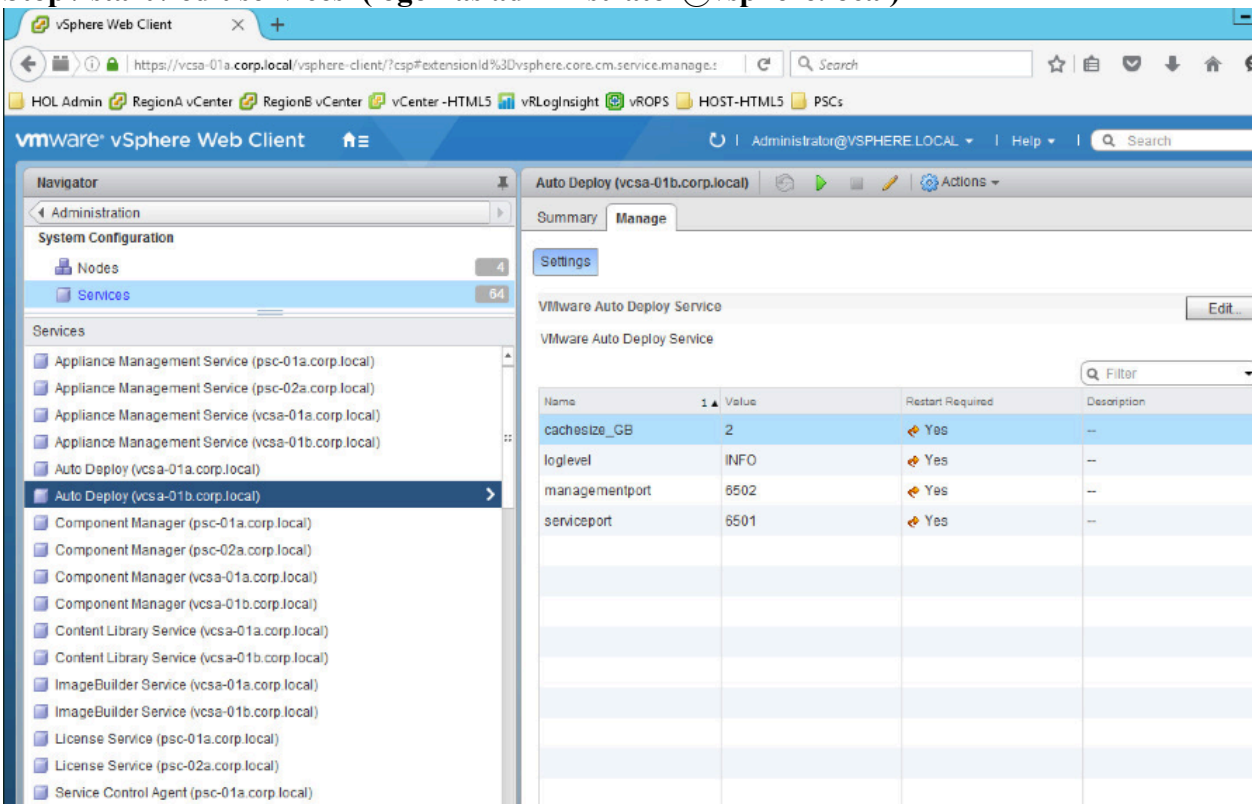
For example to copy use Control-C and to paste use Control-V



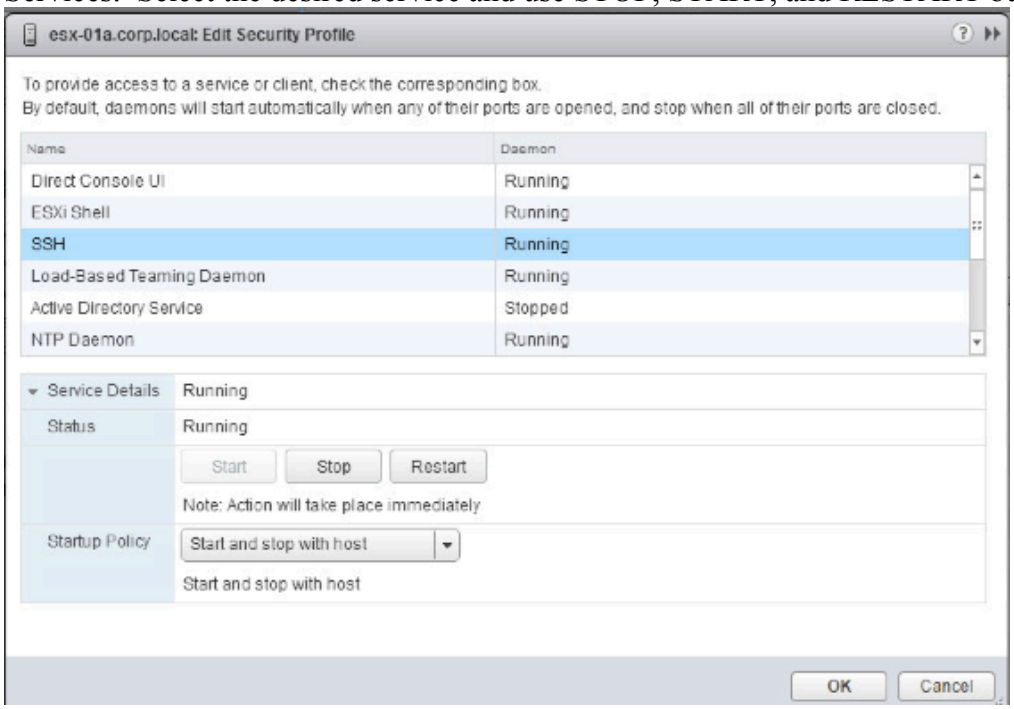
Search for a file in linux:
In case you need to search for a file in ESXi or vCenter Appliance
Find / -name "rbd-ca*"

TROUBLESHOOTING TIPS:
In case you need to start and stop services when troubleshooting

Stop / start / edit services (logon as administrator@vsphere.local)



Restart management services on ESXi host:
REF http://bit.ly/2bcNR4B
OR
In vSphere Web Client, select the host, click **Manage** > **Settings** > **Security Profile** and Edit the Services. Select the desired service and use STOP, START, and RESTART buttons



More Advice from Dave Davis at VirtualizeStuff.com
http://www.virtualizestuff.com/2016/08/02/vcap6-exam-interface-tips-tricks/?utm_campaign=VMUG+Voice&utm_source=hs_email&utm_medium=email&utm_content=34594412&_hsenc=p2ANqtz-9eSJdP2LN146d76nb5PLHmvY9EU4ApTbO7BJ7ni76GH0qQiwgmnc3xpckghgvLZtUTbBuEubfRMBOKdc-b3PfZvEuFRw&_hsmi=34594412

ON THE DAY OF THE EXAM:

- Take *2 forms* of photo ID!!!!
- Arrive at least 15 minutes early to be processed
- Be ready to move quickly through the exam.

Section 1 - Create and Deploy vSphere 6.x Infrastructure Components

Objective 1.1 - Perform Advanced ESXi Host Configuration

Configure and Manage Auto Deploy configurations

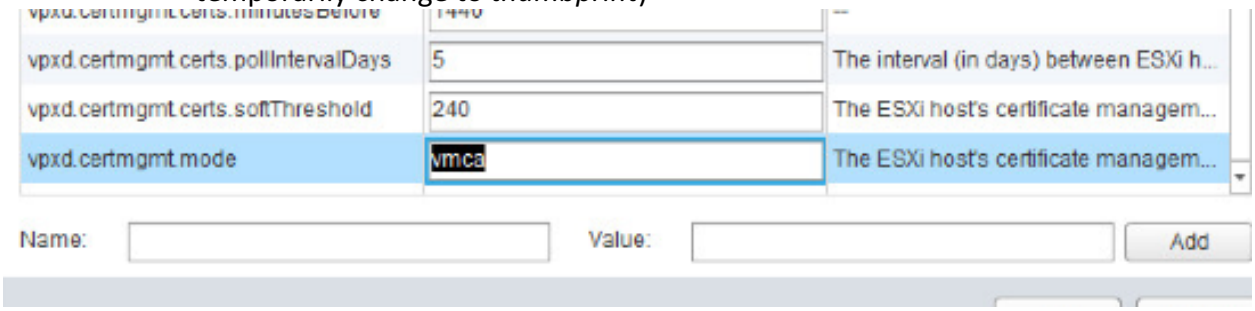
REF: *VCP6-DCV Cert Guide:* page 532

Use custom certs (CA) with Auto Deploy:
Some key steps are:

- Request a cert from CA that meets requirements
  - Key size at least 2048 bit. PEM format
  - X509 version 3
  - `SubjectAltName` contains DNS Name=<machine_FQDN>
  - Contains key usages: digital signature, non repudiation, key encipherment
- Name the cert `rbd-ca.crt` and key `rbd-ca.key`
- Stop Auto Deploy service
- Copy the files to `/etc/vmware-rdb/ssl`
- Use **vecs-cli entry** delete and **vecs-cli entry create** to update the TRUSTED_ROOTS store to use new certs.

```
        help
vecs-cli failed. Error 87: Operation failed with error ERROR_INVALID_PARAMETER (87)
root@vcsa-01b [ /usr/lib/vmware-vmafd/bin ]# ./vecs-cli entry delete --store TRUSTED_ROOTS
--alias rbd_cert
Warning: This operation will delete entry [rbd_cert] from store [TRUSTED_ROOTS]
Do you wish to continue? Y/N [N]
```

- Create the `castore.pem` file that contains the contents of TRUSTED_ROOTS
- Change the vCenter Certificate Mode:
  - Change the vCenter Server's Advanced Setting **vpxd.certmgmt.mode** from *vmca* to *custom* to manage your own certs. (for troubleshooting / failback, you could temporarily change to *thumbprint*)



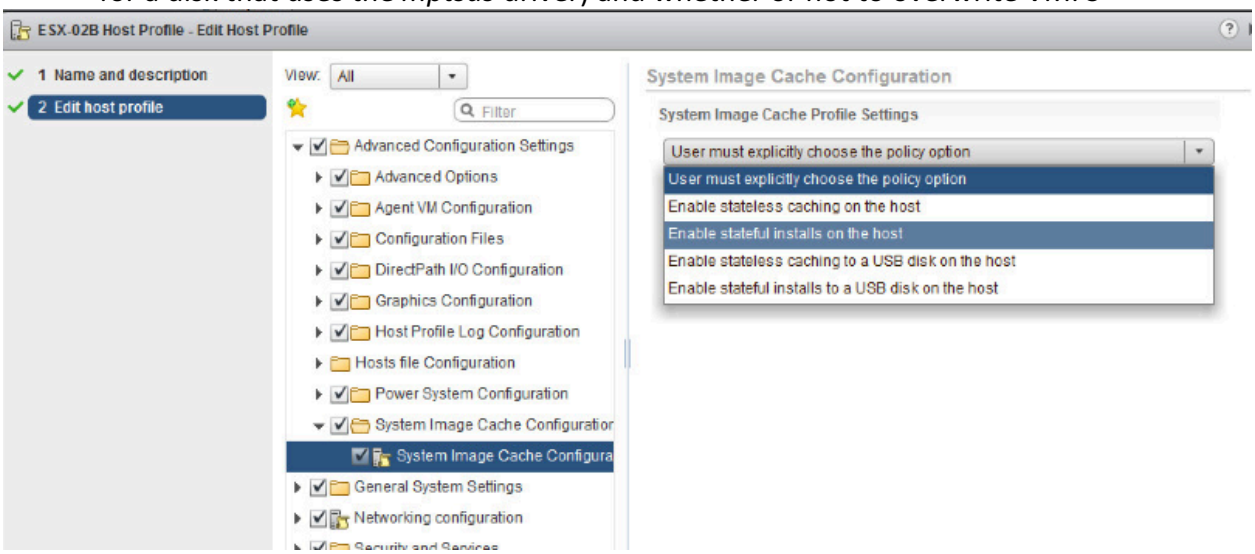
- Restart the vCenter Service and Auto Deploy service

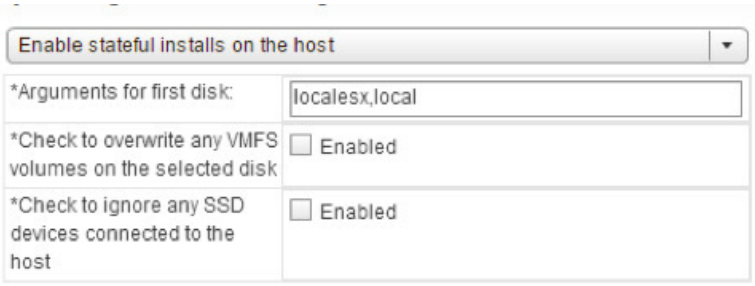
REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-24065DD3-5730-4F3D-BBF9-AE5FADA50EA5.html

Determine use case for Stateless vs Stateful installs

Enable Stateful Install:

- Prep host for auto deploy (REF: http://bit.ly/2fzx4eK)
- In the host profile, set **Advanced Configuration Settings** > **System Image Cache Configuration** > **System Image Cache Configuration** = `Enable Stateful installs on the host` (or `Enable stateful installs to a USB disk on the host`) and set **Arguments for first disk** (such as `ST3120814A,mptsas,local` .. to first look for a disk namEd *ST3122081*, then look for a disk that uses the *mptsas* driver) and whether or not to overwrite VMFS

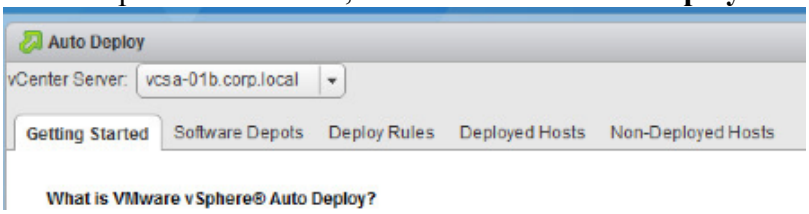


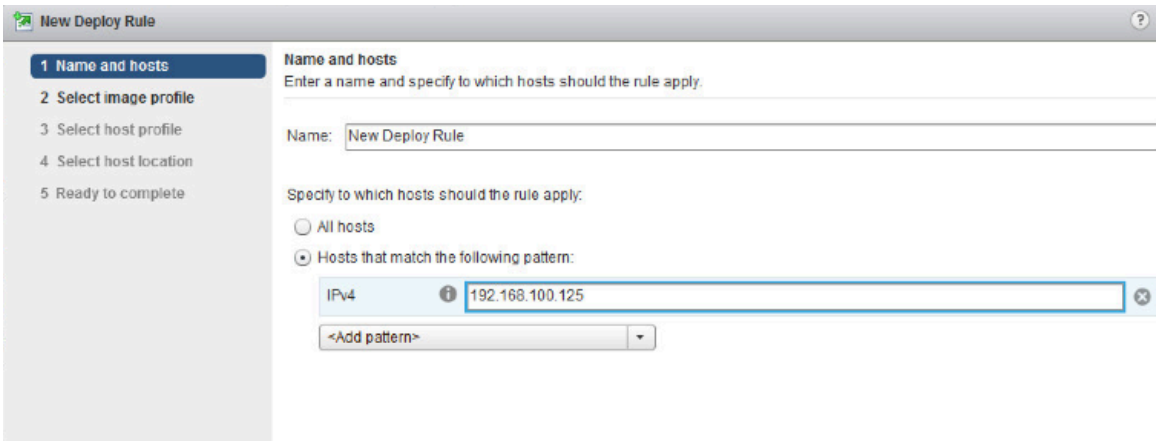


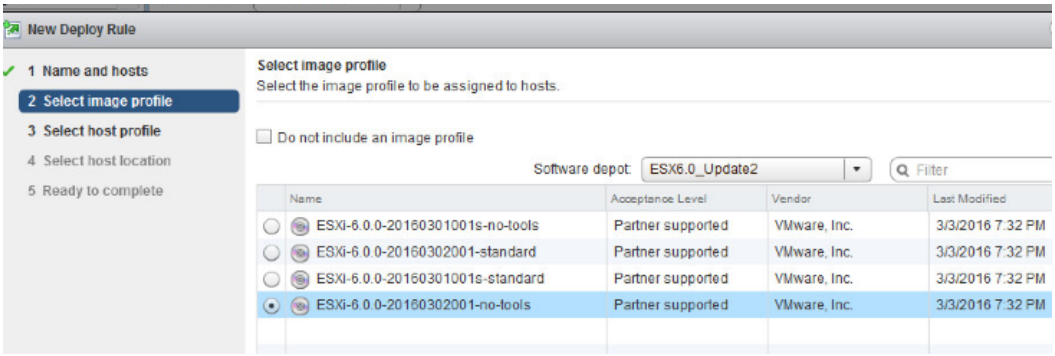
REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-2140AE92-D092-4640-9B1A-0AF425BC88AB.html

Create / Modify rules and rule sets

In the vSphere Web Client, drill to **Home** > **Auto Deploy > Deploy rules.**







REF: *VCP6-DCV Cert Guide:* page 537

REF: http://bit.ly/2fjzRI7

Create and associate Host Profiles for an Auto Deploy reference host

Right-click the host and select **Host Profile** > **Create Profile** from Host,

Configure Kernel Boot Parameters for scripted install according to a deployment plan:

Modify scripted weasel install (ks.cfg)

Copy the `ks.cfg` file from an installed host, modify it, place it an assessable location. In scripted install / upgrade, use ks= to specify path

- ks=cdrom:/path
- ks=file://path
- ks=http://path
- ks=https://path
- ks=nfs://path
- ks=usb:/path

REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-C3F32E0F-297B-4B75-8B3E-C28BD08680C8.html

Create / Modify scripted installation

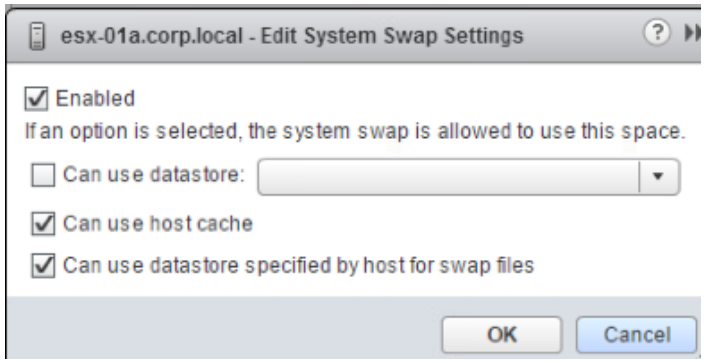
REF: *VCP6-DCV Cert Guide:* page 435

Configure Advanced System Settings according to a deployment plan:

Edit System Swap / Scratch Configuration

System Swap:

- Select host, drill to **Manage** > **Settings** > **System Swap**
- Click **Edit** and check boxes for each option I want:
  - datastore (vSAN / vVol cannot be used)
  - host swap cache
  - preferred swap file location (select a specific datastore)

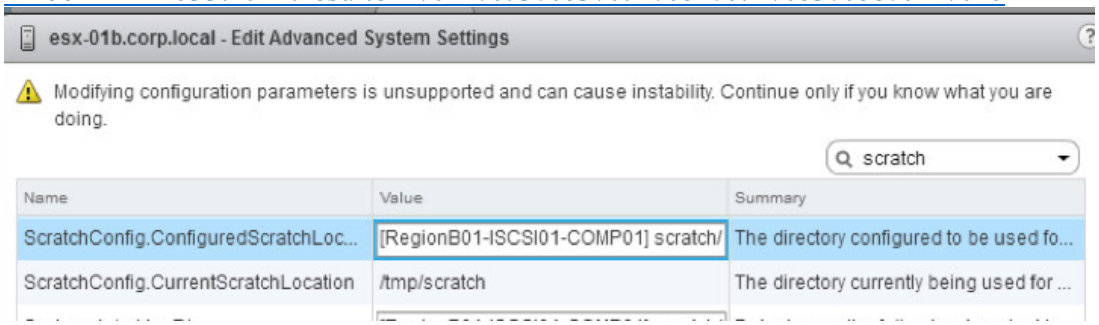


REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.resmgmt.doc/GUID-56608D3C-3C93-4D03-B565-172C08478EA3.html?resultof=%22%73%77%61%70%22%20

Scratch partition

Set **ScratchConfig.ConfiguredScratchLocation** to the desired path, such as /vmfs/volumes/DatastoreUUID/DatastoreFolder:

Set via web client: Ref: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-6A4FCA6C-498C-4080-BFE8-AB9911A4B033.html?resultof=%22%73%63%72%61%74%63%68%22%20



Via vSphere Client: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.hostclient.doc/GUID-9DD57870-ACB9-431A-BA13-E88CF7B54ECE.html?resultof=%22%73%63%72%61%74%63%68%22%20

Configure ESXi host to use a central Syslog Server

esxcli system syslog config get

```
[root@esx-01b:~] esxcli system syslog config get
   Default Network Retry Timeout: 180
   Dropped Log File Rotation Size: 100
   Dropped Log File Rotations: 10
   Enforce SSLCertificates: true
   Local Log Output: /vmfs/volumes/57281322-2d689290-0710-005056018fc5/scratch/log
   Local Log Output Is Configured: true
   Local Log Output Is Persistent: true
   Local Logging Default Rotation Size: 1024
   Local Logging Default Rotations: 2
   Log To Unique Subdirectory: false
   Message Queue Drop Mark: 90
   Remote Host: udp://log-01a.corp.local:514
[root@esx-01b:~]
```

set remote syslog:

```
esxcli system syslog config set --loghost vc01.vmlab.loc
```

another example with rotation, unique directory name and size settings

```
esxcli system syslog config set --
logdir=/path/to/vmfs/directory/ --loghost=RemoteHostname --
logdir-unique=true|false --default-rotate=NNN --default-size=NNN
```

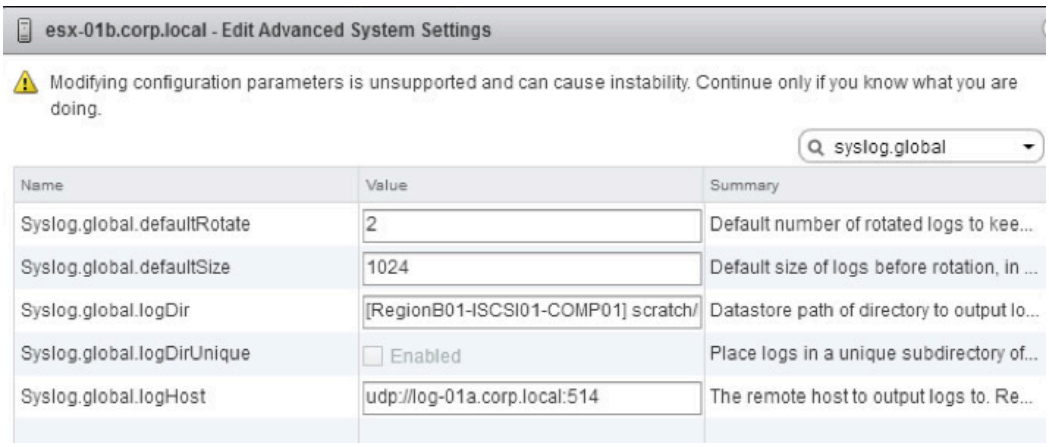
set multiple remote syslogs and protocols:

```
esxcli system syslog config set -loghost
vc01.vmlab.loc,tcp://10.10.10.1:514,ssl://10.10.10.2:1514
```

Configure syslog per ESXi host

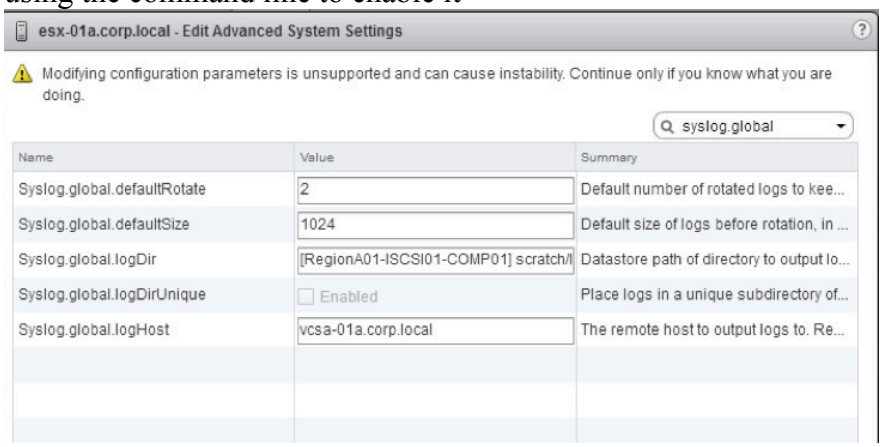
- Syslog.global.defaultRotate (def = 8)
- Syslog.global.defaultSize (def = 1024 KB)
- Syslog.global.LogDir (source log location, ex: [storage1] /systemlogs)
- Syslog.global.LogDirUnique (unique sub-dir per host)
- Syslog.global.LogHost (ex: ssl://hostName1:1514)

Select the host, select **Manage** > **Settings** > **Advanced System Settings**, change the global syslog settings (such as /syslog.global.defaultSize)

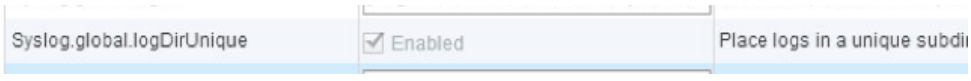


REF:
https://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.upgrade.doc/GUID-9F67DB52-F469-451F-B6C8-DAE8D95976E7.html?resultof=%2522%2573%2579%2573%256c%256f%2567%2522%2520

TIP: If the checkbox to enable unique directory names based on host names is disabled, try using the command line to enable it




```
esxcli system syslog config set --logdir-unique="true"
```

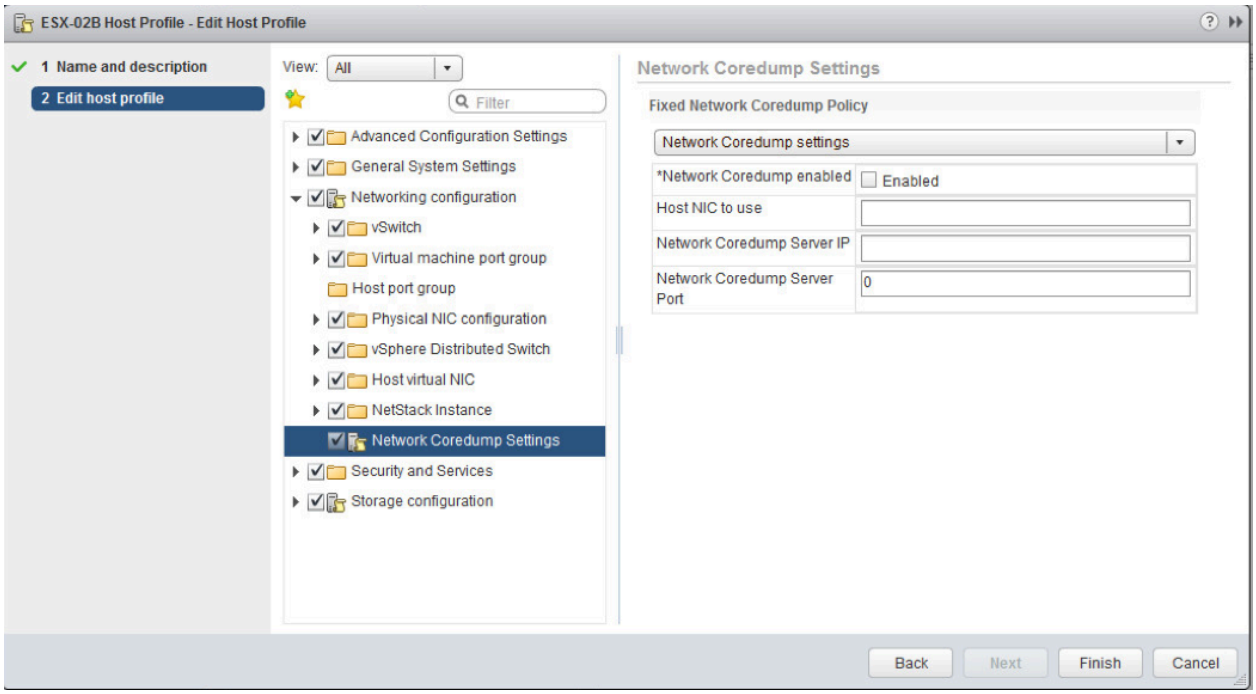



```
[root@esx-01a:~] ls /vmfs/volumes/RegionA01-ISCSI01-COMP01/scratch/log
Xorg.log                hostprofiletrace.log   vmauthd.log
auth.log                iofiltervpd.log        vmkdevmgr.log
clomd.log               lacp.log               vmkernel.0.gz
ddecomd.log             nfcd.log               vmkernel.log
dhclient.log            osfsd.log              vmkeventd.log
epd.log                 rabbitmqproxy.log      vmksummary.log
esx-01a.corp.local      rhttpproxy.0.gz        vmkwarning.log
```

VMware vSphere Syslog Collector on Windows based vCenter Server and **VMware Sphere Syslog Service** for the vCenter Server Appliance REF: http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.upgrade.doc/GUID-6AF21A92-A67E-4DD9-8AC6-46F990118037.html

Manage/Edit the Core Dump configuration of an ESXi host

Configure network core dump settings in host profiles: REF: *VCP6-DCV Cert guide* page 546



Create a rule to apply the host profile (with core dump settings) to specific hosts REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-7EDD1093-D1F2-4798-9C51-71D6ABC1485A.html

And
https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-775F602C-7432-4259-B132-4EC1F38A7EE7.html?resultof=%22%64%75%6d%70%22%20%22%63%6f%6c%6c%65%63%74%6f%72%22%20

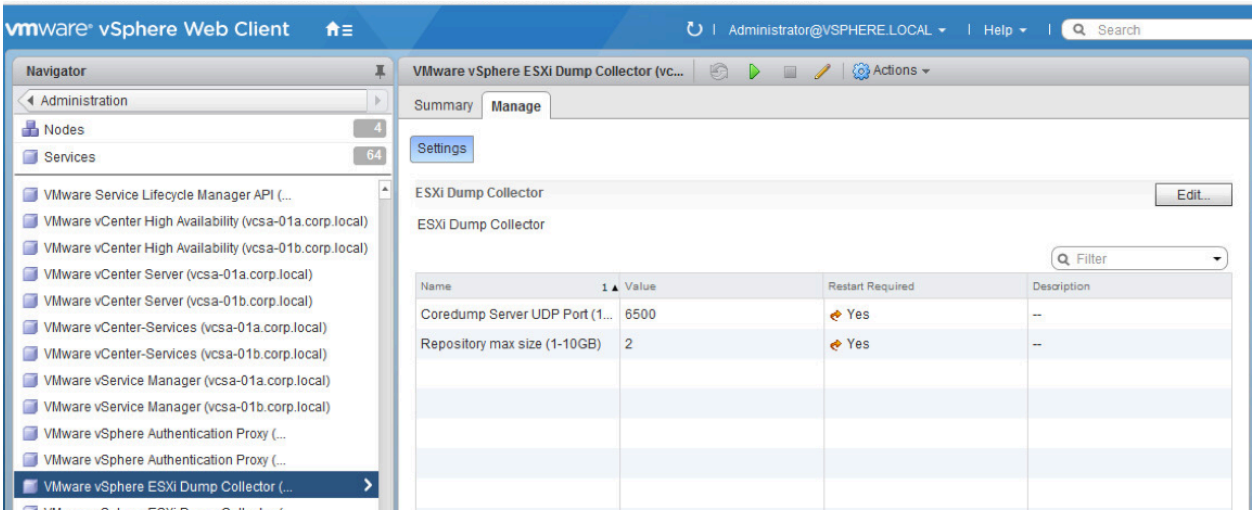
This first attempt produced an error because Auto Deploy was not running. In this example, the host profile is named *esx-04a* and the target ESXi hosts' IP address = *192.168.1.10 to .20*

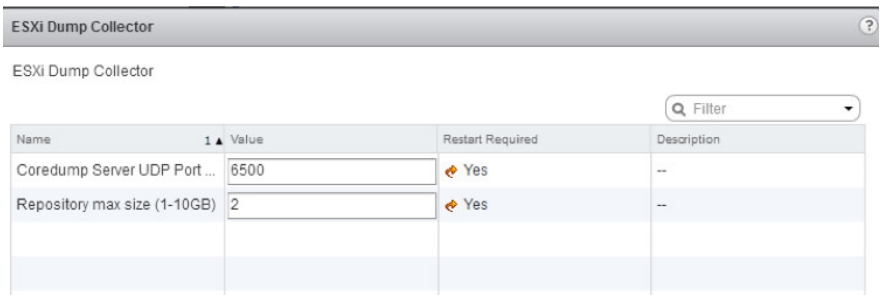
```
PowerCLI C:\> New-DeployRule -name "jadrule" -item  esx-04a -pattern "vendor=Acme", "ipv4=192.168.1.
10-192.168.1.20"
New-DeployRule : 6/27/2016 5:38:20 PM    New-DeployRule        Unable to connect to the remote
server
At line:1 char:1
+ New-DeployRule -name "jadrule" -item  esx-04a -pattern "vendor=Acme", "ipv4=192. ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [New-DeployRule], VimException
    + FullyQualifiedErrorId : Core_BaseCmdlet_UnknownError,VMware.DeployAutomation.Commands.NewDep
   loyRule

PowerCLI C:\> _
```

second attempt, after starting the Auto Deploy service

```
PowerCLI C:\> New-DeployRule -name "jadrule" -item  esx-04a -pattern "vendor=Acme", "ipv4=192.168.1.
10-192.168.1.20"


Name        : jadrule
PatternList : {ipv4=192.168.1.10-192.168.1.20, vendor=Acme}
ItemList    : {esx-04a}


PowerCLI C:\> _
```

configure vSphere ESXi Core Dump Collector Service: REF: *VCP6-DCV Cert Guide* page 356





managing core dumps and vicfg-dumppart:
REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vcli.examples.doc/cli_performance.12.4.html?resultof=%22%64%75%6d%70%22%20

esxcli system coredump network set: manage network core dumps (sent to ESXi Dump Collector)

this command is picky. Set just the interface-name and server-ip first:

```
esxcli system coredump network set --interface-name=vmk0 --server-ip=192.168.110.22
```

then enable the network core dump

```
esxcli system coredump network set --enable=true
```

then, check your settings

```
[root@esx-04a:~] esxcli system coredump network get
   Enabled: true
   Host VNic: vmk0
   Is Using IPv6: false
   Network Server IP: 192.168.110.22
   Network Server Port: 6500
```

REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vcli.examples.doc/cli_performance.12.4.html?path=1_1_0_9_2_1#991573

vicfg-dumppart manages dump partition (or esxcfg-dumppart) . These commands do not create disk partitions, but can be used to set a partition as a target for core dumps.

- esxcfg-dumppart -t get (show) active core dump partition
- esxcfg-dumppart -d deactivate the current core dump partition

- esxcfg-dumppart -s set active core dump partition
- esxcfg-dumppart -C copy a core dump file from a partition

```
[root@esx-01b:~] esxcfg-dumppart -f
Partition name mpx.vmhba1:C0:T0:L0:7 -> /vmfs/devices/disks/mpx.vmhba1:C0:T0:L0:7
[root@esx-01b:~] esxcfg-dumppart -d
Dump partition deactivated.
[root@esx-01b:~] esxcfg-dumppart -f
Partition name mpx.vmhba1:C0:T0:L0:7 -> /vmfs/devices/disks/mpx.vmhba1:C0:T0:L0:7
[root@esx-01b:~] esxcfg-dumppart -t
none
[root@esx-01b:~] esxcfg-dumppart -s mpx.vmhba1:C0:T0:L0:7
[root@esx-01b:~] esxcfg-dumppart -t
mpx.vmhba1:C0:T0:L0:7
[root@esx-01b:~]
```

REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vcli.examples.doc/cli_performance.12.4.html?resultof=%22%64%75%6d%70%22%20

Manage core dump partitions with **esxcli system coredump partition**

```
[root@esx-01b:~] esxcli system coredump partition get
   Active: mpx.vmhba1:C0:T0:L0:7
   Configured: mpx.vmhba1:C0:T0:L0:7
[root@esx-01b:~] esxcli system coredump partition list
Name                    Path                                      Active  Configured
----------------------  ----------------------------------------  ------  ----------
mpx.vmhba1:C0:T0:L0:7  /vmfs/devices/disks/mpx.vmhba1:C0:T0:L0:7    true        true
[root@esx-01b:~] esxcli system coredump partition set --unconfigure
[root@esx-01b:~] esxcli system coredump partition get
   Active:
   Configured:
[root@esx-01b:~] esxcli system coredump partition set --partition=mpx.vmhba1:C0:T0:L0:7
[root@esx-01b:~] esxcli system coredump partition get
   Active: mpx.vmhba1:C0:T0:L0:7
   Configured: mpx.vmhba1:C0:T0:L0:7
[root@esx-01b:~]
```

REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vcli.examples.doc/cli_performance.12.4.html?path=1_1_0_9_2_0#991555

Objective 1.2 - Deploy and Configure Core Management Infrastructure Components

Deploy vCenter core components according to a deployment plan:

Deploy and Configure a Platform Services Controller (PSC):

Windows based vCenter Server: built-in system account vs Windows account, impacts use of SQL Authentication or Windows Authentication

- if vCenter Server service is running under the Windows built-in System account, then if you use SQL Server, you must use SQL Server Authentication for the DSN
- if you want to use a DSN with Windows Authentication, then configure it to use the same user account that runs the VMware VirtualCenter Management Webservices

REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-A93112F3-5827-4DC3-B785-C64E66A4D007.html?resultof=%22%62%75%69%6c%74%2d%69%6e%22%20%22%62%75%69%6c%74%22%20%22%73%79%73%74%65%6d%22%20%22%61%63%63%6f%75%6e%74%22%20

Multiple SSO sites, multiple PSC instances in same SSO site, and sharing the same SSO domain: REF: *VCP6-DCV Cert Guide* page 44.

Replication is not available with embedded PSCs. Enhanced Linked Mode does not use ADAM, it uses PSC replication (or two vCenters connected to the same PSC). External PSCs can support multiple vCenter instances.

The vpxd command can be used to fix some issues, such as change the database password:

```
Usage: /usr/lib/vmware-vpx/vpxd [FLAGS]
Flags:
      -b      Recreate database repository
      -v      Print the version number to stdout
      -p      Reset the database password
      -f cfg  Use the specified file instead of the default vpxd.cfg
      -o newSchemaOwner  Use the specified schema name to create database reposi
tory in SQL server
      -C      install new SSL certificate file
      -F      Force Full Host Sync for all hosts
      -K      install new SSL private key file
      -Q      install new Symmetric encryption keygen data file
      -L      Migrate permissions in the VCDB
```

vCenter Server Cannot Connect to the Database

After you replace default vCenter Server certificates, you might be unable to connect to the vCenter Server database.

Problem

vCenter Server is unable to connect to the vCenter Server database after you replace default vCenter Server certificates, an management web services do not start.

Cause

The database password must be updated in its encrypted form.

Solution

Update the database password by running the following command: **`vpxd -P pwd`**.

vCenter Server Cannot Connect to Managed Hosts

After you replace default vCenter Server certificates and restart the system, vCenter Server might not be able to connect to managed hosts.

Problem

vCenter Server cannot connect to managed hosts after server certificates are replaced and the system is restarted.

Solution

Log into the host as the root user and reconnect the host to vCenter Server.

New vCenter Server Certificate Does Not Appear to Load

After you replace default vCenter Server certificates, the new certificates might not appear to load.

Problem

When you install new vCenter Server certificates, you might not see the new certificate.

Cause

Existing open connections to vCenter Server are not forcibly closed and might still use the old certificate.

Solution

To force all connections to use the new certificate, use one of the following methods.

- Restart the network stack or network interfaces on the server.
- Restart the vCenter Server service.

Determine use case for embedded vs external PSC

External vs Embedded PSC deployments REF: *VCP6-DCV Cert Guide* page 42

Re-point a vCenter Server Appliance to another External PSC

Repoint vCenter to PSC (if two PSC share the same SSO domain, then if one fails, you can repoint a vCenter server to the other. You can also repoint to re-balance the workload)

- logon to a command prompt on vCenter Appliance or Windows based vCenter
- if using Windows, navigate to this directory: `C:\Program Files\VMware\vCenter Server\bin`
- `cmsso-util repoint --repoint-psc` *`psc_fqdn_or_static_ip`* `[--dc-port port_number]`

```
vcsa-01a:~ # cmsso-util  repoint --repoint-psc psc-01a.corp.local
Validating Provided Configuration ...
Error: The provided Platform Services Controller(PSC) psc-01a.corp.local is alre
ady the current active PSC of this vCenter Server
```

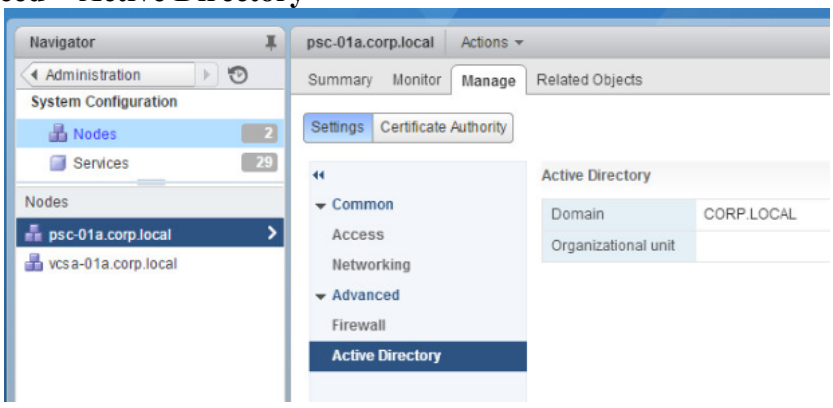
REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.upgrade.doc/GUID-07D2C988-67A5-4FE2-A276-8B99E4909370.html?resultof=%22%72%65%70%6f%69%6e%74%22%20

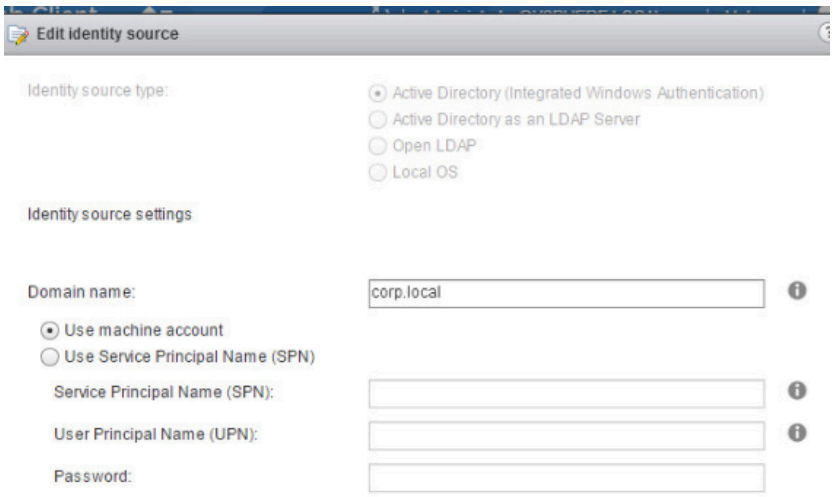
Deploy and Configure Identity Sources for Single Sign-On:

Configure Single Sign-On users and groups

SSO users and groups REF: *VCP6-DCV Cert Guide* page 52

WHEN USING VCENTER APPLIANCE, JOIN THE EXTERNAL PSC TO THE AD DOMAIN. **Administration** > **System** > **Nodes**, select the psc device, **Manage** > **Settings** > **Advanced** > **Active Directory**





Change Default domain for Single Sign-On

SSO default domain (**Administration** > **Single Sign-On** > **Configuration** >**Identify Sources**, select the identity source and click the **Set as Default Domain button**
REF: *VCP6-DCV Cert Guide page* 55

List services registered with Single Sign-on

For Linux based SSO (PSC):

```
/usr/lib/vmidentity/tools/scripts/lstool.py  --url  http://localhost:7080/lookupservice/sdk
```

which, provides a long list of results, so pipe it to grep. Perhaps filter for Type:
or a specific service name.

```
root@psc-01a [ ~ ]# /usr/lib/vmidentity/tools/scripts/lstool.py list --url  http://localhost:7080/lookupservice/sdk | grep Type:
2016-10-18 23:55:50,915 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext - Re
.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@5fe5c6f: startup date [Tue Oct 18 23:
16]; root of context hierarchy
2016-10-18 23:55:50,950 INFO  org.springframework.beans.factory.xml.XmlBeanDefinitionReader - Loading XML bean definitions from clas
rce [com/vmware/vim/binding/vmodl/context_v2.xml]
2016-10-18 23:55:51,178 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext - Cl
ware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@5fe5c6f: startup date [Tue Oct 18 23:55:
; root of context hierarchy
2016-10-18 23:55:51,182 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl - Package com.vmware.vim.binding.vmodl loaded in
2016-10-18 23:55:51,183 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext - Re
.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@77e4c80f: startup date [Tue Oct 18 23
016]; root of context hierarchy
2016-10-18 23:55:51,184 INFO  org.springframework.beans.factory.xml.XmlBeanDefinitionReader - Loading XML bean definitions from clas
rce [com/vmware/vim/binding/vmodl/context_v2.xml]
2016-10-18 23:55:51,204 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext - Cl
ware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@77e4c80f: startup date [Tue Oct 18 23:55
]; root of context hierarchy
2016-10-18 23:55:51,206 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl - Package com.vmware.vim.binding.vmodl loaded in
2016-10-18 23:55:51,207 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext - Re
.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@c8e4bb0: startup date [Tue Oct 18 23:
16]; root of context hierarchy
2016-10-18 23:55:51,208 INFO  org.springframework.beans.factory.xml.XmlBeanDefinitionReader - Loading XML bean definitions from clas
rce [com/vmware/vim/binding/lookup/context.xml]
2016-10-18 23:55:51,291 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext - Cl
ware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@c8e4bb0: startup date [Tue Oct 18 23:55:
; root of context hierarchy
2016-10-18 23:55:51,292 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl - Package com.vmware.vim.binding.lookup loaded i
2016-10-18 23:55:51,701 INFO  com.vmware.vim.lookup.client.SiteAffinityServerEndpointProvider - Site affinity is disabled
2016-10-18 23:55:52,272 WARN  com.vmware.vim.vmomi.client.http.impl.HttpConfigurationCompilerBase$ConnectionMonitorThreadBase - Shut
e connection monitor.
2016-10-18 23:55:52,274 WARN  com.vmware.vim.vmomi.client.http.impl.HttpConfigurationCompilerBase$ConnectionMonitorThreadBase - Inte
more connection pool cleanups will be performed.
        Service Type: cs.identity
                Type: com.vmware.cis.cs.identity.admin
                Type: com.vmware.cis.cs.identity.openidconnect
                Type: com.vmware.cis.cs.identity.websso
                Type: com.vmware.cis.cs.identity.sso
                Type: com.vmware.cis.cs.identity.groupcheck
                Type: com.vmware.cis.cs.identity.admin.idm.rest
                Type: com.vmware.cis.common.healthstatus
                Type: com.vmware.cis.cs.identity.idpprovisioning
        Service Type: cis.vmonapi
                Type: com.vmware.cis.common.resourcebundle
                Type: com.vmware.appliance.vmon
        Service Type: sca
                Type: com.vmware.cis.sca
        Service Type: cs.componentmanager
```

In Windows:

Note: In vSphere 6.x, the command to list the registered services is:

```
"%VMWARE_PYTHON_BIN%" "%VMWARE_CIS_HOME%\VMware Identity
Services\lstool\scripts\lstool.py" list --url http://localhost:7080/lookupservice/sdk
```

REF:
https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2043509

Deploy and configure vCenter Server

Windows based vCenter Server requirements
https://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.upgrade.doc/GUID-F072712B-F568-4C3A-A4BC-

EE6856D50CDA.html?resultof=%2522%2563%2568%2565%2563%256b%2565%2572%2522%2520

If your vCenter Server service is running in a user account other than the Local System account, verify that the user account in which the vCenter Server service is running has the following permissions:

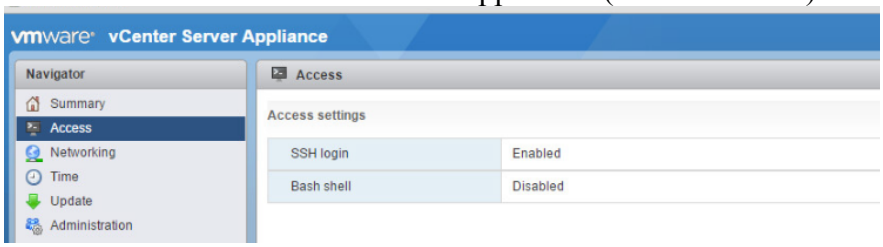
- **Member of the Administrators group**
- **Log on as a service**
- **Act as part of the operating system (if the user is a domain user)**

Windows based vCenter upgrade pre-checker – runs automatically during upgrade process. https://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.upgrade.doc/GUID-AE9F946D-F7C4-4104-92BC-235343A47058.html?resultof=%2522%2563%2568%2565%2563%256b%2565%2572%2522%2520

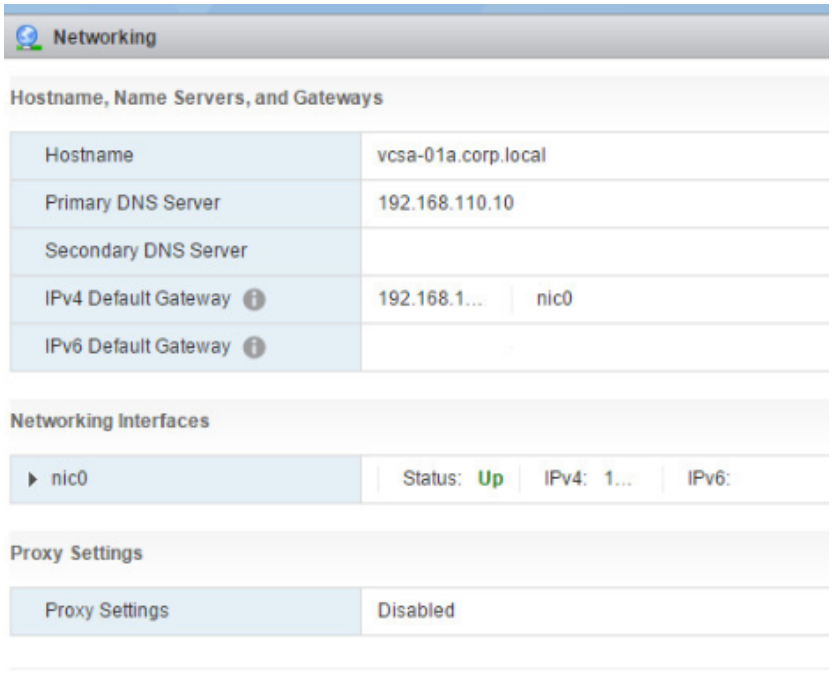
Remediate vCenter upgrade issue: *During the uninstallation phase, the vCenter Server 5.x instance is unregistered from the SSO server. During the import phase, the vCenter Server 6.0 instance is registered with the SSO server. If a failure occurs prior to the registration, SSO does not have an entry for the vCenter Server. You may need to revert back to the vCenter 5.x server. If a failure occurs prior to the registration, SSO does not have an entry for the vCenter Server. You may need to revert back to the vCenter 5.x server. If a failure occurs during the import or first boot phase, after the export phase, you can re-attempt to upgrade to vCenter Server 6.0 rather than revert to vCenter Server 5.x. For more details, see VMware KB 2108938.* pp 432

Configure the vCenter Appliance:

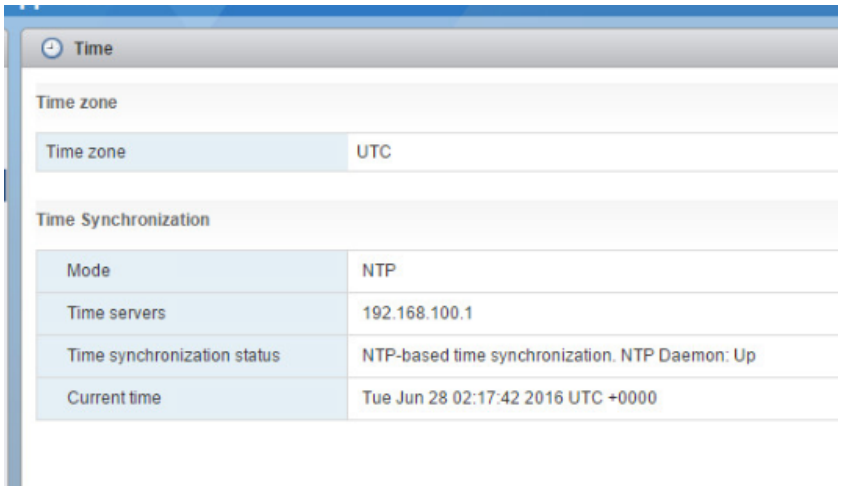
Enable SSH and BASH on vCenter appliance (Drill to **Access**)



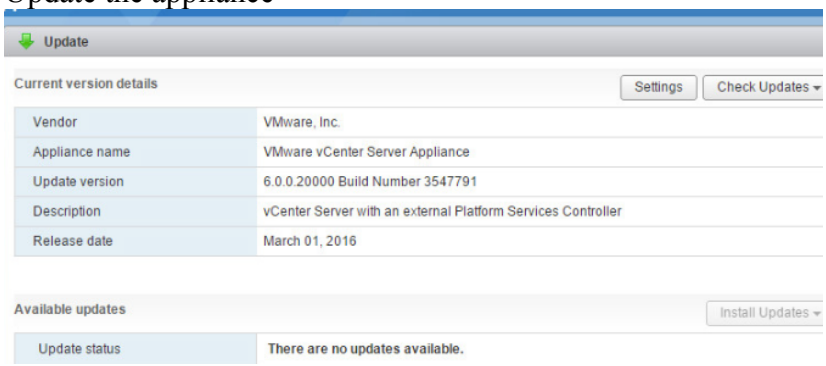
Configure Networking:



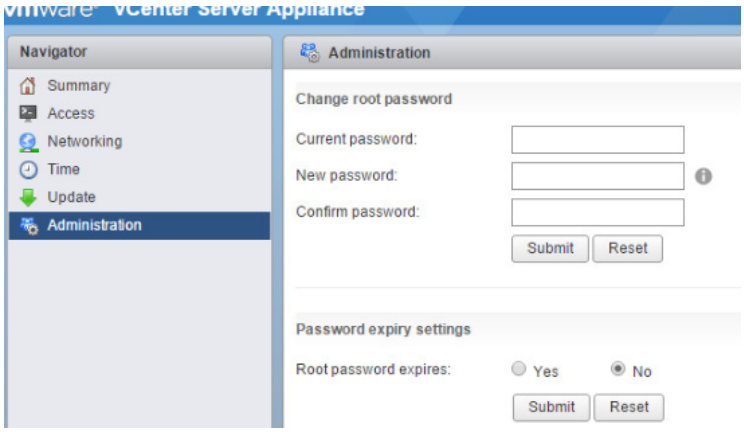
Configure Time Zone and Time Sync (NTP)



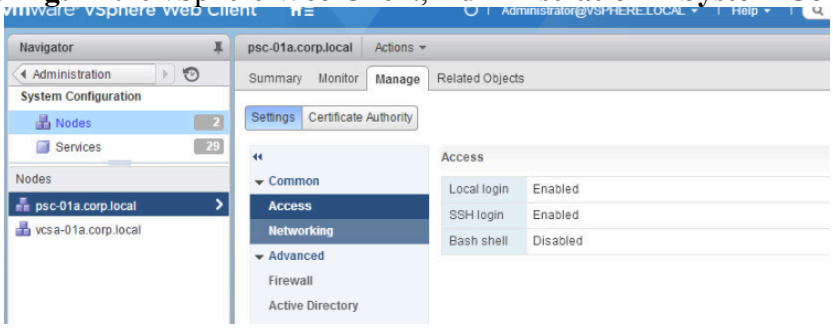
Update the appliance

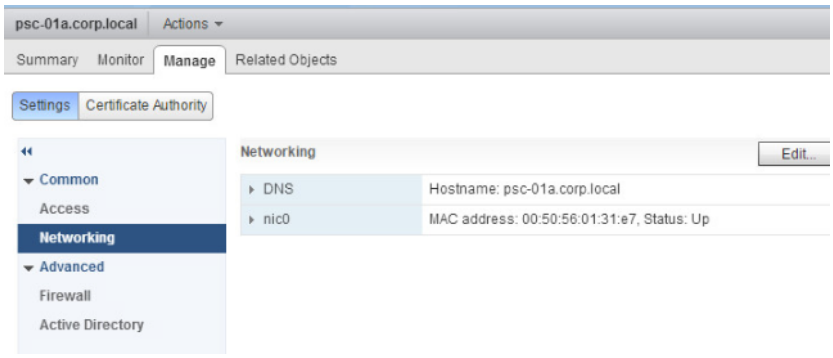


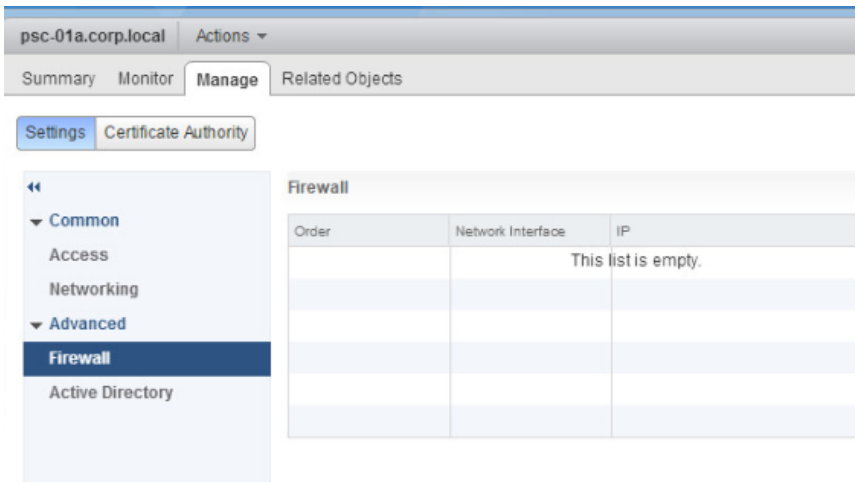
Configure root password:



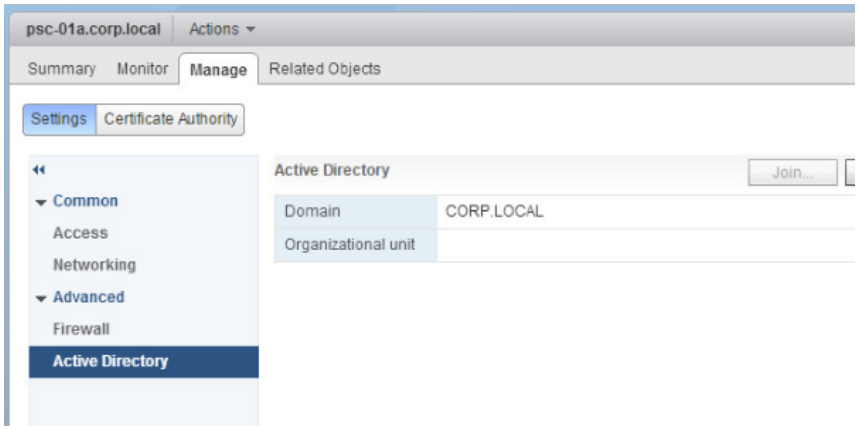
PSC config: In the vSphere Web Client, **Administration** > **System Configuration**> **Nodes**







JOIN ACTIVE DIRECTORY



REF: *VCP6-DCV Cert Guide* pp 48

Deploy / Configure Enhanced Link Mode

To join vCenter Server systems in Enhanced Linked Mode, connect them to the same Platform Services Controller, or to Platform Services Controllers that share the same vCenter Single Sign-On domain.

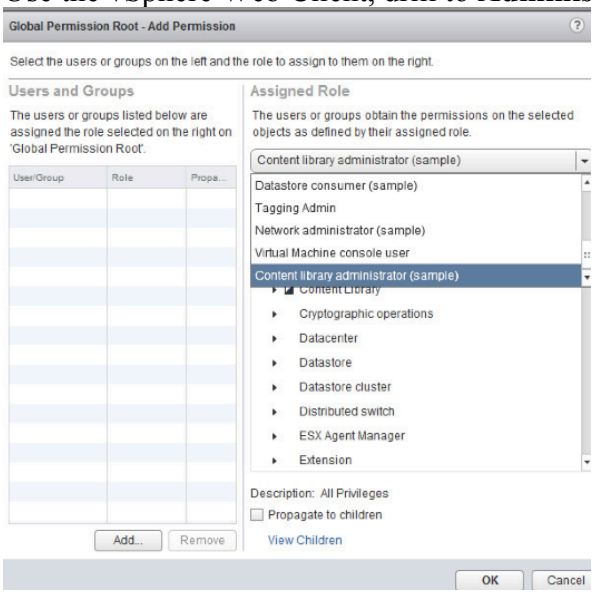
Ref: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.vcenterhost.doc/GUID-6ADB06EF-E342-457E-A17B-1EA31C0F6D4B.html?resultof=%22%65%6e%68%61%6e%63%65%64%22%20%22%65%6e%68%61%6e%63%22%20%22%6c%69%6e%6b%22%20

REF: *VCP6-DCV Cert Guide* page 44

Manage / Configure vCenter components according to a deployment plan:

Configure Global Permissions for vCenter services

Use the vSphere Web Client, drill to **Administration** > **Global Permissions** > **Manage**

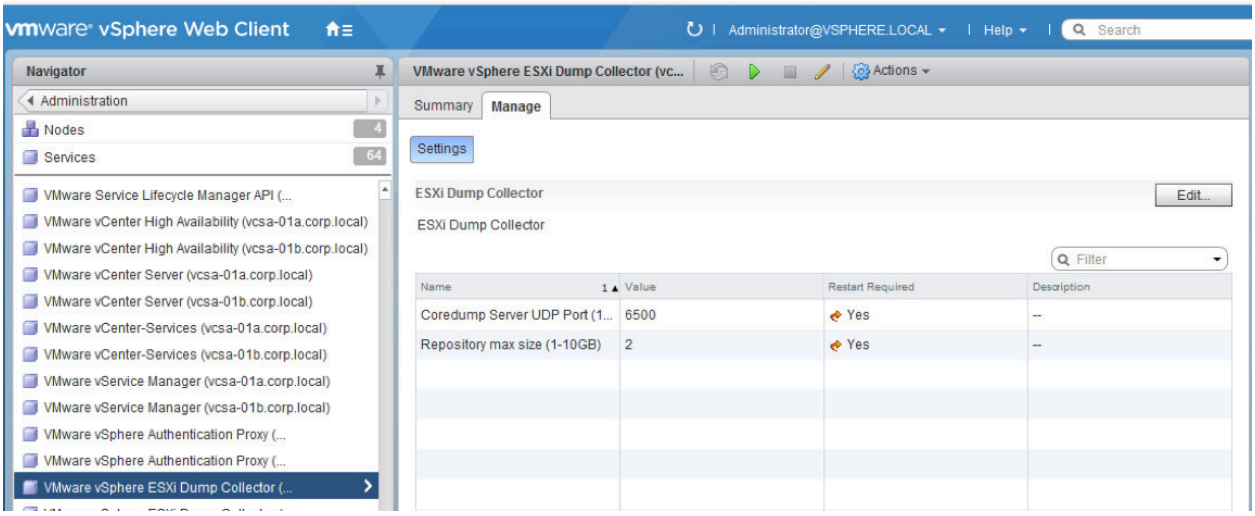


Global Permissions inheritance: REF: *VCP6-DCV Cert Guide* page 10

Content Library access is controlled by permissions on global root object: REF: *VCP6-DCV Cert Guide* page 11

Configure Dump Collector service

configure vSphere ESXi Core Dump Collector Service: REF: *VCP6-DCV Cert Guide* page 356



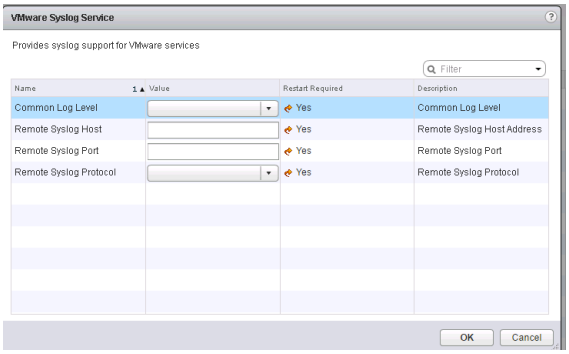
Configure the Syslog Collector / Syslog service

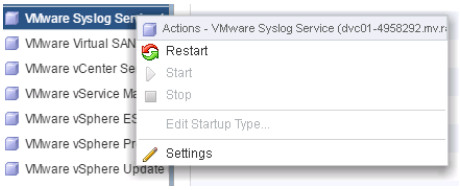
VMware Syslog service:

The VMware vSphere Syslog Collector runs in a Windows based vCenter. The VMware vSphere Syslog Service runs in a vCenter Appliance. Per this text from the vSphere 6 Documentation Center

- *The VMware Platform Services Controller group of infrastructure services contains vCenter Single Sign-On, License service, Lookup Service, and VMware Certificate Authority.*
- *The vCenter Server group of services contains vCenter Server, vSphere Web Client, Inventory Service, vSphere Auto Deploy, vSphere ESXi Dump Collector, VMware vSphere Syslog Collector on Windows and VMware Sphere Syslog Service for the vCenter Server Appliance.*

- Administration > System Configuration > Services
- Select the appropriate VMware Syslog Service instance
- Click Manage > Edit
- Set the log level (info, notice, warn, error, crit, alert, emerg)
- Set the remote syslog host (*The IP address of the host you want to use for storing ESXi messages and logs. This is also the IP address of the remote syslog server on the network you use to redirect logs and ESXi messages.),* port and protocol (TCP, UDP, TLS)
- Click OK
- Restart the service



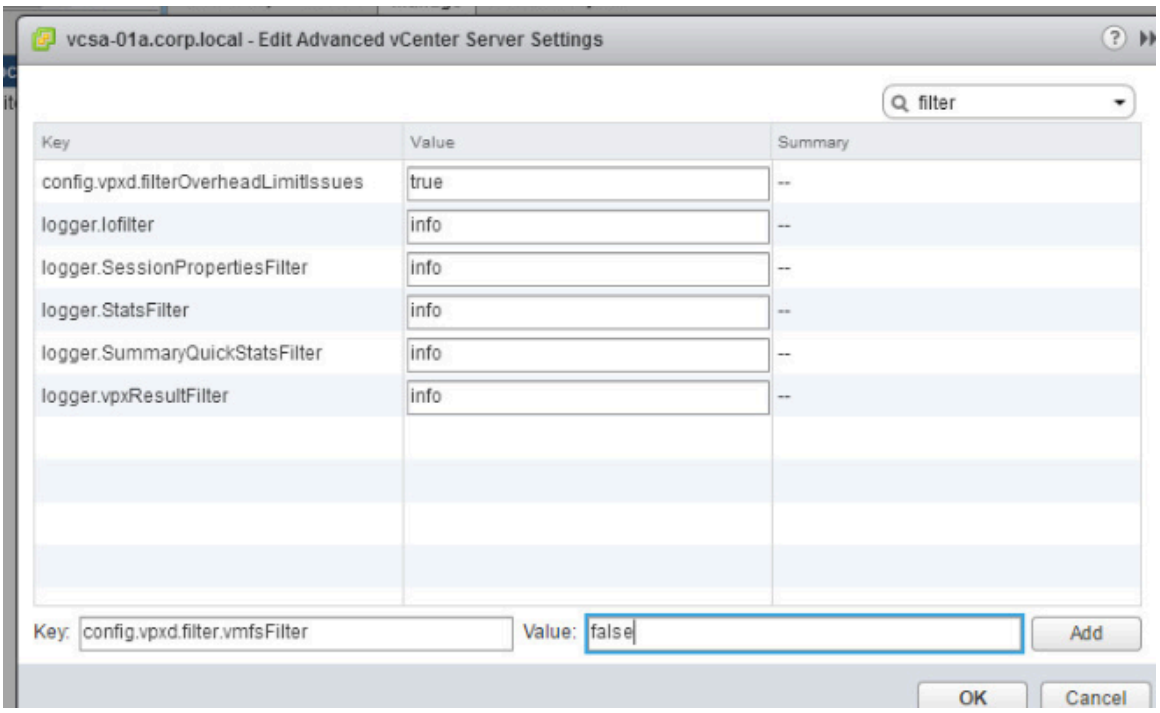


REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.vcenterhost.doc/GUID-61E7E2EA-F531-4665-9225-58BA899F55A5.html?resultof=%22%73%79%73%6c%6f%67%22%20

Managing vCenter Server advanced configurations

Storage filters: REF: *VCP6-DCV Cert Guide* page 175

- Select the vCenter Server
- Manage > Settings > Advanced Settins
- use the search box to search for *filter*. By default, none of the following storage filters exist in the interface, but their default value is *true*.
- To set any of these to *false*, add the appropriate storage filter and set value to *false*.
  NOTE: each setting begins with **config.vpxd.filter.** No need to restart anything.
  - config.vpxd.filter.**rdmFilter**
  - config.vpxd.filter.**vmfsFilter**
  - config.vpxd.filter.**hostRescanFilter**
  - config.vpxd.filter.**SameHostAndTransportsFilter**



Objective 1.3 - Deploy and Configure Update Manager Components

Deploy / Configure Update Manager components according to a deployment plan:

Configure VUM Update Manager download service

Install VUM download service: REF: http://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.update_manager.doc/GUID-AB1032CF-2C9A-44E5-94BA-216396F167F9.html?resultof=%22%64%6f%77%6e%6c%6f%61%64%22%20%22%73%65%72%76%69%63%65%22%20%22%73%65%72%76%69%63%22%20

- do not install UMDS on same server as VUM
- do not install UMDS 6.X on same machine as UMDS 5.X, they must not share the same repository

Procedure

1. Log in to the machine where UMDS is installed, and open a Command Prompt window.
2. Navigate to the directory where UMDS is installed.

   The default location in 64-bit Windows is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`.
3. Specify the updates to download.
   - To set up a download of all ESXi host updates and all virtual appliance upgrades, run the following command:

     ```
     vmware-umds -S --enable-host --enable-va
     ```
   - To set up a download of all ESXi host updates and disable the download of virtual appliance upgrades, run the following command:

     ```
     vmware-umds -S --enable-host --disable-va
     ```
   - To set up a download of all virtual appliance upgrades and disable the download of host updates, run the following command:

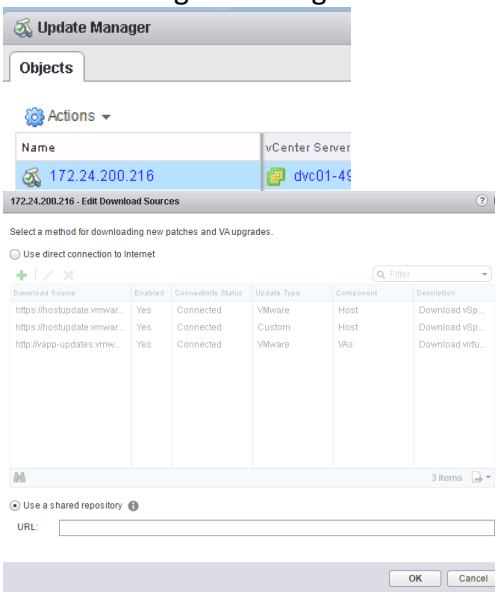
     ```
     vmware-umds -S --disable-host --enable-va
     ```

What to do next

Configure a VUM shared repository

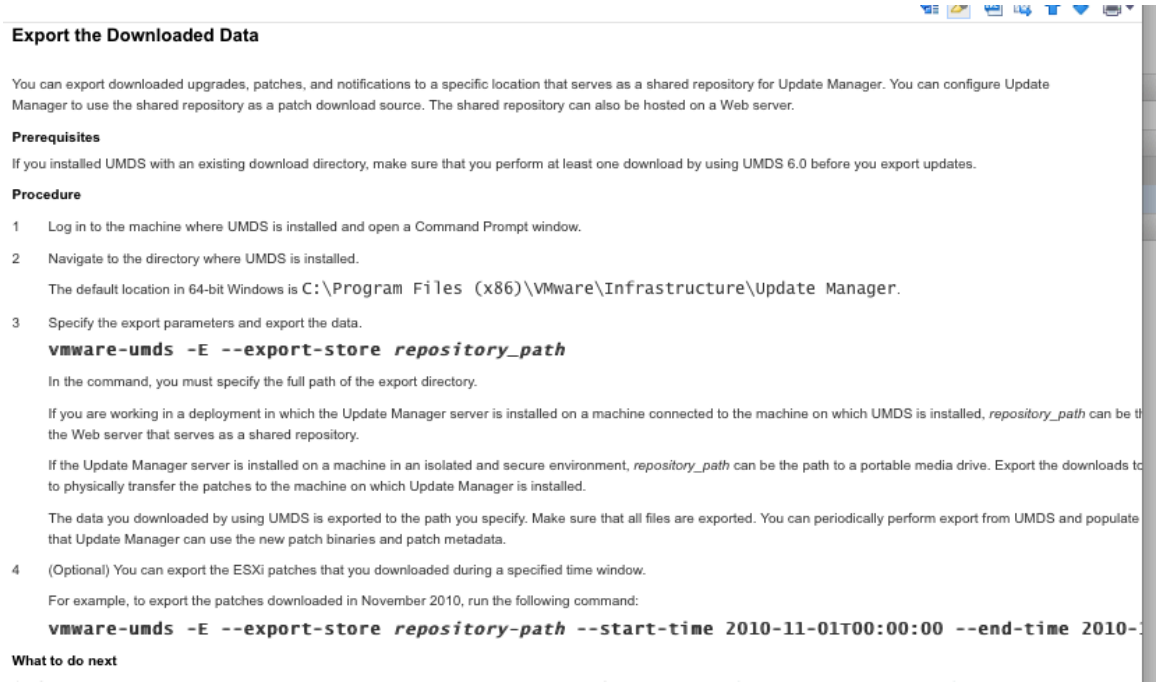
UMDS shared repository REF: http://bit.ly/2eFEYHo

- in vSphere Web Client, Home > Update Manager
- drill into the VUM server assigned to your vCenter Server
- Manage > Settings > Download Settings



- You cannot download updates from the Internet and use a shared repository at the same time. Choose one or the other.
- You cannot use network folders or mapped drives for the shared repository. You can use a local drive path on the VUM server. Or you can use an HTTP/HTTPS path to a Web Server

Export the downloaded data: `use vmware-umds -E --export-store path`



Export the Downloaded Data

You can export downloaded upgrades, patches, and notifications to a specific location that serves as a shared repository for Update Manager. You can configure Update Manager to use the shared repository as a patch download source. The shared repository can also be hosted on a Web server.

Prerequisites

If you installed UMDS with an existing download directory, make sure that you perform at least one download by using UMDS 6.0 before you export updates.

Procedure

1 Log in to the machine where UMDS is installed and open a Command Prompt window.

2 Navigate to the directory where UMDS is installed.

The default location in 64-bit Windows is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`.

3 Specify the export parameters and export the data.

```
vmware-umds -E --export-store repository_path
```

In the command, you must specify the full path of the export directory.

If you are working in a deployment in which the Update Manager server is installed on a machine connected to the machine on which UMDS is installed, *repository_path* can be th
the Web server that serves as a shared repository.

If the Update Manager server is installed on a machine in an isolated and secure environment, *repository_path* can be the path to a portable media drive. Export the downloads to
to physically transfer the patches to the machine on which Update Manager is installed.

The data you downloaded by using UMDS is exported to the path you specify. Make sure that all files are exported. You can periodically perform export from UMDS and populate
that Update Manager can use the new patch binaries and patch metadata.

4 (Optional) You can export the ESXi patches that you downloaded during a specified time window.

For example, to export the patches downloaded in November 2010, run the following command:

```
vmware-umds -E --export-store repository-path --start-time 2010-11-01T00:00:00 --end-time 2010-
```

What to do next

Configure VUM smart rebooting

Disable vum smart rebooting, which is enabled by default to restart VMs in a vApp as needed to maintain startup dependencies.

- in vSphere Web Client, Home > Update Manager
- drill into the VUM server assigned to your vCenter Server
- Manage > Settings > vApp Settings
- Edit the **Smart reboot after remediation** setting (Enabled by default)

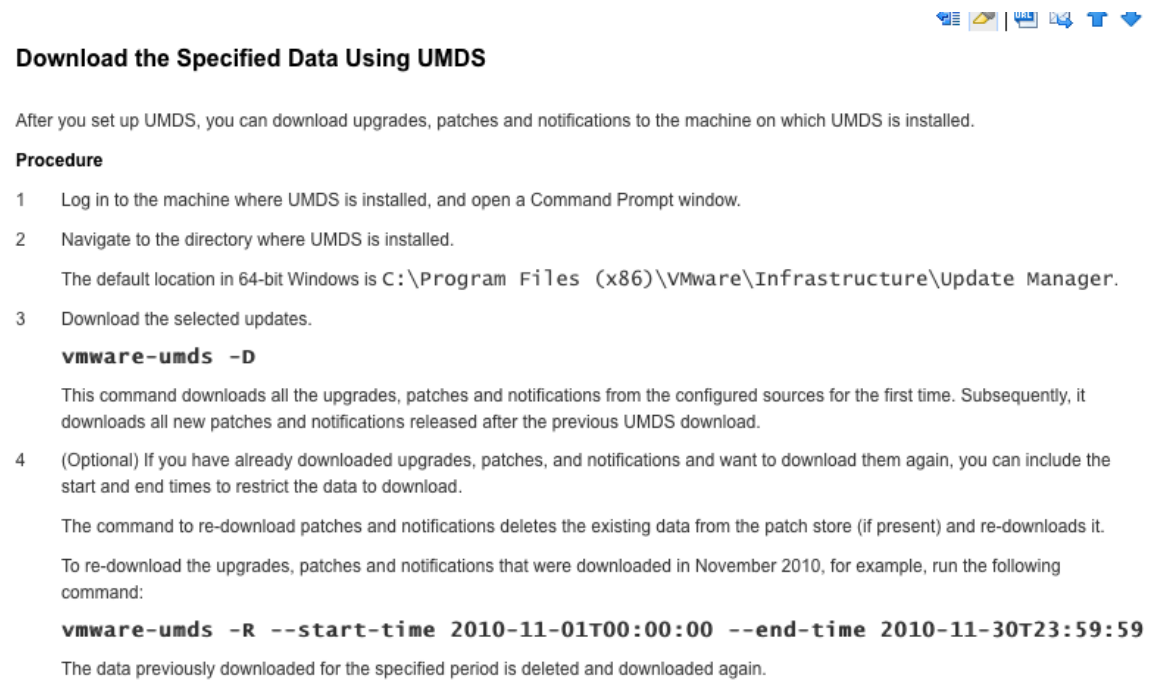
REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.update_manager.doc/GUID-DC8E2DDC-1611-4619-B3C2-C9BE231758AD.html?resultof=%22%73%6d%61%72%74%22%20%22%72%65%62%6f%6f%74%22%20

Manually download updates to a VUM repository

Import or Download patches into VUM repository

- **Download**
  - In vSphere Web Client, drill into the Update Manager
  - Manage > Settings >Download Schedule
  - Click **Download Now** button
  - Alternatively, use the **`vmare-umds -D`** command
- **Import**
  - In vSphere Web Client, drill into the Update Manager
  - Manage > Settings > Import Patches
  - In the wizard select the ZIP file where the patches were previously downloaded
  -

REF: https://blogs.vmware.com/vsphere/2012/03/understanding-esxi-patches-manually-adding-patches-to-update-manager.html



Download the Specified Data Using UMDS

After you set up UMDS, you can download upgrades, patches and notifications to the machine on which UMDS is installed.

Procedure

1 Log in to the machine where UMDS is installed, and open a Command Prompt window.

2 Navigate to the directory where UMDS is installed.

The default location in 64-bit Windows is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`.

3 Download the selected updates.

```
vmware-umds -D
```

This command downloads all the upgrades, patches and notifications from the configured sources for the first time. Subsequently, it downloads all new patches and notifications released after the previous UMDS download.

4 (Optional) If you have already downloaded upgrades, patches, and notifications and want to download them again, you can include the start and end times to restrict the data to download.

The command to re-download patches and notifications deletes the existing data from the patch store (if present) and re-downloads it.

To re-download the upgrades, patches and notifications that were downloaded in November 2010, for example, run the following command:

```
vmware-umds -R --start-time 2010-11-01T00:00:00 --end-time 2010-11-30T23:59:59
```

The data previously downloaded for the specified period is deleted and downloaded again.

Change the UMDS Patch Repository Location:

- `vmware-umds -S --patch-store` *`your_new_patchstore_folder`*

REF: http://bit.ly/2e7GXFa

Add 3rd party URLs to UMDS:

- `vmware-umds -S --add-url https://host_URL/index.xml --url-type HOST`
- `vmware-umds -S --add-url https://virtual_appliance_URL/index.xml --url-type VA`

REF: http://bit.ly/2ekvXns

Create and modify VUM baseline groups

Baselines:

- In vSphere Web Client, drill into the Update Manager
- Select Manage > Host Baselines
- On the left side of the window, use the Green plus sign to create a new baseline
  - In the wizard, select Host patch, Host extensions or Host upgrade
  - For patches, select fixed or dynamic and select the specific patches or set the criteria
  - For extensions, select the extensions
  - For upgrades, select the ESXi Images, which you must first import at Mangage > ESXi images

REF: http://bit.ly/2etM669

Baseline Groups: REF: http://bit.ly/2e62eMQ

Perform VUM orchestrated vSphere upgrades

VUM orchestrated host upgrade
REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.update_manager.doc/GUID-E96E5ACF-F7EF-4CA8-9E2B-35CE71399DAD.html?resultof=%22%6f%72%63%68%65%73%74%72%61%74%65%64%20%75%70%67%72%61%64%65%22%20

VUM orchesteded vm upgrade
REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.update_manager.doc/GUID-82DC93CC-C998-4A38-99E7-217F9F4D9155.html?resultof=%22%6f%72%63%68%65%73%74%72%61%74%65%64%20%75%70%67%72%61%64%65%22%20

Troubleshoot Update Manager problem areas and issues

Troubleshoot VUM REF: *VCP6-DCV Cert Guide* page 430

- Prior to an upgrade, you can use the VUM pre-check script and review this log file **vmware-vum-server-log4cpp.log**
- During install / upgrade, the interactive installer may produce errors / warnings prompting you to confirm or cancel the install / upgrade
- Such issues are recorded in the installation log file

Utilize Update Manager to reconfigure VUM settings

Use the VUM Utility REF: *VCP6-DCV Cert Guide* page 430

- The VUM utility is automatically installed on the VUM and UMDS servers
- Its name is **VMwareUpdateManagerUtility.exe**
- Use the utility to change:
  - Proxy settings
  - Database user and password
  - vCenter Server IP address
  - SSL certificate

Objective 1.4 - Perform Advanced Virtual Machine Configurations

VM advanced settings REF: *VCP6-DCV Cert Guide* page 606

Tune Virtual Machine disk controller configurations according to a deployment plan

Configure .vmx file for advanced configuration scenarios

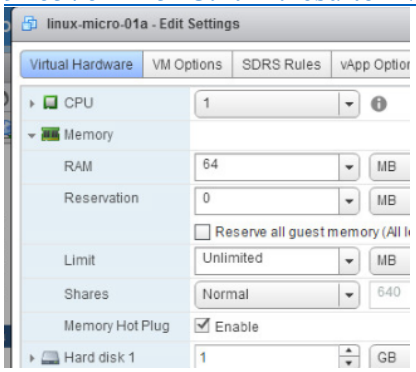
REF: *VCP6-DCV Cert Guide* page 610

Configure a virtual machine for Hot Add features

CPU and Memory Hot-add REF: *VCP6-DCV Cert Guide* page 606

- power off the VM
- edit the VM
- on Virtual Hardware tab, select CPU Hot Plug and Memory Hot Plug check boxes

Ref: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.vm_admin.doc/GUID-223C31D1-181D-4E3B-99EA-9165764A151C.html?resultof=%22%68%6f%74%2d%61%64%64%22%20



Upgrade virtual machine hardware and VMware Tools

upgrade vmware tools: REF: *VCP6-DCV Cert Guide* page 271

To automatically upgrade VMware Tools, the virtual machine must be powered on, and the guest OS must be running. You can determine whether the VM is running the latest version of VMware Tools by viewing the Summary tab of the virtual machine (see Figure 7-10). If VMware Tools needs to be upgraded, you see the message ***Automatic Tools Upgrade****, which you can click to open up a window to begin the process. The Advanced Options text box allows you to add options to the VMware Tools Upgrade. For example, if you want to perform a silent upgrade of VMware Tools for a Windows operating system, you could enter the following in the Advanced Options text box:*

/s /v “qn” /l “c:\windows\filename.log”

Configure VM to automatically upgrade VMware Tools: REF: http://bit.ly/2f8N4Ue

Schedule a Compatabilty Upgrade for a Single VM: REF: http://bit.ly/2fDXOOl

Troubleshoot virtual machine deployment issues

Section 2 - Deploy and Manage a vSphere 6.x Storage Infrastructure

Mark SSD as capacity:
use `esxcli storage core device list` to identify the device name of flash drive (look for property: Is SSD = true) and use the device name in this command

```
esxcli vsan storage tag add -d <device name> -t capacityFlash
```

Ref: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.virtualsan.doc/GUID-42E65085-1DA5-4C0B-A397-3497CBBC600E.html?resultof=%22%74%61%67%22%20%22%73%73%64%22%20

Mark a drive as flash:

- In the vSphere Web Client, select the vSAN cluster
- Manage > Setings > Virtual SAN > Disk Management
- Select an ESXi host to view its available devices
- In the **Show** drop down box, **Select Not in Use**. (to view drives that are not currently used)
- Select a drive and click the **Mark the selected disks as flash disks** icon
- Click **Yes**

REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.virtualsan.doc/GUID-DFE6A79D-1043-47A8-9F17-ABCA1729AEED.html

Objective 2.1 - Implement Complex Storage Solutions

Determine use cases for Raw Device Mapping
REF: *VCP6-DCV Cert Guide* page 233

Apply storage presentation characteristics according to a deployment plan:

VMFS re-signaturing

VMFS resignature https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.storage.doc/GUID-EEFEB765-A41F-4B6D-917C-BB9ABB80FC80.html?resultof=%22%72%65%73%69%67%6e%61%74%75%72%65%22%20%22%72%65%73%69%67%6e%61%74%75%72%22%20

LUN masking using PSA-related commands

REF: VCP6-DCV Cert Guide page 211

Unmask Paths: REF: http://bit.ly/2eBygTn

Mask Paths: REF: http://bit.ly/2f4Emvd

List existing claim rules and identify available rule numbers:

esxcli storage core claimrule list

rule numbers 0 through 100 are reserved for VMware use

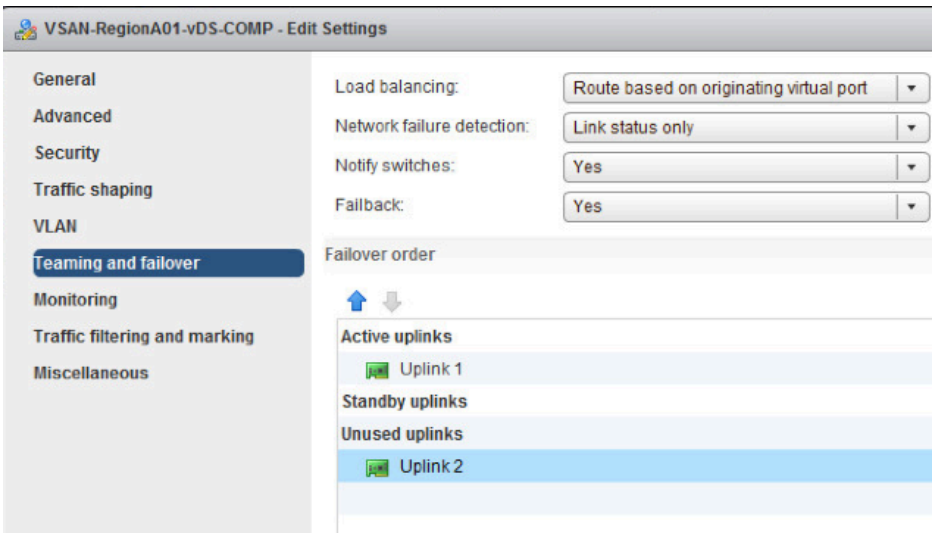
Example: create a rule to mask LUN 20 on target T2 accessed via vmhba3

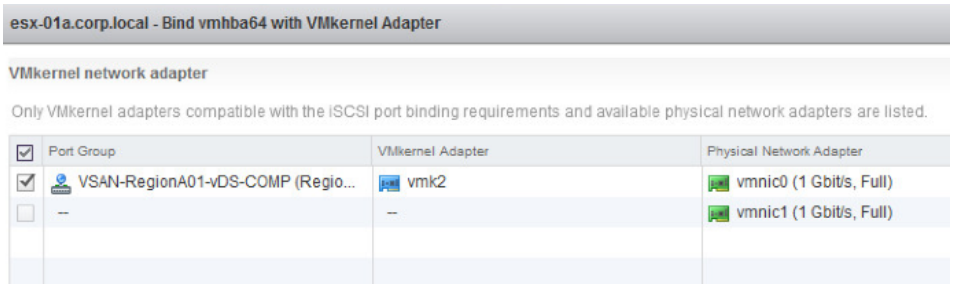
```
esxcli --server=server_name storage core claimrule add -P
MASK_PATH -r 112 -t location -A vmhba3 -C 0 -T 2 -L 20

esxcli storage core claimrule load

esxcli storage core claimrule list

esxcli storage core claimrule run
```

Create / Configure multiple VMkernels for use with iSCSI port binding

iSCSI binding for two vmk vNICs REF: *VCP6-DCV Cert Guide* page 179

iSCSI Binding may not be available if you have not configured the associated port group(s) (where the associated vmkernel virtual adapter is connected) with a single Active uplink.





Configure / Manage vSphere Flash Read Cache

vFlash REF: *VCP6-DCV Cert Guide* page 301, 310

- Ensure that one or more flash drives are identified as Virtual Flash resources on the ESXi hosts. (right-click the host, click Storage > Add Virtual Flash Resource Capacity)
- After a host is configured with virtul flash resources, those resources can be used for VM read cache and host swap cache:
    - Configure for VM Read Cache:
        - Verify the VM is compatablie with ESXi 5.5 or later
        - Edit the settings for a VM, Virtual Hardware > Hard disk
        - Set a value (GB) in the **Virtual Flash Read Cache**
        - Click the **Advanced** link next to Virtual Flash Read Cache
        - Check the **Enable Virtual Flash Read Cache**
        - Set a **Reservation** (GB) **and Block Size** (KB). Click **OK**.
    - Configure for host swap cache

Create / Configure Datastore Clusters

Create Datastore Clusters: REF: http://bit.ly/2eOihAT

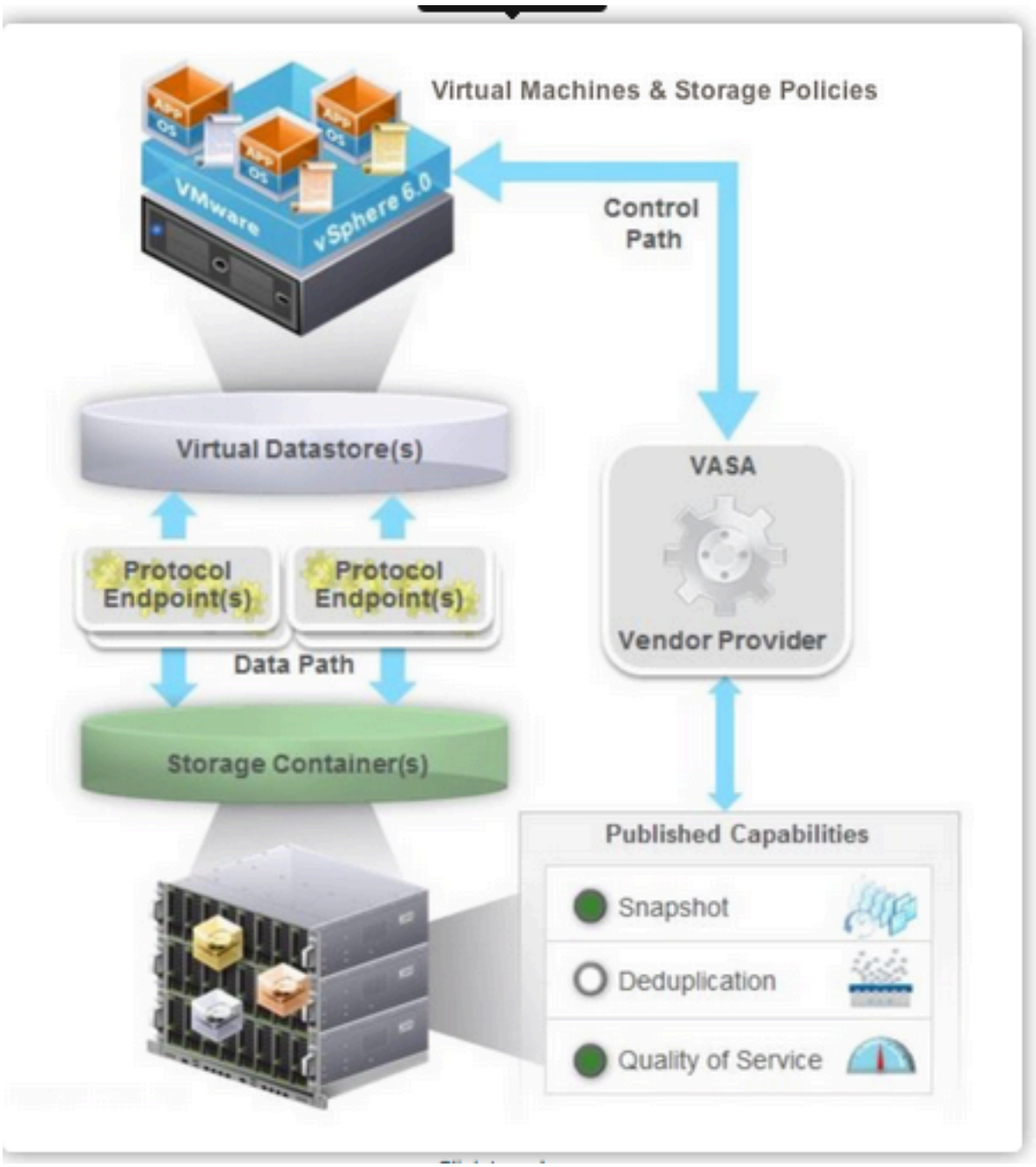
- Home > Storage
- Right-click a datacenter, select **Storage** > **New Datastore Cluster**
- In the wizard, provide a cluster name and select **Turn ON Storage DRS**
- Configure SDRS settgins

Troubleshoot SDRS datastore clusters: REF: *VCP6-DCV Cert Guide* page 414

Upgrade VMware storage infrastructure

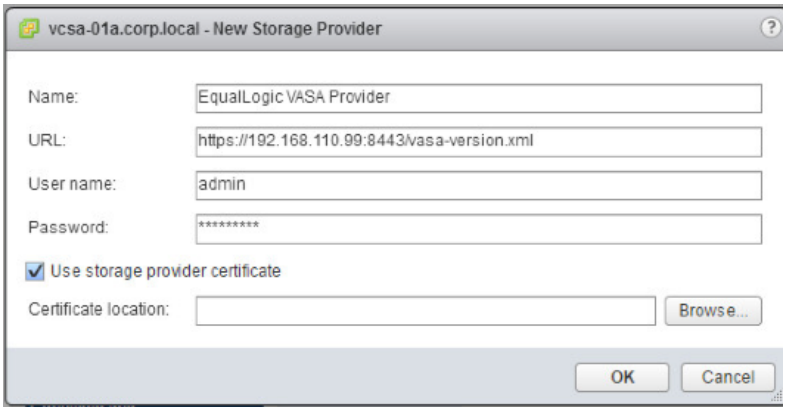
Deploy virtual volumes

VMWare Hands on Labs: HOL-1708-SDC-2 Virtual Volumes



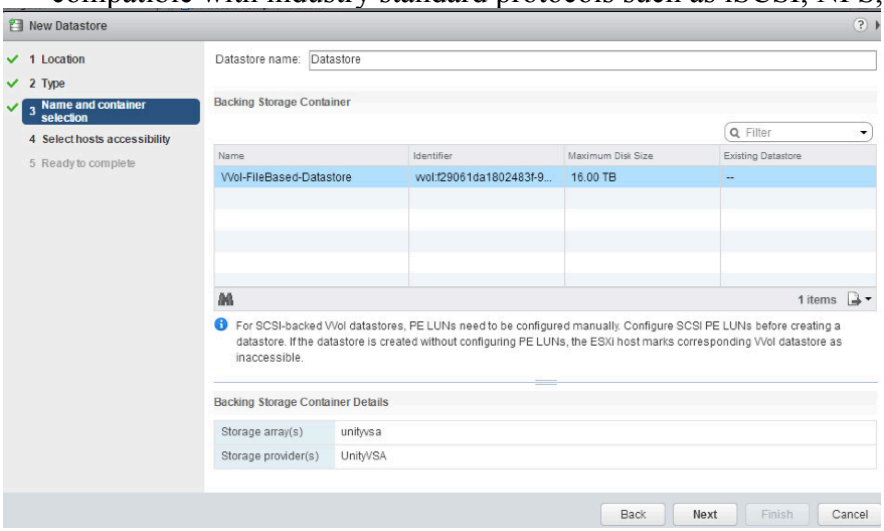
deploy virtual volumes REF: *VCP6-DCV Cert Guide* page 196, 201

- Register the storage provider

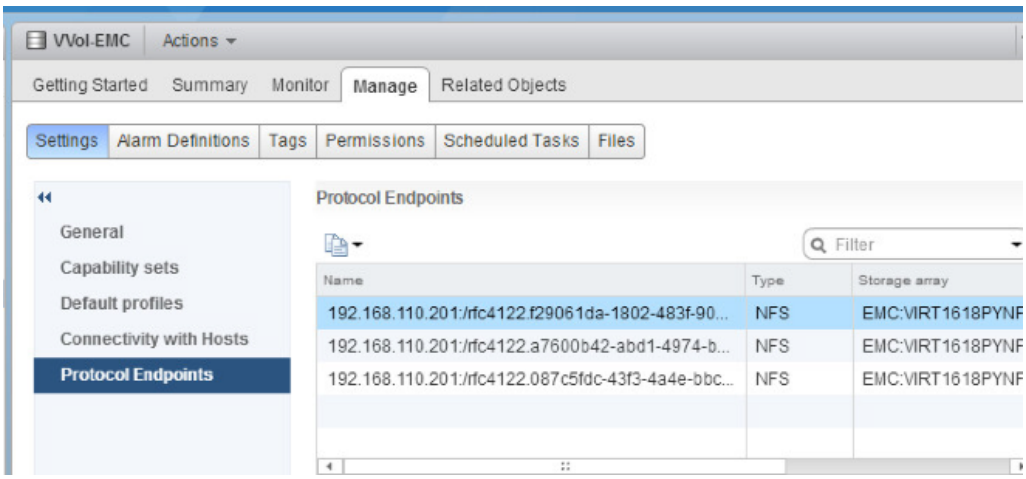


- Create a vvol datastore (map a datastore name to a storage container)
    - Right-click on a host cluster or data center object, select **Storage** > **New Datastore**

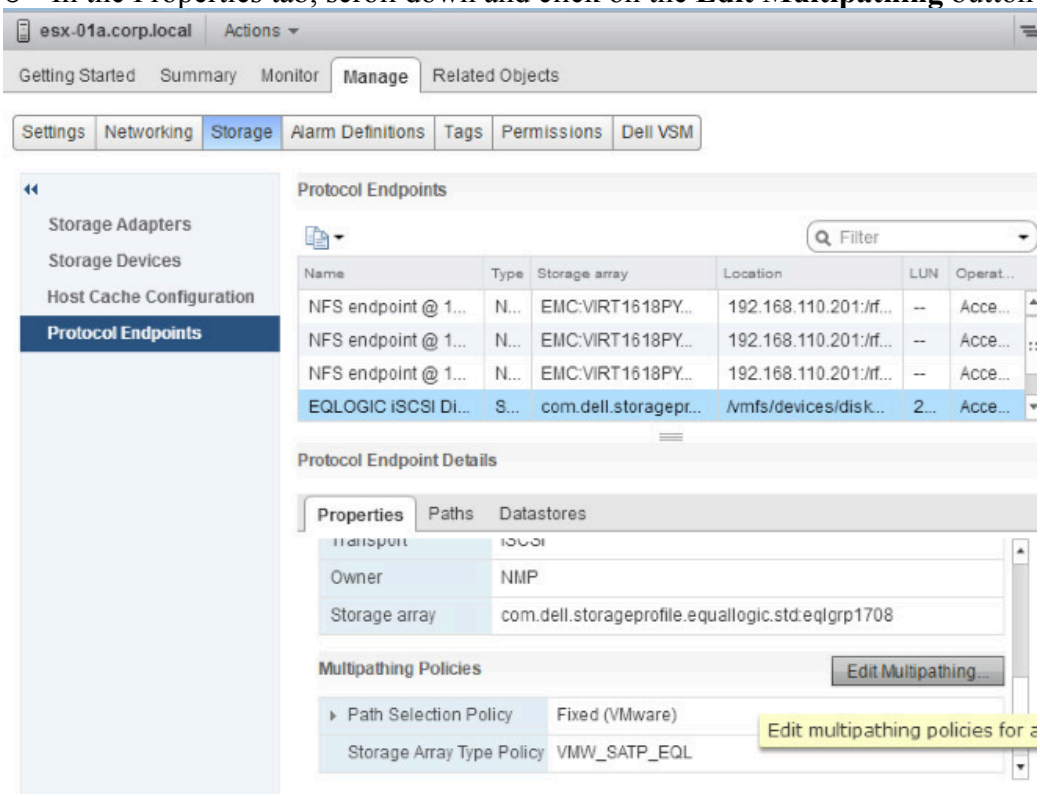
    - In the wizard, select VVOL and select the desired storage container (from the list of containers that are automatically detected. This implies that the storage container was already created in the storage system and presented to vCenter via the storage provider. (The storage container is a logical pool of raw storage, in the storage system.) This also implies the storage administrator configured the Protocol Endpoints, which are logical I/O proxies that are used by the ESXI hosts because hosts do not have direct access to the virtual volumes. PEs are compatible with industry standard protocols such as iSCSI, NFS, FC, and FCoE.)



    - Select the ESXi hosts to which the datastore will be presented
- View the auto assigned protocol endpoints (one or more PEs are pre-configured and assigned by storage system)
    - **Home** > **Storage**, select the VVOL based datastore
    - **Manage** > **Settings** > **protocol endpoints**



- Configure storage multipath policies to PEs (such as Round Robin)
    - Dill to and select the ESXi host
    - **Manage** > **Storage** > **Protocol Endpoints**
    - Select the desired endpoint
    - In the Properties tab, scroll down and click on the **Edit Multipathing** button



create a virtual volume REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.storage.doc/GUID-0CAD6480-5414-4287-9007-51A1E4635E97.html?resultof=%22%76%69%72%74%75%61%6c%22%20%22%76%6f%6c%75%6d%65%22%20%22%76%6f%6c%75%6d%22%20

commands to manage virtual volumes REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vcli.examples.doc/cli_manage_storage.6.13.html?resultof=%22%76%69%72%74%75%61%6c%22%20%22%76%6f%6c%75%6d%65%22%20%22%76%6f%6c%75%6d%22%20

- `esxcli storage vvol vendorprovider list`
- `esxcli storage vvol protocolendpoint list`
- `esxcli storage vvol storagecontainer list`

Deploy and configure VMware Virtual SAN

VMWare Hands on Labs: HOL-1708-SDC-1 – Virtual SAN 6.2 from A to Z

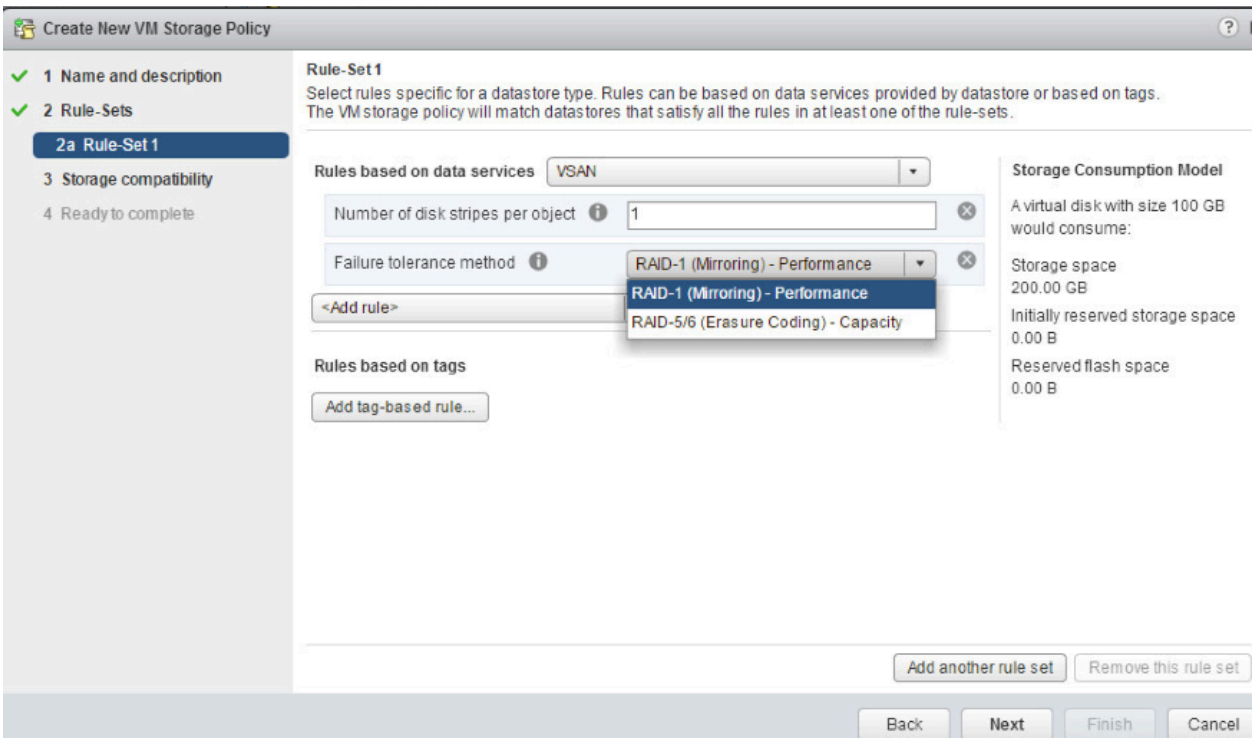
Configure vSAN REF: *VCP6-DCV Cert Guide* page 197

- configure a distributed switch port group and vmkernel virtual adapters, with VSAN service enabled, on each ESXi host that is connected to the VSAN network (such as a dedicated VLAN)
- Enable vsan on cluster (at least 3 hosts in the cluster, or 2 hosts in cluster and a witness appliance on a separate host)
- Automatically or manually assign disks to VSAN
- Create disk groups (1 SSD, up to 7 HDD per group) (at least one SSD for cache, at least one SSD / HDD for capacity)

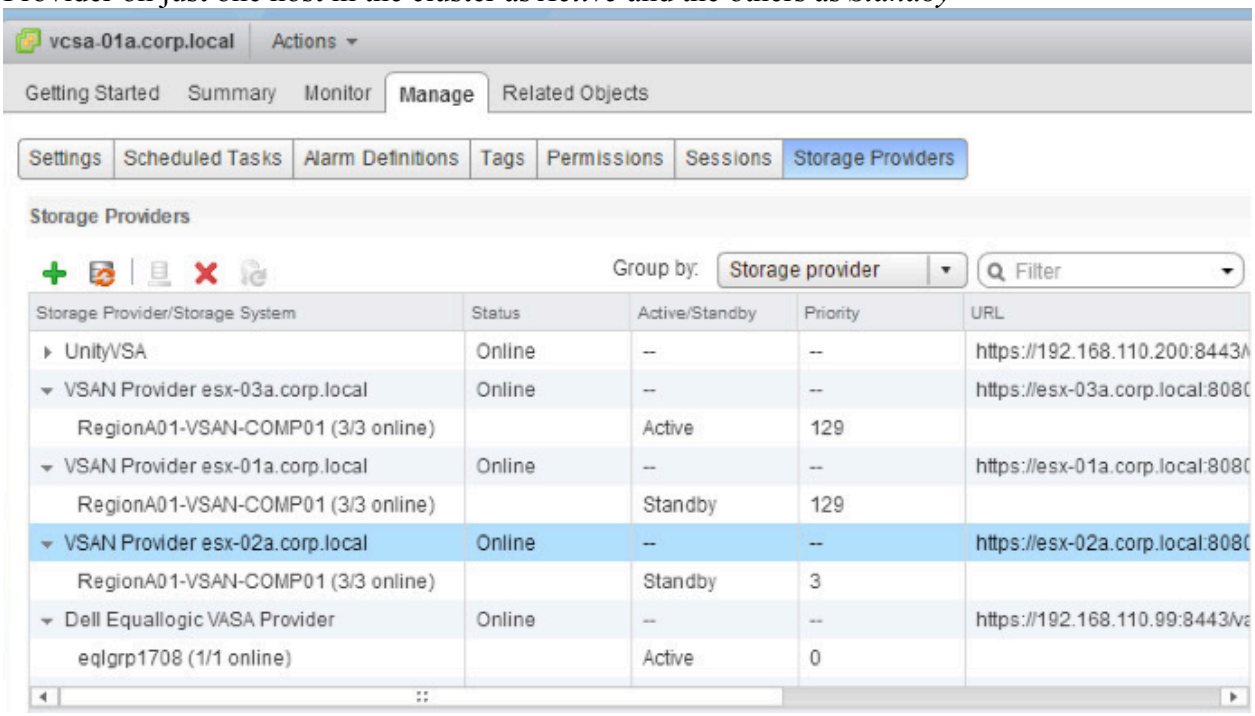
Create vsan fault domains (subsets of hosts) REF: *VCP6-DCV Cert Guide* page 203

Custom vSan storage policy REF: *VCP6-DCV Cert Guide* page 202

- **Home** > **Policies and Profiles** > **VM Storage Policies**
- **Create a New VM Storage Policy**
- Choose **Rules based on data services**: *VSAN*
- Add rules for stripes, ft method, etc



In a VSAN datastore, Manage > Storage Providers, you should expect to see the VSAN Provider on just one host in the cluster as *Active* and the others as *Standby*



Sizing vsan REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.virtualsan.doc/GUID-07EFD36A-F844-4E7D-830D-

3863E4AA617C.html?resultof=%22%76%69%72%74%75%61%6c%22%20%22%73%61%6e%22%20%22%73%63%61%6c%65%22%20

Fault Tolerance Method: Perfomance (RAID-1) or Capacity (RAID-5 / 6)
You can configure RAID 5 on all-flash clusters with four or more fault domains. You can configure RAID 5 or RAID 6 on all-flash clusters with six or more fault domains. RAID 5 or RAID 6 erasure coding requires less additional capacity to protect your data than RAID 1 mirroring. For example, a VM protected by a Number of failures to tolerate value of 1 with RAID 1 requires twice the virtual disk size, but with RAID 5 it requires 1.33 times the virtual disk size. RAID-5 method requires a minimum of 4 hosts. RAID-6 method requires a minimum of 6 hosts.

In VSAN 6.2, a new advanced host option SwapThickProvisionDisabled has been created to allow the VM swap option to be provisioned as a thin object

Configure / View VMFS locking mechanisms

ATS-Only mechanism

Get vaai (ATS) status REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.storage.doc/GUID-0520FD37-D7AD-4FBA-9A2E-E5F8211FCBBB.html?resultof=%22%76%61%61%69%22%20

esxcli --server=server_name storage core device vaai status get -d=*device_ID*

```
[root@esx-01a:~] esxcli storage core device vaai status get -d=naa.6589cfc000000cfd9bc58d680c24402e
naa.6589cfc000000cfd9bc58d680c24402e
   VAAI Plugin Name:
   ATS Status: supported
   Clone Status: supported
   Zero Status: supported
   Delete Status: supported
```

ATS_SCSI mechanism

Change to ATS SCSI REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.storage.doc/GUID-6887003D-2322-49AC-A56C-7AFE7350DB5D.html?resultof=%22%61%74%73%22%20%22%61%74%22%20%22%73%63%73%69%22%20

List VMFS extents:

```
[root@esx-01a:~] esxcli storage vmfs extent list
Volume Name                VMFS UUID                            Extent Number  Device Name                              Partition
-------------------------  -----------------------------------  -------------  ---------------------------------------  ---------
RegionA01-ISCSI01-COMP01   5727fe90-1aaae6f7-7179-005056018fc3              0  naa.6589cfc000000cfd9bc58d680c24402e          1
```

List lockmode settings for VMFS extents:

```
[root@esx-01a:~] esxcli storage vmfs lockmode list
Volume Name                UUID                                 Type    Locking Mode           ATS Compatible  ATS Upgrade Modes  ATS Incompatibi
lity Reason
-------------------------  -----------------------------------  ------  ---------------------  --------------  -----------------  ---------------
-----------
RegionA01-ISCSI01-COMP01   5727fe90-1aaae6f7-7179-005056018fc3  VMFS-5  ATS DOWNGRADE PENDING            true  Online/Offline
```

Set ATS to SCSI using the VMFS label:

```
esxcli storage vmfs lockmode set -s -l=RegionA01-ISCSI01-COMP01
```

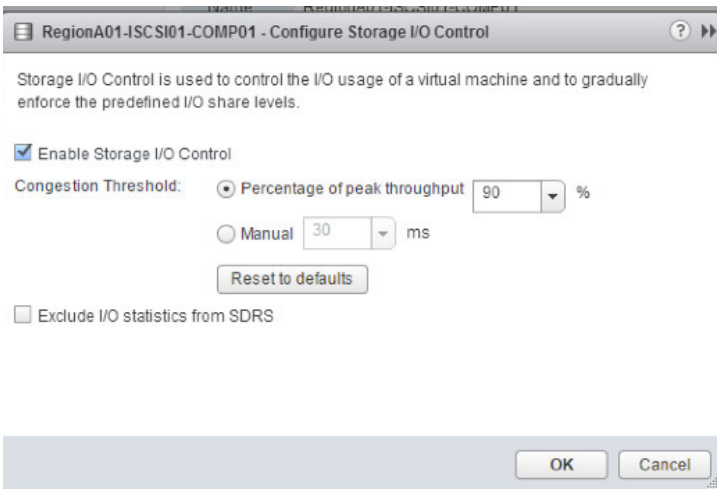
Set ATS to SCSI using the UUID

```
esxcli storage vmfs lockmode set -s -u=5727fe90-1aaae6f7-7179-005056018fc3
```

Configure Storage I/O Control to allow I/O prioritization

REF: *VCP6-DCV Cert Guide* page 246

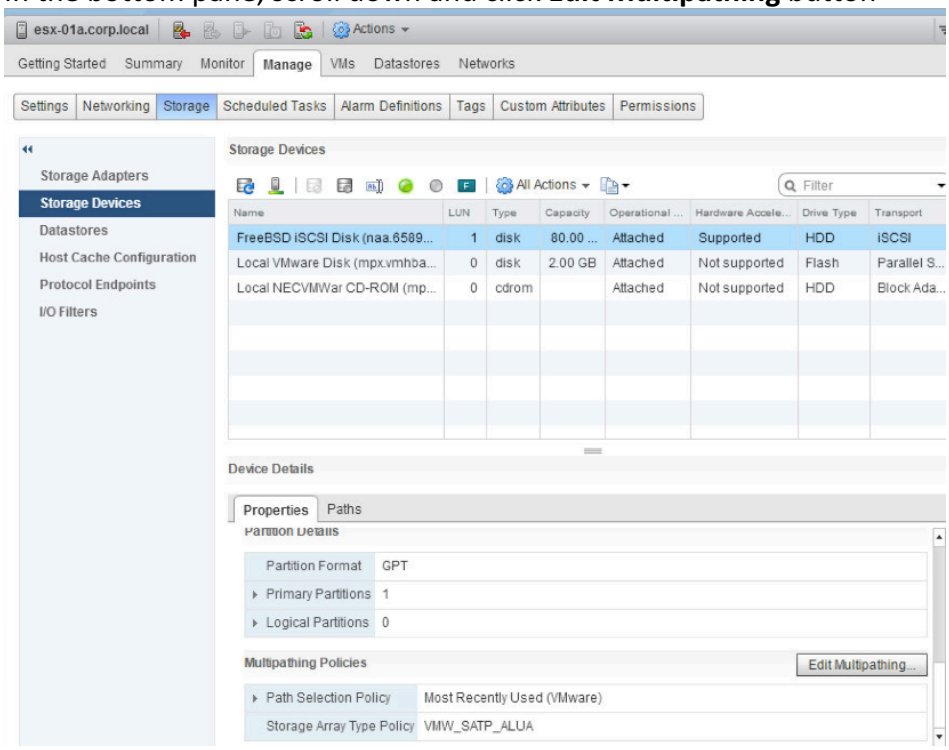
- In vSphere Web Client, select the datastore
- Click **Manager** > **Settings** > **General**
- In **Datastore Capabilities**, click the Edit button
- Check the **Enable Storage I/O Control** check box and configure settings

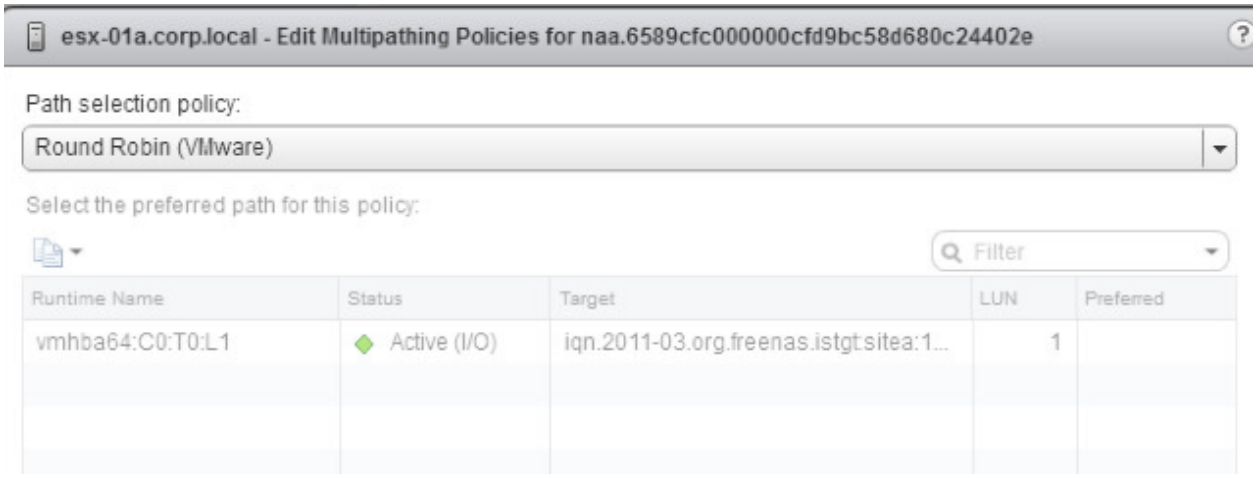


Configure Storage Multi-pathing according to a deployment plan

REF: *VCP6-DCV Cert Guide* page 213

- Select an ESXi host
- Click **Manage** > **Settings** > **Storage** > **Storage Devices**
- Select a storage device
- In the bottom pane, scroll down and click **Edit Multipathing** button



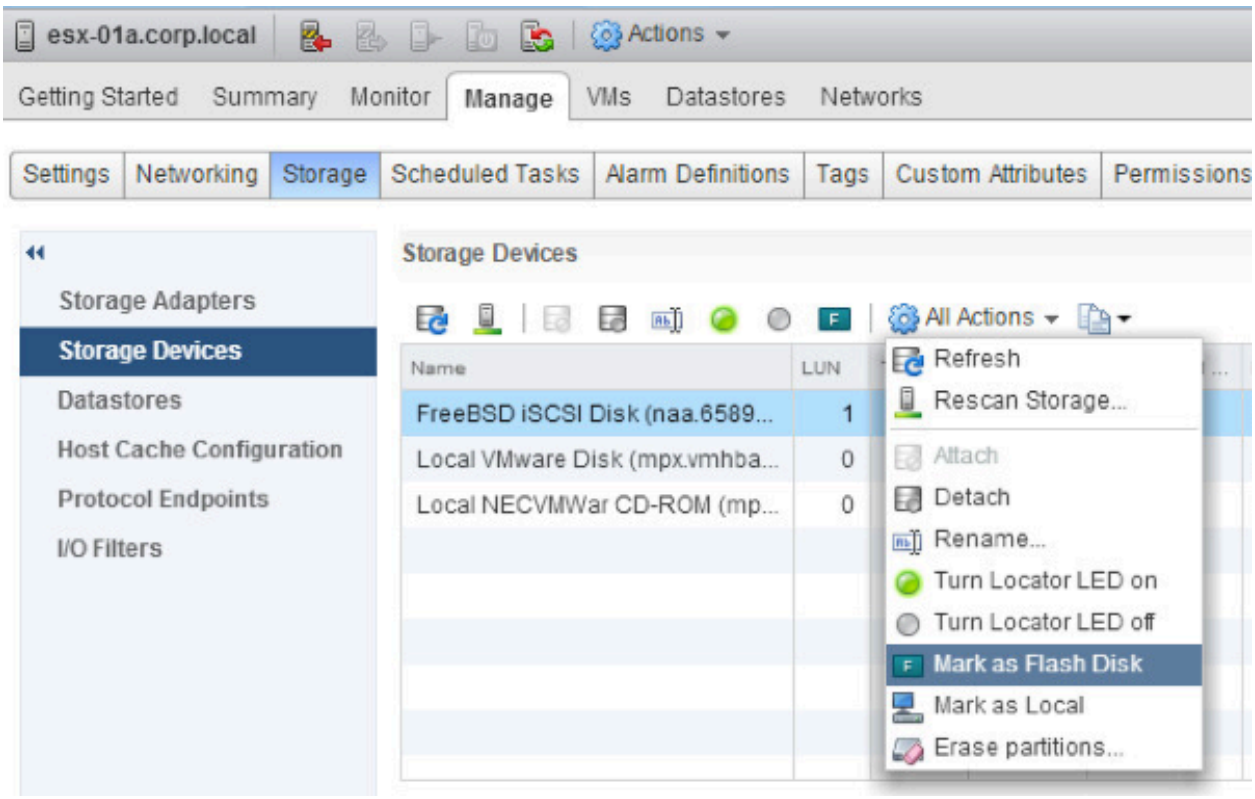


set multipathing using commands: REF: *VCP6-DCV Cert Guide* page 244

Objective 2.2 - Manage Complex Storage Solutions

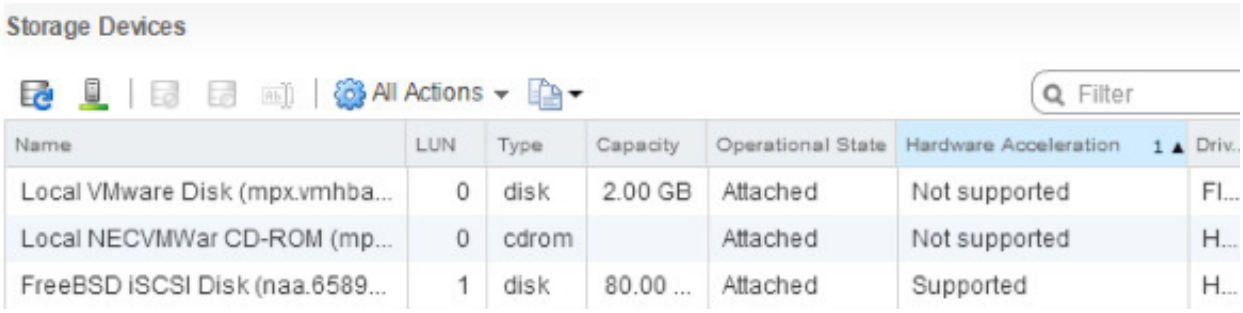
Identify and tag (mark) SSD and local devices

- Select an ESXi host
- Click **Manage** > **Settings** > **Storage** > **Storage Devices**
- Select a storage device
- Click **All Actions** > **Mark as Flash Disk** or select Mark as Local



Administer hardware acceleration for VAAI

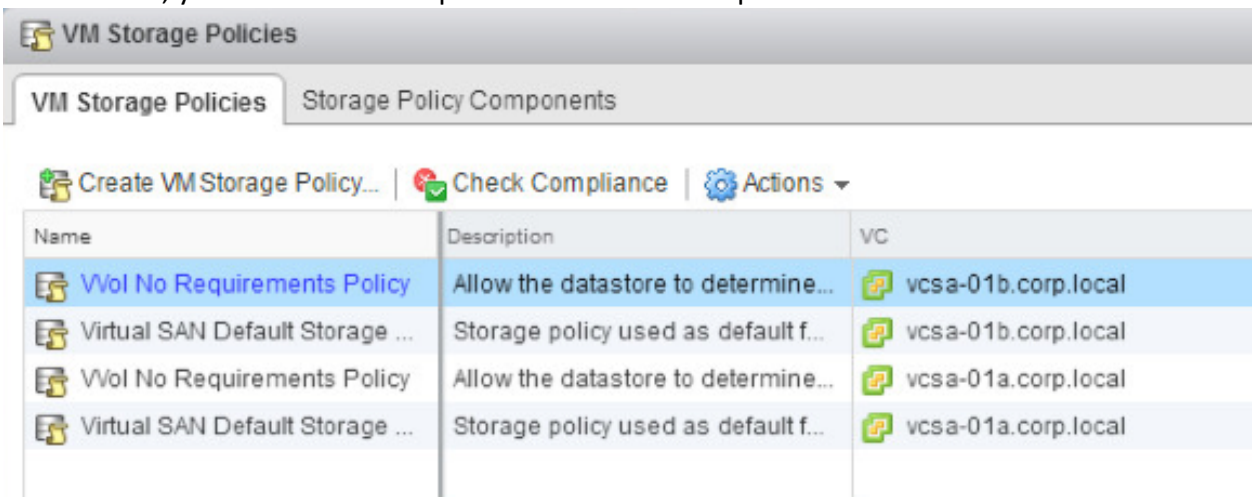
In the list of stoage devices, examine the Hardware Acceleration column for each device



Configure, administer, and apply storage policies

- **Home** > **VM Storage Policies**

- Here, you can create new policies and check compliance



Manage storage policies REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.storage.doc/GUID-85A1164B-09B4-430E-9DBF-FFC694C18C3E.html?resultof=%22%73%74%6f%72%61%67%65%22%20%22%73%74%6f%72%61%67%22%20%22%70%6f%6c%69%63%22%20

Prepare storage for maintenance

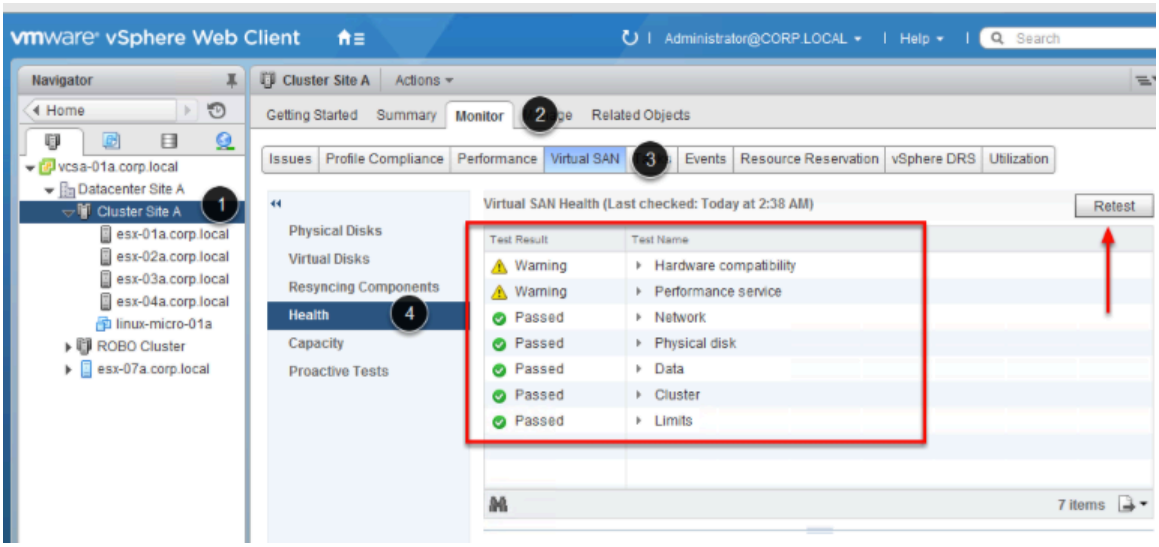
Right-click the datastore, click **Mantenance Mode > Enter Maintenance Mode**

Apply space utilization data to manage storage resources

Provision and manage storage resources according to Virtual Machine requirements

Configure datastore alarms, including Virtual SAN alarms

VSAN alarms REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.virtualsan.doc/GUID-BA67B6CA-9185-410A-AC35-F45985AE3595.html?resultof=%22%76%69%72%74%75%61%6c%22%20%22%73%61%6e%22%20%22%61%6c%61%72%6d%22%20



Expand (Scale up / Scale Out) Virtual SAN hosts and diskgroups

REF: http://bit.ly/2flcPkh

Add host to VSAN cluster REF: http://bit.ly/2gG8BJF

Add devices to a disk group: REF: http://bit.ly/2f2mxwp

Objective 2.3 - Troubleshoot Complex Storage Solutions

Analyze and resolve storage multi-pathing and failover issues

Manage storage paths and multipath plugins: REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.storage.doc/GUID-9B19EF2E-DA5A-43D2-B41F-8E7C112D2E00.html

- Display multipath modules
- List Multipath claim rules
- Delete Multipath claim rules
- Add Multipath claim rules
- Mask / Unmask paths
- Display SATPs

Troubleshoot storage device connectivity

Analyze and resolve Virtual SAN configuration issues

Troubleshoot VSAN REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.virtualsan.doc/GUID-440A7F88-1F7F-415F-949E-AFD7BA37035E.html?resultof=%22%74%72%6f%75%62%6c%65%73%68%6f%6f%74%22%20%22%76%69%72%74%75%61%6c%22%20%22%73%61%6e%22%20

Troubleshoot iSCSI connectivity issues

Verify proper associated settings:

- Vmkernel virtual adapter on the ESXi host (proper IP settings and virtual port group configuration)
- iSCSI software adapter configuration
    - adapter is activated
    - iSCSI adapter name (IQN)
    - Bind iSCSI adapter to vmkernel virtual adapters REF: http://bit.ly/2gcaiK2
    - dynamic target configuration (IP address, port) REF: http://bit.ly/2gceWrj
- CHAP configuration REF: http://bit.ly/2gGfVFd

- iSCSI Network troubleshooting: REF: http://bit.ly/2gggW3p

Analyze and resolve NFS issues

Primarily, double-check all the NFS related settings:

- vmkernel virtual adapter (proper IP settings, virtual port group settings)
- IP (or hostname) of NFS server and folder name used to connect to the NFS datastore

Create an NFS datastore: REF: http://bit.ly/2g3nosO

- Prerequisites:
  - prepare a vmkernel virtual adapter on each ESXi host that can reach the NFS target via the network
  - The storage admin should prepare the NFS share and grant access
- Select the host, click Manage > Related Objects > Datastore
- Click the Create New Datastore button
- Choose NFS, select a version (3 or 4.1), provide the IP, folder name, etc

Failure to mount NFS datastore: REF: https://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.troubleshooting.doc/GUID-5850A6B6-E266-47A9-A8E5-27C9CC09D0F5.html?resultof=%2522%256e%2566%2573%2522%2520%2522%256e%2566%2522%2520

Troubleshoot RDM issues

Section 3 - Deploy and Manage a vSphere 6.x Network Infrastructure

Objective 3.1 - Implement and Manage vSphere Standard Switch (vSS) Networks

Create and manage vSS components according to a deployment plan:

VMkernel ports on standard switches

Advanced vSS settings

Advanced settings include: REF: http://bit.ly/2fnal86

- MTU
- Failover groups

Configure TCP/IP stack on a host

First, create the custom stack using command line, then it becomes usable in vSphere Web Client.

custom tcp stack

- Create: REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.networking.doc/GUID-660423B1-3D35-4F85-ADE5-FE1D6BF015CF.html?resultof=%22%74%63%70%22%20%22%73%74%61%63%6b%22%20

```
esxcli network ip netstack add -N="stack_name"
```

- Monitor REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.html.hostclient.doc/GUID-703A1489-C367-417C-B80D-3029C704AA1D.html?resultof=%22%74%63%70%22%20%22%73%74%61%63%6b%22%20
- Change REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.networking.doc/GUID-D4AF4F9F-F274-4ADE-98F4-1CB44ABCC505.html?resultof=%22%74%63%70%22%20%22%73%74%61%63%6b%22%20

Create a custom TCP/IP stack

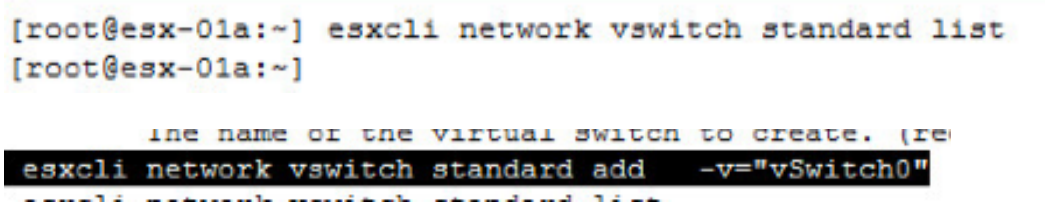
After creating a custom stack using a command, configure it in the vSphere Web Client. Select the host and click **Manage > Networking > TCP/IP Configuration**

If the new stack does not yet appear, refresh the page. It should appear under Custom Stacks. Select the stack and click the edit (pencil) button. Provide:

- Name
- Dns settings
- Routing
- advanced

Configure and analyze vSS settings using command line tools

esxcli network vswitch standard REF: *VCP6-DCV Cert Guide* page 375



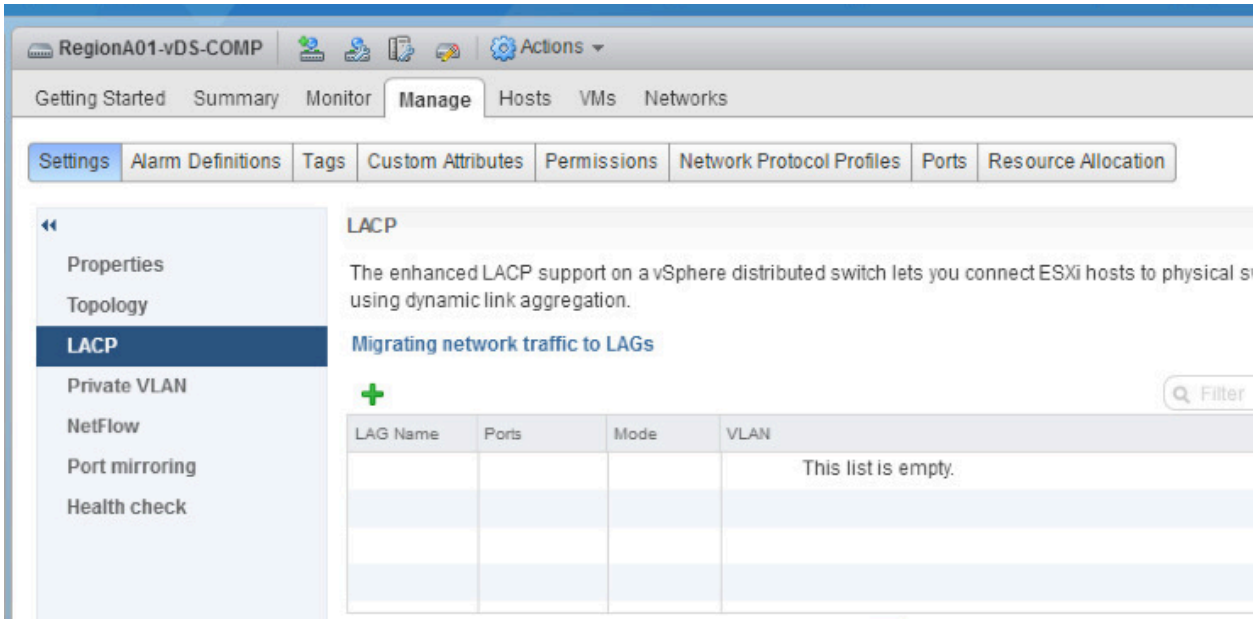
```
[root@esx-01a:~] esxcli network vswitch standard list
vSwitch0
   Name: vSwitch0
   Class: etherswitch
   Num Ports: 1536
   Used Ports: 1
   Configured Ports: 128
   MTU: 1500
   CDP Status: listen
   Beacon Enabled: false
   Beacon Interval: 1
   Beacon Threshold: 3
   Beacon Required By:
   Uplinks:
   Portgroups:
```

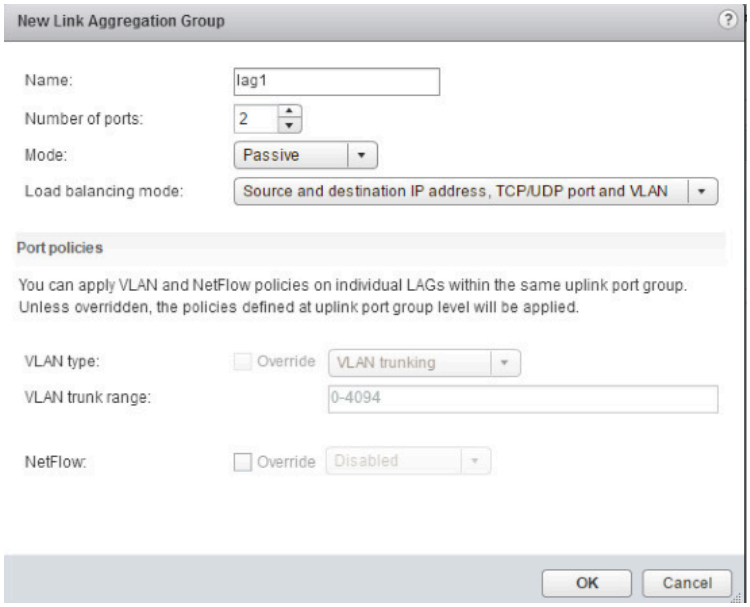
Objective 3.2 - Implement and Manage vSphere 6.x Distributed Switch (vDS) Networks

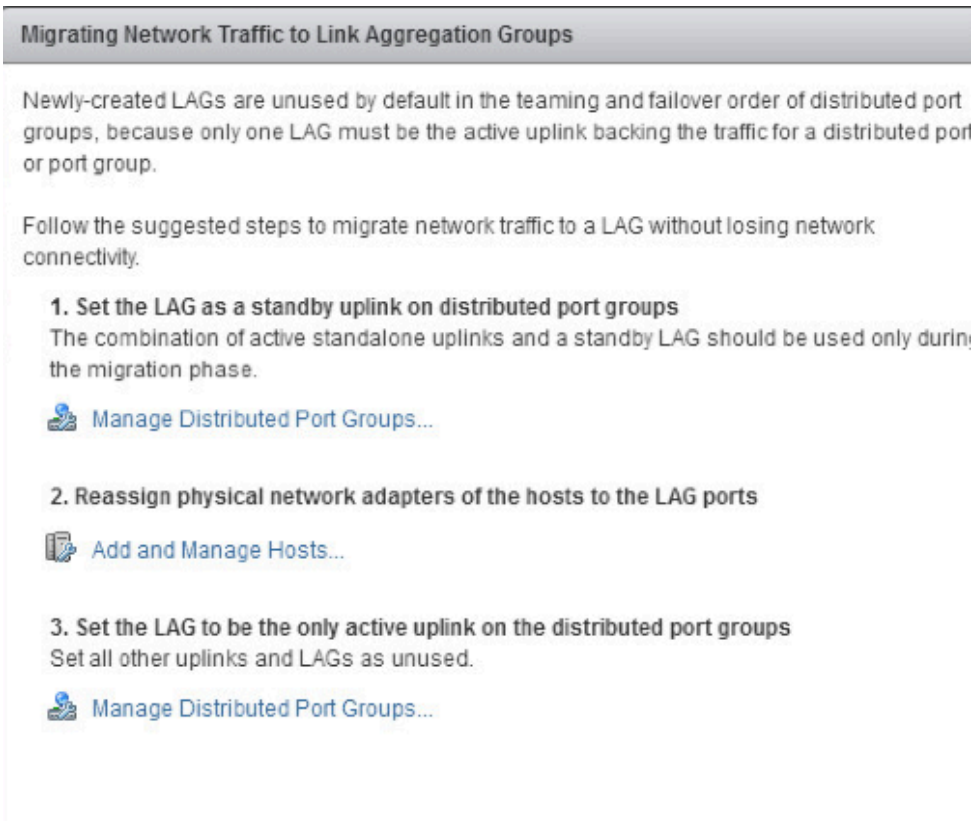
Deploy a LAG and migrate to LACP

REF: *VCP6-DCV Cert Guide* page 101

- Select a distributed switch, click **Manage** > **Settings** > **LACP**
- Click the Green plus **(+)** sign to create a LAG
- Click the **Migrating network traffic to LAGs** link
- As directed:
    - Set the LAG as standby on the distributed port group
    - Re-assign the hosts' physical NICs to the LAG
    - Set the LAG as the `Active` on the port group

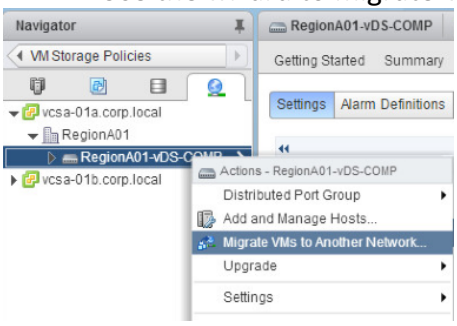

RegionA01-vDS-COMP
Actions
Getting Started
Summary
Monitor
Manage
Hosts
VMs
Networks
Settings
Alarm Definitions
Tags
Custom Attributes
Permissions
Network Protocol Profiles
Ports
Resource Allocation
Properties
Topology
LACP
Private VLAN
NetFlow
Port mirroring
Health check
LACP
The enhanced LACP support on a vSphere distributed switch lets you connect ESXi hosts to physical s
using dynamic link aggregation.
Migrating network traffic to LAGs
Filter
LAG Name
Ports
Mode
VLAN
This list is empty.


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 NetFlow policies on individual LAGs within the same uplink port group.
Unless overridden, the policies defined at uplink port group level will be applied.
VLAN type:
Override
VLAN trunking
VLAN trunk range:
0-4094
NetFlow:
Override
Disabled
OK
Cancel



Migrate a vSS network to a hybrid or full vDS solution

- Right-click the dv swith and select **Migrate VMs to Another Network**
- Use the wizard to migrate VMs and vmk ports on a standard vswtich to the dvSwitch



Analyze vDS settings using command line tools

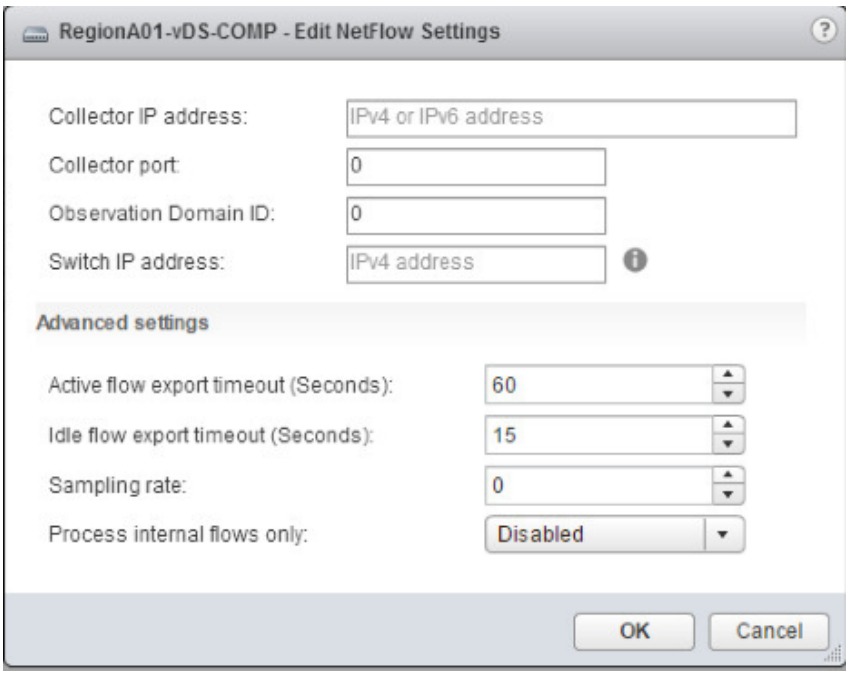
esxcli network vswitch dvs vmware REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vcli.examples.doc/cli_manage_networks.11.6.html?resultof=%22%65%73%78%63%6c%69%22%20%22%6e%65%74%77%6f%72%6b%22%20%22%76%73%77%69%74%63%68%22%20%22%64%69%73%74%72%69%62%75%74%65%64%22%20%22%64%69%73%74%72%69%62%75%74%22%20

```
[root@esx-01a:~] esxcli network vswitch  dvs vmware list
RegionA01-vDS-COMP
   Name: RegionA01-vDS-COMP
   VDS ID: 50 37 c1 cc 33 27 28 8b-a7 a3 66 f2 9c e7 3a 53
   Class: etherswitch
   Num Ports: 1536
   Used Ports: 10
   Configured Ports: 512
   MTU: 1500
   CDP Status: listen
   Beacon Timeout: -1
   Uplinks: vmnic1, vmnic0
   VMware Branded: true
   DVPort:
         Client: vmnic0
         DVPortgroup ID: dvportgroup-14
         In Use: true
         Port ID: 32

         Client: vmnic1
         DVPortgroup ID: dvportgroup-14
         In Use: true
         Port ID: 33

         Client: vmk0
         DVPortgroup ID: dvportgroup-16
         In Use: true
```

Configure Advanced vDS settings (NetFlow, QOS, etc.)

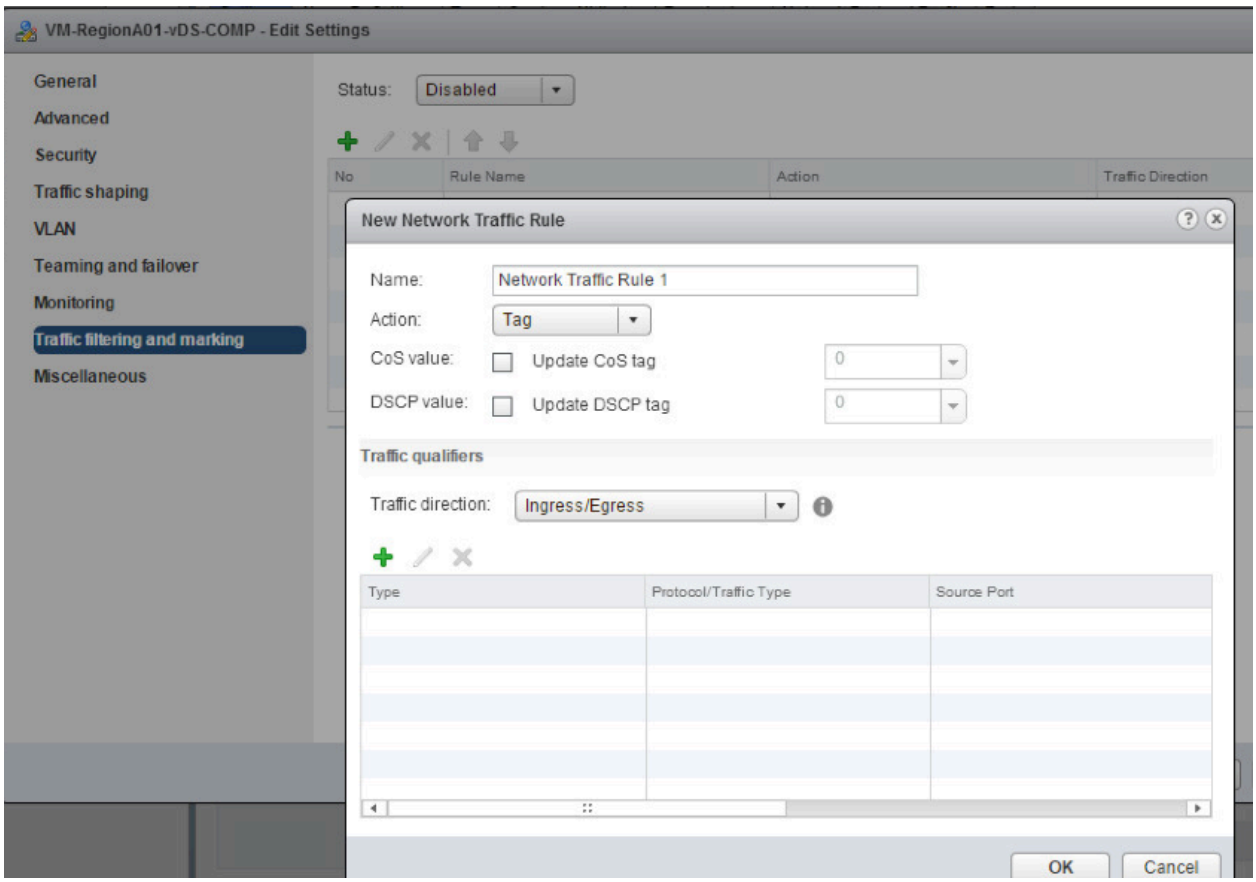
configure netflow REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.hostclient.doc/GUID-E19FECAD-8629-4E8A-B61C-1F1C16770B3B.html?resultof=%22%6e%65%74%66%6c%6f%77%22%20

- Select the dvSwitch
- Click **Manage** > **Settings** > **Netflow**
- Cliick **Edit** button
- Set the collector IP and port for the collector. Set the Switch IP address to vCenter IP or some designated IP that you arbitrary associate to the dvSwithc



QoS (System Traffic Qualifier):

- Configure on port group or uplink port group
- Edit the port group
- Select Traffic filtering and marking
- Set status = Enabled and add a Network Traffic Rule



REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.networking.doc/GUID-C47946DB-6FA6-48F5-A03C-087F69DE598C.html?resultof=%22%71%6f%73%22%20%22%71%6f%22%20
and
https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.networking.doc/GUID-67CA4C18-4F18-4E23-A5C7-BC33112D4433.html?resultof=%22%71%6f%73%22%20%22%71%6f%22%20

LLDP REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.hostclient.doc/GUID-FA7A38BA-002B-4AF0-B50A-9F371B2AF06A.html?resultof=%22%6c%6c%64%70%22%20

Determine which appropriate discovery protocol to use for specific hardware vendors

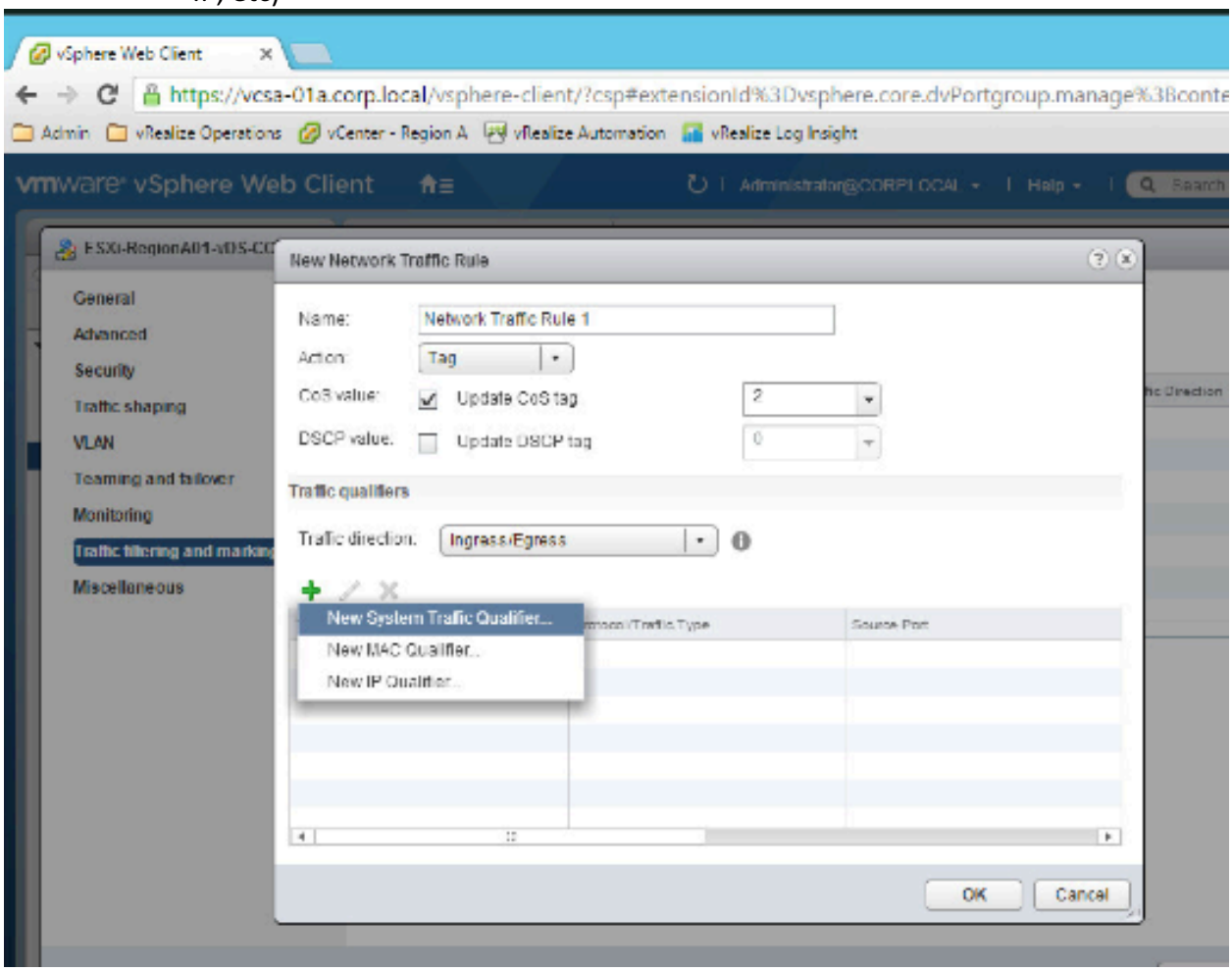
Configure VLANs/PVLANs according to a deployment plan

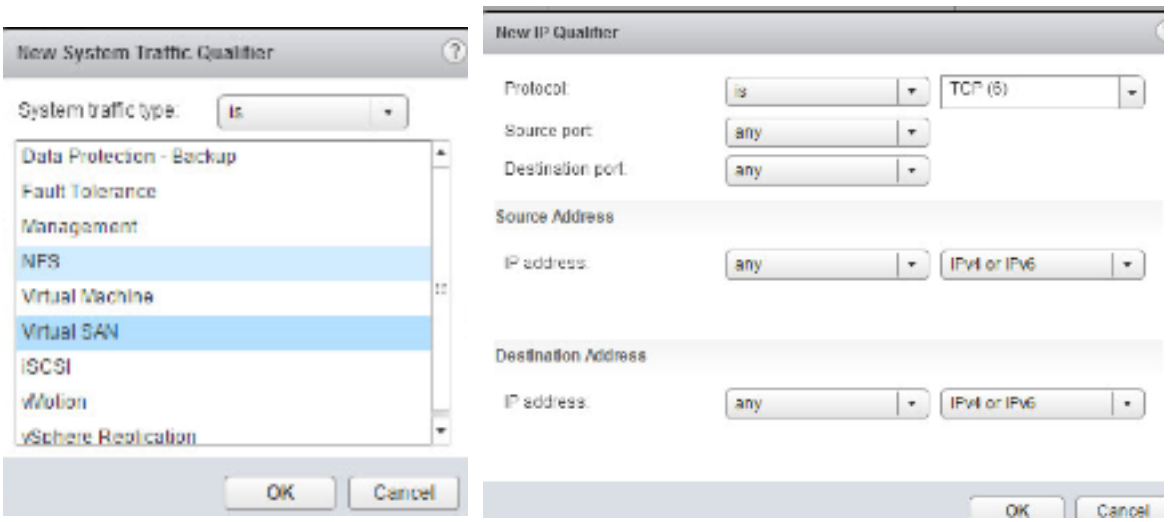
REF: *VCP6-DCV Cert Guide* page 114

Private VLANs REF: *VCP6-DCV Cert Guide* page 116

Create / Apply traffic marking and filtering rules

- Ref: http://bit.ly/2eWpxaZ
- Enable traffic filtering/ marketing
- Create a rule with action = Tag, configure CoS, directon and qualifiers (type, mac, IP, etc)





Objective 3.3 - Scale a vSphere 6.x Network Implementation

Configure appropriate NIC teaming failover type and related physical network settings

REF: *VCP6-DCV Cert Guide* page 66

- Port based
- Mac based
- IP Hash

Determine and apply failover settings according to a deployment plan

REF: *VCP6-DCV Cert Guide* page 113

Configure and manage network I/O control 3

NIOC REF: *VCP6-DCV Cert Guide* page 140

- Edit the dvSwitch settings
- in **General** settings, set **Network I/O Control** = *Enabled*
- select the dvSwitch, click **Manage** > **Resource Allocation tab**.
- Right-click on a traffic type (such as FT), set shares, reservation, limit

-

To create network resource pools, first set a reservation on Virtual Machine traffic. Set a reservation on the pool. Then modify one or more dvPortgroups and set its network resource pool.

Upgrade: right-click a dvSwitch and select Upgrade Distributed Switch or Upgrade Network IO Control

Determine and configure vDS port binding settings according a deployment plan

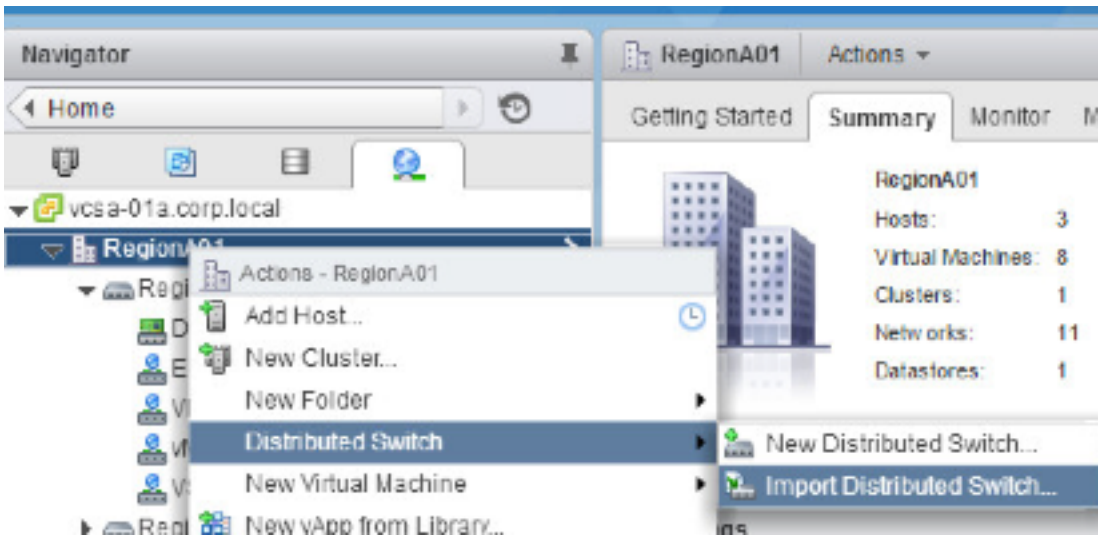
- Static
- Dynamic
- ephemeral

Objective 3.4 - Troubleshoot a vSphere 6.x Network Implementation

Distributed Switch:

- **import**: Right-click data center, select > Distirbuted Switch > Import Distributed Switch

  REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.networking.doc/GUID-092D0756-F57A-4327-BBA8-C53CD14EC824.html?resultof=%22%64%69%73%74%72%69%62%75%74%65%64%22%20%22%64%69%73%74%72%69%62%75%74%22%20%22%73%77%69%74%63%68%22%20



- **restore**
  Right-click on a dvSwitch and choose **Restore Configuration**
  REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.networking.doc/GUID-5D2CE5A7-0B56-4810-8885-9DEF3EC63CB5.html?resultof=%22%64%69%73%74%72%69%62%75%74%65%64%22%20%22%64%69%73%74%72%69%62%75%74%22%20%22%73%77%69%74%63%68%22%20

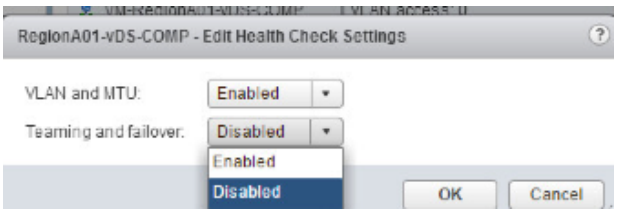
- **save (Export)**: right-click the dvSwitch, select **Settings** > **Export Configuration**
  REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.networking.doc/GUID-9B33EBCE-1BCC-4362-9BE5-4F477056B169.html?resultof=%22%64%69%73%74%72%69%62%75%74%65%64%22%20%22%64%69%73%74%72%69%62%75%74%22%20%22%73%77%69%74%63%68%22%20

Perform a vDS Health Check for teaming, MTU, mismatches, etc.

DVS health check

When enabled, the dvSwtich runs a health check again once per minute

Right-click a dvSwitch, select **Settings** > **Edit Health Check**



- Enable REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.networking.doc/GUID-6D155482-0743-4252-A8DC-3F608AB3654A.html?resultof=%22%68%65%61%6c%74%68%22%20%22%63%68%65%63%6b%22%20
- View REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.networking.doc/GUID-6396C307-AE1E-4FBA-AE6F-C9DB6AA59C76.html
-

Configure port groups to properly isolate network traffic

Configure VLAN and PVLAN settings on the port groups

PVLAN: REF: *VCP6-DCV Cert Guide* page 152

Use command line tools to troubleshoot and identify configuration issues

REF: *VCP6-DCV Cert Guide* page 372

Deploy vMA from OVF. This error represents the lack of a trust relationship

```
Connect to server-01.mydomain.com failed. Server SHA-1 thumbprint 5D:01:0
6:63:55:9D:DF:FE:30:01:6E:2C:FA:71:BC:63:02:C5:16:51 <not trusted>
```

use this command to add the thumbprint

```
usr/lib/vmware-vcli/apps/general/credstore_admin.pl add -s
server -t thumbprint
```

Another option is to download the trusted root certificate from the vCenter Server using a web browser to connect to the vCenter Server and selecting **Download Trusted Root Certificates**. Save the certificates as a ZIP file. The ZIP file contains nested files that have the extensions .0 or .1, which are certificates, and nested files that have the extensions .r0 and .r1, which are associated CRL files

Verify Network Configuration: REF: *VCP6-DCV Cert Guide* page 404

Use command line tools to troubleshoot and identify VLAN configurations

```
esxcli network vswitch standard portgroup set -p PGNAME --vlan-id  VLANID
```

REF:
https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1008127

Use DCUI network tool to correct network connectivity issue

Rollbacks and network restore options: REF: *VCP6-DCV Cert Guide* page 405

- Restore Network Settings
- Restore Standard Switch (if this option is disabled, it may be that the host's management network adapter is already connected to a standard switch)
- Restore vDS

Section 4 - Configure a vSphere Deployment for Availability and Scalability

Objective 4.1 - Implement and Maintain Complex vSphere Availability Solutions

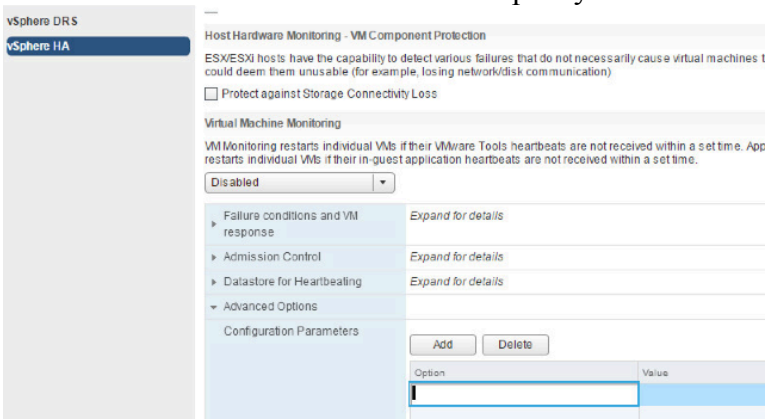
Configure a HA cluster to meet resource and availability requirements

HA Admission control / VM overrides REF: *VCP6-DCV Cert Guide* page 505

`das.defaultisolationaddressX` where X is 0 to 9
`das.usedefaultisolationaddress` set to false when default gateway should not be used as an isolation address.

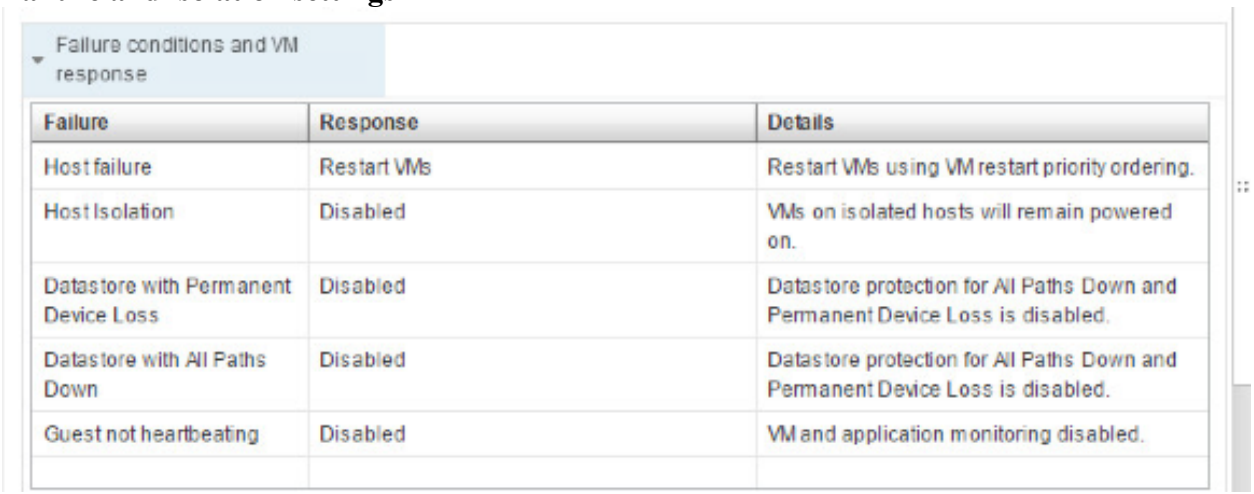
HA – Advanced Options: REF: http://bit.ly/2dXz4Mu

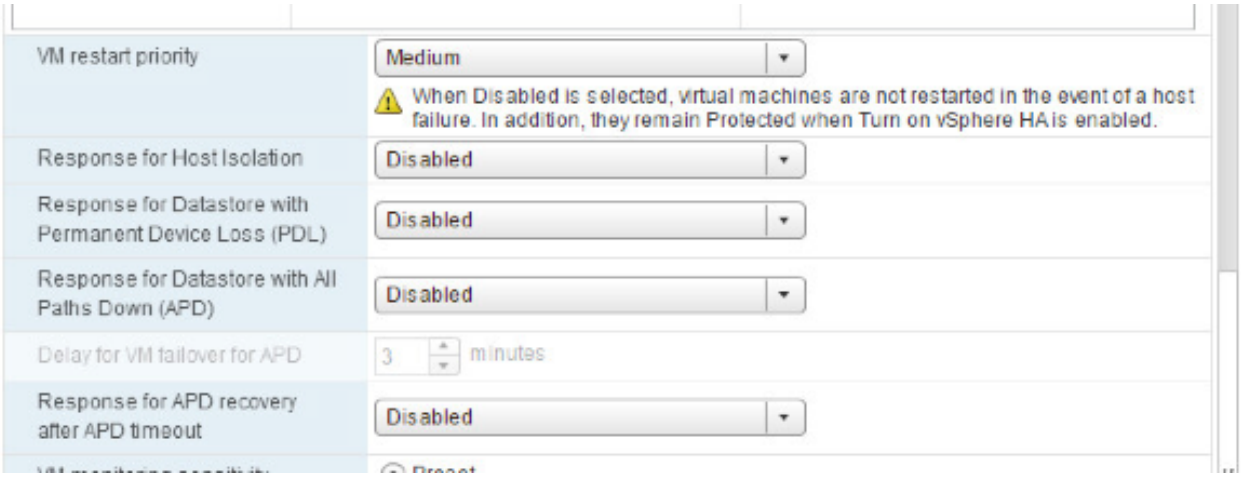
- das.slotmeminmb MAX (notice this variable name does not contain the text *MIN*, it contains *Mem In*) (don't confuse with vpxd.das.slotMemMinMB which is a vCenter setting controlling the MIN memory reservation size, which can be overridden by das.vmMemoryMinMB)
- das.slotcpuinmhz MAX
- das.vmmemoryminmb = 0 by default, mem assigned to vm when vm resv = 0
- das.vmcpuminmhz = no value (32 MHz) by default
- das. Ignoreinsufficientdatastore
- das.heartbeatdsperhost
- fdm.isolationpolicydelaysec
- das.respectvmvmaffinityrules
- das.maxresets – max reset attempts by VMCP\



Configure custom isolation response settings

Failure and isolation settings





Configure VM Component Protection (VMCP)

VMCP overrides turns off FT protection on associated VMs REF: https://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.avail.doc/GUID-F5264795-11DA-4242-B774-8C3450997033.html

Troubleshoot VMCP: REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.troubleshooting.doc/GUID-21D4E343-3753-4886-B654-1D2F4027BAF5.html?resultof=%22%76%6d%63%70%22%20

The PDL condition was added in vSphere 5.0. The storage device sends a SCSI sense code to the ESXi Host, specifying that the storage device has become unavailable. A good example of a PDL is a LUN failing but the storage array continuing to function. The storage array sends a SCSI sense code to inform the ESXi Host that the LUN is permanently disabled. Once this occurs, the ESXi Host stops sending I/O requests to the storage array

Configure HA redundancy settings:

Management network

REF: https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1006421

Datastore heartbeat

REF: http://bit.ly/2fBkTxY

Network partitions

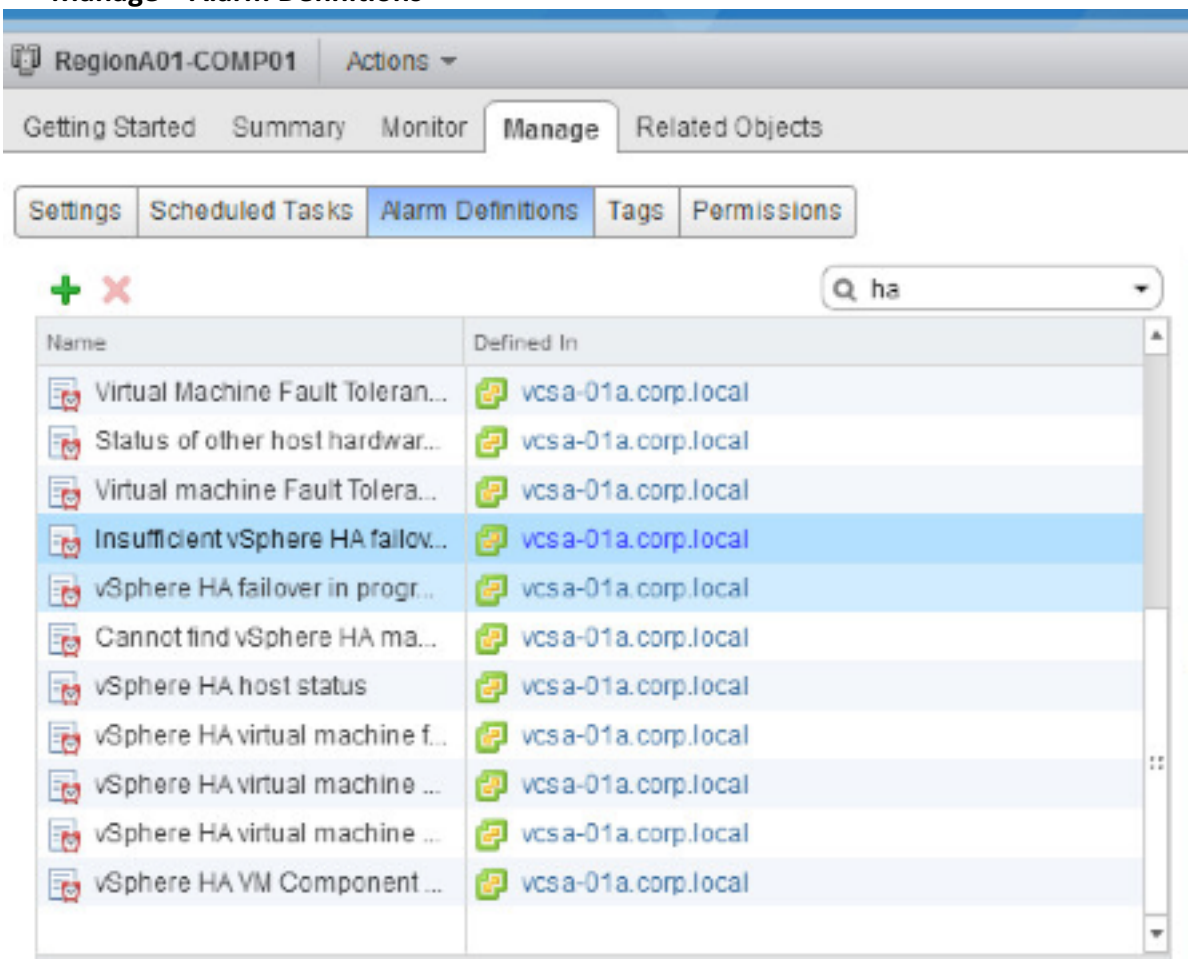
Network partiion vs network isolated:

- Network Partitioned: This happens when the master is unable to communicate to this host via the heartbeat network but can communicate via the heartbeat datastores and the ESXi server is not isolated.
- Network Isolated: An ESXi server is isolated only if all of the following are true:
    - It has lost access to its heartbeat network.
    - It has lost access to all of its isolation addresses (VMkernel default gate-
    - way and/or any additional isolation addresses).

- It has lost access to its heartbeat datastores.
- Its unable to reach any HA agents on any other ESXi servers in the cluster.

Configure HA related alarms and analyze a HA cluster

- Select the cluster
- **Manage** > **Alarm Definitions**



Configure VMware Fault Tolerance for single and multi-vCPU virtual machines

Using FT http://bit.ly/2eZWOBq

- Compatible hardware
- Configure vmkernel virtual adapters per host

- Configure vMotion and HA
- Enable FT per VM
    - Right-click on VM
    - **Fault Tolerance, Furn On FT**
    - Select the datastores to place secondary VM disks and config files
    - Select host for secondary VM

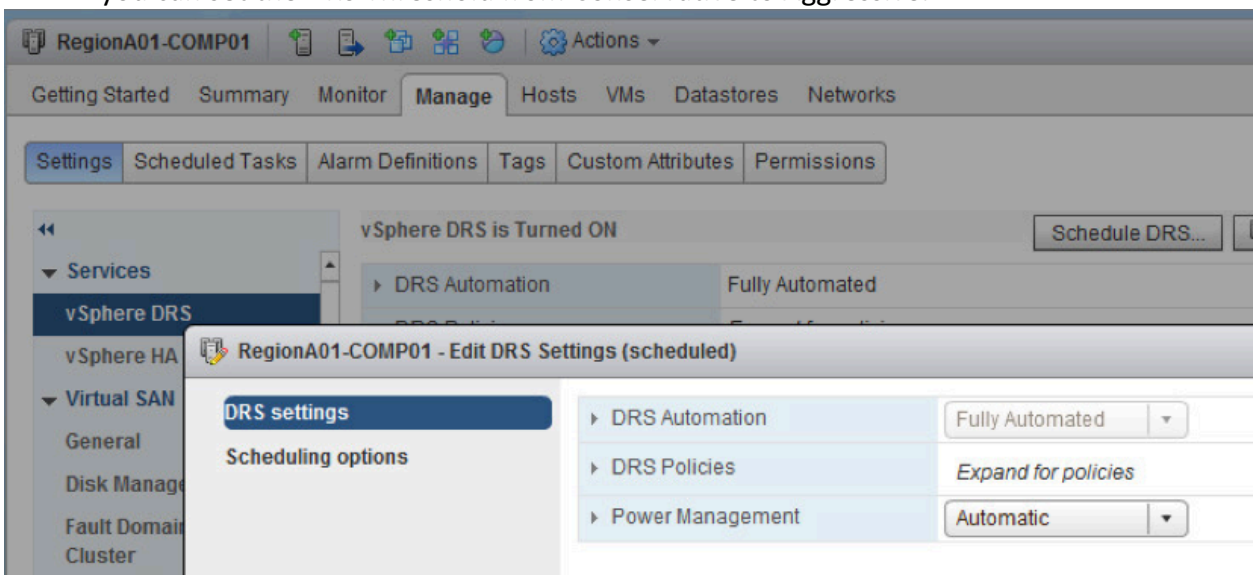
Use vm.uselegacyft REF: *VCP6-DCV Cert Guide* 517, 389

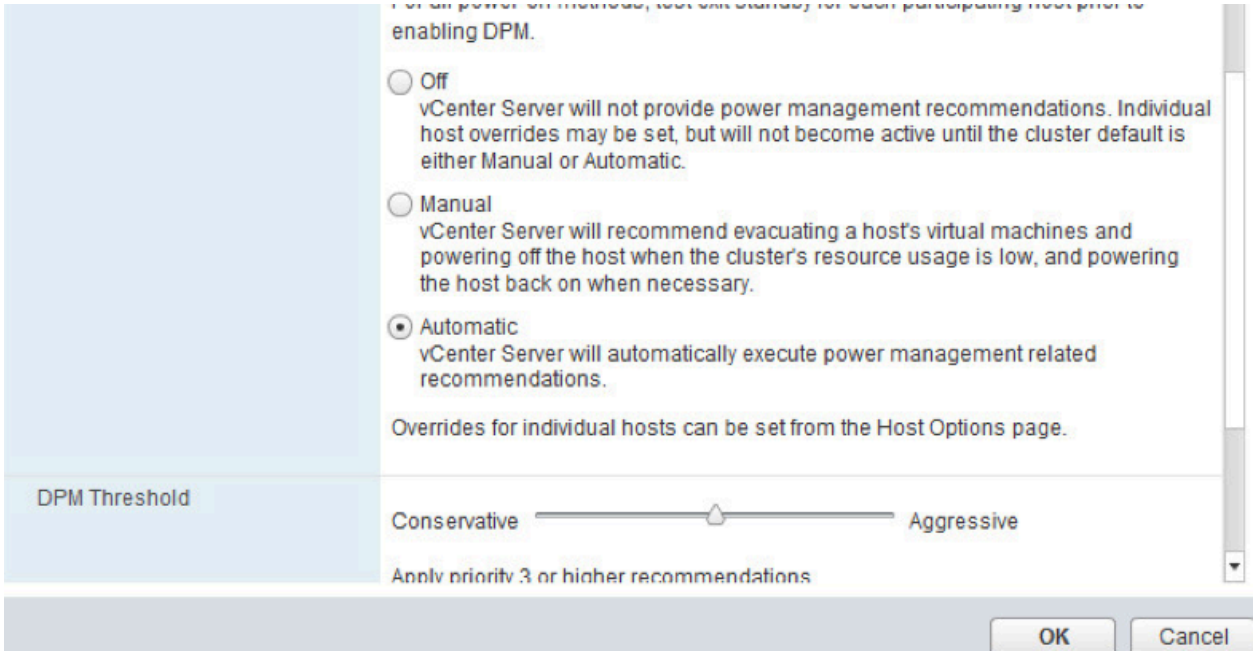
In the Configuration Parameters window, enter `vm.uselegacyft` in th
Name field and type `true` for the Value (see Figure 13-13).

Objective 4.2 - Implement and Manage Complex DRS solutions

Configure DPM, including appropriate DPM threshold

- Configure IPM / iLO on each ESXi host:
    - **Manage** > **Settings** > ***System*** > **Power Management** (NOT *Hardware* > Power Management). Set the BMC IP address and credentials
    - On the cluster, enable DRS and Power Management, for example set DRS = Fully Automated and set Power Management = Automatic
    - Choose the cluster, **Manage** > **Settings** > **vSphere DRS** > **Schedule DRS**. Here you can set the DRS Threshold from Conservative to Aggressive.

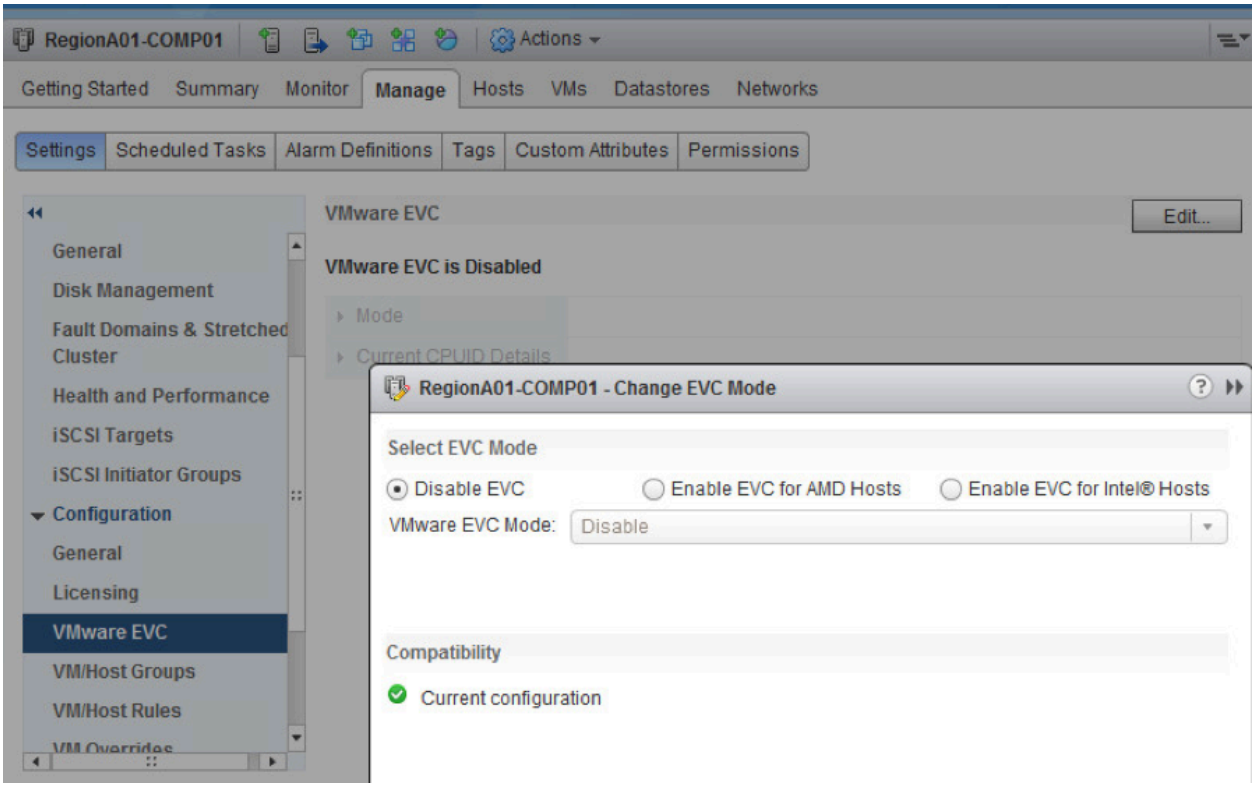


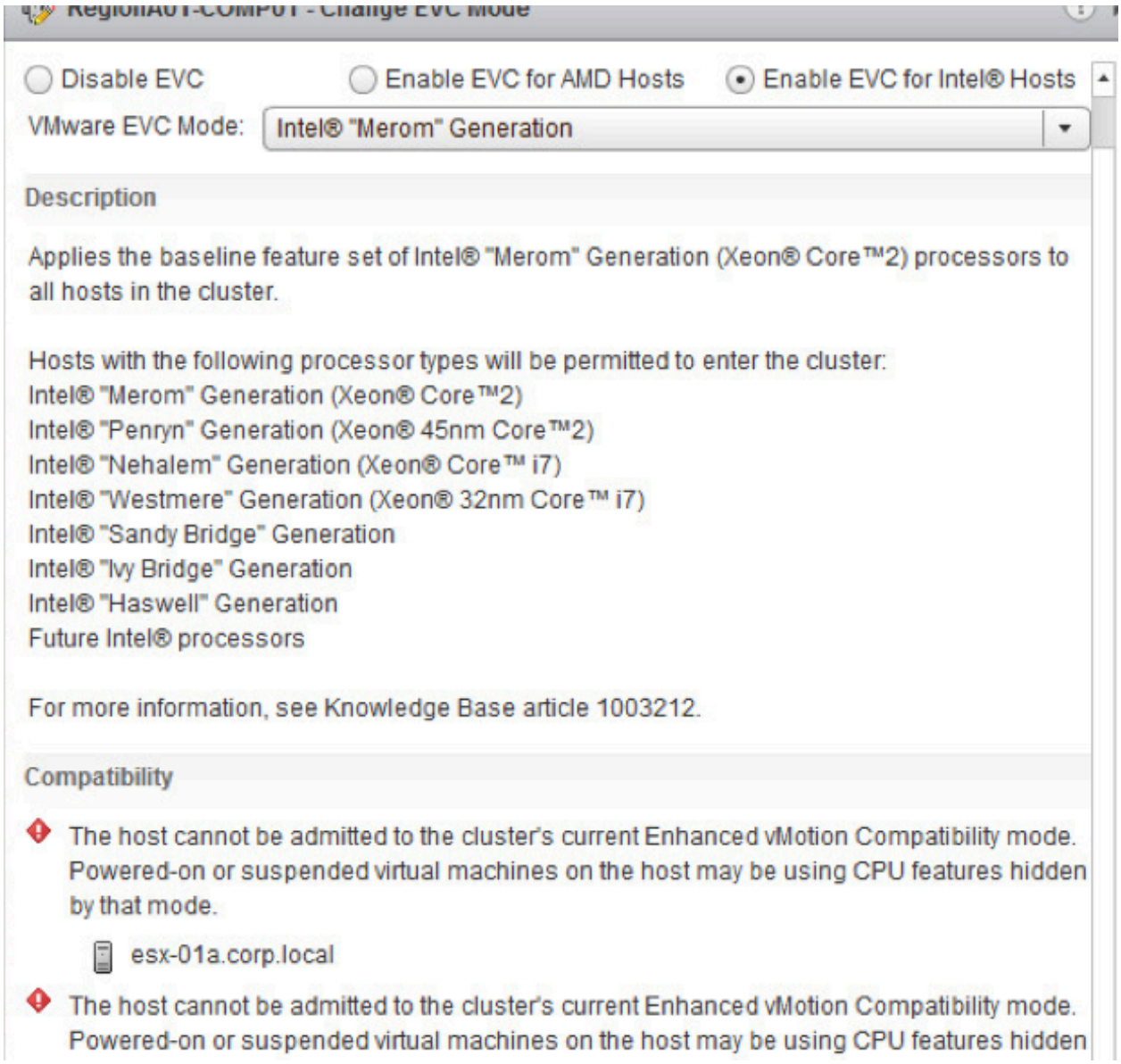


DPM REF: https://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.resmgmt.doc/GUID-D247EC2C-92C5-4B9B-9305-39099F30D3B5.html

Configure / Modify EVC mode on an existing DRS cluster

- Select the cluster, click Manage > Settings > VMware EVC
- Select Disable, enable for AMD, or enable for Intel
- Select the EVC Mode


RegionA01-COMP01
Actions
Getting Started
Summary
Monitor
Manage
Hosts
VMs
Datastores
Networks
Settings
Scheduled Tasks
Alarm Definitions
Tags
Custom Attributes
Permissions
General
Disk Management
Fault Domains & Stretched Cluster
Health and Performance
iSCSI Targets
iSCSI Initiator Groups
Configuration
General
Licensing
VMware EVC
VM/Host Groups
VM/Host Rules
VMware EVC
Edit...
VMware EVC is Disabled
Mode
Current CPUID Details
RegionA01-COMP01 - Change EVC Mode
Select EVC Mode
Disable EVC
Enable EVC for AMD Hosts
Enable EVC for Intel® Hosts
VMware EVC Mode:
Disable
Compatibility
Current configuration

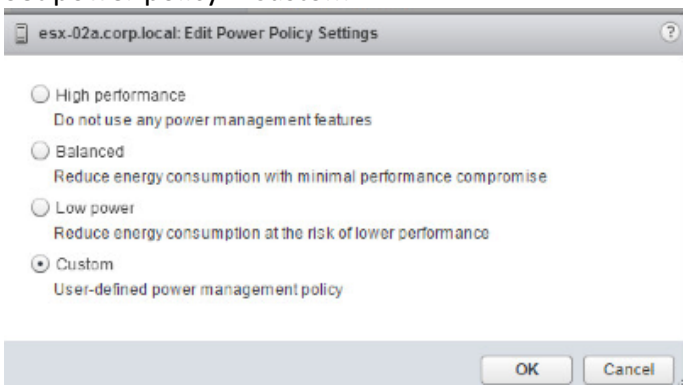


Create DRS and DPM alarms

Configure applicable power management settings for ESXi hosts

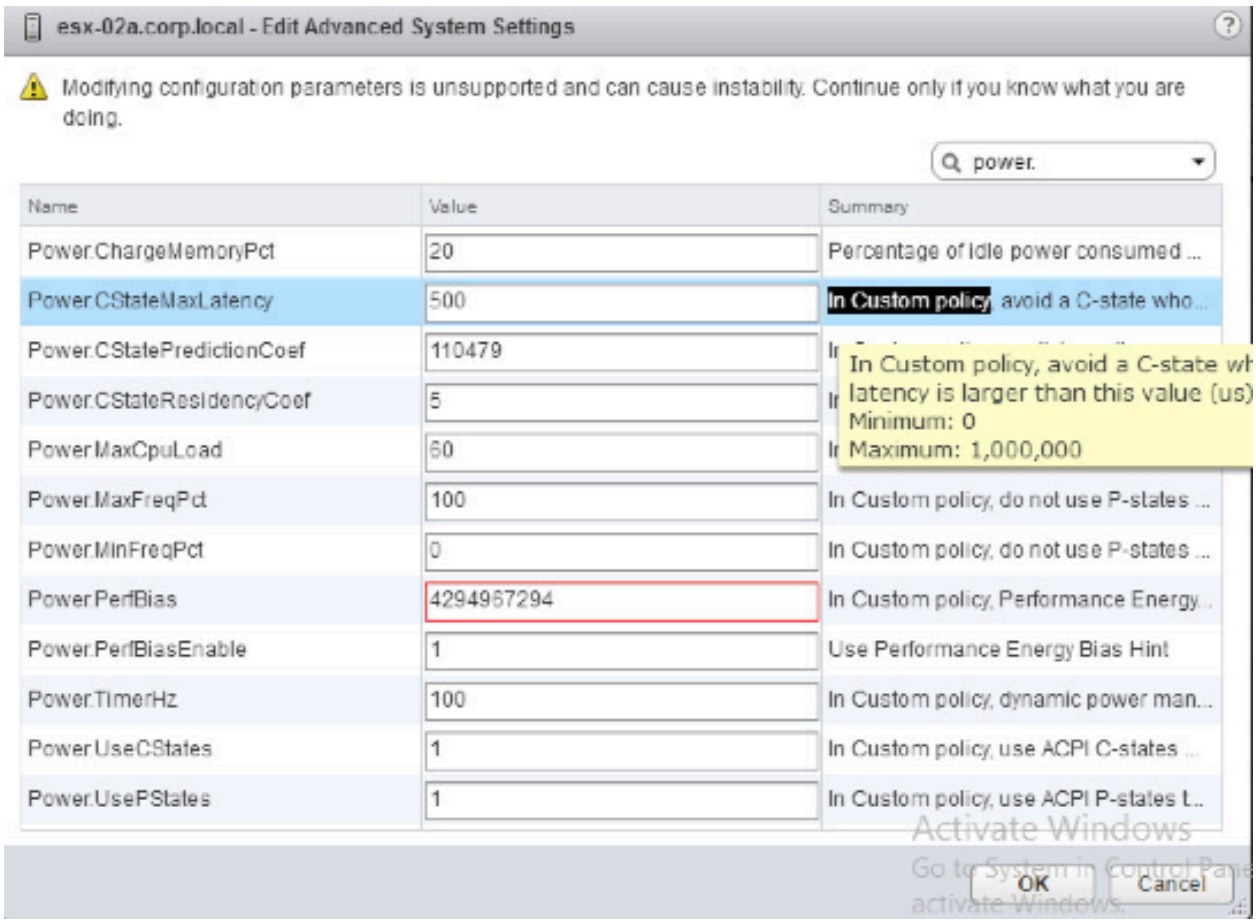
Custom host power management settings **REF:** https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.hostclient.doc/GUID-B1C20A79-9385-4A7B-8A6A-7393E27CE167.html?resultof=%22%63%75%73%74%6f%6d%22%20%22%70%6f%77%65%72%22%20

- Select the host, click **Manage** > **Settings** > ***Hardware*** > **Power Management** (be sure to choose *Hardware,* not *System*)
- Set power policy = Custom

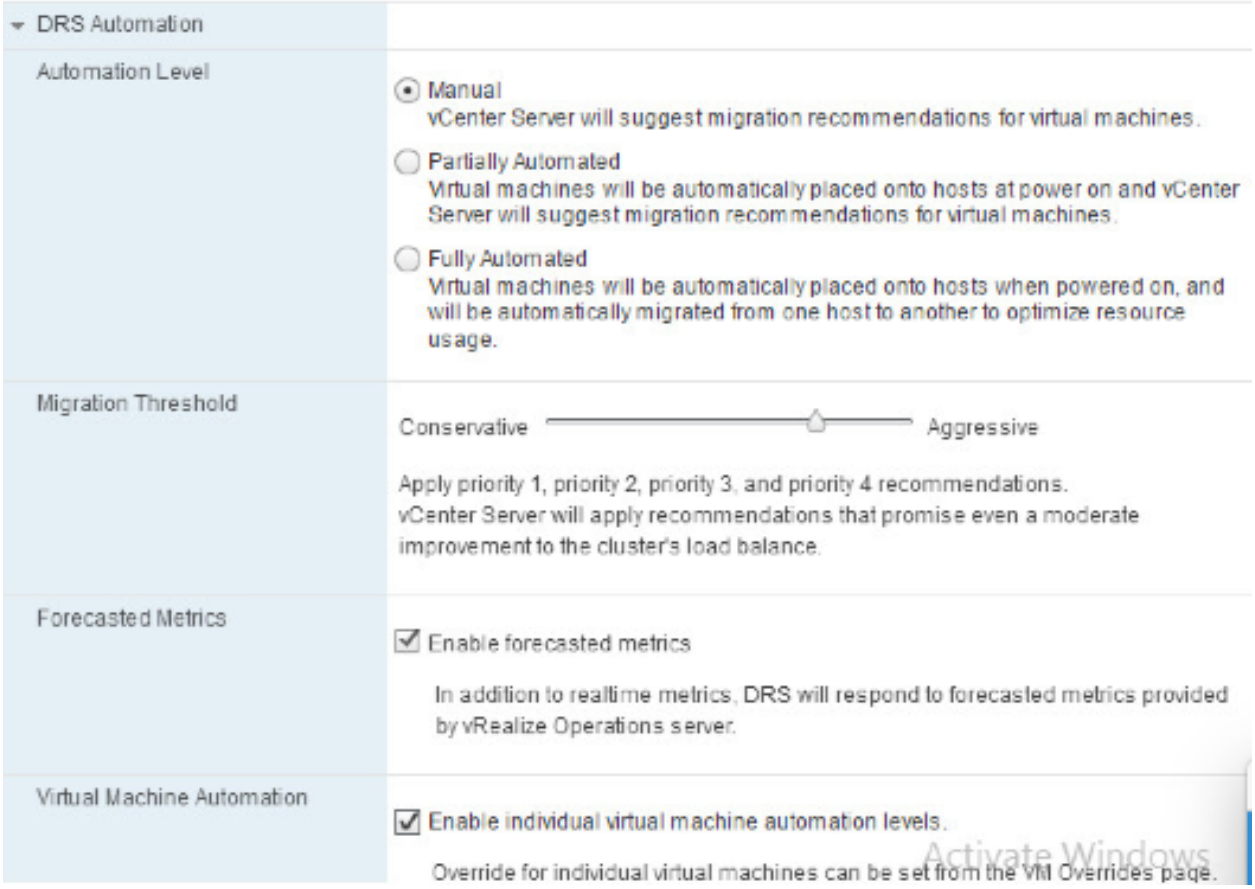


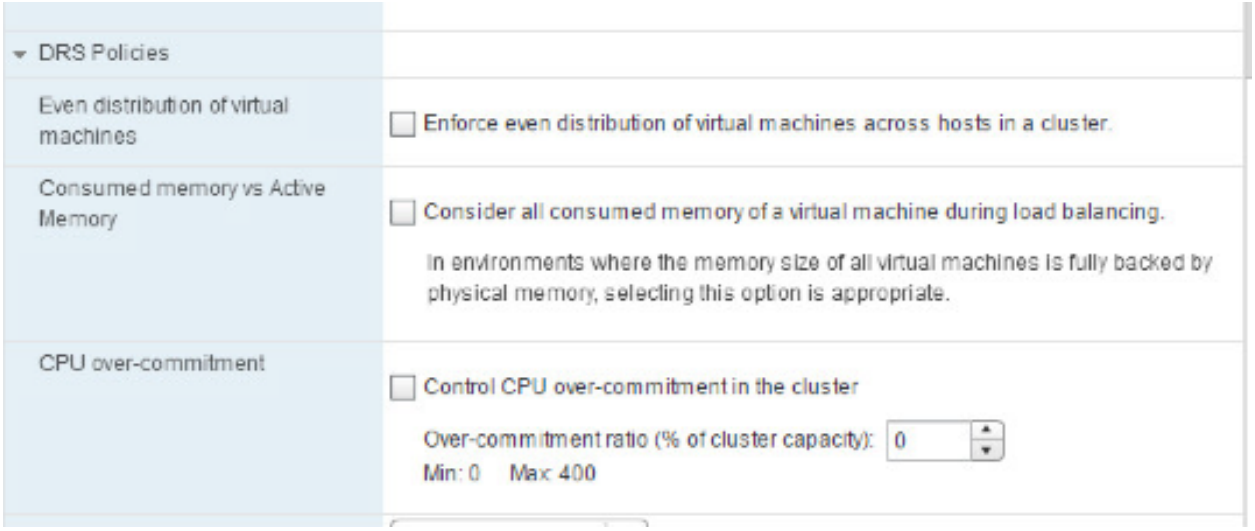
- **Manage** > **Settings** > **Advanced System Settings**, filter for "power.", such as
  - Power.UsePState (Use ACPI P-states to save power when the processor is busy.)
  - Power.MaxCpuLoad (Use P-states only when the CPU is busy for less than the given percentage of real time)
  - Power.MinFreePct (do not use any pstates slower than the given CPU %)

Many of these settings are only applied when Custom Policy is selected


esx-02a.corp.local - Edit Advanced System Settings
Modifying configuration parameters is unsupported and can cause instability. Continue only if you know what you are doing.
power.
Name
Value
Summary
Power.ChargeMemoryPct
20
Percentage of idle power consumed ...
Power.CStateMaxLatency
500
In Custom policy avoid a C-state who...
Power.CStatePredictionCoef
110479
Power.CStateResidencyCoef
5
Power.MaxCpuLoad
50
Power.MaxFreqPct
100
In Custom policy, do not use P-states ...
Power.MinFreqPct
0
In Custom policy, do not use P-states ...
Power.PerfBias
4294967294
In Custom policy, Performance Energy...
Power.PerfBiasEnable
1
Use Performance Energy Bias Hint
Power.TimerHz
100
In Custom policy, dynamic power man...
Power.UseCStates
1
In Custom policy, use ACPI C-states ...
Power.UsePStates
1
In Custom policy, use ACPI P-states t...
In Custom policy, avoid a C-state wh
latency is larger than this value (us)
Minimum: 0
Maximum: 1,000,000
Activate Windows
Go to System in Control Pan
activate Windows.
OK
Cancel

Configure DRS cluster for efficient/optimal load distribution





Properly apply virtual machine automation levels based upon application requirements

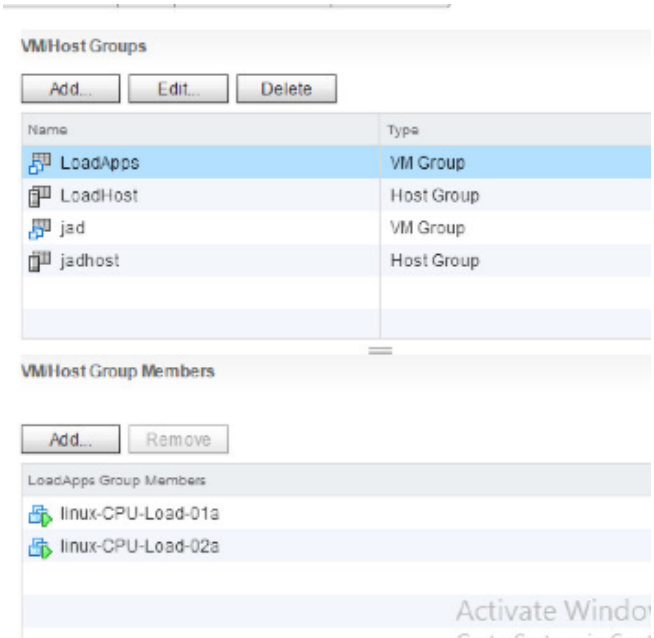
- In DRS cluster settins, ensrue the **Enable individual virtual machine automation** levels is checked.
- Use VM Overrides (select cluster, select Manage > Setttings > VM Overrides) to directly configure fully, partially, or manual automation on the VM
-

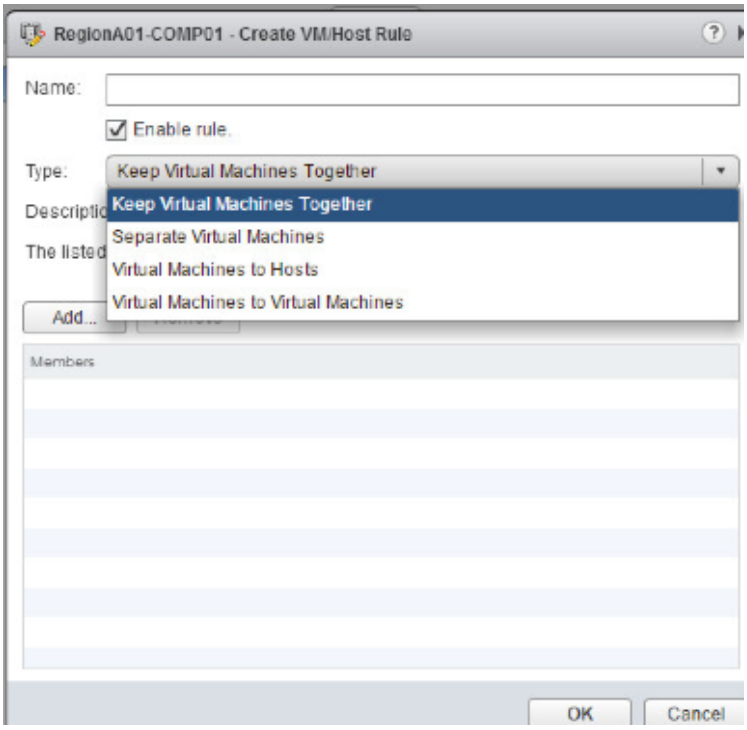
Administer DRS / Storage DRS

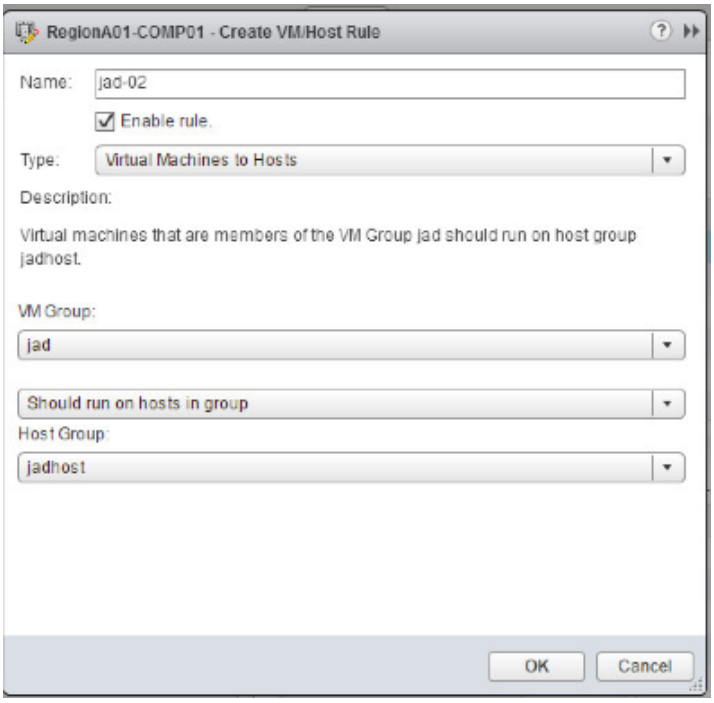
View the target and current standard deviation in vSphere Client (not web client) REF: *VCP6-DCV Cert Guide* page 522

Create DRS / Storage DRS affinity and anti-affinity rules

- Select the cluster, select **Manage** > **Settings** > **VM / Hosts Groups**
- Use the **Add** button to add VM and Host groups
- Create the rules





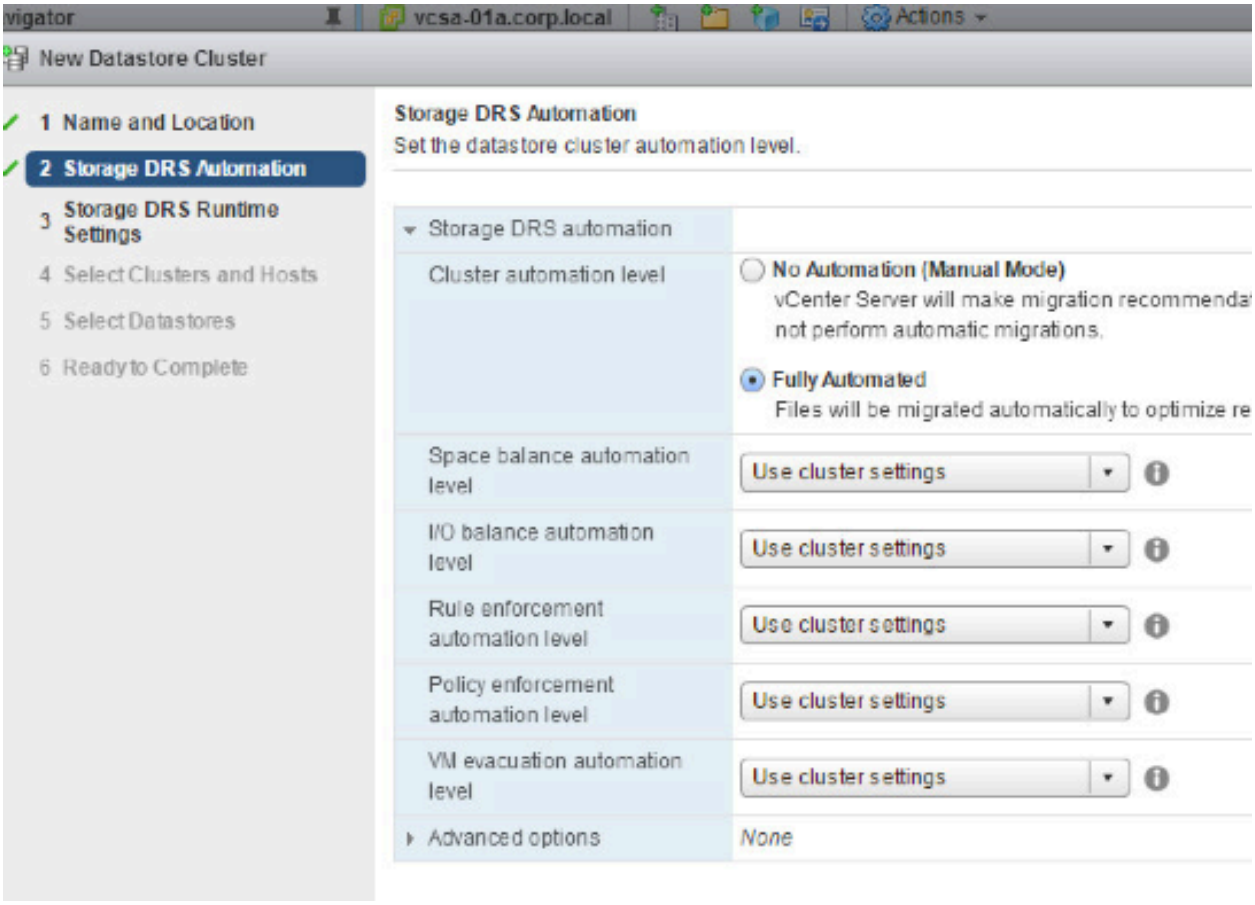


Configure advanced DRS / Storage DRS settings

Set automation levels for:

- Space balance

- IO balance
- Rule enforcement
- Policy enforcement
- Vm evacuation



Configure and Manage vMotion / Storage vMotion

vMotion REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.vcenterhost.doc/GUID-D19EA1CB-5222-49F9-A002-4F8692B92D63.html?resultof=%22%76%6d%6f%74%69%6f%6e%22%20

Storage vMotion REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.vcenterhost.doc/GUID-AB266895-BAA4-4BF3-894E-47F99DC7B77F.html?resultof=%22%73%74%6f%72%61%67%65%22%20%22%73%74%6f%72%61%67%22%20%22%76%6d%6f%74%69%6f%6e%22%20

Create and manage advanced resource pool configurations

REF: http://bit.ly/2floeR7

Objective 4.3 - Troubleshoot vSphere clusters

Analyze and resolve DRS/HA faults

- Unreachable: vCenter is unable to communicate to the master host, and one or more agents has failed.
- Uninitialized: The host can't access any of the datastores or has lost access to its local datastore. The agent can also be in this state if the agent is inaccessible or cannot open the needed firewall port (8182).
- Initialization Error: vCenter cannot connect to the ESXi server when the HA agent is being installed or configured on the host. The agent can also enter this state if there is not enough space (75 MB) on the local storage to install the HA agent or when the agent successfully installed but the host doesn't be- come a master or slave within the timeout period.
- Uninitialization Error: vCenter lost connectivity to the ESXi Host at the time the HA agent was being unconfigured.
- Host Failed: This ESXi Host is unable to reach the master through the net- work and is also unable to access its heartbeat datastores (isolation).
- Network Partitioned: This happens when the master is unable to communicate to this host via the heartbeat network but can communicate via the heartbeat datastores and the ESXi server is not isolated.
- Network Isolated: An ESXi server is isolated only if all of the following are true:
    - It has lost access to its heartbeat network.
    - It has lost access to all of its isolation addresses (VMkernel default gate-
    - way and/or any additional isolation addresses).
    - It has lost access to its heartbeat datastores.
    - Its unable to reach any HA agents on any other ESXi servers in the cluster.

- Configuration on Hosts Times Out: The HA agent didn't completely install on the ESXi server before the timeout. This timeout can be extended by using the vCenter advanced setting vpxd.das.electionWaitTimeSec and changing the value to the VMware recommended value, 240.

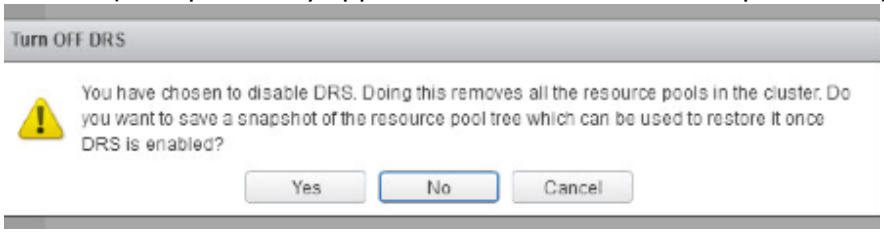
Troubleshoot DRS/HA configuration issues

HA log files: /var/log/fdm.log

Set `vpxd.das.electionWaitTimeSec` to higher value: pp 510

Save resource pool tree snapshot and use it to restore pp510

- Select the cluster, click Manage > Settings > vSphere DRS, click Edit
- De-select Turn on vSphere DRS
- Click OK
- When prompted, select option to save the resource pools and provide a location to save the file. (the option only appears if at least one resource pool exists)



restore DRS resource pools:

- Right-click the cluster, select Restore Resource Pool Tree
- Browse to and select the snapshot file.

Cannot Configure vSphere HA When Using Custom SSL Certificates

After you install custom SSL certificates, attempts to enable vSphere High Availability (HA) fail.

Problem

When you attempt to enable vSphere HA on a host with custom SSL certificates installed, the following error message appears:
`vSphere HA cannot be configured on this host because its SSL thumbprint has not been verified.`

Cause

When you add a host to vCenter Server, and vCenter Server already trusts the host's SSL certificate, `VPX_HOST.EXPECTED_SSL_THUMBPRINT` is not populated in the vCenter Server database. vSphere HA obtains the host's SSL thumbprint from this field in the database. Without the thumbprint, you cannot enable vSphere HA.

Solution

1. In the vSphere Web Client, disconnect the host that has custom SSL certificates installed.
2. Reconnect the host to vCenter Server.
3. Accept the host's SSL certificate.
4. Enable vSphere HA on the host.

Troubleshoot Virtual SAN/HA interoperability

Resolve vMotion and storage vMotion issues

Troubleshoot vMotion: For traditional issues with traditional vMotion, verify all requirements are met:

- Connectivity between Vmkernel virtual adapters on each host, that is set for vMotion traffic
- VMs connected to a network that is not on an internal only switch. For standard switches, ensure the port group is named consistently on each host. For dvSwitches, ensure the VMs are connected to distributed port group that is accessible by each host.
- Ensure the VM resides on a datastore that is shared with each host.

Troubleshoot VMware Fault Tolerance

Upgrading ESXi servers does not upgrade FT. If VMs are configured to use FT before you upgrade the ESXi servers to vSphere 6, the VMs will be using legacy FT.

Adjust default max FT VMs and vCPUs per host: das.maxftvmsperhost, das.maxftvcpuperhost REF: *VCP6-DCV Cert Guide* page 518

Issues enabling FT on a VM REF: *VCP6-DCV Cert Guide* page 518

- The virtual machine is on an ESXi server that is in maintenance or standby mode or disconnected.
- The permission to enable FT is not present in the user's vCenter role.

- The virtual machine's files are inaccessible.
- Hardware virtualization is not enabled on the host(s).
- There must be enough memory on the ESXi server for the full amount of the configured RAM of the VM plus overhead.

Section 5 - Configure a vSphere Deployment for Manageability

Objective 5.1 - Execute VMware Cmdlets and Customize Scripts Using PowerCLI

Install and configure vSphere PowerCLI

REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.powercli.ug.doc/GUID-ACD2320C-D00F-4CCE-B968-B3C41A95C085.html

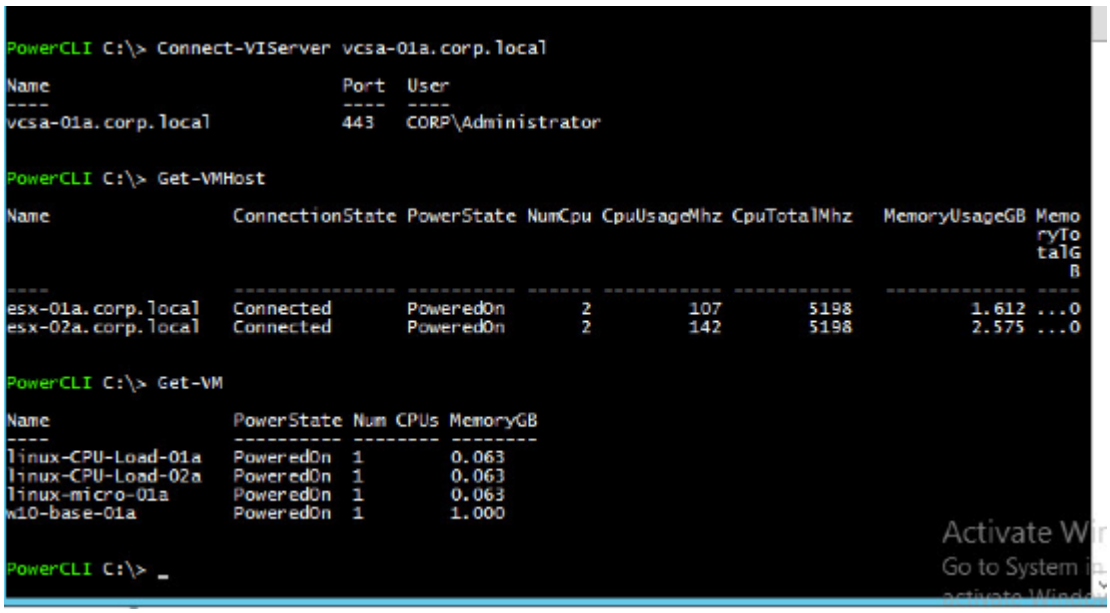
On first use, issue this command: `Set-ExecutionPolicy RemoteSigned.` Use Get-ExectutionPolicy to view the current policy. Use Set-ExececutionPolicy –List to view the options.

Use basic and advanced PowerCLI Cmdlets to manage a vSphere deployment

You can customize PowerCLI by creating a file named `Initialize-PowerCLIEnvironment_Custom.ps1` in the Scripts folder. PowerCLI will automatically detect and load this custom file after loading the default script config file (`Initialize-PowerCLIEnvironment.ps1`)

Use these commands to get started:

- Connect-VIserver
- Get-VMHost
- Get-VM



```
PowerCLI C:\> Get-VirtualSwitch
WARNING: The output of the command produced distributed virtual sw
obsolete and may change in the future. To retrieve distributed swi
 the VDS component. To retrieve standard switches, use -Standard.

Name                           NumPorts   Mtu    Notes
----                           --------   ---    -----
RegionA01-vDS-COMP             36         1500


PowerCLI C:\> Get-Datastore

Name                                 FreeSpaceGB      CapacityGB
----                                 -----------      ----------
RegionA01-ISCSI01-COMP01                  56.389          79.750
```

Get all members for a VM named VM-2:

- $MyVM = Get-VM VM-2
- $MyVM | Get-Member

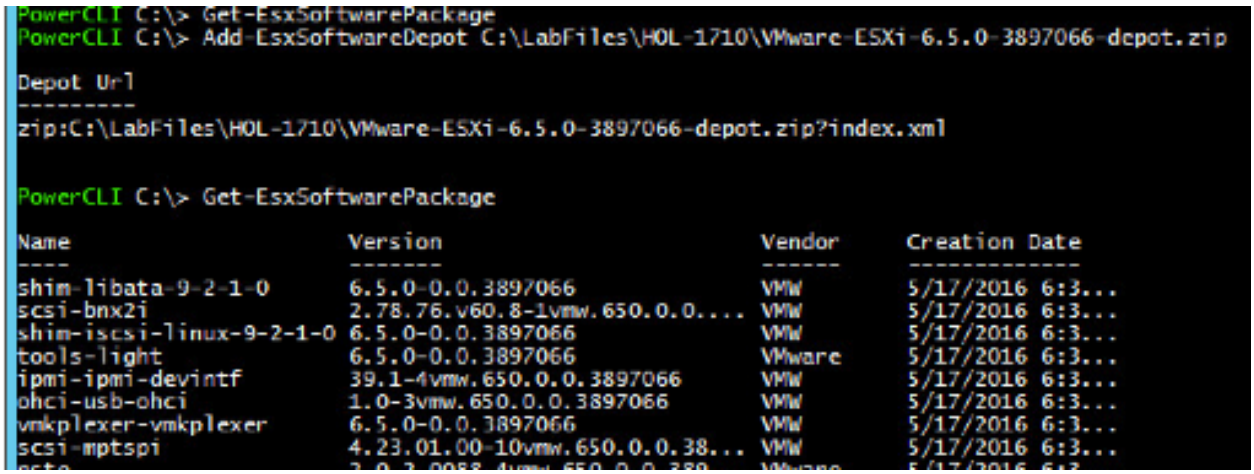
```
PowerCLI C:\> $MyVM = get-vm linux-CPU-Load-01a
PowerCLI C:\> $MyVM | get-member


   TypeName: VMware.VimAutomation.ViCore.Impl.V1.VM.UniversalVirtualMachineImpl

Name                      MemberType Definition
----                      ---------- ----------
ConvertToVersion          Method     T VersionedObjectInterop.ConvertToVersion[T]()
Equals                    Method     bool Equals(System.Object obj)
GetConnectionParameters   Method     VMware.VimAutomation.ViCore.Interop.V1.VM.RemoteConsoleVMPara..
GetHashCode               Method     int GetHashCode()
GetType                   Method     type GetType()
IsConvertableTo           Method     bool VersionedObjectInterop.IsConvertableTo(type type)
LockUpdates               Method     void ExtensionData.LockUpdates()
ObtainExportLease         Method     VMware.Vim.ManagedObjectReference ObtainExportLease.ObtainExp..
ToString                  Method     string ToString()
UnlockUpdates             Method     void ExtensionData.UnlockUpdates()
Client                    Property   VMware.VimAutomation.ViCore.Interop.V1.VIAutomation Client {g..
CustomFields              Property   System.Collections.Generic.IDictionary[string,string] CustomF..
```

Sample script from the *VCAP5-DCV: Official Cert Guide* (VMware Press) – display, toggle, and re-display the connection state for each vNIC for each VM

Analyze a sample script, then modify the script to perform a given action

Use PowerCLI to configure and administer Auto Deploy (including Image Builder)

Import software depots into Image Builder:
`Add-EsxSoftwareDepot` *`zip_file_name_and_location_or_URL`*
Get all software packages in the depot: `Get-EsxSoftwarePackage`



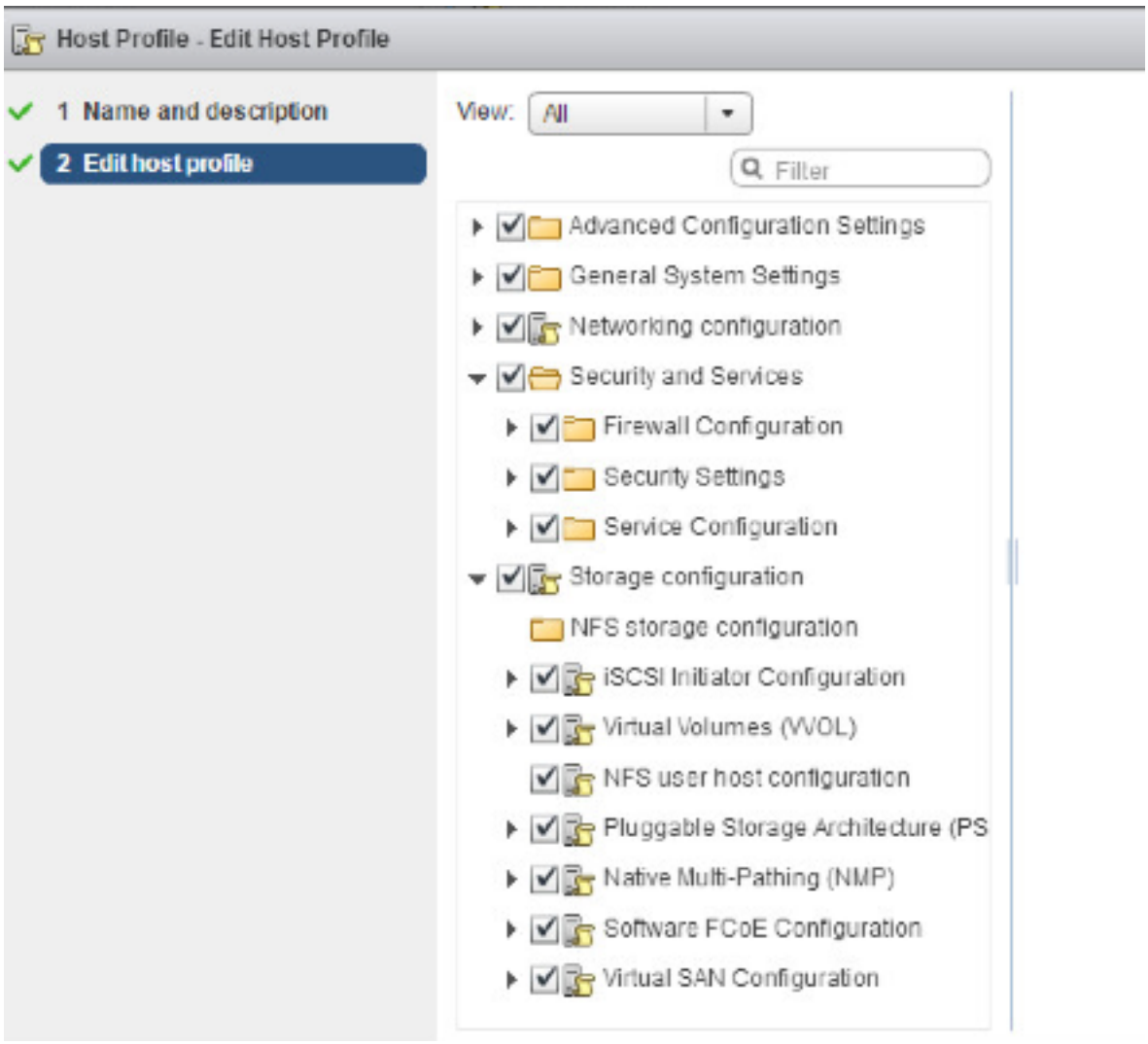
Create a report from a PowerCLI script

Objective 5.2 - Implement and Maintain Host Profiles

Host profiles REF: *VCP6-DCV Cert Guide* page 537

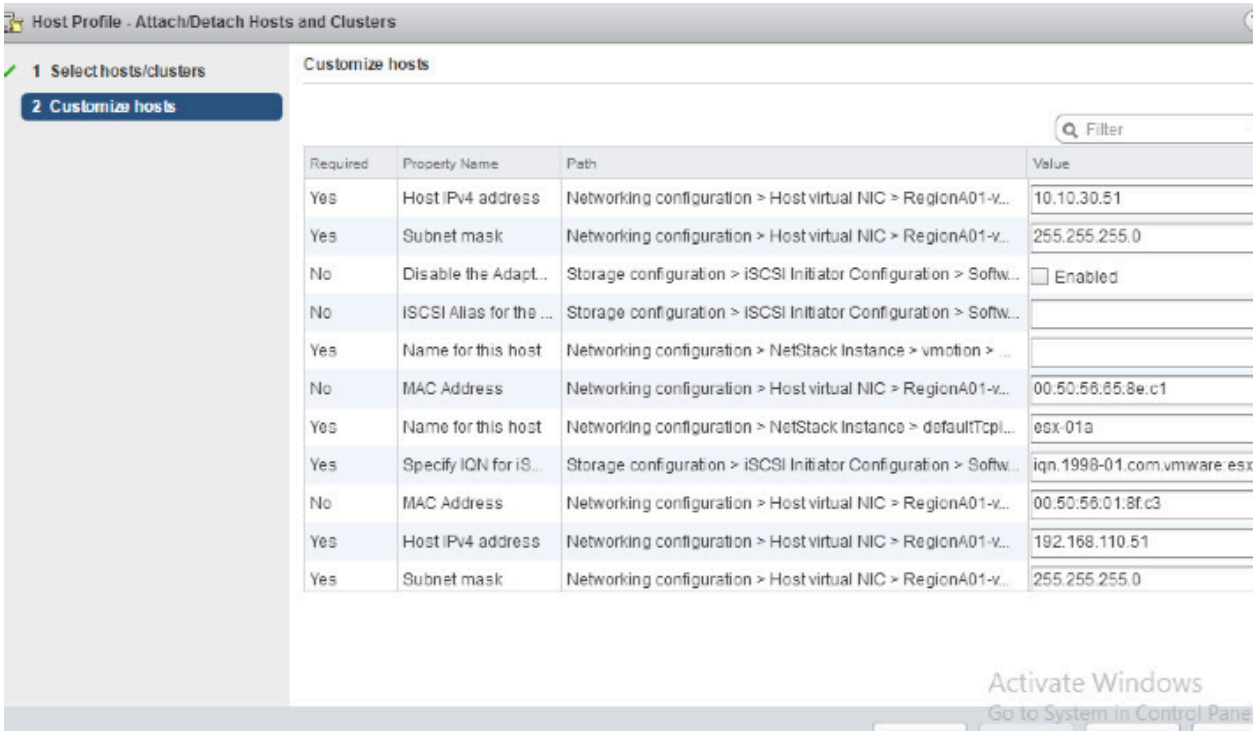
Use Profile Editor to edit and / or disable policies

Edit a host profile and uncheck some items. For example, uncheck Storage Configuration and uncheck Security and Services > Firewall Configuration

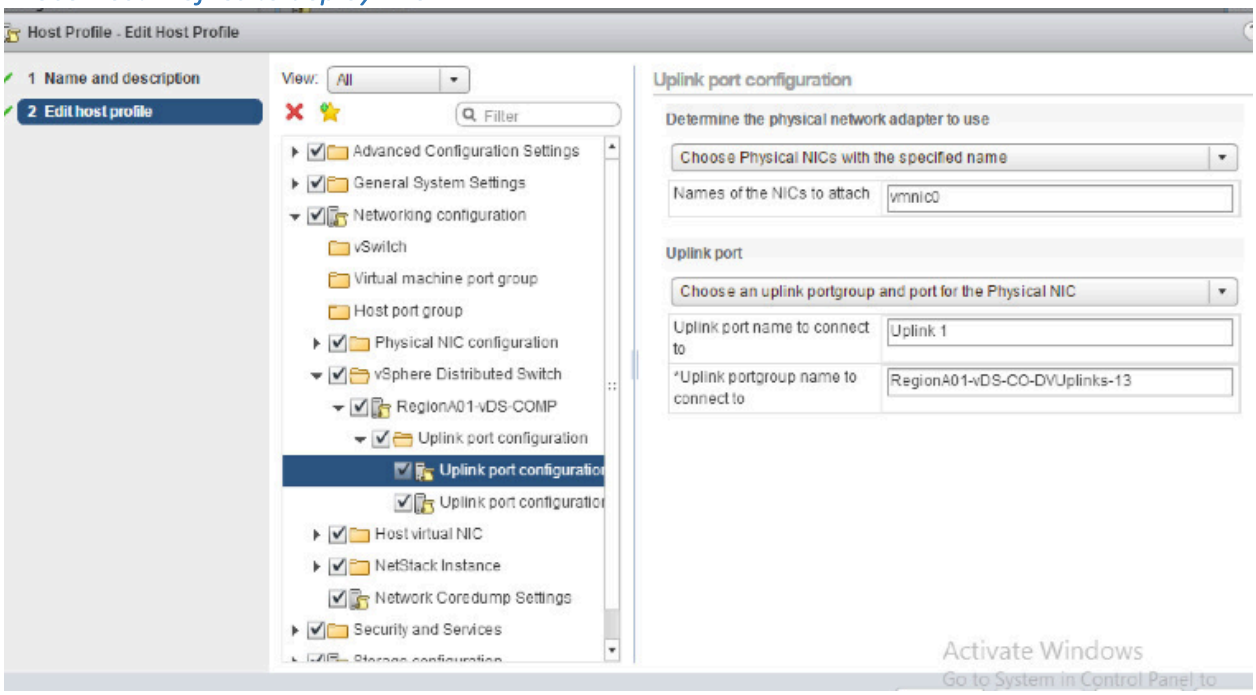


Create and apply host profiles

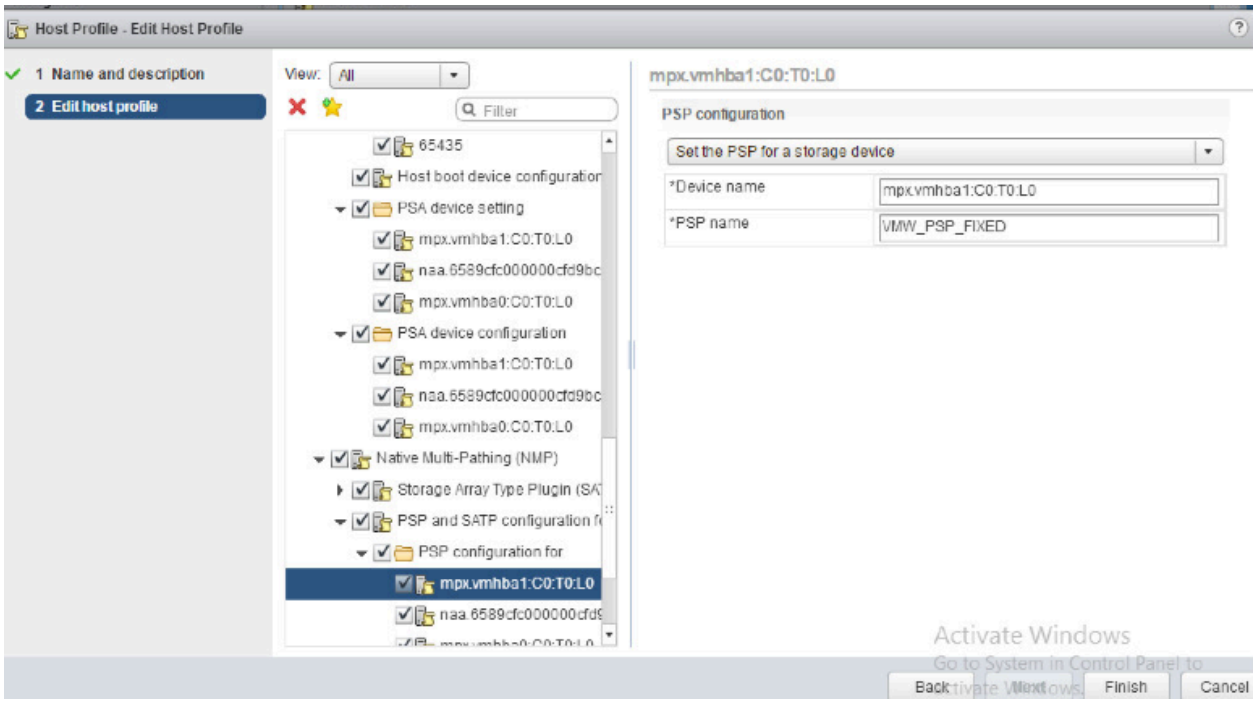
When ATTACHING host profiles, the wizard prompts for values that are typically unique per host

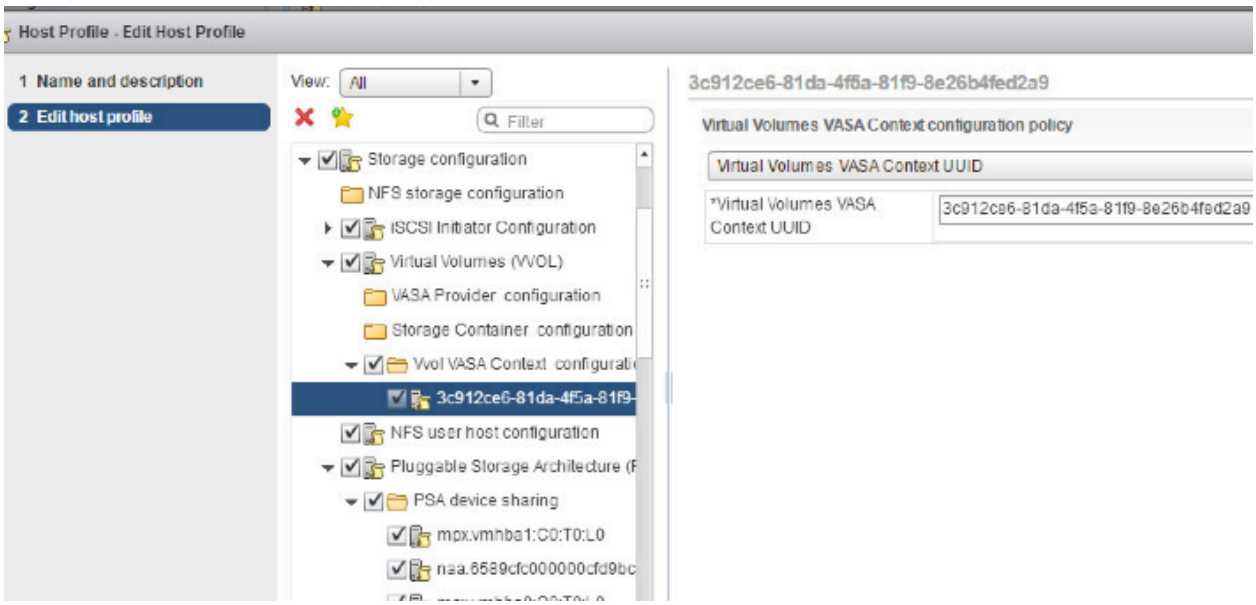


Use Host Profiles to deploy vDS



Use Host Profiles to deploy vStorage policies

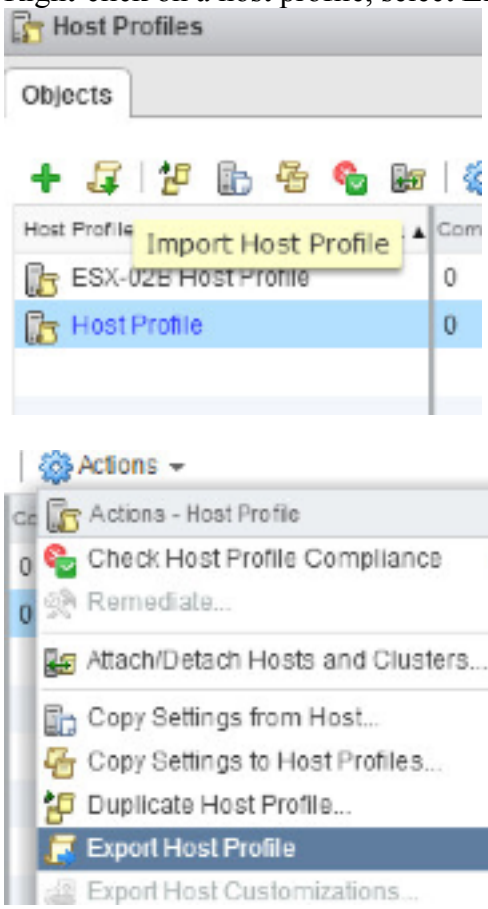




Import / Export Host Profiles

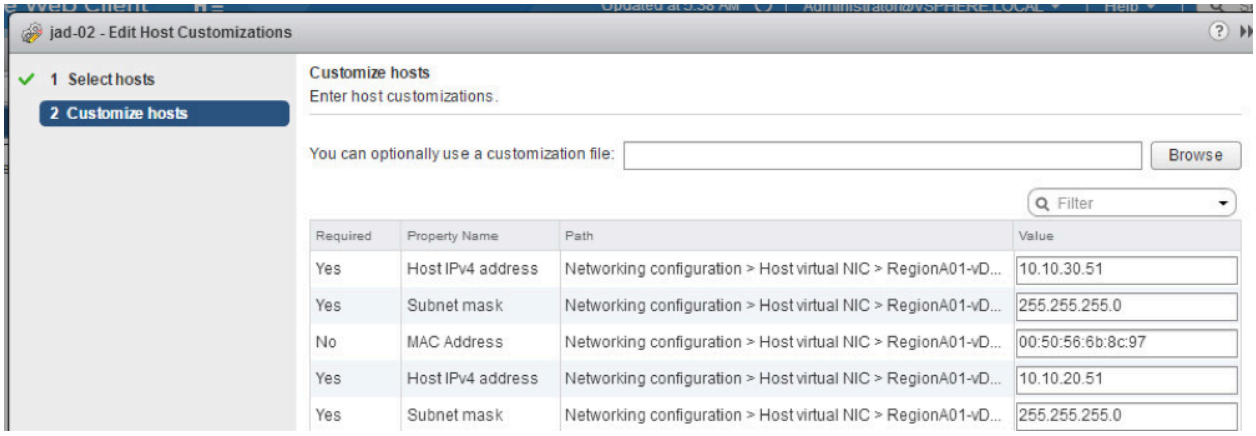
Import host profile REF: *VCP6-DCV Cert Guide* page 548

Right-click on a host profile, select **Export Host Profile**



if a profile has host customizations, you can **export the Host Customizations.**

To import a host customization, first edit the host profile customizations of the host profile then use the Browse button

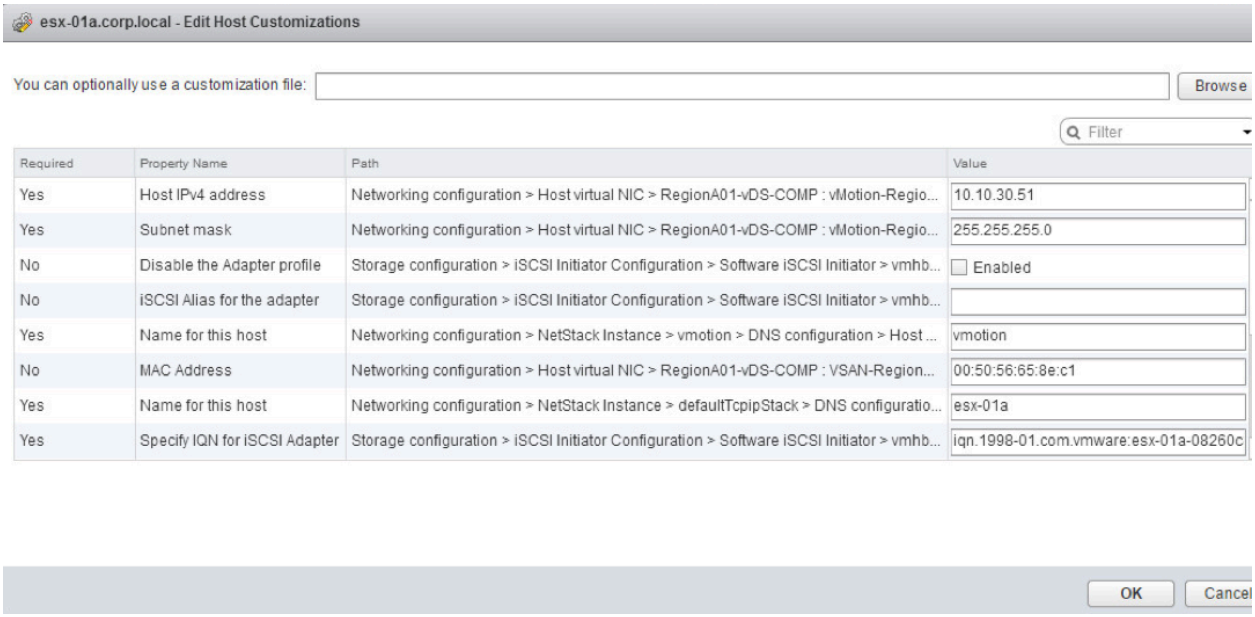


Manage Answer Files

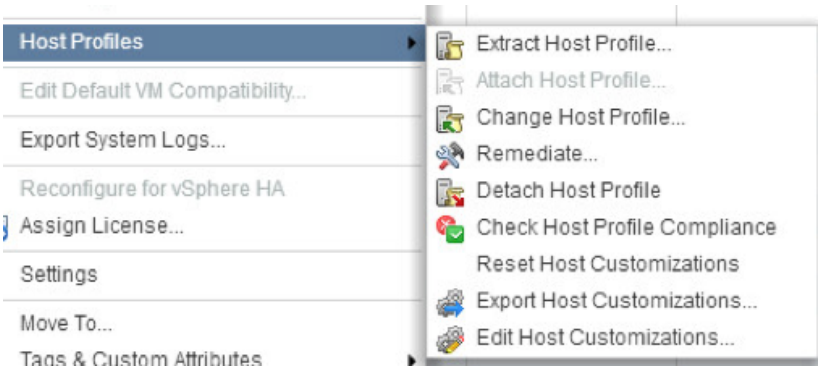
In vSphere 6, answer files are replaced with host customizations

Host profile answer files REF: *VCP6-DCV Cert Guide* page 543

- **Home** > **Monitoring** > **Host Profiles**
- Select a profile in left pane and click the Hosts tab
- right-click a host in the center pane
- Select **Edit Host Customizations**



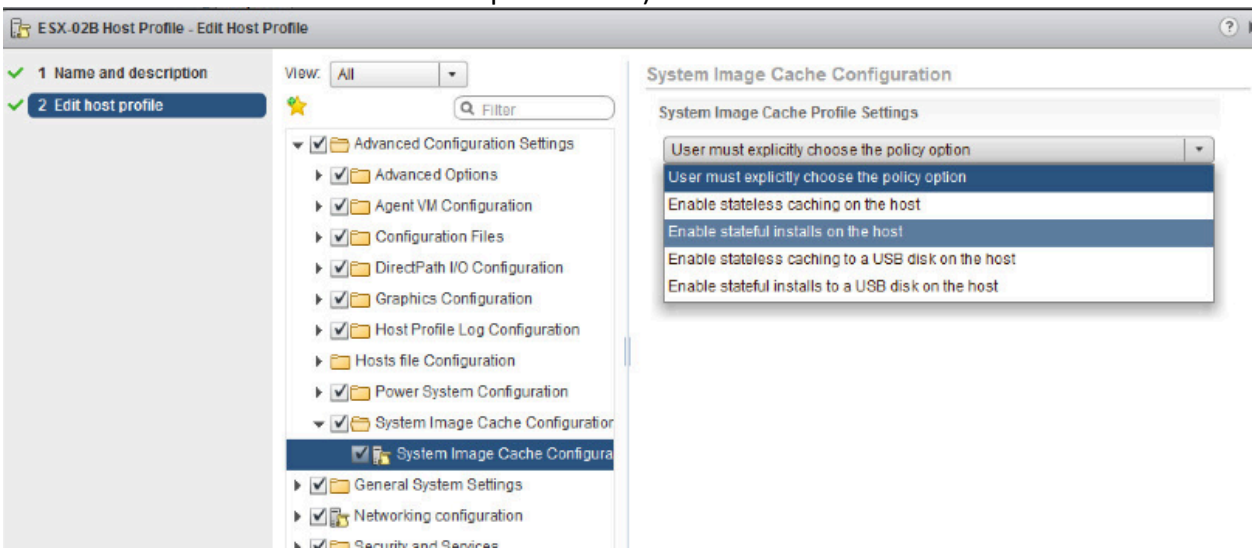
you can **export, import and reset host configuration files**:



Configure stateful caching and installation for host deployment

Enable Stateful Install:

- Prep host for auto deploy (bios is set to boot from disk then from PXE??)
- In the host profile, set **Advanced Configuration Settings** > **System Image Cache Configuration** > System Image Cache Configuration = Enable Stateful installs on the host (or Enable stateful installs to a USB disk on the host) and set Arguments for first disk (such as *ST3120814A,mptsas,local* .. to first look for a disk namd ST3122081, then look for a disk that uses the mptsas driver) and whether or not to overwrite VMFS



REF:: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-2140AE92-D092-4640-9B1A-0AF425BC88AB.html

Objective 5.3 - Manage and analyze vSphere log files

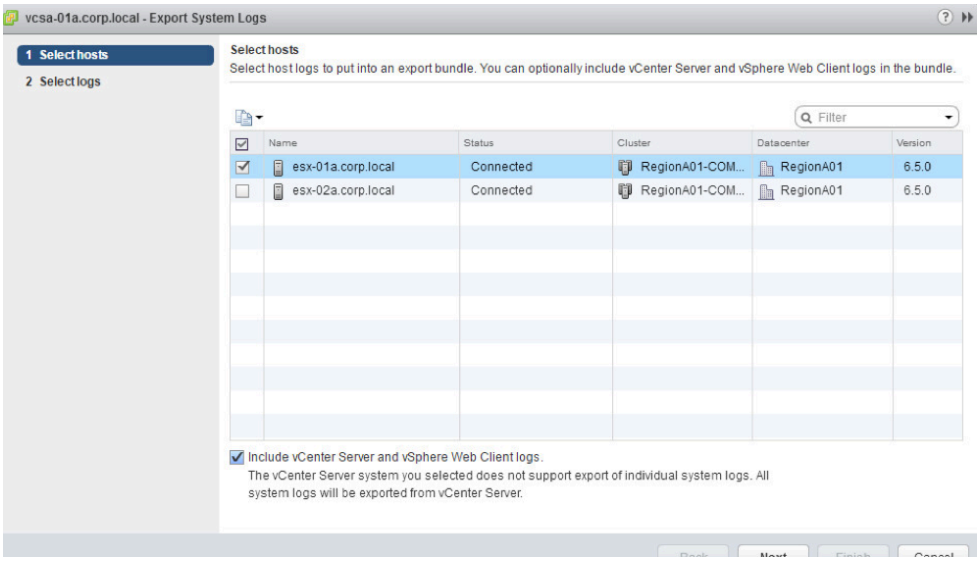
Generate vSphere log bundles

Using vSphere Web Client:
Logon as user with Global.diagnostic privilege and generate / download log bundle REF: *VCP6-DCV Cert Guide* page 431

- In the inventory, select the vCenter Server. In the center pane, click **Actions > Export System Logs**
- Select any ESXi hosts that you wish to include and click Next

- Select the logs you want. Optionally, select **Gather Performance Data** and optionally provide a password for encrypted core dumps
- Provide a file name / location.

To upload directly to VMware, select **Administration > Support > Upload File to Service Request**



From windows on a windows based vCenter
Start > Programs > VMware > Generate vCenter Server log bundle.

Configure and test centralized logging

Test central syslog http://buildvirtual.net/configure-centralized-logging-on-esxi-hosts/

Example: esxcli system syslog config set --loghost vc01.vmlab.loc

Analyze log entries to obtain configuration information

the following commands could be used to run vm-support and to unpack its data, where the working directory is set to a VMFS datastore named NFSA. In this example, assume that the vm-support command automatically named the resulting TGZ file esx-esxi02-2015-10-20--22.14.tgz:

```
vm-support –w /vmfs/volumes/NFSA
cd /vmfs/volumes/NFSA
tar –xzf esx-esxi02-2015-10-20--22.14.tgz
```

Use vm-support to generate data to input into ESXTOP. For example, the following command can be used to collect performance data for 60 seconds at 2-seconds intervals, using a datastore named NFSA as the working directory:

```
vm-support -p -d 60 -i 2 –w /vmfs/volumes/NFSA

tar –xzf esx-esxi02-2015-10-20--22.14.tgz

cd esx-esxi02-2015-10-20--22.14

./reconstruct.sh

esxtop –R esx-esxi02-2015-10-20--22.14
```

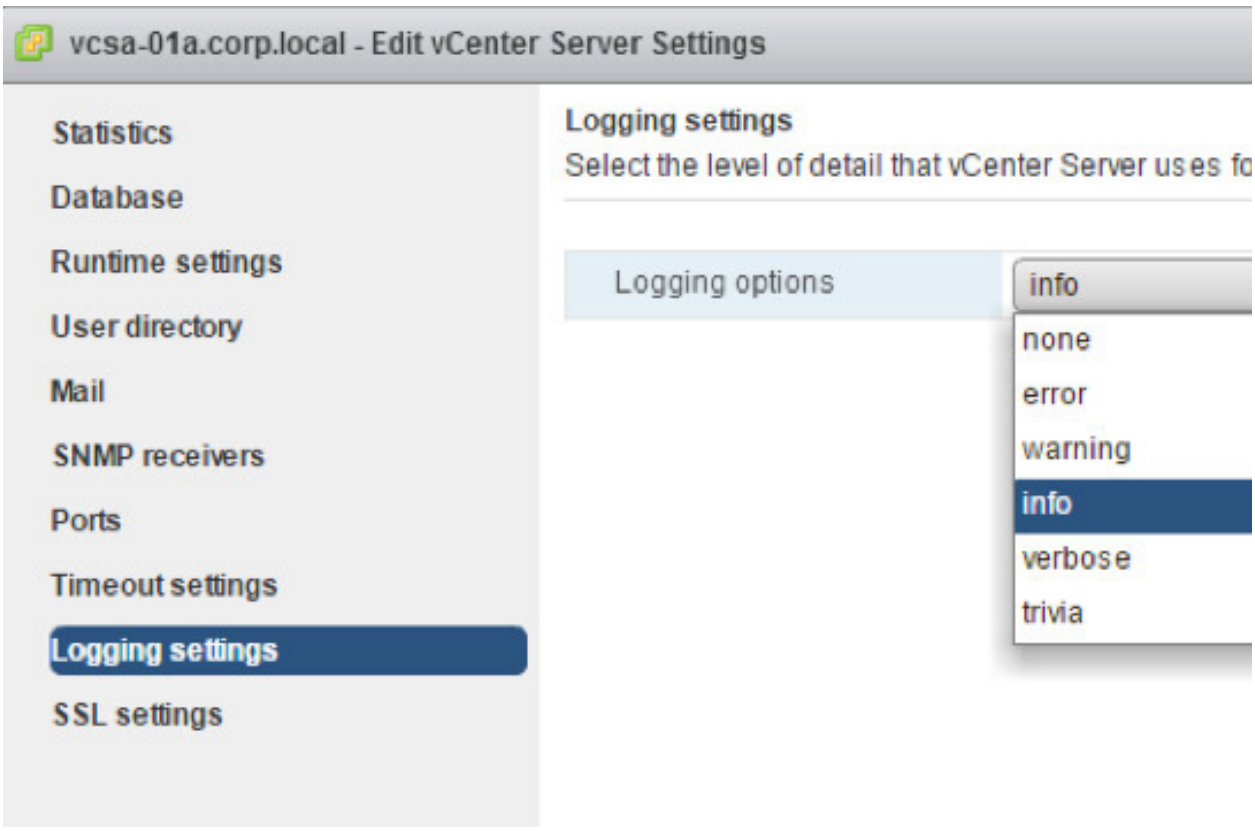
Analyze log entries to identify and resolve issues

Analyze logs REF: *VCP6-DCV Cert Guide* page 362

Configure logging levels for vSphere

Vcenter logging levels REF: *VCP6-DCV Cert Guide* page 440

- Select the vCenter Server
- Click **Manage** > **Settings** > **General** >**Edit**
- Select **Logging Settings**
- Set the logging option to a value, such as verbose, which is useful for troubleshooting



the logging levels are

Logging Option	Description
None (Disable logging)	No vCenter Server logging occurs.
Error (Errors Only)	The vCenter Server collects only error entries into its log files.
Warning (Warning and Errors)	The vCenter Server collects warning and error entries into its log files.
Info (Normal logging)	The vCenter Server collects information, warning, and error entries into its log files.
Verbose (Verbose)	The vCenter Server collects verbose, information, warning, and error entries into its log files.
Trivia (Extended verbose)	The vCenter Server collects trivia, verbose, information, warning, and error entries into its log files.

Esxi host logging level REF: *VCP6-DCV Cert Guide* page 369

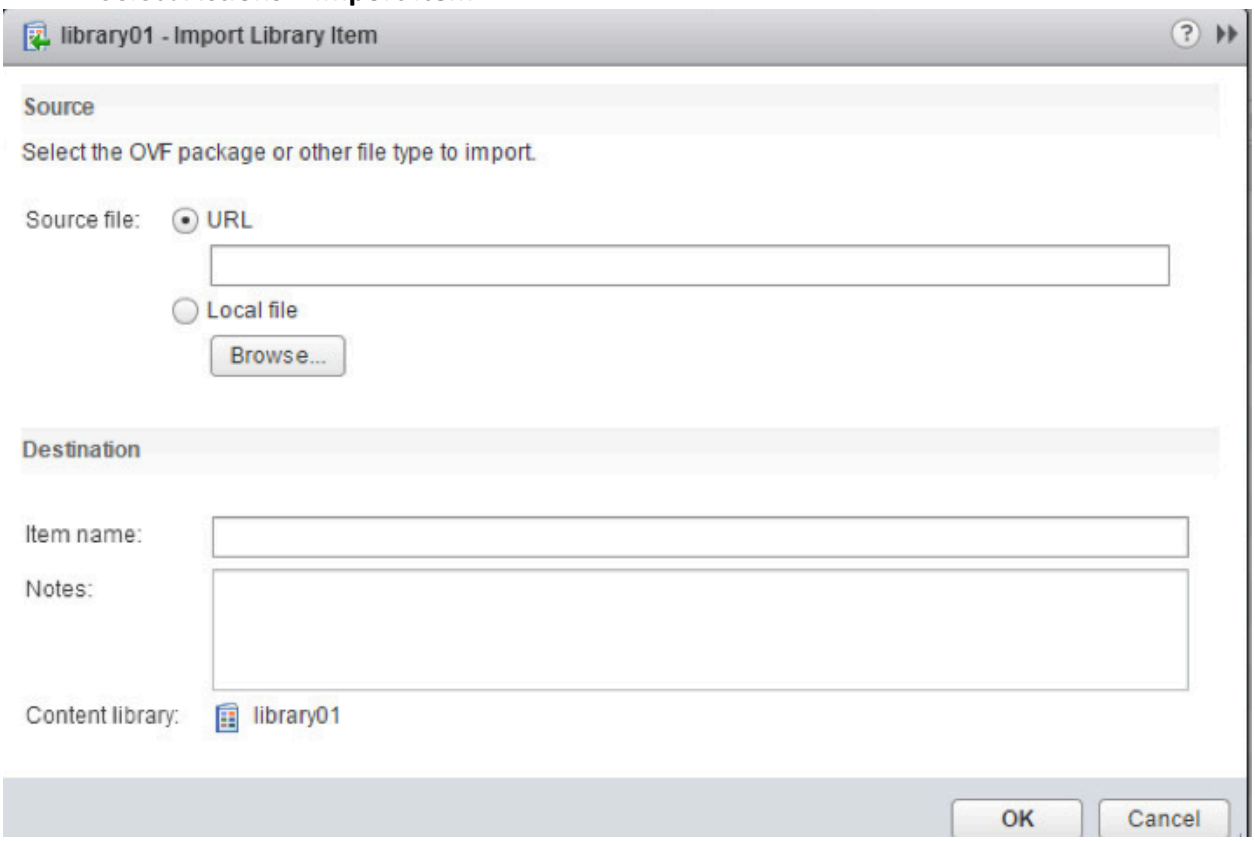
Objective 5.4 - Configure and manage Content Library

Content library:

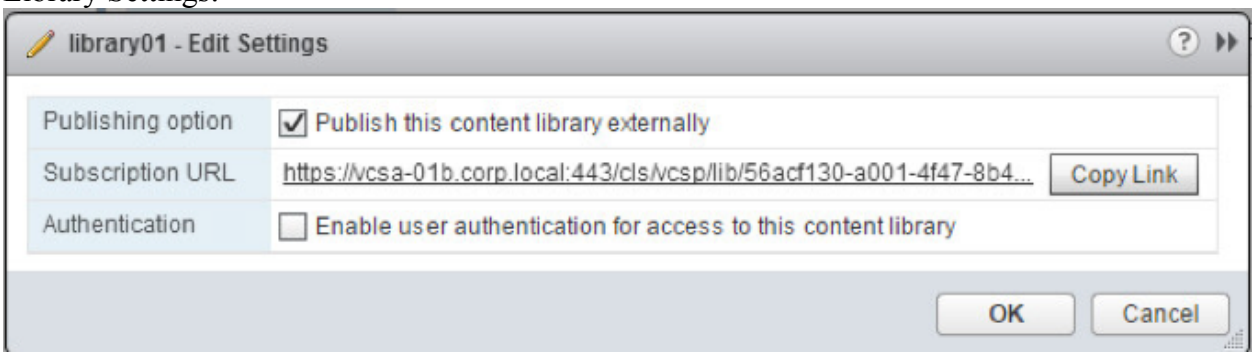
- publish and subscribe REF: *VCP6-DCV Cert Guide* page 614
- global permission (authentication, roles) pp 616
- auto vs on-demand syn pp 614
- space efficiency = on-demaind sync

upload files to a content library

- Home > vCenter Server Lists > Content Libraries
- Select **Actions > Import Item**



Library Settings:



To subscribe to this content library from another vCenter Server, use the Copy Link button (above) and paste it into Subscription URL field.

Create a Global User

Create and manage SSO Users: REF: *VCP6-DCV Cert Guide* page

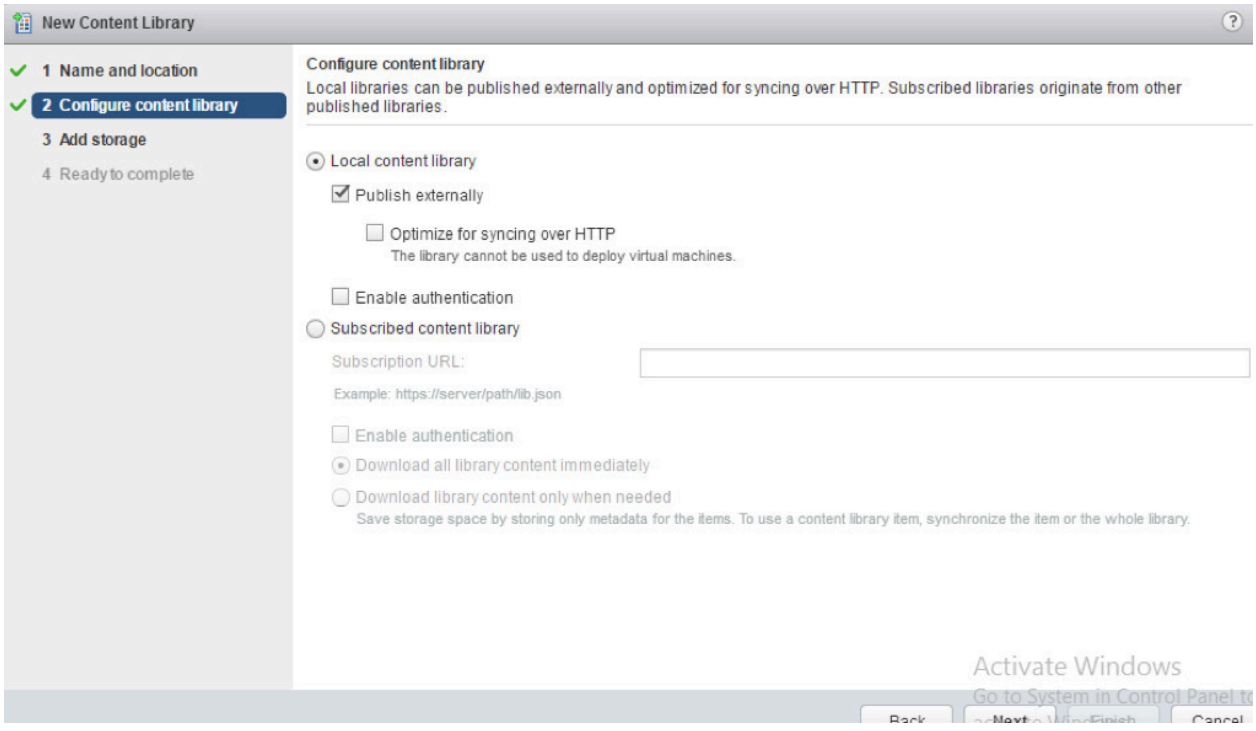
Global Permissions: REF: *VCP6-DCV Cert Guide* page 14

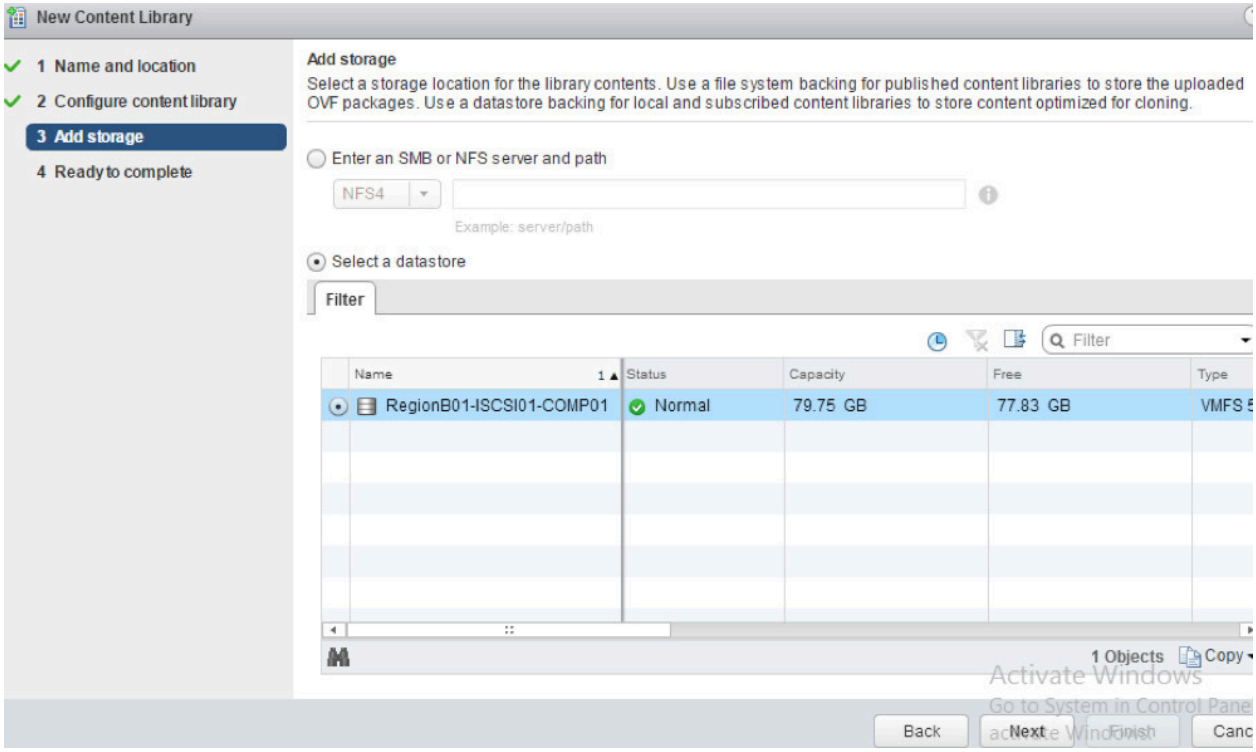
Create a Content Library

REF: *VCP6-DCV Cert Guide* page 612

- drill to Home > vCenter Inventory Lists
- Select **vCenter Home** in the left pane and click on **Summary** tab in the right pane
- In the Actions list, choose **Create Content Library**
- Select **Local content library** (or subscribe to a pre-published path)
    - Optionally, select **publish externally**
    - Add storage, such as a datastore or an NFS / SMB path
    -
-

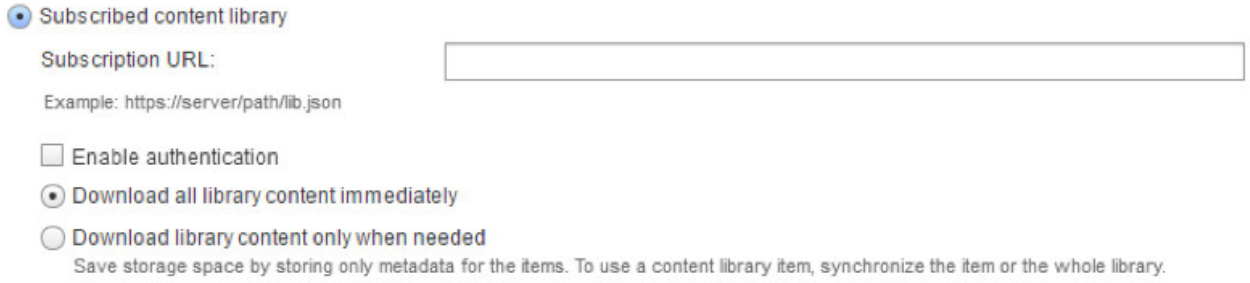

vmware vSphere Web Client
Navigator
Home
vCenter Inventory Lists
vCenter Home
Virtual Machines
vApps
VM Templates in Folders
Content Libraries
Resources
vCenter Servers
Datacenters
Hosts
Clusters
Resource Pools
Datastores
Datastore Clusters
Networks
vCenter Home
Getting Started
Summary
vCenter
Version 6.0
Actions
Create new content library
Create new datacenter
Create new cluster
Create new datastore cluster
Create new distributed switch


New Content Library
1 Name and location
2 Configure content library
3 Add storage
4 Ready to complete
Configure content library
Local libraries can be published externally and optimized for syncing over HTTP. Subscribed libraries originate from other published libraries.
Local content library
Publish externally
Optimize for syncing over HTTP
The library cannot be used to deploy virtual machines.
Enable authentication
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.
Activate Windows
Go to System in Control Panel to
Back
Next
Finish
Cancel



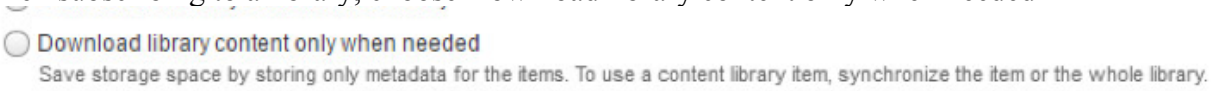
Subscribe to a Content Library

Copy the subscription URL from the published library and paste into the subscribed lib



Configure a Content Library for space efficiency

When subscribing to a library, choose Download library content only when needed



- When creating a local content library that you intend to publish, choose SMB/NFS. So, templates are stored as OVF for published content
- To store content that is optimized for cloning (native format), use a datastore for the local content library

Synchronize a subscribed Content Library

Section 6 - Configure a vSphere Deployment for Performance

Objective 6.1 - Utilize Advanced vSphere Performance Monitoring Tools

Configure esxtop / resxtop custom profiles

esxtop customization (W command, .esxtop50rc)
default profile for resxtop is /home/vi-admin/.esxtop/esxtop50rc
REF: *VCP6-DCV Cert Guide* page 164

alternatives for generating vcenter log bundles (start>programs, vc-support) REF: *VCP6-DCV Cert Guide* page 366

to save a custom provide named /JAD:

- in ESXTOP, after making configuration changes, press **W**
- type in the file name path: `/JAD`
- press q to quit
- `esxtop -c /JAD`

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

vm-support with ESXTOP replay pp 363

Use vm-support to generate data to input into ESXTOP. For example, the following command can be used to collect performance data for 60 seconds at 2-seconds intervals, using a datastore named NFSA as the working directory:

```
vm-support -p -d 60 -i 2 –w /vmfs/volumes/NFSA

tar –xzf esx-esxi02-2015-10-20--22.14.tgz

cd esx-esxi02-2015-10-20--22.14

./reconstruct.sh

esxtop –R esx-esxi02-2015-10-20--22.14
```

Use vScsiStats to gather storage performance data

vscsistat REF: *VCAP5-DCV* page 168

- list info on currently running VMs: `vscsiStats -l`

```
[root@esx-01b:~] vscsiStats -l
Virtual Machine worldGroupID: 69884, Virtual Machine Display Name: linux-App-01a, Virtual Machine Config F
ile: /vmfs/volumes/57281322-2d689290-0710-005056018fc5/linux-App-01a/linux-App-01a.vmx, {
   Virtual SCSI Disk handleID: 8192 (ide0:0)
}
Virtual Machine worldGroupID: 70051, Virtual Machine Display Name: linux-App-02a, Virtual Machine Config F
ile: /vmfs/volumes/57281322-2d689290-0710-005056018fc5/linux-App-02a/linux-App-02a.vmx, {
   Virtual SCSI Disk handleID: 8193 (ide0:0)
}
```

- start vscsiStats collection on a VM whose world ID is 69884: `vscsiStats -s -w 69884`

```
}
[root@esx-01b:~] vscsiStats -s -w 69884
vscsiStats: Starting Vscsi stats collection for worldGroup 69884, handleID 8192 (ide0:0)
Success.
[root@esx-01b:~]
```

- print a histogram on the latency metric: `vscsiStats -p latency`

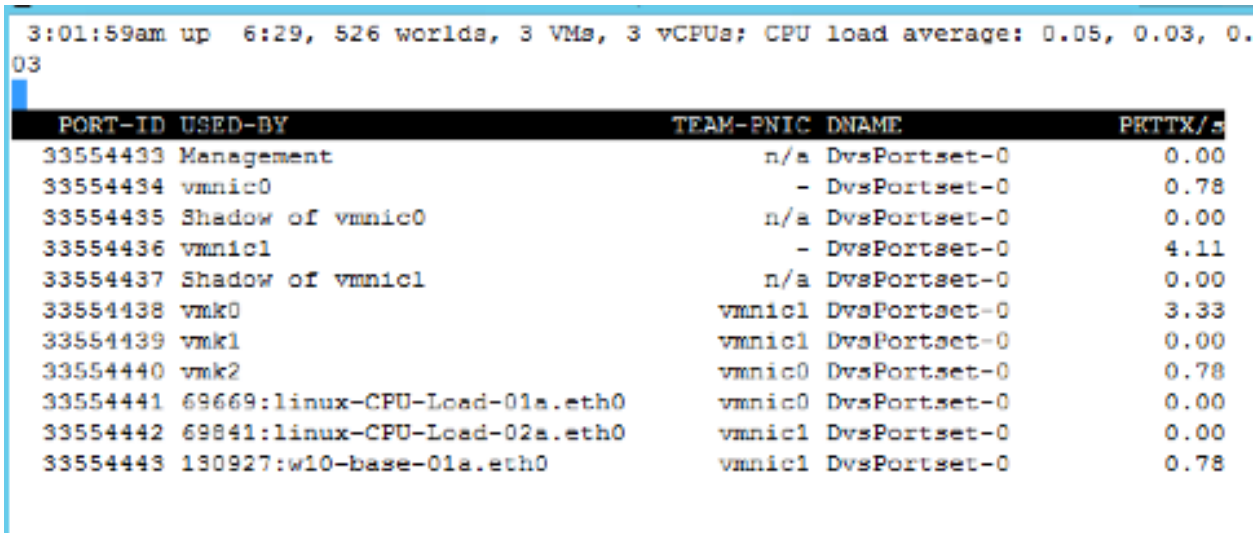
```
Success.
[root@esx-01b:~] vscsiStats -p latency
Histogram: latency of IOs in Microseconds (us) for virtual machine worldGroup
leID : 8192 (ide0:0) {
 min : 0
 max : 0
 mean : 0
 count : 0
   {
      0                    (<=                  1)
      0                    (<=                 10)
      0                    (<=                100)
      0                    (<=                500)
      0                    (<=               1000)
      0                    (<=               5000)
      0                    (<=              15000)
      0                    (<=              30000)
      0                    (<=              50000)
      0                    (<=             100000)
      0                    (>               100000)
   }
}
```

Use esxtop / resxtop to collect performance data

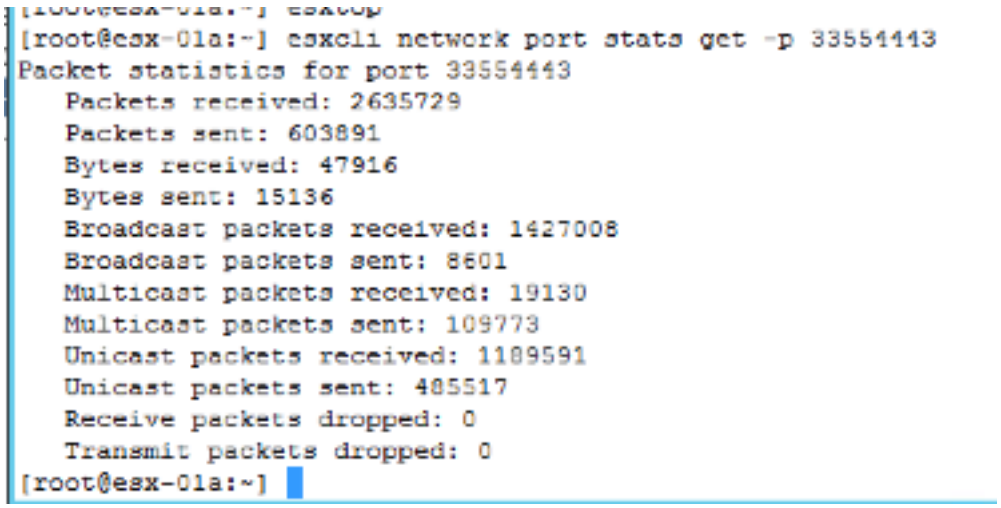
In esxtop, navigate view performace data using these keys:

- c: CPU metrics
- m: memory metrics
- n: network metrics
- u: disk unit (LUN / devices) metrics
- d: storage adapter metrics
- v: virtual disk metrics

The values in the PortID column in the ESXTOP network (n) can be used in the `esxcli network port` command to view port statistics



```
 3:01:59am up  6:29, 526 worlds, 3 VMs, 3 vCPUs; CPU load average: 0.05, 0.03, 0.
03

   PORT-ID USED-BY                          TEAM-PNIC DNAME              PKTTX/s
  33554433 Management                             n/a DvsPortset-0          0.00
  33554434 vmnic0                                   - DvsPortset-0          0.78
  33554435 Shadow of vmnic0                       n/a DvsPortset-0          0.00
  33554436 vmnic1                                   - DvsPortset-0          4.11
  33554437 Shadow of vmnic1                       n/a DvsPortset-0          0.00
  33554438 vmk0                                vmnic1 DvsPortset-0          3.33
  33554439 vmk1                                vmnic1 DvsPortset-0          0.00
  33554440 vmk2                                vmnic0 DvsPortset-0          0.78
  33554441 69669:linux-CPU-Load-01a.eth0       vmnic0 DvsPortset-0          0.00
  33554442 69841:linux-CPU-Load-02a.eth0       vmnic1 DvsPortset-0          0.00
  33554443 130927:w10-base-01a.eth0            vmnic1 DvsPortset-0          0.78
```



```
[root@esx-01a:~] esxtop
[root@esx-01a:~] esxcli network port stats get -p 33554443
Packet statistics for port 33554443
   Packets received: 2635729
   Packets sent: 603891
   Bytes received: 47916
   Bytes sent: 15136
   Broadcast packets received: 1427008
   Broadcast packets sent: 8601
   Multicast packets received: 19130
   Multicast packets sent: 109773
   Unicast packets received: 1189591
   Unicast packets sent: 485517
   Receive packets dropped: 0
   Transmit packets dropped: 0
[root@esx-01a:~]
```

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

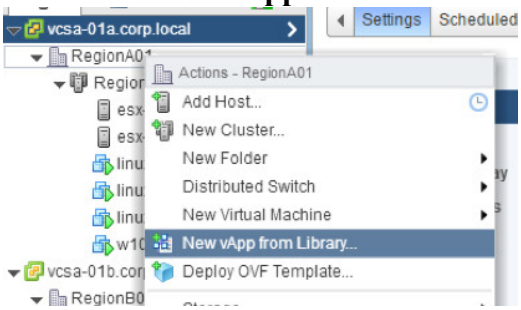
The values in the PortID column in the ESXTOP network (n) can be used in the `esxcli network port` command to view port statistics

```
 3:01:59am up  6:29, 526 worlds, 3 VMs, 3 vCPUs; CPU load average: 0.05, 0.03, 0.
03

   PORT-ID USED-BY                                  TEAM-PNIC DNAME              PKTTX/s
  33554433 Management                                     n/a DvsPortset-0          0.00
  33554434 vmnic0                                           - DvsPortset-0          0.78
  33554435 Shadow of vmnic0                               n/a DvsPortset-0          0.00
  33554436 vmnic1                                           - DvsPortset-0          4.11
  33554437 Shadow of vmnic1                               n/a DvsPortset-0          0.00
  33554438 vmk0                                         vmnic1 DvsPortset-0          3.33
  33554439 vmk1                                         vmnic1 DvsPortset-0          0.00
  33554440 vmk2                                         vmnic0 DvsPortset-0          0.78
  33554441 69669:linux-CPU-Load-01a.eth0                vmnic0 DvsPortset-0          0.00
  33554442 69841:linux-CPU-Load-02a.eth0                vmnic1 DvsPortset-0          0.00
  33554443 180927:w10-base-01a.eth0                     vmnic1 DvsPortset-0          0.78
```

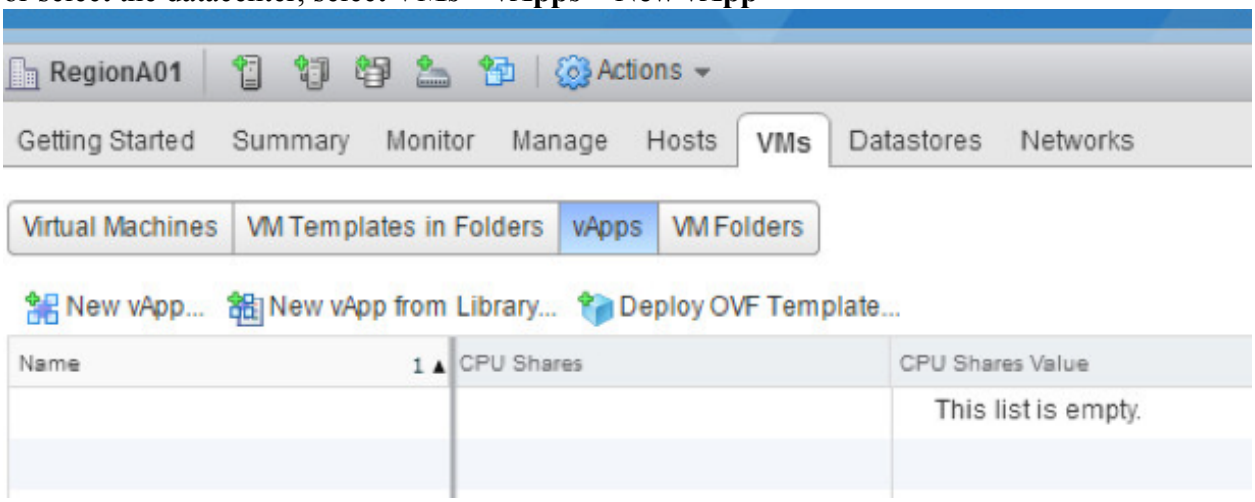
```
[root@esx-01a:~] esxcli network port stats get -p 33554443
Packet statistics for port 33554443
   Packets received: 2635729
   Packets sent: 603891
   Bytes received: 47916
   Bytes sent: 15136
   Broadcast packets received: 1427008
   Broadcast packets sent: 8601
   Multicast packets received: 19130
   Multicast packets sent: 109773
   Unicast packets received: 1189591
   Unicast packets sent: 485517
   Receive packets dropped: 0
   Transmit packets dropped: 0
[root@esx-01a:~]
```

Objective 6.2 - Optimize Virtual Machine resources

How to create a vApp: Select a the datacenter and choose **New vApp from Library**



or select the datacenter, select **VMs** > **vApps** > **New vApp**



Tune VM scsi controller config REF: *VCP6-DCV Cert Guide* page 163

Adjust Virtual Machine properties according to a deployment plan:

Network configurations

CPU configurations

Storage configurations

Troubleshoot Virtual Machine performance issues based on application workload:

REF: *VCP6-DCV Cert Guide* page - 473

Modify Transparent Page Sharing and large memory page settings

REF: http://bit.ly/2f6tQQ3

VMware KB: http://bit.ly/1TVoST9

Advanced Memory Attributes

Attribute	Description	Default
Mem.ShareForceSalting	Mem.ShareForceSalting 0: Inter-virtual machine Transparent Page Sharing (TPS) behavior is still retained. The value of VMX option **`sched.mem.pshare.salt`** is ignored even if present. Mem.ShareForceSalting 1: By default the salt value is taken from **`sched.mem.pshare.salt`**. If not specified, it falls back to old TPS (inter-VM) behavior by considering salt values for the virtual machine as 0. Mem.ShareForceSalting 2: By default the salt value is taken from **`sched.mem.pshare.salt`** if present, or **`vc.uuid`**. If it does not exist, then the page sharing algorithm generates random and unique value for salting per virtual machine, which is not configurable by users.	2
Mem.SamplePeriod	Specifies the periodic time interval, measured in seconds of the virtual machine's execution time, over which memory activity is monitored to estimate working set sizes.	60
Mem.BalancePeriod	Specifies the periodic time interval, in seconds, for automatic memory reallocations. Significant changes in the amount of free memory also trigger reallocations.	15
Mem.IdleTax	Specifies the idle memory tax rate, as a percentage. This tax effectively charges virtual machines more for idle memory than for memory they are actively using. A tax rate of 0 percent defines an allocation policy that ignores working sets and allocates memory strictly based on shares. A high tax rate results in an allocation policy that allows idle memory to be reallocated away from virtual machines that are unproductively hoarding it.	75
Mem.ShareScanGHz	Specifies the maximum amount of memory pages to scan (per second) for page sharing opportunities for each GHz of available host CPU resource. For example, defaults to 4 MB/sec per 1 GHz.	4
Mem.ShareScanTime	Specifies the time, in minutes, within which an entire virtual machine is scanned for page sharing opportunities. Defaults to 60 minutes.	60
Mem.CtlMaxPercent	Limits the maximum amount of memory reclaimed from any virtual machine using the memory balloon driver (`vmmemctl`), based on a percentage of its configured memory size. Specify 0 to disable reclamation for all virtual machines.	65
Mem.AllocGuestLargePage	Enables backing of guest large pages with host large pages. Reduces TLB misses and improves performance in server workloads that use guest large pages. 0=disable.	1
Mem.AllocUsePSharePool and Mem.AllocUseGuestPool	Reduces memory fragmentation by improving the probability of backing guest large pages with host large pages. If host memory is fragmented, the availability of host large pages is reduced. 0 = disable.	15
Mem.MemZipEnable	Enables memory compression for the host. 0 = disable.	1
Mem.MemZipMaxPct	Specifies the maximum size of the compression cache in terms of the maximum percentage of each virtual machine's memory that can be stored as compressed memory.	10
LPage.LPageDefragEnable	Enables large page defragmentation. 0 = disable.	1
LPage.LPageDefragRateVM	Maximum number of large page defragmentation attempts per second per virtual machine. Accepted values range from 1 to 1024.	32
LPage.LPageDefragRateTotal	Maximum number of large page defragmentation attempts per second. Accepted values range from 1 to 10240.	256
LPage.LPageAlwaysTryForNPT	Try to allocate large pages for nested page tables (called 'RVI' by AMD or 'EPT' by Intel). If you enable this option, all guest memory is backed with large pages in machines that use nested page tables (for example, AMD Barcelona). If NPT is not available, only some portion	

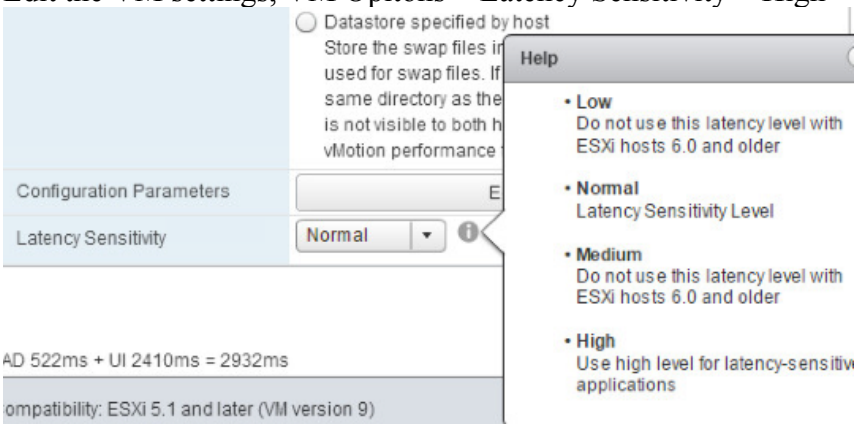
of guest memory is backed with large pages. 0= disable.

Salting: REF: *VCP6-DCV Cert Guide* page 607
`sched.mem.pshare.salt` controls the virtual machine's ability to participate in transparent page sharing. ESXi 6.0 and recent patches to ESXi 5.x introduced the concept of salting to address recent security concerns associated with transparent page sharing (TPS). TPS is allowed only within a virtual machine (intra-VM TPS) by default. Because the ESXi Host configuration option `Mem.ShareForceSalting` is set to 2, the `sched.mem.pshare.salt` is not present in the virtual machine configuration file, and thus the virtual machine salt value is set to a unique value. In this case, to allow TPS among a specific set of virtual machines, set `sched.mem.pshare.salt` for each virtual machine in the set to an identical value. Alternatively, to enable TPS among all virtual machines (inter-VM TPS), you can set `Mem.ShareForceSalting` to 0. In this case, the value of `sched.mem.pshare.salt` is ignored and has no impact. Or to enable inter-VM TPS as the default but yet allow the use of `sched.mem.pshare.salt to` control the effect of TPS per virtual machine, set the value of Mem.ShareForceSalting to 1. In this case, change the value of `sched.mem.pshare.salt` per virtual machine to prevent it from sharing with all virtual machines

and restrict it to sharing only with those that have an identical setting.

Optimize a Virtual Machine for latency sensitive workloads

Edit the VM settings, VM Opitons > Latency Sensitivity = High



Edit the VM and set CPU and Memory reservation, limit and shares.

Configure Flash Read Cache reservations

REF: *VCP6-DCV Cert Guide* page 301

- Verify the VM is compatablie with ESXi 5.5 or later
- Edit the settings for a VM, Virtual Hardware > Hard disk
- Set a value (GB) in the **Virtual Flash Read Cache**
- Click the **Advanced** link next to Virtual Flash Read Cache
- Check the **Enable Virtual Flash Read Cache**
- Set a **Reservation** (GB) **and Block Size** (KB). Click **OK**.

Section 7 - Configure a vSphere 6.x Environment for Recoverability

Objective 7.1- Deploy and manage vSphere Replication

Configure and manage a vSphere Replication infrastructure:

Vsphere replication and VMCA certs REF: *VCP6-DCV Cert Guide* page 341

vRA installation and configuration REF: *VCP6-DCV Cert Guide* page 34

Isolate vSphere Replication network traffic

You can designate that specific vmkernel virtual adapters are used for vSphere Replication. REF: http://bit.ly/2gkuET3

- To control which vmkernel adapters are used to send replication data from the source host, check the vSphere Replication Traffic checkbox in the vmkernel virtual adapter settings.
- To control which vmkernel adapters are use to receive NFC traffic on the target host, select vSphere Replication NFC Traffic.
- To use multiple vNICs in a vSphere Replication Appliance and designate one for inbound replication traffic, add a 2nd vNIC to the appliance and used the VAMI to set **IP Address for Incoming Storage Traffic**
- Likewise, you can add another vNIC and set **IP Address for VRMS Management Traffic**

Enable data compression of vSphere Replication traffic

Verify that vSphere 6.x is used from end to end. In the wizard used to configure replication on a set of VMs, choose the **Enable Network Compression for VR Data** option. REF: REF: *VCP6-DCV Cert Guide* page page 344

Configure and manage vSphere Replication of virtual machines

REF: *VCP6-DCV Cert Guide* page 342

Analyze and resolve vSphere Replication issues:

To migrate a protected VM from an ESXi 6 host to ESXi5, you may need to disable data compression.

Storage configuration

No special storage configuration is required other than ample space is required to accommodate the replication settings. Note that including points in time for VM replication requires additional space.

Multiple point in time snapshots

REF: *VCP6-DCV Cert Guide* page 343

Enabling vSphere Replication on VMs

REF: *VCP6-DCV Cert Guide* page 342

Objective 7.2 - Deploy and Manage vSphere Data Protection

Create, edit and clone a vSphere Data Protection backup job

configure VDP REF: *VCP6-DCV Cert Guide* page 327:
Deploy VDP appliance from OVA: REF: *VCP6-DCV Cert Guide* page 331

initial VDP config REF: *VCP6-DCV Cert Guide* page 332

- Browse to https://VDP-IP-adrress:**8543/vdp-configure/**
- Logon as root (pass = `changeme` by default)
- Configure networking settings, credentials, and vCenter regirstration

create VDP backup job REF: *VCP6-DCV Cert Guide* page 334

Modify a preconfigured backup job.

Backup and restore a Virtual Machine (file level restore, full VM backup)

restore using VDP REF: *VCP6-DCV Cert Guide* page 335

file level VDP restore REF: http://bit.ly/2fkjqxr

Create a replication job according to a deployment plan

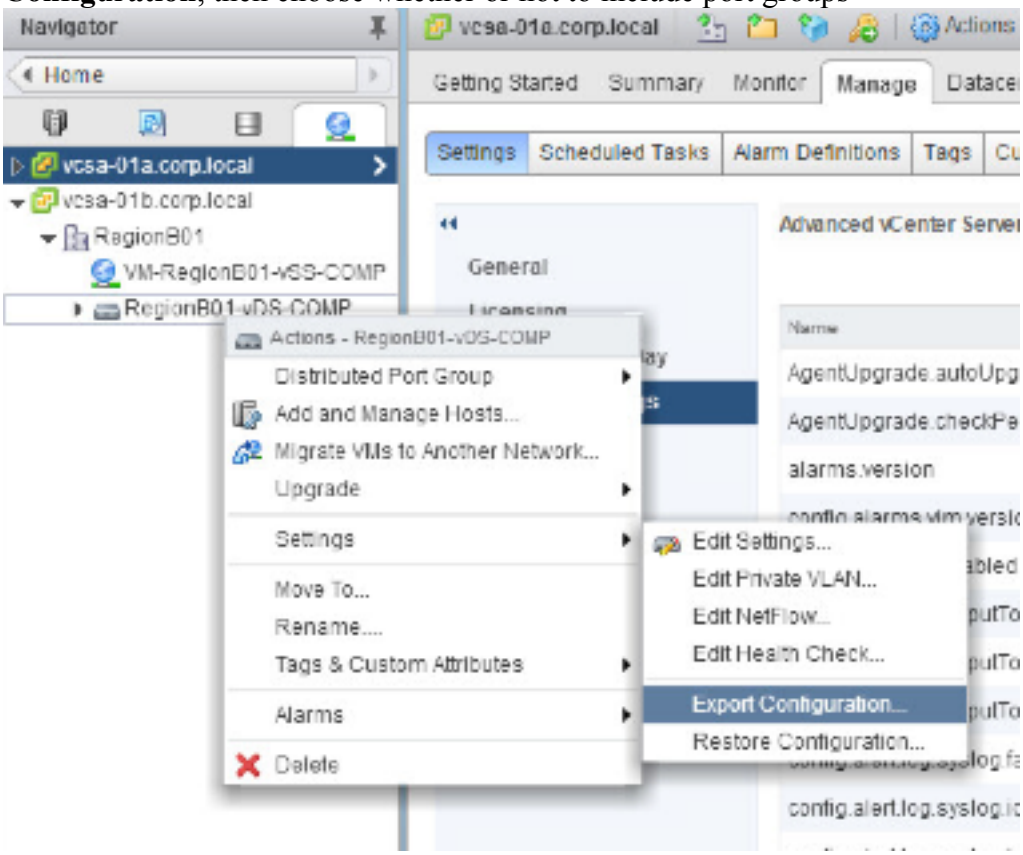
REF: *VCP6-DCV Cert Guide* page : 324

Configure a Backup Verification job to ensure integrity of restore points

Objective 7.3 - Backup and Recover vSphere Configurations

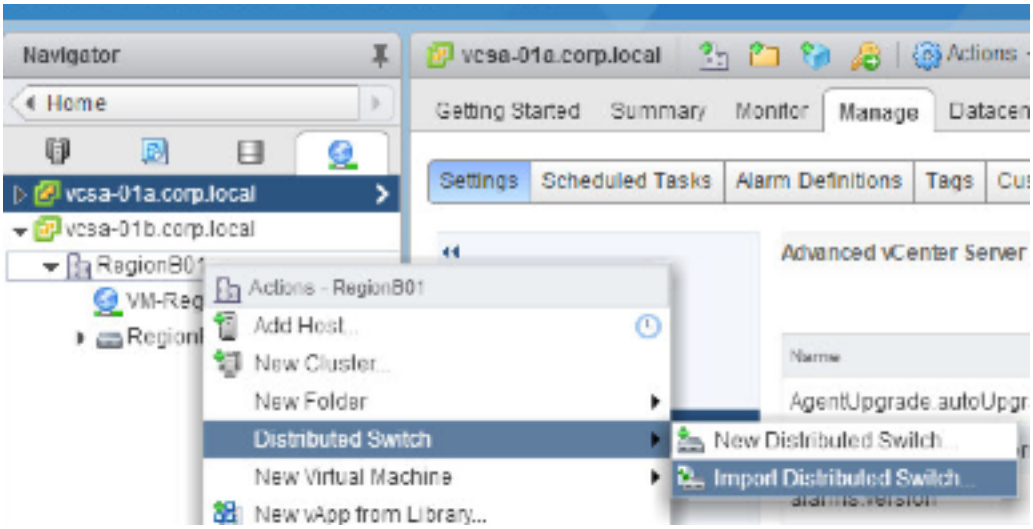
Backup and restore distributed switch configurations

Export dvSwitch Configuration: right-click on dvSwitch, select **Settings** > **Export Configuration**, then choose whether or not to include port groups



Restore dvSwitch Configuration: right-click on dvSwitch, select **Settings** > **Restore Configuration**, then choose whether or not to include port groups

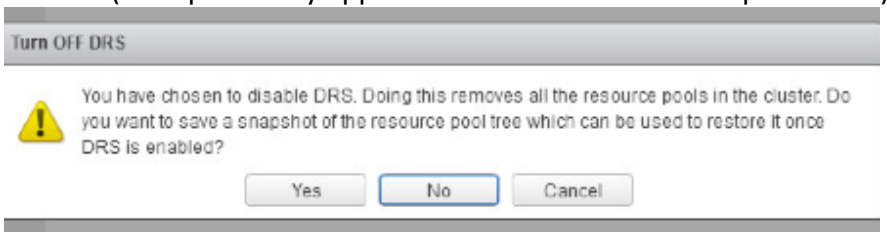
Import dvSwitch:



Backup and restore resource pool configurations

Save resource pool tree snapshot and use it to restore REF: *VCP6-DCV Cert Guide* page 510

- Select the cluster, click **Manage** > **Settings** > **vSphere DRS**, click **Edit**
- *De-select* **Turn on vSphere DRS**
- Click **OK**
- When prompted, select option to save the resource pools and provide a location to save the file. (the option only appears if at least one resource pool exists)



restore DRS resource pools:

- Right-click the cluster, select **Restore Resource Pool Tree**
- Browse to and select the snapshot file.

Export Virtual Machines to OVA/OVF format

Right-click on VM, click **Templates** > **Export OVF Template**. In the wizard choose to export to OVF (a folder of files) or OVA (a single file).

Use a Host profile to recover an ESXi host configuration

- Right-click the host, select **Host Profile** > **Check Host Profile Compliance**
- Right-click the host, select **Host Profile** > **Remediate**
- In the remediation wizard, use the **Pre-Check Remediation** button.
- If all looks good, then optionally select Reboot Hosts when required and Finish the wizard
-

Section 8 - Configure a vSphere 6.x Environment for Security

Objective 8.1 - Manage authentication and end-user security

Add/Edit Remove users on an ESXi host

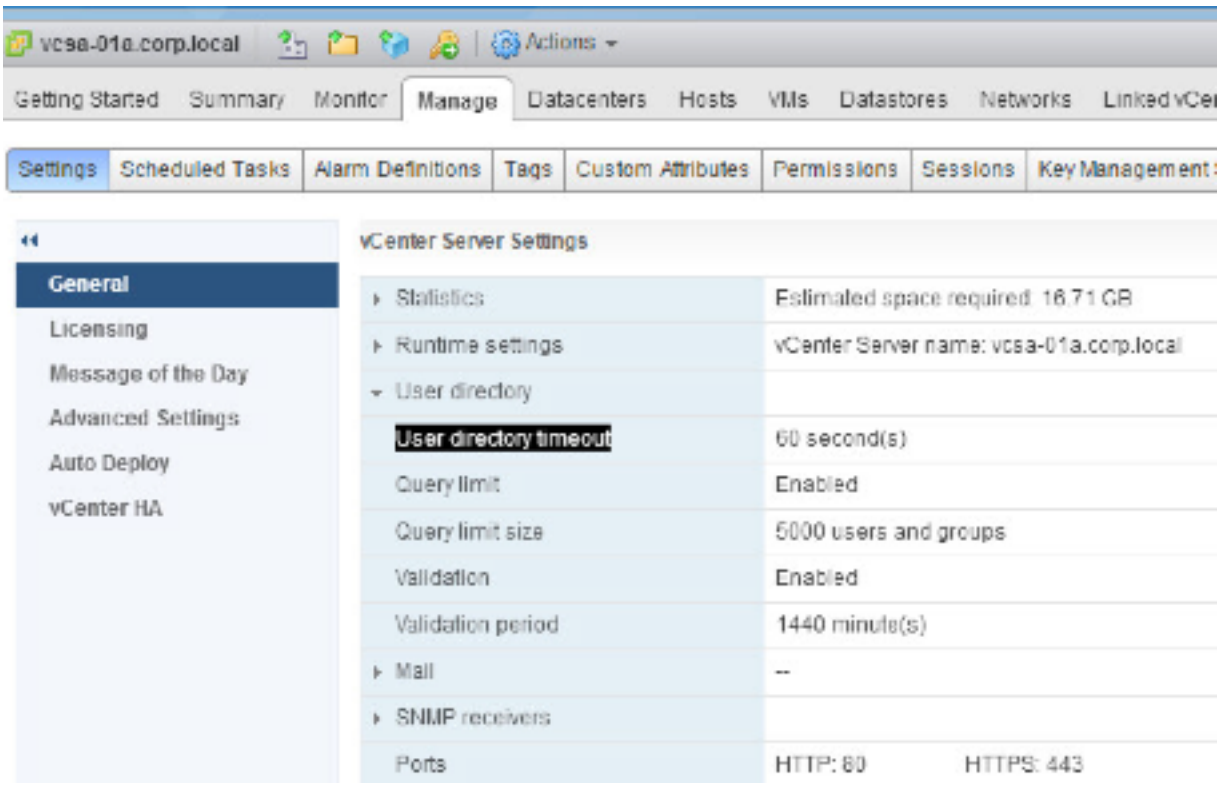
Use the vSphere client (not the vSphere Web client) to logon directly to the ESXi host and drill to the Local Users and Groups tab
REF: http://bit.ly/2ejLCOp

Configure vCenter Roles and Permissions according to a deployment plan

Configure and manage Active Directory integration

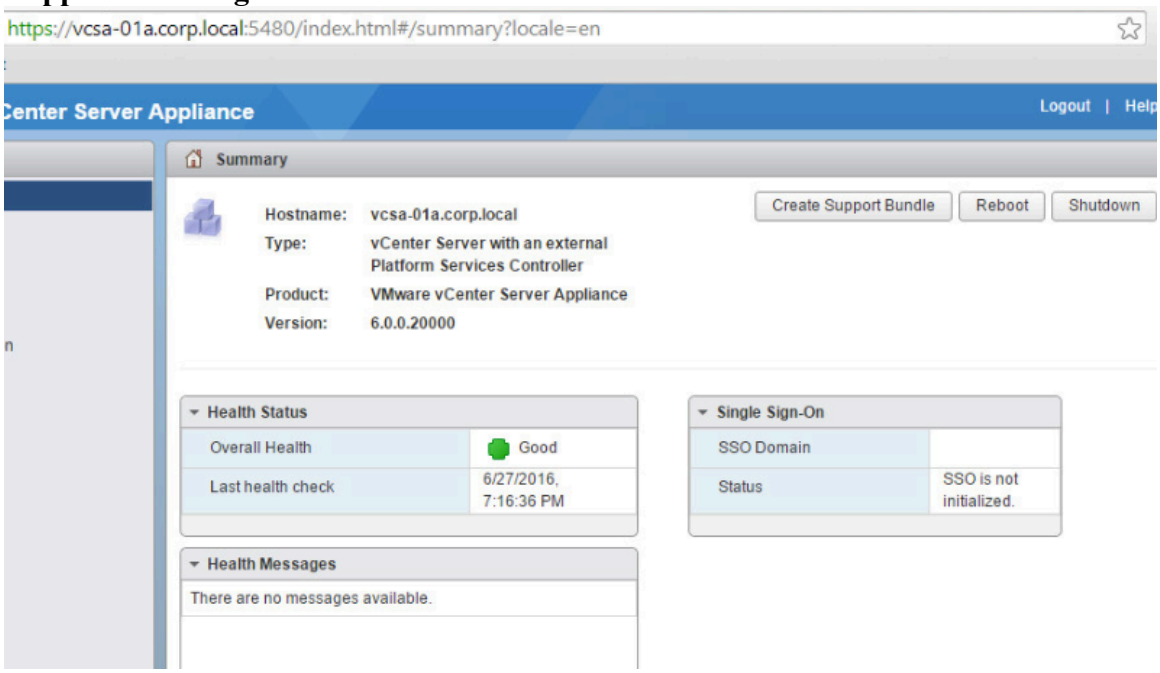
vCenter – AD integration REF: *VCP6-DCV Cert Guide* page 17

vCenter User Directory settings:



add **AD (Integrated Windows Auth) identity source** when SSO is a member in AD domain. Use AD as LDAP otherwise REF: *VCP6-DCV Cert Guide* page 45

vCenter appliance config



add ESXi to AD domain REF: *VCP6-DCV Cert Guide* page 35

Analyze logs for security-related messages

Examine these logs on the ESXi host, using SSH

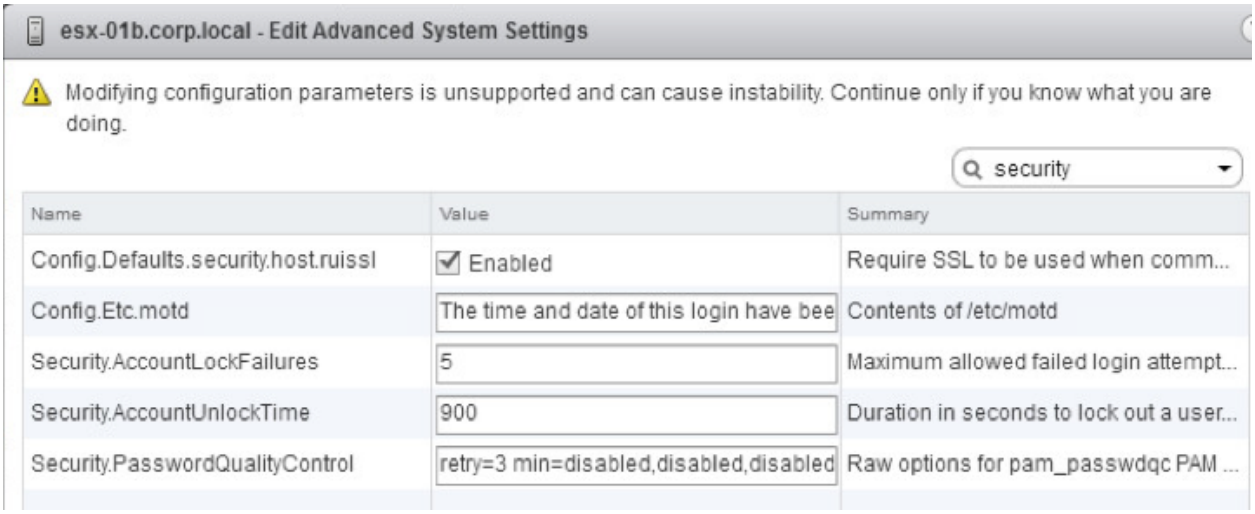
- /var/log/auth.log: ESXi Shell authentication success and failure attempts.
- /var/log/shell.log: ESXi Shell usage logs, including enable/disable and every command entered.
- /var/log/esxupdate.log: ESXi patch and update installation logs.

REF: http://bit.ly/2eFg9XI

Enable and configure an ESXI Pass Phrase

REF: *VCP6-DCV Cert Guide* page page 34
`Security.PasswordQualityControl` Default value:
`retry=3 min=disabled,disabled,disabled,7,7`

Example setting: to require a passphrase with a minimum of 16 characters and 3 words, set the **Security.PasswordQualityControl** to:
`retry=3 min=disabled,disabled,16,7,7,passphrase=3`



Disable the Managed Object Browser (MOB) to reduce attack surface

Enable MOB REF: *VCP6-DCV Cert Guide* page 39
You can use the vSphere Web Client to enable or disable the `Config.HostAgent.plugins.solo.enableMob` advanced system setting.

Objective 8.2 - Manage SSL certificates

VMCA: REF: *VCP6-DCV Cert Guide* page 51
During an up- grade to vSphere 6.0, all self-signed certificates are replaced with certificates signed by VMCA.

VMware Certificate Manager
REF:
https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2097936
REF: *VCP6-DCV Cert Guide* page 39, 50-51

Run certificate-manager in a command prompt. In vCenter Appliance (actually the PSC appliance), run this command:
`/usr/lib/vmware-vmca/bin/certificate-manager`.

VECS-cli REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-80C30209-028D-4F92-9551-CDB6B25A8403.html?resultof=%22%76%65%63%73%22%20%22%76%65%63%22%20

Troubleshoot vCenter / ESXi certs REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.troubleshooting.doc/GUID-2C61E02D-D0D3-4BB5-B4FD-B0DD97791EE9.html?resultof=%22%67%65%6e%65%72%61%74%65%22%20%22%67%65

%6e%65%72%22%20%22%65%73%78%69%22%20%22%63%65%72%74%69%66%69%63%61%74%65%22%20%22%63%65%72%74%69%66%22%20

Stop the vmdir service: use this command on the PSC appliance:
`service-control --stop vmdird`
REF: pp 16

Configure and manage VMware Certificate Authority

Replace Existing VMCA-Signed Certificates With New VMCA-Signed Certificates: REF http://bit.ly/2etrNat

Generate new cert:
certool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config <config_file>

replace the existing root cert
certool --rootca --cert <cert_file_path> --privkey <key_file_path>

Generate a new sigining request:
`certool --initcsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>`

Configure and manage VMware Endpoint Certificate Store

VECS does not store ESXi certificates. ESXi certificates are stored locally on the ESXi Host, in the /etc/vmware/ssl directory. REF: *VCP6-DCV Cert Guide* page 55

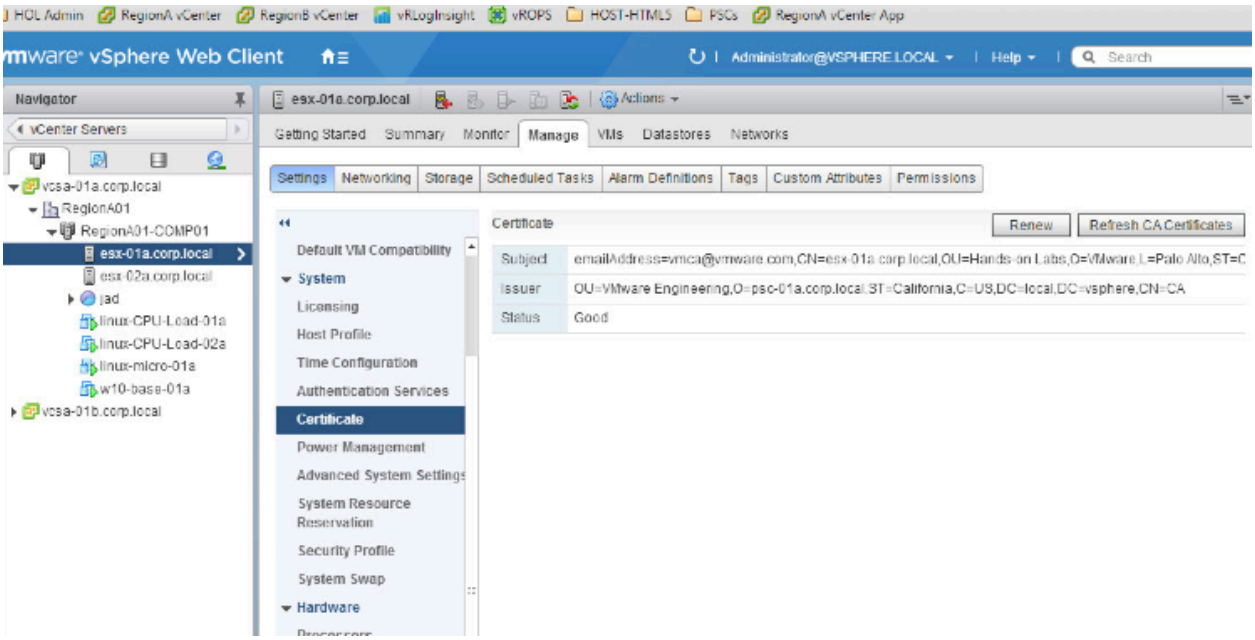
VECS CLI commands: REF: http://bit.ly/2f6Ug4l

Example: create a store:
`vecs-cli store create --name <store>`

Enable / Disable certificate checking

Select the vCenter Server, click Manage > Settings > SSL Settings. Check the box for vCenter requires verifired host certs

Generate ESXi host certificates



Renew / refresh ESXi certs – select the host, select Manage > Settings and click the **Renew** or **Refresh Certificates** button

REF: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-ECFD1A29-0534-4118-B762-967A113D5CAA.html?resultof=%22%65%73%78%69%22%20%22%63%65%72%74%69%66%69%63%61%74%65%22%20%22%63%65%72%74%69%66%22%20

Replace default certificate with CA-signed certificate

Configure SSL timeouts according to a deployment plan

configure vCenter SSL timeout setting https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.vcenterhost.doc/GUID-11E78203-C7E8-4076-8350-1EA5FABA498F.html?resultof=%22%73%73%6c%22%20%22%74%69%6d%65%6f%75%74%22%20

Objective 8.3 - Harden a vSphere 6.x Deployment

Enable and configure ESXi Lockdown mode (Strict / Normal)

REF: *VCP6-DCV Cert Guide* page 37

Configure a user on the Lockdown Mode Exception Users list

ESXi lockdown mode, exception users REF: *VCP6-DCV Cert Guide* page 37

Customize SSH settings for increased security

ESXi Shell Availability Timeout and Idle Timeout REF: *VCP6-DCV Cert Guide* page 38

Create a Timeout for ESXi Shell Availability in the Direct Console User Interface

The ESXi Shell is disabled by default. You can set an availability timeout for the ESXi Shell to increase security when you enable the shell.

The availability timeout setting is the amount of time that can elapse before you must log in after the ESXi Shell is enabled. After the timeout period, the service is disabled and users are not allowed to log in.

Procedure

1. From the Troubleshooting Mode Options menu, select **Modify ESXi Shell and SSH timeouts** and press Enter.
2. Enter the availability timeout.

   You must restart the SSH service and the ESXi Shell service for the timeout to take effect.
3. Press Enter and press Esc until you return to the main menu of the Direct Console User Interface.
4. Click **OK**.

If you are logged in when the timeout period elapses, your session will persist. However, after you log out or your session is terminate

SSH PermitRootLogin REF: *VCP6-DCV Cert Guide* page 39

Enable strong passwords and configure password policies

ESXi pass phrase

we can set the password / pass phrase in the web client on the ESXi host with Advanced System Settings > Password quality control or with a command.

ESXi Pass Phrase

Instead of a password, you can also use a pass phrase, however, pass phrases are disabled by default. You can change this default or other settings, by using the `Security.PasswordQualityControl` advanced option for your ESXi host from the vSphere Web Client.

For example, you can change the option to the following:

```
retry=3 min=disabled,disabled,16,7,7
```

This example allows pass phrases of at least 16 characters and at least 3 words, separated by spaces.

Making changes to the `/etc/pamd/passwd` file is still supported for legacy hosts but is deprecated for future releases.

Changing Default Password or Pass Phrase Restrictions

You can change the default restriction on passwords or pass phrases by using the `Security.PasswordQualityControl` advanced option for your ESXi host. By default, option is set as follows:

```
retry=3 min=disabled,disabled,disabled,7,7
```

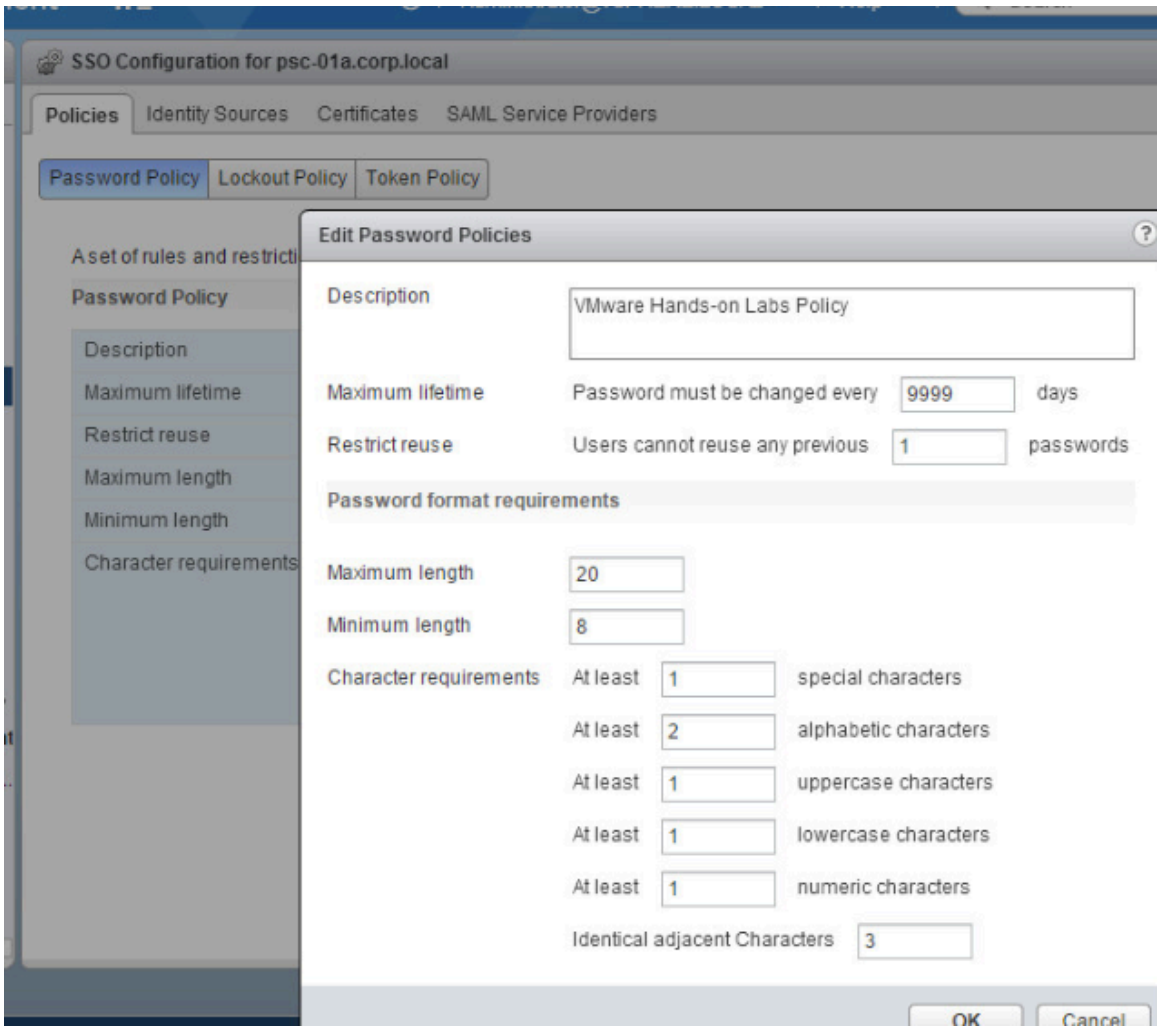
You can change the default, for example, to require a minimum of 15 characters and a minimum number of four words, as follows:

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

See the manpage for `pam_passwdqc` for more information.

So, the key to understanding the parameters is:
min=N0,N1,N2,N3,N4
N0 is used for passwords consisting of characters from one character class only. The character classes are: digits, lower-case letters, upper-case letters, and other characters. There is also a special class for non-ASCII characters, which could not be classified, but are assumed to be non-digits.
N1 is used for passwords consisting of characters from two character classes that do not meet the requirements for a passphrase.
N2 is used for passphrases. Note that besides meeting this length requirement, a passphrase must also consist of a sufficient number of words (see the passphrase option below).
N3 and N4 are used for passwords consisting of characters from three and four character classes, respectively.
To require a passphrase, include this: *passphrase=N*

SSO password policy



Configure vSphere hardening of virtual machines according to a deployment plan

Harden VMs:

- VM tools auto upgrade REF: *VCP6-DCV Cert Guide* page 24
- Vm tools ver 6.0 compatibility hw ver 11 128 cores 4080 GB ESXi 6.0 and later REF: *VCP6-DCV Cert Guide* page 25
- Vm tools settins REF: *VCP6-DCV Cert Guide* page 26

Upgrade VMware Compatibility:

- Right-click the VM, Compatiability > Upgrade VM Compatability (or schedule it)

- If you schedule the upgrade, you can select the option to upgrade only after the next normal geust OS shutdown