# Section 1 – VMware vSphere Architectures and Technologies

## Objective 1.1 – Identify the pre-requisites and components for vSphere implementation

### ESXi Hosts

* Requirements
  + HCL server hardware
  + MIN 2 CPU core
  + 64 bit x86 proceSSOr after Sept 2006
  + NX/XD bit enabled in BIOS
  + MIN 4GB RAM
  + Intel VT-x or AMD RVI enabled to support 64 bit VMs
  + 1GB Ethernet controllers
  + SCSI disk or local non network raid LUN with unpartitioned space for VMs

### vCenter Servers

* Can still be installed on windows but this is the last release
* VCSA preferred
  + Appliance runs photon
* VCSA Requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Size** | **Hosts/VMs** | **vCPU** | **RAM(GB)** | **Storage(GB)** |
| Tiny | 10/100 | 2 | 10 | 250 |
| Small | 100/1000 | 4 | 16 | 290 |
| Medium | 400/4000 | 8 | 24 | 425 |
| Large | 1000/10000 | 16 | 32 | 640 |
| X-Large | 2000/35000 | 24 | 48 | 980 |

* DB Requirements
  + Embedded postgres DB works fine for up to small
  + Medium and larger needs external SQL or Oracle
* Ports

|  |  |
| --- | --- |
| Port Number | What its uses for |
| 22 | SSH to VCSA |
| 80 | HTTP which is auto redirected to HTTPS |
| 88 | Vmware key distribution |
| 389 | Directory services |
| 443 | HTTPS connections to web client, sdk clients, etc |
| 514 and 1514 | Syslog connector connections |
| 636 | Enhanced Link Mode |
| 902 | ESX host management |
| 2012 | SSO Control |
| 2014 | VMCA API |
| 2020 | Authentication framework management |
| 7444 | STS |
| 9443 | Web client HTTPS |
| 11717 and 11712 | VMWare directory service LDAP and LDAPS |
|  |  |
|  |  |
|  |  |

* Enhanced Link Mode
  + Multiple instances of VCSA that share information
  + Share licensing and permissions
  + Used when single VCSA not big enough for all your hosts / vms
  + All vCenter servers use same PSC and SSO ( can be multiple PSC but all connected )
  + PSC replicates
    - Connection information ( distributed port groups and ports)
    - Certificates and thumbprints
    - Licensing information
    - User roles and permissions
    - Policies and tags
  + Multiple vcenter servers used for geographically or organizational constraints
  + Up to 15 vcenter servers connected to one PSC
  + Requirements
    - All vcenter servers must be registered to same SSO domain
      * Diff AD domains fine with two way trusts
    - DNS names correct
    - Same version of vcenter and PSC for all
    - Can be linux and windows in same group
    - Can be appliance and stand alone in same group
    - Each vcenter server must have its own DB
      * Either separate backend on embedded
  + Vmotion now works between vcenters
  + Uses same user name password for all linked vcenter servers
    - Duh because they all use the same SSO

#### Clients

* vSphere Web Client
  + flash version
  + https://IP/vsphere-client
* vSphere Client
  + html5
  + https://IP/ui
* ESX Host Client
  + Web client to manage ESX directly
* VAMI
  + VMWare Appliance management Interface
  + <https://IP:5480>
  + Admin UI for VCSA and other solutions
  + Used to
    - Change host name
    - Change network config
    - NTP
    - Applying patches and updates
    - Monitoring VCSA

#### Post Install

##### ESX Host

* Static IP
* ETC

##### Core Dump

* VMKernel Core Dump
* Diagnostic information during a host crash
* Local Partition
  + Partiion on local harddrive
  + Requirements
    - Can’t use ISCSI LUN if Software ISCSI or Depented ISCSI (duh ESX has crashed so no access to these)
    - Can use LUN accessed thru software FCOE.
    - Use local partition unless using diskless hosts
    - Each host must have 2.5 GB
  + Configure via VCenter
    - Private Local
      * Local disk
    - Private SAN
      * Non shared LUN
    - Shared SAN
      * Shared LUN
* File
  + Used when there is not enough space for a partition
  + Do not use software ISCSI or Software FCOE
  + Excli system coredump file add
    - Creates a VMFS coredump file

##### Logging

* Amount of logging details
  + None
  + Errors
  + Warning
    - Errors and warnings
  + Info
    - Normal logging
    - Info, error, and warning
  + Verbose
    - Info, error, warning and verbose
  + Trivia
    - Info, error, warning, verbose and trivia

##### Persistent Scratch

* VMkernel logs when ESX installed on USB or SD Card
* 1GB min
* Without persistent scratch you
  + could run into HA issues
  + or general system errors in VUM
* create
  + scratchconfig.configuredscratchlocation
* default location is
  + /tmp/scratch

#### PSC - Platform Service Controller

##### Provides the following services

* Licensing
* Certificate Management
  + Certificate service
* Authentication with SSO
  + Identity Management
  + STS
  + Authentication framework
* http reverse proxy
* Service control agent
* Common logging service
* Directory service

|  |  |
| --- | --- |
| **Service Name** | **Description** |
| Applmgmt | * VMware appliance management Service * Appliance configuration and public API endpoints |
| Vmware-cis-license | * Vmware license service * Centralized license management and reporting * Replicates across all PSC in SSO domain |
| Vmware-cm | * VMware component Manager * Registration and lookup functionalities |
| Vmware-sts-idmd  Vmware-stsd | * Vmware identity management service * Vmware Security Token Service * Part of SSO |
| Vmafdd | * Vmware authentication framework * Client-side framework for vmdir authentication and server the VMware Endpoint Certificate store |
| Vmcad | * Vmware certificate Service (daimon) * Provisions certificates for all ESX hosts and components * Uses VMware Endpoint Certificate Store (VECS) to store certs |
| Vmdird | * VMware directory service * Multitenant, multimastered LDAP directory service |
| Vmdnsd | * VMware domain name service * Not used |
| Vmonapi  Vmware-vmon | * Vmware lifecycle manager API * Vmware service lifecycle manager * Start and stop vcenter services and monitor health |
| Lwsmd | * Likewise service manager * Used to join photon OS to AD |
| Pschealth | * VMware platform services controller health monitor * Monitors health and status of all core PSC services |
| Vmware-analytics | * Vmware analytics service * Gather and upload telemetry data from vsphere components to analytics cloud and CEIP |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

##### Deployment types

* (It is possible to switch between these types after deployment)
* vCenter server with embedded PSC
  + preferred method
  + fully supports enhanced link mode
  + all services are bundled in one install
  + has its own SSO with a single site
  + can be joined to other embedded vCenter PSC with enhanced Link Mode
  + advantages
    - communication direct not over network
    - fewer windows licenses if installed on windows
    - fewer VMs or physical servers
* PSC
  + PSC only
  + Can be appliance or windows
    - Does not need to match the vCenter server
* vCenter server with external PSC
  + only vCenter server installed.
  + Requires PSC to be already deployed
  + Can be new SSO domain or join existing SSO domain
  + Can have multiple vCenter servers attached to single PSC
    - These will be linked with Enhanced Link Mode
    - Can be mixed appliance / windows installs
  + Disadvantages
    - Could have network connectivity issues
    - Windows licenses
    - More servers to admin

##### HA

* + You can join an existing PSC Deployment in same site
  + All instances of PSC must be behind a load balancer for automatic failover
    - When using a load balancer the PSC must be of the same type OS
  + Manual repoint PSC if no load balancer is uses
    - There will be downtime to repoint
  + Multi-site PSC
    - PSC installed in multiple locations
    - Allows you to log in from anywhere
    - Can repoint VCSA to another sites PSC
  + Installed in same SSO
    - Cannot be installed concurrently

##### Managing PSC

* VAMI
  + Reconfigure system settings
* Appliance shell
  + Command line interface to manage VMCA, VECS and VMDIR

##### SSO

* Authentication broker and Security token exchange infrastructure
* Services
  + STS
    - Security Token Service
    - Issues , validates and renews tokens
  + SSL for secure traffic
  + Authentication of uses through AD or OpenLDAP
  + Authentication of solutions with certs
* How it works
  + User logs into client
  + SSO checks if the user is in a configured identity source
  + If authenticated SSO returns token
  + Clent passes token to vCenter
  + vCenter checks with SSO to make sure token is still valid
  + user is allowed access
* SSO Components
  + STS
    - Security Token Service
    - Issues SAML tokens
      * Represent ID of user
  + Administration Server
    - vCenter client
    - Configures SSO and manage users and groups
  + Vmware Directory Service ( VMDIR)
    - ASSOciated with SSO domain
    - Port 389 and 11711 for older hosts
  + Identity management service
    - Handles identity sources and STS authentication requests
* SSO Groups

|  |  |
| --- | --- |
| **Group** | **Description** |
| Uses | * Users in the SSO domain |
| SolutionUsers | * Solution users * Authenticate with Cert * Do not add users explicitly |
| CAAdmins | * Admin priviledges to VMCA |
| DCAdmins | * Can admin DC for VMDIR |
| SystemConfiguration.BashShellAdministrators | * VCSA only * Can enable /disable BASH shell |
| ActAsUsers | * Get act as tokens from SSO |
| ExternalPDUsers | * vCloud air uses this |
| SystemConfiguration.Administrators | * view and manage system configuration |
| DCClients | * used internally to allow management node access to data in VMDIR |
| ComponentManager.Administrators | * invoke component manager API that register or unregister services |
| licensService.Administrators | * write access to all licensing related data * can add, remove, assign etc serial keys for all products |
| Administrators | * VMDIR admins * Can perform SSO Admin tasks |

##### Security Certificates

* Certs are used to
  + Encrypt communications between two nodes
  + Authenticate vsphere services
  + Perform internal actions such as signing tokens
* VMCA
  + VMWare Certificate Authority
  + Internal CA
  + Provides self signed certs by default
* Managing Certificates
  + VMCA Default Certificates
    - Provides all certs to vCenter and ESX
    - Simple low overhead
  + VMCA Default Certs with External SSL Certs (Hybrid Mode)
    - PSC and vCenter Server certs replaced with External SSL certs
    - Default self-signed for all else
  + VMCA as an intermediate CA
    - Root cert signed by third party
* VMware Endpoint Certificate Store (VECS)
  + Local client-side repository for certs
  + Stores all vCenter certs
  + Does not store ESX certs
  + Stores

|  |  |
| --- | --- |
| **Store** | **Description** |
| Machine SSL Store ( Machine\_ssl\_Cert ) | * Used by reverse proxy on every node * Used by VMDIR on embedded deployments on each PSC node |
| Trusted Root Store (Trusted\_ROOTS) | * Trusted root certs |
| Solution User Stores  Machine  Vpxd  Vpxd-extension  Vsphere-webclient | * One store for each solution user |
| Vsphere cert manager utility backup store (BACKUP\_STORE) | * Used by VMCA to support certificate revert * Only most recent is used as a backup |
| Other stores | * Some solutions add their own stores |

#### VAMI

* vCenter Server Appliance Management Interface
* <https://IP:5480>
* Basic Admin web interface for VCSA
  + Monitoring VCSA
  + Change host name
  + Change network config
  + NTP Config
  + Apply patches and updates
  + Backup (backup scheduler)
  + Start and stop services on VCSA

## Objective 1.2 – Identify vCenter high availability (HA) requirements

### VCSA HA

* Protects against host and hardware failures but also against VCSA failures
* Options for VCSA HA and PSC
  + PSC embedded and installed with active and passive VCSA
    - Data is replicated between passive and active PSC
  + Deploy two or more PSC with load balancer in front
* Requires at least three hosts in a compute cluster
  + One for each node
  + If DRS / SDRS enabled, anti-affinity rules are auto created
  + NFS, VMFS, VSAN
  + ESX 5.5 or higher
  + vCenter 6.5 or higher
* Nodes communicate over HA network separate from management
  + Requires separate vNIC per VM
* Not available for vCenter installed on windows
* Deployment options VCSA HA
  + Basic
    - Clones active node to passive and witness
    - Configures them for you
  + Advanced
    - You are responsible for cloning the active node
    - You must also configure them manually ( IPs and such )
* Lifecycle manager
  + Monitors vmware services and restarts if necessary
  + Can be configured to not restart if multiple attempts fail
* VCSA Instances
  + Active
    - Primary
    - All are cloned from this one
  + Passive
    - Standby node
    - Fails over to this one if /when the active fails
  + Witness
    - Witness node

## Objective 1.3 – Describe storage types for vSphere

### Block Storage

#### Local

* Local storage are disks attached directly to the host physical machine

#### Network Storage

* Types of Network attached

##### Fibre Channel (FC)

* + - Specialized high speed network that connects your hosts to high performance storage
    - Uses FC protocol to transport SCSI traffic
    - Host needs FC HBAs installed
    - Storage Area Network (SAN)
    - Zoning
      * Restricts what host has access to the WWPN of the array LUN
      * Define which HBAs can connect to witch SP (Storage ProceSSOrs)
      * Devices outside zone are not able to see inside zone
      * Effects
        + Reduces number of targets and LUNs presented to a host
        + Controls and isolates paths in a fabric
        + Can prevent non-esx systems from accessing a storage system
        + Can be used to separate different environments
    - WWPN
      * World Wide Port Name
      * Globally unique ID for a port that allows certain applications to access the port
    - Fibre channel storage types
      * Active-active
        + Access to LUN simultaneously through all the storage ports that are available without significant degredation
      * Active-passive
        + Only one storage proceSSOr is actively providing access to LUn
        + Passive is the backup SP
      * Asymmetrical Storage System
        + ALUA

Asymmetrical Logical Unit Access

Host can determine states of target ports and prioritize paths

Optimized (connected to SP where the LUN lives)

Non-optimized (connected to SP where the LUN does not live)

* + - Restrictions
      * ESX does not allow FC tape devices
      * Cannot use multipathing inside a VM
    - N-Port ID Virtualization (NPIV)
      * Allows single FC HBA to register several WWPN
      * Each WWPN can be assigned to separate VMs
      * Only VMs with RDM can have WWN assignments
    - Fibre channel over Ethernet
      * Encapsulates FC frames into Ethernet frames
      * Does not need special FC links to connect
      * Uses 10 GB lossless Ethernet
      * Adapters
        + Hardware FCoE

Specialized offload converged Network Adapters (CAN) that contain FC functionality on the NIC

Has both Ethernet and FC on same card

* + - * + Software FCoE Adapter

Uses the native FCoe protocol stack in ESX to process FCoE

Must use with a compatible NIC

NICS with partial FCoE Offload

NICs without offload

Include Data Center Bridging

* + - Boot ESX from FC SAN
      * Host’s boot image is stored on one or more LUNs in the SAN storage system
      * Host boots from LUN
      * Each host must have its own boot LUN
      * Multipathing not supported because BIOS does not support
      * Benefits
        + Cheaper servers
        + Easier server placement
        + Less wasted space
        + Easier backup
        + Improved management
        + Better reliability
    - Boot ESX with software FCoE
      * Only NICs with partial FCoE offload support booting with software FCoE
      * Configuring Software FCoE boot is done via NIC ROM
      * Multipathing not supported
      * Each host needs its own LUN

##### ISCSI

* ISCSI packages SCSI traffic into the TCP/IP Protocol
* Host is the initiator talking to target (storage array)
* LUN Masking
  + Makes a LUN available to some hosts and not to others
* Storage Device or LUN
  + Terms are interchangeable
* Block storage
* ISCSI Connections
  + Hardware ISCSI
    - Host connection
      * Hardware ISCSI
        + Third party hardware adapter
        + Offloads the ISCSI and network processing
        + Dependent

Depends on VMware networking

Uses VMK

Can be used for both network and ISCSI

Offloads ISCSI processing

* + - * + Independent

Implements own networking and ISCSI config

No vmk

Offloads ISCSI

* + - * Software ISCSI
        + Software initiator
        + Uses standard network adapter
        + Vmware code built into VMKernel
* Naming
  + IQN
    - Iqn.yyy-mm.naming-authority:uniqueName
  + Enterprise Unique Identifier
    - EUI
    - Eui.16\_hex\_digits
* ISCSI storage types
  + Active-active
    - Access to LUN simultaneously through all the storage ports that are available without significant degredation
  + Active-passive
    - Only one storage proceSSOr is actively providing access to LUn
    - Passive is the backup SP
  + Asymmetrical Storage System
    - ALUA
      * Asymmetrical Logical Unit Access
      * Host can determine states of target ports and prioritize paths
        + Optimized (connected to SP where the LUN lives)
        + Non-optimized (connected to SP where the LUN does not live)
  + Virtual Port Storage System
    - Access to all LUNs through a single port
    - Active-active that hide connections through a single prt
* Discovery
  + Returns the set of targets that you can ascess
  + Dynamic discovery
    - Obtains a list of accessbile targets from the ISCSI storage system
  + Static discovery
    - Can only access the targets that have been specifically named on the host
* Authentication
  + Supports CHAP authentication
  + Methods
    - Unidirectional
      * Target authenticates initiator
      * All types of initiators
    - Bidirectional
      * Target auths initiator and initiator auths target
      * Software and dependent adaptors
* Boot from ISCSI LUN

### File Storage

#### NFS

* NAS Storage
* Directory or volume is created on NAS server by storage admin and exported
* NFS does not need to be formatted with local file system as it is share and already formatted
* Mount volume directly to ESX hosts
* ESX supports NFS 3 and NFS 4.1
* Capabilities of diff versions

|  |  |  |
| --- | --- | --- |
| **Characteristic** | **NFS 3** | **NFS 4.1** |
| Security Mechanisms | AUTH\_SYS | AUTH\_SYS and Kerberos (krb5 and krb5i) |
| Encryption Algorims with Kerberos | N/A | AES256-CTS-HMAC-SHA1-96 and AES128-CTS-HMAC-SHA1-96 |
| Mulitpathing | Not Supported | Supported through session trunking |
| Locking mechanisms | Proprietary client side locking | Server side locking |
| Hardware acceleration | Supported | Supported |
| Thick virtual disks | Supported | Supported |
| IPv6 | Supported | Supported |
| ISO images presended as CD-ROM to virtual machines | Supported | Supported |
| VM Snapshots | Supported | Supported |
| VM with virtual disks greater than 2TB | Supported | supported |

* Vsphere solutions that support NFS

|  |  |  |
| --- | --- | --- |
| **Vsphere feature** | **NFS 3** | **NFS 4.1** |
| Vmotion and storage vMotion | X | X |
| HA | X | X ( not legacy FT ) |
| FT | X | X |
| DRS | X | X |
| Host Profiles | X | X |
| Storage DRS | X |  |
| SIOC | X |  |
| SRM | X |  |
| VVOL | X | X |
| Vsphere replication | X | X |
| vRealize Operations Manager | X | X |

* Upgrading NFS
  + Cannot upgrade while online
  + Must storage vMotion to new version of NFS datastore
  + Or unmount and remount as NFS 4.1 datastore
* Best practices
  + NFS Server Configuration
    - Hardware on HCL
    - Share as both NFS 3 or NFS4.1 on same folders
    - NFS3 or non Kerberos NFS4.1 needs root access to the volume
  + NFS Networking
    - Standard NIC is ESX
    - Vmk port group for NFS
  + NFS File Locking
    - NFS3 and NFS 4.1 use different locking mechanisms
* Firewall
  + Located /etc/vmware/firewall
  + Nfsclient rule acts different
    - Configured when you mount or unmount and NFS datastore
    - NFS3
      * Add or mount datastore
        + If nfsclient rule set is disabled, ESX enabled the rule set and disables the allow all IP addresses policy by setting the allowedall flag to false. NFS server IP is added to allowed
        + If nfsclient rule set is enabled, the state of the rule set and the allowed IP address policy are not changed, the NFS IP address is added
      * Remove or unmount datastore
        + If no other NFS3 datastores are mounted from the NFS Server, the IP address is removed from the allow list
        + If no other NFS3 datastores are mounted, the nfsclient rule is disabled
    - NFS4.1
      * Mount first NFS4.1 datastore, ESX enabled the nfs4client rule set and opens 2049 port for all IP addresses
      * Unmounting NFS4.1 data store does not affect the firewall

### Raw Device Mapping (RDM)

* Allow VMs to have direct access to LUN on the physical storage
* Block storage only
* Mapping file on VMFS that maps to physical device
* Contains metadata for managing and redirecting disk access to physical disk
* Compatibility modes
  + Virtual RDM
    - Acts like a virtual disk file
    - RDM can use snapshots
    - Only read and write are sent to mapped device
    - Disk mode
      * Dependent
        + Included in snapshots
      * Independent – Persistent
        + Data written to disk is retained during reboots
      * Independent – nonpersistent
        + Changes discarded when rebooted or powered off
  + Physical RDM
    - Direct access to the SCSI device
    - Lower level control
    - Passes all SCSI commands to the device
    - Usefull to run SAN management agents or other SCSI target based software
    - Allows virtual to physical clustering
* Use Case
  + When SAN snapshot or other layered applications run in the virtual machine, RDM enables backup offloading systems
  + If MSCS spans physical hosts like virtual to virtual clusters and physical to virtual clusters.
* Creating
  + Specify LUN to be mapped
  + Specify datastore for the RDM

### Storage API

#### Pluggable Storage Architecture (PSA)

* vSPhere API for Multipathing
* allows storage partners to create and deliver multipathing and load-balancing plugins

#### VASA

* vSphere API for Storage Array
* awareness of storage capabilities
* used to build storage policies
* Primary level failure to tolerate ( PFTT )
  + Defines the number of hosts and or device failures to tolerate
* Fault Domains
  + Collection of hosts
  + Usually a rack
  + 2n+1 fault domains with host contributing to VSAN required
    - N = 1 to 3
* Secondary Level of Failures to tolerate ( SFTT )
  + In a stretched cluster, this rule defines number of additional host failures to tolerate
  + 1 to 3
  + Default = 1
* Number of disk stripes per object
  + Minimum number of capacity devices ( HDD ) the data will be striped across
  + 1 to 12
* Force Provisioning
  + If yes, object is created on VSAN even if the previous values mean the storage policy cannot be satisfied
* Object space reservation %
  + % of VMDK that must be reservered on VSAN for VM
* Flash Read cache reservation %
  + % flash cache reserved for VM
* Affinity
  + Only if PFTT = 0
  + Limit VM to selected site in stretched cluster
* Disable Object Checksum
* Failure Tolerance method
  + Optimize for performance or capacity
  + RAID 1 - Performance
    - Uses more disk space but better performance
  + RAID 5/6 (Erasure Coding) – capacity
    - Less disk space used but worse performance
    - Requires all flash
    - RAID 5
      * 4 or more fault domains and set PFTT = 1
    - RAID 6
      * 6 or more fault domains and set PFTT = 2
* IOPS limits for object
  + Throttles IOPS when limit is reached
* SP = Storage provider
  + Part of VASA that communicates with vCenter about storage capabilities
  + Each host registers SP but only one is active
* VASA is middle man between VM and storage
  + Fulfills storage policy
* Disk group
  + Max 5 disk groups per host
  + 1 SSD and 1-7 HDD that comprise data container
  + If one drive fails the data is offline until the disk group can be rebuilt
  + Smaller disk group = faster rebuilt times

#### VAAI

* vSphere API for Array Integration
* Hardware acceleration API
  + Offloading storage operations to an array
    - Migrating VM with storage vMotion
    - Deploying VM from template
    - Cloneing VM or templates
    - VMFS clustered locking and metadata operations for VM Files
    - Provisioning Thick VMDK
    - Create FT VMs
    - Creating and cloning this disks on NFS Datastores
  + Operations
    - Full Copy
      * Clone blocks or copy offload
      * Make full copies with in the array without the host read or write
      * Reduces time and network traffic
    - Block Zeroing
      * Write same
      * Zero out large number of blocks to provide newly allocated storage
    - Hardware assisted locking
      * Atomic test
      * Discrete VM locking without use of ISCSI reservations
    - Reserver Space
      * Only on NAS Devices
      * Allow you to change from thin to thick provisioned VMDK
    - Array based snapshots
      * Only on NAS devices
      * Create snapshots
  + Reduced Host CPU overhead
  + Block storage only
    - FC
    - ISCSI
    - NAS

### VMFS

* operates on top of block storage
* creates a shared storage pool ( up to 64 hosts ) that is used for one or more VMs
* can be extended to span severall physical devices but must be of the same type 512n, 512e, 4Kn
* With VAAI, locking updates are transparent
  + Metadata in hidden section of file system
  + Metadata updates do not affect scaling or performance
* Versions

|  |  |  |
| --- | --- | --- |
| **Fetures and functionalities** | **VMFS 5** | **VMFS6** |
| Access for esx hosts 6.5 and later | Yes | Yes |
| Access for ESX 6.0 and earlier | Yes | No |
| Datastores per host | 512 | 512 |
| 512n storage devices | Yes | Yes(default) |
| 512e storage devices | Yes. Not supported on local 512e devices | Yes(default) |
| 4Kn storage devices | No | Yes |
| Automatic space reclamation | No | Yes |
| Manual space reclamation through the esxclie command | Yes | Yes |
| Space reclamation from guest OS | Limited | Yes |
| GPT Storage device partitioning | Yes | Yes |
| MBR | Yes(if upgraded from VMFS3) | no |
| Storage devicves greater than 2 TB | Yes | Yes |
| Support for VM with large capacity VMDK greater than 2TB | Yes | Yes |
| Small files of 1KB | Yes | Yes |
| Default use of ATS only locking | Yes | Yes |
| Block size | 1MB | 1MB |
| Default snapshots | * VMFSsparse for disks smaller than 2TB * SEsparse for disks larger than 2TB | SEsparse |
| Virtual disk emulation type | 512n | 512n |
| Vmotion | Yes | Yes |
| Storage vMotion across diff datastore types | Yes | Yes |
| HA and FT | Yes | Yes |
| DRS and SDRS | Yes | Yes |
| RDM | Yes | Yes |
|  |  |  |
|  |  |  |

* VMFS 3 when mounted to 6.7 host will auto update to VMFS 5
* VMFS6
  + UNMAP
    - Automatic reclaim dead blocks
    - Free up space on a thin-provisioned storage array
    - Crawler mechanism will free dead space on VMFS 6 datastores within 12 hours
    - For Newer OS, ESX supports the UNMAP command issued directly from a guest OS
      * Allows the dead space to be reclaimed automatically when you delete files within guest
* Uniform block size of 1 MB
* 64 TB max size
* VMFS Migration / Upgrade
  + Create new VMFS 6 datastore
    - Size must be equal or larger than VMFS 5
  + Migrate data to new datastore
  + Remove older VMFS 5 datastore

### vSphere Flash Read cache ( vFRC )

* Flash based storage on host, portions used for VM read I/O that usually comes from SAN or NAS
* Can be reserved for any individual virtual disk
* Created only when powered on
* Can be migrated with vMotion
* Does not support physical RDM
* DRS monitors and load balances vFRC
* Powered on VMs have a soft affinity to the host and will move for only mandatory over utilized migrations

### Hyper Converged or Software Defined Storage

#### Storage Policy Based Management

* Abstracts storage services delivered by VVOL, VSAN , i/o filters, etc
* Mechanisms
  + Advertisements of storage capabilities and data services offered by storage arrays
  + Bidirectional communication between ESX/VCenter and storage arrays
  + VM provisioning based on VM storage policies
* VM Storage Policies
  + Control which type of storage is provided for the VM and how the VM is placed within the storage
  + Information about the storage is gathered via Tags and VASA providers
  + Rules
    - Basic element of VM storage policy
    - Statement describing single requirement for virtual machine storage and data services
  + Rule Set
    - Collection of rules
    - Datastore specific rule sets
      * Must include placement rules describing VM storage requirements
      * Can include data services for the VM
    - Placement rules: Cabability Based
      * Specify a particular storage requirement for the VM allowing the correct datastore to be selected
    - Placement rules: Tag based
      * Reference tags
    - Rules for host based services
      * Activates data services provided by host ( encryption, replication, etc)
      * Does not include placement rules
  + Storage Policy Components
    - Describes a particular data service to be provided for the VM
    - Provider of service can be storage system, I/O filter, or anther entity
    - Each component can include only one set of rules
    - Cannot delete component if it is referenced in a VM storage policy
  + Storage policies are applied when provisioning the VM or configuring its VMDK
  + Default VM Storage policy is uses if you do not specify one.

#### I/O Filters

* VAIO
* Software components installed on ESX hosts to provide additional data services to VMs
* Gain direct access to VM I/O path
* Independent of storage
* Registered via VASA
* Make data service visible to VM storage policy
* Types of filters
  + Replication
    - Replicates all write I/O to an external target
  + Encryption
    - Encrypt VM
  + Caching
    - Cache for virtual disk data
  + Storage I/O Control
    - Throttles I/O loads towards a datastore and controls amount of storage I/O that is allocated to VMs during congestion

#### VSAN

* Pools locally attached storage from VSAN enabled ESX hosts in cluster
* Requirements
  + ESX 5.5 or higher
  + vCenter 5.5 or higher
  + one or more SSD per host
  + one or more HDD for hybrid mode per host
  + hardware on HCL
  + 3 hosts minimum
  + 1 GBs minimum NIC
* All Flash
  + Highest performance
  + SSD for cache and data
* Hybrid Mode
  + SSD for cache
  + HDD for data
* Uses a combo of VASA and storage policies to ensure VM is located on more than one disk and on more than one host depending on requirements
* Storage Policies
  + Key to VSAN
  + Allow admin to assign requirements (policies) to a VM or VMDK
  + Once VSAN or vVol sees policy it makes decision on where to place VM Files

#### vVOL

* Virtual volume
* Virtualize external storage
* Storage containers created by storage team and then used by vsphere to create pools for VM files
* Uses VASA
  + Vsphere API storage awareness
  + Communicates with storage containers
* Supports any storage that has VASA
  + ISCSI
  + FC
  + FCoE
  + NFS
* VM uses storage policies to find matching VASA advertised vVOL for its use
* VM Centric storage
  + Maps VMDK and derivatives directly to objects (VVOL) on storage system
  + Allows offloading to storage system
* Concepts
  + Virtual Volumes
    - Encapsulations of virtual machine files
    - Created automatically when you perform VM management operations
    - Types of VVOLs
      * Data-VVol
        + Each VMDK
        + Thick or thin provisioned
      * Config-VVol
        + Metadata files for the VM
        + .vmx, descriptor files, logs, etc
        + Thin provisioned
      * Swap-VVol
        + Created when VM is first powered on
        + VM Swap file
        + Thick provisioned
      * Snapshot-VVol
        + VM memory for snapshots
        + Thick provisioned
      * Other
        + Storage for specific featues
    - Three volumes created for each VM at minimum
      * Data-vvol, config-vvol, swap-vvol
  + Virtual volumes and storage providers
    - VASA provider
    - Communication between vCenter and array
  + Storage Containers
    - Pool of raw storage or aggregation of storage capabilities that a storage system can provide
    - Cannot span different physical arrays
  + Protocol Endpoints
    - Used by ESX to communicate with virtual volumes
    - Data path on demand from VM to their virtual volumes
    - A single endpoint can connect to thousands of VVOLs
    - Multiple esx hosts can mount same protocol endpoint
    - Advertised via VASA
  + binding and unbinding virtual volumes to protocol endpoints
    - esx or vcenter sends bind request to virtual volume to creat protocol enpoint for communication
  + virtual volume datastores
    - represents a storage container in VCenter
  + virtual volumes and VM Storage policies
    - required for a VM to use VVOL

## Objective 1.4 – Differentiate between NIOC and SIOC

### NIOC

* vDS only
* guarantee a minimum bandwidth to system traffic for vsphere features and to VM traffic
* system traffic
  + allocate amount of bandwidth for vsphere traffic like FT, HA, vMotion, etc
* for VMs
  + allocate bandwidth for VM across entire VDS based on resource pools and allocaton on the physical adapter
* Network Resource Pool
  + Aggregate bandwidth for VMs in the pool
  + Allocate bandwidth from the pool to individual VMs
  + Pool is assigned bandwidth quota from system traffic, then VMs use portion of this bandwidth
  + One id named default with no quota that all VMs are assigned to by default.
  + Port group assigned to resource pool so VMs can use its bandwidth
  + All port groups must be removed prior to deleting resource pool
* Shares, reservations and limits are defined on the VM hardware settings
* Shares
  + 1 to 100
  + Reflect priority of a system traffic type against other types on same physical adapter
* Reservation
  + Mimimum bandwidth that must be guaranteed on a single physical adapter
  + Total bandwidth reserve among all system traffic types cannot exceed 75%
  + Total bandwidth for VMs cannot exceed reserved bandwidth that is configured for the VM system traffic
* Limit
  + Max bandwidth that a system traffic type can consume on a single physical adapter
* NIOC is considered with admission control when starting a VM

### SIOC

* Storage IO Control
* SIOC is an I/O filter
  + VAIO
    - IO Filter framework API
  + Allows SIOC to use storage policies to place VMs
* Storage policies
  + Control type of storage provided to VM
  + How the VM is placed within the storage
  + Which data services offered to VM
* Uses metrics to determine storage utilization
  + Latency
    - Milliseconds
    - Above threshold SIOC kicks in
    - Can be tuned to your environment
  + Peak throughput
    - Uses IO injector to test
      * Overlaps in disk system which allows storage p to make correct placement
    - Knowing max throughput means SIOC activates before contention starts
    - Can be adjusted
* Provides prioritization for VMs during IO contention
* Storage IO Control enabled by default with SDRS
* SIOC can be used on FC, FCoE, ISCSI and NFS
* SIOC compare shares across all VMs at the vCenter Level
* Requirements
  + All datastore must be managed under single vcenter
  + NFS, VMFS over ISCSI or FC
  + RDM are not Supported
  + Datastore can have only one extent
* SIOC is enabled per datastore
* Configured on each VMDK
  + Shares
  + IOPS allowed
* Shares and limits are assigned to individual VMs
  + When congested VMs are assigned bandwidth in proportion to their shares
* Queue depth vs SIOC
  + LUN Que depth
    - Determines number of outstanding IO that can be sent to a disk
  + Dynamic Que depth throttling
    - Adaptive queue depth algorithm
    - Engages when que full or busy codes received
    - Cuts que in half
* Limitations
  + Datastore cannot have multiple extents
  + SAN with auto tiering has to be certified for SIOC
  + Datastore Managed by single vCenter server
  + Must be disabled before removing datastore
  + RDM is not supported

## Objective 1.5 – Manage vCenter inventory efficiently

### Tags

* Allow you to attach metadata to vsphere objects
* Makes inventory more sortable and searchable
* categories
  + When creating a tag, you assign it to a category
  + Allows you to group related tags together
  + Also defines which object types a categories tags can be applied to
  + Also if more than on category tag can be applied to object
* Tags and tag categories are replicated across enhanced link mode to all vCenter server instances
* Tags and categories replicated across hybrid linked mode so cloud instances and on prem have same tags
* Apply tags only to important objects
* Tags replace custom attributes
  + Can migrate custom attributes to tags
  + Names are converted to categories
  + Values become tag names

### Folders

* Used to organize the views in vCenter
* can be used to assign permissions and set alarms to objects
* only one type of object per folder
* folder can contain other folders
* types of folders
  + host and cluster
  + network
  + storage
  + vm and template

### vApps

* collection of VMs that make up one multi tier application
* assign resources and startup order
* can be in folder, stand alone, resource pool, drs cluster or another vApp
* any operation conducted on vApp, is carried out on all objects within the vApp
* vapp can be distributed across multiple hosts
* can backup vApps to an OVF package
* snapshots of a vApp do not retain vApp configs

## Objective 1.6 – Describe and differentiate among vSphere, HA, DRS, and SDRS functionality

### HA – High Availability

* FDM
  + Agent running on hosts
  + Fault Domain Manager
  + Location = opt/vmware/fdm
* Master is chosen when HA comes online
  + new master is chosen if old one fails
  + monitors slave hosts and restarts vm if slave is offline
  + Monitors power on protected VM, restart if power is off
  + Manages adding and removing hosts rom HA cluster
  + Manages list of protected VMs
  + Caches cluster configuration
  + Sends heartbeat messages to slave hosts to let them know the master is alive
  + Reports state info to vCenter
* Slave hosts are all other hosts in the HA cluster
  + Watch and monitor runtime state of VMs on host
  + Monitor health of the master
  + Implement features that don’t require central control
    - Lite VM health monitoring
* HA protects
  + Protects against a server failure
    - Restarts VM if host hardware fails
  + VM and Application Monitoring
    - Protects against application failure by continuously monitoring a VM and resetting it in event that a failure is detected
    - Monitors VM and application heartbeats and restarts if missing heartbeat
    - Requires VM Tools
    - Also monitors VM I/O activity, if no heartbeats and no I/O the VM is restarted
    - Restart a VM if guest OS or App fails
    - Uses heartbeat from VM tools
    - Takes a screenshot of VM console to help with troubleshooting
    - VM Monitoring Sensitivity

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Failure Interval | Minimum uptime | Maximum per-VM resets | Maximum resets time window |
| Low | 120 secs | 480 secs | 3 | 7 days |
| Medium | 60 secs | 240 secs | 3 | 24 hrs |
| High | 30 secs | 120 secs | 3 | 1 hr |

* + VM Component Protection
    - Monitors datastore accessibility and restarts VM if host can’t reach
    - Purpose to detect storage failures
    - Prevents host split brain where a VM is running on two hosts.
    - PDL
      * Permanent data lose
      * Host receives SCSI sense code
      * Can still communicate with the array
      * Can’t access storage
    - APD
      * All Paths down
      * No way to communicate with the array
      * Timeout = 140
      * Retry operation until timeout
      * Considered Transitional
  + Network Isolation and partitioned
    - Monitors other hosts in HA cluster and restarts VMs if host becomes isolated
    - Network Partition
      * Can’t communicate with master nor with isolation network, but it can communicate with the datastore heartbeat
    - Network Isolation
      * Can’t communicate with master nor with isolation nor with data store heartbeat
      * No communication at all
* Proactive HA
  + Requires DRS
  + Requires a plugin from hardware vendor that talks with the central system to get hardware status
  + Can monitor (depending on vendor plugin)
    - Power supply
    - Fans
    - Local storage devices
    - Memory modules
    - Network cards
  + Event state
    - Gray = unknown
    - Green = good / healthy
    - Yellow = moderately unhealthy
    - Red = critically unhealthy
  + Automation level
    - Manual
      * Simply alerts when evet states are yellow or red
    - Automated
      * Takes action without approval (Uses DRS)
  + Remediation Mode
    - Quarantine for all
    - Quarantine for yellow, maintenance for red
    - Maintenance mode for all
  + Quarantine
    - Migrate VM unless cluster resources won’t allow or affinity rules violated
* Configuring HA
* Requirements
  + All hosts access to same datastores
  + All networking on host same
  + HA uses management network for heartbeating so management network should be redundant
    - When VSAN is configured, HA heartbeats use the VSAN network
  + Should be at least two datastores for heart beating
  + Configure more than on isolation address
* Fdm.log
* Responses
  + Failure Response
    - Default is to restart VM
  + APD
    - Disabled
    - Issue Events
    - Power off and restart VMs (Conservative)
      * Only shutdown if resources exist to restart the VM
    - Power off and restart ( Aggressive )
      * Restart all VMs
  + PDL
    - Disabled
    - Issue Events
    - Power off and restart VMs
* Restart Priority
  + Started in order of priority
    - Highest
    - High
    - Medium
    - Low
    - Lowest
    - Disabled
* VM Dependency restart condition
  + Delay between VMs
  + Guest Heartbeats – wait for the heartbeat before starting the next VM
  + Application heartbeats

### DRS – Distributed Resource Scheduler

* Migrate VMs to other hosts in cluster to distribute the load
  + DRS Migration Threshold
    - Measure of how much cluster imbalance across host (CPU an RAM) loads is acceptable
    - Determines what vmotion recommendations/moves are made
      * Conservative = 1
        + Only mandatory priority 1 moves
        + Affinity / anti-affinity rules
      * Aggressive = 5
        + All recomendations
* Admission Control
  + Automatically places VMs when new vms created or powered on
  + Checks for enough resources to run VM
* DRS considers CPU, RAM and Network bandwidth
* Does not load balance FT protected VMs unless using EVC
* ProceSSOr Compatibility
  + Host CPUs must be similar and from same vendor / family
  + Enhanced vMotion Capatibility (EVC
    - Limits features presented to VM so it can migrate between hosts
    - Configured via cluster
  + CPU compatibility Mask
    - Can hide certain CPU features of the destination from the VM
* Requirements
  + Minimum 3 hosts and activated DRS in cluster
  + vCenter server
  + vMotion network enabled on all hosts in cluster
  + enterprise Plus
  + shared storage connected to all hosts in cluster
  + does not support raw disks
  + does not support Microsoft cluster service VMs
* Modes
  + No Automation (Manual)
    - Shows only recommendations
    - Can manually run them
  + Partially automated
    - Placement recommendations run but migration recommendations require manually run
  + Automation
    - Auto moves VMDKs on storage
    - Placement automatic
* Addind host to Cluster
  + - Can choose to include resource pools or VMs
    - Resource pool can be added to cluster root or grafted lower
* Removing VM from Cluster
  + Removing host removes powered off VMs from cluster as well
    - can remove host only if it is in maint mode or disconnected
  + migrate VM from cluster
* Virtual Flash and DRS
  + Only one flash device can be used for vFRC per host
  + Virtual flash reservations if the host does not have the available flash cache then the VM does not start or migrate.
  + VMs with virtual flash have soft affinity to host
    - DRS will not migrate unless mandatory reason
* Disabling DRS
  + Clusters resource pool hierarchy and affinity rules are not kept.
* Predictive DRS
  + Requires vROPS
  + Based on trends can migrate to load balance
* ROBO enterprise License and DRS
  + Remote Office Branch Office
  + Enabled by default and you cannot make changes to DRS config
  + Affinity rules created prior to maint mode and evacuation.
    - This is so vCenter knows where to place VMs when the host is back online

### FT – Fault Tolerance

* Protects VM with no downtime or loss of data
* Provides a primary and secondary VM that are in lockstep. Secondary takes over when primary has issue on host
* Auto anti-affinity rules to keep the two VMs on separate hosts
* If you use affinity rules on the primary, the secondary is affected by these rules also
* Can handle SMP multi proceSSOr up to 4 vCPUs
* Use Cases
  + Applications the must always be available
  + Applications that have long lasting client connections that users want to maintain during hardware failure
  + Custom applications that have no other way of clustering
  + Custom clustering of app is too complicated to configure or maintain
  + On demand fault tolerance
    - Long running job or app can be protected prior to starting and unprotected when complete
* Requirements
  + CPUs must be compatible with vMotion
  + 10 GB loggin network for FT and verify low latency
    - Dedicated network recommended
  + HA must be enabled on cluster before you can power on FT VMs or add host to cluster hat already has FT VMs
* Limits
  + Das.maxftvmsperhost
    - Max number fo FT VMs allowed on a host in the cluster
    - Primary and secondary count towards this
    - Default = 4
  + Das.maxftvcpupsperhost
    - Max number of vCPUs aggregated across all fault tolerant VMs on a host
    - Default is 8
  + 8 vCPU in single VM and spread across all hosts in cluster
  + 128 GB RAM
* Licensing
  + Standard and enterprise = 2 vCPUs
  + Enterprise Plus = 8 vCPUs
* vSphere features not supported by FT
  + Snapshots
    - When enabling FT the VM cannot have snapshots
    - Nor can you take snapshots while protected
  + Storage vMotion
  + Linked clones
  + Virtual volume (vVol) datastores
  + Storage-based policy management
  + I/O Filters
  + Disk encryption
  + TPM
  + VBS enabled VMs
  + UPIT
* Incompatible devices
  + Physical Raw Disk Mapping
    - Legacy FT supports virtual RDM
  + CD Rom or floppy virtual devices backed by physical device
  + USB and sound devices
  + N\_Port ID Virtualization (NPIV)
  + NIC Passthrough
  + Hot pluggin devices
  + Serial or parallel ports
  + Video devices that have 3D enabled
  + Virtual machine communication interface (VMCI)
  + VMDK over 2 TB
* Must be enabled on cluster and VM
* Best Practices
  + DPM can cause host proceSSOrs to vary CPU frequencies. If the secondary VM restarts more frequently disable all power management modes on the host, or ensure the hosts are running the same power management modes
  + Networking
    - Distribute NIC teaming over separate physical switches
    - Use deterministic teaming polices to ensure particular traffic types have affinity to a particular NIC or set of NICs
    - FT Logging is unencrypted and should use a separate VLAN
    - 10 GB NIC recommended
  + FT Clusters should be as similar as possible
* Troubleshooting
  + If the FT Logging network is suspended or deleted, then the existing protected VMs will run and fail over but a new secondary will not be created.
  + Unknown error message
    - If FT enabled and VM will not power on check the memory resources on the host. FT requires all VM mem be available plus overhead.
  + Secondary VM cannot power on as there are no compatible hosts
    - Hardware virtualization enabled for primary VM Host but not for any other hosts in cluster
    - No resources available.

### Storage DRS – Storage Distributed Resource Scheduler

* Datastore cluster
  + Collection of datastores with shared resources and shared management interface
  + Similar or interchangeable datastores
  + Mix of datastores with different sizes and I/O capacities
  + Can be from diff arrays and vendors
* Resource balance on datastore cluster by
  + Space Utilization Load balancing
    - Set a threshold for space use
    - When space used over threshold, SDRS will storage vMotion to balance
  + I/O Latency load balancing
    - Set I/O threshold. Same as space
    - IO imbalance threshold
      * Amount of imbalance that SDRS should tolerate
      * Aggressive = corrects small imbalances if possible
      * Conservative = very high only
  + Anti-Affinity rules
    - By default all VMDKs are kept together on same datastore
    - VM Anti-Affinity rules
      * Specify which VM should never be kept on same datastore
      * Inter VM anti affinity rules
        + Specify which VM should never be kept on the same data store
    - VMDK anti-Affinity rules
      * Specify which VMDK aSSOciated with a VM must be on different datastores
      * Intra VM anti affinity rules
        + Specify which VMDK aSSOciated with a VM must be kept on a different datastore
* Manages the initial placement of virtual disks based on space and IO workload
  + Happens when
    - VM being create or cloned
    - VMDK migrated from another datastore
    - Adding VMDK to VM
* Can disable IO related functions separately from space balancing functions
* Modes
  + No Automation (Manual)
    - Shows only recommendations
    - Can manually run them
  + Partially automated
    - Placement recommendations run but migration recommendations require manually run
  + Automation
    - Auto moves VMDKs on storage
    - Placement automatic
* Modes can be overridden per VM
  + Default =
    - placement and migration recommendations are displayed but must be manually applied
  + Fully Automated =
    - placement and migrations run automatically
  + Disabled
    - Does not migrate or provide placement recommendations
    - Cannot put datastore in maintenance unless this VM is manually migrated off.
* Affinity rules can be overridden
  + Affinity rules indicate that VMDK in a datastore cluster associated with a VM are located on the same datastore
  + Enabled by default
  + Can be overridden at cluster or per VM
  + If VM VMDK violates affinity rule then SDRS makes recommendations to correct or reports the violation
* Requirements
  + The use similar or interchangeable datastores for a datastore cluster is allowed.
  + There can be a mix of datastores with different sizes and I/O capacities and can be from different arrays and vendors
  + Cannot mix NFS and VMFS in same cluster
  + Cannot mix replicated with no-replicated datastores in SDRS cluster
  + Cannot share datastoers across multiple datacenters
  + Best practice not to use datastores with hardware acceleration
* Managing DRS
  + Maintenance Mode
    - VMs are storage VM to another datastore
    - You can choose to ignore anti affinity rules when placing in maintenance mode
  + Recommendations
    - can override suggested DRS recommendations when manually applying
  + can use schedulted task to change automation level aggressiveness so migratiions happen at off peak hours

## Objective 1.7 – Describe and identify resource pools and use cases

### Benefits

* Flexible hierarchical organization
* Isolation between pools, sharing within pool
* Access control and delegation
* Separation of resources from hardware
  + Think about aggregate resources instead of per host
* Manage sets of multi tier VMs as a service
* Partitions available CPU and memory resources
  + Shares, reservations and limits can be set on both CPU and Memory
* Whenever a resource pool is not using all of its resources they become available to the parent (and thus sibling) pools / VMs. Unless reservations are involved.
* Based on hierarchies
* Each host and DRS cluster have a root resource pool (invisible)
* Resource pools can contain other resource pools and/or VMs
* Expandable Resource pool
  + Pool can borrow resources from its parent pool
  + Recursive as long as each parent is expandable
* Requires DRS to be enabled if used in a cluster
* Also if in a cluster you cannot create a child resource pool off the host
* Admission Control
  + Vcenter checks resource pool when power on VM to make sure resources are available
  + Reservation type
    - Fixed
      * Resource pool must have the resources for the VM or it will not be allowed to poer on, join pool, etc
    - Expandable
      * Can borrow resources from its ancestors
  + Does not violate preconfigured reservations or limits
* Use case
  + When you need to limit or guarantee resources to VMs
    - Don’t have to limit or guarantee to individual VMs but only at the pool level
  + Allow permissions to be set a pool instead of individual VMs
  + Isolation between pools (expandable disabled)
* CPU and Memory Resources
  + Shares
    - Indicated proportion of parents pool resources the resource pool will get
    - Relitive to any sibling VM or resource pool

|  |  |  |
| --- | --- | --- |
| Setting | CPU Share Values | Memory Share Values |
| High | 2000 per vCPU | 20 per MB |
| Normal | 1000 per vCPU | 10 per MB |
| Low | 500 per vCPU | 5 per MB |

* + - Share type
      * Custom
  + Reservation
    - Guaranteed resource for this resource pool
    - Defaults to 0
  + Limit
    - Upper limit for the resource pools resources
* Vapps and resource pools
  + Reservations on VApps only count if VMs are powered on
  + Can assign shares / reservations / limits like a regular resource pool
  + Can be expandable
* Adding VM to pool
  + VM reservation and limits do not change
  + If VM Shares are High, Medium or low, the % shares adjusts to reflect the total number of shares in use in the new resource pool
  + If Custom shares the share value is maintained
* Removing from the pool
  + Total number of shares decrease so % for remaining VMs is increased

## Objective 1.8 – Differentiate between VDS and VSS

### vDS – virtual Distributed Switch

|  |  |
| --- | --- |
| vDS version | New Features Added |
| 5.00 | * User defined network resource pool in NIOC * Netflow * Port Mirroring |
| 5.1.0 | * Network Rollback and recovery * Health check * Enhanced Port Mirroring * LACP |
| 5.5.0 | * Traffic filtering and marking * Enhanced support for LACP |
| 6.0.0 | * NIOC 3 * Multicast snooping and filtering |
| 6.5.0 | * ERSPAN port mirroring |
| 6.6.0 | * MAC Learning |

* Single switch across all aSSOciated hosts
  + Centralized provisioning, admin, monitoring
* vDS requies vcenter
  + switch lives in vcenter with configuration
  + proxy on ESX host
    - traffic will still work with vcenter down
* can’t remove vDS if VM still connected to distributed port group
  + Resource x in use error
* Healthchecks
  + Identifies mismatch VLAN and MTU configurations
  + Identifies mismatch NIC teaming policies
* Network Rollback
  + Protect host from changes that would disconnect ESX from vCenter
    - If change results in loss connectivity to vCenter, the change is rolled back
  + Manual rollback via DCUI
* Can backup vDS and distributed port groups
* vDS requires Enterprise Plus licensing
* distributed port group
  + port group attached to vDS
  + specifies port configuration options for each member port
* vDS supports
  + vswitch features plus all else

#### Port Mirroring

* mirror distributed ports traffic to other distributed ports
* Port Mirroring Types

|  |  |
| --- | --- |
| **Option** | **Description** |
| Distributed Port Mirroring (SPAN) | Mirror packets from distributed port to other distributed port on same host.  Will not function if the source and dest are on different hosts |
| Remote Mirroring Source (RSPAN) | Mirror packets from remote source. Still same L2 address. Mirror packets from a number of distributed ports to specific uplin port |
| Remote Mirroring Destination (RSPAN) | Mirror packets to remote destination. Still Same L2 address. Mirror packets from a number of VLANs to distributed ports |
| Encapsulated Remote Mirroring (L3) Source (ERSPAN) | Mirror packets across different L3 networks. |
|  |  |

### vSS – vSwitch – Virtual Switch

* similar to physical switch
* physical uplinks connect vSwitch to physical switch
* VMs connect to Ports in port groups
* Lives on ESX Host
  + Each host has a separate switch meaning that each host in a cluster must have identically named port groups for vMotion to work.
* Standard port group
  + Define how a connection is made through the switch to the network
  + One or more per vswitch
  + Specifies port configuration options such as bandwidth limitations and VLAN tagging policies for each member port
* vSwitch supports
  + VLAN
    - Enabled single physical LAN to be segmented so that groups of ports are isolated from one another
    - 802.1Q
  + IPv6
  + NIC Teaming
    - Multiple uplinks band tighter to form single team
    - Either shares load of traffic or provides failover
  + Outbound traffic shaping
* Ports
  + Dynamically scaled up and down
  + Max determined by number of VMs the host can handle

## Objective 1.9 – Describe the purpose of cluster and the features it provides

### Cluster

* Group of host with aggregate resources
* Created at datacenter

### HA

* Monitors all servers in cluster and detects server failures
  + Failure
    - Host stops functioning
  + Isolation
    - Host becomes network isolated
  + Partition
    - Host loses network connectivity with the master host
* Heartbeats between nodes and storage to check if all is up
* Restarts VMs on another host in cluster if the host the VM was on fails
* Checks resources to ensure there is enough capacity available should one host fail
  + Admission control

### DRS

* Balances the cluster so that CPU / Memory / Network resources are as equal as possible for all hosts

### Predictive DRS

* Rebalances Hosts in a cluster based on predictive patterns in the cluster workload
* Requires vRealize Operations Manager ( vROPS)

### vSAN cluster

* Allows the cluster to pool local hard drives, share and replicate data

### DPM

* Power management
* Turns off hosts if capacity demand is low enough to allow it.
* Requires Wake On LAN
* Integrates with DRS to migrate and shutdown hosts if capacity allows it

## Objective 1.10 – Describe virtual machine (VM) file structure

### Files

|  |  |  |
| --- | --- | --- |
| **File** | **Usage** | **Description** |
| .vmx | Vmname.vmx | Configuration file |
| .vmxf | Vmname.vmxf | Addition configuration files |
| .vmdk | Vmname.vmdk | Virtual disk characteristics |
| -flat.vmdk | Vmname-flat.vmdk | Virtual disk data |
| .nvram | Vmname.nvram or nvram | BIOS or EFI configuration |
| .vmsd | Vmname.vmsd | VM Snapshots |
| .vmsn | Vmname.vmsn | VM Snapshot data file |
| .vswp | Vmname.vswp | * Swap file * Size of swap file = VM memory – reserved memory |
| .vmss | Vmname.vmss | Suspend file |
| .log | Vmware.log | Current VM Log file |
| -#.log | Vmware-#.log | Old VM Log file |
| .hlog |  | Vcenter keep tack of VM files that must be removed after operation completes |
| .vmtx |  | Created when you convert a VM to a template and replaces vmx file |
| .ctk |  | * Used by Changed Block Tracking * Lists the block changes made since the last backup * Fixed size (only grows if the VMDK is expanded) * Used by backup software for differential backups |

### Snapshots

* When snapshot is created, all attached disks are snapshotted simultaneously
  + One delta disk per VMDK per snapshot

### Virtual Machine Options

## Objective 1.11 – Describe vMotion and Storage vMotion technology

### vMotion

* Live migration without interruption
* Can vMotion over routed networks
  + <= 100 ms RTT
* vMotion process 3 phases
  + phase 1
    - vmotion requested and vCenter checks If existing VM is in a stable state with current host
  + Phase 2
    - VM State info ( memory, registers and network connections) copied to the target host
  + Phase 3
    - control of VM moved to new host
* Memory Bitmap
  + As memory copied , vcenter keeps track of changed memory, which then can be copied to destination
* Requirements
  + ProceSSOrs on each host must be similar
    - From same vendor
    - From same CPU Family
    - CPUs support same features
    - Intel VT or AMD-V for x64 VM
  + Each host must have at least one vmk configured for vMotion
  + VM Requirments
    - No connection to physical host device
    - Not connected to internal only vSwitch
    - CPU affinity not set to specific CPU
    - Both host must be able to access the datastore the VM files are stored on
    - 3D graphics enabled requires destination host to have the same card installed or be set to automatic
    - Host usb attached to VM must be enabled for vMotion
* Limits
  + Network Limit
    - Each migration requires 250 MB per second
    - 1GB NIC = 4 simultaneous migrations
    - 10GB = 8
    - Can configure multiple NICs to improve vMotion bandwidth
    - By default you cannot migrate a VM attached to vSwitch with no physical uplink
  + Datastore limit
    - 128 per datastore at same time
  + Host Limit
    - Max of 8 per simultaneous vMotion
* Encrypted vMotion
  + Used by default when migrating encrypted VM
  + Options when VM not encrypted
    - Disabled
      * Do not use encrypted vMotion
    - Opportunistic
      * Use if available on both target and source
      * Default
    - Required
  + Encrypted vMotion of unencrypted VM works cross-vCenter but not for encrypted VM
  + Encrypted VMs are always vMotioned with encryption
  + Encrypted VMs are not required to use encrypted vMotion
* vMotion Boundry
  + when CPU in same cluster are different
* Per-VM CPU Masking
  + Generally not supported except
  + Show or mask NX/XD bit
    - Allows for greatest vMotion capability
* Enhanced vMotion Compatibility
  + Sets CPU-ID to a baseline so different CPUs appear the same
  + Can set per cluster
  + Per-VM EVC
    - Determines which cpu features VM needs from host to be migrated and powered on
    - Can only be changed when powered off
    - HTML5 client only
    - When VM moved outside of cluster a power reset will reset VM EVC to cluster’s setting
    - Overrides cluster but can’t be set higher than cluster
* Cross-vCenter vMotion
  + Everything transfers with VM except performance data (which is stored in vCenter)
  + Additional requirements
    - Destination and source vCenter must be >= 6.0
    - Destination and source vCenter must be in same SSO
    - ESX Hosts >= 6.0
    - RTT <= 150 ms
* vMotion Types
  + vMotion
    - compute resource only
  + long-distance vMotion
    - sites separated by high network latency
    - license only requirement
    - Round trip > 150 ms
  + Migrate to another datacenter
    - Hot or cold migration
    - Can select port group for networking
  + Migrate to another vCenter Server
    - Via Enhanced Linked Mode
    - Over long distance
  + Storage vMotion
    - Move VM backend storage
  + Nothing shared vMotion
    - Move computer and backend storage at same time
  + Transferred state information
    - Includes memory
  + Migrate to another switch
* Cold Migration
  + Vm is powered off or suspended
  + Manual or scheduled via scheduled task
  + Cannot cold migrate across different subnets
  + Powered Off - Does not check CPU compatibility ( except for bitness of CPU )
  + Suspended – CPU compatibility is checked
  + Cold migration traffic
    - Default goes over management network
    - Traffic is provisioning traffic

### Storage vMotion

* For encrypted disks, data is transmitted encrypted
* Storage vMotion ecryption is not supported for unencrypted disks
* Can vmotioning VMDKs to separate datastores or all to one
* Can change disk provisioning type
* Changes vm files to match VM name in vCenter
* Use case
  + Storage maintenance
  + Redistribute storage load
* Requirements and limitations
  + VM disks must be persistent mode or RDM
    - Virtual RDM can be converted or mappings copies
    - Physical mappings migrated only
  + Host must have access to source and destination datastore

# Section 2 – VMware Products and Solutions

## Objective 2.1 – Describe vSphere integration with other VMware products

### VRealize

#### vRealize Orchestrator

* Process automation platform
* Instegrates with cloud suite as well

#### vRealize Automation

* Allows authorized admins, developers, or users request new IT services

#### vRealize Log Insight

* Helps with searching thru logs

### VMWare NSX

* Logical switching, in-kernel routing, in-kernel distributed firewalling, load balancing, dynamic routing
* Virtualized networking
* SDDC

### Site Recovery Manager

* Test and failover replicated VMs

### vSphere Replication

* Replicates VM from one site to another, or within site
* Fail over and fail back is manual
* Compression to reduce bandwidth
  + FastLZ algorithm
* Replicates only change blocks

### Horizon Suite

* VDI

### Integrated Containers

## Objective 2.2 – Describe HA solutions for vSphere

### HA – High Availability

* FDM
  + Agent running on hosts
  + Fault Domain Manager
  + Location = opt/vmware/fdm
* Master is chosen when HA comes online
  + new master is chosen if old one fails
  + monitors slave hosts and restarts vm if slave is offline
  + Monitors power on protected VM, restart if power is off
  + Manages adding and removing hosts rom HA cluster
  + Manages list of protected VMs
  + Caches cluster configuration
  + Sends heartbeat messages to slave hosts to let them know the master is alive
  + Reports state info to vCenter
* Slave hosts are all other hosts in the HA cluster
  + Watch and monitor runtime state of VMs on host
  + Monitor health of the master
  + Implement features that don’t require central control
    - Lite VM health monitoring
* HA protects
  + Protects against a server failure
    - Restarts VM if host hardware fails
  + VM and Application Monitoring
    - Protects against application failure by continuously monitoring a VM and resetting it in event that a failure is detected
    - Monitors VM and application heartbeats and restarts if missing heartbeat
    - Requires VM Tools
    - Also monitors VM I/O activity, if no heartbeats and no I/O the VM is restarted
    - Restart a VM if guest OS or App fails
    - Uses heartbeat from VM tools
    - Takes a screenshot of VM console to help with troubleshooting
    - VM Monitoring Sensitivity

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Failure Interval | Minimum uptime | Maximum per-VM resets | Maximum resets time window |
| Low | 120 secs | 480 secs | 3 | 7 days |
| Medium | 60 secs | 240 secs | 3 | 24 hrs |
| High | 30 secs | 120 secs | 3 | 1 hr |

* + VM Component Protection
    - Monitors datastore accessibility and restarts VM if host can’t reach
    - Purpose to detect storage failures
    - Prevents host split brain where a VM is running on two hosts.
    - PDL
      * Permanent data lose
      * Host receives SCSI sense code
      * Can still communicate with the array
      * Can’t access storage
    - APD
      * All Paths down
      * No way to communicate with the array
      * Timeout = 140
      * Retry operation until timeout
      * Considered Transitional
  + Network Isolation and partitioned
    - Monitors other hosts in HA cluster and restarts VMs if host becomes isolated
    - Network Partition
      * Can’t communicate with master nor with isolation network, but it can communicate with the datastore heartbeat
    - Network Isolation
      * Can’t communicate with master nor with isolation nor with data store heartbeat
      * No communication at all
* Proactive HA
  + Requires DRS
  + Requires a plugin from hardware vendor that talks with the central system to get hardware status
  + Can monitor (depending on vendor plugin)
    - Power supply
    - Fans
    - Local storage devices
    - Memory modules
    - Network cards
  + Event state
    - Gray = unknown
    - Green = good / healthy
    - Yellow = moderately unhealthy
    - Red = critically unhealthy
  + Automation level
    - Manual
      * Simply alerts when evet states are yellow or red
    - Automated
      * Takes action without approval (Uses DRS)
  + Remediation Mode
    - Quarantine for all
    - Quarantine for yellow, maintenance for red
    - Maintenance mode for all
  + Quarantine
    - Migrate VM unless cluster resources won’t allow or affinity rules violated
* Configuring HA
* Requirements
  + All hosts access to same datastores
  + All networking on host same
  + HA uses management network for heartbeating so management network should be redundant
    - When VSAN is configured, HA heartbeats use the VSAN network
  + Should be at least two datastores for heart beating
  + Configure more than on isolation address
* Fdm.log
* Responses
  + Failure Response
    - Default is to restart VM
  + APD
    - Disabled
    - Issue Events
    - Power off and restart VMs (Conservative)
      * Only shutdown if resources exist to restart the VM
    - Power off and restart ( Aggressive )
      * Restart all VMs
  + PDL
    - Disabled
    - Issue Events
    - Power off and restart VMs
* Restart Priority
  + Started in order of priority
    - Highest
    - High
    - Medium
    - Low
    - Lowest
    - Disabled
* VM Dependency restart condition
  + Delay between VMs
  + Guest Heartbeats – wait for the heartbeat before starting the next VM
  + Application heartbeats

## Objective 2.3 – Describe the options for securing a vSphere environment

### ESX

* Out of the box
  + Shell and SSh disabled by default
  + Only limited number of firewall ports are open by default
  + Runs only essential services
  + Weak ciphers are disabled
  + Internal tomcat web site for admin only runs function required for admin and monitoring
* Harden esx host
  + Keep shell and ssh disabled unless needed for troubleshooting
  + Firewall
    - Only ports needed are open. Can open others as needed
  + Host Certificate Modes
    - VMCA
      * Host certs signed by VMCA by default
      * Issues certs to hosts
      * VMCA either top level or intermediate
      * Can be self signed if root cert not installed
    - Custom Certificate authority
      * Cert signed by third party CA
      * You must renew certs when they expire
    - Thumprint mode
      * Backwards compatible with 5.5
      * Do not use unless problems
  + Consider using UEFI Secure Boot
  + Join to AD to prevent local accounts maintenance
    - When you join domain ESX Admins group get full admin access to hosts
  + Lockdown Mode
    - Strict Mode
      * DCUI disabled and no one can use it
    - Normal
      * Some users can use DCUI
    - Exception Users
      * Members who are admins can use DCUI, shell and SSH in normal lockdown
      * Main use for service accounts to log onto ESX
      * Members who are admins can use SSH and Shell when in Strict mode
      * Configured on each host separately
    - DCUI.Access
      * Can access DCUI in normal lockdown
      * Advanced setting
      * Root member by default
  + Set timeout on shell and SSH – ESXi.set-shell-timeout
  + Availability timeout
    - Amount of time that can elapse before you must log in after the esxi shell is enabled
* Host Profiles Apply Permissions
  + Standardize config
  + Possible to apply same security settings to all hosts with host profiles
* Control access to SSH, Shell and MOB
  + Disable mob via advanced setting
    - Config.HostAgent.Plugins.solo.enablemob
* Restrict permissions to admin
  + Least Privilege
* VIB Acceptance Levels
  + VMWare Certified
    - Only VIBs that are tested by VMWare in-house
    - Supported by VMWare
  + VMWare Accepted
    - Verification testing
    - Partner runs test and VMWare verifies
    - Support calls sent to VIB partner
  + Partner supported
    - Published by partner VMware trusts
    - VMware does not verify
    - Support calls sent to partner
  + Community Supported
    - Published by companies outside of VMware partner programs

### VCenter

* Follow Least privilege
* Restrict datastore browser access
  + Datastore.browser
  + Prevents users from viewing, uploading downloading files on datastore
* Vpxuser (account used to access the host) changed by default every 30 days
  + Can be changed – VimPasswordExpirationInDays advanced setting

### VM

* Secure Boot
* Treat like physical machine
* Use Templates to deploy
* Minimize use of the VM Console
* Prevent VM from taking over resources
* Disable Unnecessary functions inside VM
* Encrypt VM
  + Requirements
    - KMS
  + Keys
    - Data Encryption Keys - DEK
      * Used by ESX to encrypt VM and VMDK
    - Key Encryption Keys – KEK
      * Used by VCenter
      * Obtained from KMS
      * Used by ESX to encrypt the internal keys and stores the keys on disk
  + Most VM files are encrypted except
    - Log Files
    - VMX config files
    - Virtual disk descriptor file
* Encrypt VMDK on storage
  + Not all VMDK on an encrypted VM need to be encrypted
  + Cannot add an encrypted disk to a non encrypted VM
  + Controlled thru storage policies
* Enable host encryption mode
  + Determins if a host is ready to accept cryptographic material for the purpose of encrypting VMs
  + Core dumps are encrypted in this mode
* Use vTPM
* Disable the ability to shrink a VMDK from within the guest OS

### Virtual Networking

* VLAN
* Secure physical switch
* Secure standard switch ports with security policies

# Section 3 – Planning and Designing -- There are no testable objectives for this section.

# Section 4 – Installing, Configuring, and Setting Up a VMware vSphere Solution

## Objective 4.1 – Understand basic log output from vSphere products

### Syslog

* You can forward vCenter appliance logs to syslog server
* Configure
  + VAMI
  + Syslog -> Configure -> Edit
* Protocols
  + TLS
  + TCP
  + RELP
  + UDP
* Can send logs to 3 different syslog servers

<https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vcenter.install.doc/GUID-8DC3866D-5087-40A2-8067-1361A2AF95BD.html>

## Objective 4.2 – Create and configure vSphere objects

## Objective. 4.3 – Set up a content library

### Overview

* Container objects for
  + VM Templates,
  + vApp templates
  + ISO, Scripts
  + and other types of files ( Not VMDK )
* Can be shared across multiple vCenter Server instances
* C
* Optimized libraries
  + Two synchronized libraries whose datastores are managed by ESX hosts that are directly connected to each other
  + Transfer is handled by direct ESX host to host transfer
  + If datastores have VAAI, content is transferred from Datastore to datastore by array directly
* Types of libraries
  + Local Library
    - Store items for a single vCenter instance
  + Published
    - Local library that is published for sharing
    - Can be configured with password
  + Subscribed
    - Subscribe to remote published library
    - Content is either synced or only metadata is synced and actual files copied when first used

## Objective 4.4 – Set up ESXi hosts

### Deploy

#### AutoConfiguration

* Runs immediately after installing ESX
* Configures system network and storage devices with defaults
  + DHCP and formats blank internal disks with VMFS

#### Host Profiles

* Allows ESX Configurations to be consistent
* Can be used to config PSP
  + SATP = Storage array tape plugin
  + PSP = Path selection policy
* Create host profile only from reference host
* Passwords do not get exported with the host profile
* Can be applied to a host, cluster or all hosts and clusters
* Can check compliance with profile
  + Compliance check can be scheduled
* Can disable part of host profile so it is not checked
* Export Host profile
  + Exprots as .vpf
* Update host profile
  + If reference host changes you can copy settings from host to update profile
* Using with autodeploy
  + Allows host to be configured from scratch
* Host Customizations
  + Used to set specific values for that host
  + Can prompt for user input
  + Export as .csv

#### DCUI

* Direct Console User Interface
* Can be used to
  + Change the password of the root user
  + Configure management network
    - Management VMK
    - IP Address
  + DNS
  + Host name
  + Enable shell / SSh

#### Joining to AD

* Authentication Proxy
  + Point host to AD Domain and IP of proxy
  + Automatically adds host being provisioned to AD without needing credentials to AD
    - They are already stored in the proxy
  + Auto deploy
    - Set up ref host that points to Authentication proxy and create host profile
  + Other ESX Hosts
    - Manually add host IP to authentication proxy ACL
    - Assign host profile that has auth proxy configured
  + Configure
    - Service running on VCenter server
    - Does not support IPv6
    - Can add domain to proxy via web client or using camconfig via ssh

#### Power Policies

* Not to be confused with DPM
* Configures power settings for each host

|  |  |
| --- | --- |
| **Power Management Policy** | **Description** |
| High Performance | * Do not use any power management features * High performance low efficiency |
| Balanced (Default) | * Reduce energy consumption with minimal performance compromise |
| Low Power | * Reduce energy consumption at the risk of lower performance * Less performance high efficiency |
| Custom | * User defined |
|  |  |

* ESX can control CPU frequencies so that VM performance is not affected
  + Lower freq means less power used
* ESX can apply deep halt states
  + When CPU is Idle
  + C-States
  + Deeper C state = less power CPU uses but takes longer to start using CPU again

### Security

* Not integrated with SSO
* Local users exist on single ESX host only
* Can be joined to AD
* DCUI
  + Access limited to Local admins only
  + DCUI user acts as agent for direct console – not interactive
    - Primary purpose is to config lockdown
  + Smart card authentication
    - Join host to AD
    - Use web client to enable smartcard and copy certs to host
  + If host looses management network connectivity, you can
    - Restore Network Settings
      * Set ESX host back to factory settings
    - Restore Standard switch
      * Creates new VMK on new vSwitch
      * Uplick is migrated to vswitch
      * Connectivity restored
    - Restor vDS
      * Creates a new Epheral port on vDS
  + Restart Management agent

## Objective 4.5 – Configure virtual networking

### vDS

#### vDS Settings

* Number of uplinks
  + Physical uplinks that each host will provide
* Network I/O Control
  + Enable / disable
* MTU
* Multicast Filtering Mode
  + Basic
    - Distributed switch forwards traffic that is related to a multicast group based on a MAC address generated from the last 23 bits of the IPv4 address of the group
  + IGMP/MLD Snooping
    - Forwards traffic based on IP addresses using messages defined by internet group management protocol and Multicast listener discovery protocol
* Discovery protocol
  + CDP
    - Cisco proprietary
  + LLDP
    - Anyone

#### Managing VDS

* Can use templates when adding multiple hosts to a vDS to ensure they are all configures alike
* Remove host from VDS
  + Migrate physical NICs to different switch
  + Vmkernel adapters migrated to diff switch
  + No vms using VDS (doesn’t matter if off on on)

#### Distributed Port Group Settings

* Port Binding
  + When a port is assigned to a VM
  + Static
    - When VM connects to group
  + Dynamic
    - When VM is powered on
  + Ephemeral
    - No port binding
    - Doesn’t take up a port
    - Use if vCenter is offline
* Port Allocation
  + Elastic
    - Default number of ports = 8
    - When all ports are assigned, 8 more ports are created
    - Default
  + Fixed
    - Default = 8
    - No additional ports are created
  + Number of ports
  + Network resource pool
    - Assign distributed port group to a user defined network resource pool
  + VLAN
    - None = do not use VLAN
    - VLAN = vland ID between 1 to 4094
    - VLAN Trunking = multiple VLAN range
    - Private VLAN
* Security
  + Promiscous mode
    - Accept or reject traffic from other ports not directly addressed to this one
    - Reject = Default
  + Mac Address Changes
    - Initial MAC address
      * Vmware mac assigned in VMX
      * Cannot be changed to non vmware mac
    - Effective MAC
      * Assigned by OS
      * Usually same as initial MAC but can be anything
    - Mac address changes check incoming traffic to see if initial mac and effective mac matches
    - Default = Reject
  + Forged Transmits
    - Outbound
    - Drops outbound frames if source mac is different that initial mac
    - Reject = default
* Traffic Shaping
  + Establishes hard coded limits for peak bandwidth, average bandwidth and burst size to reduce VM outbound bandwidth (inbound also with VDS)
  + Average Bandwidth
    - Data transfer per second across the virtual switch
  + Peak bandwidth
    - Max bandwidth switch can pass without dropping packets
  + Burst size
    - Max data included in burst
  + Set on vdport group or port level
  + Inherited from upper level
  + Can be overridden
* Teaming and failover
  + Load Balancing
    - Route Based on originating virtual port
      * Choose uplink based on virtual port
      * Traffic on that port will always use the same uplink
      * Advantages
        + Even distribution of traffic if vNICs is greater than pNICs
        + Low resource consumption
        + No physical switch configuration required
      * Disadvantages
        + Virtual switch is not aware of load on uplinks
        + Bandwidth is a limited if only one NIC in VM
    - Route based on IP Hash
      * Choose uplink based on hash of source and destination IP
      * Any VM can use any uplink
      * Advantages
        + More even distribution of the load
        + Potentially higher throughput for VM that communicate with multiple IPs
      * Disadvantages
        + Highest resource consumption
        + Virtual switch is not aware of the actual load of the uplinks
        + Requires changes to the physical network
        + Complex to troubleshoot
    - Route based on source MAC hash
      * Based on hash of source Ethernet mac
      * Advantages
        + More even distribution of traffic because switch calculates route for every packet
        + VM uses same uplink because MAC is static
        + No changes to physical switch
      * Disadvantages
        + Bandwidth limited to speed of uplink unless VM has more than one NIC
        + Higher resource consumption
        + Virtual switch is not aware of load
    - Route based on physical NIC load
      * Choose uplingk based on current load on uplinks
      * Advantages
        + Low resource consumption because swtich calculates uplinks only once
        + Distributed switch is aware of load on uplinks
        + No changes on the physical switch
      * Disadvantages
        + Bandwidth that is available to a VM is limited to the uplinks tat are connected
    - Use explicit failover order
      * Only use the highest uplink that is active
  + Network Failure detection
    - Used to check when a unplink is available
    - Link Status Only
      * Detects cable pulls and physical switch power failures but no config errors or errors downsteam of physical switch
    - Beacon probing
      * Sends out and listens for probes on all NICs in the team
      * Requires three NICs
      * Do not use with IP HASH
  + Notify switches
    - Notify switches in case of failover (Yes / No )
    - Physical switches keep mac address lookup tables so they know where to send traffic
    - Usually want this enabled
    - Lowest latency when a failover or a migration with vMotion occurs
  + Failback
    - Switch back to original uplink when restored
* Netflow
  + Enabled or disabled

#### Overrides

* Override settings inherited from port group on a per port basis
* Configure reset at disconnect
  + When VM disconnected from port, overrides are set back to port group settings
* Override port Policies
  + Select polices to be overridden per port

## Objective 4.6 – Deploy and configure VMware vCenter Server Appliance (VCSA)

### PSC

* Stage 1
  + Deploy OVA
  + Basically give you options like any VM
    - IP
    - Network
    - Name
    - Which host
* Stage 2
  + Configure Deployment
  + Time
    - Sync time with ESX host
    - Sync time with NTP Server
  + SSO
    - Create new SSO domain
    - Join existing SSO domain
  + VMWare CEIP

### After Installation

#### Repoint vCenter server with embedded or external PSC to Embedded or external PSC in a different SSO domain

* Can move one vCenter server at a time to a PSC in different domain
* can move vcenter servers that point to same PSC to different PSC in diff domain
* can point vcenter server from embedded PSC to external PSC in diff domain
* cmSSO-util domain-repoint –mode execute

#### Converging vCenter server with external PSC to embedded PSC

* either use vcenter client
* or vcsa-util converge

#### Reconfigure vcenter with embedded PSC to external PSC

* install external PSC
* cmSSO-util reconfigure

#### VCSA Backup and Restore

* File based backup and restore
* Use VAMI to create backup of appliance and PSC
  + Backs up
    - Ore configuration
    - Inventory
    - Historical data
* Restore using install GUI
  + Deploy new appliance and copy data from backup
* Backed up to
  + FTP
  + FTPS
  + HTTP
  + HTTPS
  + NFS
  + SCP
  + SMB
* For VCSAHA only the primary server is backed up
* Schedule backup
  + New to 6.7

### Upgrading to 6.7

* Can upgrade from 6.0 or 6.5
* Upgrade is migration to new appliance
  + Temp IP assigned to new appliance and then changed once migration is complete
* External DB migrated to postgress DB on new appliance
* External VUM migrated to embedded VUM
* External PSC requires PSC to be migrated firstlog

## Objective 4.7 – Set up identity sources

### SSO

* Single sign on
  + STS
    - Secure Token Service
  + IDM
    - Identy Management Service
* Requires SSO Administrator privileges to modify
* Identity sources attach one or more domains to SSO
  + Domain is a repo of users and groups used for authentication
* Identity sources
  + Active Directory (Integrated Windows Authentication)
    - AD 2003 and later
    - Settings

|  |  |
| --- | --- |
| **Setting** | **Description** |
| Domain Name | * FQDN of the Domain * Must be DNS resolvable |
| Use Machine Account | * Use local machine account as the SPN * Faster config |
| User Service Principal Name | * Use this if you expect to rename local machine |
| Service Principal Name | * Helps Kerberos ID AD |
| User Principal Name password | * Name and password of a user who can authenticate with this Identity source |

* + Active Directory as an LDAP Server
    - Compatibility with vsphere 5.1
  + OpenLDAP

|  |  |
| --- | --- |
| **Option** | **Descriptiion** |
| Name | * + - * Name of Identity Source |
| Base DN for users | * + - * Base distiguised name for users |
| Base DN for groups |  |
| Domain Name | * + - * FQDN of the domain |
| Domain alias | * + - * Ad * Use Netbios name if using SSPI authentication   + - * OpenLDAP * Domain name in all caps is added if left blank |
| Username | * + - * ID of user in domain with read-only access |
| Password | * + - * Username password |
| Connect to | * + - * Domain controller to connect |
| Primary Server URL | * + - * Primary domain LDAP server |
| Secondary Server URL | * + - * Secondary LDAP server for failover |
| SSL Certs | * + - * Cert for LDAPS |

* + - Settings
  + Localos
    - Users are local to OS that SSO is installed on
    - Not available with multiple SSO instances
    - Should only be used if PSC is embedded
* Add or Edit identity Source
  + The PSC windows deployment server must be joined to AD to add AD as a ID Source

## Objective 4.8 – Configure an SSO domain

### Default Domain

* Users in the default domain can leave their domain off when logging in.
* Can only be one default domain in SSO
* Modify
  + Home -> Administration -> Single Sign On -> Configuration
  + Click Identity Source and set as default

### Windows Session Authentication (SSPI)

* Speeds up login process by using account of user logged into client machine
* Prerequisites
  + Join PSC to AD
  + Install enhanced authentication plug-in

### Two-Factor Authentication

* Smart Card authentication
  + CAC
  + Setup PKI and CAC readers with certs
  + Configure by vsphere client or SSO-Config
* RSA SecureID authentication
  + Uses tokens that change routinely
  + Must use SSO-config to configure

### SSO as Identity Provider for another service provider

* SSO can be uses as identity provider for other service providers
  + I imagine this is other VMWare solutions

# Section 5 – Performance-tuning and Optimizing a VMware vSphere Solution

## Objective 5.1 – Determine effective snapshot use cases

* Snapshots freeze VMDK and start writing to delta disk
* Options
  + Snaptshot VM memory
    - Include RAM
    - Current contents of RAM written to .VMSN file
  + Quiesce guest file system
* Can cause performance issues when left overtime
* Snapshot Consolidate
  + Sometimes backup apps fail to compress after deleting the snapshot
  + Commits delta back to base disk
* Limitations
  + Does not support
    - Raw Disks
    - Physical RDM
    - Guest with ISCSI initiator
    - Direct I/O
    - Independent disks
  + VM w/ independent disk must be powered off
  + No VM bus sharing
  + Not meant to be long term backup / restore
  + Can cause performance issues
  + Larger than 2 TB takes long time to snapshot

## Objective 5.2 – Monitor resources of VCSA in a vSphere environment

### Performance Charts

#### Data Collection Levels

* Determins the amount of data gathered and which counters are available for display in charts
* Statistic levels
  + 1
    - Default collection level for all intervals
    - Log-term performance monitoring when device statistics are not required
  + 2
    - Level 1 metrics
    - More than just basics
  + 3
    - Level 1 and 2
    - Metrics for all counters excluding min and max rollup
    - Device metrics
    - Short term performance monitoring after encountering problems
  + 4
    - All metrics including min and max

### VAMI

* Overview of health status
* Monitor CPU, memory, database, storage , swap
  + Can see this info in various ranges up to past year
* Firewall – create rules as well as enable / disable builtin
* Set NTP servers
* Backup / restore

### vCenter

* Since VCSA is a vm performance data can be gathered from vCenter itself
* From shell
  + Df
    - Disk space

#### Watchdog

* Vmware-watchdog
* Shell script on VCSA
* Detects failure in services
* Services monitored
  + Rhttpproxy – Reverse Proxy
  + Vws – vCenter Management Web Service
  + Syslog – syslog collector
  + Vmware-postgress – postgres database
  + Vpxd – vCenter erver
  + Vsan-health – vsan health check

### VIMTOP

* SSH into VCSA and run TOP for performance counters
* Preinstalled
* Similar to ESXTOP

## Objective 5.3 – Identify impacts of VM configurations

### ESXTOP

#### Counters – CPU

* %RDY
  + Percentage of time the resource pool, VM, or world was ready to run but was not provided a CPU resource on which to execute
  + Indicates CPU over commitment
* %CSTP
  + Co Stop
  + Percentage of time a resource pool spends in ready , co-scheduled state
  + Waiting for other CPU to be available
  + Indicates CPU over commitment
* %Wait
  + Percentage of time a resource was in blocked or busy wait state
* %MLMTD
  + Max Limited
  + Time not running because the Memory Limit has been reached
  + Part of %RDY
* %SWPWT
  + Swap Wait
  + Time spent waiting for swap memory

#### Counters – Memory

* Memory State

|  |  |  |
| --- | --- | --- |
| **Memory State** | **Threshold** | **Actions** |
| High | 400% of minimum Free | Break large pages when below threshold (Wait for next Transparent page sharing (TPS) run ) |
| Clear | 100% min free | Break large pages and actively call TPS to collapse pages |
| Soft | 64% of min free | TPS + Balloon |
| Hard | 32% min Free | TPS + Compress + Swap |
| Low | 16% min free | Compress + Swap + Block |

* SW
  + SWAP
  + Swap usage
* MEMCTL
  + Ballon statistics
* MEMSZ
  + Amount of memory assigned to resource pool / VM

### vTMP 2.0

* Trusted Platform Module
* Specialized microcontroller cryptoproceSSOr to securely create and store assets
  + Stores identifying artifacts
    - Encryption keys
    - Platform measurments
* 6.7 can only use 2.0
* Attestation
  + Known good boot securely stored to compare w/ each new boot
  + Attestation key
* HTML5 only
* vTPM works with VM only
* window 10 and 2016
* stores attestation in NVRAM with vm files
* encrypt VM for security of vTPM NVRAM

### Network

* Dropped packets
  + ESXTOP or advanced performance chart
    - droppedTX and dropped RX
  + if dropped packets adjust VM shares (NIOC)
* performance without dropped packets check
  + size of network packets
  + data receive and transfer rates

### VM Debugging and Statistics

* setting the VM to collect additional debugging and information helpful to troubleshooting
* poweroff VM
* options
  + Run Normally
  + Record Debugging information
  + Record Statistics
  + Record Statistics and Debugging information

# Section 6 – Troubleshooting and Repair -- There are no testable objectives for this section.

# Section 7 – Administrative and Operational Tasks in a VMware vSphere Solution

## Objective 7.1 – Manage virtual networking

### Networking Policies

* Applied to vSS or VDPort group apply to all of the port groups / ports
  + Exception are the options that are overridden
* See VDS
* Port Binding
  + When a port is assigned to a VM
  + Static
    - When VM connects to group
  + Dynamic
    - When VM is powered on
  + Ephemeral
    - No port binding
    - Doesn’t take up a port
    - Use if vCenter is offline
* Bandwidth
  + Teaming Policies
  + LACP
  + Traffic Shaping
  + NIOC

## Objective 7.2 – Manage datastores

### Storage arrays

* Active / Active
  + Most use FIXED routing policy
* Active Passive
* ALUA

### Storage components

* PSA
  + Pluggable Storage Architecture
  + Modular framework coordinates software modules responsible for multipathing
* NMP
  + Native Multipathing Plugin
  + Provided by default
  + Assiciates physical paths with specific storage devices and privied default path selection based on array type
  + Manages
    - PSP
      * Path Selection Plugin
      * Select physical path for I/O Request
      * Rout Selection
        + MRU

Most Recently Used

No failback

* + - * + Fixed

Preferred path

Failback

* + - * + RR

Round Robin

Uses all paths depending on algorithm

* + - SATP
      * Storage Array Type Plugin
      * Array specific operations
* MPP
  + Multipathing plugin
  + Specific load balancing and failover functionalities for storage arry
  + Vendor specific
  + Run in addition to NMP
* HPP
  + VMWare High Performance Plugin
  + Replaces NMP for high speed devices
  + Only single pathed devices
* Claim Rules
  + Determin wheter MPP or NMP owns the path to particular storage device

Thin vs Thick Provisioning

VMFS 5 vs VMFS 6

## Objective 7.3 – Configure a storage policy

### Storage Policy Based Management

* Aligns storage with application demands of VMs
* Abstracts VVol, vSAN, IO filters, etc
* Offerings
  + Advertise storage capabilities and data services
  + Bidirection communication between esx / vCenter and storage arrays
  + Virtual machine provisioning based on VM storage policies

#### Virtual machine storage policies

* Control which type of storage is provided for the VM and how the VM is placed within the storage
* Determine data services that the VM can use
* Workflow
  + Populate VM Storage policies interface
    - Information about storage and data services
    - Storage capabilities and Services
      * Storage providers (VASA) advertise capabilities
      * Used when creating rules and rulsets
    - Data Services
      * I/O Filters
    - Tags
      * VMFS and NFS datastores do not advertise their capabilities or services
      * Tags can represent
  + Create predefined storage policy components
    - Each component describes a data service to be provided for the VM
    - Can be aSSOciated with multiple policies
    - Types of services
      * Compression
      * Caching
      * Encryption
      * Replication
    - Guidelines
      * Each component can include only one set of rules belonging to a single provider
      * If referenced in VM storage policy, the component cannot be deleted
      * Policies can have on ly one component from the same category
  + Create VM storage policies
    - Storage requirements for applications to run on a VM
  + Apply the VM Storage policy to the VM
    - Apply when provisioning VM or configuring its VMDKs
    - If no policy is specified, the default policy is used
  + Check compliance for the VM Storage policy
* Rules
  + Basic element of VM storage policy
  + Statement describing single requirement for virtual machine storage and data services
* Rule Set
  + Collection of rules
  + Datastore specific rule sets
    - Must include placement rules describing VM storage requirements
    - Can include data services for the VM
  + Placement rules: Cabability Based
    - Specify a particular storage requirement for the VM allowing the correct datastore to be selected
  + Placement rules: Tag based
    - Reference tags
  + Rules for host based services
    - Activates data services provided by host ( encryption, replication, etc)
    - Does not include placement rules
* Storage Policy Components
  + Describes a particular data service to be provided for the VM
  + Provider of service can be storage system, I/O filter, or another entity
  + Each component can include only one set of rules
  + Cannot delete component if it is referenced in a VM storage policy
* After you edit an applied storage policy, you must reapply the policy as there will be an error indicating the compliance status of the VM is out of date

## Objective 7.4 – Configure host security

## Objective 7.5 – Configure role-based user management

## Objective 7.6 – Configure and use vSphere Compute and Storage cluster options

## Objective 7.7 – Perform different types of migrations

### Cold Migration

* Migration with the VM powered off
* Usefull when VM is migrating from host with Intel to AMD proceSSOr. ( must be powered off to migrate between different proceSSOr vendors or families )
* Does not check for CPU compatibility when powered off except for bitness
* Uses provisioning network VMK ( or management if provisioning traffic is not defined)

### vMotion

* Requirements
  + Source and dest access to shared datastore
  + 250GBS network for each concurrent vMotion
  + Source dest IP should be in same l2 network
  + GPU must be same on both dest and SRC
  + USB backed VM must have the USB enabled for vMotion
  + Can’t vmotion VM if the vm has a physical device attached (Other than USB)
  + Flash cache must exist on dest
* Max 8 over 10 GB NIC
* MAX 4 over 1 GB NIC

### Storage vMotion

* Migrate from one datastore to another
* Can put VMDK on separate datastores
* Can change disk provisioning type
* Requirements
  + Persistent mode disks or RDMs
  + Access to source and dest datastores

### Shared Nothing vMotion

* sVmotion and vMotion at same time
* c

### Cross vCenter vMotion

* performance data is lost
* requirements
  + esx 6 and later
  + enterprise plus
  + time synch
* can vmotion storage or compute or both
* network compatibility checks
  + MAC address compatibility
  + vMotion from VDS to VSS
  + vMotion between distributed switchs of different versions
  + vMotion to an internal network
  + vMotion to a distributed switch that is not working properly

### Long distance VMotion

* Requirements
  + License cover long distance vMotion – Enterprise plus
  + RTT <= 150 ms

## Objective 7.8 – Manage resources of a vSphere environment

### CPU Scheduler

* Places vCPU onto physical CPU
* Schedules vCPUs on Physical CPUs
* Optimizes vCPUs onto same socket or different socket multi core proceSSOrs

### NUMA

#### Expose NUMA to VMs

* ESX 5.0 and later
* Hardware version 8 and later
* Enabled by default when vCPU is greater than 8
* NUMA topology does not consider VM Meory nor is it influenced by the number of virtual sockets and cores
* Virtual NUMA Controls
  + Advanced options

|  |  |  |
| --- | --- | --- |
| **Option** | **Description** | **Default Value** |
| Cupid.coresPerSocket | Number of virtual Cores per socket | 1 |
| Numa.vcpu.maxPerVirtualNode | Number of virtual NUMA nodes by splitting the total vCPU count evenly with this value | 8 |
| Numa.autosize.once | True means the numa topology will be evaluated every time the VM is powered on. False will only do it the first time | TRUE |
| Numa.vcpu.min | Min number of vCPUs in a VM that are required to generat virtual NUMA topology | 9 |
| Numa.vcpu.followcorespersocket | If 1 reverst to NUMA node sizing being tied to cupid.corespersocket | 0 |

#### Numa Controls

* Usefull with memory intensive workloads
* Numa Node Affinity
  + NUMA can schedule a VM only on the nodes specified in the affinity
  + Still managed by NUMA Scheduler
  + Numa.nodeAffinity
* CPU Affinity
  + VM uses only the processors specified
* Memory Affinity
  + Server allocates memory only on the specified NUMA Nodes

#### NUMA Scheduler

* Dynamically balances processor load and memory locality
* Scheduler assigns home node. CPU and Memory are preferred to come from this node
* Scheduler can migrate home node to another node if processor / memory becomes unbalanced
* Does not manage VMs with memory affinity or CPU affinity
* Can span NUMA nodes if the number of vCPU is greater than the number within a VM

## Objective 7.9 – Create and manage VMs using different methods

### Create VM

* Open wizard from any container object
* Create a new VM
  + Create VM from scratch
* Deploy VM from Template
  + Wizard to deploy from a premade template
* Clone a VM
  + Copy of an existing VM
* Clone VM to template
  + Copy of existing VM as a template
* Clone Template to template
  + Copy of existing template as template
* Convert Template to Vm
  + Converts a template to VM
  + Allows you to update the software and settings and patches

### Templates

* Can export VM, appliances and vApps to OVF and OVA

### Virtual Disks

* Inflate This VMDK
  + Remove snapshots
  + Power off VM
  + Use datastore browser and right click vmdk to inflate

### Memory

#### Persistent Memory

* Non volital memory ( NVM )
* PMem
* Low access latency
* Retain stored data through reboots / power outages
* Modes
  + Virtual PMem (vPMem)
    - PMem aware guest OS can have direct acces to the physical PMem
    - Can Uses NVDIMM to access / represent PMem to VM
      * Requires Hardware version 14
  + Virtual PMem Disk (vPMemDisk)
    - VM does not have direct access to PMem
    - Uses SCSI disk that is then places on PMem on host

#### PVRDMA

* Paravirtualized Remote Direct Access memory
* Direct memory access from one computer to another without involving the CPU or OS
* Transfer offloaded to RDMA capable host channel adapter
* VMs must be connected to same vDS
* Linux x64 only

## Objective 7.10 – Create and manage templates

* Create template
  + Convert to template
    - VM becomes a template and no longer exists
  + Clone to template
    - Creates a second VM that is a template
* VM Customization
  + Answer file used with a template to create a VM
  + Used
    - During cloning
    - When personalizing OS of a VM deployed from a template
    - On existing VM
      * Apply customization to VM
* Content library
  + OVF based template can be stored in content library

## Objective 7.11 – Manage different VMware vCenter Server objects

* DataCenters
  + Aggregation of all different types
* Clusters
  + Collection of hosts and VMs
  + When add host to cluster the resources become part of the clusters aggregate
* Datastores
  + Storage location for VMs
  + Can be local, ISCSI, NFS, etc
* Folders
  + Use to group objects
  + Can set permissions and alarms on folders to propagate to member objects
  + Can contain only one type of object
  + Can contain folders
* Hosts
* Networks
  + Set of vNICs, VDS, VSS, port groups, distributed port groups that connect VMs to each other and the physical network
* Resource pools
  + used to compartmentalize the CPU and memory resources of a host or cluster
  + VMs run in and draw resources from
  + Can contain other resource pools
  + Can delegate control of resource pool (permissions)
* Virtual machine
* vApps
  + can contain multiple virtual machines
  + like resource pool
  + can contain other vApps

## Objective 7.12 – Setup permissions on datastores, clusters, vCenter, and hosts

* Users or Groups are assigned to roles that have privileges
* Users
  + Authentication
* Group
  + Collection of users
* Privileges
  + Action that you can perform
* Role
  + Collection of privileges
* Permission
  + Pairs user/group with role at inventory object to allow permission to do something
* Allowing AD user to login
  + After joining to domain , user / group should be paired with role at vcenter object to allow user to login with AD credentials
  + Because account exists outside ESX, the actions by user creast task that then calls VPXUser on ESX to Run it
    - Used to communicate between VCSA and ESX
    - Stored in ESX DB
    - No shell access
* Effective Permissions
  + Object lower in hierarchy permissions overwrite inherited permissions
  + Groups at same level are joined / unioned / cumulative
  + User permissions at same level as group takes precedence
  + No access overrides all
* Global root
  + Assign permissions across all solutions

## Objective 7.13 – Identify and interpret affinity/anti affinity rules

### DRS Affinity Rules

* Controls the placement of VMs
* VM-Host Affinity Rules
  + Between group of VMs and Group of Hosts
  + Specifies if the VMs can run on the Hosts
  + Each rule is weighted equally
    - If a vm belongs to multiple rules. All rules must be satisified for the VM to start
  + Conflicts
    - Older takes precedence
    - Newer rule is disable
  + Use case
    - Licensing
    - Hardware requirements of the software
  + Must
    - Required
    - DRS, HA and DPM will not violate these
  + Should
    - Preferred
  + Rules are not ranked but applied equally
  + Rules are not checked against other rules so it is possible to create confilicting rules
    - When two conflict. Oldest rule takes precedence
* VM-VM Affinity Rules
  + Between individual VMs
  + Conflicts
    - Rules cannot be enabled if in conflict
    - Older rule takes precedence
    - Newer rule is disabled
* Anti affinity higher precedence than affinity
* HA Advanced options to enforce the desired failover behavior for HA
  + HA must respect VM anti-affinity rules during failover
    - Will not fail over a VM if it will violate a rule
    - Issues event stating issufficiate resources to perform failover
  + HA should respect Vm to host affinity rules during failover
    - Attempt to place VM with this rule but will ignore if need be

## Objective 7.14 – Understand use cases for alarms

* Alarms created at a higher point in the hierarchy will propagate down
* Types of alarms
  + Event
    - Might need to be manually reset if the clear event is not captured by alarms
  + State of an object
  + Set of conditions
* One objects alarms won’t apply to a different object type
* Target – defines vCenter object the alarm applies to
* Alarm Rule or Trigger
  + Defines event, condition or state that triggers the alarm
* Tolerance Threshold
  + Additional restrictions on condition and state triggers that must be exceeded before the alarm is triggered

## Objective 7.15 – Utilize VMware vSphere Update Manager (VUM)

### Quick Boot

* Restarts hyper visor without rebooting physical host
* Speeds up the upgrade process of an ESX server
* Option presented by update manager if hardware supports
* Potential issues if
  + Host not supported
  + Host is configured with TPM
  + Pass-through devices configured for VMs
  + Vmklinux drivers loaded
  + Non-certificed drivers loaded
  + Quick boot is disabled in Update manager
* Check for hardware compatibility
  + Run /usr/lib/vmwre/loadesx/bin/loadESXCheckCompat.py
* Troubleshoot
  + Log = LoadESX.log

### VUM

* Provides
  + Download patches and recall / notifications
* Updates hosts, appliances, and VM tools / hardware version
  + Determins the virtual hardware available to the Vm

|  |  |
| --- | --- |
| **Hardware version** | **ESX version** |
| 15 | ESX 6.7 update 2 and later |
| 14 | ESX 6.7 and update 2 |
| 13 | ESX 6.5 – ESX 6.7 Update 2 |
| 11 | ESX 6.0 – ESX 6.7 Update 2 |
| 10 | ESX 5.5 – ESX 6.7 Update 2 |
| 9 | ESX 5.1 – ESX 6.7 Update 2 |
| 8 | ESX 5.0 – ESX 6.7 Update 2 |
| 7 | ESX 4.0 – ESX 6.7 Update 2 |
| 4 | ESX 3.5 – ESX 6.7 Update 2 |

* + Update third party software on hosts
* Baseline
  + One or more patches, extensions or upgraded you want to apply
  + Host or VM Baselines
  + Dynamic
    - Auto downloads patches
  + Fixed
    - Patches don’t change
  + Patch baselines – hold patches
  + Extension baselines – software modules for Hosts, could be VMware or third party
* System Managed Baselines
  + Update content periodically
  + Only appear and only can be used if you have vSAN
* Predefined Baselines
  + Cannot be edited or deleted
  + Critical Host Patches (Predefined)
    - Checks Hosts for compliance with all critical patches
  + Non-Critical Host Patches (Predefined)
    - Optional patches
* Custom Baselines
  + Created by you
* Baseline Groups
  + Include multiple baselines
  + Set of Non conflicting baselines
* Admin settings
  + Patch downloads
    - Where updates come from
  + Patch setup
    - Proxy to get to internet
  + Recall Notification
  + Network Connectivity
    - Ports and hostnames
* Remediation settings
  + Hosts
    - Which hosts to exclude , PXE Booted hosts, hosts with VMs, Retries, etc
  + VMs
    - Take snapshot automatically
    - How long to keep
* Stage Baseline
  + Will copy patches to host which allows you to save time during the actual remediation
* Remediating a cluster, default sequencial. Can be configured to be in parallel where VUM figures out how many hosts can safely be in maintenance mode at one time.

#### Update Manager Download Service

* Optional module
* Downloads patch metadata, patch binaries, and patch recalls and notifications
* Used when VUM is not able to download from internet directly

## Objective 7.16 - Configure and manage host profiles

* Allows ESX Configurations to be consistent
* Create host profile only from reference host
* Passwords do not get exported with the host profile
* Can be applied to a host, cluster or all hosts and clusters
* Can check compliance with profile
  + Compliance check can be scheduled
* Can disable part of host profile so it is not checked
* Export Host profile
  + Exprots as .vpf
* Extract host profile from ref image
  + Original ref image does not need to be to use host profile but a similar one does need to be there.
* Attach to host to apply
  + Scan and remediate
* Update host profile
  + If reference host changes you can copy settings from host to update profile
* Using with autodeploy
  + Allows host to be configured from scratch
* Host Customizations
  + Used to set specific values for that host
  + Can prompt for user input
  + Export as .csv

# Key

No Data – Need Own notes, VLADAN.fr, and VMWare docs

Need VLADAN.fr, VMWare docs

Need VMWare Docs

Research complete

<https://www.vladan.fr/vcp6-7-dcv/>

<http://www.it-muscle.com/vcp-2019-study-guide/>

<https://vloreblog.files.wordpress.com/2019/09/vcp-dcv-subtopics.pdf>

<https://www.tayfundeger.com/objective-2-1-describe-vsphere-integration-with-other-vmware-products.html>