VMware VCP-IaaS Study Notes

Based on Exam Blueprint 1.2
Exam Blueprint 1.2 Sections (same in 2.4)

Section 1 – Install and Configure vCloud Director
Objective 1.1 - Install vCloud components
Objective 1.2 – Configure and Administer vCloud Connector
Objective 1.3 – Configure vCloud Director and vShield Manager System Settings

Section 2 – Administer Users, Roles and Privileges in a vCloud
Objective 2.1 – Create Roles and Apply Privileges to Roles in a vCloud
Objective 2.2 – Configure AD/LDAP Integration in a vCloud
Objective 2.3 – Configure and Administer vShield Edge

Section 3 – Configure and Administer vCenter Chargeback
Objective 3.1 – Configure and Administer vCenter Chargeback Roles and Privileges
Objective 3.2 – Configure and Generate vCenter Chargeback Reports
Objective 3.3 – Configure and Manage vCenter Chargeback Cost Elements
Objective 3.4 – Troubleshoot Common vCenter Chargeback Issues

Section 4 – Configure and Administer vCloud Networking
Objective 4.1 – Create and Administer vCloud External and Organization Networks
Objective 4.2 – Configure and Administer vCloud Network Pools
Objective 4.3 – Configure and Administer vApp Networks
Objective 4.4 – Administer vCloud Network Services

Section 5 – Configure and Administer vCloud Organizations
Objective 5.1 – Create vCloud Organizations
Objective 5.2 – Administer vCloud Organizations

Section 6 – Allocate and Manage vCloud Resources
Objective 6.1 – Create and Administer Provider VDCs
Objective 6.2 – Create and Administer Organization VDCs

Section 7 – Create and Administer vCloud Catalogs
Objective 7.1 – Create vApp Templates, Media and Catalogs
Objective 7.2 – Administer vCloud Catalogs

Section 8 – Monitor a vCloud Implementation
Objective 8.1 – Troubleshoot and Audit Resources and Events in a vCloud
Objective 8.2 – Map vCloud Resources to vSphere Resources
Introduction:

This document are my ramblings on the not so new VCP-IaaS exam. Taking this exam gives you the VCP-Cloud certification.

There are two ways you can take to get teh VCP-Cloud certification, and I went through both of them in one of my blog posts: VCP-IaaS vs. VC-Cloud: Cloud Exam Faceoff

The main difference between the two is that you can get the VCP-Cloud without having the VCP5. Instead you can take a qualifying course.

More on these here: VCP-Cloud and VCP-IaaS.

The document are my notes when I was going through the VCP-IaaS blueprint (1.2) and I hope this will help you in your journey towards the VCP-IaaS.

I recently compared the new blueprint (2.4) to 1.2 and there is NO additions of sections or subsections so the information is still relevant.

Most of the content was COPIED from the corresponding tools stated at the end of each Section, with minor editorial changes, only changing something when the text didn’t make sense or I though it needed further explanation.

Even though these Study Notes can be helpful I recommend setting up your own vCloud environment in a lab if you haven’t done so before.

All you need is a 8 GB workstation/laptop and the glorious Autolab. http://www.labguides.com/autolab/

(and lots of ISOs and installation packages, but that should be a problem for most techs)

For other study material Gregg Robertson over at theSaffaGeek.co.uk has a great overview of study material to ease your googling.

Also I recommend reading through the vCloud, vShield, Chargeback and Security Hardening Guides before taking the exam.

Please feel free to contact me on Twitter (@lhjartarson) or LinkedIn for any questions.

Let the notes begin!
Objective 1.1- Install vCloud components

Knowledge

- **Identify required vCloud components and pre-requisites for installation**
  - Components (Figure 1.1)
    - vCloud Director Cell or Cells
    - vCloud Director Database
    - vCenter and ESXi hosts
    - vCenter Database
    - vShield Manager
    - Connected to each vCenter.

  - Pre-requisites vCloud Director
    - Networks to be used as external networks should be available to all hosts for the vCloud Director to use.
    - DVS must be used for cross-fencing and network pool allocation.
    - Automated DRS must be configured.
    - vCenter 5.0 cluster can not use storage DRS.
    - vCenter server must trust their ESXi hosts. (certificates)
    - Need to have the appropriate licences :)
    - Supported OS:
      - Red Hat Enterprise 5 (64bit), U4,U5 or U6.
      - 950Mb for installation files
      - 1 GB min memory, 2 GB recommended.
      - MSSQL and Oracle supported as databases.
      - SSL certificates for each vCloud network interface (http and consoleproxy)
  - Pre-requisites vShield
    - 8GB Memory
    - Disk space - 8GB vShield Manager, 5GB vShield App per ESX host, 200mb per vShield Edge.
    - 2x Gigabit NICs on ESX hosts for all vShield components.

- **Describe installation order of vCloud components**
  - Install vCenter and ESXi hosts
- Configure a cluster with a DVS, Automatic DRS, and External DVS portgroup for external networks.
  - Setup vShield Manager
  - Setup the vCloud Database
  - Install vCloud Director instances.
  - Verify DNS resolution.
  - Verify NTP between vCloud Director Cells and databases
  - Open necessary ports

- **Explain the purpose and use case of each vCloud component**
  - VMware vCloud Director (vCD)
    - Cloud Coordinator and UI. Abstracts vSphere resources.
  - vCloud API
    - API used to programmatically interact with a vCloud
  - VMware vSphere
    - Underlying foundation of virtualized resources.
  - VMware vShield
    - Provides network security services
  - VMware vCenter Chargeback
    - Optional component that provides resource metering and reporting to facilitate resource showback/chargeback
  - VMware vCenter Orchestrator
    - Optional component that facilitates orchestration at the vCloud API and vSphere levels.
  - VMware vCloud Request Manager
    - Optional component that provides provisioning request and approval workflows, software license tracking, and policy-based cloud partitioning.
  - VMware vCloud Connector
    - Optional component to facilitate transfer of a powered-off vApp in OVF format from a local vCloud or vSphere to a remote vCloud

- **Create a SysPrep package**
  - You will need access to the Sysprep binary files from Windows.
    1. Copy the Sysprep binary files for each operating system to a convenient location on a vCloud Director server host.
Each operating system requires its own folder. NOTE Folder names are case-sensitive.

<table>
<thead>
<tr>
<th>Guest OS</th>
<th>Copy Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2003 (32-bit)</td>
<td>SysprepBinariesDirectory /win2k3</td>
</tr>
<tr>
<td>Windows 2003 (64-bit)</td>
<td>SysprepBinariesDirectory /win2k3_64</td>
</tr>
<tr>
<td>Windows XP (32-bit)</td>
<td>SysprepBinariesDirectory /winxp</td>
</tr>
<tr>
<td>Windows XP (64-bit)</td>
<td>SysprepBinariesDirectory /winxp_64</td>
</tr>
</tbody>
</table>

SysprepBinariesDirectory represents a location you choose to which to copy the binaries.

- Run the /opt/vmware/cloud-director/deploymentPackageCreator/createSysprepPackage.sh SysprepBinariesDirectory command.
  - For example, /opt/vmware/clouddirector/deploymentPackageCreator/createSysprep Package.sh /root/MySysprepFiles.
- Use the service vmware-vcd restart command to restart the cloud cell.
- If you have multiple cloud cells, copy the package and properties file to all cloud cells.
  
  
  - scp /opt/vmware/cloud-director/guestcustomization/vcloud_sysprep.properties
    /opt/vmware/clouddirector/guestcustomization/windows_deployment_package_sys
    prep.cab
  - root@next_cell_IP:/opt/vmware/cloud-director/guestcustomization

- Restart each cloud cell to which you copy the files.

- **Install vCloud Director**
  - Download installation package to target server
  - Verify checksum
    - md5sum -c checksum-value installation-file
  - Ensure installation file is executable
    - chmod u+x installation-file
  - Run the installation file in console:
    - ./installation-file
  - Press N to run the configuration script later.
  - Setup a NFS volume to be used as temporary storage for uploads and downloads
    - Root needs write permission.
    - The path is /opt/vmware/vcloud-director/data/transfer
    - Need several hundred GB volume.
    - To mount a NFS drive in Red Hat
      - Edit /etc/fstab and add this line
        - IP_of_NFS_Server:/path/mount /opt/vmware/vcloud-director/data/transfer<nfs> intr 0 0
      - Save your /etc/fstab.
      - Run this command: mount-a
      - Try writing on the newly mounted NFS volume. (vi test, :wq!)
  - Run the configure script again - /opt/vmware/vcloud-director/bin/configure
    - At this time you will need to have your database and SSL certificates ready.
    - Select which IP address will be used for HTTP and Console Proxy.
    - Specify the full path to the Java keystore file. (eg. opt/keystore/certificates.ks)
    - Type keystore and certificate password.
    - Configure audit message handling - send to a syslog server & vCloud database or just the vCloud database.
    - Specify database type. SQL or Oracle.
    - Enter IP address of database.
    - Enter port to listen to. (1521 for Oracle, and 1433 SQL)
- Type the database service name
  - Note, in SQL don’t change the default value.
  - Type username and password.
- **Install vShield Manager**
  - Obtain the vShield Manager OVA file.
  - Install the Virtual Appliance.
  - Configure Network settings
    - Go to Console - login as admin/default
    - Go to Enabled mode - command: enable.
    - Run the Setup wizard - command: setup.
  - Go to IP address of appliance in a browser
    - Log in with user admin/default.
    - Change password
  - Sync with vCenter
    - Settings and Reports -> Configuration -> vCenter
  - Register vShield Manager plug-in with vSphere Client
    - Settings and Reports -> Configuration -> vSphere Plug-in
- **Install vCenter Chargeback**
  - Pre-req:
    - Ports HTTP-8080, Load-balancer-8009 and HTTPS-443 need to be free.
    - Static IP.
    - Installation files need to be run locally.
    - 2GHz CPU, 4GB RAM, 2-3GB Disk space, 10-100-1000 ethernet
    - SQL or Oracle 10g
    - Open ports in Windows firewall if needed.
  - Run vCenter-CB.exe
    - Next->Accept EULA->Choose path for installation->Enter database info->Enter load-balancer related info->Install vCenter Chargeback Server-
      - Enter username and pw for vCenter Chargeback Manager administrative account-
        - Select data collectors that you want to install-
          - If installing vCloud data collector enter database info->Press install -
            - Generate my own SSL certificate.
- **Install vCloud Connector**
  - Download vCC Server virtual appliance and the vCC Node virtual appliance from VMware.com
  - You can install the server&node appliance in a vSphere environment or an vCloud environment (1.0, 1.0.1, 1.5).
  - vSphere Environment
    - Import the OVA and assign an IP.
  - vCloud Environment
    - Make the appliances as vApp Template in the vCloud
    - Create the vCloud Connector Server/Node from the template
    - Setup NAT mapping for the Server or Node
- **Configure vCloud Director network connections**
  - You need two IP addresses. One for HTTP and one for the ConsoleProxy.
  - When you run the configuration script it asks you what IP you will be using for each.
  - Then you need to point to the SSL certificate keystore.
- **Configure vCloud Director database settings**
  - In the same configuration script you select what kind of database will be used: SQL or Oracle
  - Host IP->Port->Database Service name->Database user and password
- **Troubleshoot basic installation issues**
I've had trouble with the database connection when running the configure script. Do not change the default name of the SQL Database Service Name.

Objective 1.2 – Configure and Administer vCloud Connector

Knowledge

• Identify components of vCloud Connector
  o vCloud Connector UI
  o vCloud Connector Server
  o vCloud Connector Nodes

- Describe cross-cloud vApp flow
  o Customer requests transfer using vCC UI.
  o vCC Server tells Node to transfer vApp.
  o Node tells vCenter Server to "export" using VIM API.
  o Content is moved from datastores to source Node cache via vmkernel network.
  o Content is transferred from source to destination Node via multipart using checkpoint-restart.
  o Destination Node tells vC to do an "import" using vCloud API.
  o Content transfers from destination Node cache to vCD transfer server storage.
  o vCD commands the appropriate vCenter import.
  o Content transfers from vCD transfer server storage to destination datastore via vmkernel network and is made available through the vCD catalog.
- **Identify VM state (shutdown/power down)**
  - Click workloads in the vCloud Connector GUI.
  - Select the appropriate entry
  - If you are changing the state of a vApp with multiple VMs, the status of the child VMs will not reflect their new state automatically. To see the updated status, refresh the screen.

- **Differentiate between functionality of components of vCloud Connector**
  - **vCloud Connector UI**
    - vCloud Connector UI is the user interface that vCloud Connector Server produces. It can be surfaced in vSphere Client or at vcloud.vmware.com. If you decide to display your UI via vcloud.vmware.com, and your vCC Server is behind a firewall, only browsers also behind the firewall can see the UI. You decide where to display the UI during the configuration process.
  - **vCloud Connector Server**
    - vCloud Connector Server is a virtual appliance that coordinates the activity of vCloud Connector, controls vCloud Connector Nodes, and produces the vCloud Connector UI. Only one vCloud Connector Server is needed.
  - **vCloud Connector Nodes**
    - vCloud Connector Nodes are virtual appliances that handle transferring content from one cloud to another. Transfers between clouds that are interrupted, for example because of network problems, can be resumed at the point that they were interrupted. A vCloud Connector Node must be installed in every vSphere or vCloud cloud that vCloud Connector oversees.

- **Explain the relationship between the components of vCloud Connector**
  - vCloud Connector Server is installed at local vSphere environment
    - Only one Connection Server is needed.
  - A vCloud Node is the installed in the local vSphere environment or the local private vCloud.
  - Another vCloud node is installed at a public vCloud.
  - The GUI is either accessible through the vSphere client or vcloud.vmware.com.
  - There you manage your vCloud connections and do your copy tasks between vClouds.

- **Determine and implement required network and security settings**
  - These ports need to be open in NAT connection in the vCloud
    - Port 8443: For communication between vCC Server and Node and between Nodes.
    - Port 5480: For communication with the Web admin interface for the appliance, for example during the registration process.
- You can change the password, adjust log level and manage SSL certificates in the Connector Server
- You will need to replace the self signed SSL certificates before production use.

**Determine storage requirements and add storage for use by a vCC node**

- Copy operations rely on staging storage when you copy resources between clouds. To successfully copy resources, make sure you have enough storage in your vSphere and vCloud Director clouds. Default storage on Nodes is 40 GB. You may need to increase this if you will be copying large VMs or templates or if you will be copying many items simultaneously.

- Pre-req
  - Take a snapshot of the appliance

- In vSphere
  - Add a second hard drive to the VM
  - Go to console and run: `sudo /opt/vmware/hcagent/scripts/resize_disk.sh`

- In vCloud
  - Turn off VM in vApp
  - Select properties ->Hardware->Add->Disk.
  - Power on VM - Open console
  - Logon - admin/vmware
  - Name the new disk, command: `ls /dev/sd*`
  - Add the new disk, command: `sudo /opt/vmware/hcagent/scripts/add_disk.sh <diskname>`

**Register vCloud Connector with vCenter Server**

- In the vCloud Connector GUI click the vSphere Client button
- Fill in the information
  - IP and name of vCC server and vCenter, user and pw for vCenter.
- If you previously registered a vSphere client you can choose: Overwrite existing registration
- Click register.

**Objective 1.3 – Configure vCloud Director and vShield Manager System Settings**

**Knowledge**

- **Identify vCloud Director pre-requisites**
  - See section 1.1: Identify required vCloud components and pre-requisites for installation

- **Cite the steps to deploy a vShield Manager appliance**
  - See section 1.1: Install vShield Manager

- **Identify relationship between vCenter Server and vShield Manager**
  - At first time logon into the vShield GUI you will be prompted to connect to a vCenter server
  - The vShield Manager connects to the vCenter Server, logs on, and utilizes the VMware Infrastructure SDK to populate the vShield Manager inventory panel. The inventory panel is presented on the left side of the screen. This resource tree should match your VMware Infrastructure inventory panel.

- **Generate self-signed certificates**
  - vShield
    - You can generate or import an SSL certificate into the vShield Manager to authenticate the identity of the vShield Manager web service and encrypt information sent to the vShield Manager web server. As a security best practice,
you should use the generate certificate option to generate a private key and public key, where the private key is saved to the vShield Manager.

- Settings and Reports->Configuration->SSL certificate->Generate Certificate Signing Request.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name</td>
<td>Enter the name that matches the site name. For example, if the IP address of vshield Manager management interface is 192.168.1.10, enter 102.168.1.10.</td>
</tr>
<tr>
<td>Organization Unit</td>
<td>Enter the department in your company that is ordering the certificate.</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Enter the full legal name of your company.</td>
</tr>
<tr>
<td>City Name</td>
<td>Enter the full name of the city in which your company resides.</td>
</tr>
<tr>
<td>State Name</td>
<td>Enter the full name of the state in which your company resides.</td>
</tr>
<tr>
<td>Country Code</td>
<td>Enter the two-digit code that represents your country. For example, the United States is US.</td>
</tr>
<tr>
<td>Key Algorithm</td>
<td>Select the cryptographic algorithm to use from either RSA or DSA.</td>
</tr>
<tr>
<td>Key Size</td>
<td>Select the number of bits used in the selected algorithm.</td>
</tr>
</tbody>
</table>

- vCloud
  - Create an untrusted certificate for the HTTP service.
    - This command creates an untrusted certificate in a keystore file named certificates.ks.
      
      ```
      keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -genkey -keyalg RSA -alias http
      ```
      - Create an untrusted certificate for the console proxy service.
        - This command adds an untrusted certificate to the keystore file created in Step 1.
          
          ```
          keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -genkey -keyalg RSA -alias consoleproxy
          ```
      - To verify that all the certificates are imported, list the contents of the keystore file.
        
        ```
        keytool -storetype JCEKS -storepass passwd -keystore certificates.ks -list
        ```
  - Import self-signed or CA issued certificates
    - vShield
      - Click Settings & Reports from the vShield Manager inventory panel.
      - Click the Configuration tab.
      - Click SSL Certificate.
      - Under Import Signed Certificate, click Browse at Certificate File to find the file.
      - Select the type of certificate file from the Certificate Type drop-down list.
      - Click Apply.
    - vCloud - will be listing the main commands
      - `/opt/vmware/vcloud-director/jre/bin/keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -certreq -alias http -file http.csr`
      - CN = name of your site as it will be called, eg. vcloud.corp.com
      - OU = Corp
      - O = Corp Inc
      - L = City
      - S = City
      - C = US
      - `/opt/vmware/vcloud-director/jre/bin/keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -genkey -keyalg RSA -alias consoleproxy -keysiz 2048`
      - CN = name of your site as it will be called, eg. vcloud.corp.com
      - OU = Corp
      - O = Corp Inc
      - L = City
      - S = City
      - C = US
      - `/opt/vmware/vcloud-director/jre/bin/keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -genkey -keyalg RSA -alias consoleproxy -keysiz 2048`
      - CN = name of your site as it will be called, eg. vcloud.corp.com
      - OU = Corp
      - O = Corp Inc
      - L = City
      - S = City
      - C = US
CN = name of your console site as it will be called, eg. vmrc.corp.com
OU = Corp
O = Corp Inc
L = City
S = City
C = US

- /opt/vmware/vcloud-director/jre/bin/keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -certreq -alias consoleproxy -file consoleproxy.csr
- Send the *.csr files to a Certification company that will send you a signed certificates.
- When you get your certificate you will need to open it up and save it into three parts. One root certificate, one intermediate certificate and one http certificate and consoleproxy certificate.
  Note that the certificates need to be use these exact names. (root.cer, intermediate.cer, http.cer and consoleproxy.cer)

- Next thing to do is to import them into the vCloud installation
  - /opt/vmware/vcloud-director/jre/bin/keytool -keystore certificates.ks -import -alias intermediate -file intermediate.cer
  - /opt/vmware/vcloud-director/jre/bin/keytool -keystore certificates.ks -import -alias http -file http.cer
  - /opt/vmware/vcloud-director/jre/bin/keytool -keystore certificates.ks -import -alias consoleproxy -file consoleproxy.cer

- Add additional vCenter Servers to a vCloud Director implementation
  a. Type the host name or IP address of the vCenter Server.
  b. Select the port number that vCenter Server uses. The default port number is 443.
  c. Type the user name and password of a vCenter Server administrator.
     i. The user account must have the Administrator role in vCenter.
  d. Type a name for the vCenter Server.
     i. The name you type becomes the display name for the vCenter Server in vCloud Director.
  e. (Optional) Type a description for the vCenter Server.
  f. Click Next to save your choices and go to the next page.

- Configure licensing for vCloud Director and vShield Manager
  - vCloud
    - When logging onto the webportal for the first time you enter the licence for the vCloud.
    - Also you can change the licence in the portal in Administration->License.
  - vShield
    - After you attach a vCenter Server to vCloud Director, you must use the vSphere Client to assign a vShield for VMware vCloud Director license key.
      i. From a vSphere Client host that is connected to the vCenter Server system, select Home >Licensing.
      ii. For the report view, select Asset.
      iii. Right-click the vShield-edge asset and select Change license key.
      iv. Select Assign a new license key and click Enter Key.
      v. Enter the license key, enter an optional label for the key, and click OK.
        1. Use the vShield for VMware vCloud Director license key you received when you purchased vCloud Director. You can use this license key in multiple vCenter Servers.
vi. Click OK.

Objective 2.1 – Create Roles and Apply Privileges to Roles in a vCloud

Knowledge

- **Identify vCloud Director predefined roles and their specific privilege levels**
  - System Administrator
    - Can do everything that is possible to do in the vCloud GUI.
  - Organization Administrator
    - Can do everything in the Organization tab (when logging into a Org vCloud page)
  - Catalog Author
    - Create and change vApps and VM's.
    - Can create a new Catalog and Change it. (Can not change owner)
    - Create vApps from Catalog.
  - vApp Author
    - Create and change vApps and VM's.
    - Create vApps from Catalogs.
    - Can not change vApp owner.
  - vApp User
    - Delete, Edit Properties, Start/Stop/Suspend, Share, Copy, Access to console, VM properties, VM network, Manage VM pw.
  - Console Access Only
    - Access to console and Manage VM pw.

- **List the steps to create a custom role in vCD**
  - Click the Administration tab and click Roles in the left pane.
  - Click New.
  - Type a name and optional description for the role.
  - Select the rights for the role and click OK.

- **Identify operations that can be performed on predefined roles**
  - See above in first bullet.

- **Identify the types of users that can be granted access to a vCloud**
  - Local System Administrators
    - Administrators created in the vCloud GUI.
  - LDAP System Administrators
    - Administrators imported from a connected LDAP server.
  - Local Users
    - Users created inside Organizations for user access to vApps
    - Users that use predefined roles or custom roles.
  - LDAP Users
    - Users imported from LDAP server for acces to vApps.
    - Users that use predefined roles or custom roles.

- **Explain the purpose of a custom role in vCD**
  - If the existing roles do not meet your needs, you can create a role and assign rights to the role. When you create a role, it becomes available to all of the organizations in the system.

- **Determine when to create a custom role.**
  - ... Ehh... Monday? (see the above bullet)

- **Given an end-user’s job description, determine which role would be granted**
  - Just an example:
    - Organization IT admin: Organization Admin
    - Department Manager: Catalog Author
    - Department Sub Manager: Catalog User
- Regular User: vApp User.
- Contractor: Console Access only.
- **Validate the functionality allowed by a newly created role**
  - Log in test the if the permission granted are correct.
- **Select specific access rights in a security role.**
  - Open up the vCloud GUI
  - Select Administration
  - Select Roles
  - Select a role you want to change access rights
  - Right click and select Properties.
- **Troubleshoot common customized role access issues.**
  - If you know what the issue is, you can quickly find out what Role the user has and inform him what he's able to do with these rights. Move to a more privileged role if needed.

**Objective 2.2 – Configure AD/LDAP Integration in a vCloud**

- **Identify AD/LDAP infrastructure components**
  - An LDAP server is a authentication server in it self. When a user logs on vCloud Director checks the credentials of the user against the LDAP directory.
- **Configure Open LDAP with vCD**
  - OpenLDAP is supported with authentication method of Simple and Simple SSL.
  - Click the Administration tab and click LDAP in the left pane.
  - Type the host name or IP address of the LDAP server.
  - Type a port number.
    - For LDAP, the default port number is 389. For LDAP over SSL (LDAPS), the default port number is 636.
  - Type the base distinguished name (DN).
    - The base DN is the location in the LDAP directory where vCloud Director connects. VMware recommends connecting at the root. Type the domain components only, for example, DC=example, DC=com.
    - To connect to a node in the tree, type the distinguished name for that node, for example, OU=ServiceDirector, DC=example, DC=com. Connecting to a node limits the scope of the directory available to vCloud Director.
  - Select the SSL check box to use LDAPS and choose one of the certificate options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept all certificates</td>
<td>Select the check box.</td>
</tr>
<tr>
<td>SSL Certificate</td>
<td>Click Browse to locate the SSL certificate.</td>
</tr>
<tr>
<td>SSL Keystore</td>
<td>Click Browse to locate the SSL keystore. Type and confirm the keystore password.</td>
</tr>
</tbody>
</table>

- Select an authentication method.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple</td>
<td>Simple authentication consists of sending the LDAP server the user's DN and password. If you are using LDAP, the LDAP password is sent over the network in clear text.</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Kerberos issues authentication tickets to prove a user's identity. If you select Kerberos, you must select a realm.</td>
</tr>
</tbody>
</table>

- Type a user name and password to connect to the LDAP server.
If anonymous read support is enabled on your LDAP server, you can leave these text boxes blank.

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>User Name Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple</td>
<td>Type the full LDAP DN.</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Type the name in the form of <a href="mailto:user@REALM.com">user@REALM.com</a>.</td>
</tr>
</tbody>
</table>

- **Configure Active Directory with vCD**
  - Most ADs use Kerberos as the main authentication method so before you configure AD with vCD you will need to add a Kerberos realm. Other than that the process is the same as simple LDAP configuration (see bullet above).
  - Click the Administration tab and click LDAP in the left pane.
  - Click Edit All Realms.
  - (Optional) On the Realm tab, select Allow lower-case realms to allow realm names that include lowercase letters.
  - On the Realm tab, click Add.
  - Type a realm and its Key Distribution Center (KDC) and click OK.
    - If you did not choose to allow lower-case realms, the realm name must be all capital letters. For example, REALM.
  - On the DNS tab, click Add.
  - Type a DNS, select a realm, and click OK.
    - You can use the period (.) as a wildcard character in the DNS. For example, type .example.com.
  - Click Close and click Apply.

- **Test connectivity to external LDAP**
  - Click the Administration tab and click LDAP in the left pane.
  - Click Test LDAP Settings.
  - Type the name of a user in the LDAP directory and click Test.
  - Review the attribute mapping and click OK.

- **Import users and groups from external LDAP**
  - LDAP attributes provide vCloud Director with details about how user and group information is defined in the LDAP directory. vCloud Director maps the information to its own database. Modify the syntax for user and group attributes to match your LDAP directory.
  - vCloud Director automatically synchronizes its user and group information with the LDAP server on a regular basis. You can also manually synchronize with the LDAP server at any time.
  - Users and groups are ready to be used after configuring, testing and syncing to the LDAP server.

- **Troubleshoot common LDAP external connectivity issues**
  - Ports not open, LDAP user used to connect with wrong credentials, wrong DN, SSL misconfigured, lower case REALM name, incorrect attributes.
  - Not to much work to fix.

**Objective 2.3 – Configure and Administer vShield Edge**

**Knowledge**

- **Identify where to set firewall rules within vCloud Director**
  - Click the Manage & Monitor tab and click Organization Networks in the left pane.
  - Right-click the organization network name and select Configure Services.
  - Click the Firewall tab and select Enable firewall.
Select the default firewall action.
(Optional) Select the Log check box to log events related to the default firewall action.
Click OK.

- **Explain vShield firewall concepts as they relate to a vCloud environment**
  - The vShield Edge firewall provides network perimeter security and services to a tenant. It isolates the tenant’s stub network from the shared (uplink) networks and provides common perimeter security services such as DHCP, VPN and NAT.
  - The vShield Edge virtual machine has two network interfaces. One of the interfaces is connected to the uplink port through the PG-C port group and provides access to the external world. The other interface of the vShield Edge virtual machine is connected to the internal port group PG-X, which is part of the company X network.
  - All virtual machines of the company X tenant connect to PG-X port group, and these virtual machines are allowed to communicate with each other without going through the vShield Edge firewall virtual machine.
    However, if the company X virtual machine attempts to access external devices, traffic must flow through the vShield Edge virtual machine. Depending on the security rules defined, the access will be allowed or denied.
  - Also, the vShield Edge firewall virtual machine is protected through the VMware DRS and VMware HA features of the vSphere platform. So when a host on which vShield Edge is running goes down, that virtual machine gets restarted immediately on another available host in that cluster.

- **Determine which firewall rules need to be applied or modified**
  - What port will your application need to communicate through.

- **Identify ordering for firewall rules**
  - Firewall rules are enforced in the order in which they appear in the firewall list. You can change the order of the rules in the list. When you add a new firewall rule to an organization network, it appears at the bottom of the firewall rule list. If you want to enforce the new rule before an existing rule, make sure to reorder the rules.
    - Click Administration.
    - Select Cloud Resources > Networks.
    - Right-click the organization network name and select Configure Services.
    - Click the Firewall tab.
    - Drag and drop the firewall rules to establish the order in which the rules are applied.
    - Click OK.

- **Enable/Disable firewall**
  - See the first bullet in this section.

- **Add/Modify/Delete firewall rules**
  - Click the Manage & Monitor tab and click Organization Networks in the left pane.
  - Right-click the organization network name and select Configure Services.
  - Click the Firewall tab and click Add.
  - Type a name for the rule.
  - Select the traffic direction.
  - Type the source IP address and select the source port.
    - For incoming traffic, the source is the external network. For outgoing traffic, the source is the organization network.
  - Type the destination IP address and select the destination port.
    - For incoming traffic, the destination is the organization network. For outgoing traffic, the destination is the external network.
  - Select the protocol.
Select the action.
- A firewall rule can allow or deny traffic that matches the rule.
- Select the Enabled check box.
- (Optional) Select the Log network traffic for firewall rule check box.
  - If you enable this option, vCloud Director sends log events to the syslog server for connections affected by this rule. Each syslog message includes logical network and organization UUIDs.
- Click OK and click OK again.

- **Determine which vShield devices impact a given service**
  - What port is the service trying to communicate through? Where is the service located in the vCloud Organization network? On an internal NAT-ed network? On an external NATed network?

- **Verify firewall rule operation**
  - Allow the port and check for connectivity.

- **Troubleshoot common firewall service issues**
  - vShield Edge appliances are protected by HA so they should restart on another ESXi host if the first one fails.
  - Open port 80 to check for internet connection. Can rule out physical mis-configuration issues.
  - Etc...

---

**Objective 3.1 – Configure and Administer vCenter Chargeback Roles and Privileges**

**Knowledge**
- **Identify vCenter Chargeback permissions**
  - vCenter Chargeback Manager provides five different permissions, create, read, update, delete, and entity cost modify, which can be set on a role for the different resource types.

---

**Table 3-2. Permissions Applicable for Each Resource Type**

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Entity Cost Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vCenter Server</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Data Collector</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SMTP Server</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Chargeback Hierarchy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Chargeback Hierarchical Entity</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Attribute</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Tier</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cost Model</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Cost Template</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Fixed Cost</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Report</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Schedule</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Role</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Billing Policy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Automatic Report</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
- **Identify Resource types**
  
  vCenter Chargeback Manager defines various resource types and authorizes access to a resource on the basis of the role assigned to a user.

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vCenter Server</td>
<td>This resource type refers to the vCenter Server instances added to vCenter Chargeback Manager. A user must have read permission on the vCenter Server to read its entities and add them to a chargeback hierarchy.</td>
</tr>
<tr>
<td>vCenter Server Entity</td>
<td>This resource type refers to the entities in the vCenter Server hierarchy.</td>
</tr>
<tr>
<td>Data Collector</td>
<td>This resource type refers to data collectors registered with vCenter Chargeback Manager. Only a super user has all permissions on this resource type. A user with the Administrator role has only read permission on this resource type.</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>This resource type refers to the LDAP servers configured in vCenter Chargeback Manager. An LDAP user, by default, has read permission on the corresponding LDAP server.</td>
</tr>
<tr>
<td>SMTP Server</td>
<td>This resource type refers to the SMTP server configured in vCenter Chargeback Manager. Only a super user has all permissions on this resource type.</td>
</tr>
<tr>
<td>Chargeback Hierarchy</td>
<td>This resource type refers to the hierarchies created in vCenter Chargeback Manager. A user must have read permission on a chargeback hierarchy to access the hierarchy.</td>
</tr>
<tr>
<td>Chargeback Hierarchical Entity</td>
<td>This resource type refers to any entity created or added to a hierarchy in vCenter Chargeback Manager. A user must have read permission on the entity and the corresponding hierarchy to access it.</td>
</tr>
<tr>
<td>Attribute</td>
<td>This resource type refers to any attribute created or imported in vCenter Chargeback Manager. Only users with the Administrator role and Super User role have create permission for this resource type.</td>
</tr>
<tr>
<td>Tier</td>
<td>This resource type refers to the storage tiers created in vCenter Chargeback Manager. A user must have read permission on the vCenter Server to access storage tiers.</td>
</tr>
<tr>
<td>Cost Model</td>
<td>This resource type refers to the cost models defined or created in vCenter Chargeback Manager. A user must have read permission on a cost model to use it for cost configuration and report generation.</td>
</tr>
<tr>
<td>Cost Template</td>
<td>This resource type refers to the cost templates created in vCenter Chargeback Manager. A user must have read permission on a cost template to use it for cost configuration.</td>
</tr>
<tr>
<td>Fixed Cost</td>
<td>This resource type refers to the fixed costs created in vCenter Chargeback Manager. A user must have read permission on a fixed cost to use it for cost configuration.</td>
</tr>
<tr>
<td>Report</td>
<td>This resource type refers to the reports created in vCenter Chargeback Manager. A user must have read permission on a report to access the report.</td>
</tr>
<tr>
<td>Schedule</td>
<td>This resource type refers to the reporting schedules created in vCenter Chargeback Manager. A user must have read permission on a schedule to access the reporting schedule.</td>
</tr>
<tr>
<td>Role</td>
<td>This resource type refers to the roles defined or created in vCenter Chargeback Manager. Only users with the Administrator role or Super User role have create permission for this resource type.</td>
</tr>
<tr>
<td>Billing Policy</td>
<td>This resource type refers to the billing policies defined or created in vCenter Chargeback Manager. A user must have read permission on a billing policy to use it for cost configuration and report generation.</td>
</tr>
<tr>
<td>Automatic Report Scheduler</td>
<td>This resource type refers to the automatic report schedulers defined or created in vCenter Chargeback Manager. A user must have read permission on an automatic report scheduler to access it and the corresponding schedules.</td>
</tr>
</tbody>
</table>

- **Identify Resources that cannot be manually assigned permissions**
  
  You can assign permissions on a resource type to a user only through a role. However, you cannot assign permissions for the following resource types:
  - Data Collector
  - LDAP Server
  - SMTP Server
vCenter Server Entity
Attribute
Role
- The application automatically handles permissions for these resource types. Also, you cannot assign the create, update, and delete permissions for the VMware vCenter Server resource type during custom role creation.

- **Identify default vCenter Chargeback roles**
  - vCenter Chargeback Manager provides various predefined roles that can be assigned to the application users. The predefined roles are Super User, Administrator, Hierarchy Manager, Report Generator, vCenter Guest User, No Access, Dependent Resource Update, and Dependent Resource Read.
    - **Super User:**
      - Can do anything available in permission on the resource types.
    - **Administrator:**
      - Has read access on data collectors and no access to SMTP servers. Otherwise just like the super-users.
    - **Hierarchy Manager:**
      - Read access on vCenters, no access on Data collectors, LDAP, SMTP, Attribute, Tier, Role. Everything else allowed.
    - **Report Generator**
      - Has read access on Chargeback Hierarchy, and Hierarchical Entity. No access to vCenter, DC, LDAP, SMTP, Attribute, Tier and Role. Access to everything else.
    - **vCenter Guest User**
      - Read access for vCenter, Chargeback Hierarchy, and Hierarchical Entity.
    - **No Access**
      - No permission and can only be assigned on the Chargeback Hierarchial Entity resource type.
    - **Dependent Resource Update Role**
      - Create, Read, Update - Fixed Cost.
      - Read, Update - Report
      - Read, Update - Schedule
      - Read, Update - Billing Policy.
    - **Dependent Resource Read**
      - Read - Fixed Cost.
      - Read - Report
      - Read - Schedule
      - Read - Billing Policy.

- **Create/Modify/Delete a role**
  - **Create**
    - In the Users & Roles tab, click Roles.
      - A table listing all the roles defined in the application is displayed.
    - Click Create.
      - The Create Role screen is displayed.
    - Enter a name and description for the role.
    - Select the required permissions for the available resource types.
    - Click Create.
  - **Modify**
    - In the Users & Roles tab, click Roles.
      - A table listing all the roles defined in the application is displayed.
    - Select the role that you want to modify, and click Edit.
      - The Edit Role screen is displayed.
    - Modify the required information.
- You can modify the name and description of the role and also the set of permissions assigned to the role.
  - Click Save.
  - Delete
    - In the Users & Roles tab, click Roles.
      - A table listing all the roles defined in the application is displayed.
    - Select the role that you want to delete, and click Delete.
      - A dialog box confirming the action is displayed.
  - Click OK.
- **Determine when a new role should be created**
  - When the default roles don't have the correct permission/resource combination.
- **Associate a role to a user**
  - When you create a user, no roles or permissions are assigned to it by default.
  - You can assign only a single role to a user on vCenter Chargeback Manager. If the user already has a role assigned to it, the same is removed and the new role is set on the user.
  - In the Users & Roles tab, click Permissions.
    - A page listing the users, their type, whether the user has the Super User role or the Administrator role, and if the user is a vCenter Server user then the vCenter Server name or if the user is an LDAP user or group then the IP address of the LDAP server is displayed. The page also provides an option to select a resource type.
  - Select the user from the table listing the users.
    - If any role has already been assigned to the user on vCenter Chargeback Manager, the same is displayed under Currently Assigned Role.
  - Select the required role from the menu under Set/Reset Role.
    - Ensure that you do not select any resource on the left-side pane.
    - **NOTE** You cannot assign the Super User role on an LDAP user or group.
  - Click Apply.
  - A user can access a resource created in the application only if he has created it or has privileges to access it. A user can be given privileges to access a resource by assigning a role to him for the required resource.
  - When you assign a role to a user for a resource, vCenter Chargeback Manager automatically assigns either the Dependent Resource Update role or the Dependent Resource Read role to the user for the dependent resources.

<table>
<thead>
<tr>
<th>Table 3-10. Dependent resources in vCenter Chargeback Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Resource</td>
</tr>
<tr>
<td>Cost Model</td>
</tr>
<tr>
<td>Cost Template</td>
</tr>
<tr>
<td>Schedule</td>
</tr>
<tr>
<td>Automatic Report Scheduler</td>
</tr>
</tbody>
</table>

- **Troubleshoot common permission issues**
  - User doesn't have access to something he thinks he is supposed to have access to - Check permission and modify if needed.
Objective 3.2 – Configure and Generate vCenter Chargeback Reports

Knowledge

- Identify vCenter Chargeback report types
  - Cost Report
    - A cost report provides the cost and utilization information for each computing resource for the hierarchy or entity on which the report is generated based on the cost configured in the hierarchy and the cost model selected during report generation. An exported chargeback cost report includes various sections.
      - Report Summary
        - Name, Description, Bill date, Bill Period, Hierarchy, Chargeback Model, Report Addressed to, Total Charges.
      - Chargeback Cost Summary
        - This section specifies the total cost for the entity and all its child entities. The total cost for an entity is the rolled-up cost. That is, the costs of all the child entities are considered while calculating the cost of the parent entity.
      - Chargeback Resource Summary
        - This section provides cost for each chargeable computing resource, the fixed costs, and the total cost for the entity and its immediate child entities.
        - These details are displayed for each entity levels starting from the entity on which the report is generated to the leaf entities, that is, entities without any child entity.
        - The costs displayed in the report for each entity and for each resource are the rolled-up costs at that entity level. This section also displays the actual resource utilization details at each entity level. In a cost report, this section also includes the following graphs for each entity level starting with the entity on which the report is generated:
          - Cost per Resource
          - Cost per Child Entity
          - Usage per Child Entity
        - If the cost and usage data is not available for a specified period, then the graphs for this period are excluded from the exported report. Also, if a report is generated on a virtual machine or an entity without any child entities, then the report does not include any graphs.
      - Chargeback Cost Details
        - This section lists all the costs charged on each entity, the rolled-up costs of its child entities, and the total fixed costs. It also provides information about the cost model, the attributes set on the entities, and informational messages for the entities. The report contains a separate cost details section for each entity. This section displays the base rates, rate factors, used units, attribution percentage, and total cost for each computing resource of each virtual machine.
  - Usage Report
    - A usage report is similar to a cost report except that it provides only the computing resource utilization data. This report type is useful when you only want to analyze the resource utilization for various entities in a hierarchy. The report structure is similar to the cost report with the following exceptions:
      - No Cost Summary
      - Report Summary section has no cost information
      - Resource Summary section has no cost information
Resource Summary only includes the Usage per Child Entity graph
No Cost details section - instead it has a Usage details section
Bottom line = NO COST INFORMATION

Cost Comparison Report
- A cost comparison report enables you to compare the costs for each resource and entity based on two different cost models. The report structure is similar to the cost report with the following exceptions:
  - Report summary section does not display the total cost.
  - No graphs are available in the resource summary.

Showback Report
- A showback report lets you analyse how the costs are distributed among the entities based on a specified distribution policy. This report type is useful when you know the total cost and want to analyze how this cost is distributed among the entities by selecting different distribution policies. The report structure is similar to the cost report with the following exceptions:
  - Report summary section displays the distribution policy instead of the chargeback cost model.
  - No graphs are available in the resource summary.
  - Report does not include the Cost details section.

- Identify components of the reporting dashboard
- Given a reporting requirement, determine what report type should be run
- Schedule reports
  - When creating a report, you can choose to schedule the report generation from the Create Report screen. You can schedule cost reports, cost comparison reports, and usage reports. Showback reports cannot be scheduled.
  - Other than the create privilege for report and schedule resource types, you must have read privilege on the hierarchy, chargeback hierarchical entities, and cost models to perform this task.

- Manage archived reports
- Generate custom reports

Objective 3.3 – Configure and Manage vCenter Chargeback Cost Elements

Knowledge
For this section I HIGHLY recommend trying all these procedures in vCenter Chargeback before taking the exam. This is a dry subject but it will get a little bit better if you have the Chargeback GUI in front of you while going through this section. Chargeback is a very neccesary part of the vCloud and expect to be asked on this subeject.

Identify vCenter Chargeback cost elements
- You must know about the vCenter Chargeback Manager cost-related elements to effectively create and configure a cost model. vCenter Chargeback Manager includes the following cost related elements.
  - Chargeable computing resource
  - Base rate
  - Rate factor
  - Fixed cost
  - Billing policy
  - Cost model
  - Cost template
List cost element attributes

- Chargeable computing resource
  - vCenter Chargeback Manager accounts for the following computing resources:
    - **CPU** The CPU usage is measured in GHz.
    - **Memory** The memory usage is measured in GB.
    - **Network bandwidth** The network usage (both upload and download) is measured in GB/hour.
    - **Storage** The usage is measured in GB.
    - **Disk Read and Write** The usage is measured in GB/hour.
    - **vCPU** The number of virtual CPUs in the virtual machine.
    - If the VMware Cloud Director Data Collector and vShield Manager Data Collector is installed, vCenter Chargeback Manager also accounts for the following resources:
      - **Count of Networks** The number of networks that belong to an organization or a vApp in VMware Cloud Director.
      - **NAT Service** Whether the NAT service for VMware Cloud Director network is enabled or not.
      - **DHCP Service** Whether the DHCP service for VMware Cloud Director network is enabled or not.
      - **Firewall Service** Whether the firewall service for VMware Cloud Director network is enabled or not.
      - **IPSec VPN Tunnel Count** The number of enabled IPSec VPN tunnels.
      - **External network transmit and receive** The external network usage (both upload and download) is measured in MB.
      - **External network transmit and receive rate** The external network usage (both upload and download) is measured in MB/hour.

- **Base rate**
  - Base rate is a global rate that you want to charge for a unit of chargeable computing resource used, reserved, or allocated for a specific duration.
  - The base rate duration is configurable. vCenter Chargeback Manager lets you define the base rate for an hour, day, week, month, quarter, half-year, or year for each computing resource. The precision for a base rate value is four digits.

<table>
<thead>
<tr>
<th>Chargeable Resource</th>
<th>Unit</th>
<th>Duration</th>
<th>Base Rate ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>GHz</td>
<td>Hourly</td>
<td>0.0399</td>
</tr>
<tr>
<td>Memory</td>
<td>GB</td>
<td>Hourly</td>
<td>0.0048</td>
</tr>
<tr>
<td>Network Received and Transmitted</td>
<td>GB/hour</td>
<td>Hourly</td>
<td>0.0008</td>
</tr>
<tr>
<td>Storage</td>
<td>GB</td>
<td>Hourly</td>
<td>0.0013</td>
</tr>
<tr>
<td>Disk Read and Write</td>
<td>GB/hour</td>
<td>Hourly</td>
<td>0.0008</td>
</tr>
<tr>
<td>vCPU</td>
<td>Count</td>
<td>Hourly</td>
<td>0.04</td>
</tr>
</tbody>
</table>

- **Rate factor**
  - Rate factor is the multiplication factor to be used along with the base rate to calculate the charge for a unit of chargeable computing resource used or allocated for a specified duration. Rate factors are useful when you want to charge the entities in a hierarchy differently.
- The rate factors enable you to apply a cost that is a multiple or a fraction of the base rate. The rate factor value can be between 0 and 999.99. The precision is up to two decimal places.

<table>
<thead>
<tr>
<th>Chargeable Resource</th>
<th>Base Rate ($)</th>
<th>Rate Factor</th>
<th>Total Charge ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>0.0399</td>
<td>1.1</td>
<td>0.0439</td>
</tr>
<tr>
<td>Memory</td>
<td>0.0048</td>
<td>1.1</td>
<td>0.0053</td>
</tr>
<tr>
<td>Network Received and Transmitted</td>
<td>0.0008</td>
<td>1</td>
<td>0.0008</td>
</tr>
<tr>
<td>Storage</td>
<td>0.0013</td>
<td>1</td>
<td>0.0013</td>
</tr>
<tr>
<td>Disk Read and Write</td>
<td>0.0008</td>
<td>0.75</td>
<td>0.0006</td>
</tr>
<tr>
<td>vCPU</td>
<td>0.04</td>
<td>1</td>
<td>0.04</td>
</tr>
</tbody>
</table>

- Fixed cost
  - A fixed cost is a definite cost that can be charged on an entity. Fixed costs can be recurring costs or one-time costs.
  - Recurring costs that are charged periodically for specific resources or services can be defined as fixed costs in the application. For example, the annual maintenance cost for the network or for each server. Costs that are applicable to almost all the entities and hierarchies can be defined as fixed costs. This lets you update such costs periodically and manage them centrally. It also ensures that all the entities and hierarchies are uniformly charged for common services and resources.
  - A one-time fixed cost is a charge that you want to levy once on an entity for a service provided. For example, virtual machine provisioning fees. This is a one-time cost that you want to charge for every virtual machine provisioned. If the time when the fixed cost is applied on an entity falls within the reporting duration, then the report generated on the entity or its parent includes this cost.

- Billing policy
  - A billing policy determines the cost types and the amount of chargeable computing resources units to be considered for calculating the chargeback cost. vCenter Chargeback Manager provides the various billing policies. Each billing policy only accounts for the amount of resource consumed, reserved, or allocated during the reporting duration.
  - See next bullet for descriptions.

- Cost model
  - A cost model defines base rates for the chargeable computing resources, the currency, the billing policy to be used for calculating the total cost, and other costs.
  - The other costs include cost for the guest operating system installed on the virtual machine and cost for vServices such as, High Availability, Fault Tolerance, and virtual machine creation and deletion cost. A cost model also enables you to define different billing policies for different time periods. After you define a cost model in the application, you can define rate factors and fixed costs on entities or hierarchies for the selected cost model. You can also use the cost model to generate various reports.

- Cost template
  - A cost template consists of entity-specific cost configuration details. These are rate factors for the chargeable computing resources and the fixed costs.
  - You can set these values in a cost template and use the template to configure the costs on one or more entities in the hierarchies.

Describe default billing policies and cost models
- **Fixed Cost**
  - Only the fixed costs associated with each entity in the chargeback hierarchy is considered for billing. The **actual usage of the chargeable computing resources is ignored**.

- **Actual Usage**
  - In this policy, the actual utilization of the chargeable computing resources of the virtual machines is determined. The total cost is then calculated by using the base rates set in the cost model and the actual used units of the chargeable computing resources.

- **Reservation Based**
  - This policy takes into account the capacity of a chargeable resource reserved for a virtual machine. vCenter Server allows only CPU and memory reservation. This reserved capacity of CPU and memory along with the actual utilization of other chargeable computing resources is used for calculating the total cost.

- **Allocation Based**
  - This policy takes into account the **user-defined allocation units of chargeable computing resources** for the chargeback entities. The allocated units along with the base rates defined in the cost model is used for calculating the total cost.

- **CPU Reservation**
  - CPU capacity reserved for a VM
  - Actual utilization of the chargeable computing resources

- **Memory Reservation**
  - Memory capacity reserved for a VM
  - Actual utilization of the chargeable computing resources

- **Maximum of Usage and Reservation**
  - Maximum used and reserved units of CPU and memory
  - Uses the higher amount, eg. If used is higher one day than it is used etc. Pay for at least the reserved and if you use more, you pay for what you use.
  - Actual utilization of the chargeable computing resources

- **Maximum of CPU Usage and CPU Reservation**
  - Maximum used and reserved units of CPU
  - Uses the higher amount, eg. If used is higher one day than it is used etc. Pay for at least the reserved and if you use more, you pay for what you use.
  - Actual utilization of the chargeable computing resources

- **Maximum of Memory Usage and Memory Reservation**
  - Maximum used and reserved units of memory
  - Uses the higher amount, eg. If used is higher one day than it is used etc. Pay for at least the reserved and if you use more, you pay for what you use.
  - Actual utilization of the chargeable computing resources

- **Fixed Cost and Actual Usage**
  - Fixed Costs
  - Actual utilization of the chargeable computing resources

- **Fixed Cost and Allocation**
  - Fixed Costs
  - User-defined allocations units of the chargeable computing resources

- **Fixed Cost and Reservation**
  - Fixed Costs
  - Reserved capacity of CPU and memory
  - Actual utilization of the chargeable computing resources

- **Fixed Cost and CPU Reservation**
  - Fixed Costs
  - Reserved capacity of CPU
  - Actual utilization of the chargeable computing resources
• **Fixed Cost and Memory Reservation**
  - Fixed Costs
  - Reserved capacity of memory
  - Actual utilization of the chargeable computing resources

• **Fixed Cost and Maximum of Usage and Reservation**
  - Fixed Costs
  - Maximum used and reserved units of CPU and memory
  - Calculated like the Maximum of Usage and Reservation Billing Policy.
  - Actual utilization of the chargeable computing resources

• **Fixed Cost and Maximum of CPU Usage and CPU Reservation**
  - Fixed Costs
  - Maximum used and reserved units of CPU
  - Calculated like the Maximum of Usage and Reservation Billing Policy.
  - Actual utilization of the chargeable computing resources

• **Fixed Cost and Maximum of Memory Usage and Memory Reservation**
  - Fixed Costs
  - Maximum used and reserved units of Memory
  - Calculated like the Maximum of Usage and Reservation Billing Policy.
  - Actual utilization of the chargeable computing resources

• **vCPU Count and Memory Size**
  - Number of vCPUs
  - Total amount of memory allocated
  - Actual utilization of the chargeable computing resources

• **Fixed Cost and vCPU Count and Memory Size**
  - Fixed Costs
  - Number of vCPUs
  - Total amount of memory allocated
  - Actual utilization of the chargeable computing resources

• If you install the VMware Cloud Director Data Collector, then the following billing policies are also available:
  - **VMware Cloud Director Billing Policy – Actual Usage**
    - User-defined allocations units for count of networks, enabled IPSec VPN tunnels, NAT, DHCP and firewall services.
    - Actual usage for all other computing resources
  - **VMware Cloud Director Billing Policy – Allocation Pool**
    - Actual usage for external network transmit and external network receive computing resources.
    - User-defined allocation units for all other resources.
  - **VMware Cloud Director Billing Policy – Overage Allocation Pool**
    - The overage cost for CPU based on the actual usage and for memory based on allocation.
    - Actual usage for external network transmit and external network receive computing resources.
    - User-defined allocation units for all other resources.
  - **VMware Cloud Director Billing Policy - Reservation Pool**
    - Actual usage for external network transmit and external network receive computing resources.
    - User-defined allocation units for all other resources.
  - **VMware Cloud Director Billing Policy - Pay As You Go Fixed Charging**
    - Actual usage for external network transmit and external network receive computing resources.
User-defined allocation units for all other resources.

Fixed cost on entities.

- VMware Cloud Director Billing Policy - Pay As You Go Resource Based Charging
  - User-defined allocation units for vCPUs and memory ONLY if VM is powered on.
  - Actual usage for external network transmit and external network receive computing resources.
  - User-defined allocation units for all other resources.

- VMware Cloud Director Billing Policy – Networks
  - Actual usage for external network transmit and external network receive computing resources.
  - User-defined allocation units for all other resources.

Create/Edit billing policies

- Create
  - A billing policy defines an expression that is used for identifying the amount of computing resources units to be considered for calculating the costs. Therefore, a billing policy must account for all the computing resources. The billing policy contains an expression for each resource. The expression includes an attribute value that identifies the computing resource units to be considered for cost calculation. The attribute values can be allocation, reservation, size, and usage. The attribute value reservation is available only for CPU and memory. The attribute value size is available only for memory.
  - The expression can be set to obtain the maximum of available attributes. You can also define an expression that calculates the resource units only if the virtual machine is on. Also, for storage resources, you can specify whether the expression must account for thin provisioned disks as thick provisioned. A billing policy can also account for the fixed costs and the state of the virtual machine.
    - In the Manage Cost tab, click Billing Policy.
    - Click Create.
    - Provide a name and description for the billing policy.
    - Select the Expression tab.
    - Select a resource and define an expression for it.
    - To include only an attribute, select the required attribute from the Attribute drop-down menu. The following attributes are available in vCenter Chargeback Manager.
      - Allocation: The user-defined allocation value for the resource is considered for cost calculation.
      - Usage: The actual resource usage is considered for cost calculation.
      - Reservation: The amount of resource reserved by the user is considered for cost calculation. This attribute is available only for CPU and memory.
      - Burstable Utilization: This attribute lets you account for the 95th percentile of actual utilization. This attribute is available only for the external network transmit rate and external network receive rate computing resources.
    - To obtain a maximum of a set of attribute values, click MAX and then select the required attributes from the Attribute drop-down menu.
    - To calculate the resource units only for the powered-on virtual machine, first select the VM Power On/Off option and then define the required expression for the selected resource.
    - To account for the storage linked clones, select the Distribute Linked Clones option. This option is available only if you define an expression for the storage
resource. Accounting for linked clones is only supported with vCenter Server 4.0 and later.

- To charge thin provisioned disks as thick provisioned, select the **Charge as Thick Provisioning** option. This option is available only if you define an expression for the storage resource. Charging as thick provisioning is only supported with vCenter Server 4.0 and later.

- Repeat this step for each computing resource. You can select **All other resources** from the Resource drop-down menu and define an expression for all the computing resources for which an expression has not been defined in the billing policy.

- (Optional) Select **Add/Include Fixed Cost** to consider the fixed costs during cost calculation.

  - Click **Create**.

  - Example: a billing policy that accounts for the maximum of reservation and usage for CPU and memory only for virtual machines that are powered on, maximum of allocation or usage for storage and also consider the linked clones, and allocation value for all other resources.

<table>
<thead>
<tr>
<th>Table 5-3. Sample Billing Policy Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource</strong></td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td>CPU</td>
</tr>
<tr>
<td>Memory</td>
</tr>
<tr>
<td>Storage</td>
</tr>
<tr>
<td>All other resources</td>
</tr>
</tbody>
</table>

- **Edit**
  - In the Manage Cost tab, click Billing Policy.
  - Select the required billing policy from the table and click Edit.
  - (Optional) Modify the name and description on the General tab.
  - Select the Expression tab and modify the required expressions.
  - To modify only the expression for a resource, select the resource, click Clear selected expression, and define the new expression.
  - If you want to delete a resource from the list of resources and corresponding expression, select the resource from the list and click Delete row. You can delete all the resources by clicking Delete All.
  - You can include or exclude fixed costs by selecting or deselecting the Add/Include Fixed Cost option.
  - Click **Save**.

**Manage cost models**

- vCenter Chargeback Manager provides a default cost model called Default Chargeback Cost Model. The cost models defined in the application can be viewed and managed from the Cost Models page of the **Manage Cost** tab.

- You can start using the application by creating a chargeback hierarchy and generating basic reports using the default cost model. You can modify this cost model as per your requirements. You can also create and manage multiple other cost models.

- If you have installed the VMware Cloud Director Data Collector, vCenter Chargeback Manager provides few more cost models:
VMware Cloud Director Actual Usage Cost Model
VMware Cloud Director Allocation Pool Cost Model
VMware Cloud Director Overage Allocation Pool Cost Model
VMware Cloud Director Reservation Pool
VMware Cloud Director Pay As You Go - Fixed Charging Cost Model
VMware Cloud Director Pay As You Go - Resource Based Charging Cost Model
VMware Cloud Director Networks Cost Model

- **NOTE!** These cost models do not define any base rates or fixed costs. You must modify the cost models and set the required base rates and fixed costs before using them for generating reports. If you define and include fixed costs in these cost models, ensure that you modify the corresponding billing policies and select the **Add/Include Fixed Cost** option.

- **Create:**
  - In the **Manage Cost** tab, click **Cost Models**.
  - Click **Create**.
  - Provide a name description for the cost model and set the currency type in the **General** tab.
  - In the **Billing Policy** tab, set the period for which the billing policy will be effective.
  - Default is Update from now onwards, can also be Update for the effective period.
  - Select the required policy from the **Billing Policy** list.
  - In the **Base Rates** tab, set the period for which the base rates will be effective.
  - Default is Update from now onwards, can also be Update for the effective period.
  - Set the base rate and the corresponding duration for the computing resources.
  - The duration can be Hourly, Daily, Weekly, Monthly, Quarterly, Half-yearly, or Yearly. In vCenter Chargeback Manager, a duration value of Monthly is equal to 30 days, Quarterly is equal to 91 days, Halff yearly is equal to 182 days, and Yearly is equal to 365 days.
  - (Optional) Select **Overage** to define an overage rate for the corresponding computing resource.
  - An overage rate lets you charge different rates for the allocated units and the units used beyond the allocation.
  - (Optional) If you have selected the **Overage** option, specify the rate to be charged for the allocated units of the computing resource and that for the units used beyond the allocation.
  - Set the cost for vServices in the **Other Costs** tab.
  - vServices include high availability, fault tolerance, and creation and deletion of virtual machines. You can specify whether these vServices costs are prorated and also whether the virtual machine power state needs to be considered.
  - Specify the fixed cost for various guest operating systems and the duration for charging the same.
  - Click **Create**.

- **Edit:**
  - In the **Manage Cost** tab, click **Cost Models**.
  - Select the cost model that you want to modify, and click **Edit**.
  - In the **General** tab, modify the name and description as required. (cannot change the currency).
  - In the **Billing Policy** tab, modify the billing policy and the effective time period.
  - (Optional) To fetch the current billing policies set in the cost model, select the **Update for the effective period** option, specify the required time period, and click **Get**.
  - To add another billing policy, set the effective time period, select the billing policy, and then click **Set**.
  - In the **Base Rates** tab, modify the base rates for the chargeable computing resources, the duration, and the effective time period.
(Optional) To fetch the historical base rate values, select the **Update for the effective period** option, specify the required time period, and click **Get**.

- Click the **Show** link next to **Historical values**.
- To add another set of base rates, set the effective time period, set the base rates and corresponding duration, and then click **Set**.
- Optional) To create or modify the overage rate for a computing resource, select **Overage** and provide the rate to be charged for the allocated units of the computing resource and that for the units used beyond the allocation.
- Modify the fixed cost for vServices and guest operating systems in the **Other Costs** tab.
- Click **Save** to save all your changes.

**Edit cost configuration of an entity**

- The entity-specific cost configuration details can be set from the **Configure Cost** tab.
- The cost configuration is applied on an entity for the specified cost model and time period. These cost configuration details will be considered when a report is generated on the entity using the specified cost model.
  - In the **Configure Cost** tab, click **Edit Entity Cost**.
  - Select the required hierarchy from the hierarchies included in the drop-down menu.
  - Expand the hierarchy and select the entity for which you want to configure the costs.
  - Select the cost model for which you want to specify entity-specific cost configuration details on the selected chargeback entity.
  - Specify the duration for which the cost configuration will be effective.
  - Default is Update from now onwards, can also be Update for the effective period.
  - (Optional) Select a cost template from the **Apply a Cost Template** drop-down menu.
  - The rate factors and fixed costs defined in the cost template are populated in the corresponding fields on the screen.
  - Enter the rate factors for the computing resources in the **Rate Factors** tab and click **Update Rate Factors**.
  - In the **Fixed Costs** tab, select the required fixed cost from the **Apply a Fixed Cost** drop-down menu and click Add to the list.
  - (Optional) Check the **Propagate** option corresponding to an added fixed cost, if the cost has to be applied to the child entities of the entity on which the cost template is applied. You can also specify whether the cost must be applied to all descendants or only to the immediate child entities. You can also select a filter to ensure that the cost is applied to specific entity types. When a cost report is generated, the fixed costs on the child entities are rolled-up to the parent entity.
  - Click **Update Fixed Costs** to set the added fixed costs on the entity.
  - Select the **Enable/Disable Billing** tab to configure the billing status.
    - **Enable**: This option enables billing on the entity for the specified time period. You can use this option if billing was earlier disabled on the entity for the specified time period.
    - **Disable**: Select this option if you want to disable billing on the entity for the specified time period.
  - Click **Update Billing**.

**Manage physical infrastructure costing**

- In vCenter Chargeback Manager you can define rate factors also at the host and cluster level and the datastore level. You can do this from the Edit Infrastructure Cost page of the **Configure Cost** tab.
- When you create a report Chargeback first checks whether any entity-specific cost configuration is set on the entity/entities for the selected cost model, and uses that to create the report.
• If there are no entity-specific cost configuration details for the selected cost model, Chargeback checks whether any rate factors are set at the host and cluster level and the datastore level for the virtual machines on which reports are being generated.

• vCenter Chargeback Manager lets you set rate factors at the hosts and clusters level. You can charge all the virtual machines in a cluster or on an ESXi host uniformly by setting rate factors at the hosts and clusters level.
  - In the Configure Cost tab, click Edit Infrastructure Cost.
  - Select Hosts & Clusters from the drop-down menu.
  - Expand the Hosts & Clusters folder by clicking the plus sign.
  - Click the plus sign next to Clusters to view the clusters defined in the vCenter Server instances added to vCenter Chargeback Manager.
  - Select the cluster or an individual ESXi host for which you want to define the rate factors.
  - Select a cost model from the drop-down menu.
  - Specify the duration for which the rate factors will be effective.
  - (Optional) Click Show next to Historical values to view the historical base rate and rate factor values of all the computing resources for the specified time period.
  - Specify the rate factors for the required computing resources and click Update Rate Factors.
  - Click OK in the information dialog box.
  - vCenter Chargeback Manager lets you define rate factors for individual datastores. You can also create tiers, add datastores to the tiers, and set rate factors at the tier level.
  - Set the same rate factor for multiple datastores or VM storage profile.

• Create a tier:
  - In the Configure Cost tab, click Edit Infrastructure Cost.
  - Select DataStores from the drop-down menu.
  - Click Create Tier at the bottom of the left panel.
  - Provide a name for the newly created tier and click outside the editable tier name field.

• Modify a name of a tier:
  - In the Configure Cost tab, click Edit Infrastructure Cost.
  - Select DataStores from the drop-down menu.
  - Right-click the tier folder whose name you want to modify and select Edit label.
  - Enter the new name for the tier folder and click outside the editable tier name field.

• Add Datastore to Tier:
  - In the Configure Cost tab, click Edit Infrastructure Cost.
  - Select DataStores from the drop-down menu.
  - Expand the ungrouped folder by clicking the plus sign (+) next to it.
  - Right-click the datastore that you want to add to a tier and select Move this Datastore to another tier.
  - Right-click the tier folder to which you want to add this datastore and select Put the Datastore/Storage Profile in this tier.

• Set Rate Factor on a Tier, Datastore or Storage Profile:
  - In the Configure Cost tab, click Edit Infrastructure Cost.
  - Select DataStores from the drop-down menu.
  - Select the tier for which you want to configure the rate factor.
  - Select the cost model from the drop-down menu.
  - Select the duration for which the rate factor will be effective.
  - Specify the rate factor and click Set.
  - Click OK on the information dialog box.
  - Move a Datastore or Storage Profile to another Tier:
In the **Configure Cost** tab, click **Edit Infrastructure Cost**.
- Select **DataStores** from the drop-down menu.
- Expand the tier folder containing the datastore or storage profile that you want to move.
- Right-click the datastore or storage profile that you want to move to another tier and select **Move this Datastore to another tier**.
- Right-click the tier folder to which you want to move this datastore and select **Put the Datastore/Storage Profile in this tier**.

**Manage pricing matrix for virtual machine**

- vCenter Chargeback Manager provides functionality to charge a fixed cost for virtual machines in a hierarchy based on the vCPU count and memory.
- You can define one or more pricing matrices for the virtual machines in your hierarchies, such that the virtual machines are charged a fixed cost based on the vCPU count and memory bundle. This cost is applied only for the duration when a virtual machine is powered on and is not pro-rated.
- A price matrix is associated with a cost model and can contain multiple cost entries for different vCPU count and memory bundles. You can also define a criterion to specify the hierarchies for which the price matrix is applicable. You can define multiple pricing matrices with different hierarchy selection criteria for each cost model defined in vCenter Chargeback Manager. Each hierarchy selection criteria for a selected cost model must be unique. Also, each entry in the pricing matrix must be unique.
- vCenter Chargeback Manager applies the fixed cost defined in the pricing matrix on the virtual machines in a hierarchy by running a job that periodically checks for new and updated hierarchies, and hierarchy selection criteria and the corresponding pricing matrix. Based on the hierarchy and entity selection criteria, the application uses the corresponding pricing matrix to apply the fixed cost on the virtual machines in the hierarchies that match the specified criterion as follows:
  - vCenter Chargeback Manager checks for the hierarchy selection criteria and the corresponding pricing matrices defined in it.
  - vCenter Chargeback Manager uses the pricing matrix corresponding to the first matching criterion for each hierarchy.
  - vCenter Chargeback Manager first searches for a row in the pricing matrix that has the same vCPU count as in the virtual machine.
  - If such a row is not found, then vCenter Chargeback Manager selects the row with the next higher value of vCPU count than in the virtual machine.
  - For the selected vCPU count, vCenter Chargeback Manager checks for a memory value equal to or higher than the memory in the virtual machine.
  - If a row with the vCPU count or memory value equal to or higher than the vCPU count or memory in the virtual machine is not found, then vCenter Chargeback Manager uses the default cost configured in the matrix.

**NOTE** For hierarchies imported from vCloud Director, the vCPU count and memory allocation values synchronized from the vCloud Director database is considered for applying the fixed cost. For hierarchies created in vCenter Chargeback Manager, the vCPU count and memory utilization values synchronized from the vCenter Server database is used for applying the fixed cost. If a virtual machine configuration is changed, then the corresponding change in the fixed cost is applicable from the time the configuration change is effected. If the fixed cost in the pricing matrix is changed, then the change is effected from the next run of the job.
Objective 3.4 – Troubleshoot Common vCenter Chargeback Issues

Knowledge

- **Collect logs**
  - You must run the troubleshooting utility to collect the required logs for troubleshooting the application.
  - Run the troubleshooting utility by running the following command from the command prompt.
    - `cd Installation_Directory\vCenter-CB-Tools\troubleshooting\bin\vCenterCB-support.bat`
    - You can also run this utility by selecting Collect vCenter Chargeback Manager Logs from the Start > Programs > VMware > VMware vCenter Chargeback > vCenter Chargeback Manager Tools menu.
  - Provide the folder name and directory path where the generated logs have to be stored when prompted.
    - You can choose to collect the system event logs.
    - The Application log and System log is collected.
    - Enter the number of stand-alone data collector instances (not embedded) installed on the same machine.
    - If you have any standalone data collector instance running, you must provide the path of each such data collector installation.

- **Run troubleshooting utility**
  - See first bullet.

- **Explain impact of vSphere statistics levels on report generation**
  - A vCenter Chargeback Manager report displays the disk read and write information and the corresponding cost if the disk read and disk write computing resources are selected when the report is generated.
  - A vCenter Chargeback Manager report displays the memory usage and cost information if the memory computing resource is selected when the report is generated.
  - A vCenter Chargeback Manager report displays the network bandwidth usage and cost information if the network transmitted and network received computing resources are selected when the report is generated.
    - For all these report statistics you will need to:
      - For vCenter Server 2.5 Update 3, vCenter Server 2.5 Update 4, and vCenter Server shipped with vSphere 4.0 and later, the statistics collection level must be set to 3 or above for the average disk read and write counters to be available.

- **Explain impact of local firewall settings on vCenter Chargeback services**
  - Although you have provided the correct URL, you are unable to access the application.
    - The application-related services are not started or not running.
    - Windows Firewall is enabled on the machine on which vCenter Chargeback Manager and the load balancer is installed and running.
      - If Windows Firewall is enabled, ensure that port exceptions are added for the HTTP, load balancer, and HTTPS ports that are configured for vCenter Chargeback Manager during the installation. Ensure that you set an inbound rule for these port. That is, allow access to the machine through these ports.

- **Given a service failure, determine root cause**
  - Best way to find out what is not working is using the Health Dashboard.
  - I recommend reading over Troubleshooting Issues chapter in Best Practices and Troubleshooting Guide, just to get an overview of what could potentially be wrong.
Objective 4.1 – Create and Administer vCloud External and Organization Networks

Knowledge
- **Identify and differentiate the types of vCloud Organization networks**
  - **External network:**
    - Service Provider external network, either with public IP addresses or NAT'ed internally.
  - **External direct organization network:** vApps are connected directly to the external network.
    - Accessible by multiple organizations. Virtual machines belonging to different organizations can connect to and see traffic on this network. This network provides direct layer 2 connectivity to machines outside of the organization. Machines outside of this organization can connect to machines within the organization directly.
  - **External NAT-routed organization network:** Network behind a vShield Edge appliance which controls the NAT, DHCP, VPN and other vServices.
    - Accessible only by this organization. Only virtual machines within this organization can connect to this network. This network also provides controlled access to an external network. System administrators and organization administrators can configure network address translation (NAT) and firewall settings to make specific virtual machines accessible from the external network.
  - **Internal Organization network:** Network which different vApps (with different VM's) can connect to internally. (Do not get this mixed up with vApp networks). DHCP service available.
    - Accessible only by this organization. Only virtual machines within this organization can connect to and see traffic on this network. This network provides an organization with an isolated, private network that multiple vApps can connect to. This network provides no connectivity to machines outside this organization. Machines outside of this organization have no connectivity to machines within the organization.
- Create/Modify/Delete an external network
  
  **Create**
  
  - Add an external network to register vSphere network resources for vCloud Director to use. You can create organization networks that connect to an external network. Prerequisites: A vSphere port group is available. If the port group uses VLAN, it can use only a single VLAN. Port groups with VLAN trunking are not supported.
  
  **Procedure**
  
  1. Click the Manage & Monitor tab and click External Networks in the left pane.
  2. Click the Add Network button.
  3. Select a vCenter Server and a vSphere port group and click Next.
  4. Type the network settings and click Next.
  5. Type a name and optional description for the network and click Next.
  6. Review the network settings and click Finish.

  **Modify**
  
  - Name/Description
    
    1. Click the Manage & Monitor tab and click External Networks in the left pane.
    2. Right-click the external network name and select Properties.
    3. On the Name and Description tab, type a new name and description and click OK.
  
  **Specification**
  
  1. Click the Manage & Monitor tab and click External Networks in the left pane.
  2. Right-click the external network name and select Properties.
  3. On the Network Specification tab, modify the network settings and click OK.
    
    - You cannot modify the network mask or default gateway. If you need an external network with a different netmask or gateway, create one.

  - Add IP Addresses to IP Pool
Click the Manage & Monitor tab and click External Networks in the left pane.
Right-click the external network name and select Properties.
On the Network Specification tab, type an IP address or a range of IP addresses in the text box and click Add.
Click OK.

- Delete
  - Before you can delete an external network, you must delete all of the organization networks that rely on it.
  - Click the Manage & Monitor tab and click External Networks in the left pane.
  - Right-click the external network name and select Delete Network.

- Create/Modify/Delete an external direct organization network
  - Create
    - You can create an external direct organization network that multiple organizations can access. You typically use the external network to connect to the Internet. The organization connects directly to this network.
      - Procedure
        - Click the Manage & Monitor tab and click Organization Networks in the left pane.
        - Click Add Network.
          - The Create Organization Network wizard starts.
        - Select an organization and click Next.
        - Select the type of setup and network type and click Next.
          - You can create an external direct organization network using either method.
            - Typical: Select the external network check box and select direct connection from the drop-down menu.
            - Advanced: Select External organization network - direct connection.
        - Select an external network and click Next.
          - You can deselect the Only use networks accessible by this organization check box to view external networks that are not currently available to the organization through its organization vDCs. When you deselect this check box, you can choose an arbitrary network and later create an organization vDC that can access the network.
        - Type a name and optional description and click Next.
        - Review the settings for the organization network.
  - Modify
    - Modify name and description
      - Click the Manage & Monitor tab and click Organization Networks in the left pane.
      - Right-click the organization network name and select Properties.
      - On the Name and Description tab, type a new name and optional description and click OK.
    - Modify DNS settings:
      - Click the Manage & Monitor tab and click Organization Networks in the left pane.
      - Right-click the organization network name and select Properties.
      - On the Network Specification tab, type the new DNS information and click OK.
  - Delete
    - You can delete an organization network to remove it from the organization.
Prerequisites: Verify that no virtual machines are connected to the organization network.

Procedure
- Click the Manage & Monitor tab and click Organization Networks in the left pane.
- Right-click the organization network name and select Delete.

Create/Modify/Delete an external NAT-routed organization network
- Create
  - You can create an external NAT-routed organization network that only this organization can access. An external NAT-routed organization network provides NAT connectivity to machines outside this organization for better control on what is accessible.
  - Prereq: External network and a network pool.
  - Procedure
    - Click the Manage & Monitor tab and click Organization Networks in the left pane.
    - Click Add Network.
    - The Create Organization Network wizard starts.
    - Select an organization and click Next.
    - Select the type of setup and network type and click Next.
    - You can create an external routed organization network using either method.
      - Typical: Select the external network check box and select routed connection from the drop-down menu.
      - Advanced: Select External organization network - NAT-routed connection.
    - Select an external network and network pool and click Next.
    - You can deselect the Only use networks accessible by this organization check box to view external networks and network pools that are not currently available to the organization through its organization vDCs. When you deselect this check box, you can choose an arbitrary network or network pool and later create an organization vDC that can access the network or network pool
    - Use the default network settings or type your own and click Next.
    - (Optional) Type an external IP address for the network to use for NAT services, click Add, and click Next.
      - This setting is available only in advanced setup. You can add more than one external IP address.
    - Type a name and optional description and click Next.
    - Review the settings for the organization network.
    - Click Finish to accept the settings and create the organization network, or click Back to modify the settings.
- Modify
  - View IP Use:
    - Click the Manage & Monitor tab and click Organization Networks in the left pane.
    - Right-click the organization network name and select IP Allocations.
  - Add IP Addresses to IP Pool:
    - Click the Manage & Monitor tab and click Organization Networks in the left pane.
    - Right-click the organization network name and select Properties.
- On the Network Specification tab, type an IP address or a range of IP addresses in the text box and click Add.
- Click OK.
- **Modify name and description**
  - Click the Manage & Monitor tab and click Organization Networks in the left pane.
  - Right-click the organization network name and select Properties.
  - On the Name and Description tab, type a new name and optional description and click OK.
- **Modify DNS settings:**
  - Click the Manage & Monitor tab and click Organization Networks in the left pane.
  - Right-click the organization network name and select Properties.
  - On the Network Specification tab, type the new DNS information and click OK.

**Delete**
- You can delete an organization network to remove it from the organization.
- **Prerequisites:** Verify that no virtual machines are connected to the organization network.
  - **Procedure**
    - Click the Manage & Monitor tab and click Organization Networks in the left pane.
    - Right-click the organization network name and select Delete.

**Create/Modify/Delete an internal organization network**
- **Create**
  - You can create an internal organization network that only this organization can access. The new network provides the organization with an internal network to which multiple vApps can connect.
  - **Prereq:** Network pool.
  - **Procedure**
    - Click the Manage & Monitor tab and click Organization Networks in the left pane.
    - Click Add Network.
    - Select an organization and click Next.
    - Select the type of setup and network type and click Next.
      - You can create an internal organization network using either method.
        - Typical: Select the internal network check box.
        - Advanced: Select Internal organization network.
    - Select a network pool and click Next.
      - You can deselect the Only use networks accessible by this organization check box to view network pools that are not currently available to the organization through its organization vDCs. When you deselect this check box, you can choose an arbitrary network pool and later create an organization vDC that can access it.
      - Use the default network settings or type your own and click Next.
      - Type a name and optional description and click Next.
      - Review the settings for the organization network.
      - Click Finish to accept the settings and create the organization network, or click Back to modify the settings.
Modify
- Same as the Modify bullet for External routed networks.

Delete
- You can delete an organization network to remove it from the organization.
- Prerequisites: Verify that no virtual machines are connected to the organization network.
  - Procedure
    - Click the Manage & Monitor tab and click Organization Networks in the left pane.
    - Right-click the organization network name and select Delete.

- **Explain the relationship between external networks and vSphere port groups**
  - How virtual networking in your virtual infrastructure is set up is critical to ensuring the security of VMware vCloud Director in general and isolation of individual tenants in particular. VMware vCloud Director leverages the virtual switches and portgroups set up in the virtual infrastructure when creating Organization Networks (via External Networks and Network Pools). The different types of networks and pools at the VMware vCloudDirector layer provide different types of isolation:
    - An External Network provides no isolation between virtual machines, vApps, or organizations by design. It is “external” in order to connect to systems outside the cloud. Connecting directly to that network doesn’t give the protection of the other types of networks.
    - A VLAN-backed Network Pool provides isolation using VLANs across a vNetwork Distributed Switch. A VMware vCloud Director network isolation–backed Network Pool provides isolation by encapsulating Layer 2 packets in other Layer 2 packets (MAC-in-MAC) in the ESX or ESXi kernel, allowing the kernel when encapsulating packets to direct them to the correct guest virtual machines connected to the networks created out of this sort of pool.
    - A vSphere portgroup-backed Network Pool does not enforce isolation directly, but is dependent on the portgroups not being connected to the same vSwitches and physical networks. Isolation can be provided at the physical network with VLANs or other mechanisms. Further discussion of this network type is out of the scope for this document.
  - None of the provider-level network types provide confidentiality if packets are intercepted at the physical network.

- **Explain the purpose and use cases for external networks**
  - An external network provides connectivity “outside” an organization through an existing, preconfigure vSphere network port group. The vSphere port groups can be created using standard vSwitch port groups, vNetwork Distributed Switch port groups, or the Cisco Nexus 1000V.
  - In a public vCloud, these preconfigured port groups will provide access through the Internet to customer networks, typically using VPN or MPLS terminations.
  - When creating an external network, make sure to have sufficient vSphere port groups created and made available for virtual machine access in the vCloud.

- **Explain the relationship between organization networks and vShield Edge**
  - External direct organization network:
    - No vShield Edge appliance.
  - External NAT-routed organization network:
    - As this is a routed network a vShield Edge Appliance is created.
    - vShield Edge is leveraged for firewalling and NAT to keep traffic separated from other organizations on the same external provider network
  - Internal Organization network:
    - As this is a routed network a vShield Edge Appliance is created.
• **Explain best practices related to organization networks**
  o Public vCloud
    • Create two different organization networks for each organization, one external organization network and one private internal organization network. You can do this as one step in the vCloud Director UI wizard by selecting the default (recommended) option when creating a new organization network. When naming an organization network, it is a best practice to start with the organization name and a hyphen, for example, ACME-Internet.
  o Private vCloud
    • At least one organization external network is required to connect vApps created within the organization to other vApps and/or the networking layers beyond the Private vCloud.
    • To accomplish this, create an external network in the Cloud Resources section (under Manage & Monitor of the System Administration section of the vCloud Director UI). In the wizard, be sure to select a direct connection. This external network maps to an existing vSphere network for virtual machine use as defined in the External Networks section (above).

• **Given organization requirements, determine the appropriate organization network type.**
  o Really depends on the service the organization will be running.

**Objective 4.2 – Configure and Administer vCloud Network Pools**

**Knowledge**

• **Describe the concept of a Network Pool**
  o A Network Pool is a set of pre-allocated networks that vCloud Director can draw upon as needed to create private networks and NAT-routed networks.
  o A network pool is a group of undifferentiated networks that is available for use within an organization vDC. A network pool is backed by vSphere network resources such as VLAN IDs, port groups, or Cloud isolated networks. vCloud Director uses network pools to create NAT-routed and internal organization networks and all vApp networks. Network traffic on each network in a pool is isolated at layer 2 from all other networks. Each organization vDC in vCloud Director can have one network pool. Multiple organization vDCs can share the same network pool. The network pool for an organization vDC provides the networks created to satisfy the network quota for an organization vDC. Only system administrators can create and manage network pools.
  o vCloud Director creates a private network as needed from a pool of networks to facilitate VM-to-VM communication and NAT-routed networks. vCloud Director supports one of three methods to back network pools:
    • vSphere port group. vCloud Director uses one of many existing, preconfigured vSphere networks. The networks themselves can have VLAN tagging for additional security.
    • VLAN. vCloud Director automatically uses VLAN tagging from a range provided to segment networks to create internal networks (organization and vApp networks) as needed. This assumes that vCloud Director and all the managed hosts have access to the VLANs on the physical network.
    • vCloud Director Network Isolation. vCloud Director automatically creates internal networks using MAC-in-MAC encapsulation.

• **Create/Delete a Network Pool**
  o vSphere port group:
    • You can add a network pool that is backed by port groups to register vSphere port groups for vCloud Director to use. Unlike other types of network pools, a network pool that is backed by port groups does not require a vSphere distributed switch.
- **CAUTION** The port groups must be isolated from all other port groups at the layer 2 level. The port groups must be physically isolated or must be isolated by using VLAN tags. Failure to properly isolate the port groups can cause a disruption on the network.

- Prereq: The port groups must be available on each ESX/ESXi host in the cluster, and each port group must use only a single VLAN.
  - Click the Manage & Monitor tab and click Network Pools in the left pane.
  - Click Add Network Pool.
  - Select vSphere Port Group-backed and click Next.
  - Select a vCenter Server and click Next.
    - Select one or more port groups, click Add, and click Next.
    - You can create one network for each port group.
  - Type a name and optional description for the network and click Next.
  - Review the network pool settings and click Finish.

- **VLAN backed:**
  - You can add a VLAN-backed network pool to register vSphere VLAN IDs for vCloud Director to use. A VLAN-backed network pool provides the best security, scalability, and performance for organization networks.
  - Prereq: Verify that a range of VLAN IDs and a vSphere distributed switch are available in vSphere. The VLAN IDs must be valid IDs that are configured in the physical switch to which the ESX/ESXi servers are connected.
    - Click the Manage & Monitor tab and click Network Pools in the left pane.
    - Click Add Network Pool.
    - Select VLAN-backed and click Next.
    - Type a range of VLAN IDs and click Add.
      - You can create one network for each VLAN ID.
    - Select a vCenter Server and vSphere distributed switch and click Next.
    - Type a name and optional description for the network and click Next.
    - Review the network pool settings and click Finish.

- **vCloud Director Network Isolation:**
  - You can create a network pool that is backed by cloud isolated networks. A cloud isolated network spans hosts, provides traffic isolation from other networks, and is the best source for vApp networks. An isolation-backed network pool does not require preexisting port groups in vSphere.
  - Prereq: Verify that a vSphere distributed switch is available.
    - Click the Manage & Monitor tab and click Network Pools in the left pane.
    - Click Add Network Pool.
    - Select VCD Network Isolation-backed and click Next.
    - Type the number of networks to create from the network pool.
    - (Optional) Type a VLAN ID.
    - Select a vCenter Server and a vSphere distributed switch and click Next.
    - Type a name and optional description for the network and click Next.
    - Review the network pool settings and click Finish.

- **Deletion of Network Pools** work the same for all types:
  - Prerequisites: Verify that the following conditions exist:
    - No organization vDC is associated with the network pool.
    - No vApps use the network pool
    - No NAT-routed or internal organization networks use the network pool.
  - Procedure
    - Click the Manage & Monitor tab and click Network Pools in the left pane.
    - Right-click the network pool name and select Delete.
    - Click Yes.
• **Expand a Network Pool**
  - **Add a Port Group to a Network Pool**
    - You can add port groups to a network pool that is backed by port groups.
    - **Prerequisites**
      - Verify that you have a network pool that is backed by a port group
      - Verify that you have an available port group in vSphere
    - **Procedure**
      - Click the Manage & Monitor tab and click Network Pools in the left pane.
      - Right-click the network pool name and select Properties.
      - On the Network Pool Settings tab, select a port group, click Add, and click OK.
  - **Add Cloud Isolated Networks to a Network Pool**
    - You can add Cloud isolated networks to a VCD network isolation-backed network pool.
    - **Prerequisites**
      - A VCD network isolation-backed network pool
    - **Procedure**
      - Click the Manage & Monitor tab and click Network Pools in the left pane.
      - Right-click the network pool name and select Properties.
      - On the Network Pool Settings tab, type the number of VCD isolated networks and click OK.
  - **Add VLAN IDs to a Network Pool**
    - You can add VLAN IDs to a network pool that is backed by a VLAN.
    - **Prerequisites:** Verify that your system includes the following items:
      - A network pool that is backed by a VLAN
      - Available VLAN IDs in vSphere
    - **Procedure**
      - Click the Manage & Monitor tab and click Network Pools in the left pane.
      - Right-click the network pool name and select Properties.
      - On the Network Pool Settings tab, type a VLAN ID range and click Add.
      - Select a vSphere distributed switch and click OK.

• **Determine appropriate backing for a given Network Pool**
  - **When To Use VLAN-Backed Network Pools**
    - Networks created from VLAN-backed Network Pools are slightly faster than those created from VMware vCloud Director Network Isolation–backed Network Pools, but they require one VLAN per Organization Network created from the pool. For that reason, there may be concerns regarding the use of VLAN-backed Network Pools in an environment where the provider is trying to maximize the number of hosts, organizations, and vApps in the vCenter cluster. In one where the number of Organization and vApp networks is not expected to be large, VLAN-backed Network Pools may be a perfectly appropriate choice. VLANs may also be consumed by the underlying computing and networking fabric, so it is important to pay attention to the total number of VLANs available per cluster.
  - **When To Use VMware vCloud Director Network Isolation–Backed Network Pools**
    - While networks created from VMware vCloud Director Network Isolation–backed Network Pools are slightly slower than those created from VLAN-backed Network Pools, they do not require the use of any VLANs. This is an advantage when there are many Organizations, hosts, and vApps assigned to a vCenter cluster and the available number of VLANs is of concern. These types of Network Pools are also useful when it is not feasible to assign large numbers of VLANs (or a trunk port) to the hosts in the cluster. This type of Network Pool is easier to manage, as you don’t need to keep track of large numbers of VLANs and their usage across computing
and networking infrastructure. It is thus also easier to lock down the propagation of the optional VLAN to only the hosts that are part of the vNetwork Distributed Switch.

- **When To Use Port Group Backed Network Pools**
  - When you don’t want to use the other two for some reason. No free VLAN ranges, Static environments, Small environment, no physical vCenters to use VDS (not fun when host running vCenter dies), etc.

- **Configure Network Pool properties**
  - Modify a Network Pool Name and Description
    - As your vCloud Director installation grows, you might want to assign a more descriptive name or description to an existing network pool.
    - Procedure
      - Click the Manage & Monitor tab and then click Network Pools in the left pane.
      - Right-click the network pool name and select Properties.
      - On the General tab, type a new name or description and click OK.

- **Add a Port Group to a Network Pool**
  - You can add port groups to a network pool that is backed by port groups.
  - Prerequisites
    - Verify that you have a network pool that is backed by a port group
    - Verify that you have an available port group in vSphere
  - Procedure
    - Click the Manage & Monitor tab and click Network Pools in the left pane.
    - Right-click the network pool name and select Properties.
    - On the Network Pool Settings tab, select a port group, click Add, and click OK.

### Objective 4.3 – Configure and Administer vApp Networks

**Knowledge**

- **Identify vApp Network types**
  - The virtual machines in a vApp can connect to vApp networks (isolated or routed) and organization network (direct or fenced).
  - **Isolated:**
    - A vApp network can be isolated by selecting None in the Connection drop-down menu. An isolated vApp network is totally contained within the vApp.
  - **Routed:**
    - You can also route a vApp network to an organization network to provide connectivity to virtual machines outside of the vApp. For routed vApp networks, you can configure network services, such as a firewall and static routing.
  - **Direct:**
    - Connected directly to a Organization network.
  - **Fenced:**
    - Takes a direct network and turns it into a Routed network. VMs still have Organization IPs but a vShield Edge device is place in between the VMs and the Organization network.
  - Nice blog-post by Jake Robinson at geekafterfive.com about vApp networks is a recommended read.

- **Explain the purpose and use cases for vApp networks**
  - A network visible within a vApp. It can be connected to other vApp networks within an organization and use a direct or routed connection, or it can be an internal network visible only to virtual machines within the vApp.
A vApp network is contained within a vApp and allows virtual machines in the vApp to communicate with each other. You can connect a vApp network to an organization network to allow the vApp to communicate with other vApps in the organization and outside of the organization, if the organization network is connected to an external network.

- **Explain the relationship between vApp networks and vShield Edge devices**
  - Isolated
    - Will create a vShield Edge device to handle DHCP services.
  - Routed:
    - Will use a vShield Edge device to handle routing.
  - Direct-Fenced:
    - Will use a vShield Edge device to "fence" IPs from other VM's

- **Create/Modify/Delete a direct vApp network**
  - Create
    - Add an organization network to a vApp to make the network available to virtual machines in the vApp.
      - Click My Cloud.
      - In the left pane, click vApps, right-click, and select Open.
      - On the Networking tab, select the Show networking details check box.
      - Click the Add Network button.
      - Select Organization Network and click Next.
      - Select an organization network and click Finish.
      - vCloud Director adds the organization network and displays it in the network list.
      - (Optional) Select the Fence vApp check box.
      - This changes the connection from Direct to Fenced for all organization networks in the vApp. Fencing allows identical virtual machines in different vApps to be powered on without conflict by isolating the MAC and IP addresses of the virtual machines.
      - Click Apply.
  - Modify
    - Reset your vApp Network
      - If the network services, such as DHCP settings, firewall settings, and so on, that are associated with a vApp network are not working as expected, an organization administrator can reset the network. Network services are not available during the reset.
      - Click My Cloud.
      - In the left pane, click vApps.
      - Select a vApp, right-click, and select Open.
      - On the Networking tab, select the Show networking details check box.
      - Select a vApp network, right-click, and select Reset Network.
      - Click Yes.
  - Modify Network Properties
    - Select Administration.
    - Select Cloud Resources > Networks.
    - Select a network, right-click, and select Properties.
      - You can modify the name, description, and portions of the network specification.
      - Modify the relevant properties and click OK.
      - Click Apply.
  - Configure IP Address Persistence
• By default, when you stop a running vApp or power off a virtual machine, vCloud Director releases any IP and MAC addresses the virtual machines were using. You can configure a vApp to retain the network addresses of its virtual machines until the vApp, VM, or network is deleted. Static routing relies on the IP addresses of the virtual machines and virtual routers in a vApp. For vApps that use static routing, enable IP persistence to make sure that static routes to and from the vApp remain valid.
  • Click My Cloud.
  • In the left pane, select vApps.
  • Select a vApp, right-click, and select Open.
  • On the Networking tab, select the Always use assigned IP addresses... check box and click Apply.

  ○ Delete
  • Prerequisites
    ▪ The vApp is stopped and no virtual machines in the vApp are connected to the network.
  • Procedure
    ▪ Click My Cloud.
    ▪ In the left pane, select vApps.
    ▪ Select a vApp, right-click, and select Open.
    ▪ On the Networking tab, select the Show networking details check box.
    ▪ Right-click a network in the list and select Delete.
    ▪ Click Apply.

• Create/Modify/Delete a NAT-routed vApp network
  ○ Create
    • Click My Cloud.
    • In the left pane, click vApps, right-click, and select Open.
    • On the Networking tab, select the Show networking details check box.
    • Click the Add Network button.
    • Select vApp Network and click Next.
    • Type the network specifications and click Next.
    • Type a network name and optional description and click Next.
    • Review your vApp network settings and click Finish.
      ▪ vCloud Director creates an isolated vApp network and displays it in the network list.
      ▪ (Optional) Select an organization network in the Connection drop-down menu.
        ▪ This routes the vApp network to the organization network.
  ○ Modify
    • Same as direct vApp network.
  ○ Delete
    • Same as direct vApp network.

• Create/Modify/Delete an internal vApp network
  ○ Create
    • Click My Cloud.
    • In the left pane, click vApps, right-click, and select Open.
    • On the Networking tab, select the Show networking details check box.
    • Click the Add Network button.
    • Select vApp Network and click Next.
    • Type the network specifications and click Next.
    • Type a network name and optional description and click Next.
    • Review your vApp network settings and click Finish.
- vCloud Director creates an isolated vApp network and displays it in the network list.
  - Modify
    - Same as direct vApp network.
  - Delete
    - Same as direct vApp network.
- **Troubleshoot vApp networks using the visual mapping tool**
  - You can access and display the networks in a vApp.
    - Procedure
      - Click My Cloud.
      - In the left pane, click vApps.
      - Select a vApp, right-click, and select Open.
      - Click on the Networking tab.
      - Select the Show networking details to display details about each network.
  - A vApp diagram provides a **graphical view** of the virtual machines and networks in a vApp.
    - Procedure
      - Click My Cloud.
      - On the vApps page, select a vApp, right-click, and select Open.
      - Click the vApp Diagram tab.
      - The vApp diagram is displayed.

**Objective 4.4 – Administer vCloud Network Services**

**Knowledge**
- **Identify available vShield Edge network services**
  - DHCP
  - Firewall
  - NAT
  - VPN

<table>
<thead>
<tr>
<th>Network Type</th>
<th>DHCP</th>
<th>Firewall</th>
<th>NAT</th>
<th>VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>External organization network - direct connection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External organization network - NAT-routed connection</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Internal organization network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Configure DHCP/NAT/VPN services**
  - DHCP
    - You can configure certain organization networks to provide DHCP services to virtual machines in the organization.
    - When you enable DHCP for an organization network, connect a NIC on virtual machine in the organization to that network, and select DHCP as the IP mode for that NIC, vCloud Director assigns a DHCP IP address to the virtual machine when you power it on.
    - Both system administrators and organization administrators can configure DHCP.
      - Click the Manage & Monitor tab and click Organization Networks in the left pane.
      - Right-click the organization network name and select Configure Services.
      - Click the DHCP tab and select Enable DHCP.
      - Type a range of IP addresses or use the default range.
- vCloud Director uses these addresses to satisfy DHCP requests. The range of DHCP IP addresses cannot overlap with the static IP pool for the organization network.
  - Set the default lease time and maximum lease time or use the default values.
  - Click OK.
- **NAT: First add IP then NAT mapping (Port Forwarding or IP translation)**
  - **Add External IP Addresses to an Organization Network**
    - Before you can configure NAT mapping for an organization network, you must add one or more external IP addresses.
    - Only a system administrator can add external IP addresses to an organization network.
    - Prerequisites
      - An external NAT-routed organization network.
    - Procedure
      - Click the Manage & Monitor tab and click Organization Networks in the left pane.
      - Right-click the organization network name and select Configure Services.
      - Click the NAT - External IPs tab.
      - Type an IP address and click Add.
        - The IP address must be routable on the external network and unique across internal networks.
      - Click OK.
  - **Configure Port Forwarding for an Organization Network**
    - You can configure certain organization networks to provide port forwarding. Port forwarding provides external access to services running on virtual machines on the organization network.
    - When you configure port forwarding, vCloud Director maps an external IP address and a port to a service running on a port on a virtual machine for inbound traffic.
    - When you add a new port forwarding rule to an organization network, it appears at the bottom of the NAT mapping rule list.
      - Click the Manage & Monitor tab and click Organization Networks in the left pane.
      - Right-click the organization network name and select Configure Services.
      - Click the NAT Mapping tab and click Add.
      - Select Port Forwarding and configure the port forwarding rule.
        - Select an external IP address.
        - Select an external port.
        - Type the IP address of the destination virtual machine.
        - If the virtual machine is fenced, type its external IP address.
        - If the virtual machine is not fenced, type its internal IP address.
        - Select an internal port.
        - Select a protocol for the type of traffic to forward.
        - Click OK.
      - Click OK.
  - **Configure IP Translation for an Organization Network**
    - You can configure certain organization networks to provide IP translation.
    - When you add a new IP translation rule to an organization network, it appears at the bottom of the NAT mapping rule list.
    - Procedure
- Click the Manage & Monitor tab and click Organization Networks in the left pane.
- Right-click the organization network name and select Configure Services.
- Click the NAT Mapping tab and click Add.
- Select IP Translation and configure the rule.
  - Select an external IP address.
  - Type the IP address of the destination virtual machine.
    - If the virtual machine is fenced, type its external IP address.
    - If the virtual machine is not fenced, type its IP address.
  - Click OK.
- Click OK.

- Enable IP Masquerading for an Organization Network
  - You can configure certain organization networks to provide IP masquerade services. You can use IP masquerading on an organization network to hide the internal IP addresses of virtual machines from the external network.
  - When you enable IP masquerade, vCloud Director translates a virtual machine's private, internal IP address to a public IP address for outbound traffic.
  - Both system administrators and organization administrators can enable IP masquerade.
- Prerequisites
  - Verify that you have an external NAT-routed organization network.
- Procedure
  - Click the Manage & Monitor tab and click Organization Networks in the left pane.
  - Right-click the organization network name and select Configure Services.
  - Click the NAT Mapping tab and select Enable IP Masquerade.
  - Click OK.

- VPN:
  - Enable Site-to-Site VPN for an Organization Network
    - You can enable site-to-site VPN for an organization network and then create a secure tunnel to another network.
    - vCloud Director supports site-to-site VPN between organization networks in the same organization, organization networks in different organizations (including organization networks in different instances of vCloud Director), and remote networks.
    - Both system administrators and organization administrators can enable site-to-site VPN.
- Prerequisites
  - An external NAT-routed organization network.
  - vShield Manager 5.0.
- Procedure
  - Click the Manage & Monitor tab and click Organization Networks in the left pane.
  - Right-click the organization network name and select Configure Services.
  - Click the Site-to-Site VPN tab and select Enable site-to-site VPN.
  - (Optional) Type a public IP address.
If the external network to which the organization network is routed is behind a NAT device, you must provide a publicly accessible IP address that faces the Internet.

- Click OK.

Create a VPN Tunnel Within an Organization

- You can create a VPN tunnel between two organizations networks in the same organization.
- Both system administrators and organization administrators can create VPN tunnels.
- If there is a firewall between the tunnel endpoints, you must configure it to allow the following IP protocols and UDP ports:
  - IP Protocol ID 50 (ESP)
  - IP Protocol ID 51 (AH)
  - UDP Port 500 (IKE)
  - UDP Port 4500

Prerequisites

- At least two external NAT-routed organization networks with non-overlapping IP subnets and site-to-site VPN enabled on both networks.
- vShield Manager 5.0.

Procedure

- Click the Manage & Monitor tab and click Organization Networks in the left pane.
- Right-click the organization network name and select Configure Services.
- Click the Site-to-Site VPN tab and click Add.
- Type a name and optional description.
- Select a network in this organization from the drop-down menu and select a peer network.
- Review the tunnel settings and click OK.

Create a VPN Tunnel Between Organizations

- You can create a VPN tunnel between two organizations networks in different organizations. The organizations can be part of the same vCloud Director installation or a different installation.
- Both system administrators and organization administrators can create VPN tunnels.
- If there is a firewall between the tunnel endpoints, you must configure it to allow the following IP protocols and UDP ports:
  - IP Protocol ID 50 (ESP)
  - IP Protocol ID 51 (AH)
  - UDP Port 500 (IKE)
  - UDP Port 4500

Prerequisites

- An external NAT-routed organization network in each of the organizations. The organization networks must have non-overlapping IP subnets and site-to-site VPN enabled.
- vShield Manager 5.0.

Procedure

- Click the Manage & Monitor tab and click Organization Networks in the left pane.
- Right-click the organization network name and select Configure Services.
- Click the Site-to-Site VPN tab and click Add.
- Type a name and optional description.
- Select a network in another organization from the drop-down menu.
- Click Connect to another organization, type the login information for the peer organization, and click Continue.

### Create a VPN Tunnel to a Remote Network

- You can create a VPN tunnel between an organization network and a remote network.
- Both system administrators and organization administrators can create VPN tunnels.
- If there is a firewall between the tunnel endpoints, you must configure it to allow the following IP protocols and UDP ports:
  - IP Protocol ID 50 (ESP)
  - IP Protocol ID 51 (AH)
  - UDP Port 500 (IKE)
  - UDP Port 4500

### Prerequisites

- An external NAT-routed organization network and a routed remote network that uses IPSec.
- vShield Manager 5.0.

### Procedure

- Click the Manage & Monitor tab and click Organization Networks in the left pane.
- Right-click the organization network name and select Configure Services.
- Click the Site-to-Site VPN tab and click Add.
- Type a name and optional description.
- Select a remote network from the drop-down menu.
- Type the peer settings.
- Review the tunnel settings and click OK.

### Add a SNAT/DNAT rule

- When you create an IP translation rule for a network, vCloud Director adds a DNAT and SNAT rule to the vShield Edge associated with the network’s port group. The DNAT rule translates an external IP address to an internal IP address for inbound traffic. The SNAT rule translates an internal IP address to an external IP address for outbound traffic. If the network is also using IP masquerade, the SNAT rule takes precedence.
The vShield Admin Guide states how to configure SNAT and DNAT rules (page 40&41) in the vSphere client but this happens automatically when configuring IP translation in the vCloud GUI.

- **Add a DHCP IP pool**
  - When configuring the DHCP pool to be used the range of DHCP IP addresses cannot overlap with the static IP pool for the network.
    - Click the Manage & Monitor tab and click Organization Networks in the left pane.
    - Right-click the organization network name and select Configure Services.
    - Type a range of IP addresses or use the default range.
    - Set the default lease time and maximum lease time or use the default values.
    - Click OK.
  - The vShield Admin Guide states how to configure a new IP pool (page 41&42) in the vSphere client but this happens automatically when configuring the DHCP range in the vCloud GUI.

- **Add DHCP static binding**
  - You can enable static binding to bind an IP address to the MAC address of a virtual machine.
  - **Procedure**
    - In the vSphere Client, go to Inventory > Networking.
    - Select an internal port group that is protected by a vShield Edge.
    - Click the vShield Edge tab.
    - Click the DHCP link.
    - Under DHCP Bindings, click Add Binding.
    - Select the VM Name that you want to bind.
    - Select the Interface for which you want to create the binding.
    - Type the IP Address to which you want to bind the MAC address of the selected virtual machine.
    - Type the Domain Name.
    - Type the Primary Nameserver and Secondary Nameserver, which refer to the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution.
    - Type the Default Gateway address.
    - For Lease Time, select whether you want to lease the address to the client for the default time (1 day) or specify a value in seconds.
    - Click OK.

- **Configure the VPN service**
  - For some reason it seems as the Blueprint wants you to know how to configure VPN services on a vShield Edge device in the vSphere client as well even though this is supposed to be done in the vCloud GUI.
    - You must configure an external IP address on the vShield Edge to provide VPN service.
    - **Procedure**
      - In the vSphere Client, go to Inventory > Networking.
      - Select an internal port group that is protected by a vShield Edge.
      - Click the vShield Edge tab.
      - Click the VPN link.
      - Under Global Configuration, click Enable VPN.
        - The Add VPN Configuration dialog box opens.
        - Type the IP address of the vShield Edge instance in Local Service IP Address.
        - Type the pre-shared key in PSK for Sites with any Peer IP if anonymous sites are to connect to the VPN service.
        - Type a name for the VPN connection in VPN Gateway ID.
Select Log to log VPN activity.
Click OK.

- **Configure Syslog**
  - Apply Syslog Server Settings to an Organization Network
    - You can apply syslog server settings to a routed organization network to enable firewall rule logging.
    - Apply syslog server settings to any organization network that was created before the initial creation of those settings. Apply the syslog server settings to an organization network any time the settings are changed.
    - If you are unsure whether an organization network's syslog settings are up-to-date, you can view the organization network's syslog settings.
  - Prerequisites
    - Verify that you have an external NAT-routed organization network.
  - Procedure
    - Click the Manage & Monitor tab and click Organization Networks in the left pane.
    - Select an organization network, right-click, and select Synchronize syslog server settings.
    - Click Yes.
  - View Syslog Server Settings for an Organization Network
    - You can view the syslog server settings for a routed organization network.
    - vCloud Director supports logging events related to firewall rules to a syslog server that a system administrator specifies.
    - If an organization network lacks syslog server settings and you think that it should have them, or if the settings are not what you expected, synchronize the network with the most current syslog server settings.
  - Prerequisites
    - Verify that you have an external NAT-routed organization network.
    - Verify that you are an organization administrator.
  - Procedure
    - Click the Manage & Monitor tab and click Organization Networks in the left pane.
    - Select an organization network, right-click, and select Properties.
    - Click the Syslog Server Settings tab.

You can Select Log network traffic for firewall rule check box when configuring a firewall rule.

- **Use logs to troubleshoot common network service issues**
  - The system event message logged in the syslog has the following structure.
    - `syslog header (timestamp + hostname + sysmgr/)`
    - `Timestamp (from the service)`
    - `Name/value pairs`
      - `Name and value separated by delimiter '::' (double colons)`
      - `Each name/value pair separated by delimiter ';;' (double semi-colons)`
  - The fields and types of the system event contain the following information.
    - `Event ID :: 32 bit unsigned integer`
    - `Timestamp :: 32 bit unsigned integer`
    - `Application Name :: string`
    - `Application Submodule :: string`
    - `Application Profile :: string`
    - `Event Code :: integer (possible values: 10007 10016 10043 20019)`
    - `Severity :: string (possible values: INFORMATION LOW MEDIUM HIGH CRITICAL)`
    - `Message :: `
Objective 5.1 – Create vCloud Organizations

Knowledge

- **Identify the URL name of a newly created Organization**
  - The format is [https://www.example.com/cloud/org/myOrg](https://www.example.com/cloud/org/myOrg)
  - When naming the Organization the myOrg is the name used in the URL.

- **Create/Modify/Delete vCloud Organizations**
  - **Create**
    - **Open the New Organization Wizard**
      - Open the New Organization wizard to start the process of creating an organization.
      - Procedure
        - Click the Manage & Monitor tab and then click Organizations in the left pane.
        - Click the New Organization button.
      - The New Organization wizard starts.
    - **Name the Organization**
      - Provide a descriptive name and an optional description for your new organization.
      - Procedure
        - Type an organization name.
          - This name provides a unique identifier that appears as part of the URL that members of the organization use to log in to the organization.
        - Type a display name for the organization.
          - This name appears in the browser header when an organization member uses the unique URL to log in to vCloud Director. An administrator or organization administrator can change this name later.
        - (Optional) Type a description of the organization.
        - Click Next.
    - **Specify the Organization LDAP Options**
      - You can use an LDAP service to provide a directory of users and groups for the organization. If you do not specify an LDAP service, you must create a user account for each user in the organization. LDAP options can only be set by a system administrator and cannot be modified by an organization administrator.
      - Procedure
        - Select the source for organization users.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not use LDAP</td>
<td>Organization administrator creates a local user account for each user in the organization. You cannot create groups if you choose this option.</td>
</tr>
<tr>
<td>VCD system LDAP service</td>
<td>Use the vCloud Director system LDAP service as the source for organization users and groups.</td>
</tr>
<tr>
<td>Custom LDAP service</td>
<td>Connect the organization to its own private LDAP service.</td>
</tr>
</tbody>
</table>

- Provide any additional information that your selection requires.
<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not use LDAP</td>
<td>Click Next</td>
</tr>
</tbody>
</table>
| VCD system LDAP service | (Optional) Type the distinguished name of the organizational unit (OU) to use to limit the users that you can import into the organization and click Next. If you do not enter anything, you can import all users in the system LDAP service into the organization. Note: Specifying an OU does not limit the LDAP groups you can import. You can import any LDAP group from the system LDAP root. However, only users who are in both the OU and the imported group can log in to the organization. *Add Local Users to the Organization*  
  ▪ Every organization should have at least one local, non-LDAP, organization administrator account, so that users can log in even if the LDAP service is unavailable.  
  ▪ Procedure  
    ▪ Click Add.  
    ▪ Type a user name and password.  
    ▪ Assign a role to the user.  
    ▪ (Optional) Type the contact information for the user.  
    ▪ Select Unlimited or type a user quota for stored and running virtual machines and click OK.  
    ▪ These quotas limit the user's ability to consume storage and compute resources in the organization.  
    ▪ Click Next.  
  *Set the Organization Catalog Publishing Policy*  
  ▪ A catalog provides organization users with a library of vApp templates and media that they can use to create vApps and install applications on virtual machines.  
  ▪ Generally, catalogs should only be available to users in a single organization, but a system administrator can allow the organization administrator to publish their catalogs to all organizations in the vCloud Director installation.  
  ▪ Procedure  
    ▪ Select a catalog publishing option.  
    ▪ Cannot publish catalogs - Org administrator cannot publish catalogs to users outside of the organization.  
    ▪ Allow publishing catalogs to all organizations - Can publish catalogs to all users in all organizations.  
  *Configure Email Preferences*  
  ▪ vCloud Director requires an SMTP server to send user notification and system alert emails. An organization can use the system email settings or use its own email settings.  
  ▪ Procedure  
    ▪ Select an SMTP server option.  
    ▪ Use system default SMTP server - The organization uses the system SMTP server.  
    ▪ Set organization SMTP server - The organization uses its own SMTP server. Type the DNS host name or IP address and port number of the SMTP server.  
    ▪ Select a notification settings option.
- Use system default notification settings - The organization uses the system notification settings.
- Set organization notification settings - The organization uses its own notification settings. Type an email address that appears as the sender for organization emails, type text to use as the subject prefix for organization emails, and select the recipients for organization emails.

- **Configure Organization Lease, Quota, and Limit Settings**
  - Leases, quotas, and limits constrain the ability of organization users to consume storage and processing resources. Use these settings to prevent users from depleting or monopolizing an organization's resources.
  - **Procedure**
    - Select the lease options for vApps and vApp templates.
    - **Leases provide a level of control over an organization's storage and compute resources by specifying the maximum amount of time that vApps can run and that vApps and vApp templates can be stored.** You can also specify what happens to vApps and vApp templates when their storage lease expires.
    - Select the quotas for running and stored virtual machines.
    - **Quotas determine how many virtual machines each user in the organization can store and power on in the organization's virtual datacenters.** The quotas that you specify act as the default for all new users added to the organization.
    - Select the limits for resource intensive operations.
      - Certain vCloud Director operations, for example copy and move, are more resource intensive than others. **Limits prevent resource intensive operations from affecting all the users in an organization and also provide a defense against denial-of-service attacks.**
    - Select the number of simultaneous VMware Remote Console connections for each virtual machine.
      - **You might want to limit the number of simultaneous connections for performance or security reasons.**
    - **NOTE** This setting does not affect Virtual Network Computing (VNC) or Remote Desktop Protocol (RDP) connections.
    - (Optional) Select the Account lockout enabled check box, select the number of invalid logins to accept before locking a user account, and select the lockout interval.
    - Click Next.

- **Confirm Settings and Create the Organization**
  - Before you create the organization, review the settings you entered.
  - **Procedure**
    - Review the settings for the organization.
    - (Optional) Click Back to modify the settings.
    - Click Finish to accept the settings and create the organization.

- **Modify**
  - **NOTE:** In almost every case you can change the same thing as when creating a new organization so I will just post where you need to click to modify the setting.

- **Name**
  - Prerequisites
    - You must disable the organization before you can rename it.
  - **Procedure**
- Click the Manage & Monitor tab and click Organizations in the left pane.
- Right-click the organization name and select Properties.
- On the General tab, type a new organization name and click OK.
  - The internal organization URL changes to reflect the new name.
- **Full Name and Description**
  - Click the Manage & Monitor tab and click Organizations in the left pane.
  - Right-click the organization name and select Properties.
  - On the General tab, type a new full name or description and click OK.
- **LDAP Options**
  - Click the Manage & Monitor tab and click Organizations in the left pane.
  - Right-click the organization name and select Properties.
  - Click the LDAP Options tab.
  - System administrators and organization administrators who are currently logged in cannot import users and groups using the modified LDAP options until the cache for their current session expires or they log out and log in again.
- **Catalog Publishing Policy**
  - Click the Manage & Monitor tab and click Organizations in the left pane.
  - Right-click the organization name and select Properties.
  - Click the Catalog Publishing tab.
  - For users who are currently logged in to the organization, changes to the catalog publishing policy do not take effect until the cache for their current session expires or they log out and log in again.
- **Email Preferences**
  - Click the Manage & Monitor tab and click Organizations in the left pane.
  - Right-click the organization name and select Properties.
  - Click the Email Preferences tab.
  - You can Test the email setting with Test Email Settings button.
- **Lease, Quota and Limit Settings**
  - Click the Manage & Monitor tab and click Organizations in the left pane.
  - Right-click the organization name and select Properties.
  - Click the Policies tab.
  - **Delete**
    - Prerequisites
      - Before you can delete an organization, you must disable it and delete or change ownership of all objects that the organization users own.
    - Procedure
      - Click the Manage & Monitor tab and click Organization in the left pane.
      - Right-click the organization name and select Delete.
      - Click Yes.
- **Configure VM lease times**
  - The goal of a runtime lease is to prevent inactive vApps from consuming compute resources. For example, if a user starts a vApp and goes on vacation without stopping it, the vApp continues to consume resources.
  - A runtime lease begins when a user starts a vApp. When a runtime lease expires, vCloud Director stops the vApp.
  - How to configure see button 2: Configure Organization Lease, Quota, and Limit Settings
- **Configure Storage lease times**
  - The goal of a storage lease is to prevent unused vApps and vApp templates from consuming storage resources.
A vApp storage lease begins when a user stops the vApp. Storage leases do not affect running vApps. A vApp template storage lease begins when a user adds the vApp template to a vApp, adds the vApp template to a workspace, downloads, copies, or moves the vApp template.

When a storage lease expires, vCloud Director marks the vApp or vApp template as expired, or deletes the vApp or vApp template, depending on the organization policy you set.

How to configure see button 2: Configure Organization Lease, Quota, and Limit Settings

- **Configure SMTP server information**
  - vCloud Director requires an SMTP server to send user notification and system alert emails. You can modify the settings you specified when you created the organization.
  - Procedure
    - Click the Manage & Monitor tab and click Organizations in the left pane.
    - Right-click the organization name and select Properties.
    - Click the Email Preferences tab.
    - Select an SMTP server option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use system default SMTP server</td>
<td>Organization uses the system SMTP server.</td>
</tr>
<tr>
<td>Set organization SMTP server</td>
<td>Organization uses its own SMTP server. If you select this option, type the DNS host name or IP address and port number of the SMTP server. (Optional) Select the Requires authentication check box and type a user name and password.</td>
</tr>
</tbody>
</table>

- Select a notification settings option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use system default notification settings</td>
<td>Organization uses the system notification settings.</td>
</tr>
<tr>
<td>Set organization notification settings</td>
<td>Organization uses its own notification settings. If you select this option, type an email address that appears as the sender for organization emails, type text to use as the subject prefix for organization emails, and select the recipients for organization emails.</td>
</tr>
</tbody>
</table>

- (Optional) Type a destination email address and click Test Email Settings to verify that all SMTP server settings are configured as expected.
- Click OK.

- **Configure notification settings**
  - vCloud Director sends system alert emails when it has important information to report. For example, vCloud Director sends an alert when a datastore is running out of space. You can configure vCloud Director to send email alerts to all system administrators or to a specified list of email addresses.
  - Organizations can use the system notification settings, or use custom notification settings.
  - Prerequisites
    - A valid connection to an SMTP server.
  - Procedure
    - Click the Administration tab and click Email in the left pane.
    - Select the recipients of system alert emails and click Apply.

- **Apply policies to a vCloud Organization**
  - Password policy - Account lockout policy: When creating a Org.
○ Catalog publishing policy: Creating and modifying a Org.
○ Storage lease policy: Creating and modifying a Org.
○ These policies are mentioned in the notes above.

Objective 5.2 – Administer vCloud Organizations

Knowledge

- **List operations that can be performed on an Organization**
  ○ See Section 5.1 for modify Organization.

- **List the vCloud constructs that make up an Organization**
  ○ Organizations provide resources to a group of users and set policies that determine how users can consume those resources. Create an organization for each group of users that requires its own resources, policies, or both.
    
    - Policies
    - Resources
    - vDC with allocation models and Provider specified tier.

- **Given a tier of server determine the appropriate Organization vDC**
  ○ If your vCloud will have different tiers, eg. Gold, Silver, and Bronze.
    - Gold will have the fastest hardware, SSD disks + SAS disks, or/and other services like Backup.
    - Silver has SAS disks.
    - Bronze has SATA disks.
  ○ Most of the time the storage layer will change between vDC tiers.
  ○ Plan the placement of the workload according to its recommendations for performance.

- **Edit leases/quotas/limits applied to an Organization**
  ○ Leases, quotas, and limits constrain the ability of organization users to consume storage and processing resources. You can modify these settings to prevent users from depleting or monopolizing an organization's resources.
  ○ Procedure
    - Click the Manage & Monitor tab and click Organizations in the left pane.
    - Right-click the organization name and select Properties.
    - Click the Policies tab.
    - Select the lease options for vApps and vApp templates.
      - Leases provide a level of control over an organization's storage and compute resources by specifying the maximum amount of time that vApps can be running and that vApps and vApp templates can be stored. You can also specify what happens to vApps and vApp templates when their storage lease expires.
    - Select the quotas for running and stored virtual machines.
      - Quotas determine how many virtual machines each user in the organization can store and power on in the organization's virtual datacenters. The quota you specify acts as a default for all new users added to the organization.
    - Select the limits for resource intensive operations.
      - Certain vCloud Director operations, for example copy and move, are more resource intensive than others. Limits prevent resource intensive operations from affecting all the users in an organization and also provide a defense against denial-of-service attacks.
- Select the number of simultaneous connections for each virtual machine and click OK.

- **Revise Catalog(s) attached to an Organization**
  - **Share A Catalog**
    - Share a catalog to make its contents available to users in your organization. Users with the proper rights and access level can use vApp templates and media from the shared catalog to create their own vApps.
    - You are at least a catalog author.
    - **Procedure**
      - Click Catalogs > My Organization's Catalogs.
      - Select a catalog, right-click, and select Share.
      - Click Add Members.
      - Select the users and groups with whom you want to share the catalog.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone in the organization</td>
<td>Select this option to share the catalog with everyone.</td>
</tr>
<tr>
<td>Specific users and groups</td>
<td>Select this option, click specific users and groups, and click Add.</td>
</tr>
</tbody>
</table>

- Select an access level and click OK.

<table>
<thead>
<tr>
<th>Option</th>
<th>Supported Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Only</td>
<td>Open, Add to My Cloud, Download, Copy to Catalog</td>
</tr>
<tr>
<td>Read/Write</td>
<td>Open, Add to My Cloud, Download, Copy to Catalog, Publish, Move to Catalog, Delete</td>
</tr>
<tr>
<td>Full control</td>
<td>Open, Add to My Cloud, Download, Copy to Catalog, Publish, Move to Catalog, Delete, Share</td>
</tr>
</tbody>
</table>

- The actual actions a user can perform on a catalog and its contents depends on the intersection of the rights of the user and their access level to the catalog. Sharing a catalog with full control does not grant a user rights that the user do not already have.
  - Click OK.

- **Modify the Properties of Your Catalog**
  - You can review and modify your catalog properties.
  - You are at least a catalog author.
  - **Procedure**
    - Click Catalogs.
    - In the left pane, click My Organization's Catalogs.
    - Select a catalog, right-click, and select Properties.
    - Review the properties in the General, Sharing, and Publishing tabs.
    - Modify the relevant properties and click OK.

- **Add/Remove users and groups**
  - **Add Users**
    - **Add a Local User**
      - Adding local users allows organization administrators to provide access to users who do not exist on an LDAP server. You can also add local users if you do not plan to use an LDAP server.
      - **Procedure**
        - Click Administration.
        - In the left pane, select Members > Users.
        - Click the New User button.
• Type the user name and password.
• Select a role.
  • To create a custom role, contact your system administrator.
  • (Optional) Type the contact information.
• Select the stored and running virtual machine quota limits for this user.
• Click OK.
  • The new user appears on the Users page.

• Import an LDAP User
  • Organization administrators can import users from an LDAP server.
  • Contact a system administrator to configure LDAP settings for your organization.
  • Prerequisites
    • The LDAP settings for the organization must be set up and working.
  • Procedure
    • Click Administration.
    • In the left pane, select Members > Users.
    • Click the Import Users from LDAP button.
    • Type the full or partial user name and click Search.
    • Select a user and click Add.
    • Select a role for the imported user.
    • Click OK.

○ Remove Users
  • Delete a User
    • If a user leaves the company or moves to another organization, an organization administrator can delete a user from the organization.
    • Procedure
      • Click Administration.
      • In the left pane, select Members > Users.
      • Select a user, right-click, and select Disable Account.
      • Reselect this user, right-click, and select Delete.
      • Click OK.

  • Disable or Enable User Accounts
    • An organization administrator can disable a user account to log the user out of the Web console and prevent the user from logging in again. You can enable a user to allow them to log in.
    • Procedure
      • Click Administration.
      • In the left pane, select Members > Users.
      • Select a user, right-click, and select Disable Account or Enable Account.

○ Add Groups
  • Import a Group
    • An organization administrator can import LDAP groups into an organization.
    • Contact a system administrator to configure LDAP settings for your organization.
    • Prerequisites
      • The LDAP settings for the organization must be set up and working.
    • Procedure
      • Click Administration.
      • In the left pane, select Members > Groups.
      • Click the Import Groups from LDAP button.
      • Type the full or partial group name and click Search.
      • Select a group and click Add.
- Select a role for the group.
  - All the users in the group will be assigned this role.
  - Click OK.

  - Remove Groups
    - **Delete a Group**
      - An organization administrator can delete a group to remove it from the organization.
      - Deleting a group from an organization affects users who are members of the organization based solely on their membership in the deleted group. These users will not be able to log in to the organization. When you delete a group from an organization the group still exists in LDAP.
      - **Procedure**
        - Click Administration.
        - In the left pane, select Members > Groups.
        - Select a group, right-click, and select Delete.
        - Click Yes.

- **Configure/Edit Organization settings**
  - After receive the URL of your organization from the system administrator you can set it up on the vCloud Director Home page by clicking Set up this organization
    - Change the Organization Full Name
    - Import LDAP Users and Groups
    - Add local Users to the Organization
    - Configure email preferences
    - Configure Organization Lease, Quota and Limit Settings
    - All these procedures can be found in Section 5.1.

  - **Modify Email Settings**
    - You can review and modify the default email settings that were set when the system administrator created your organization.
    - You are an organization administrator.
    - **Procedure**
      - Click Administration.
      - In the left pane, select Settings > Email.
      - Select an SMTP server option.
        - **Option** | **Description**
          | Use system default SMTP server | Organization uses the system SMTP server.
          | Set organization SMTP server | Organization uses its own SMTP server. If you select this option, type the DNS host name or IP address and port number of the SMTP server. *(Optional)* Select the Requires authentication check box and type a user name and password.
        - Select a notification settings option.
          | Use system default notification settings | Organization uses the system notification settings.
          | Set organization notification settings | Organization uses its own notification settings. If you select this option, type an email address that appears as the sender for organization emails, type text to use as the subject prefix for organization emails, and select the recipients for organization emails.
            - *(Optional)* Type a destination email address and click Test Email Settings to verify that all SMTP server settings are configured as expected.
            - Click Apply.
 Modify Your Organization’s Policies
- You can review and modify the default policies that were set by the system administrator when your organization was created.
  - Click Administration.
  - In the left pane, select Settings > Policies.
  - Select the lease options for vApps and vApp templates.
  - Select the quotas for running and stored virtual machines.
  - Select the limits for resource intensive operations.
  - Select the number of simultaneous VMware Remote Console connections for each virtual machine.
  - (Optional) Select the Account lockout enabled check box, select the number of invalid logins to accept before locking a user account, and select the lockout interval.
  - Click Apply.

 Set Default Domain for Organization Virtual Machines
- You can set a default domain which virtual machines created in your organization can join. Virtual machines can always join a domain for which they have credentials, regardless of whether or not you specify a default domain.
  - Procedure
    - Click Administration.
    - In the left pane, select Settings > Guest Personalization.
    - Select the Enable domain join for virtual machines in this organization.
    - Type the domain name, domain user name, domain password.
    - These credentials apply to a regular domain user, not a domain administrator.
    - Click Apply.

 Allocate resources to an Organization
- You allocate resources to an organization by creating an organization vDC that is partitioned from a provider vDC. A single organization can have multiple organization vDCs.

 Open the Allocate Resources Wizard
- Open the Allocate Resources wizard to start the process of creating an organization vDC for an organization.
  - Procedure
    - Click the Manage & Monitor tab and click Organizations in the left pane.
    - Right-click the organization name and select Allocate Resources from the menu.
    - The Allocate Resources wizard starts.

 Select a Provider vDC
- An organization vDC obtains its compute and storage resources from a provider vDC. The organization vDC provides these resources to vApps and virtual machines in the organization.
  - Procedure
    - Select a provider vDC.
    - The provider vDC list displays information about available resources and the networks list displays information about networks available to the selected provider vDC.
    - Click Next.

 Select an Allocation Model
- The allocation model determines how and when the provider vDC compute and memory resources that you allocate are committed to the organization vDC.
  - Procedure
- Select an allocation model.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocation Pool</td>
<td>Only a percentage of the resources you allocate are committed to the</td>
</tr>
<tr>
<td></td>
<td>organization vDC. You can specify the percentage, which allows you to</td>
</tr>
<tr>
<td></td>
<td>overcommit resources.</td>
</tr>
<tr>
<td>Pay-As-You-Go</td>
<td>Resources are only committed when users create vApps in the organization</td>
</tr>
<tr>
<td></td>
<td>vDC. You can specify a percentage of resources to guarantee, which allows</td>
</tr>
<tr>
<td></td>
<td>you to overcommit resources. You can make a Pay-As-You-Go organization</td>
</tr>
<tr>
<td></td>
<td>vDC elastic by adding multiple resource pools to its provider vDC.</td>
</tr>
<tr>
<td>Reservation Pool</td>
<td>All of the resources you allocate are immediately committed to the</td>
</tr>
<tr>
<td></td>
<td>organization vDC. Users in the organization can control overcommitment</td>
</tr>
<tr>
<td></td>
<td>by specifying reservation, limit, and priority settings for individual</td>
</tr>
<tr>
<td></td>
<td>virtual machines.</td>
</tr>
</tbody>
</table>

- Click Next.
  - **Configure the Allocation Model**
    - Configure the allocation model to specify the amount of provider vDC resources to allocate to the organization vDC.
    - **Procedure**
      - Select the allocation model options.
      - Not all of the models include all of the options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU allocation</td>
<td>Enter the maximum amount of CPU, in GHz, to allocate to virtual machines</td>
</tr>
<tr>
<td></td>
<td>running in the organization vDC.</td>
</tr>
<tr>
<td>CPU resources guaranteed</td>
<td>Enter the percentage of CPU resources to guarantee to virtual machines</td>
</tr>
<tr>
<td></td>
<td>running in the organization vDC. You can overcommit resources by</td>
</tr>
<tr>
<td></td>
<td>guaranteeing less than 100%.</td>
</tr>
<tr>
<td>Memory allocation</td>
<td>Enter the maximum amount of memory, in GB, to allocate to virtual</td>
</tr>
<tr>
<td></td>
<td>machines running in the organization vDC.</td>
</tr>
<tr>
<td>Memory resources guaranteed</td>
<td>Enter the percentage of memory resources to guarantee to virtual</td>
</tr>
<tr>
<td></td>
<td>machines running in the organization vDC. You can overcommit resources</td>
</tr>
<tr>
<td></td>
<td>by guaranteeing less than 100%.</td>
</tr>
<tr>
<td>vCPU Speed</td>
<td>Enter the vCPU speed in GHz. Virtual machines running in the organization</td>
</tr>
<tr>
<td></td>
<td>vDC are assigned this amount of GHz per vCPU.</td>
</tr>
<tr>
<td>Maximum number of VMs</td>
<td>Enter the maximum number of virtual machines that can be created in the</td>
</tr>
<tr>
<td></td>
<td>organization vDC.</td>
</tr>
</tbody>
</table>

- Click Next.
  - **Allocate Storage**
    - An organization vDC requires storage space for vApps and vApp templates. You can allocate storage from the space available on provider vDC datastores.
    - Thin provisioning can help avoid over-allocating storage and save storage space. For a virtual machine with a thin virtual disk, ESX/ESXi provisions the entire space required for the disk's current and future activities.
    - ESX/ESXi commits only as much storage space as the disk needs for its initial operations.
    - Fast provisioning saves time by using vSphere linked clones for certain operations.
    - **IMPORTANT** Fast provisioning requires vCenter Server 5.0 and ESXi 5.0 hosts. If the provider vDC on which the organization vDC is based contains any ESX/ESXi 4.x hosts, you must disable fast provisioning. If the provider vDC on which the organization vDC is based contains any VMFS datastores connected to more than 8 hosts, powering on virtual machines may fail.
Make sure that datastores are connected to a maximum of 8 hosts. NOTE changed in vCloud 5.1. Max is now 32 hosts.

- **Procedure**
  - Enter the amount of storage to allocate.
  - (Optional) Select the Enable thin provisioning check box to enable thin provisioning for virtual machines in the organization vDC.
  - (Optional) Deselect the Enable fast provisioning check box to disable fast provisioning for virtual machines in the organization vDC.
  - Click Next.

- **Select Network Pool**
  - A network pool is a group of undifferentiated networks that is used to create vApp networks and NAT-routed or internal organization networks.
  - **Procedure**
    - Select a network pool or select None.
    - If you select None, you can add a network pool later.
    - Enter the maximum number of networks that the organization can provision from the network pool.
    - Click Next.

- **Name the Organization vDC**
  - You can provide a descriptive name and an optional description to indicate the vSphere functions available for your new organization vDC.
  - **Procedure**

- **Confirm Settings and Create the Organization vDC**
  - Before you create the organization vDC, review the settings you entered.
  - **Procedure**
    - Review the settings for the organization vDC.
    - (Optional) Click Back to modify the settings.
    - Click Finish to accept the settings and create the organization vDC.

- **When you create an organization vDC, vCloud Director creates a resource pool in vSphere to provide CPU and memory resources.**

- **Explain the purpose and use case for storage options**
  - **Thin-provisioning**
    - Thin provisioning can help avoid over-allocating storage and save storage space. For a virtual machine with a thin virtual disk, ESX/ESXi provisions the entire space required for the disk's current and future activities.
    - ESX/ESXi commits only as much storage space as the disk needs for its initial operations.
    - Use cases are, to name a few, development environments, storage-static workloads, Use of VAAI UNMAP thin-provisioning feature at maintenance windows etc.
  - **Fast-provisioning**
    - Fast provisioning saves time by using linked clones for virtual machine provisioning operations.
    - A linked clone is a duplicate of a virtual machine that uses the same base disk as the original, with a chain of delta disks to track the differences between the original and the clone. If fast provisioning is disabled, all provisioning operations result in full clones.
    - A linked clone cannot exist on a different vCenter datacenter or datastore than the original virtual machine.
    - vCloud Director creates shadow virtual machines to support linked clone creation across vCenter datacenters and datastores for virtual machines associated with a
vApp template. A shadow virtual machine is an exact copy of the original virtual machine. The shadow virtual machine is created on the datacenter and datastore where the linked clone is created.

- Fast provisioning is enabled by default on organization vDCs. Fast provisioning requires vCenter 5.0 and ESXi 5.0 hosts. If the provider vDC on which the organization vDC is based contains ESX/ESXi 4.x hosts, you must disable fast provisioning.
- Use cases include fast-provisioning dev environments etc.

- **Configure storage provision options**
  - **View Shadow Virtual Machines Associated With a Virtual Machine**
    - Shadow virtual machines support linked clones of virtual machines that are associated with vApp templates across vCenter datacenters and datastores.
    - A shadow virtual machine is an exact copy of the original virtual machine that vCloud Director creates on the datacenter and datastore where a linked clone is created.
  - **Procedure**
    - Click the Manage & Monitor tab and click Organizations in the left pane.
    - Right-click the organization name and select Open.
    - Click the My Cloud tab and click VMs in the left pane.
    - Right-click the virtual machine and select Properties.
    - Click the Shadow VMs tab.
      - This tab appears only for virtual machines that have associated shadow virtual machines.
    - vCloud Director shows a list of shadow virtual machines associated with the virtual machine. This list includes the name in vCenter of each shadow virtual machine, the datastore that each shadow virtual machine exists on, and the vCenter server that the shadow virtual machine belongs to.

- **Allocate Storage**
  - See in the Allocate resources to an Organization bullet.

### Objective 6.1 – Create and Administer Provider VDCs

**Knowledge**

- **Identify where in the hierarchy a provider VDC resides**
  - It right after the vSphere resources (vCenter, ESXi, Datastores and Networks)
- **Identify where an Provider VDC gets its resources**
  - Click the Manage & Monitor tab and click Provider vDCs in the left pane.
  - Click on the Provider vDC.
  - See the list of Organization vDC, Hosts, Datastores, External Networks and Resource pools.
- **Differentiate Provider and Organization VDCs**
  - A provider virtual datacenter (vDC) combines the compute and memory resources of a single vCenter Server resource pool with the storage resources of one or more datastores connected to that resource pool.
  - A provider vDC is the source for organization vDCs.
- **Explain the concept of a Provider VDC**
  - A provider virtual datacenter (vDC) combines the compute and memory resources of a single vCenter Server resource pool with the storage resources of one or more datastores connected to that resource pool.
- **Explain when and how to Enable/Disable a Provider VDC**
  - You can disable a provider vDC to prevent the creation of organization vDCs that use the provider vDC.
resources.

- When you disable a provider vDC, vCloud Director also disables the organization vDCs that use its resources. Running vApps and powered on virtual machines continue to run, but you cannot create or start additional vApps or virtual machines.

- Procedure
  - Click the Manage & Monitor tab and click Provider vDCs in the left pane.
  - Right-click the provider vDC name and select Enable or Disable.

- **Create/Delete a Provider VDC**
  - Create:
    - You can create a provider vDC to register vSphere compute, memory, and storage resources for vCloud Director to use. You can create multiple provider vDCs for users in different geographic locations or business units, or for users with different performance requirements.
    - A provider vDC can only include a single resource pool from a single vCenter Server.
    - If you plan to add a resource pool that is part of a cluster that uses vSphere HA, make sure you are familiar with how vSphere HA calculates slot size. For more information about slot sizes and customizing vSphere HA behavior, see the VMware vSphere Availability Guide.
  - Prerequisites
    - Verify that at least one vCenter Server is attached with an available resource pool to vCloud Director. The resource pool must be in a vCenter cluster that is configured to use automated DRS. The vCenter Server must have the vShield for VMware vCloud Director license key.
  - Procedure
    - Click the Manage & Monitor tab and click Provider vDCs in the left pane.
    - Click New Provider vDC.
    - Type a name and optional description.
      - You can use the name and description fields to indicate the vSphere functions available to the provider vDC, for example, vSphere HA.
    - Select the latest supported hardware version and click Next.
      - This selection determines the latest supported hardware version for virtual machines in organization vDCs based on this provider vDC. Hardware Version 8 requires ESX/ESXi 5.0 hosts. If this provider vDC will use a resource pool that contains ESX/Esxi 5.0 and ESX/ESXi 4.x hosts, select Hardware Version 7.
    - Select a vCenter Server and resource pool and click Next.
      - If the vCenter Server has no available resource pools, no resource pools appear in the list.
    - Select one or more datastores, click Add, and click Next.
      - vCloud Director does not support the use of read-only datastores with provider vDCs. In most cases, readonly datastores do not appear in the list, but some read-only NFS datastores might appear. Do not add these datastores to your provider vDC. Use only shared storage because vSphere DRS cannot migrate virtual machines on local storage.
      - Type the root user name and password for the ESX/ESXi hosts and click Next.
      - Click Finish to create the provider vDC.
  - Delete:
    - You can delete a provider vDC to remove its compute, memory, and storage resources from vCloud Director.
    - The resources remain unaffected in vSphere.
- **Prerequisites**
  - Disable the provider vDC.
  - Disable and delete all organization vDCs and organization networks that use the provider vDC.

- **Procedure**
  - Click the Manage & Monitor tab and click Provider vDCs in the left pane.
  - Right-click the provider vDC name and select Delete.
  - Click Yes.

- **Select Resource Pools and Datastores for a Provider VDC**
  - **Add Storage Capacity to a Provider vDC**
    - You can add storage capacity to a provider vDC by adding one or more datastores.
    - **Procedure**
      - Click the Manage & Monitor tab and click Provider vDCs in the left pane.
      - Right-click the provider vDC name and select Open.
      - Click the Datastores tab.
      - Click Add/Remove.
      - Select a datastore from the list, click Add, and click OK.
      - vCloud Director does not support the use of read-only datastores with provider vDCs. In most cases, readonly datastores do not appear in the list, but some read-only NFS datastores might appear. Do not add these datastores to your provider vDC.
      - Use only shared storage because vSphere DRS cannot migrate virtual machines on local storage.
  - **Add a Resource Pool to a Provider vDC**
    - You can add additional resource pools to a provider vDC so that pay-as-you-go organization vDCs that the provider vDC provides can expand.
    - When compute resources are backed by multiple resource pools, they can expand as needed to accommodate more virtual machines.
    - **Prerequisites**
      - Verify that there is one or more available resource pool exists in the same vCenter datacenter as the provider vDC's primary resource pool.
    - **Procedure**
      - Click the Manage & Monitor tab and click Provider vDCs in the left pane.
      - Right-click the provider vDC name and select Open.
      - Click the Resource Pools tab.
      - Click Add Resource Pool.
      - Select the resource pool to add and click Finish.
      - vCloud Director adds a resource pool for the provider vDC to use, making all pay-as-you-go organization vDCs backed by the provider vDC elastic.

- **Explain when and how to Enable/Disable a Provider VDC Host**
  - You can disable a host to prevent vApps from starting up on the host. Virtual machines that are already running on the host are not affected.
  - To perform maintenance on a host, migrate all vApps off of the host or stop all vApps and then disable the host.
  - **Procedure**
    - Click the Manage & Monitor tab and click Provider vDCs in the left pane.
    - Right-click the provider vDC name and select Open.
    - Click the Hosts tab.
    - Right-click the host name and select Enable Host or Disable Host.
    - vCloud Director enables or disables the host for all provider vDCs that use its resources.

- **Prepare/Unprepare a Provider VDC Host**
When you add an ESX/ESXi host to a vSphere cluster that vCloud Director uses, you must prepare the host before a provider vDC can use its resources. You can unprepare a host to remove it from the vCloud Director environment.

You cannot prepare a host that is in lockdown mode. After you prepare a host, you can enable lockdown mode.

Prerequisites
- Before you can unprepare a host, you must disable it and ensure that no virtual machines are running on the host.

Procedure
- Click the Manage & Monitor tab and click Provider vDCs in the left pane.
- Right-click the provider vDC name and select Open.
- Click the Hosts tab.
- Right-click the host name and select Prepare Host or Unprepare Host.
- vCloud Director prepares or unprepares the host for all provider vDCs that use its resources.

Upgrade/Repair a Provider VDC Host agent

Upgrade:
- vCloud Director installs agent software on each ESX/ESXi host in the installation. If you upgrade your ESX/ESXi hosts, you also need to upgrade your ESX/ESXi host agents.

Procedure
- Click the Manage & Monitor tab and click Provider vDCs in the left pane.
- Right-click the provider vDC name and select Open.
- Click the Hosts tab.
- Right-click the host name and select Upgrade Host.
- vCloud Director upgrades the host agent. This upgrade affects all provider vDCs that use the host.

Repair
- If the vCloud Director agent on an ESX/ESXi host cannot be contacted, try to repair the host.

Procedure
- Click the Manage & Monitor tab and click Provider vDCs in the left pane.
- Right-click the provider vDC name and select Open.
- Click the Hosts tab.
- Right-click the host name and select Repair Host.
- vCloud Director repairs the host. This operation affects all provider vDCs that use the host.

Explain when and how to Enable/Disable a Provider Datastore

You can enable or disable a datastore that has been added to a provider vDC. You must disable a datastore before you can remove it from vCloud Director.

When you disable a datastore, you cannot start vApps that are associated with the datastore or create vApps on the datastore.

Procedure
- Click the Manage & Monitor tab and click Datastores in the left pane.
- Right-click the datastore name and select Enable or Disable.

Configure Low Disk Space Warnings

You can configure low disk space warnings on a datastore to receive an email from vCloud Director when the datastore reaches a specific threshold of available capacity. These warnings alert you to a low disk situation before it becomes a problem.
- Click the Manage & Monitor tab and click Provider vDCs in the left pane.
- Right-click the provider vDC name and select Open.
- Click the Datastores tab.
- Right-click the datastore name and select Properties.
- Select the disk space thresholds for the datastore.
  - You can set two thresholds, yellow and red. When vCloud Director sends an email alert, the message indicates which threshold was crossed.
- Click OK.

Objective 6.2 – Create and Administer Organization VDCs

Knowledge

- List Allocation Models

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocation Pool</td>
<td>Only a percentage of the resources you allocate are committed to the organization vDC. You can specify the percentage, which allows you to overcommit resources.</td>
</tr>
<tr>
<td>Pay-As-You-Go</td>
<td>Resources are only committed when users create vApps in the organization vDC. You can specify a percentage of resources to guarantee, which allows you to overcommit resources. You can make a Pay-As-You-Go organization vDC elastic by adding multiple resource pools to its provider vDC.</td>
</tr>
<tr>
<td>Reservation Pool</td>
<td>All of the resources you allocate are immediately committed to the organization vDC. Users in the organization can control overcommitment by specifying reservation, limit, and priority settings for individual virtual machines.</td>
</tr>
</tbody>
</table>

- Explain the concept of an Organization VDC
  - Create an organization vDC to allocate resources to an organization. An organization vDC is partitioned from a provider vDC. A single organization can have multiple organization vDCs.
  - An organization vDC obtains its compute and storage resources from a provider vDC. The organization vDC provides these resources to vApps and virtual machines in the organization.

- Create/Modify/Delete an Organization VDC
  - Create
    - You allocate resources to an organization by creating an organization vDC that is partitioned from a provider vDC. A single organization can have multiple organization vDCs.
    - Open the Allocate Resources Wizard
      - Open the Allocate Resources wizard to start the process of creating an organization vDC for an organization.
      - Procedure
        - Click the Manage & Monitor tab and click Organizations in the left pane.
        - Right-click the organization name and select Allocate Resources from the menu.
        - The Allocate Resources wizard starts.
  - Select a Provider vDC
    - An organization vDC obtains its compute and storage resources from a provider vDC. The organization vDC provides these resources to vApps and virtual machines in the organization.
    - Procedure
Select a provider vDC.
- The provider vDC list displays information about available resources and the networks list displays information about networks available to the selected provider vDC.
- Click Next.

Select an Allocation Model
- The allocation model determines how and when the provider vDC compute and memory resources that you allocate are committed to the organization vDC.
- Procedure
  - Select an allocation model.
  - Click Next.

Configure the Allocation Model
- Configure the allocation model to specify the amount of provider vDC resources to allocate to the organization vDC.
- Procedure
  - Select the allocation model options.
  - Not all of the models include all of the options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU allocation</td>
<td>Enter the maximum amount of CPU, in GHz, to allocate to virtual machines running in the organization vDC.</td>
</tr>
<tr>
<td>CPU resources guaranteed</td>
<td>Enter the percentage of CPU resources to guarantee to virtual machines running in the organization vDC. You can overcommit resources by guaranteeing less than 100%.</td>
</tr>
<tr>
<td>Memory allocation</td>
<td>Enter the maximum amount of memory, in GB, to allocate to virtual machines running in the organization vDC.</td>
</tr>
<tr>
<td>Memory resources guaranteed</td>
<td>Enter the percentage of memory resources to guarantee to virtual machines running in the organization vDC. You can overcommit resources by guaranteeing less than 100%.</td>
</tr>
<tr>
<td>vCPU Speed</td>
<td>Enter the vCPU speed in GHz. Virtual machines running in the organization vDC are assigned this amount of GHz per vCPU.</td>
</tr>
<tr>
<td>Maximum number of VMs</td>
<td>Enter the maximum number of virtual machines that can be created in the organization vDC.</td>
</tr>
</tbody>
</table>

Allocate Storage
- An organization vDC requires storage space for vApps and vApp templates. You can allocate storage from the space available on provider vDC datastores.
- Thin provisioning can help avoid over-allocating storage and save storage space. For a virtual machine with a thin virtual disk, ESX/ESXi provisions the entire space required for the disk's current and future activities.
- ESX/ESXi commits only as much storage space as the disk needs for its initial operations.
- Fast provisioning saves time by using vSphere linked clones for certain operations.
- IMPORTANT Fast provisioning requires vCenter Server 5.0 and ESXi 5.0 hosts. If the provider vDC on which the organization vDC is based contains any ESX/ESXi 4.x hosts, you must disable fast provisioning. If the provider vDC on which the organization vDC is based contains any VMFS datastores connected to more than 8 hosts, powering on virtual machines may fail. Make sure that datastores are connected to a
maximum of 8 hosts. NOTE changed in vCloud 5.1. Max is now 32 hosts.

- **Procedure**
  - Enter the amount of storage to allocate.
  - (Optional) Select the Enable thin provisioning check box to enable thin provisioning for virtual machines in the organization vDC.
  - (Optional) Deselect the Enable fast provisioning check box to disable fast provisioning for virtual machines in the organization vDC.
  - Click Next.

- **Select Network Pool**
  - A network pool is a group of undifferentiated networks that is used to create vApp networks and NAT-routed or internal organization networks.
  - **Procedure**
    - Select a network pool or select None.
    - If you select None, you can add a network pool later.
    - Enter the maximum number of networks that the organization can provision from the network pool.
    - Click Next.

- **Name the Organization vDC**
  - You can provide a descriptive name and an optional description to indicate the vSphere functions available for your new organization vDC.
  - **Procedure**
    - Type a name and optional description.
    - Click Next.

- **Confirm Settings and Create the Organization vDC**
  - Before you create the organization vDC, review the settings you entered.
  - **Procedure**
    - Review the settings for the organization vDC.
    - (Optional) Click Back to modify the settings.
    - Click Finish to accept the settings and create the organization vDC.

- **When you create an organization vDC, vCloud Director creates a resource pool in vSphere to provide CPU and memory resources.**

- **Modify**
  - **Modify an Organization vDC Name and Description**
    - As your vCloud Director installation grows, you might want to assign a more meaningful name or description to an existing organization vDC.
    - **Procedure**
      - Click the Manage & Monitor tab and click Organization vDCs in the left pane.
      - Right-click the organization vDC name and select Properties.
      - On the General tab, type a new name and description and click OK.
      - You can use the name and description fields to indicate the vSphere functions available to the organization vDC, for example, vSphere HA.

- **Edit Organization vDC Allocation Model Settings**
  - You cannot change the allocation model for an organization vDC, but you can change some of the settings of the allocation model that you specified when you created the organization vDC.
  - **Procedure**
    - Click the Manage & Monitor tab and click Organization vDCs in the left pane.
Right-click the organization vDC name and select Properties.

On the Allocation tab, enter the new allocation model settings and click OK.

- These settings only affect vApps that you start from this point on. vApps that are already running are not affected. The usage information that vCloud Director reports for this organization vDC will not reflect the new settings until all running vApps are stopped and started again.

**Edit Organization vDC Storage Settings**
- After you create and use an organization vDC, you might decide to provide it with more storage resources from its source provider vDC. You can also enable or disable thin provisioning and fast provisioning for the organization vDC.
- **Procedure**
  - Click the Manage & Monitor tab and click Organization vDCs in the left pane.
  - Right-click the organization vDC name and select Properties.
  - On the Storage tab, enter the new storage settings and click OK.
  - **IMPORTANT** Fast provisioning requires vCenter Server 5.0 and ESXi 5.0 hosts. If the provider vDC on which the organization vDC is based contains and ESX/ESXi 4.x hosts, you must disable fast provisioning.

**Edit Organization vDC Network Settings**
- You can change the maximum number of provisioned networks in an organization vDC and the network pool from which the networks are provisioned.
- **Procedure**
  - Click the Manage & Monitor tab and click Organization vDCs in the left pane.
  - Right-click the organization vDC name and select Properties.
  - On the Network Pool tab, enter the new network settings and click OK.

**Delete**
- You can delete an organization vDC to remove its compute, memory, and storage resources from the organization. The resources remain unaffected in the source provider vDC.
- **Prerequisites**
  - Disable the organization vDC and move or delete all of its vApps, vApp templates, and media.
- **Procedure**
  - Click the Manage & Monitor tab and click Organization vDCs in the left pane.
  - Right-click the organization vDC name and select Delete.
  - Click Yes.

**Enable/Disable an Organization VDC**
- You can disable an organization vDC to prevent the use of its compute and storage resources by other vApps and virtual machines. Running vApps and powered on virtual machines continue to run, but you cannot create or start additional vApps or virtual machines.
- **Procedure**
  - Click the Manage & Monitor tab and click Organization vDCs in the left pane.
  - Right-click the organization vDC name and select Enable or Disable.

**Select Organization VDC components**
Im just guessing what the blueprint is trying to tell me here, select components... Could mean a lot of things.

- Allocation Model
  - Selected when creating a new Org vDC. Cannot modify after creation.

- Network Pool
  - Selected when creating a new Org vDC. Can modify after creation.

- Provider vDC
  - Selected when creating a new Org vDC. Cannot modify after creation.

**Select/Edit Organization VDC resources**

- Allocation
  - See Modify Org vCD in the bullet: *Create/Modify/Delete an Organization VDC*

- Storage
  - See Modify Org vCD in the bullet: *Create/Modify/Delete an Organization VDC*

- Network Pool
  - See Modify Org vCD in the bullet: *Create/Modify/Delete an Organization VDC*

**Configure Allocation Model settings**

- See Modify Allocation Settings in bullet: *Create/Modify/Delete an Organization VDC*

- Example
  - Allocation Pool

<table>
<thead>
<tr>
<th>Allocation Pool Setting</th>
<th>Allocation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Resource Pool Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25 GHz</td>
<td>CPU Limit</td>
<td>25 GHz</td>
</tr>
<tr>
<td>CPU % Guarantee</td>
<td>10%</td>
<td>CPU Reservation</td>
<td>2.5 GHz</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>50 GB</td>
<td>Memory Limit</td>
<td>50 GB</td>
</tr>
<tr>
<td>Memory % Guarantee</td>
<td>20%</td>
<td>Memory Reservation</td>
<td>10 GB</td>
</tr>
</tbody>
</table>

- Pay-as-you-Go

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU % Guarantee</td>
<td>10%</td>
<td>CPU Reservation, CPU Limit</td>
<td>0.00 GHz, Unlimited</td>
</tr>
<tr>
<td>Memory % Guarantee</td>
<td>100%</td>
<td>Memory Reservation, Memory Limit</td>
<td>0.00 GB, Unlimited</td>
</tr>
</tbody>
</table>

- Resource pools created to support Pay-As-You-Go organization vDCs will always have no reservations or limits. Pay-As-You-Go settings only affect overcommitment. A 100% guarantee means no overcommitment is possible. The lower the percentage, the more overcommitment is possible.

- Reservation Pool

**Table 5-3. How Reservation Pool Settings Affect Resource Pool Settings**

<table>
<thead>
<tr>
<th>Reservation Pool Setting</th>
<th>Reservation Pool Value</th>
<th>Resource Pool Setting</th>
<th>Resource Pool Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Allocation</td>
<td>25 GHz</td>
<td>CPU Reservation, CPU Limit</td>
<td>25 GHz, 25 GHz</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>50 GB</td>
<td>Memory Reservation, Memory Limit</td>
<td>50 GB, 50 GB</td>
</tr>
</tbody>
</table>

- Determine the appropriate network pool for a given Organization vDC network
Objective 7.1 – Create vApp Templates, Media and Catalogs

Knowledge

- **Describe the function of vApp templates, media, and catalogs**
  - A catalog is a container for vApp templates and media files in an organization.
  - Organization administrators and catalog authors can create catalogs in an organization. Catalog contents can be shared with other users in the organization and can also be published to all organizations in the vCloud Director installation.
  - There are two types of catalogs in vCloud Director: organization catalogs and public catalogs. Organization catalogs include vApp templates and media files that you can share with other users in the organization. If a system administrator enables catalog publishing for your organization, you can publish an organization catalog to create a public catalog.
  - There are two ways to add vApp templates to a catalog. You can upload an OVF package directly to a catalog or save a vApp as a vApp template.
  - You can upload media files directly to a catalog.

- **Identify the location of vApp templates, media and catalogs**
  - Depending on your role in the organization, you can access catalogs in your organization and public catalogs that were published by other organizations.
    - To access a public catalog, you must be an organization administrator.
    - To access a catalog in your organization, you must be at least a vApp author.
  - Procedure
    - Click Catalogs.
    - In the left pane, click on a catalog option.
    - My Organization's Catalogs
    - Public Catalogs
    - In the right pane, select a catalog, right-click, and select Open.

- **Identify the format in which vApp templates, media, and catalogs can be stored**
  - **vApp Templates:**
    - You can upload an OVF package as a vApp template to make the template available to other users. vCloud Director supports OVF 1.0 and OVF 1.1.
    - vCloud Director supports OVF files based on the Open Virtualization Format (OVF) Specification. If you upload an OVF that includes deployment options, those options are preserved in the vApp template.
    - You can quarantine files that users upload to vCloud Director so that you can process the files before you accept them
  - **Media:**
    - You can upload an ISO or FLP file to make the media available to other users.

- **Differentiate between vApp templates, media and catalogs**
  - A catalog consists of a list of catalogs, vApp templates, and media files in your organization.
  - When you click the Catalogs button in the menu bar, these tabs appear.
    - Catalogs
    - vApp Templates
    - Media
• A vApp template is a virtual machine image that is loaded with an operating system, applications, and data.
• You can upload media files to a catalog. Users with access to the catalog can use the media files to install applications on their virtual machines.
  
  **Create/Update a vApp template**
  
  **Create:**
  1. You can upload an OVF package from remote shares and your local directory to vCloud Director as a vApp template.
  2. You are at least a catalog creator.
  3. vCloud Director supports OVFs based on the Open Virtualization Format (OVF) Specification. If you upload an OVF file that includes OVF properties for customizing its virtual machines, those properties are preserved in the vApp template.
  4. **Prerequisites**
     - The computer from which you are uploading must have Java Plug-in 1.6.0_10 or later installed.
     - vCloud Director does not support uploading compressed OVF files.
  5. **Procedure**
     - Click Catalogs > My Organization’s Catalogs.
     - On the vApp Templates tab, click the Upload button.
     - Type the name and path of the OVF file to upload, or click Browse, select the OVF file, and click Upload.
     - Type a name and optional description for the vApp template.
     - Select a destination vDC and catalog.
     - Click Upload.
     - You can click the Launch Uploads and Downloads Progress Window button to track the progress.
  
  **Update:**
  1. You can modify some basic properties of a vApp template. To make more advanced changes to a vApp template, add it to My Cloud, make the changes, then add it back to the catalog as a new vApp template.
  2. You are an organization administrator.
  3. **Procedure**
     - Click Catalogs > My Organization’s Catalogs.
     - On the vApp Templates tab, right-click a vApp template and select Properties.
     - On the General tab, modify the vApp template name and description.
     - Select a vApp creation option.
       - This option applies when creating a vApp based on this template. It is ignored when building a vApp using individual virtual machines from this template.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make identical copy</td>
<td>vApps that are created from this vApp template must follow the guest operating system settings of the vApp template. If you select this option, and guest customization is enabled, the guest operating system is personalized.</td>
</tr>
<tr>
<td>Customize VM settings</td>
<td>Guest operating system is personalized regardless of the vApp template settings, and the guest operating system is personalized when the vApp is deployed. This option requires that a supported version of VMware Tools be installed on all virtual machines in the vApp.</td>
</tr>
</tbody>
</table>

- Choose whether or not to mark the vApp template as a Gold Master in the catalog.
- If you mark a vApp template as a Gold Master, this information appears in the list of vApp templates.
To reset the vApp template storage lease, select the Reset lease check box and select a new storage lease.

- Click OK.

- **Create/Delete a Catalog**
  - **Create:**
    - You can create catalogs to group your vApp templates and media files.
    - You are at least a catalog author.
    - **Procedure**
      - Click Catalogs > My Organization's Catalogs.
      - On the Catalogs tab, click the Add Catalog button.
      - Type a catalog name and optional description and click Next.
      - (Optional) To share the catalog with members of the organization, click Add Members, select users and groups, select an access level, click OK, and click Next.
      - Select a catalog publishing option and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don't publish this catalog to other organizations</td>
<td>This catalog will not be visible or available to other organizations in the vCloud Director installation.</td>
</tr>
<tr>
<td>Publish to all organizations</td>
<td>This catalog will be visible to all other organizations in the vCloud Director installation. Users with the necessary rights (by default, organization administrators) can view catalog items and copy them to a local organization catalog.</td>
</tr>
</tbody>
</table>

- **Delete:**
  - You can delete a catalog from your organization.
  - You are at least a catalog author.
  - **Prerequisites**
    - The catalog must not contain any vApp templates or media files. You can move these items to a different catalog or delete them.
  - **Procedure**
    - Click Catalogs.
    - In the left pane, click My Organization's Catalogs.
    - Select a catalog, right-click, and select Delete.
    - Click Yes.

- **Publish a catalog to different Organizations**
  - You can publish a catalog to make its vApp templates and media files available to all organizations in the installation.
  - **Prerequisites**
    - Verify that the organization that contains the catalog allows catalog publishing.
  - **Procedure**
    - Click the Manage & Monitor tab and click Organizations in the left pane.
    - Right-click the organization name and select Open.
    - Click Catalogs and select My Organization's Catalogs in the left pane.
    - On the Catalogs tab, right-click the catalog name and select Publish.
    - On the Publishing tab, select Publish to all organizations and click OK.
  - The catalog and all of its contents appear under Public Catalogs for all organizations in the vCloud Director installation.
Objective 7.2 – Administer vCloud Catalogs

Knowledge

- **Identify frequently used Catalog properties**
  - Share
  - Change Owner
    - You can change the owner of a catalog. Before you can delete a user who owns a catalog, you must change the owner or delete the catalog.
    - You are an organization administrator.
    - Procedure
      - Click Catalogs > My Organization’s Catalogs.
      - On the Catalogs tab, right-click a catalog and select Change Owner.
      - Select a user from the list or search for one.
        - You can search for a user by full name or their user name.
      - Click OK.
  - Name

- **Explain how guest customization works in a vCloud implementation**
  When you customize your guest OS you can set up a virtual machine with the operating system that you want.
  - vCloud Director can customize the network settings of the guest operating system of a virtual machine created from a vApp template. When you customize your guest operating system, you can create and deploy multiple unique virtual machines based on the same vApp template without machine name or network conflicts.
  - I recommend reading the chapter about Guest Operating System Customization, begins at page 105 in the vCloud Director User’s Guide.

- **Deploy a vApp from a Catalog**
  - You can add a vApp template as a vApp from your catalog to My Cloud.
  - You are at least a vApp author.
  - If the vApp template is based on an OVF file that includes OVF properties for customizing its virtual machines, those properties are passed to the vApp. If any of those properties are user-configurable, you can specify the values.
  - Prerequisites
    - A vApp template is available in a published or a locally shared catalog.
  - Procedure
    - Click Catalogs.
    - In the left pane, click on a catalog option.
      - My Organization’s Catalogs
    - Public Catalogs
      - You can access vApp templates in your organization's shared catalogs or, if you are an organization administrator, from a public catalog.
      - On the vApp Templates tab, select a vApp template, right-click, and select Add to My Cloud.
    - Type a name and optional description for the vApp.
    - Select a runtime and storage lease and click Next.
    - Select a virtual datacenter, configure the virtual machines in the vApp, and click Next.
      - Configure the custom properties, if any, and click Next.
      - Configure the networking options for the vApp and click Next.
      - Review the vApp summary information and click Finish.
  - vCloud Director creates a vApp on the My Cloud > vApps page.
• **Configure a Catalog to be shared by users in an Organization**
  - Share a catalog to make its contents available to users in your organization. Users with the proper rights and access level can use vApp templates and media from the shared catalog to create their own vApps.
  - You are at least a catalog author.
  - **Procedure**
    - Click Catalogs > My Organization's Catalogs.
    - Select a catalog, right-click, and select Share.
    - Click Add Members.
    - Select the users and groups with whom you want to share the catalog.
    - Select an access level and click OK.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone in the organization</td>
<td>Select this option to share the catalog with everyone.</td>
</tr>
<tr>
<td>Specific users and groups</td>
<td>Select this option, click specific users and groups, and click Add.</td>
</tr>
</tbody>
</table>

- The actual actions a user can perform on a catalog and its contents depends on the intersection of the rights of the user and their access level to the catalog. Sharing a catalog with full control does not grant a user rights that the user does not already have.
- Click OK.

• **Copy vApp templates and media to/from a Catalog**
  - **Copy a vApp Template from a Public Catalog to an Organization Catalog**
    - You can copy a vApp template from a public catalog to your organization catalog to make it available to users in your organization.
    - You are a vApp author or organization administrator.
    - **Prerequisites**
      - You have a catalog and vDC.
    - **Procedure**
      - Click Catalogs.
      - In the left pane, click Public Catalogs.
      - On the vApp Templates tab, select a vApp template, right-click, and select Copy To Catalog.
      - Type a name and optional description for the vApp.
      - Select a destination catalog and vDC.
        - Select a shared catalog to give organization users access to the template.
      - Click OK.
    - vCloud Director copies the vApp template to the organization catalog. The vApp appears on the vApp Templates tab in My Organization's Catalogs.
  - **Copy a vApp Template Between an Organization's Catalogs**
    - You can copy a vApp template from one catalog in your organization to another catalog in the same organization. This is useful if the catalogs are shared with different users and you want both groups of users to have access to the vApp template.
    - You are an organization administrator, catalog author, or vApp author.
    - **Prerequisites**
You must have access to at least two catalogs and a vDC with available space.

Procedure
- Click Catalogs > My Organization's Catalogs.
- On the vApp Templates tab, right-click a vApp template and select Copy to Catalog.
- Type a name and optional description for the vApp template.
- Select the destination catalog and vDC.
  - If you select a published catalog, the vApp template will be available to all organizations in the vCloud Director installation.
- Click OK.

Download a vApp Template
- You can download a vApp template from a catalog locally as an OVF file.
- You are at least a catalog author.

Prerequisites
- The computer from which you are downloading must have Java Plug-in 1.6.0_10 or later installed.

Procedure
- Click Catalogs.
- In the left pane, click on a catalog option.
  - My Organization's Catalogs
  - Public Catalogs
  - You can download vApp templates from your organization's catalogs or, if you are an organization administrator, from a public catalog.
- On the vApp Templates tab, select a vApp template, right-click, and select Download.
  - Navigate to the local folder where you want to save the OVF file and click Save.
  - You can click the Launch Uploads and Downloads Progress Window button from My Organization's Catalogs to track the progress.

Upload Media Files
- You can upload media files to a catalog. Users with access to the catalog can use the media files to install applications on their virtual machines.
- You are at least a catalog author.

Prerequisites
- The computer from which you are uploading must have Java Plug-in 1.6.0_10 or later installed.

Procedure
- Click Catalogs > My Organization's Catalogs.
- On the Media tab, click the Upload button.
- Type the path to the media file path or click Browse, locate the file, and click Upload.
- Type a name and optional description for the media file.
  - This is the name that appears in vCloud Director.
- Select the destination vDC and catalog.
- Click Upload.
  - The media file is uploaded to the specified location. You can click the Launch Uploads and Downloads Progress Window button to track the progress.

Copy Media Files to a Catalog
- You can copy media files to another catalog.
- You are at least a catalog author.

Prerequisites
You have access to multiple vDCs.

- **Procedure**
  - Click Catalogs.
  - On the Media tab, select a media file, right-click, and select Copy To Catalog.
  - Type a name and description.
  - Select the destination catalog and vDC.
  - Click OK.
- The media file is copied to and stored in the selected catalog.

- **Configure Catalog properties**
  - You can review and modify your catalog properties.
  - You are at least a catalog author.
  - **Procedure**
    - Click Catalogs.
    - In the left pane, click My Organization's Catalogs.
    - Select a catalog, right-click, and select Properties.
    - Review the properties in the General, Sharing, and Publishing tabs.
    - Modify the relevant properties and click OK.
- **Given requirements, apply the appropriate properties to a Catalog**
  - You can publish, share and change its name.

### Objective 8.1 – Troubleshoot and Audit Resources and Events in a vCloud

#### Knowledge
- **Identify vCloud Director interface components used for monitoring**
  - Manage and Monitor tab is used for logging Networks and vSphere Resources.
  - All logs and tasks for the vCloud infrastructure is in the Manage and Monitor tab.
  - To see logs for individual organization open My Cloud in the organization and select Logs.
- **Identify the location of logs in vCloud Director**
  - vCloud Director provides logging information for each cloud cell in the system. You can view the logs to monitor your cells and to troubleshoot issues.
  - You can find the logs for a cell at /opt/vmware/cloud-director/logs.

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cell.log</td>
<td>Console output from the vCloud Director cell.</td>
</tr>
<tr>
<td>vcloud-container-debug.log</td>
<td>Debug level log messages from the cell.</td>
</tr>
<tr>
<td>vcloud-container-info.log</td>
<td>Informational log messages from the cell. This log also shows warnings or errors encountered by the cell.</td>
</tr>
<tr>
<td>vmware-vcd-watchdog.log</td>
<td>Informational log messages from the cell watchdog. It records when the cell crashes, is restarted, and so on.</td>
</tr>
<tr>
<td>diagnostics.log</td>
<td>Cell diagnostics log. This file is empty unless diagnostics logging is enabled in the local logging configuration.</td>
</tr>
<tr>
<td>YYYY-MM-DD.request.log</td>
<td>HTTP request logs in the Apache common log format.</td>
</tr>
</tbody>
</table>

- **View Tasks and Events as an System Administrator**
  - **Procedure**
    - Log in to the vCloud Director system as a system administrator.
    - Click the Manage & Monitor tab and click Logs in the left pane.
    - Click the Tasks tab.
      - vCloud Director displays information about each system-level task.
      - Double-click a task for more information.
- **View Organization Events**
• You can view the log for an organization to monitor organization-level events. Failed events and view events are listed by user.
• You are an organization administrator.
• Procedure
  ▪ Click the My Cloud.
  ▪ In the left pane, click Logs.
  ▪ Click the Events tab.
    • vCloud Director displays information about each organization-level event.
  ▪ Double-click an event for more information.
  ▪ Only system administrators can view the details about most events.
• Monitor CPU, Disk and Memory usage for a Provider vDC
  ○ Provider vDCs supply compute, memory, and storage resources to organization vDCs. You can monitor provider vDC resources and add more resources if necessary.
  ○ Procedure
    • Click the Manage & Monitor tab and click Provider vDCs in the left pane.
    • Click the Monitor tab.
  ○ vCloud Director displays information about CPU, memory, and storage for each provider vDC.
• Monitor CPU, Disk and Memory usage for an Organization
  ○ Organization vDCs supply compute, memory, and storage resources to organizations. You can monitor organization vDC resources and add more resources if necessary.
  ○ Procedure
    • Click the Manage & Monitor tab and click Organization vDCs in the left pane.
    • Click the Monitor tab.
  ○ vCloud Director displays information about CPU, memory, and storage for each organization vDC.
• Monitor External Network, Organization Networks, and Network Pools
  ○ External Networks
    • Procedure
      • Click the Manage & Monitor tab and click External Networks
      • There you can see the status, VLAN, Default Gateway, IP allocation, corresponding vSphere Network and to which vCenter it is mapped.
  ○ Organization Networks
    • Procedure
      • Click the Manage & Monitor tab and click Organization Networks
      • There you can see the status, Default Gateway, Type, Connected to which External Network, What network pool is being used and what Organization owns it.
  ○ Network Pools
    • Procedure
      • Click the Manage & Monitor tab and click External Network Pools.
      • There you can see status, Type of Network pool, % of IP's used, to which vDS its connected to and to which vCenter.
• Monitor IP allocation utilization
  ○ External Networks
    • Procedure
      • Click the Manage & Monitor tab and click External Networks
      • Right click the network and select IP-allocation.
  ○ Organization Networks
    • You can view a list of IP addresses that are currently in use in an organization network IP pool.
Procedure

- Click the Manage & Monitor tab and click Organization Networks in the left pane.
- Right-click the organization network name and select IP Allocations.

  - Display the IP Allocations for Your vApp Network
  - You can review the IP allocations for the networks in your vApp.

Procedure

- Click My Cloud.
- In the left pane, select vApps.
- Select a vApp, right-click, and select Open.
- On the Networking tab, select the Show networking details check box.
- Select a network, right-click, and select IP Allocations.
- Review your allocations and click OK.

- **Review and interpret tasks and events in a vCloud**
  - See bullet: Identify the location of logs in vCloud Director
  - View the system log to monitor system-level tasks that are in progress, to find and troubleshoot failed tasks, and to view tasks by owner.
  - The log can also include debug information, depending on your vCloud Director settings.
    - You can display debug info in the vCloud Director task log in the settings.
      - Procedure:
        - Click Administration
        - Select General for System Settings.
        - Click Display debug information
        - NOTE: Only System Administrator can view the debug information.

- **Troubleshoot common resource/event issues in a vCloud**
  - First enable debug information in the System Settings
  - Your best chance is to Google the task detail if the error isn’t descriptive enough. Not kidding.

**Objective 8.2 – Map vCloud Resources to vSphere Resources**

**Knowledge**

- **Differentiate components of vCloud Director and vSphere client interfaces**
  - Well it’s not the same GUI... And you shouldn’t make any changes to the vCenter inventory after connecting it to a vCloud cell.

- **Describe the relationship between vCloud storage resources and VMFS/NFS datastores**
  - In vCenter you have ESXi hosts. These ESXi hosts have datastores attached to them, be it NFS or VMFS.
  - In the vCloud GUI you can add these datastores to a Provider vDC.
  - You can than give Organizations access to that Provider vDC and in turn give access to the datastores. Or at least be able to create vApps and VM’s on those datastores.

- **Describe the relationship between vCloud network resources and vSphere virtual switches**
  - In vCenter you have ESXi hosts. These ESXi hosts have physical NICs and corresponding virtual NICs.
  - These vmNICS are physically connected to a switch/router which most likely trunks some VLANs to those vmNICS.
  - These vmNICS connect to vSwitches, Virtual Simple Switches or Virtual Distributed Switches.
  - In the vCloud GUI, you can add an External Network which is a pre-configured portgroup (VSS or VDS).
- Also you create a Network Pool which is made of one of these configurations: VLAN range, already created portgroups or vCloud Isolation backed pools. The vCloud Isolation backed pool does not need to be backed by a vmNIC.

- **Describe the relationship between vCloud compute resources and DRS/HA Clusters/Resource Pools**
  - In vCenter you have ESXi hosts. These hosts are most likely in a cluster of ESXi hosts. A cluster is a resource pool. A cluster is also a HA cluster when HA is enabled.
  - When a new Organization is created a new Resource pool is created on the cluster (using the the resources on that cluster). The allocation on that resource pool is determined by the allocation pool type that was selected for that Organization.
    - Reserved Pool means the Resource pool as resources from the cluster reserved and limited.
      - Lets say you reserved 1 GHz and 6 GB of memory.
    - Allocation pool means that the Resource pool as reserved up to a point and is limited as well.
      - Lets say you want to reserve 50% of 1 GHZ and 6 GB of memory.
      - Then you pay only for 0.5 GHz and 3 GB of memory and then usage after that (if chargeback is correctly setup that is)
    - Pay-as-you-Go means the Resource pool can have a reservation on CPU and Memory, but only limit on each vCPU.
      - Lets say you want an environment with no reservation.
      - You only pay for what you use. Or use and have reserved.

- **Determine total/current resources available to a Provider/Organization vDC relative to assigned vSphere resources**
  - Provider vDC vs. vSphere resources.
    - Provider vDC total and current resources can be monitored in the vCloud GUI.
      - Click Manage and Monitor
      - Select Provider vDC's.
      - Click the Provider vDC.
        - The Datastore tab will show the status of the datastores used by this Provider vDC.
        - The External network tab will show the status of the External Network pool.
        - The Resource Pools tab will show the status of the resource pool that is used by this Provider vDC.
  - Organization vDC vs. vSphere resources.
    - Organization vDC current resources can be monitored in the vCloud GUI.
      - Click Manage and Monitor
      - Select Organization vDC's.
      - Click Monitor
        - There you see the current usage of Processor, Memory and Storage resources.

- **Determine the explicit vSphere resource consumed by a Provider/Organization vDC**
  - To determine what exact vSphere resource is consumed by any given vDC you need to go Hosts and Clusters and look at the Resource Pools.
  - Under each Resource Pool lies an Organization and in that resource pool are VM's.
  - These VM's are on a datastore which can seen in its summary or Virtual Machine Summary for the Resource Pool.
- Determine which vSwitch resource is being used by a given vCloud network
  - vSwitch resource are port groups.
  - To see which vCloud network is using which portgroup go to:
    - External Networks in the vCloud GUI to see which Port Group is used (noted in the vSphere Network).
- Determine on which datastore a vCloud hosted virtual machine resides
- Determine on which ESXi host a vCloud hosted virtual machine resides