How to Install XenDesktop on CloudPlatform

Lee Bushen – EMEA Tech Readiness July 2014

CITRIX

How to Install XenDesktop on CloudPlatform

With the release of XenDesktop 7.5, it's possible to enjoy the benefits of Cloud Computing with your XenDesktop system. Benefits such as centralised template management, advanced network isolation for shared services, easy scale-up and integration with existing Cloud projects.

This document is intended as a "How To" guide to installing XenDesktop 7.5 on top of a CloudPlatform based cloud. This guide was written as a follow up to the XenDesktop Cloud Provisioning webinar presented by Mikael Lindholm and Lee Bushen and details the steps taken to set up the XDCCP demo shown on that webinar.

As mentioned in the webinar, there are many ways to architect this solution. **This is not an official blueprint for building XenDesktop on CloudPlatform** but this guide will, in around 1.5 days, show you a potential way in which it could be configured. We have used the example of a local government shared service Cloud for the naming structure. Amend these as appropriate for your environment.

What you will need to follow this guide:

1) Hardware:
    a. Two physical x86 servers with sufficient RAM and CPU. The servers used in the demo system had 16GB RAM, 2 CPUs.
    b. NFS based storage. The demo used around 160GB for a basic installation.
2) CloudPlatform 4.3 installation software from Citrix.com
3) CentOS 6.4 x64 DVD1 ISO from the CentOS archives here

Note: The CloudPlatform install guide below refers to CentOS 6.3. For simplicity, we recommend that you use CentOS 6.4 for both the Volume Worker VM and the CloudPlatform Management VM.

4) XenDesktop 7.5 Trial Software: http://www.citrix.com/products/xendesktop/try
5) XenServer 6.2 software http://www.citrix.com/products/xenserver/try
6) Static IP addresses for:
    a. Your CloudPlatform Management server (cpman).
    b. If you don't have an existing NFS server, we provide info on configuring your own virtual NFS server.
    c. AD Controller and XD Controller (AD1 and XD1).
7) An IP address range for your CloudPlatform System VMs. In a small lab 10-20 addresses will suffice.
8) An IP address range for your other VMs within the Cloud, including Virtual Desktops, XenApp servers, Worker VMs etc. At least 20-30 addresses.

Setting up the hosting server for the XenDesktop and CloudPlatform backend

All infrastructure servers are installed outside the CloudPlatform system on a separate XenServer. This is a requirement for the CloudPlatform Management server, which cannot exist on the host system that it is managing, but the XenDesktop system could just as easily have been installed within the CloudPlatform system itself. XenServer 6.2 SP1 (Service Packed) was used as the hosting system. Hardware was HP DL360G5 servers with 16GB RAM and NFS connection to an NFS filer for storage. We'd recommend a higher spec server for a proper proof-of-concept.

Installing Windows Servers for Active Directory and XenDesktop

Install 2 x W2K12R2 Servers. Create two VMs on your XenServer, having first copied your Windows ISOs to your XenServer's ISO Library.

- AD1 – 2GB Ram, 1 x vCPU, 24GB Disk
- XD1 – 8GB RAM, 2 or 3 vCPUs, 36GB disk
- Select **W2K12R2 DC Edition (Server with GUI)** during the installation
- Install XenServer Tools into both VMs.
- Change Hostnames of Servers to AD1 and XD1
- Assign Static IPs and make the DNS server of XD1 the IP of the AD1 host.
- Install AD Domain Services and DNS Server onto AD1
- Using **Server Manager**, promote the AD1 to be a domain controller of **XD75CCP.local** domain**,** accepting the defaults & warnings about DNS and reboot the server.
- On AD1, launch **DNS Manager**, right click on server and set up a forwarder to an existing DNS server.
- On AD1, use **Active Directory Users and Groups** to create new OU under your domain called **Woking Council** and another OU beneath it called **Desktops**
- Create a new user in Woking called "Lee Bushen".
- Right Click the **Desktops** OU and use **Delegate Control** to add Lee as an Admin for the Desktops OU. Create a **Custom Task** to Delegate, Choose Computer Objects, give create and delete rights then on next page, choose full control.
- Join the XenDesktop Controller **XD1** to the **XD75CCP.local** domain hosted on **AD1**

Tip: For easier remote admin of each server, go to Server Manager of AD1 and XD1 and click on the Local Server node. Enable Remote Desktop and select the appropriate users within AD (Administrator and other tenant admins).

A word about time syncronisation

The integration between XenDesktop and CloudPlatform uses time-based encryption keys. You need to make sure that the CloudPlatform Management server and both AD and XD servers have the same time or preferably use the same time source. One symptom of bad time sync is when XenDesktop cannot connect to CloudPlatform with a user's API keys. Also, if timesync is lost during provisioning operations, they may fail.

XenDesktop Install

- Having copied the **XenDesktop 7.5 ISO** into your XenServer's ISO repository, mount it into your **XD1** VM and run the installer
- Choose **XenDesktop** install (rather than XenApp)
- Install Delivery Controller Software, choosing all component (DC, Studio, Director, License Server) and from next screen, Storefront, SQL & Remote Assist. Choose Automatic Ports from the last screen.
- Launch **Citrix Studio** from **XD1** and choose **Site Setup**. Choose a fully configured site, using SQL Express defaults and automatically create the database.
- Choose the 30 Day trial unless you have full licenses
- In the Site setup, choose "No Machine Management" you can do this later when you have CloudPlatform.
- No App-V Publishing.
- Do not start configuring machine catalogs at this point. We do this later.

After a few minutes, you should be able to connect to the Storefront on the address similar to:

http://[XD1-IP-Address]/Citrix/StoreWeb/

Creating a XenServer or a Pool of XenServers for CloudPlatform to Manage.

XenServer is free to download and use here. If you are new to XenServer, details of how to install and configure XenServer can be found on the XenServer QuickStart Master Class here: http://www.citrix.com/tv/#videos/6702. Installing XenServer 6.2 is identical to the installation shown in the video.

Install XenServer 6.2 with all current service packs and hotfixes before adding it as a CloudPlatform Host. If you have multiple XenServers, create and join them to a pool before adding them to CloudPlatform.

Hint: If you are using an Evaluation version of XenDesktop, you can point your XenServers to the license server on the XD1 XenDesktop controller. Although you don't lose any functionality with the free version of XenServer, you will need to install all the patches via the XenServer command line. If, using XenCenter, you point your XenServers at the XenDesktop controller and select **Citrix XenServer for XenDesktop** licensing, you can use XenCenter to install the patches which will save you a lot of time.

Although you can use both Basic and Advanced networking models in CloudPlatform, the demo system we configured was based on Basic mode (flat) networking. For Basic Mode networking in CloudPlatform, you need to make sure your XenServer hosts are configured correctly. Basic mode uses IPtables rules to maintain tenant isolation, so you need to perform the following tasks:

- From the XenServer console, type "**xe-switch-network-backend bridge**"
- Enable IPtables for Basic networking, in the file /etc/sysctl.conf modify the following lines as shown:
    - **net.bridge.bridge-nf-call-iptables = 1**
    - **net.bridge.bridge-nf-call-arptables = 1**
- Now reboot the server.

Configuring CloudPlatform

There is already a great Citrix guide for installing and configuring CloudPlatform. Although the guide was written for a specific hands-on lab, the content has been adapted and is included in **Appendix 1** below for reference [Page 10]

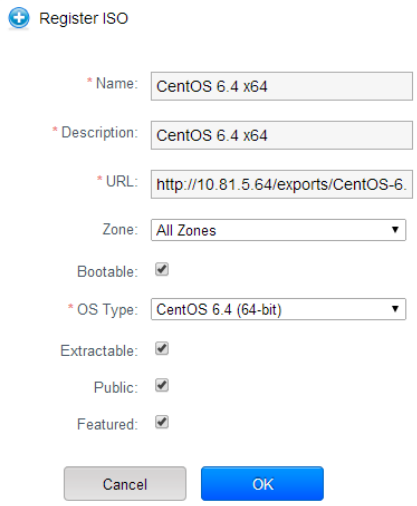
Note: The CloudPlatform Management VM in the demo was called cpman and had a 32GB disk and 1GB RAM.

Installing the Volume Worker Template into the CloudPlatform system

- Download CentOS 6.4 x86 or x64 from a CentOS repository and place it on an internal Webserver. Either 32/64 bit will work as a volume worker. The demo used 64 bit.

Note: If you don't have a webserver and you are not concerned with security, consider using your XenDesktop Storefront server (XD1) to host your ISOs for the purposes of importing. Place the ISOs in **c:\inetpub\wwwroot** and use the IP address of your Storefront server below.

- To import this ISO into the CloudPlatform system, you will need to allow CloudPlatform to download ISOs from an internal website by going to the **Global Settings** tab and searching for the parameter **secstorage.allowed.internal.sites**. Change the value to the IP Address of your Webserver (e.g. 192.168.10.10/32) and restart the CloudPlatform Management Server by typing **service cloudstack-management restart** on the CLI of the cpman server.
- Log into CloudPlatform and go to the **Templates** Tab, select **ISO** from the drop down menu
- Import the ISO for CentOS 6.4 x64 as per these settings:



- From the **Instances** tab, create a new CentOS 6.4 VM, booting from ISO, using a small footprint Compute Offering. For Example: A **Medium Instance** with **Small** (5GB) Hard Drive.
- Install CentOS in the same way you did when you created the cpman VM.

Now follow the configuration instructions for installing the **Volume Worker Template** in the **XenApp and XenDesktop concepts and deployment on CloudPlatform** guide: http://support.citrix.com/article/CTX140428

Hint: When you get to the part about copying the XenDesktop RPM to the Volume Worker VM, you will need to open a CloudPlatform ingress rule for Port 22 so that the XenDesktop host can access the Volume Worker via SSH to copy the file.

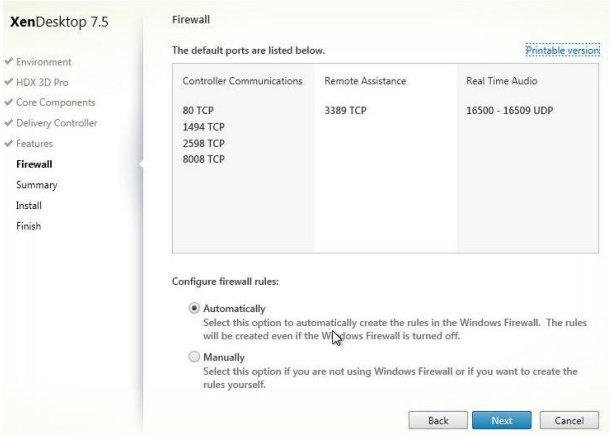
- Logged into CloudPlatform as Admin. Select **Networks** and select **Security Groups** from the drop down menu. Select the **Default Security Group** and set up the ingress rule as follows:

Loading a Windows VDI Template on CloudPlatform

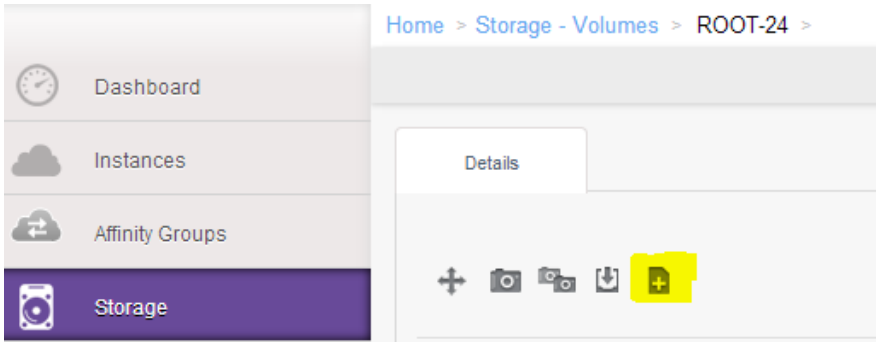
- Use the **Templates** tab in CloudPlatform and the **ISO** drop down item to import both a **Windows 7** & **XenDesktop 7.5 ISO** into CloudPlatform. You can then use these to create a Windows 7 Virtual Machine much in the same way as you installed the volume worker.

Prepare the image as you would for any normal XenDesktop deployment. The following workflow was followed in the lab.

- Install Windows 7
- Run a Windows Update and install recommended patches
- Install XenServer Tools
- Join the Windows 7 machine to the **XD75CCP.local** domain
- Set IP settings to DHCP for IP address and DNS
- Install XenDesktop 7.5 VDA using the defaults
- Ensure communication ports are opened automatically



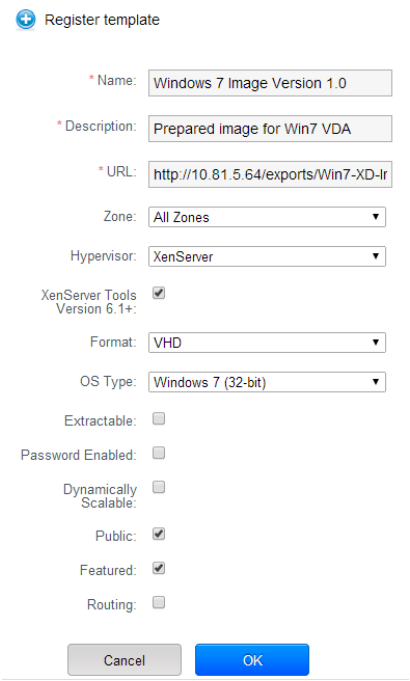
- Now **stop the Windows VM** and click on the root volume object of the VM and choose the option to **Create template** for XenDesktop to use.



Using an existing Windows image

You can create a Windows 7 base image on another XenServer and export the VM from your XenServer using OVF/OVA format. This will create a VHD file which needs to be uploaded to your webserver for importing into CloudPlatform.

Import the newly prepared Windows 7 image into CloudPlatform using the Templates/Register Templates option. Use the following settings making sure the XenServer Tools box is ticked.



Tip: When building the lab, the most reliable way was to install the templates directly from the CloudPlatform GUI, rather than importing them from a separate XenServer.

Creation a Service Offering for XenDesktop to use

Log into CloudPlatform and create a new Compute Offering within the **Service Offerings** tab. The demo used a 1Ghz CPU, 1GB RAM and 1 x vCPU offering.

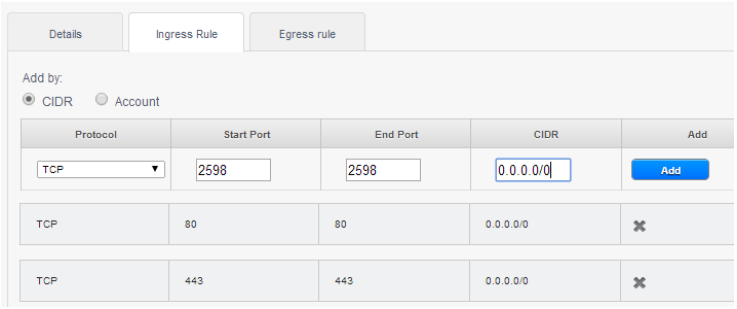
Configuring XenDesktop for Multi-Tenancy

To allow multiple administrators to manage the XenDesktop system, roles and scopes pertaining to AD users are created within Citrix Studio.

- On XD1, launch Citrix Studio, logged in as Domain Admin. Click the Administrators Node.
- Now setup a blank scope and appropriate roles for Woking Council, our new tenant.
    - Create Scope, Name, Description (e.g. **Woking Scope**) but with no objects at this stage.
    - Create a Role, Name (e.g. **CCP Tenant Admins**) and give them full rights to administer **Delivery Groups, Hosts and Machine Catalogs**.
- Enable Lee Bushen as a new Tenant Admin
    - Choose the **Administrators** tab and **Create Administrator**
    - Search for Lee Bushen and click the **Woking Scope** radio button
    - Click the **CCP Tenant Admins** role and **enable the administrator**.

Configuring a Cloud connection from XenDesktop

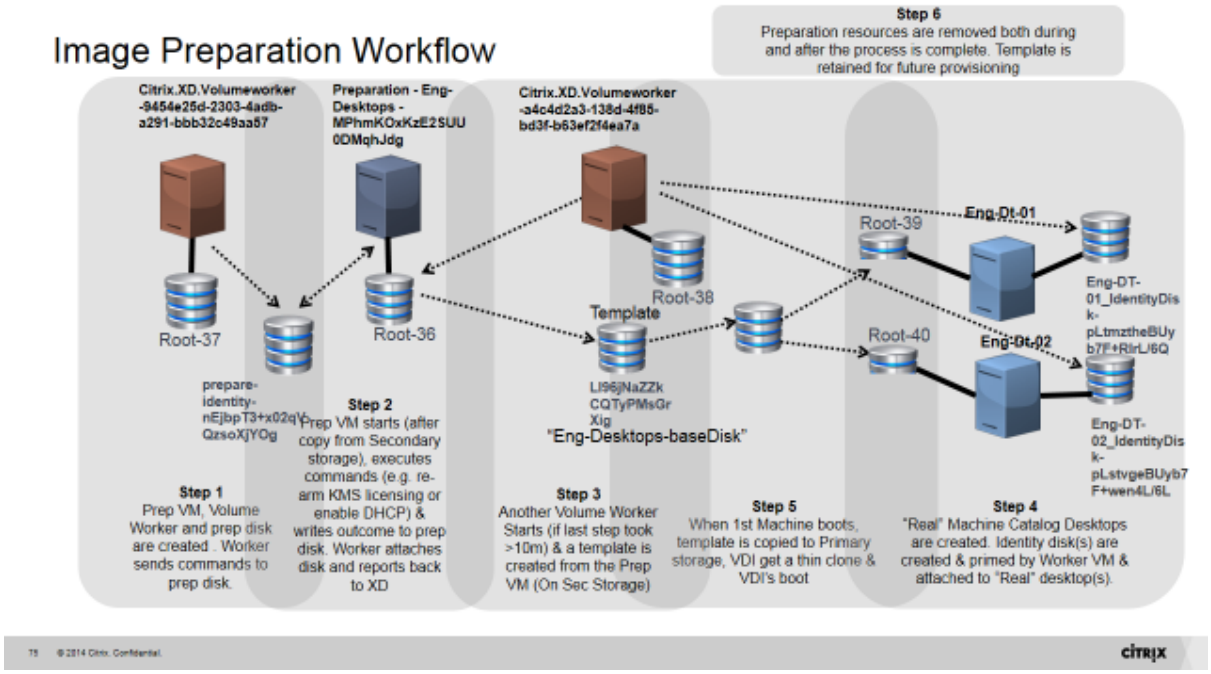
- Login to XenDesktop controller XD1 as **leeb** and observe that he can use Citrix Studio (but can't see others components)
- Launch the CloudPlatform Admin GUI and Choose the **Accounts** tab.
- Add an account called **Woking-Council** with a username of leeb. Fill in the default fields.
- Login to CloudPlatform as **leeb** and within **Networks** tab, and the **Security Groups** drop down menu, add a security group **Woking-Sec-Group-XD** with Ingress rules for TCP ports 80, 443 and 2598:



- Go to the **Accounts** tab and click on **Woking-Council**, find the **leeb** user, click on it and then click the icon to **generate keys.**
- Back in Citrix Studio, **create a new Hosting connector** to the Cloud using Lee's keys
    - Connection type : CloudPlatform
    - Address: http://[cpman IP Address]:8080/client/api
    - Use API Keys pasted from the CloudPlatform GUI
    - Connection Name **Woking Council – Cloud**
    - Choose **I want to create VMs in Zone : London**
    - Connection **London-Woking-Cloud**
- Because the Woking tenant does not have any personal templates, you need to configure the connection to look for all templates in the Cloud
    - Login to the XD1 server as **administrator**, launch Citrix Studio and change the advanced parameters of the connection to **TemplateFilter=executable** this will allow the **Woking** tenant to see templates that do not belong to them (e.g. The Windows 7 template the admin uploaded earlier). Note, at the time of writing, you need to be administrator to do this.
- In XenDesktop, **Create a Machine Catalog** with the following settings:
    - Windows Desktop OS
    - Machines are power managed and deployed using MCS in **London-Woking-Cloud**
    - Choose Random Desktops
    - Choose the Desktop image you uploaded to the Cloud earlier.
    - Choose your security group **Woking-Sec-Group-XD**
    - Provision 1 machine and specify the XenDesktop machine specification (Compute offering) you configured earlier within CloudPlatform.
    - Leave the default for NICs.
    - Create AD Accounts in Woking Council's **Desktops** OU with the name of **Woking-Win7-##**

- Catalog name **Woking Win7 Desktops**. Leave running; this will take up to 30 minutes to complete.

The following process is happening in the background:



- When the Machine Catalog has finished creating, from Citrix Studio, create a **Delivery Group** & start the VM:
    - Name **Pyrford Group**
    - Display name **Pyrford-Cloud-Desktop**
    - **Wait approx. 15 mins** as the template is copied to Primary Storage and the desktop is launched
    - After a few minutes, check that the desktop is running and that VDA registration has occurred in Citrix Studio
- Finally, launch a browser and login to your Storefront server as **xdccp\leeb.** The Storefront address will be: http://[XD1-IP-Address]/Citrix/StoreWeb/
- Launch your new Cloud Desktop!

That's it! If you got this far, you will have a fully functional XDCCP system. Congratulations!

Appendix 1

XenDesktop 7.5 and CloudPlatform 4.3

Setup CloudPlatform Cheat Sheet

Mike Palmer – Citrix Worldwide Readiness
June 2014

CITRIX

CloudPlatform Preparation

CloudPlatform Infrastructure Preparation

This module prepares the minimum infrastructure required for a CloudPlatform implementation.

You will create a Virtual Machine (VM) running on your physical XenServer host and install the CentOS Linux distribution onto the VM. This VM will become the CloudPlatform Management Server (cpman). You will then configure the VMs networking and prepare the VM for the CloudPlatform install.

NFS shared storage is required for CloudPlatform's secondary storage and is often used for CloudPlatform's primary storage. Typically in the datacenter this NFS storage would be provided by a hardware storage device such as a SAN or NAS, but in this lab the NFS storage is provided by a VM (nfs-server) running on the physical XenServer. This nfs-server VM has already been created for you in the same way as cpman, and the network has been similarly configured. You will need to install and configure the components needed to provide the NFS service onto nfs-server, and also install the services necessary to access the NFS shares onto cpman.

Exercises in this module

Exercise 1: Create the cpman VM and install CentOS 6.3
Exercise 2: Install XenServer Tools on the cpman VM
Exercise 3: Setup networking on the cpman VM
Exercise 4: Configure the nfs-server VM
Exercise 5: Configure NFS on the cpman VM

Exercise 1: Create the cpman VM and Install CentOS

Overview

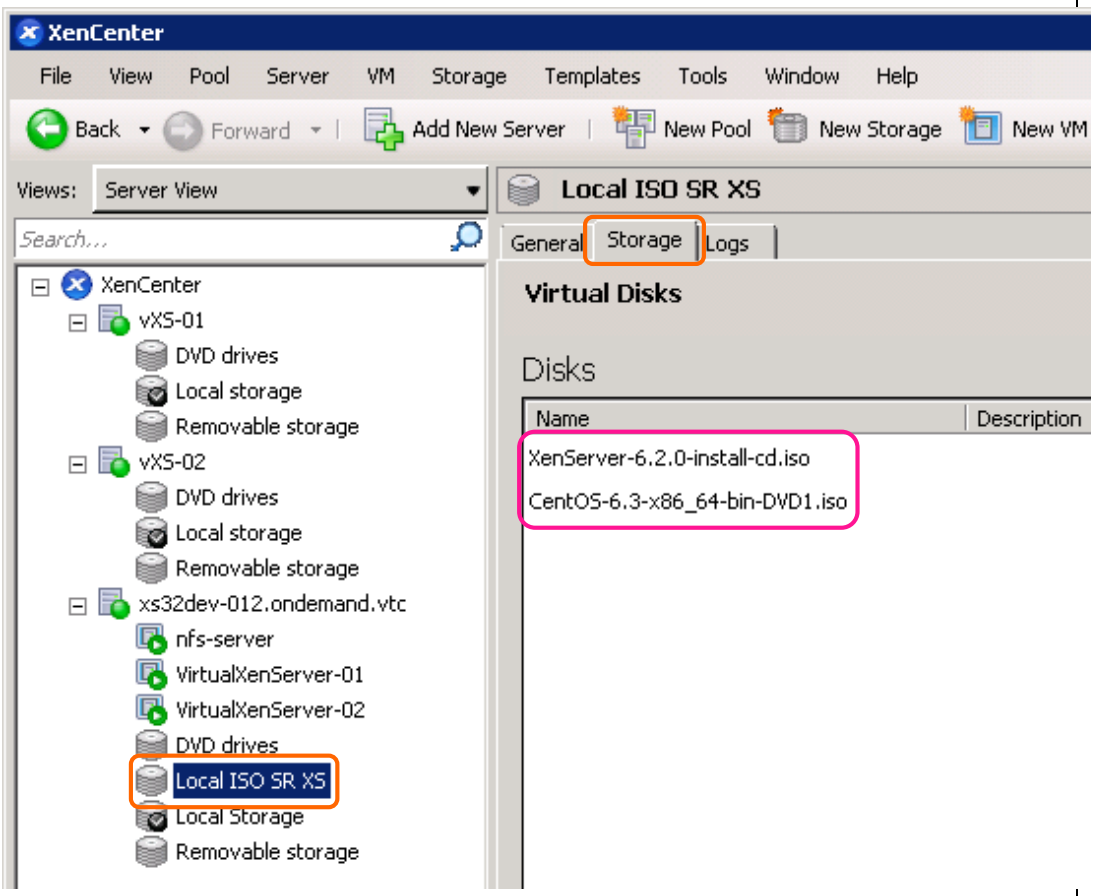
The CloudPlatform Management Server runs on a RedHat or CentOS operating system version 6.2 or above.

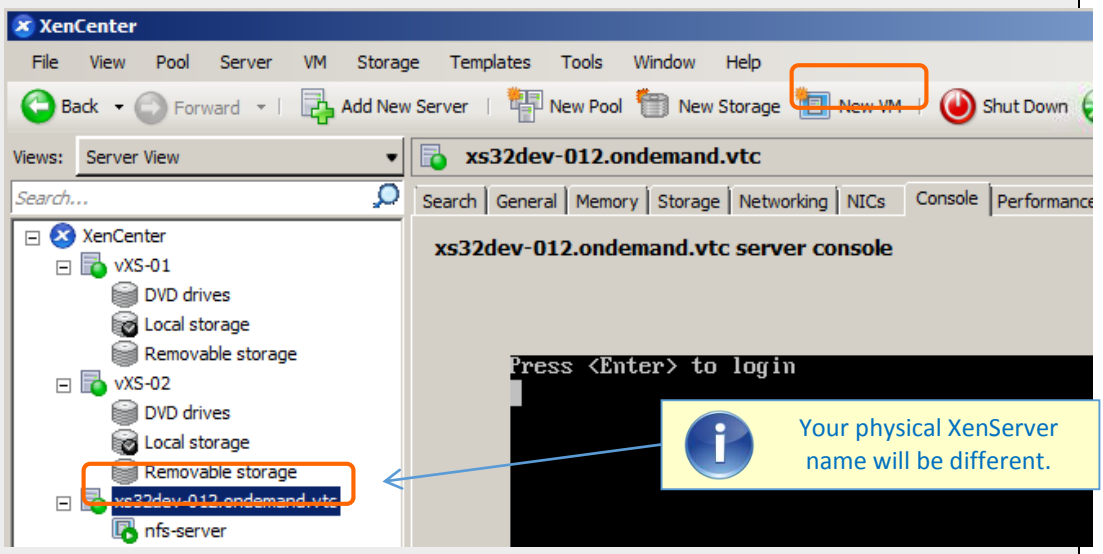
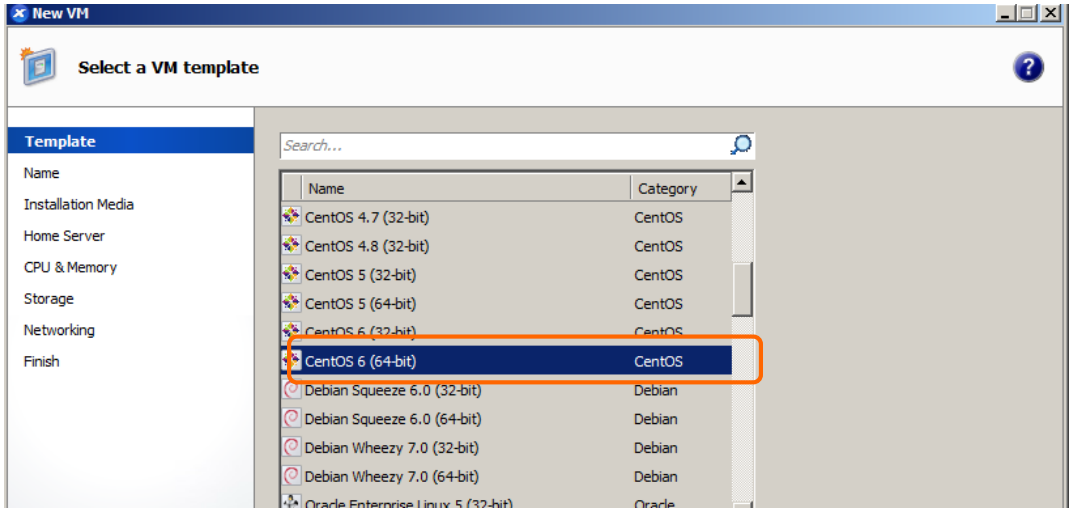
In this exercise you will:

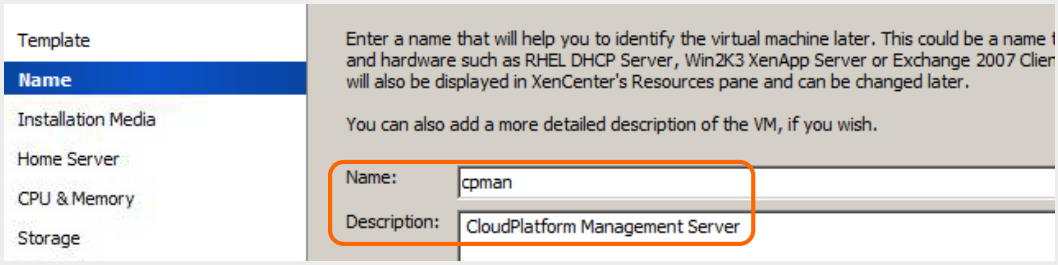
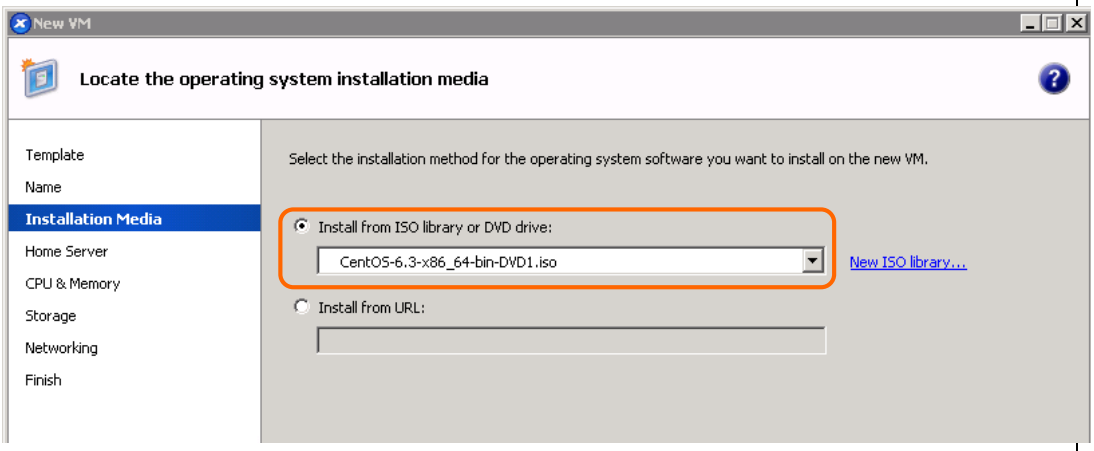
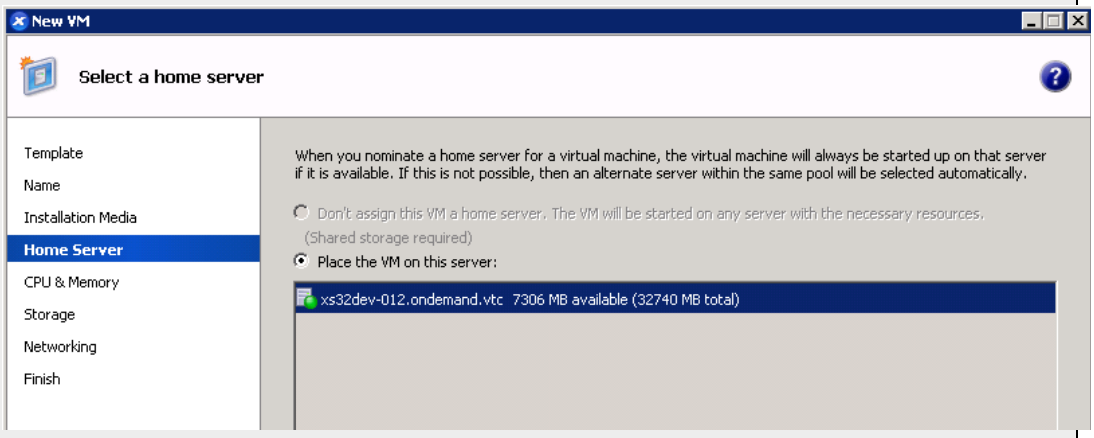
- Create a VM on your physical XenServer.
- Install the CentOS 6.3 operating system on to it.

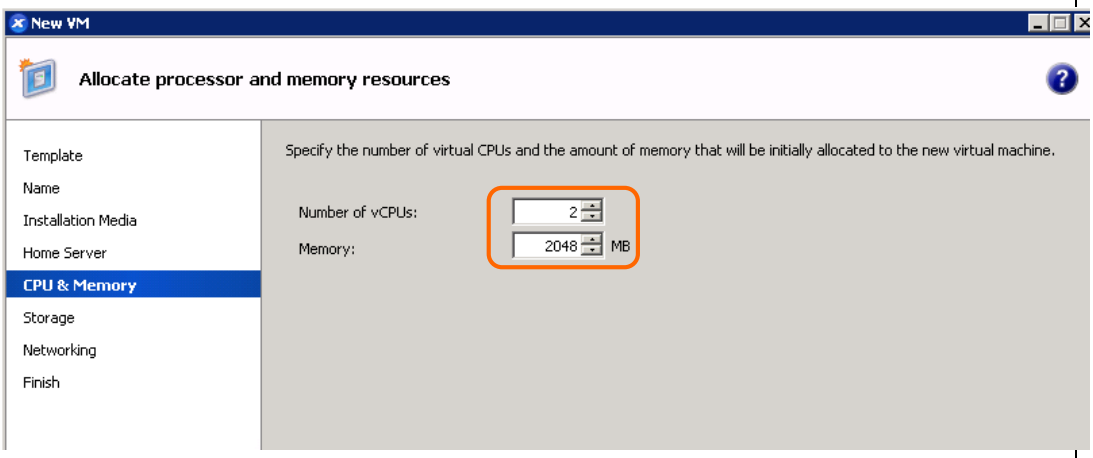
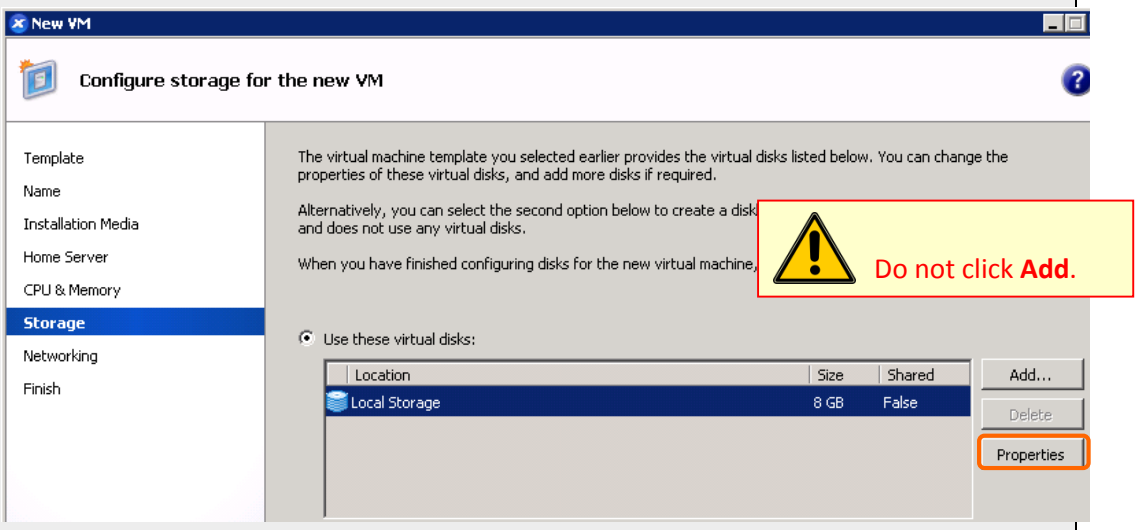
Step by step guidance

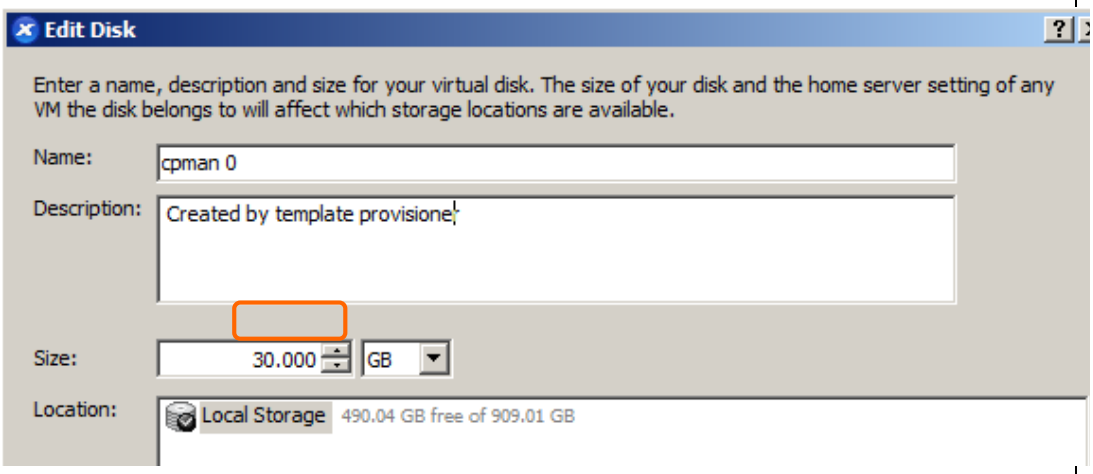
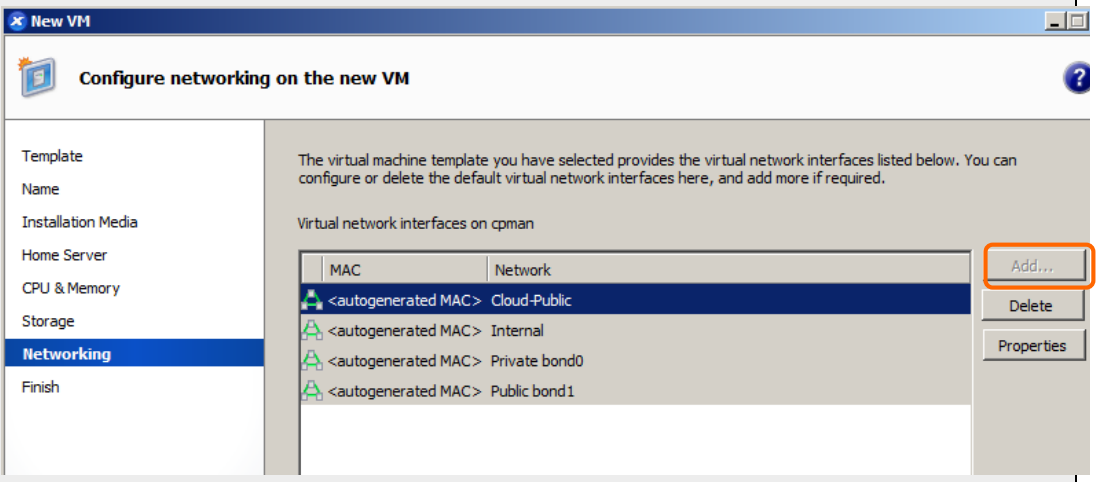
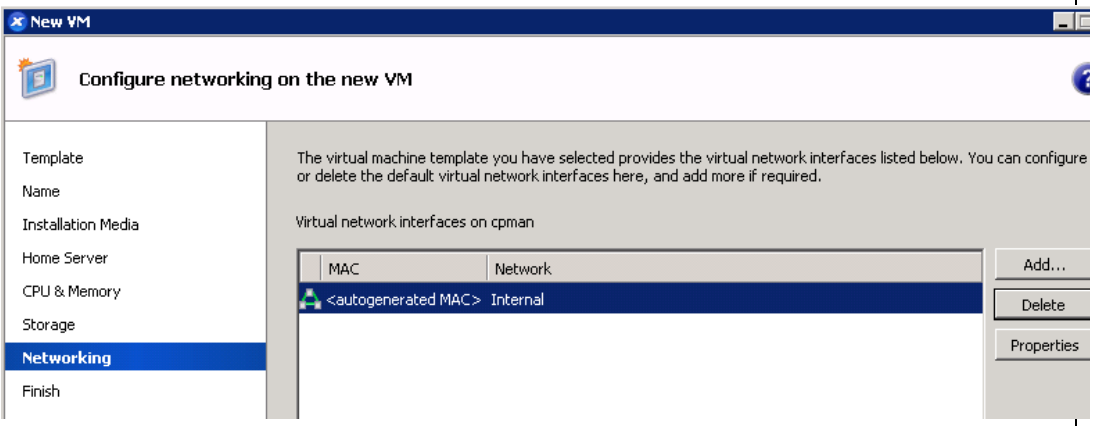
Estimated time to complete this exercise: 10 minutes.

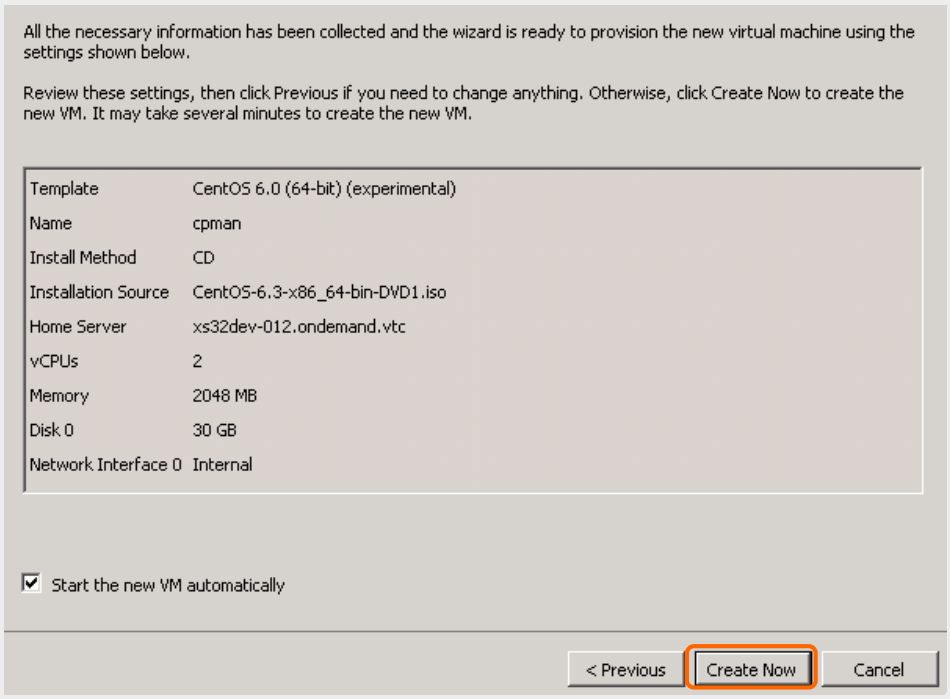
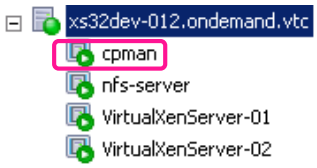
Step	Action
1.	Using XenCenter, ensure the CentOS 6.3 install DVD is available on the physical XenServer's local ISO Storage Repository.  Click the **Local ISO SR XS** node on the physical XenServer and select the **Storage** tab. You should see two ISO files here. These are the ISO files available on the local ISO Storage Repository and can be selected to be loaded into the XenServer's DVD drive for booting a VM and installing an operating system. If you don't see the two ISO files, click the **Rescan** button and they should appear.

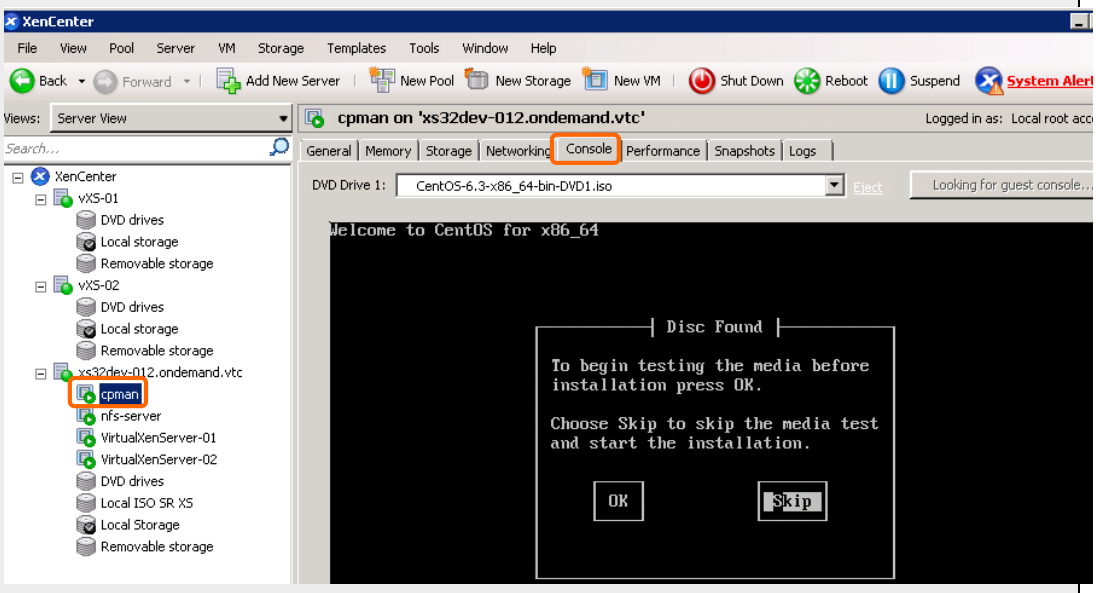
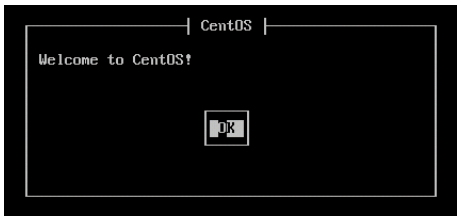
Step	Action
2.	 Select your physical XenServer node and click the **New VM** button.
3.	 You will be asked what VM template you want to use. Scroll down the list and select the **CentOS 6 (64-bit)** template. Click **Next**.

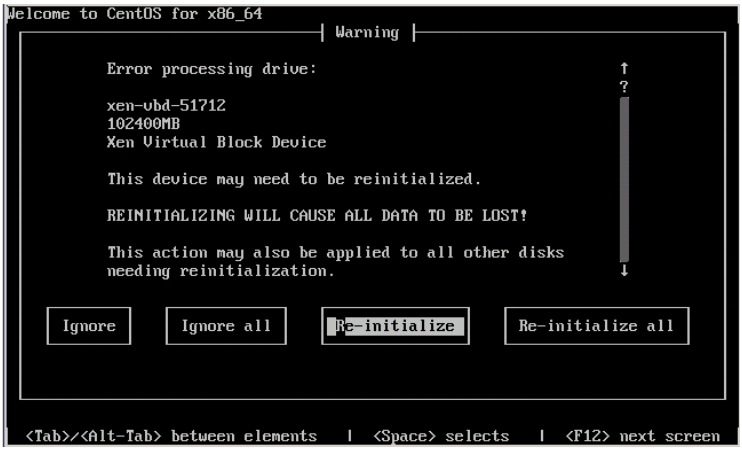
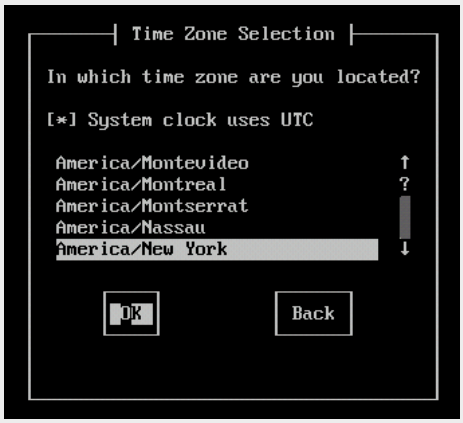
Step	Action
4.	Enter the name and description of the VM to be created: Name: `cpman` Description: `CloudPlatform Management Server`  Click **Next**.
5.	 Select the **CentOS-6.3-x86_64-bin-DVD1.iso** file as the installation media. Leave the **Advanced OS Boot parameters** at the default. Click **Next**.
6.	 Click **Next** to accept the default home server (your physical XenServer) to create the VM.

Step	Action
7.	 Next you will specify the amount of RAM and number of CPUs for the VM. Increase the **Number of vCPUs** to **2** and the **Memory** to **2048MB**, and then click **Next**.
8.	 You will increase the disk size from the default of 8GB. Click **Properties**.

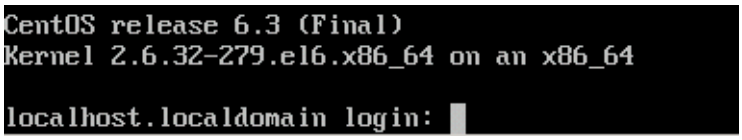
Step	Action
9.	 Change the disk size to **30GB**, click **OK** and then click **Next**.
10.	 Put the CloudPlatform Management Server on the same network as the rest of your infrastructure servers (e.g. XD controller, AD controller).
11.	 If your screen now looks like the one above, click **Next**.

Step	Action
12.	 Carefully confirm the settings you see match those shown above (except for the Home Server, which should be your physical XenServer name). Click **Create Now**.
13.	You will notice the status bar at the bottom of XenCenter shows the progress in creating the VM. Once the VM is created it will be shown in XenCenter as cpman. This VM will become the CloudPlatform Management server. 

Step	Action
14.	 Click the **cpman** node and the **Console** tab. Once the initial boot is completed, you should see the screen above. This is the console to your newly created VM. Adjust the size of the XenCenter window if necessary to show the whole of the console and click in the console to set focus. Use the **<Tab>** key to select **Skip** and then press **<Enter>.**
15.	Wait a few moments for the following screen to appear:  Press **<Enter>.**

Step	Action
16.	 Keep the language selection on **English**. Use the **<Tab>** key to select **OK** and then press **<Enter>.**
17.	 Use the **<Tab>** key to select **Re-initialize** and then press **<Enter>.**
18.	 Keep the time zone on **America/NewYork**. Use the **<Tab>** key to select **OK** and then press **<Enter>**.

Step	Action
19.	 Enter the root password twice: Password: **Citrix123** Password (confirm): **Citrix123** Passwords are case sensitive. Use the **<Tab>** key to select **OK** and then press **<Enter>**.
20.	 Use the **<Tab>** key to select **OK** and then press **<Enter>**.
21.	 Use the **<Tab>** key to select **Write changes to disk** and then press **<Enter>**.

Step	Action
22.	After a few minutes you should see the following: Press **<Enter>** to reboot.
23.	After the reboot, you should see the login prompt.  CentOS 6.3 has been installed on the cpman VM.

Exercise Summary

You have created a VM named cpman, and have installed the CentOS 6.3 operating system.

Exercise 2: Install XenServer Tools on the cpman VM

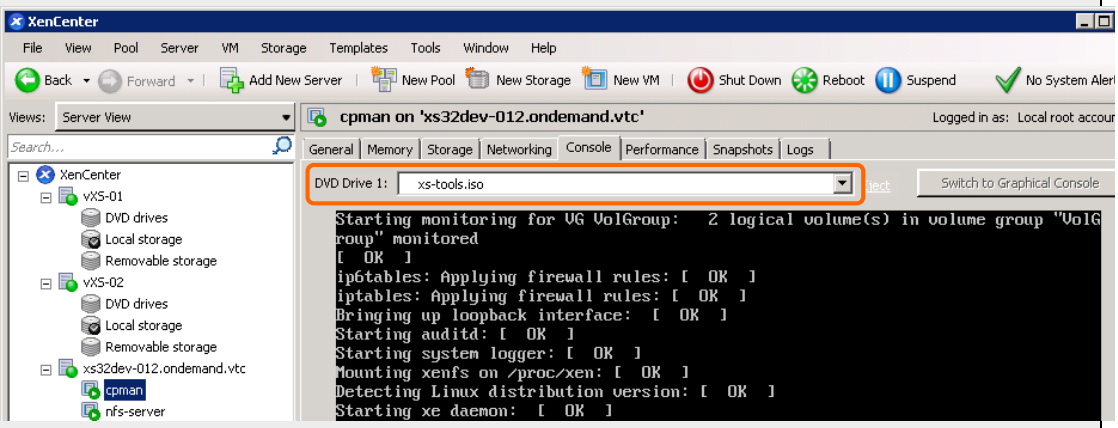
Overview

In this exercise you will:

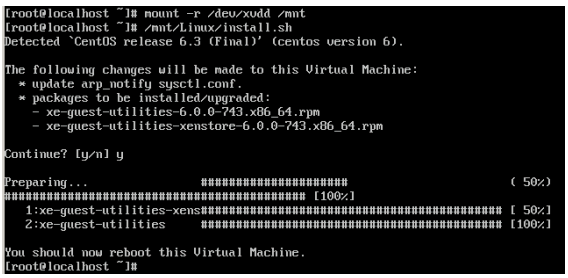
- Install XenServer tools on the cpman VM. This adds a XenServer agent that assists XenServer in monitoring and controlling the VM.

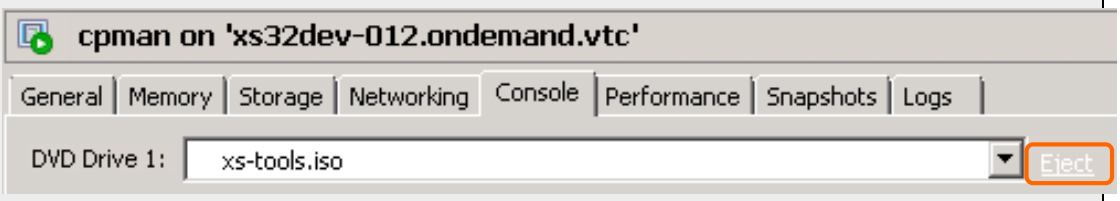
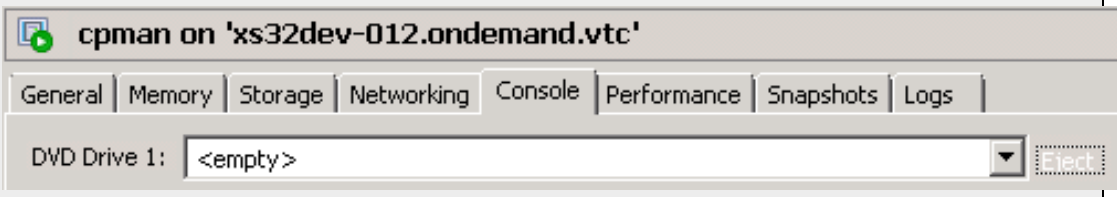
Step by step guidance

Estimated time to complete this exercise: 5 minutes.

Step	Action
1.	Login to the cpman console using the credentials: Username: **root** Password: **Citrix123**
2.	 Using the **DVD Drive 1** selector choose **xs-tools.iso**. Make sure you select the **xs-tools.iso** DVD before executing the next step.

Step	Action

3.	To install XenServer tools enter the following commands on the console:
	`mount -r /dev/xvdd /mnt`
	`/mnt/Linux/install.sh`
	Answer `y` **<Enter>** to the prompt.
	 
	To complete the installation, reboot the VM by entering the following command:
	`reboot`

4.	 Wait until cpman is in the process of booting and then click **Eject** to remove the XenServer tools DVD from the DVD drive. Ejecting a DVD when you no longer need it is a XenServer best practice.  The DVD drive should say **<empty>**.

Exercise Summary

You have installed the XenServer tools on to the cpman VM.

Exercise 3: Setup Networking on the cpman VM

Overview

In this exercise you will:

- Configure the networking of the CentOS VM you just created.

You will need to use the vi text editor for this exercise. If you are not familiar with how to use vi, the instructor provided cheat sheet will help you remember the commands needed, or, for more help, refer to Appendix 2 where you will get keystroke by keystroke instructions for editing the first file.

Step by step guidance

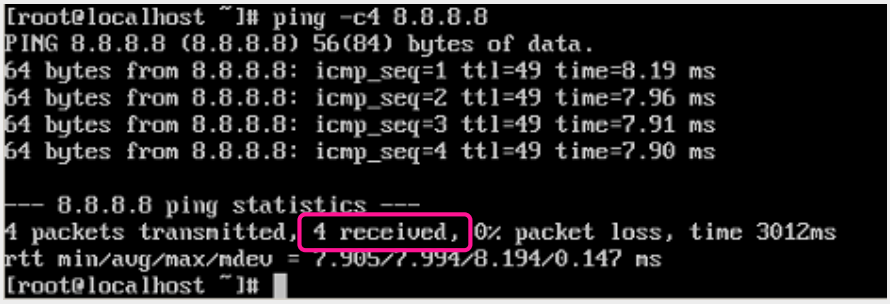
Estimated time to complete this exercise: 10 minutes.

Step	Action
1.	Login to the cpman console using the credentials: Username: **root** Password: **Citrix123**

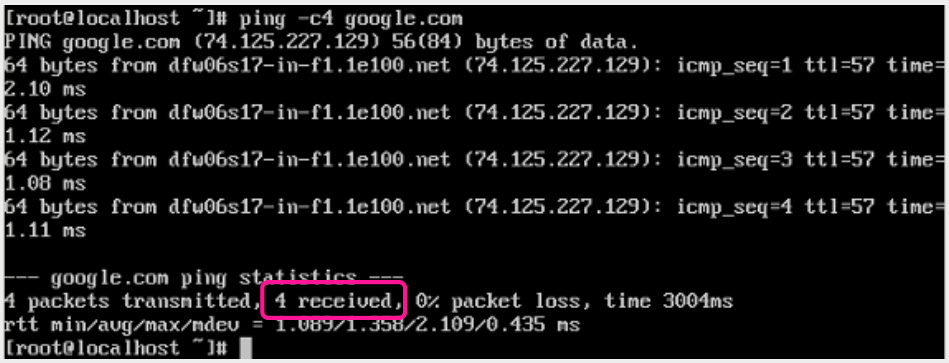
Step	Action

2.	The internal network specified when creating the VM is attached to the first NIC of the VM, which in Linux is referred to as “eth0”.
	
	You need to configure “eth0” by editing its configuration file with the command:
	
	`vi /etc/sysconfig/network-scripts/ifcfg-eth0`
	
	Delete the following two lines:
	
	`HWADDR="xx:xx:xx:xx:xxx"`
	`UUID="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"`
	
	Change the following lines:
	
	From: `BOOTPROTO="dhcp"` → To: `BOOTPROTO="none"`
	From: `ONBOOT="no"` → To: `ONBOOT="yes"`
	
	Add the following lines at the end of the file:
	
	`IPADDR=192.168.10.15`
	`NETMASK=255.255.255.0`
	`GATEWAY=192.168.10.1`
	
	Your IP details will be different from those shown in this guide.
	
	After editing, the file should look exactly like:
	
	`DEVICE="eth0"`
	`BOOTPROTO="none"`
	`NM_CONTROLLED="yes"`
	`ONBOOT="yes"`
	`TYPE="Ethernet"`
	`IPADDR=192.168.10.15`
	`NETMASK=255.255.255.0`
	`GATEWAY=192.168.10.1`
	
	Appendix 2 shows detailed step by step instructions on how to edit this file using the vi editor.
	
	Save the file and exit the editor by entering `<ESC>:wq`

3.	Restart the driver for the “eth0” NIC to read the new configuration by entering the following command:
	
	`ifup eth0`
	
	`[root@localhost ~]# ifup eth0`
	`[root@localhost ~]#`

Step	Action
4.	You can check the network is operational by pinging one of Google's internet DNS servers. `ping -c4 8.8.8.8`  Check ping packets were received.

5.	Edit the following file to point to a DNS server for this VM to use.
	
	`vi /etc/resolv.conf`
	
	The file should be empty; add the following line:
	
	`nameserver 192.168.10.10`
	
	Your IP details will be different from those shown in this guide. Use the DNS server on the AD controller if following the XDCCP cheat sheet.
	
	After editing, the file should look like:
	
	`nameserver 192.168.10.10`
	
	Save the file and exit the editor by entering `<ESC>:wq`

6.	Ping google.com to ensure name resolution is now operational. `ping -c4 google.com`  It may take a few seconds to start the ping. Check the ping packets were received.

Step	Action

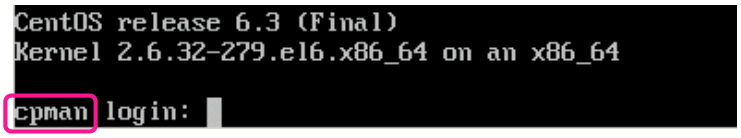
7.	Add the two VMs, cpman and nfs-server, to the local name resolution file.
	vi /etc/hosts
	Delete the 2nd line (starting with **::1 localhost**)
	Add the lines:
	127.0.0.1 cpman.cplab.local cpman
	192.168.10.12 nfs-server.cplab.local nfs-server
	After editing the file should look like:
	`127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4`
	`127.0.0.1 cpman.cplab.local cpman`
	`192.168.10.12 nfs-server.cplab.local nfs-server`
	Save the file and exit the editor by entering **<ESC>:wq**

8.	Verify local name resolution is working.
	ping -c4 nfs-server
	`[root@localhost ~]# ping -c4 nfs-server`
	`PING nfs-server.cplab.local (192.168.10.12) 56(84) bytes of data.`
	`64 bytes from nfs-server.cplab.local (192.168.10.12): icmp_seq=1 ttl=64 time=1.7`
	`6 ms`
	`64 bytes from nfs-server.cplab.local (192.168.10.12): icmp_seq=2 ttl=64 time=0.1`
	`16 ms`
	`64 bytes from nfs-server.cplab.local (192.168.10.12): icmp_seq=3 ttl=64 time=0.1`
	`27 ms`
	`64 bytes from nfs-server.cplab.local (192.168.10.12): icmp_seq=4 ttl=64 time=0.1`
	`14 ms`
	`--- nfs-server.cplab.local ping statistics ---`
	`4 packets transmitted, 4 received, 0% packet loss, time 3002ms`
	`rtt min/avg/max/mdev = 0.114/0.529/1.761/0.711 ms`
	`[root@localhost ~]#`
	Check ping packets were received.

9.	Edit the following file to change the hostname:
	vi /etc/sysconfig/network
	Change the hostname to cpman
	HOSTNAME=cpman
	After editing the file should look like:
	`NETWORKING=yes`
	`HOSTNAME=cpman`
	Save the file and exit the editor by entering **<ESC>:wq**

10.	Reboot the VM to get the new hostname registered. **reboot**

Your IP details will be different from those shown in this guide.

Step	Action
11.	 After the reboot has completed, notice the hostname.
12.	Login to the cpman console using the credentials: Username: **root** Password: **Citrix123** Check the hostname is fully qualified by entering the following command: **hostname -f** A fully qualified domain name specifies the host's exact location in the DNS tree hierarchy.

Exercise Summary

You have configured the network of the cpman VM.

Exercise 4: Configure the nfs-server VM

Overview

In this exercise you will:

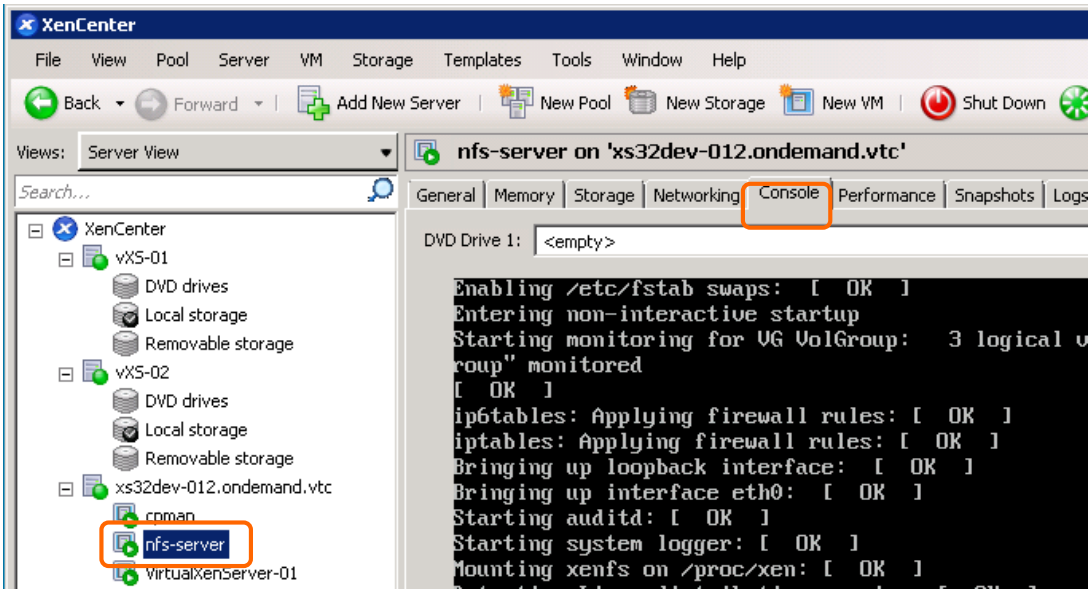
- Configure the CloudPlatform primary and secondary shared storage.

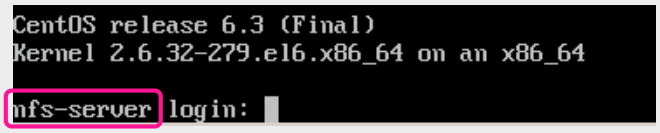
CloudPlatform requires shared storage for secondary storage and it is often also used for primary storage. While this would typically be provided by a physical storage device in the datacenter, for the lab, another CentOS based VM running on your physical XenServer will be used as an NFS server. Note: If you don't have a physical NFS server, you will need create one in the same way as in exercise 1-3.

A separate 250GB storage partition was created during the install of the NFS server to act as the primary and secondary shared storage for CloudPlatform. Keeping the OS and data partitions separate is a best practice for an NFS server like this. The partition is mounted on the `/nfs` mount point.

Step by step guidance

Estimated time to complete this exercise: 10 minutes.

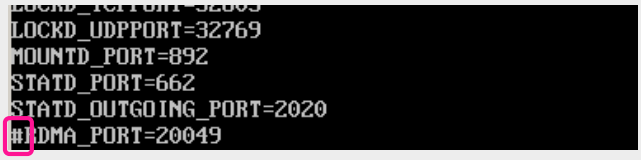
Step	Action
1.	Click the **nfs-server** node and then the **Console** tab to access the nfs-server VM console. Note: If you don't have a physical NFS server, you will need create one in the same way as in exercise 1-3 above. If you have one, skip to exercise 5. 

Step	Action
2.	Login to the nfs-server console using the credentials: Username: **root** Password: **Citrix123**  Make sure you are now on the **nfs-server** console.
3.	Install the NFS server components required by entering: `yum -y install nfs-utils`
4.	Setup NFS services to start on reboot. `chkconfig nfs on`

5.	Create directories on the storage partition to serve as the primary and secondary storage for two zones, Paris & London. Choose a directory on your NFS Server.
	
	`mkdir -p /nfs/paris/primary/cluster1`
	`mkdir -p /nfs/paris/secondary`

6.	Edit the NFS exports file to allow these directories to be shared.
	
	`vi /etc/exports`
	
	The file should be empty; add the following line (exactly as shown) to the file:
	
	`/nfs *(rw,async,no_root_squash)`
	
	After editing the file should look exactly like:
	
	`/nfs *(rw,async,no_root_squash)`
	
	Save the file and exit the editor by entering `<ESC>:wq`

7.	Edit the NFS configuration file to open various ports:
	
	`vi /etc/sysconfig/nfs`
	
	Uncomment the following lines in the file by deleting the ”#” at the beginning of each line:
	
	`#RQUOTAD_PORT=875`
	`#LOCKD_TCPPORT=32803`
	`#LOCKD_UDPPORT=32769`
	`#MOUNTD_PORT=892`
	`#STATD_PORT=662`
	`#STATD_OUTGOING_PORT=2020`
	
	Save the file and exit the editor by entering `<ESC>:wq`

Step	Action
8.	Enter the following command to verify the NFS configuration file has been edited correctly: `grep PORT /etc/sysconfig/nfs`  You should see only the last line (RDMA_PORT) is still commented.

Step	Action

9.	Configure the Linux firewall (iptables) ingress (inbound) and egress (outbound) rules to allow the NFS traffic by editing the iptables configuration file:
	
	`vi /etc/sysconfig/iptables`
	
	Add the following lines immediately after the 6th line (`OUTPUT ACCEPT`):
	
	`-A INPUT -m state --state NEW -p udp --dport 111 -j ACCEPT`
	`-A INPUT -m state --state NEW -p tcp --dport 111 -j ACCEPT`
	`-A INPUT -m state --state NEW -p tcp --dport 2049 -j ACCEPT`
	`-A INPUT -m state --state NEW -p tcp --dport 32803 -j ACCEPT`
	`-A INPUT -m state --state NEW -p udp --dport 32769 -j ACCEPT`
	`-A INPUT -m state --state NEW -p tcp --dport 892 -j ACCEPT`
	`-A INPUT -m state --state NEW -p udp --dport 892 -j ACCEPT`
	`-A INPUT -m state --state NEW -p tcp --dport 875 -j ACCEPT`
	`-A INPUT -m state --state NEW -p udp --dport 875 -j ACCEPT`
	`-A INPUT -m state --state NEW -p tcp --dport 662 -j ACCEPT`
	`-A INPUT -m state --state NEW -p udp --dport 662 -j ACCEPT`
	
	 It is highly recommended to copy and paste the above lines to ensure they are entered correctly.
	
	After editing the file should look like:
	
	`# Firewall configuration written by system-config-firewall`
	`# Manual customization of this file is not recommended.`
	`*filter`
	`:INPUT ACCEPT [0:0]`
	`:FORWARD ACCEPT [0:0]`
	`:OUTPUT ACCEPT [0:0]`
	`-A INPUT -m state --state NEW -p udp --dport 111 -j ACCEPT`
	`-A INPUT -m state --state NEW -p tcp --dport 111 -j ACCEPT`
	`-A INPUT -m state --state NEW -p tcp --dport 2049 -j ACCEPT`
	`-A INPUT -m state --state NEW -p tcp --dport 32803 -j ACCEPT`
	`-A INPUT -m state --state NEW -p udp --dport 32769 -j ACCEPT`
	`-A INPUT -m state --state NEW -p tcp --dport 892 -j ACCEPT`
	`-A INPUT -m state --state NEW -p udp --dport 892 -j ACCEPT`
	`-A INPUT -m state --state NEW -p tcp --dport 875 -j ACCEPT`
	`-A INPUT -m state --state NEW -p udp --dport 875 -j ACCEPT`
	`-A INPUT -m state --state NEW -p tcp --dport 662 -j ACCEPT`
	`-A INPUT -m state --state NEW -p udp --dport 662 -j ACCEPT`
	`-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT`
	`-A INPUT -p icmp -j ACCEPT`
	`-A INPUT -i lo -j ACCEPT`
	`-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT`
	`-A INPUT -j REJECT --reject-with icmp-host-prohibited`
	`-A FORWARD -j REJECT --reject-with icmp-host-prohibited`
	`COMMIT`
	
	Save the file and exit the editor by entering `<ESC>:wq`

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>10.</td><td>Specify the local NFS domain name in the following file:

vi /etc/idmapd.conf

Change the 5th line:

<table>
<tr><th>From</th><th>To</th></tr>
<tr><td>#Domain = local.domain.edu</td><td>Domain = cplab.local</td></tr>
</table>

Don’t forget to remove the “#” from the start of the line.

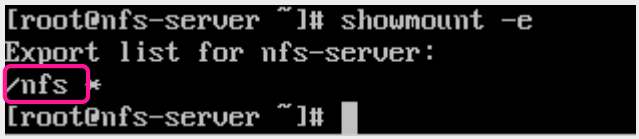
Save the file and exit the editor by entering <ESC>:wq</td></tr>
<tr><td>11.</td><td>Reboot by entering:

reboot</td></tr>
<tr><td>12.</td><td>Login to the nfs-server console using the credentials:

<table>
<tr><td>Username</td><td>root</td></tr>
<tr><td>Password</td><td>Citrix123</td></tr>
</table>

Check the /nfs directory is being exported by entering:

showmount -e

Notice the /nfs directory (containing the shared storage directories you created earlier), is in the export list.</td></tr>
</table>

Exercise Summary

You have configured the NFS server that CloudPlatform will use for primary and secondary storage.

Exercise 5: Configure NFS on the cpman VM

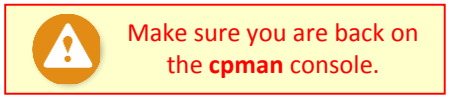
Overview

In this exercise you will:

- Configure the required NFS components on the CloudPlatform Management Server (cpman).
- Make some final infrastructure preparations.

Step by step guidance

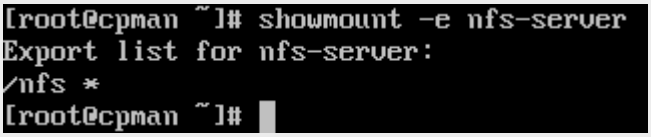
Estimated time to complete this exercise: 10 minutes.

Step	Action
1.	Switch back to the cpman console by clicking the **cpman** node. 
2.	Install the NFS components on cpman by entering: `yum -y install nfs-utils`

3.	Start essential NFS services:
	`service rpcbind start`
	`service nfslock start`
	`service nfs start`
	`chkconfig nfs on`

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>4.</td><td>Check the NFS server is accessible from cpman:

showmount -e nfs-server

 Use the hostname of your own NFS server

Notice nfs-server is accessible, and is exporting the /nfs directory.</td></tr>
<tr><td>5.</td><td>Linux access control, SELINUX, needs to be set to “permissive” for proper CloudPlatform installation and operation.

Enter the following command to set permissive mode:

setenforce permissive</td></tr>
<tr><td>6.</td><td>While the last command immediately sets permissive mode, it will not survive a reboot. Set SELINUX to permissive at boot time by editing the following file:

vi /etc/selinux/config

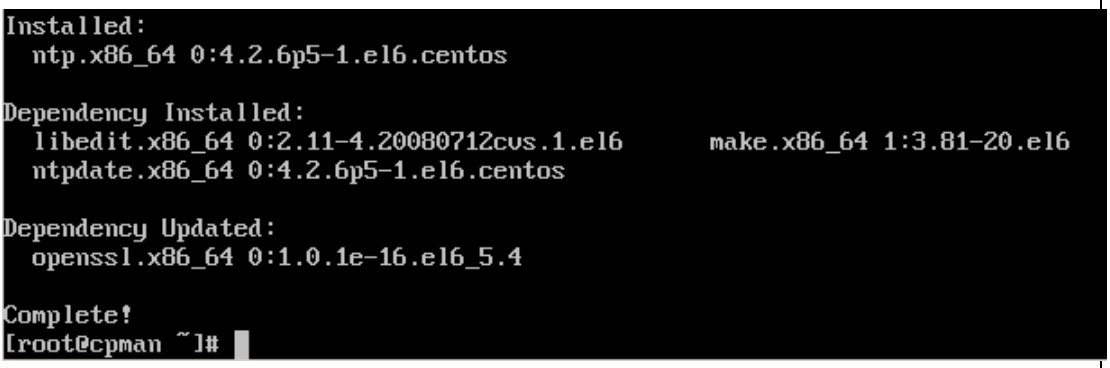
Change the 6th line:

<table>
<tr><th>From:</th><th>To:</th></tr>
<tr><td>SELINUX=enforcing</td><td>SELINUX=permissive</td></tr>
</table>

After editing, the file should look like:

<pre>
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these two values:
#   targeted - Targeted processes are protected,
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
</pre>

Save the file and exit the editor by entering <ESC>:wq</td></tr>
</table>

Step	Action
7.	Network Time Protocol (NTP) is required to synchronize the clocks of the servers in your cloud. The following command installs the NTP service on cpman. **yum -y install ntp** 
8.	Start the NTP client by entering the following command: **service ntpd start**
9.	Set NTP to start again upon reboot by entering the following command: **chkconfig ntpd on**
10.	The CloudPlatform installation is provided as a consolidated UNIX archive file known as a "TAR" file (short for Tape ARchive). TAR files can be obtained directly from web sites using the wget tool, but before you can use the tool, it must be installed. Enter the following command to install wget: **yum -y install wget** Once this tool is installed you are ready to install CloudPlatform.

Exercise Summary

You have installed and started the NFS services on cpman and configured several other services needed by CloudPlatform. You now have the entire infrastructure in place and are ready to install CloudPlatform.

Module 2

Install & Configure CloudPlatform

CloudPlatform is delivered as a TAR file (often called a “Tar Ball”). You can download the CloudPlatform install TAR file from the Citrix download site: http://www.citrix.com/downloads. To save time, the file has been placed on the Student Desktop web server for you. You will transfer the file directly from the web server onto the cpman VM using the “wget” tool. You will then use the file to install the CloudPlatform Management Server and CloudPlatform MySQL database.

Once the CloudPlatform software install is complete, the CloudPlatform System VM template file must be “seeded” for each of the zones to be built. The System template file is normally downloaded directly from the internet, but again, to save time the system VM template has been placed on the Student Desktop web server. You will run a script to download the template from the web server and install it into the secondary storage for the Paris zone. You will then repeat the seeding for the London zone secondary storage.

Exercises in this module

Exercise 1: Install CloudPlatform
Exercise 2: Prepare the System VM Template

If you are using this lab guide to install CloudPlatform in your own lab, see the notes at the end of exercises 1 & 2.

Exercise 1: Install CloudPlatform

Overview

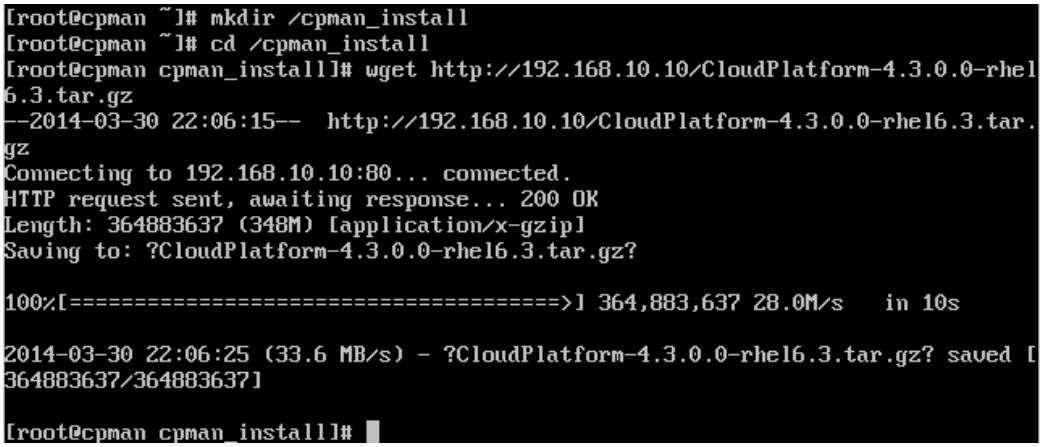
In this exercise you will:

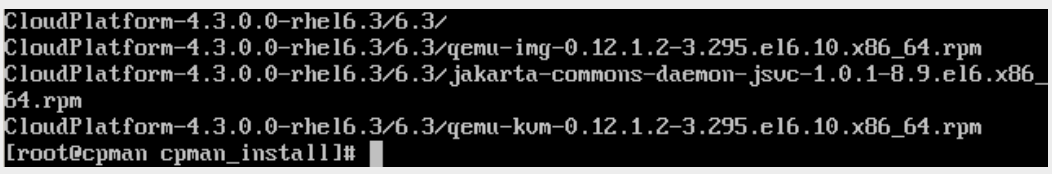
- Download the CloudPlatform Management Server software TAR file.
- Install the CloudPlatform Management Server software.

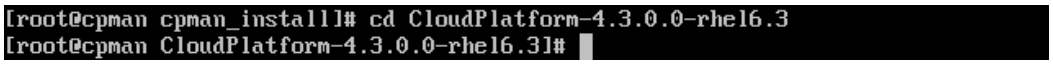
Step by step guidance

Estimated time to complete this exercise: 20 minutes.

Step	Action

1.	Download CloudPlatform from the internet and place the tarball on a local web server. You will create a directory to download the file into, and then use the "wget" tool to obtain the file. Software: www.citrix.com/products/cloudplatform/try
	
	Alternatively, you can also download the file and place it on the cpman server using a file copy utility such as WinSCP.
	
	Continuing on the **cpman** console, enter the following commands:
	
	`mkdir /cpman_install`
	`cd /cpman_install`
	`wget http://webserverurl/CloudPlatform-4.3.0.0-rhel6.3.tar.gz`
	
	 

2.	Use the tar tool to extract the contents of the installation file by entering the following command. `tar -xvf CloudPlatform-4.3.0.0-rhel6.3.tar.gz` 

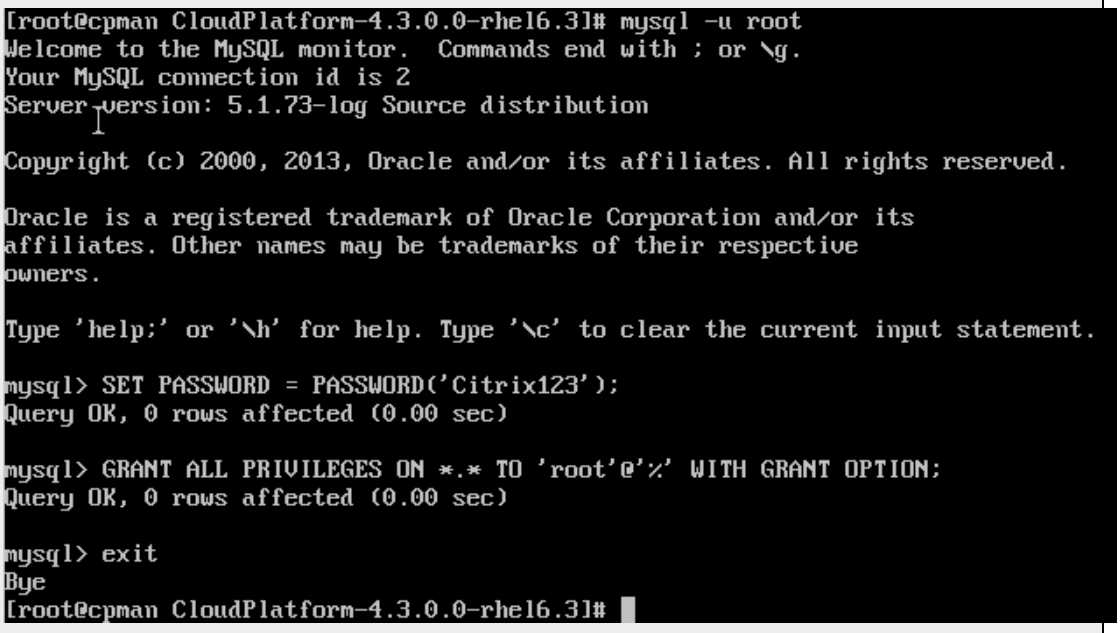
Step	Action
3.	Change directory to the CloudPlatform installation files directory. **cd CloudPlatform-4.3.0.0-rhel6.3** 
4.	Install the CloudPlatform Management Server by entering the command: **./install.sh --install-management**
5.	Install the MySQL database using the following command: **./install.sh** --install-database

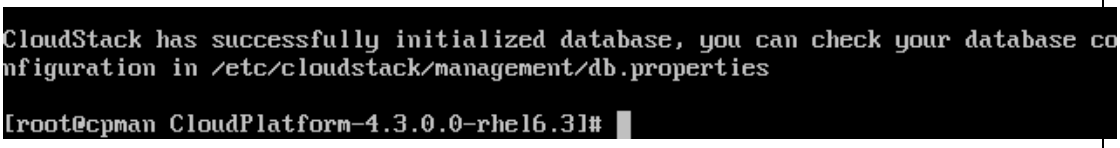
Step	Action

6.	Edit the MySQL configuration file to change some of the default configuration parameters required by CloudPlatform.
	
	`vi /etc/my.cnf`
	
	Add the following lines after the 2nd line (datadir=):
	
	`innodb_rollback_on_timeout=1`
	`innodb_lock_wait_timeout=600`
	`max_connections=350`
	`log-bin=mysql-bin`
	`binlog-format = 'ROW'`
	
	After editing, the file should look like:
	
	`[mysqld]`
	`datadir=/var/lib/mysql`
	`innodb_rollback_on_timeout=1`
	`innodb_lock_wait_timeout=600`
	`max_connections=350`
	`log-bin=mysql-bin`
	`binlog-format = 'ROW'`
	`socket=/var/lib/mysql/mysql.sock`
	`user=mysql`
	`# Disabling symbolic-links is recommended to prevent security risks`
	`symbolic-links=0`
	
	`[mysqld_safe]`
	`log-error=/var/log/mysqld.log`
	`pid-file=/var/run/mysqld/mysqld.pid`
	
	Save the file and exit the editor by entering `<ESC>:wq`
	
	The max_connections parameter should be set to 350 multiplied by the number of Management Servers you are deploying.

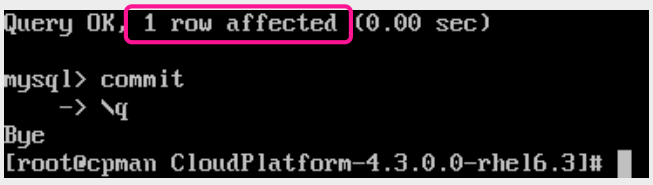
7.	Restart the MySQL service to re-read the updated configuration file by entering:
	
	`service mysqld restart`
	
	`[root@cpman CloudPlatform-4.3.0.0-rhel6.3]# service mysqld restart`
	`Stopping mysqld:  [  OK  ]`
	`Starting mysqld:  [  OK  ]`
	`[root@cpman CloudPlatform-4.3.0.0-rhel6.3]#`

Step	Action

8.	Set the MySQL database root password to “Citrix123” by entering:
	`mysql -u root`
	`SET PASSWORD = PASSWORD('Citrix123');`
	`GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' WITH GRANT OPTION;`
	`exit`
	 

9.	Setup the CloudPlatform database schema in the MySQL database by entering: `cloudstack-setup-databases cloud:cloud@localhost --deploy-as=root:Citrix123`  The CloudPlatform database is setup with username:cloud and password:cloud.

Step	Action

10.	The virtual XenServers used as hosts in the lab do not have Hardware Virtual Machine (HVM) capability like a physical CPU does. This means they are only able to run fully paravirtualized operating systems such as some versions of Linux (for example RedHat or CentOS).
	
	By default, CloudPlatform checks the host for HVM capability and will reject any host that does not have it. For the lab you must override the HVM check to allow the virtual XenServers to be used. This step is only required in the lab and would not be required with physical XenServers.
	
	Enter the following four commands (the INSERT command that is shown below on four lines, is all one line):
	
	`mysql -u root --password=Citrix123`
	`INSERT INTO `cloud`.`configuration` (`category`, `instance`, `component`, `name`,`value`, `description`) VALUES ('Advanced', 'DEFAULT', 'management-server','xen.check.hvm', 'false', 'Should we allow only the XenServers support HVM');`
	`commit`
	`\q`
	
	You can copy and paste all four commands together.
	
	 
	
	Check you see one row in the database was updated.

11.	Complete the setup of the CloudPlatform Management Server by entering the command: `cloudstack-setup-management` This completes the setup of the cpman server.

Note on Installing CloudPlatform outside of this lab environment

To speed up the install process for the lab, the CloudPlatform install file was placed on your Student Desktop web server, and the command in step one of this exercise retrieved the file from there. To install CloudPlatform outside of this lab environment, the CloudPlatform install TAR file should be downloaded from the Citrix web site

(http://www.citrix.com/downloads) and then transferred from the download location to the cpman VM using ftp or wget. Note that the TAR filename will change depending on the version of CloudPlatform and the commands in steps 2 & 3 would change accordingly.

Exercise Summary

You have downloaded, installed and configured the CloudPlatform Management Server.

Exercise 2: Prepare the System VM Template

Overview

CloudPlatform secondary storage is the storage used for all CloudPlatform VM templates for the zone, as well as snapshots and ISO images.

In this exercise you will:

- Seed secondary storage with the system VM template using the template installation script.

The system VM template will be used to create all CloudPlatform system VMs (system Virtual Routers, system Console Proxy VMs and system Storage transfer VMs) in the zone. Each zone has its own secondary storage so each zone's secondary storage must be separately seeded with the system template. It is not possible to simply copy the template from the secondary storage of one zone to the secondary storage of another zone. The install script also seeds the CloudPlatform database, so the script must be used on each zone separately.

Note about long and complex CLI commands

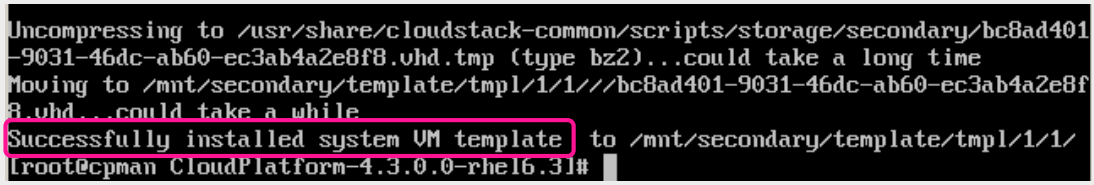
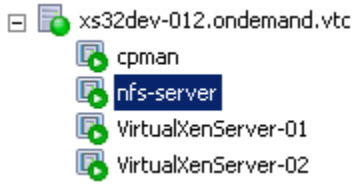
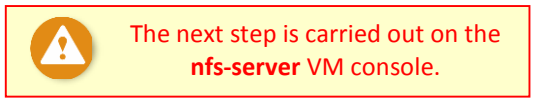
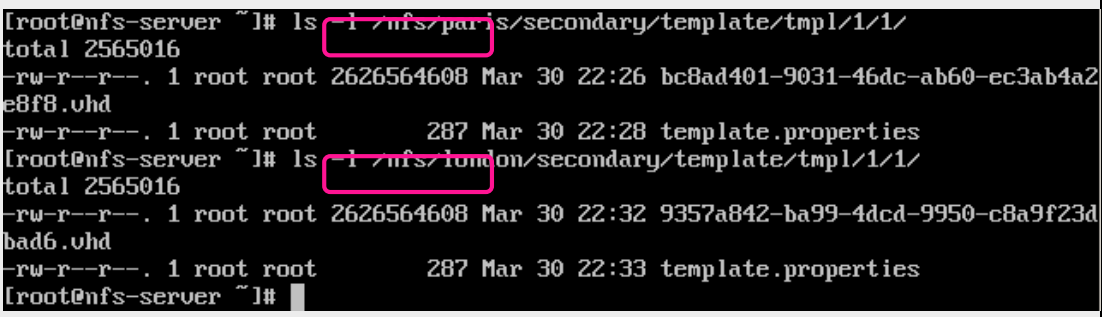
Several CLI commands in this exercise are long and complex. The commands are intended to be copied & then pasted into the cpman VM console to ensure the commands are entered accurately. When you paste the command ensure that the command pasted is the complete command from the lab guide. If you experience difficulty pasting, use a text editor on your laptop desktop as an intermediary, checking and reforming the command if necessary.

Step by step guidance

Estimated time to complete this exercise: 10 minutes.

Step	Action

1.	Continuing on the cpman console, mount the NFS secondary storage for the Paris zone with the following two commands (choose the path to your Secondary Storage NFS share):
	`mkdir -p /mnt/secondary`
	`mount -t nfs -o vers=3 nfs-server.cplab.local:/nfs/paris/secondary /mnt/secondary`

Step	Action
2.	Install the CloudPlatform system VM template by entering the following command (it's all one command): `/usr/share/cloudstack-common/scripts/storage/secondary/cloud-install-sys-tmplt -m /mnt/secondary/ -u \ download.cloud.com/templates/4.3/systemvm64template-2014-01-14-master-xen.vhd.bz2 -h xenserver` The template will be downloaded and installed. This will take several minutes.  Check for the "Successfully installed" message.
3.	Left blank. Not relevant outside CCP Lab
4.	**Left blank. Not relevant outside CCP Lab**
5.	To verify both secondary storage zones have been seeded correctly, change to the **nfs-server console**.   Login if necessary: Username: **root** Password: **Citrix123**
6.	Enter the following command: `ls -l /nfs/paris/secondary/template/tmpl/1/1/`  The two zones, Paris & London, have been seeded with the system VM template VHD file. Each template is about 2 ½ GB in size.

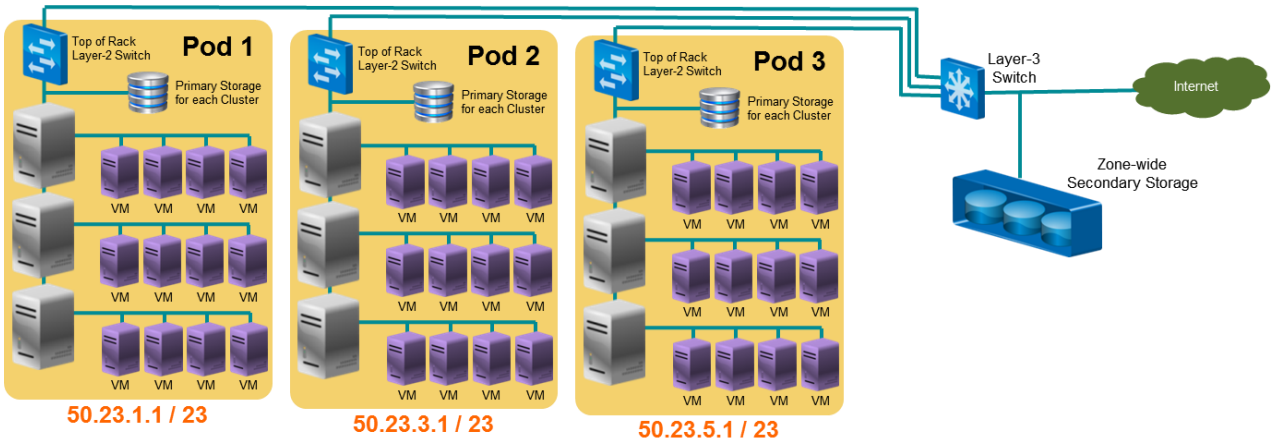
Exercise Summary

You have now seeded the CloudPlatform system templates for the London and Paris zones. CloudPlatform is now installed, configured and ready to build a cloud.

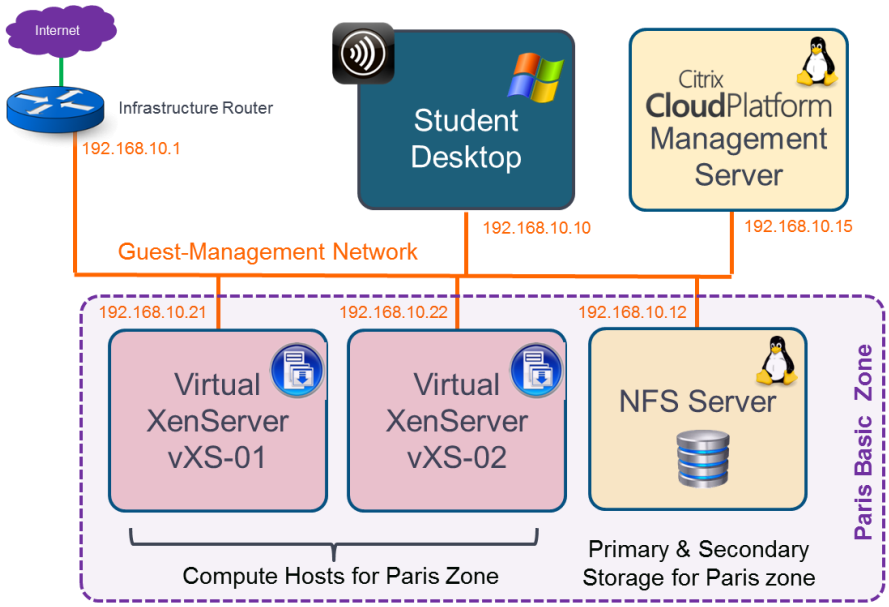
Module 3

Build a Basic Networking Zone

All the Guest VMs throughout a Basic Networking zone share a single flat network, with every Guest VM having a unique IP address assigned from the Guest IP range. Zones are built with Pods, with each Pod consisting of Clusters of Hosts and Primary Storage. Each Pod is on its own management subnet range and contains a dedicated Guest IP range, so this allows a Basic zone to be scaled horizontally by simply adding more Pods.



In this module you will build a Basic Networking zone cloud by creating your first Pod. The diagram below shows the physical networking of the lab infrastructure for the Paris Basic zone. The Paris zone components are shown in the purple dotted area.



Exercises in this module

Exercise 1: Create a XenServer Resource Pool

Exercise 1: Create a XenServer Resource Pool

Overview

When adding multiple XenServer hosts to the same CloudPlatform cluster, the XenServers must already be bound into a “Resource Pool”.

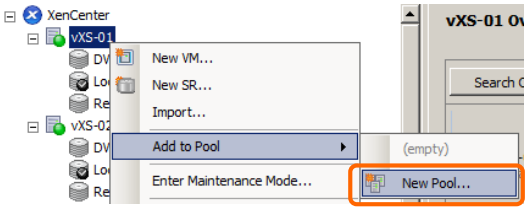
In this exercise you will:

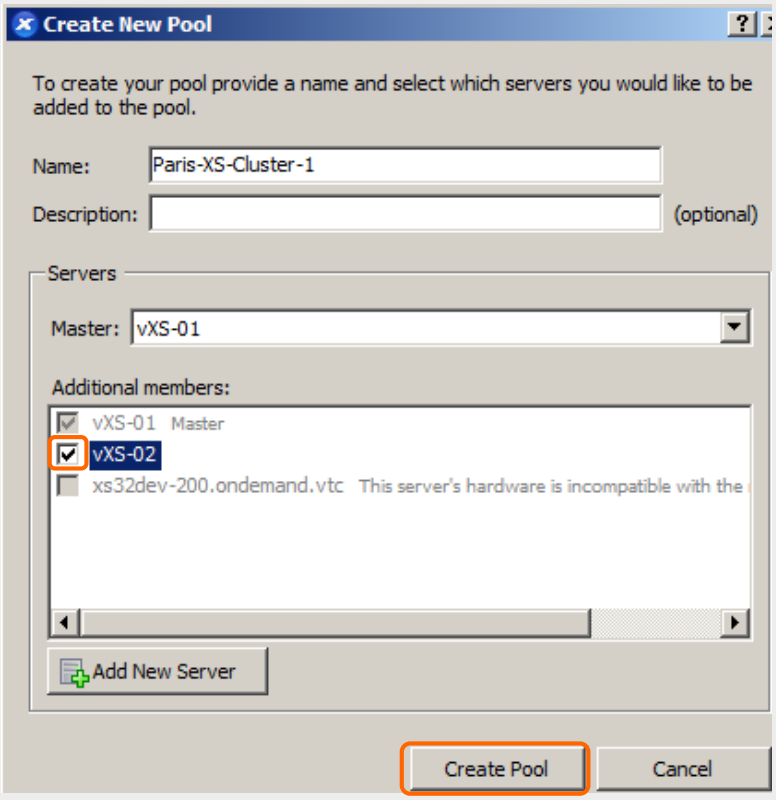
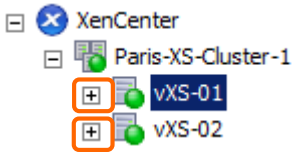
- Create a XenServer pool consisting of two virtual XenServers.

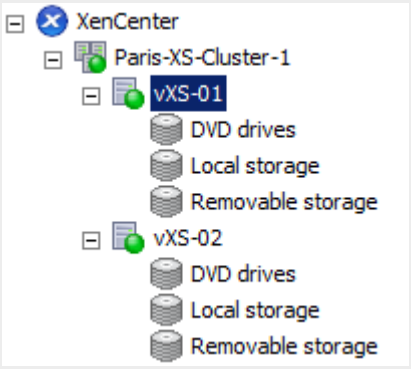
Note: Perform this step on your physical XenServers. The vXS-01/vXS-02 XenServer names are left in for reference.

Step by step guidance

Estimated time to complete this exercise: 5 minutes.

Step	Action
1.	 Using XenCenter, right-click the **vXS-01** node, select **Add to Pool** and then click **New Pool**.

Step	Action
2.	Enter the pool name: Name: **Paris-XS-Cluster-1**  Check **vXS-02** and click **Create Pool**.
3.	It takes 15 seconds or so to form the Paris-XS-Cluster-1 resource pool consisting of vXS-01 and vXS-02. XenCenter always lists the "Pool Master" server first (vXS-01).  Expand the vXS-01 and vXS-02 nodes by clicking the ⊞ on both nodes.

Step	Action
4.	 You will now be able to monitor changes to the virtual XenServers when the host XenServer Resource Pool is assimilated into CloudPlatform in the next exercise.

Exercise Summary

You have now created a XenServer Resource Pool consisting of two XenServers to provide the compute resources for your cloud's Basic zone.

Exercise 2: Build a Basic Zone

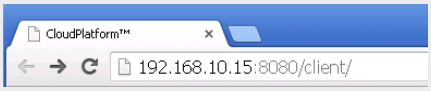
Overview

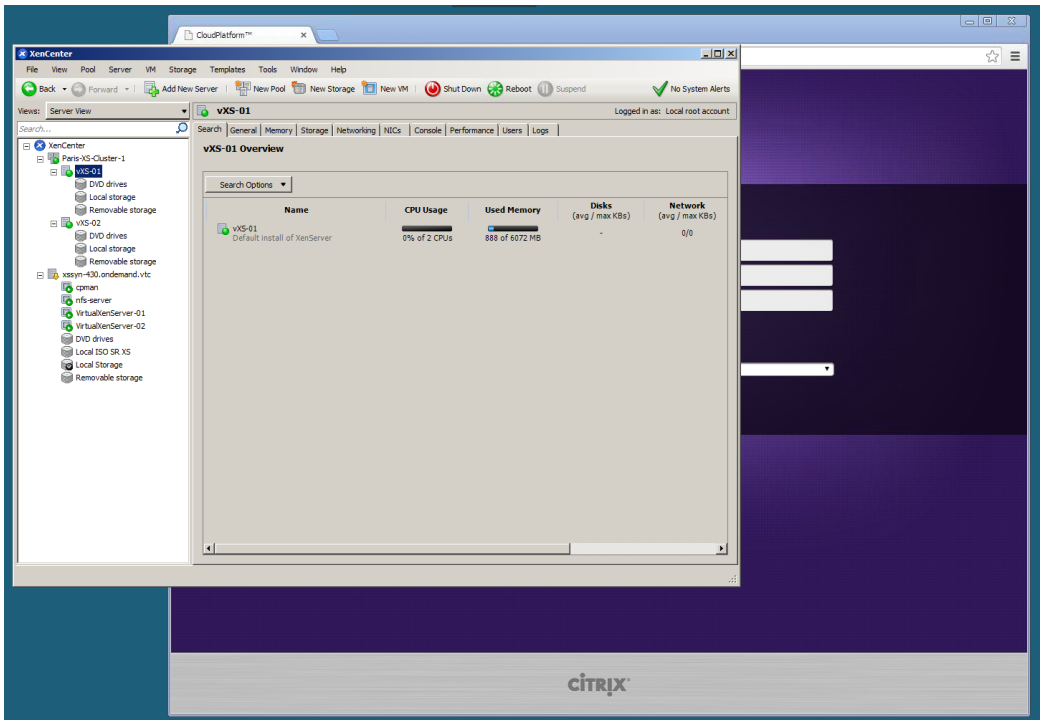
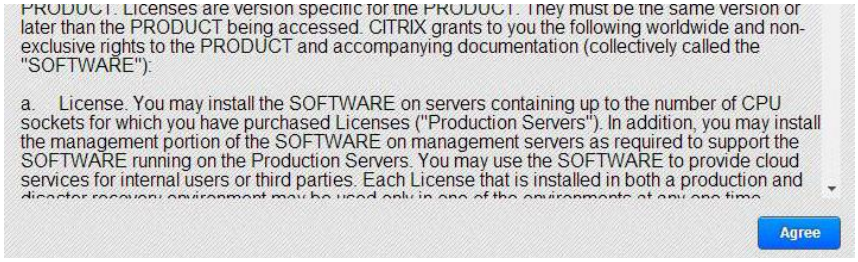
In this exercise you will:

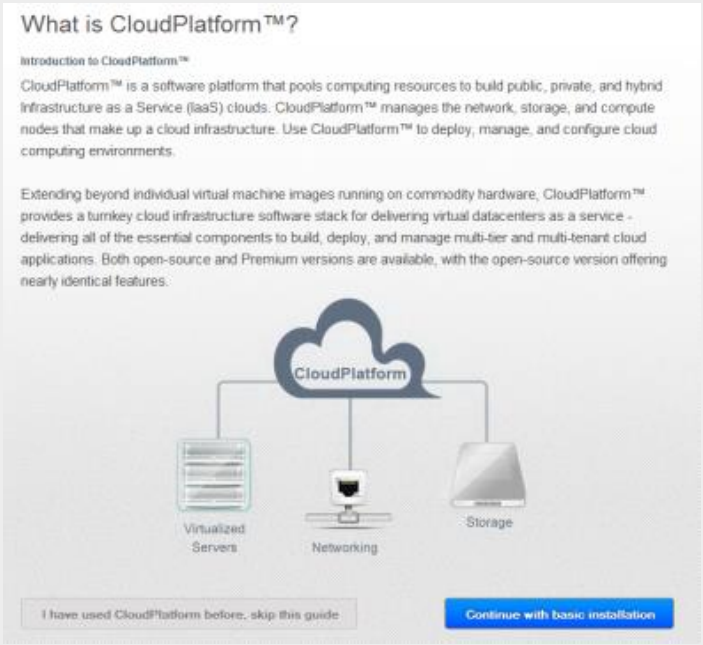
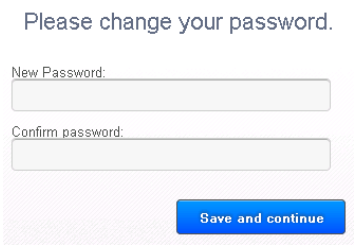
- Build your first cloud by creating a Basic zone using the CloudPlatform GUI.

Step by step guidance

Estimated time to complete this exercise: 35 minutes.

Step	Action
1.	On the Student Desktop (not your laptop), start the CloudPlatform Management server GUI by launching the **Chrome** browser
2.	Enter the following URL: `http://192.168.10.15:8080/client`  Use the IP address of your CPMAN server here.

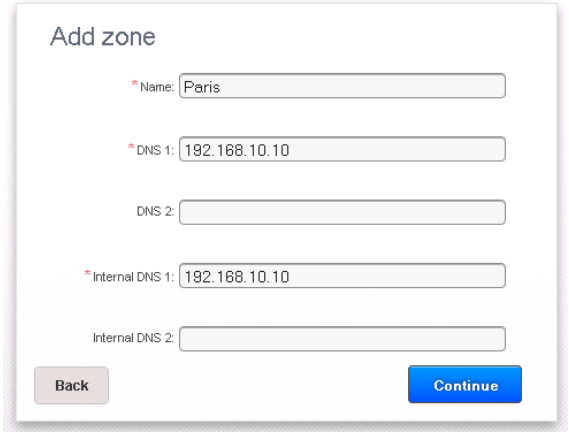
Step	Action
3.	Arrange your desktop with your browser overlapping XenCenter as shown. This will allow you to monitor the changes to the virtual XenServers as the cloud is built and VMs are started. Note that there is no requirement to use XenCenter to monitor the cloud building; it is simply used in the lab to increase understanding of what's going on behind the scenes, 
4.	Login to the CloudPlatform GUI using the following credentials: Username: **admin** Password: **password** Domain: Leave Blank Click **Login**.
5.	 Accept the license agreement by clicking **Agree** at the very bottom of the page.

Step	Action
6.	 Click **Continue with basic installation**.
7.	 Please change the password by entering: New Password: `Citrix123` Confirm Password: `Citrix123` Click **Save and Continue**.
8.	 Click **OK**.

Step	Action
9.	To start creating a zone, CloudPlatform needs to know the zone name and the DNS addresses the Guest VMs and System VMs should use. Enter the following:

Name	**Paris**	The zone name
DNS 1	**192.168.10.10**	DNS the Guest VMs will use
DNS 2	Leave Blank	
Internal DNS 1	**192.168.10.10**	DNS the System VMs will use
Internal DNS 2	Leave Blank	

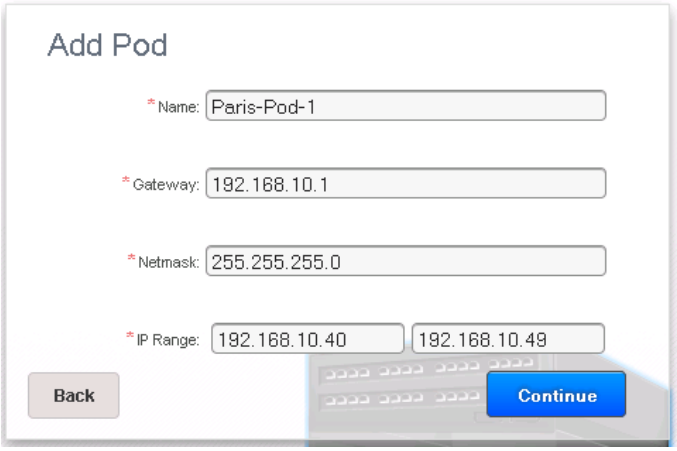
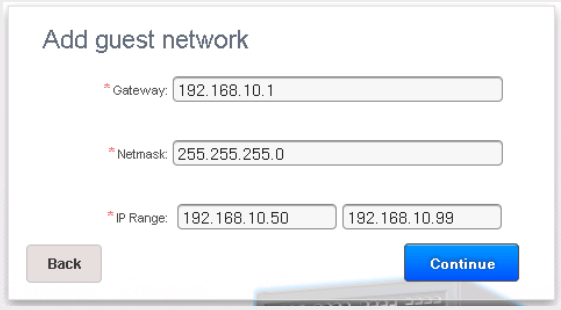
The Guest VMs usually have unrestricted internet access so are able to use external DNS, but it's not uncommon for the System VM's access to the internet being restricted, hence a separate internal DNS can be used. In the lab, the Student Desktop VM acts as the DNS for both the Guest & System VMs.

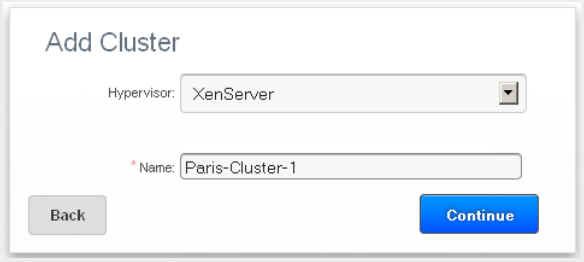
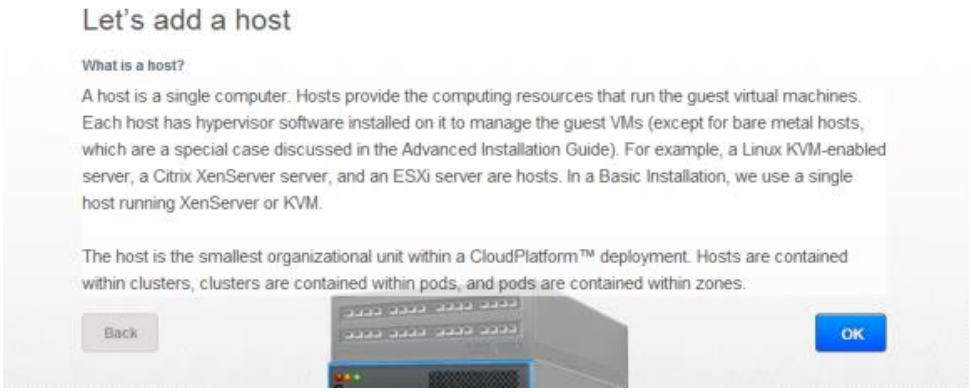


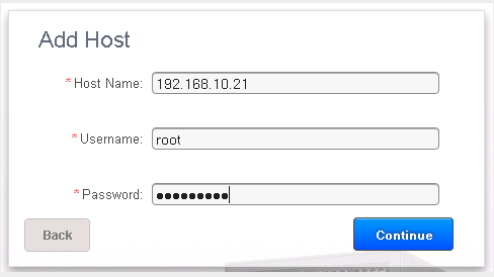
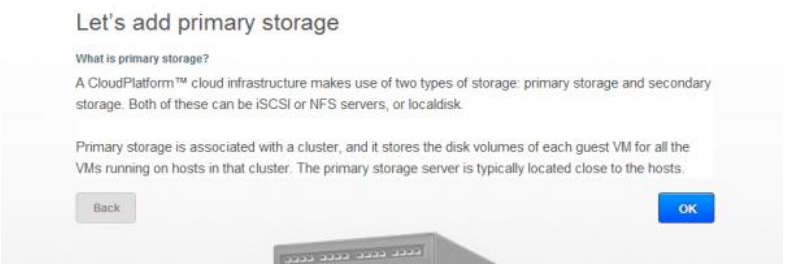
Click **Continue**.

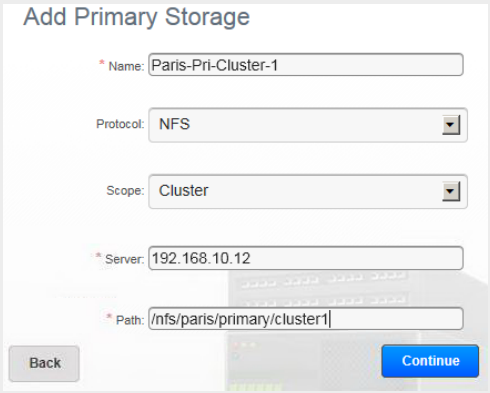
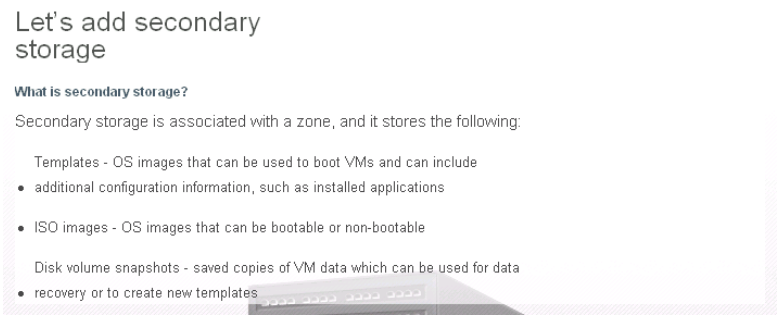
10.	

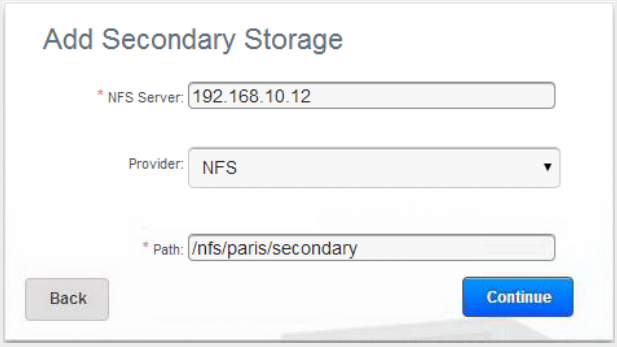
Click **OK**.

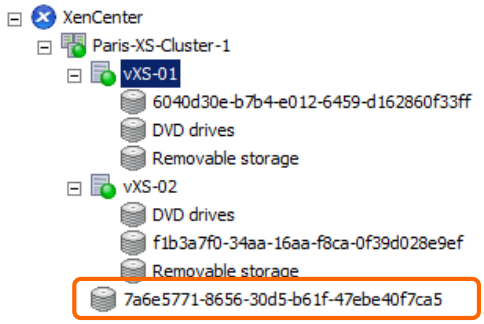
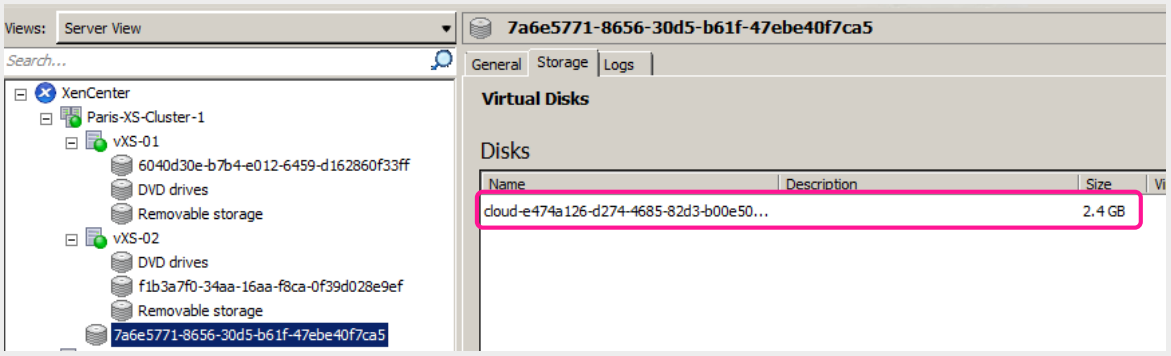
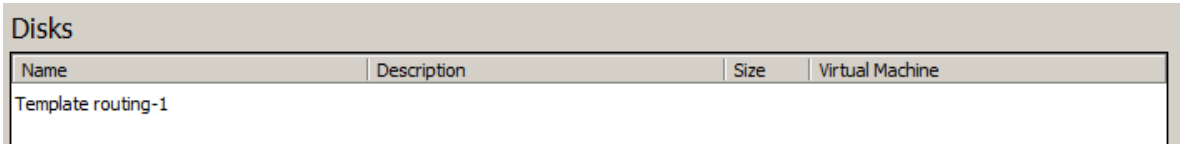
Step	Action
11.	A pod is usually a rack of servers. In this dialog you must specify a name for the pod and the range of IP addresses to be used by CloudPlatform's System VMs. Enter the following parameters: **Name** — `Paris-Pod-1` — The pod name **Gateway** — `192.168.10.1` — Gateway the compute hosts will use **Netmask** — `255.255.255.0` — Netmask the compute hosts will use **IP range** — `192.168.10.40` `192.168.10.49` — IP Range the system VMs will use The IP address of each System VM (Secondary Storage, Console Proxy and Virtual Router) will be assigned from the IP range entered above. The range must belong to the same subnet as the compute hosts (vXS-01 & vXS-02).  Click **Continue**.
12.	To specify the Guest network parameters for this pod enter the following parameters: **Gateway** — `192.168.10.1` — Gateway the Guest VMs will use **Netmask** — `255.255.255.0` — Netmask the Guest VMs will use **IP range** — `192.168.10.50` `192.168.10.99` — IP Range the Guest VMs will use The IP address of each Guest VM will be assigned from the IP range entered above. The IP range for the Guest VMs should be in the same network subnet (CIDR) as the pod.  Best practice is to separate the System VMs and Guest VMs on separate subnets, but for simplicity you will use the same subnet for these VMs in the lab. Click **Continue**.

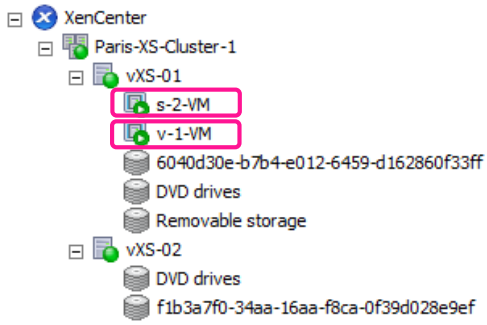
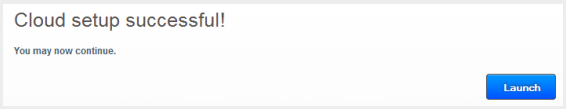
Step	Action
13.	 Click **OK**.
14.	Each pod contains one or more clusters. A cluster provides a way to group hosts. All hosts in a cluster must have identical hardware and run the same hypervisor. Ensure XenServer is selected as the hypervisor and enter the name as shown below: Hypervisor: XenServer Name: **Paris-Cluster-1**  Click **Continue**.
15.	 Click **OK**.

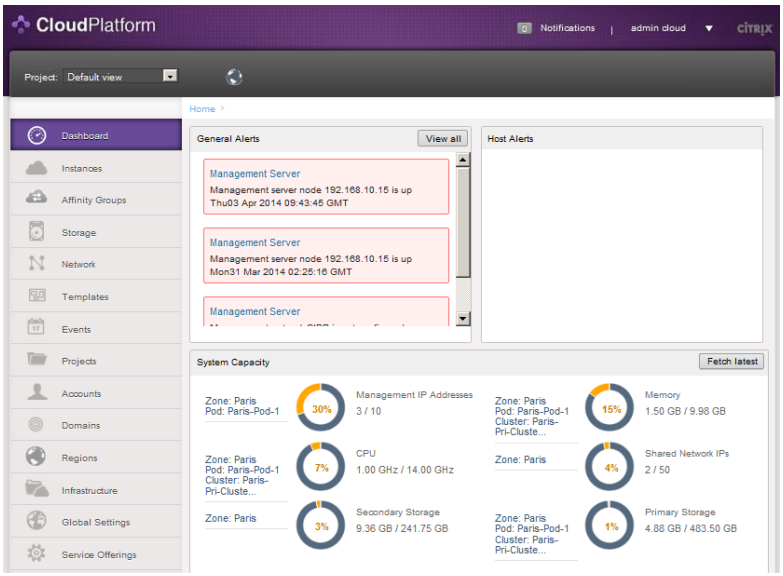
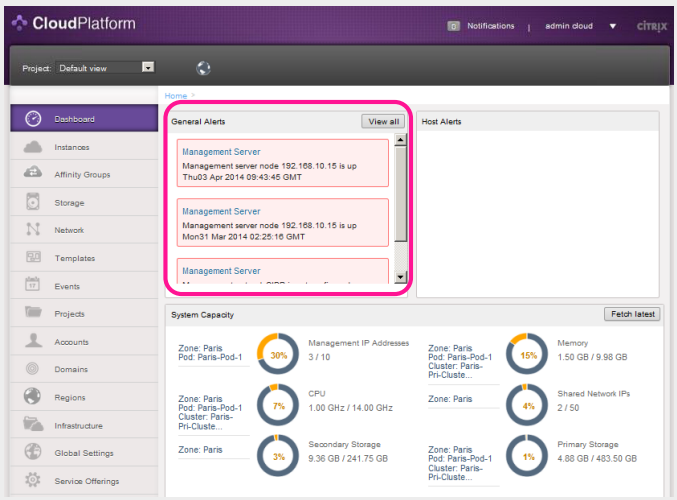
Step	Action
16.	Enter the parameters shown below to specify the first compute host IP address and login credentials. The specified IP can be a stand-alone host or a XenServer Resource Pool of hosts. In the case of a pool, use the IP address of the “Pool Master”, which in your case is vXS-01. Host name: `192.168.10.21` Username: `root` Password: `Citrix123`  Click **Continue**.
17.	 Click **OK**.

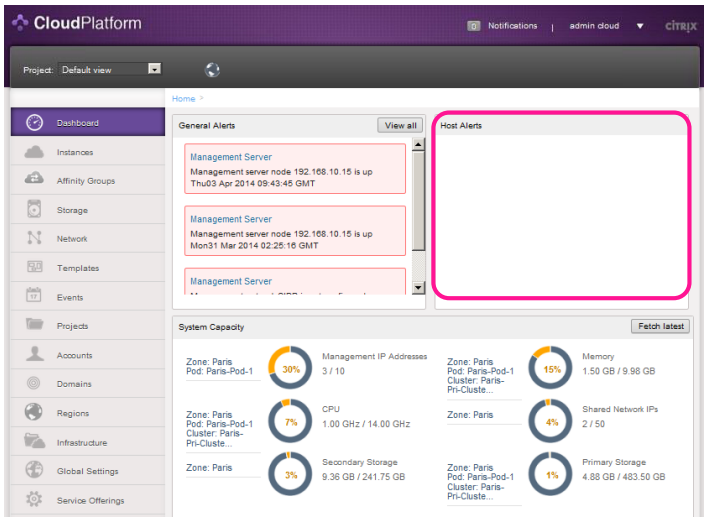
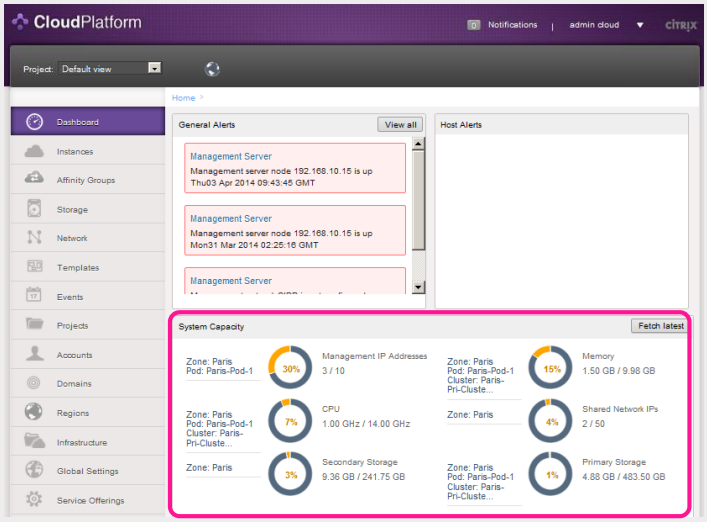
Step	Action
18.	Primary storage is used for the Virtual Disk Images (boot disks) of all VMs running in the cluster. It is shared among all hosts in the Cluster. Enter or select the following parameters: **Name:** `Paris-Pri-Cluster-1` **Protocol:** NFS **Scope:** Cluster **Server:** `192.168.10.12` **Path:** `/nfs/paris/primary/cluster1`  Click **Continue**.
19.	 Click **OK**.

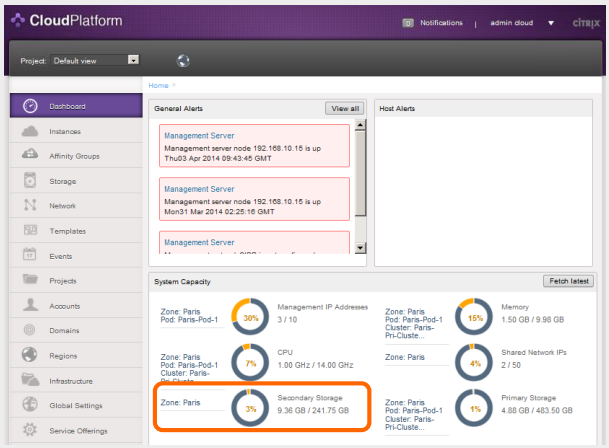
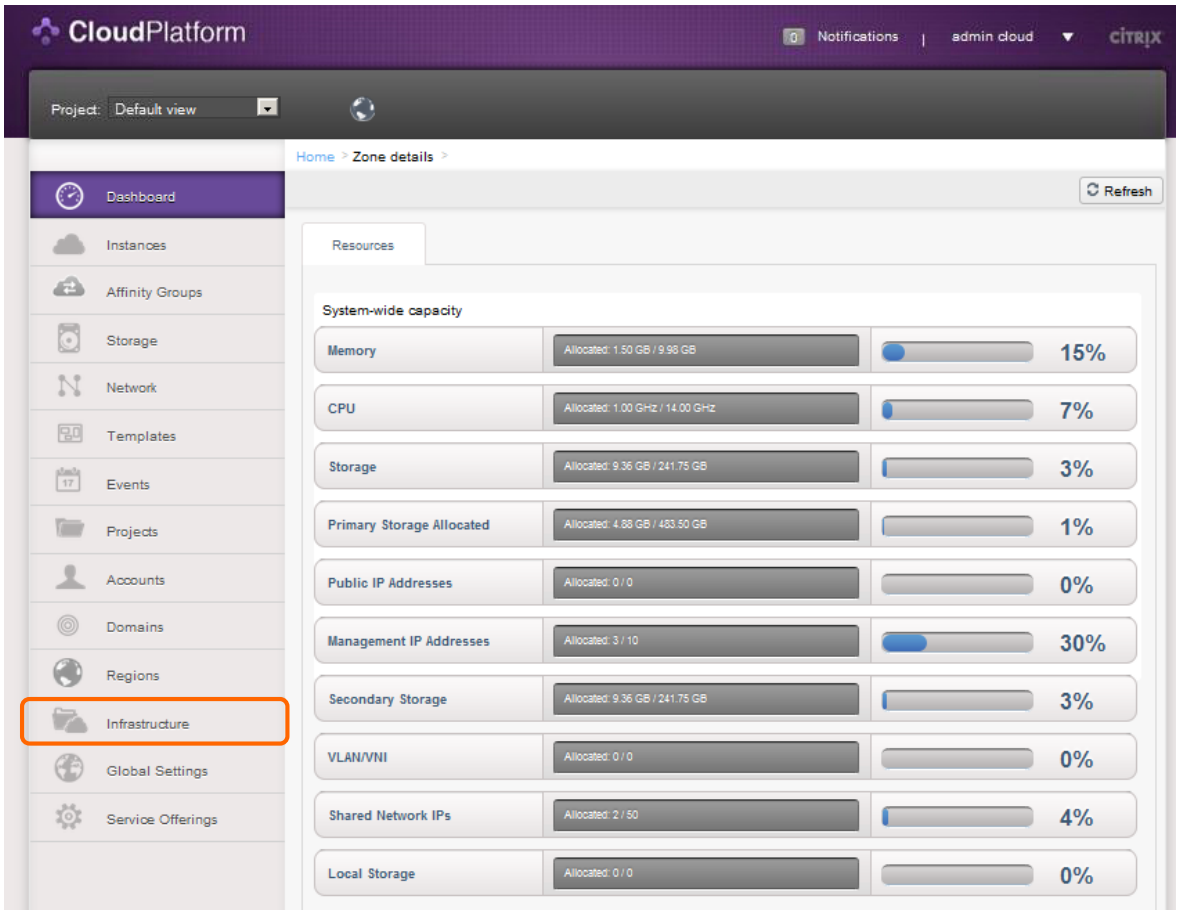
Step	Action
20.	Secondary storage is used for templates, snapshots and ISO images across the zone. Enter or select the following parameters: NFS Server: `192.168.10.12` Provider: NFS Path: `/nfs/paris/secondary`  Click **Continue**.
21.	 Click **Launch**.
22.	 Wait about 25 seconds, then, when CloudPlatform starts addding the host … move to the next step.

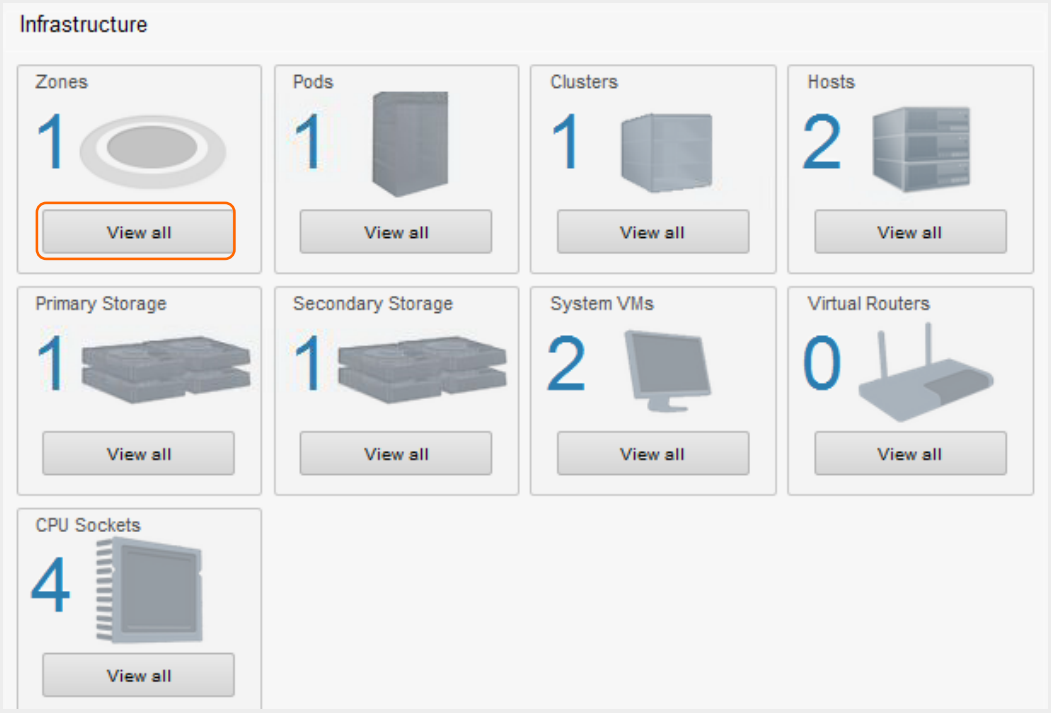
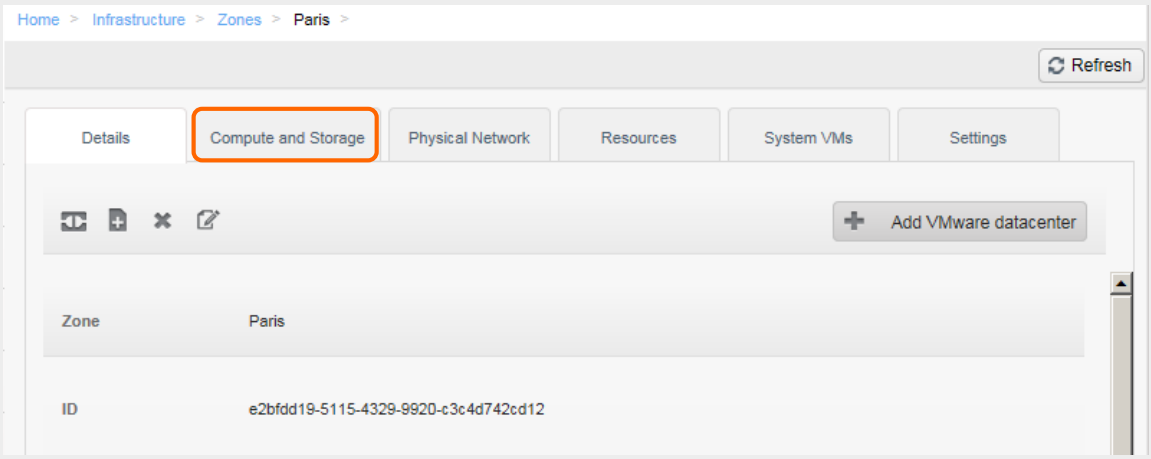
Step	Action
23.	 Roughly 40 seconds after launch, in XenCenter, notice the shared Primary Storage Repository (Primary SR) for Paris-XS-Cluster-1 is created (highlighted above). This is the SR where the Virtual Disk Images (VDIs or Boot Disks) of the VMs running in this cluster reside. It is shared amongst the cluster of hosts and is located on NFS shared storage. Click the new **Primary SR** node and select the **Storage** tab.
24.	 Roughly a minute after launch you will see a VDI is created on the SR as highlighted above. This is the System VM template that is now being copied to primary storage from the Paris zone secondary storage. It takes about five minutes to copy the 2.4GB template.
25.	The System VM template is used to create the System VMs used by CloudPlatform. Roughly six minutes after launch, the name of the template will change to “Template routing-1”. 
26.	A few seconds later you will see the VDIs for the two CloudPlatform system VMs created as linked clones of the template.

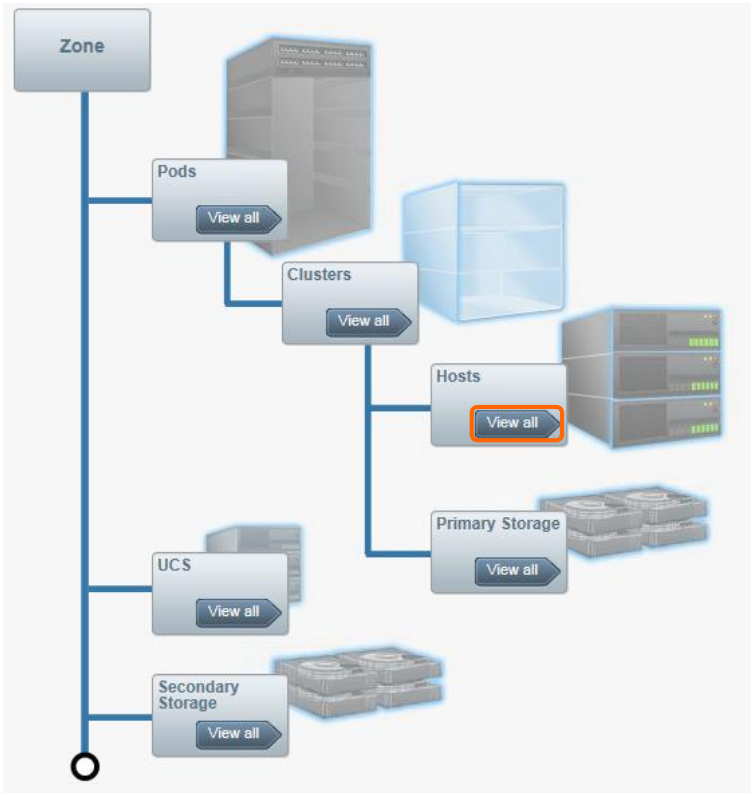
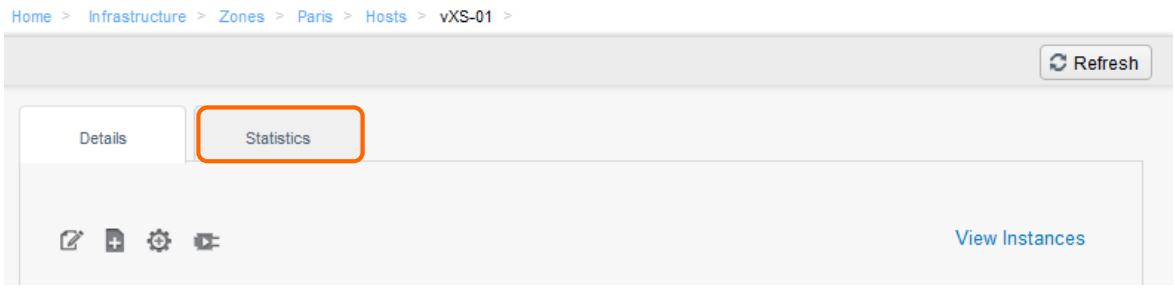
Step	Action
27.	Shortly thereafter the VMs will show up running in vXS-01 or vXS-02. It may take a minute for the second VM to show up.  There will be two system VMs, the Secondary Storage system VM (s) and the Console proxy system VM (v). The order of creation of the two system VMs is random; the first one to start is numbered 1 (e.g. v-1-VM) and the second is numbered 2 (e.g. s-2-VM). The System VMs may start on vXS-01 or vXS-02. The deployment of all VMs into hosts is based on the allocation algorithm, which, by default, is set to random. CloudPlatform will choose an appropriate host with the capacity and correct hypervisor to run the VM. You can find more information on the VM allocator algorithms here: http://support.citrix.com/article/CTX135790
28.	It takes another two minutes or so to complete building the zone. You will see the “Cloud setup successful” on the CloudPlatform GUI.  Click **Launch**.

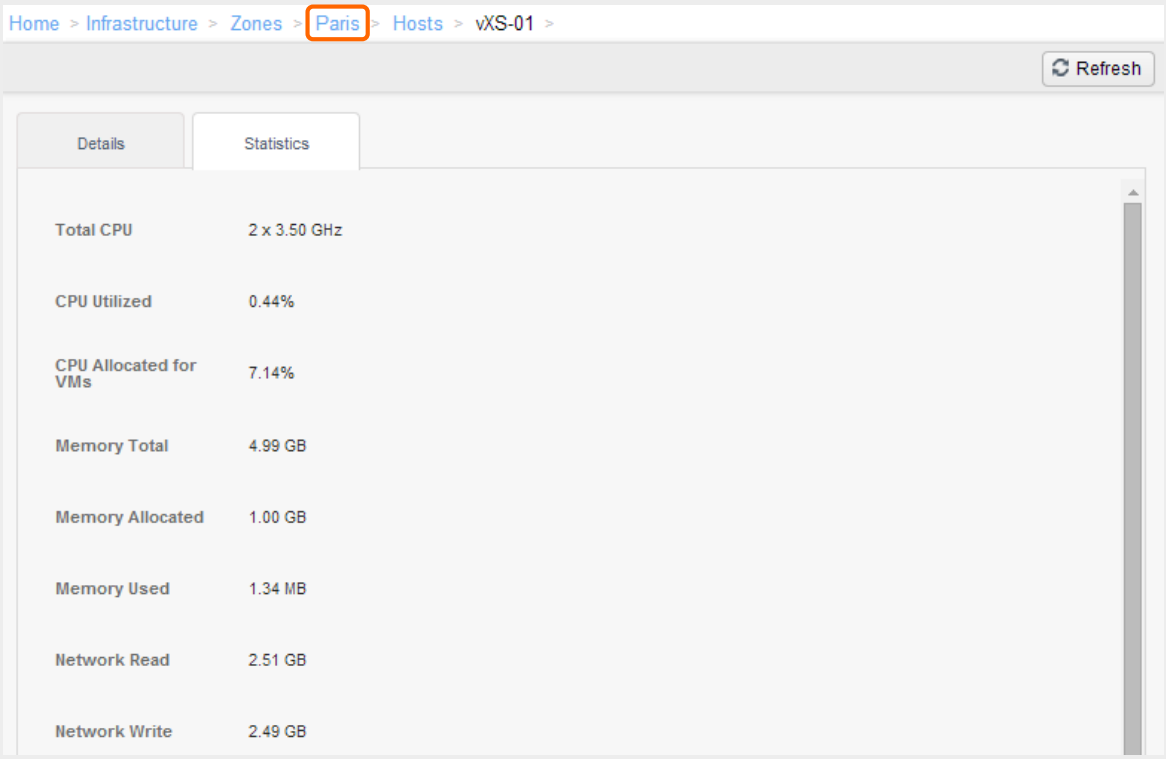
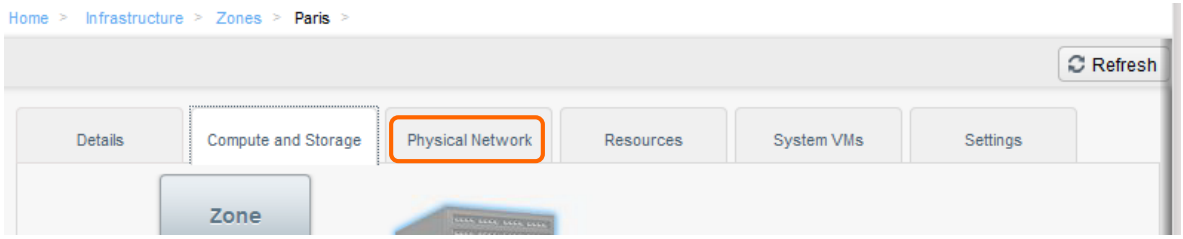
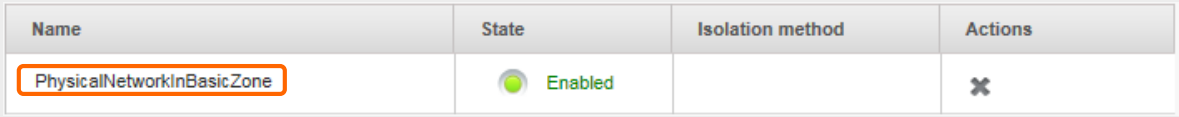
Step	Action
29.	 You will see the Cloud-Admin CloudPlatform Dashboard which provides at-a-glance status with alerts and system capacity performance parameters. Down the left side, the “navigation bar” will be present on all screens.
30.	 In the General Alerts panel you will see system wide alerts.

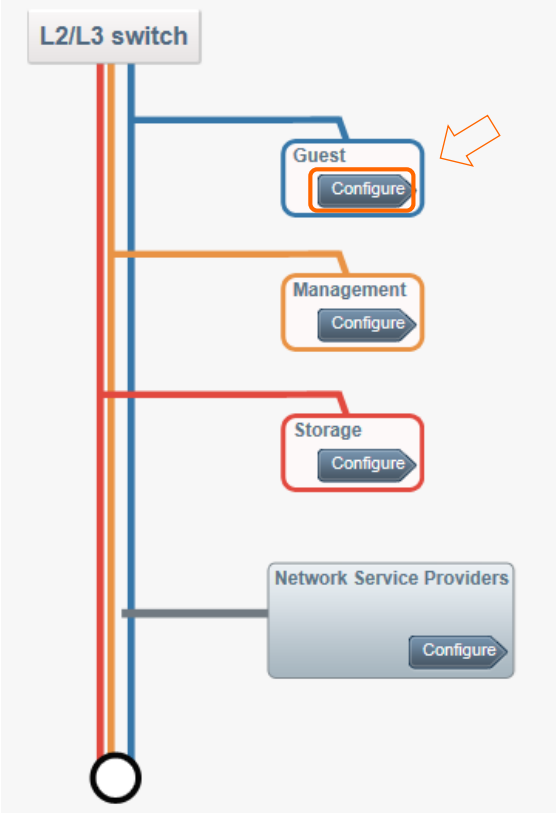
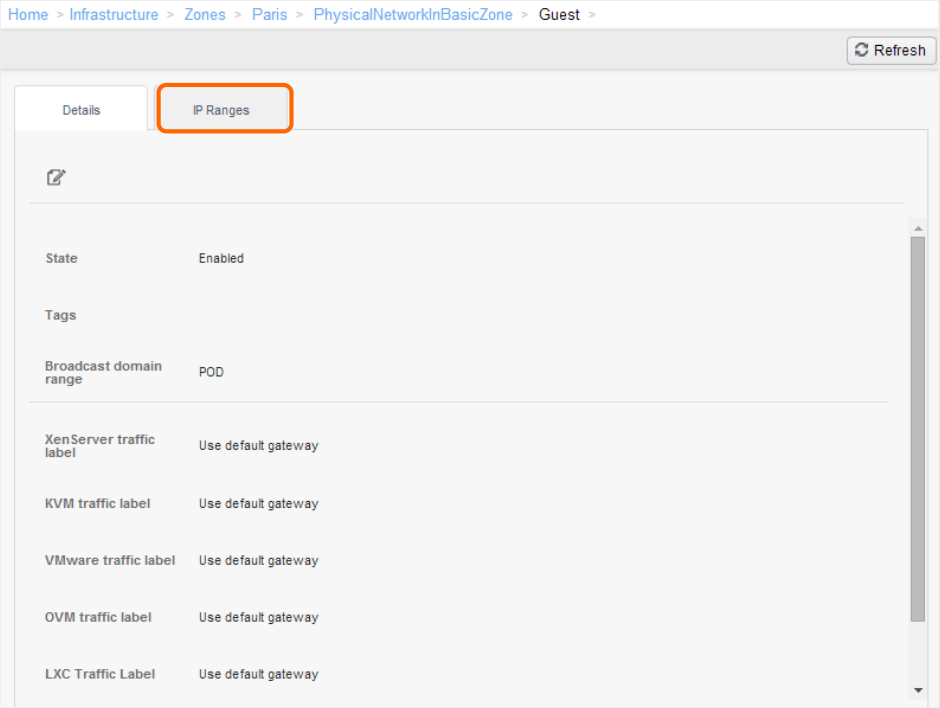
Step	Action
31.	 In the Host Alerts panel you will see host-specific alerts.
32.	 The System Capacity section shows the highest used resources at the top of the list.
33.	 The Notifications drop-down will typically alert the user to ongoing activities, such as deploying or destroying a VM instance. It will indicate how many alerts are available for viewing.

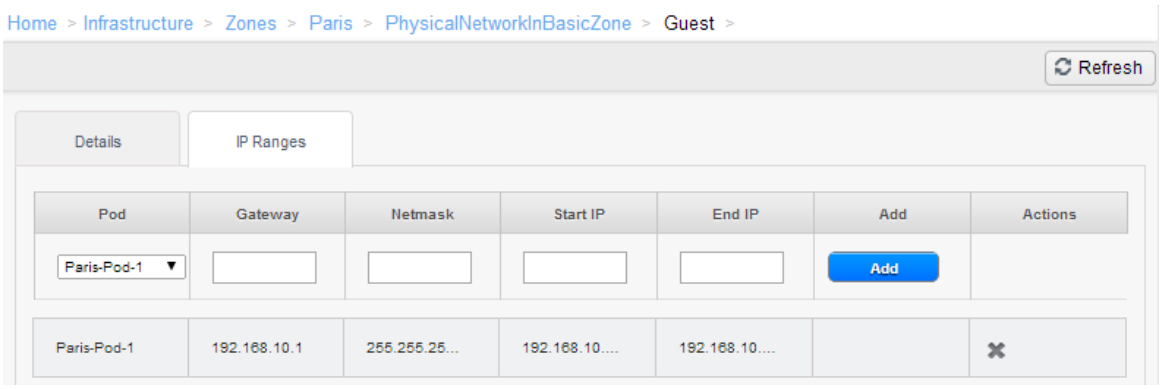
Step	Action
34.	 **Click** any of the **System Capacity** items to see all the resource usage.
35.	 In the left navigation bar of the CloudPlatform GUI, click **Infrastructure**.

Step	Action
36.	 The infrastructure display shows a summary of the Cloud infrastructure. In the **Zones** box, click **View All**.
37.	You will see the zone list: Click the **Paris** node to see details of the zone.
38.	 Click the **Compute and Storage** tab to explore the zone's components.

Step	Action
39.	 In the **Hosts** box, click **View All** arrow to see the hosts in the zone.
40.	 Notice the zone, pod & cluster of the host is shown along with each host's state. Click the **vXS-01** node to show more details.
41.	 The details of the chosen host are shown. Click the **Statistics** Tab.

Step	Action
42.	 Notice a range of host statistics are provided. Click **Paris** on the "breadcrumbs" bar to return to the Paris zone details. The breadcrumb bar is a convenient way to unwind (or back out) to the upper levels.
43.	 Click the **Physical Network** tab to see the physical network configuration of the zone.
44.	 Notice there is just one physical network. Click the **PhysicalNetworkInBasicZone** node to see a diagram of this network.

Step	Action
45.	 This physical network is carrying the Guest, Management and Storage traffic. Each of the network traffic types can be configured by clicking the appropriate configuration arrow. Click the **Guest Configure** arrow to show the Guest network details.
46.	 Click the **IP ranges** tab to view the IP ranges in use for the Guest network.

Step	Action
47.	 Additional IP ranges can be added using this screen, but do not add any at this time. (IP addresses that do not show completely in the GUI can be viewed in full by rollling over the address with the mouse.)
48.	You can explore more of the CloudPlatform GUI on your own. Just don't change anything yet!

Exercise Summary

You have built and started to explore a CloudPlatform Basic Networking zone.

Appendix 2

Appendix 2: Editing Files with vi

Overview

vi is a screen-oriented text editor originally created for the Unix operating system in 1976. That is not a typo. While vi is almost 40 years old, it is still the de-facto standard for text file editing in the Linux/Unix world and is not going away anytime soon. While there are file editors available for Linux that are easier to use, they are often not available when you need them, whereas vi is almost always there, ready and willing! If you will be working with Linux, you might as well learn vi.

Modal Editor

vi is a modal editor operating in either insert mode or command mode. vi operates only from the keyboard so, since there is no mouse to move the cursor, keystrokes are used not only to enter text into the file, but also to move the cursor and control the function of the editor. While for newbies this is cumbersome, for experts, it can be much faster than using a mouse. In the right hands vi is a very powerful editor that can run rings around any mouse driven counterpart with its rich, powerful set of features. You however, only need some simple basic functions to edit the files in this lab, so you'll be up and running in no time.

Insert mode

In insert mode most keystrokes become part of the document.

`i`	Enter Insert mode

Command mode

In command mode keystrokes control the edit session.

<ESC>	Enter command mode

Moving the cursor

You can use the arrow keys to move the cursor around in either mode.

Deleting

When in command mode you delete text using either of the following commands:

`x`	Deletes the character under the cursor
`dd`	Deletes the current line

Writing & Quitting

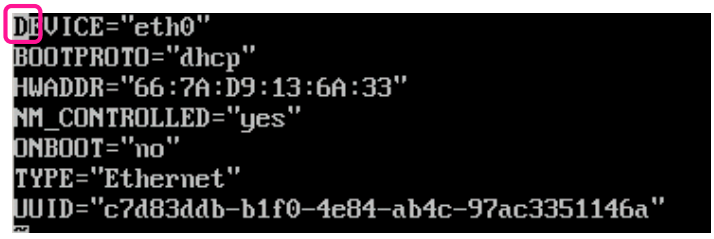
Once you have edited the file you can write the file and / or quit vi using the following commands:

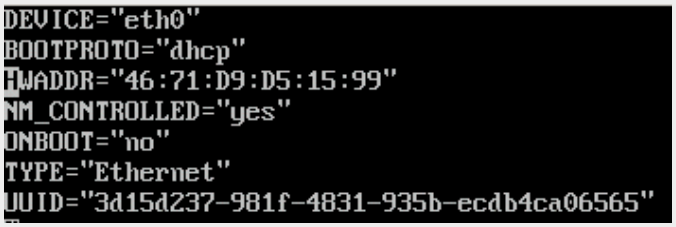
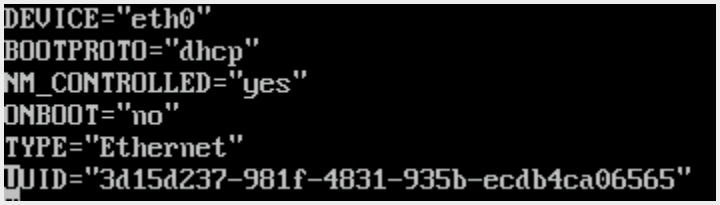
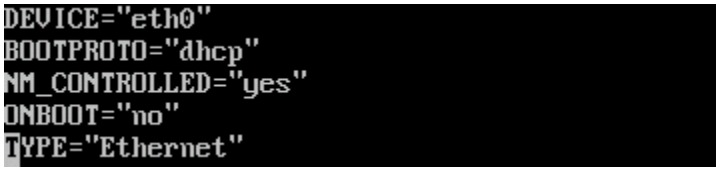
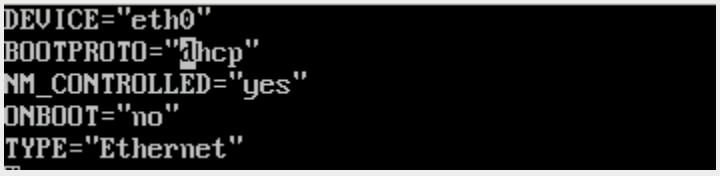
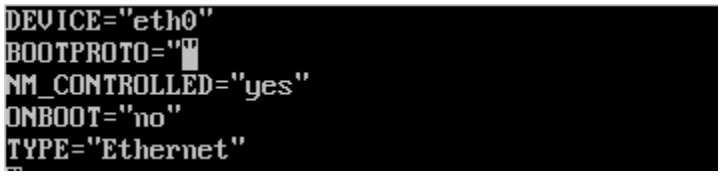
<ESC>:wq	Writes the file and quits vi
<ESC>:q!	Quits vi without writing the file (handy if you mess up)

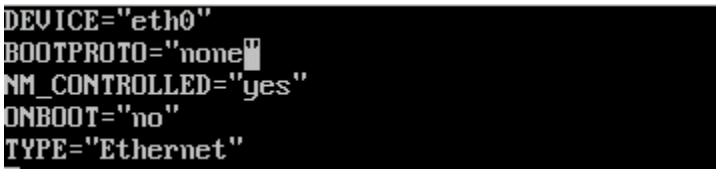
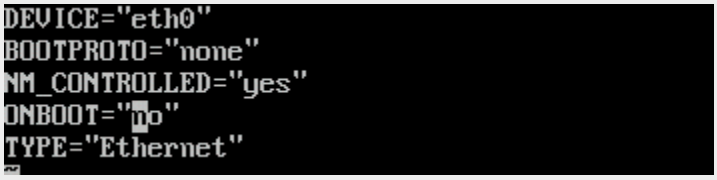
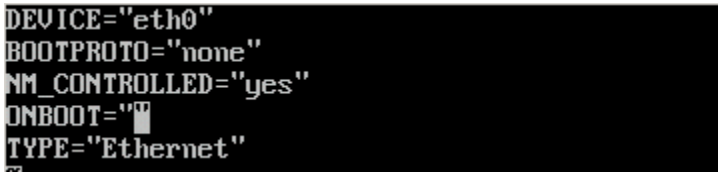
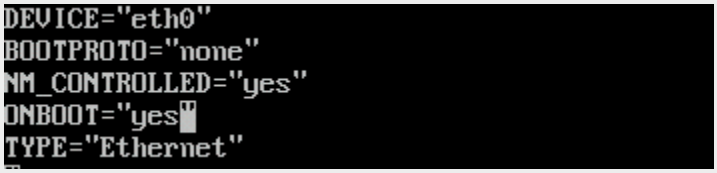
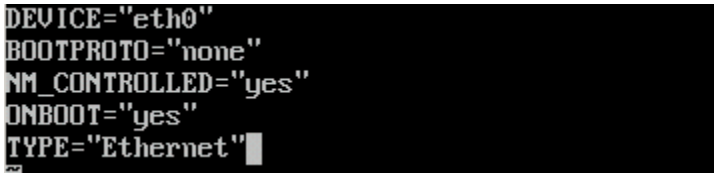
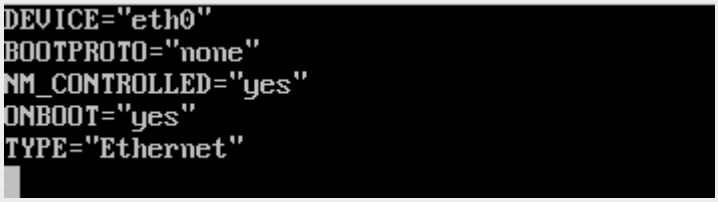
In this appendix you will edit the **/etc/sysconfig/network-scripts/ifcfg-eth0** file to setup the cpman network. The step by step assumes you have not previously edited the file.

Step by step guidance

Estimated time to complete this exercise: 10 minutes.

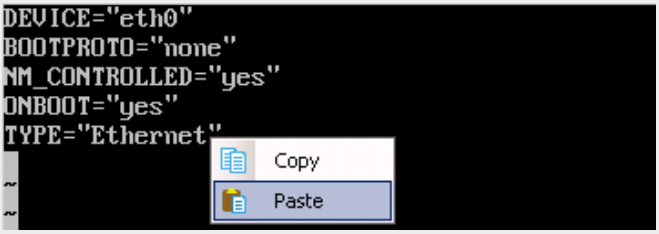
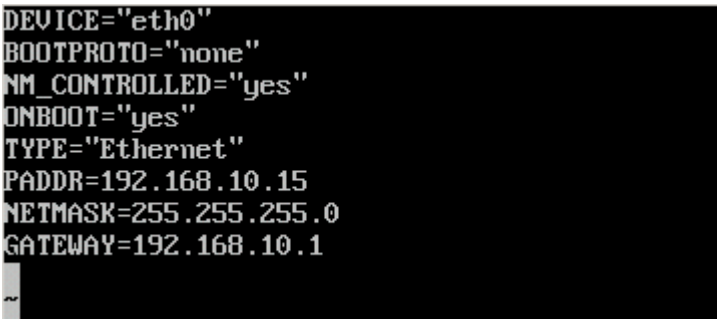
Step	Action
1.	On the cpman console, enter the following. **vi /etc/sysconfig/network-scripts/ifcfg-eth0**
2.	You will see the following (your HWADDR and UUID will be different):
3.	You will see the cursor at the top left corner (the character is shown in inverse).  The editor starts in command mode at this point, meaning keystrokes control the edit session.

Step	Action
4.	Remembering not to use the mouse, move the cursor to the third line by pressing the **down arrow key** twice: 
5.	Press the **d** key twice to delete the “HWADDR=” line.
6.	Move the cursor to the last line using the down arrow key. 
7.	Press the **d** key twice to delete the “UUID=” line. 
8.	Using the arrow keys move the cursor to the **d** of dhcp in the second line:. 
9.	Press the **x** key four times to delete four characters (dhcp). 

Step	Action
10.	Press the **i** key to put vi into insert mode: Notice the insert mode indicator at the bottom of the screen.
11.	Type the word **none**. 
12.	Hit the **<ESC>** key to come out of Insert mode and use the arrow keys to move the cursor onto the **n** of the word no in the fourth line. 
13.	Press the **x** key twice times to delete two characters (no). 
14.	Press the **i** key to put vi into insert mode and type the word **yes**. 
15.	Use the arrow key to move past the end of the last line. 
16.	Hit **<Enter>** to open up a new line. 

Step	Action

17.	Highlight and copy (**Ctrl-C**) the following three lines from this document:
	`IPADDR=192.168.10.15`
	`NETMASK=255.255.255.0`
	`GATEWAY=192.168.10.1`

18.	Back in vi, right click the console and select **Paste**: 
19.	The text has been pasted:  This completes editing of the file. Compare your file with the listing above. Yours should look exactly the same; check carefully for missing characters or typos.
20.	To save and exit press the **<ESC>** key to get out of insert mode, followed by: `:wq` That was easy, wasn't it? You can use the same principals to edit the other configuration files needed in this lab. Remember to take your time and if you mess up a file and just want to quit without saving, press the <ESC> key and then type `:q!` This will abort the edit; nothing is written to the file, so you can try again.

Appendix 2 Summary

You have learned a few basic vi commands to permit you to edit the files needed for this lab using vi.