CITRIX Summit2011

SUM409W: XenServer technical deep dive and troubleshooting

Learning Lab Exercises

October 2011

Table of Contents

Overview 3

How to log into the lab environment 3

Exercise 1: Connecting to Administrative Consoles 5

Exercise 2: Navigate to and Review Common Logs 11

Exercise 3: Collect a XenServer Status Report 20

Exercise 4: Collect and Review the Pool/Host Database 31

Exercise 5: Backing up XenServer 42

Exercise 6: Capturing a Network Trace in XenServer 59

Exercise 7: Monitoring in XenServer 73

Exercise 8: Creating and Reviewing Snapshots 84

Overview

Hands-on Training Module

This training module has the following details:

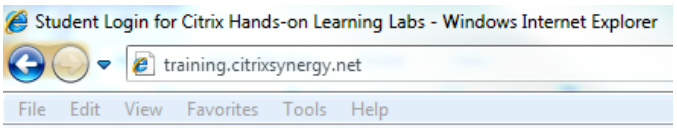
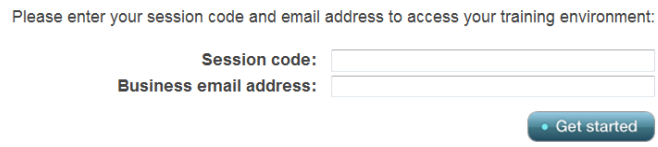
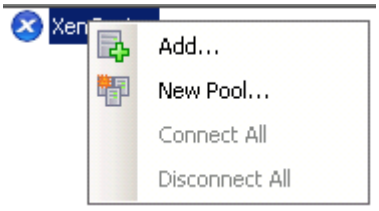
Objective	• Provide hands on experience with common tasks in XenServer • Provide hands on experience with common tools in XenServer used by Citrix Support
Audience	• Citrix Partners and XenServer Administrators/SMEs

How to log into the lab environment

The student lab environment is hosted on a Citrix XenServer. Follow the directions below to access the server.

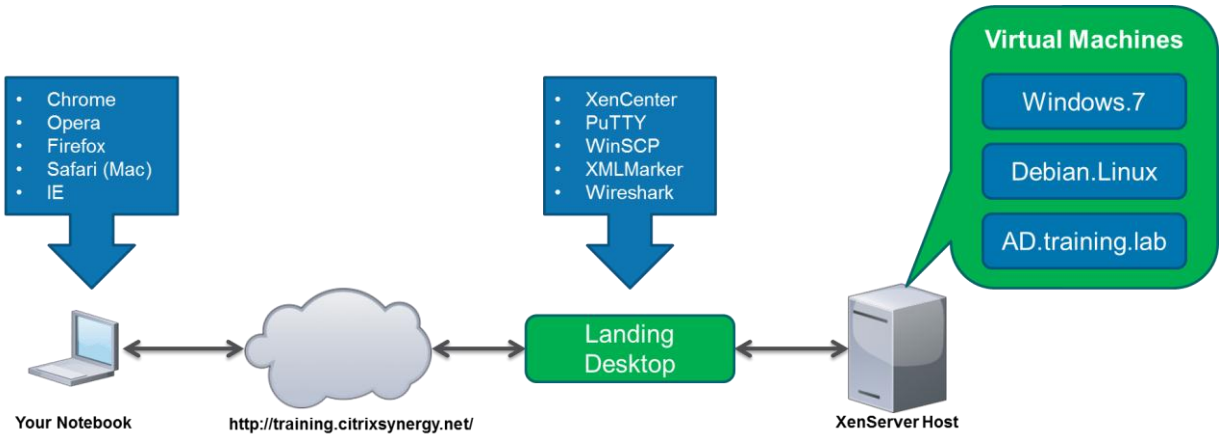
Note: Browser support: IE, Firefox, Chrome, Opera, Safari (on MAC).

Step-by-step login instructions

Step	Action
1.	Launch your web browser and go to **http://training.citrixsynergy.net** 
2.	On the website, type in the **session code provided by your instructor** and your **business email address** and click **Get Started**. 
3.	Once you've logged in, click the **Start Lab** button. This will launch your lab session. **Note:** Please wait for the application to launch.
4.	Rick-click **XenCenter** and select **Add.** 

Step	Action
5.	On the **Add New Server** screen enter the **XenServer IP address** provided on the website and in the **Password** field enter the password provided on the site.

Lab Architecture



Lab Environment Credentials

Below are the login credentials required to connect to the workshop systems and complete the lab exercises.

Machine/VM	Username	Password	Description
XenServer	root	*As per Student Portal	XenServer host
Debian.Linux	root	citrix	Debian 4.1.1 virtual machine
Windows.7	TRAINING\administrator	Citrix123	Windows 7 virtual machine
AD.training.lab	TRAINING\administrator	Citrix123	W2k8 R2 virtual machine

Lab Environment Details

This section is used to describe the lab environment and the virtual machines that are used.

VM Name	IP Address	Description
Windows.7	192.168.10.13	Virtual Machine
AD.training.lab	192.168.10.11	Virtual Machine
Debian.Linux	N/A	Virtual Machine
Landing Desktop	N/A	XenApp Published Desktop

Exercise 1: Connecting to Administrative Consoles

Overview

In this exercise we will connect to the administrative consoles used during this Learning Lab session.

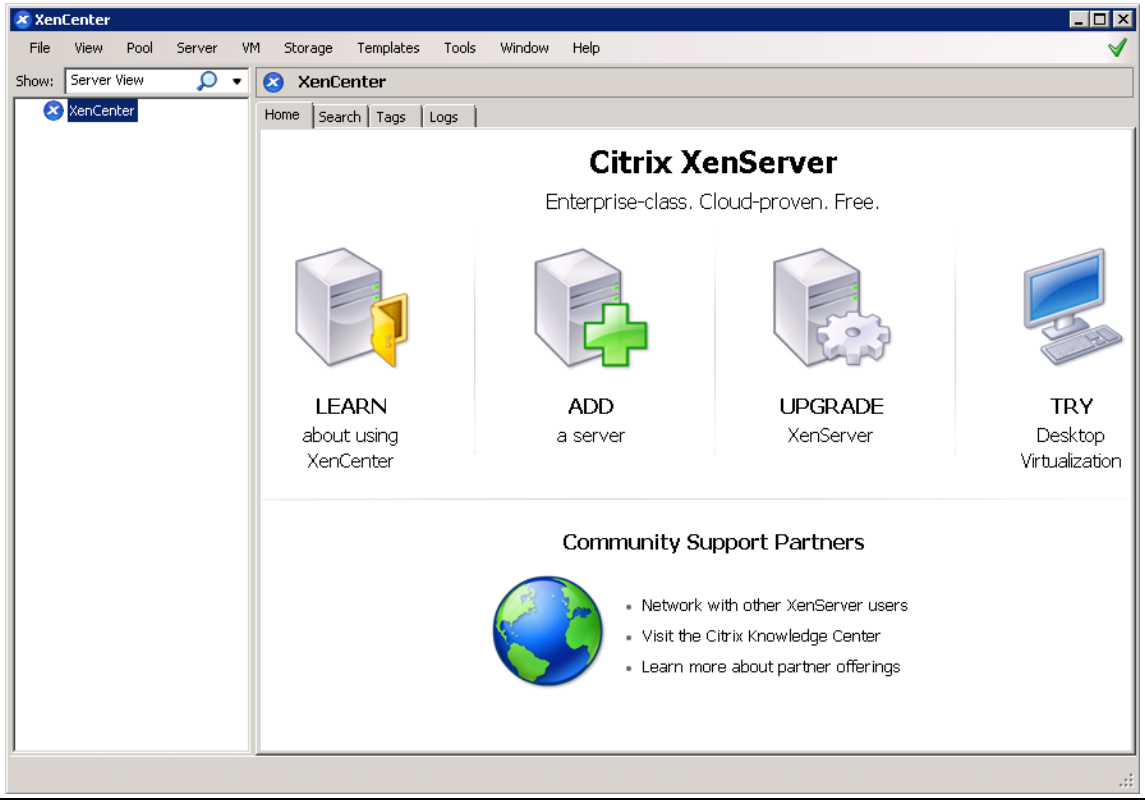
Throughout the hands-on sections of this Learning lab we will be using different consoles for certain actions. Feel free to use the console you are more familiar with to complete a desired task unless the console to be used is specifically mentioned in the lab documentation.

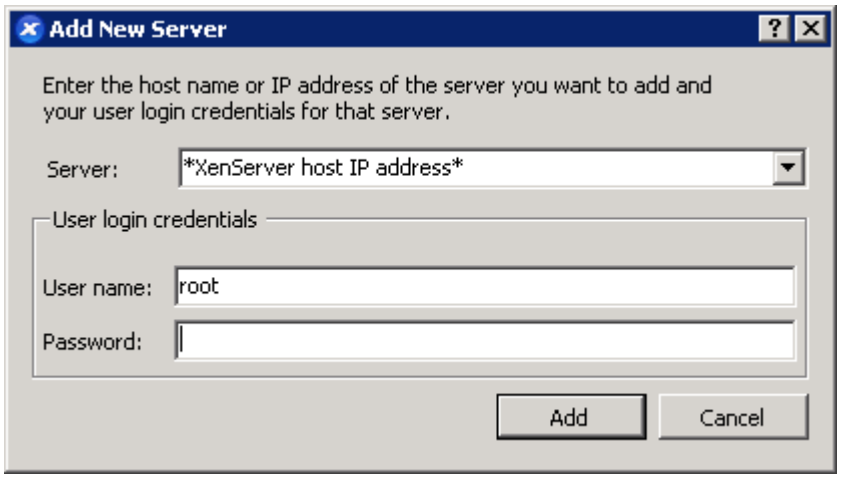
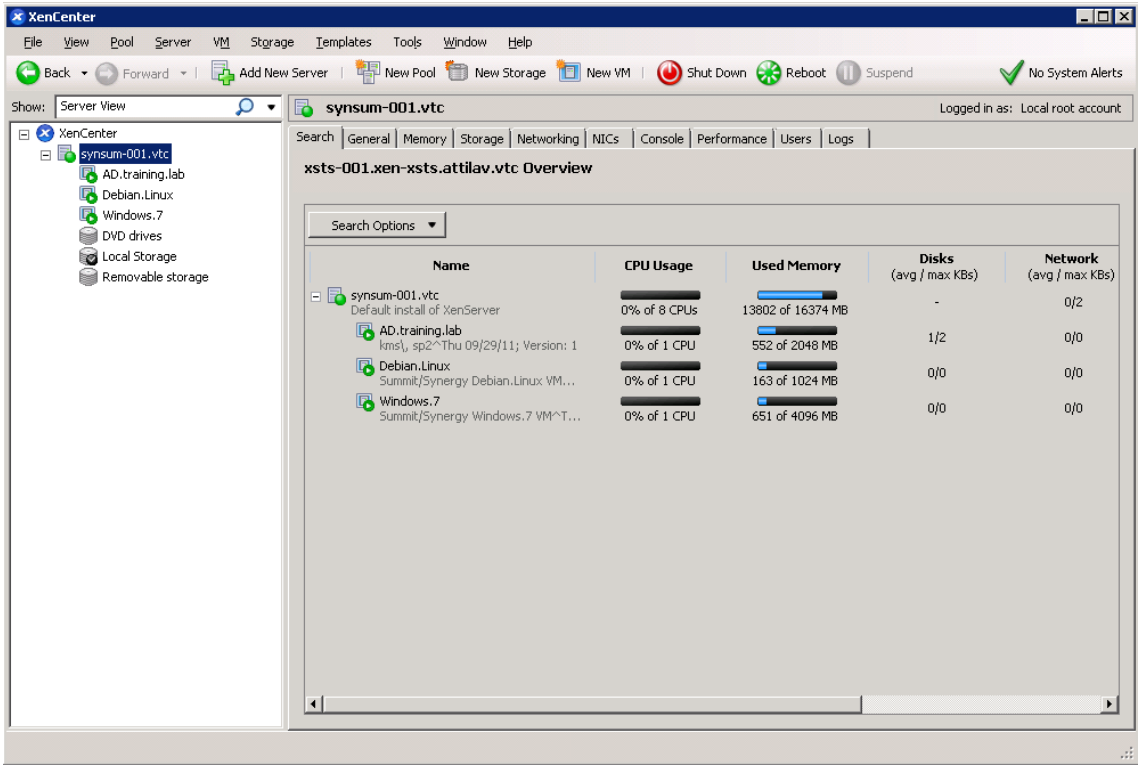
To complete this exercise, you must have the following:

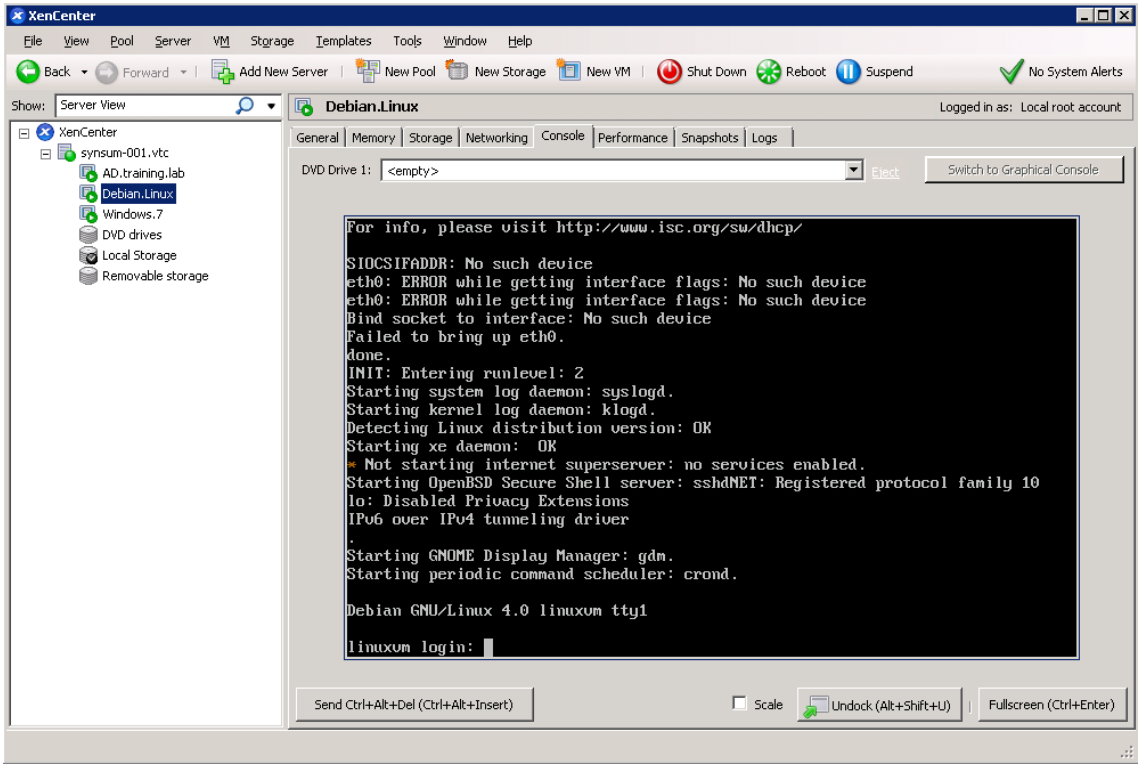
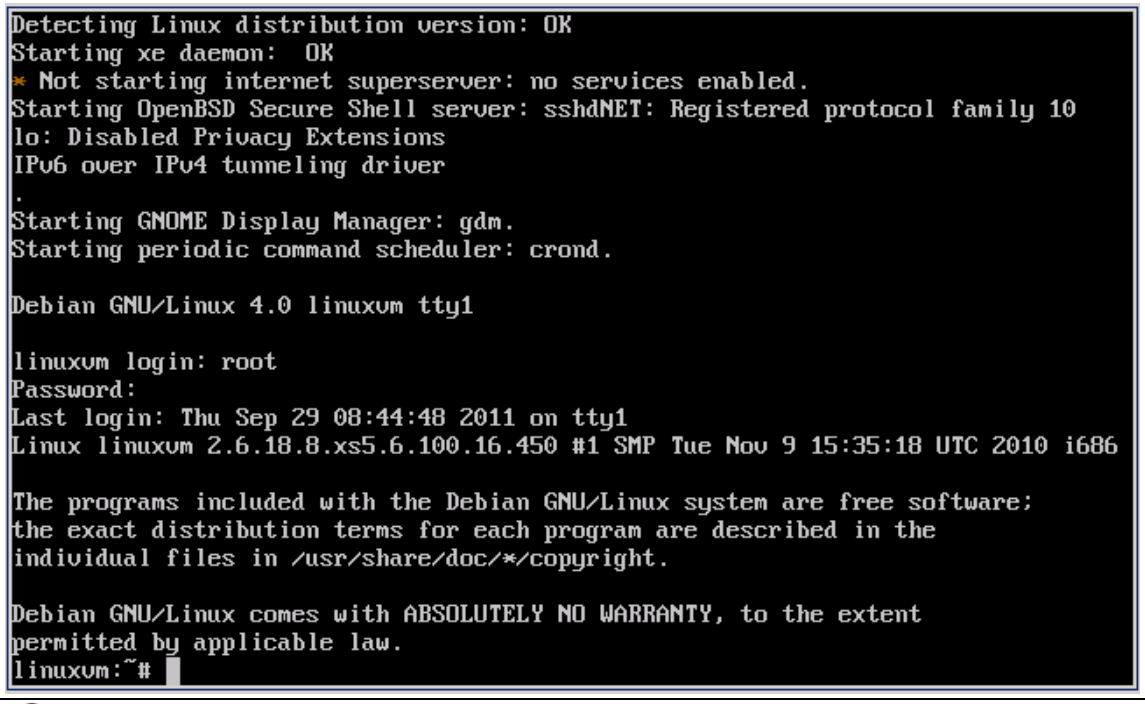
- SSH client (PuTTY)
- XenCenter

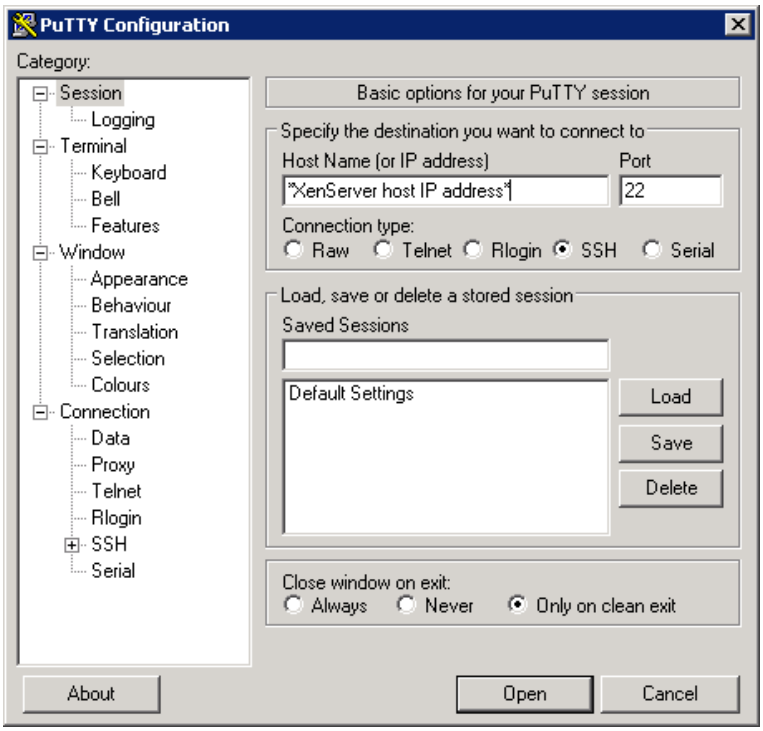
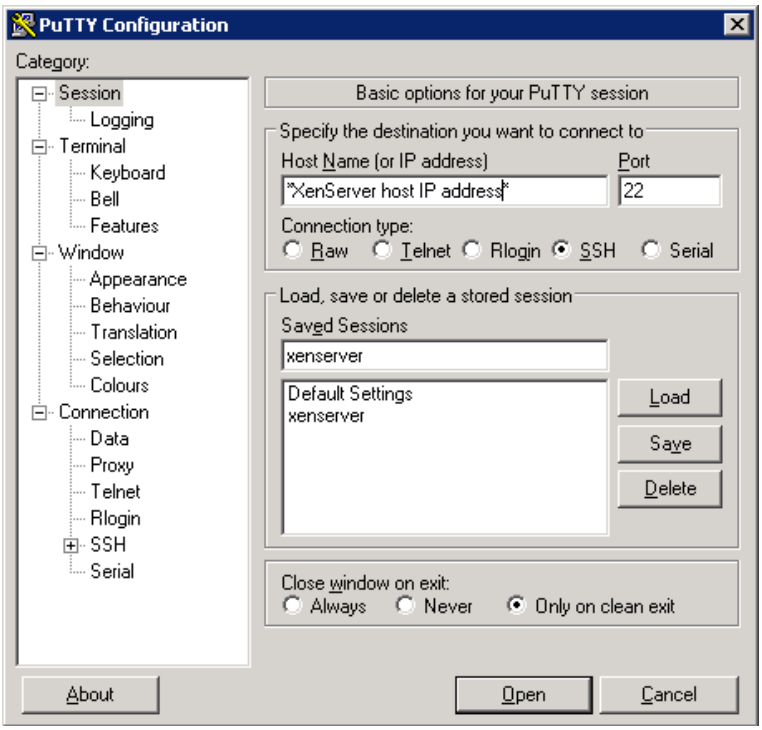
Step-by-step guidance

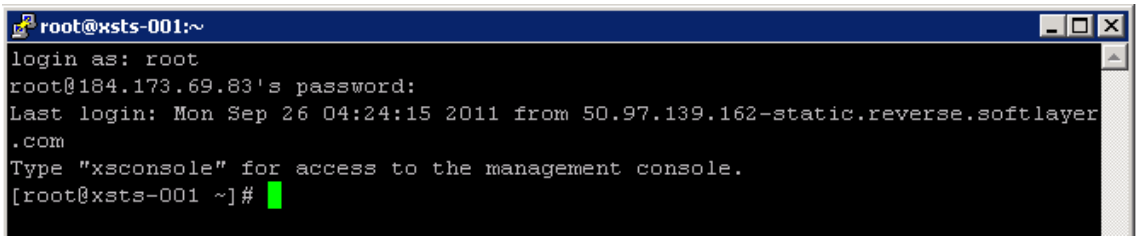
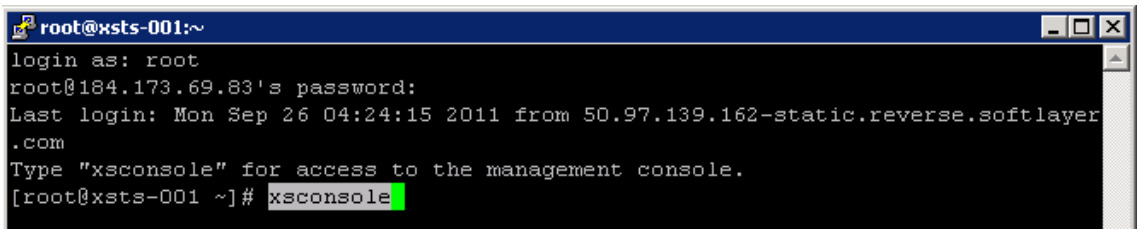
Estimated time to complete this lab: **10 minutes**.

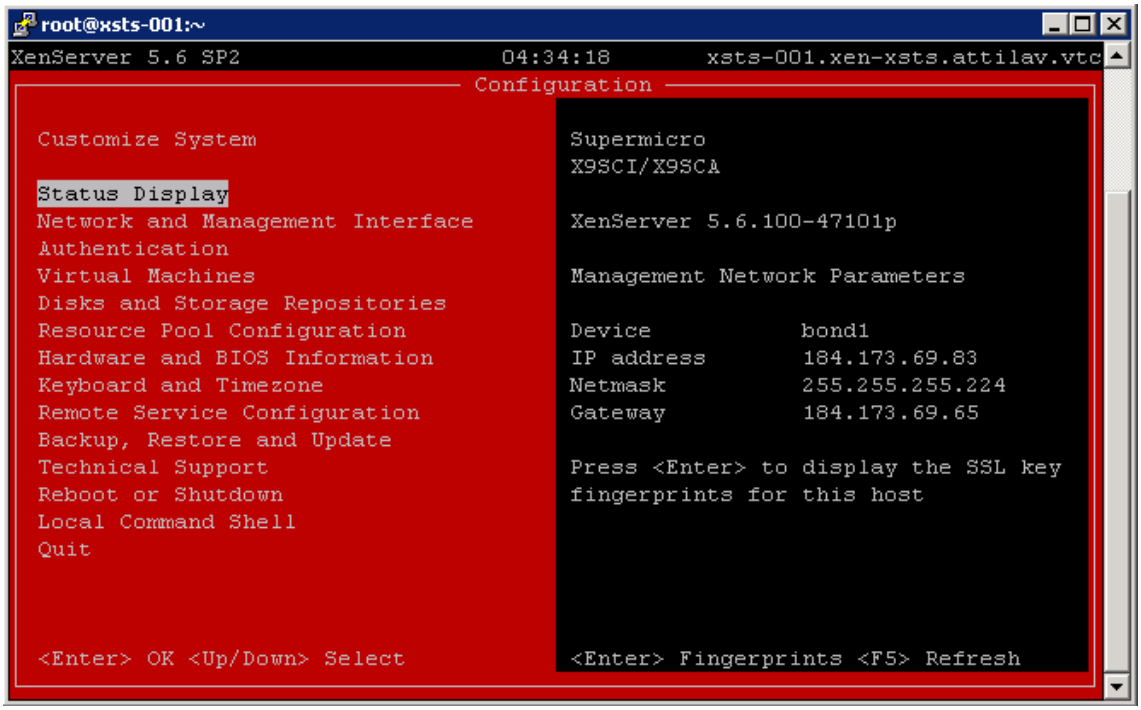
Step	Action
	Connect to your Landing Desktop and designated XenServer host:
1.	**XenCenter** should launch automatically after logging in. If not, launch it from the Landing Desktop. 

Step	Action
2.	Click **ADD a server** and enter the connection information as per the Student Portal 
3.	After a successful synchronization the XenServer host details are displayed.  **Note:** All virtual machines should be in a started state

Step	Action
4.	Click the **Console tab** for the **Debian.Linux** VM 
5.	Login (username=root, password=citrix) 
	Connect to XenServer via an SSH client (PuTTY):

Step	Action
6.	Launch **PuTTY** from the Landing Desktop and enter your XenServer host IP address. 
7.	Enter "**xenserver**" in the "**Saved Sessions**" field and click "**Save**". This will speed things up when we need to open multiple SSH connections. **Note:** Next time you need to launch an SSH connection via PuTTY simply click "**Load**" and then "**Open**" 
8.	Click **Open**

Step	Action
9.	Accept any key exchange message
10.	Enter the **credentials** to login to XenServer. **Note:** You can **copy and paste** the credentials form the Synergy/Summit portal page. To paste the credentials **right click** when prompted for the password (no text will appear) and press **ENTER**. 
	Launch the **xsconsole** via our SSH connection:
11.	Type **xsconsole** in the console window. Remember to use **tab completion** when working at the shell e.g. **xsco**Tab ⇆**.** It makes entering commands and long strings of text much easier. 

Step	Action
12.	We should now have access to the **xsconsole**. The **xsconsole** is launched by **default** at the local server console after a successful boot of XenServer i.e. the first console you see after booting XenServer. 
13.	The **xsconsole** is used for initial configuration of the XenServer host and many general **administrative** tasks can be also completed via this console.
END OF EXERCISE	

Summary

Key Takeaways	The key takeaways for this exercise are: • You will be able to connect to the administrative consoles used during this Learning Lab. • You will be familiar will all the XenServer administrative consoles available.

Exercise 2: Navigate to and Review Common Logs

Overview

In this exercise we will navigate to common log locations and review those logs.

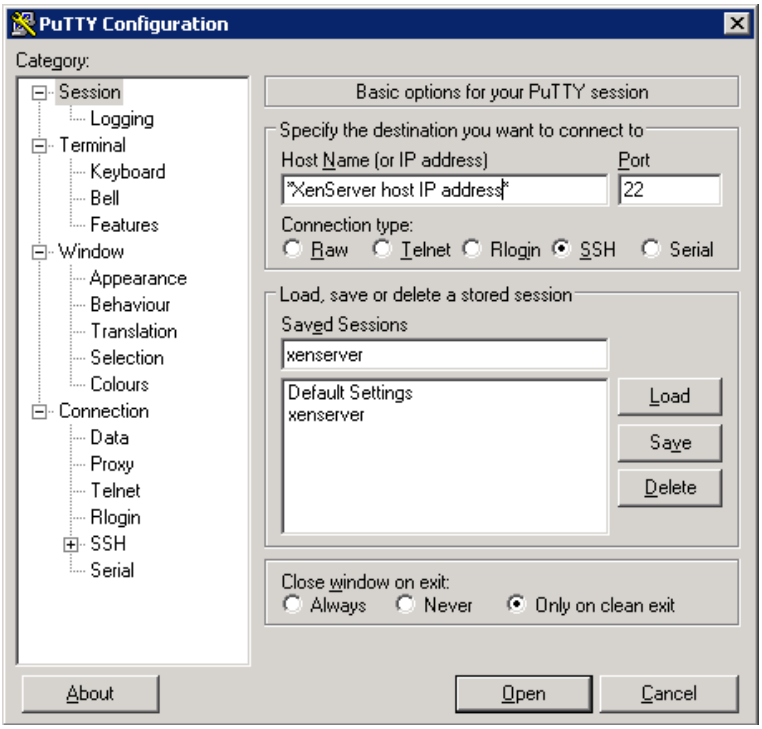
Log information can be useful when troubleshooting an issue and/or understanding how actions are performed e.g. following a log file when making a change to a XenServer host or virtual machine.

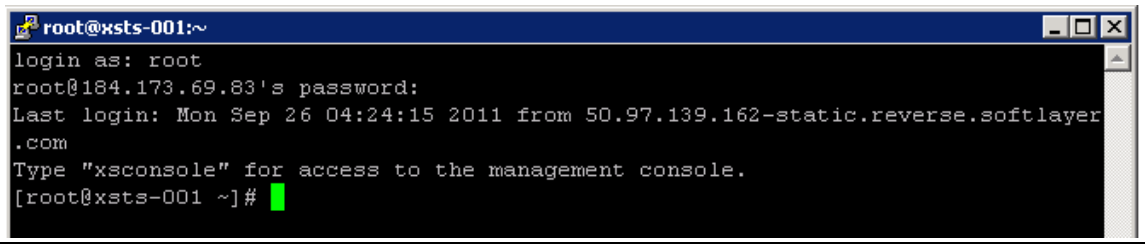
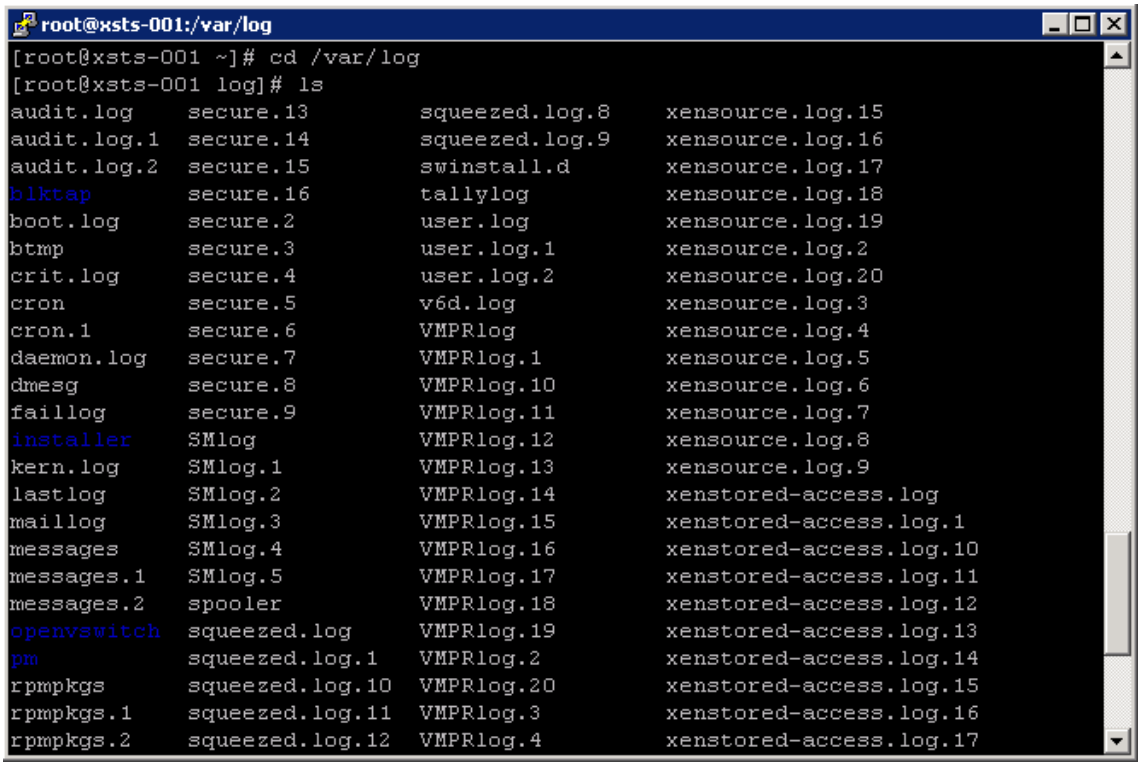
To complete this exercise, you must have the following:

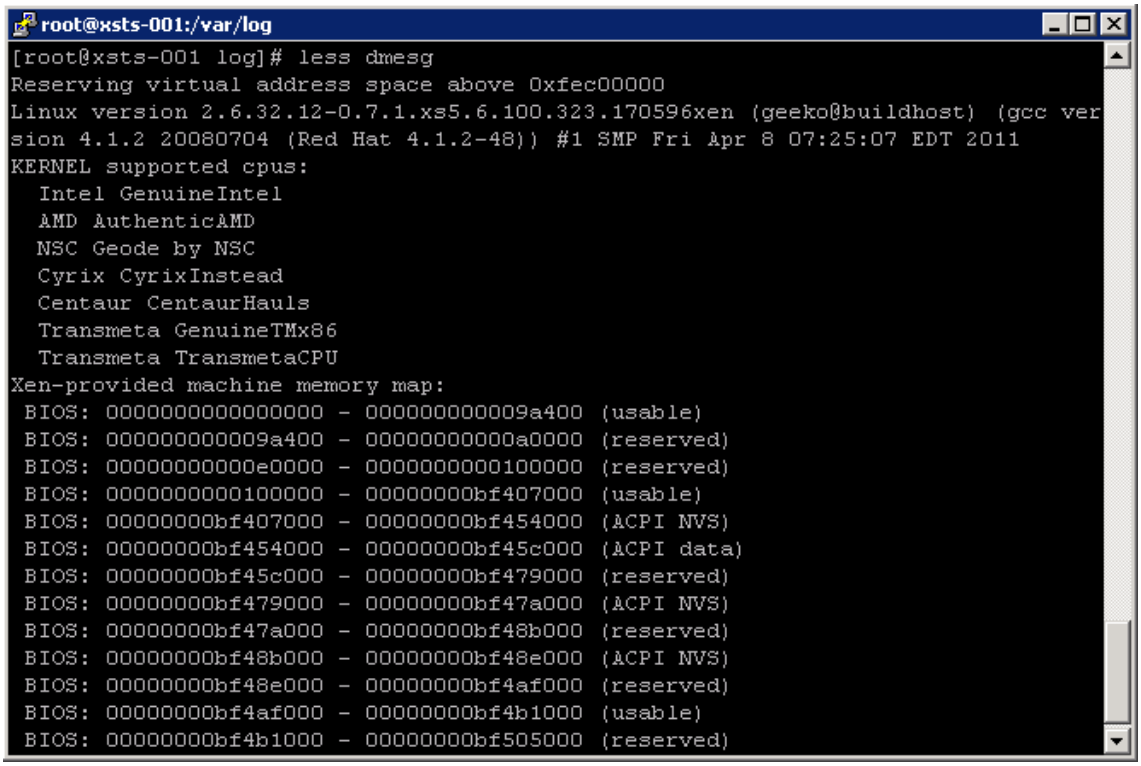
- XenCenter
- SSH client (PuTTY)

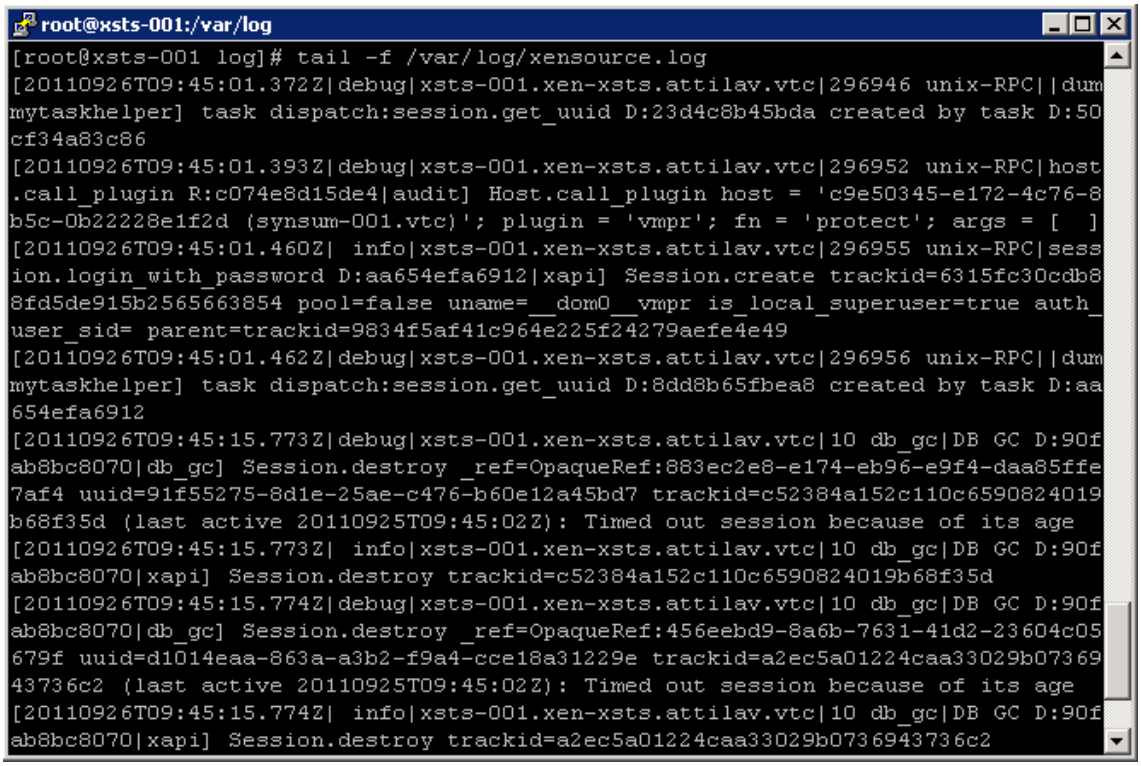
Step-by-step guidance

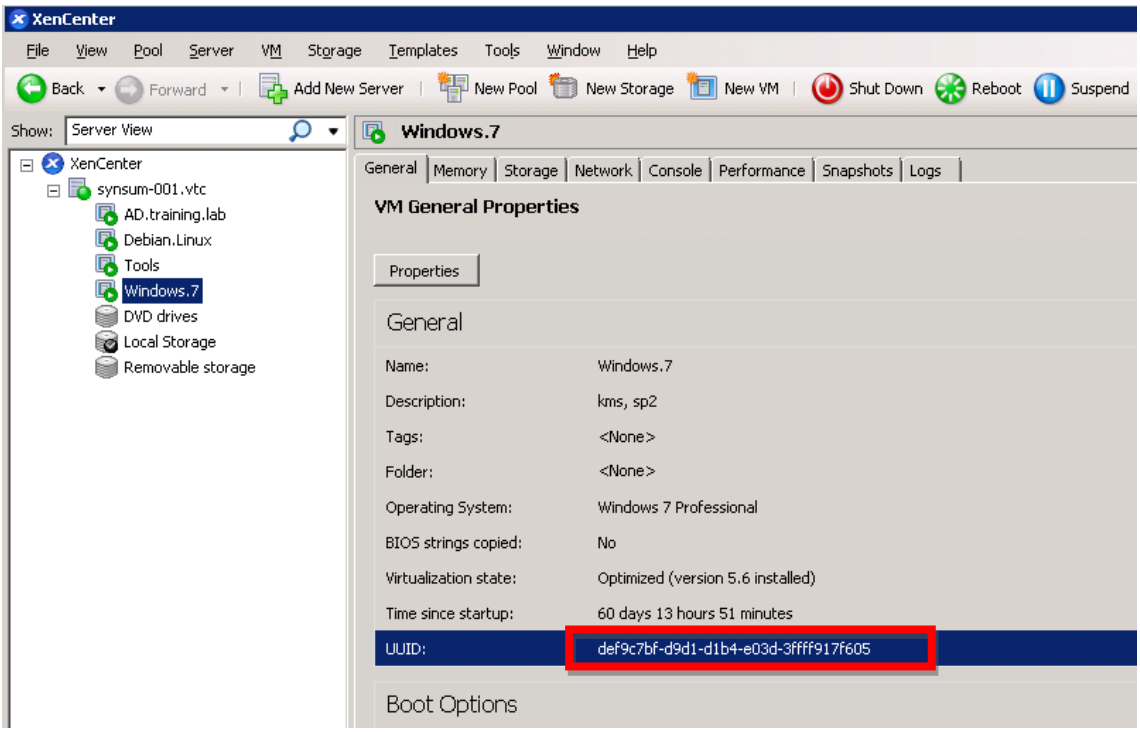
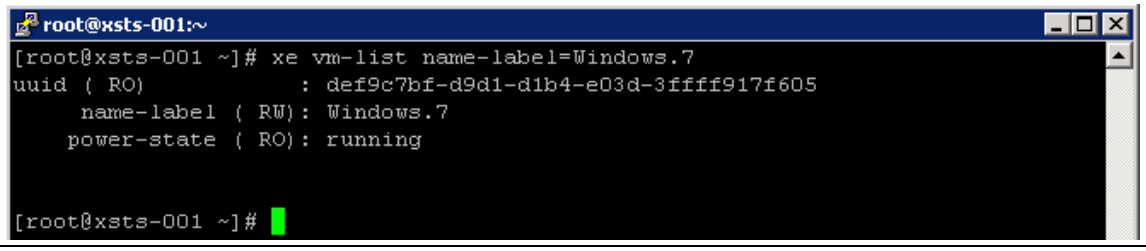
Estimated time to complete this lab: **15 minutes**.

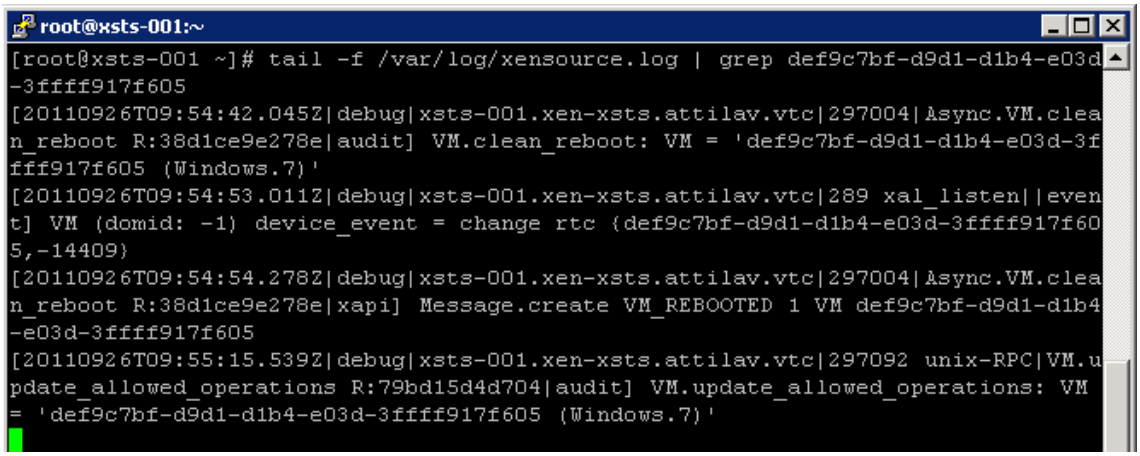
Step	Action
	Open a new SSH connection to your XenServer host using PuTTY:
1.	Launch **PuTTY** from the Landing Desktop by loading the saved session information (xenserver) and click **Open**. 

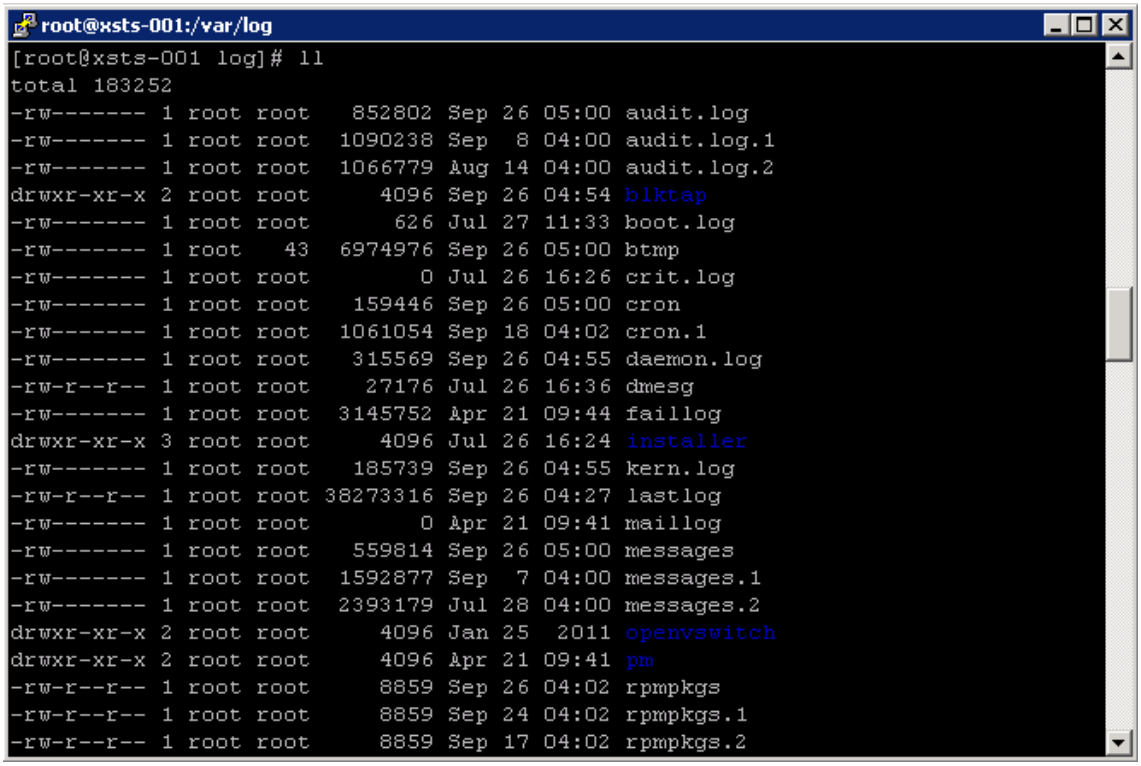
Step	Action
2.	Login with the default credentials 
3.	Change into the /var/log directory and list the contents of the directory e.g. **cd /var/log** e.g. **ls**  **Note:** Other commands to list the contents of a directory include **ls –l** and **ll.** Experiment with some of these commands to see how they display the contents of the directory differently. For more information on the **ls** command type **man ls**. To exit out of a **man** page press **q**.

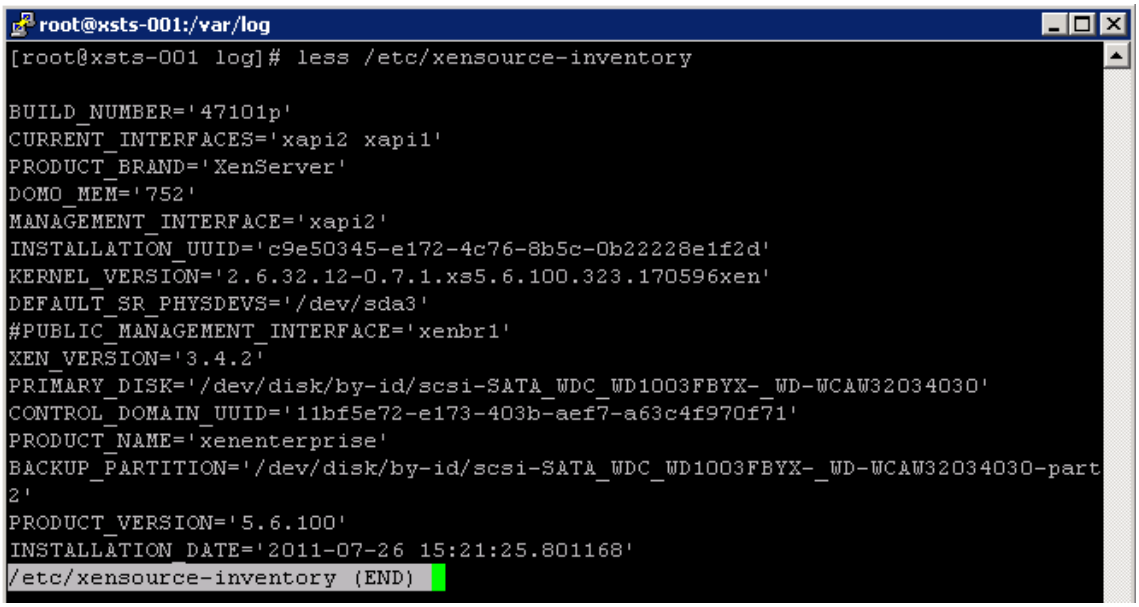
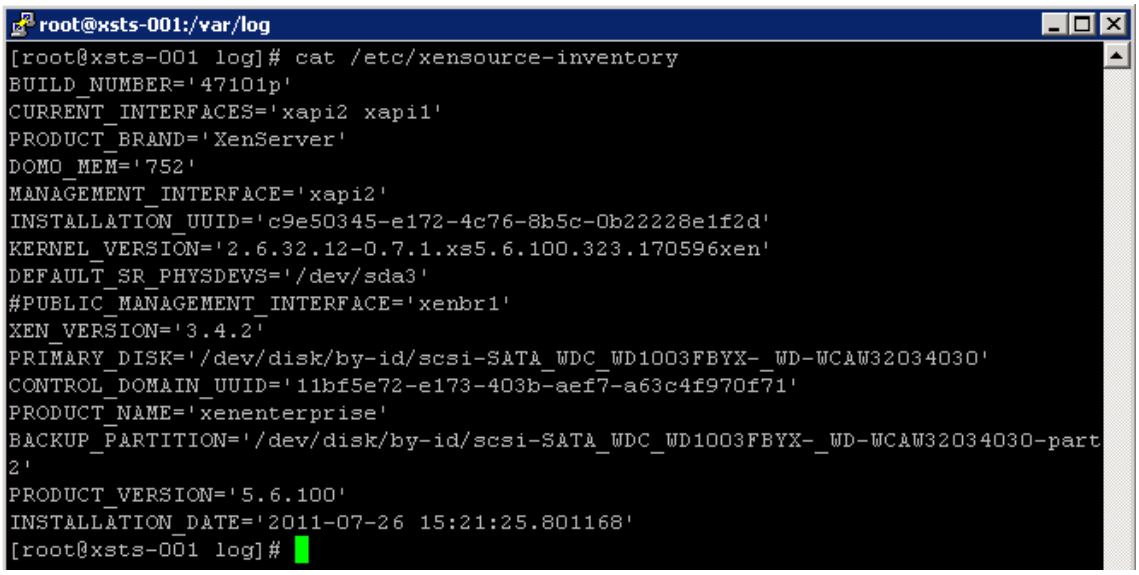
Step	Action
4.	View the contents of the **dmesg** log file. *Remember to use **tab completion** when working at the shell. e.g. **less dmesg**  Press **q** to quit **Note:** There are many tools/commands that can be used to view the contents of a file. In the above example we use the **less** command so that we are able to scroll through the file using the arrow keys. Use the spacebar to page down. Other commands include **cat**, **more**, etc. **Note:** The **dmesg** ("display messages") log file contains information related to dom0 boot. **Note:** To list the boot messages of the Xen hypervisor use the **xe host-dmesg** command.

Step	Action
5.	Follow a log file to view the latest entry updates within the file e.g. **tail –f /var/log/xensource.log**  Press **CTRL+C** to **quit** **Note:** The **tail** command lists the last 10 lines of a file. With the **–f** parameter we are able to follow the file and view the last 10 lines of the file as it is updated. • Remember to use **tab/auto completion** when working at the shell e.g. **xens** Tab ⇆. • Auto completion is also able to provide you with a list of available command or parameters by using double Tab ⇆
	Follow log file entries for a specific virtual machine:

Step	Action
6.	Find the UUID of a VM via **XenCenter**  **Note:** You can copy the UUID from XenCenter by right-clicking and selecting "copy".
7.	Find the UUID of a VM via **CLI.** e.g. **xe vm-list name-label=Windows.7** 

Step	Action
8.	Use the UUID of the VM as the search pattern for the **grep** command e.g. **tail -f /var/log/xensource.log | grep [UUID of the VM]**  **Note:** You can copy and paste the complete UUID to be used by the **grep** command or provide enough unique information for the parameter to function i.e. **def9** (in the above example). In most cases the first 4 characters of a UUID are unique. **Note:** The **tail** command lists the last 10 lines of a file. The **–f** parameter "follows" the file and automatically updates the last 10 lines displayed with any updates occurring in the file. **Note:** You will not see any updates until you move onto the **step no. 12**.
9.	**Reboot** the **Windows.7** virtual machine and follow the log updates relating to that VMs UUID
10.	Press **CTRL+C** to **quit** after the virtual machine has rebooted
11.	This type of information can also be sent to a file e.g. **tail –f [log filename] > [target filename]**

Step	Action
12.	**Long List** the contents of the **/var/log** directory to see more detailed information about the log files such as dates stamps and size. e.g. **ll /var/log**  **Note:** Commands to list the contents of a directory include **ls –l** and **ll.** Experiment with some of these commands to see how they display the contents of the directory differently. For more information on the **ls** command type **man ls**. Press **q** to quit out of the man/manual page.

Step	Action
13.	Review XenServer information via CLI: related version, build number, hypervisor version, etc. located in the **xensource-inventory** file. e.g. **less /etc/xensource-inventory**  Press **q** to quit **Note:** The contents of this inventory file will vary from a default inventory file as some modifications were made to facilitate this cloud-based lab environment.
14.	Alternatively you can use the **cat** command to view the contents of the file. e.g. **cat /etc/xensource-inventory**  **Note:** For more information about the cat command type **man cat** to display the manual for the command. Press **q** to quit of a man/manual page.

END OF EXERCISE

Summary

Key Takeaways	The key takeaways for this exercise are: • You will be able to locate, view and follow common system logs • You will be able to locate XenServer build information via the CLI

Exercise 3: Collect a XenServer Status Report

Overview

In this exercise we will collect a system status report from a XenServer host.

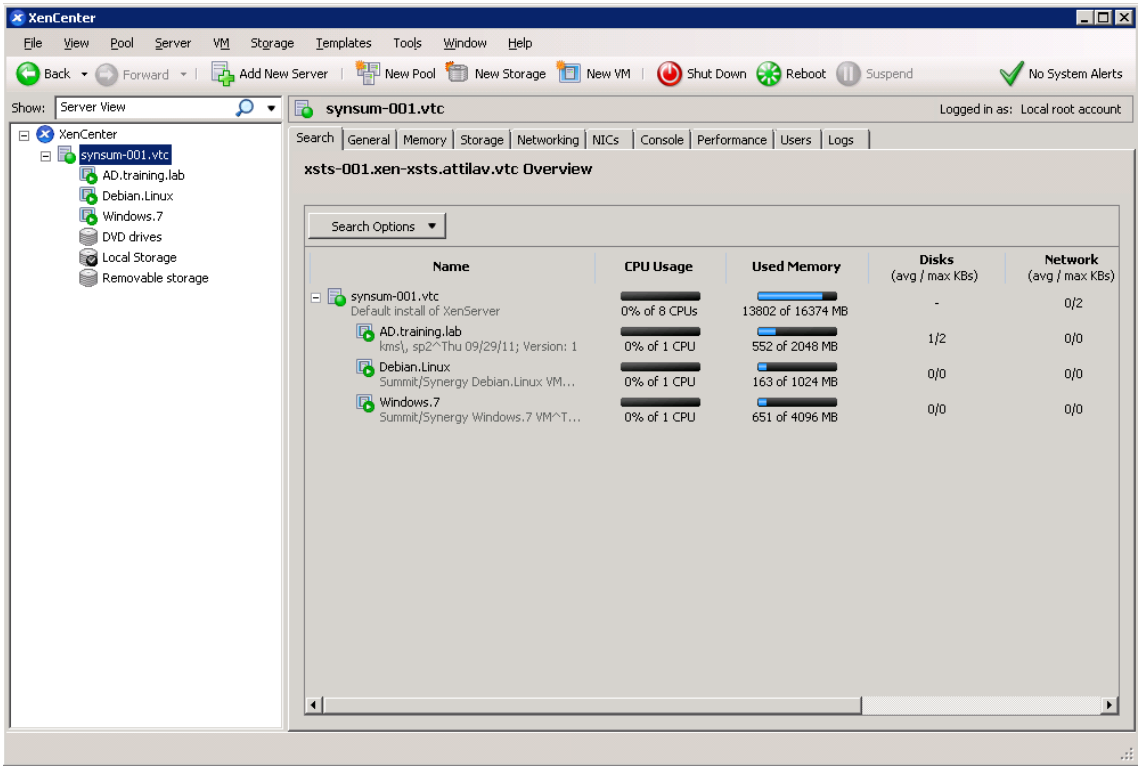
This information is valuable for your own analysis and can be forwarded to Citrix Technical Support.

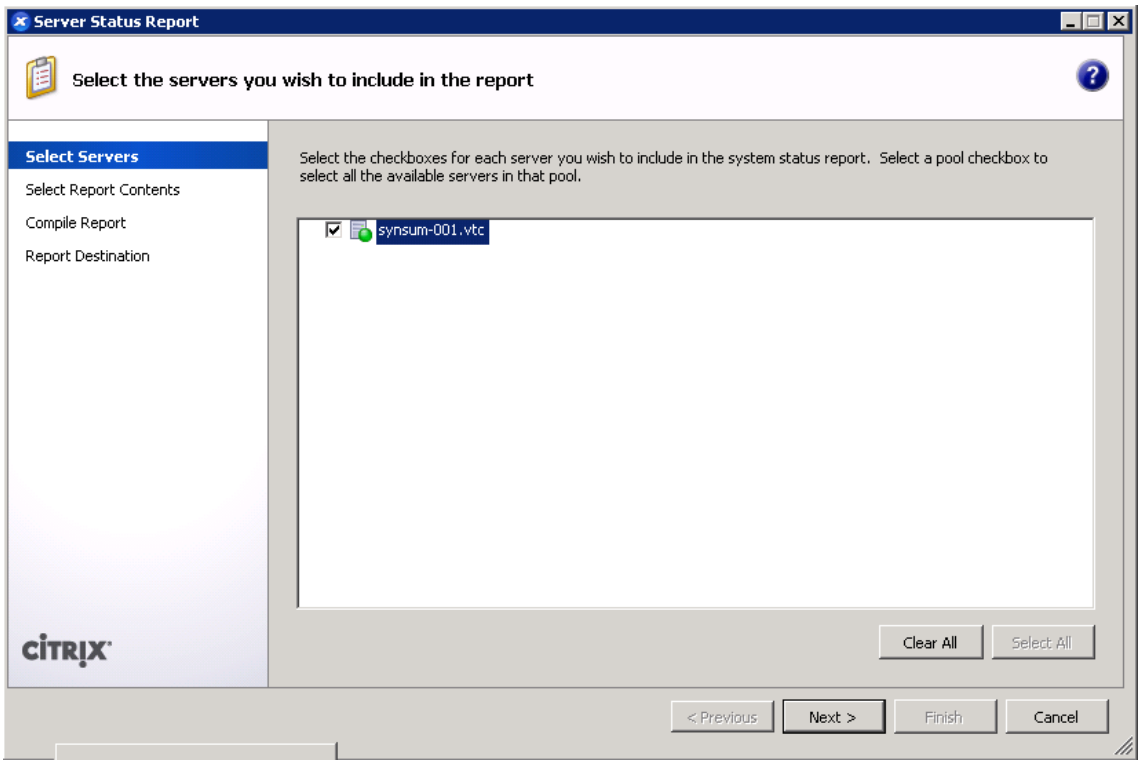
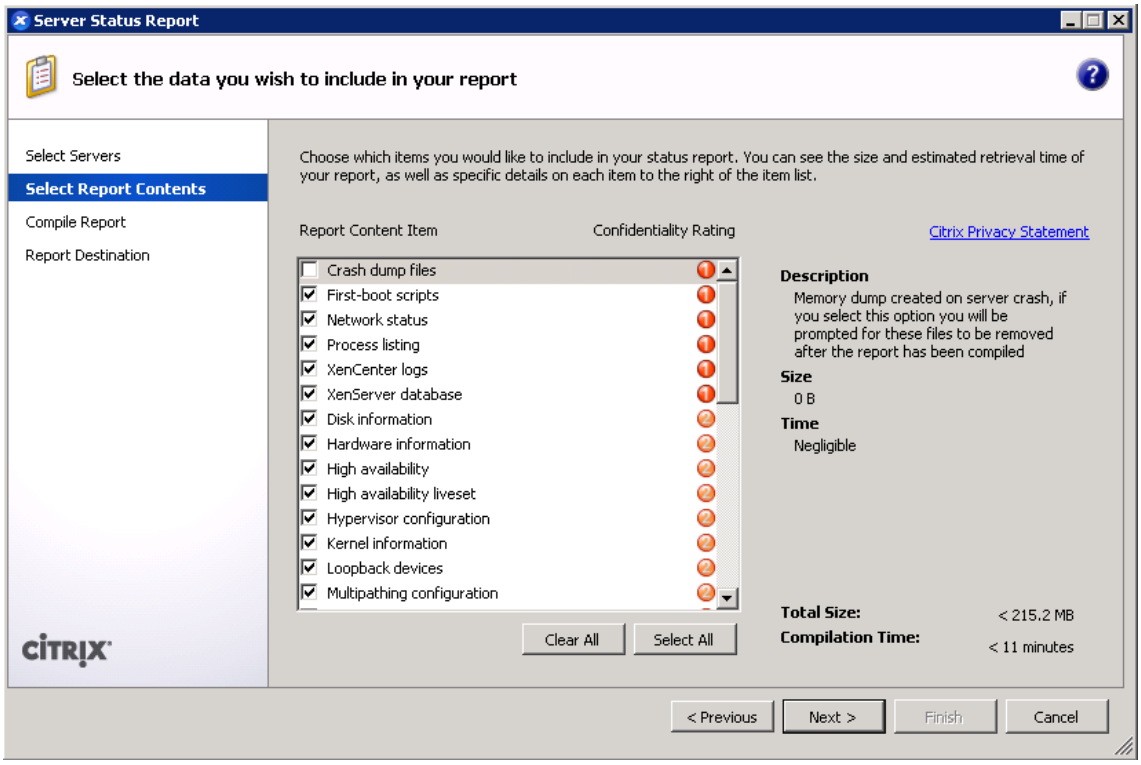
To complete this exercise, you must have the following:

- XenCenter
- SSH client (PuTTY)
- WinSCP

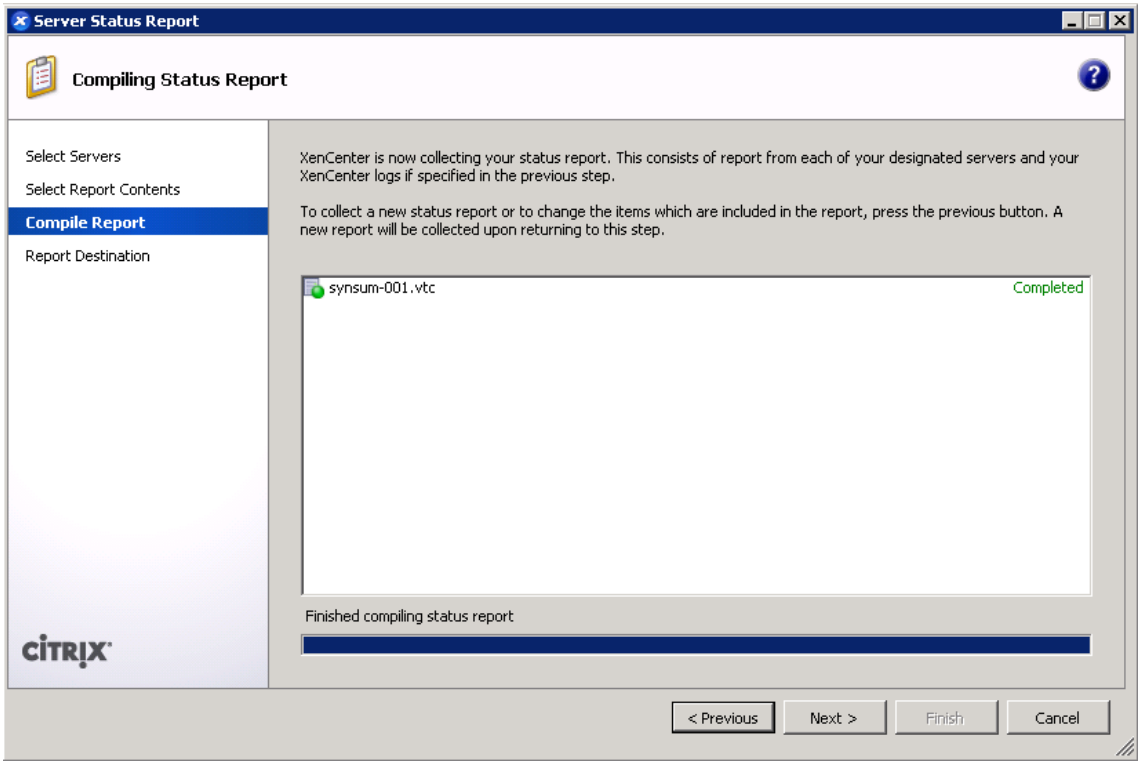
Step-by-step guidance

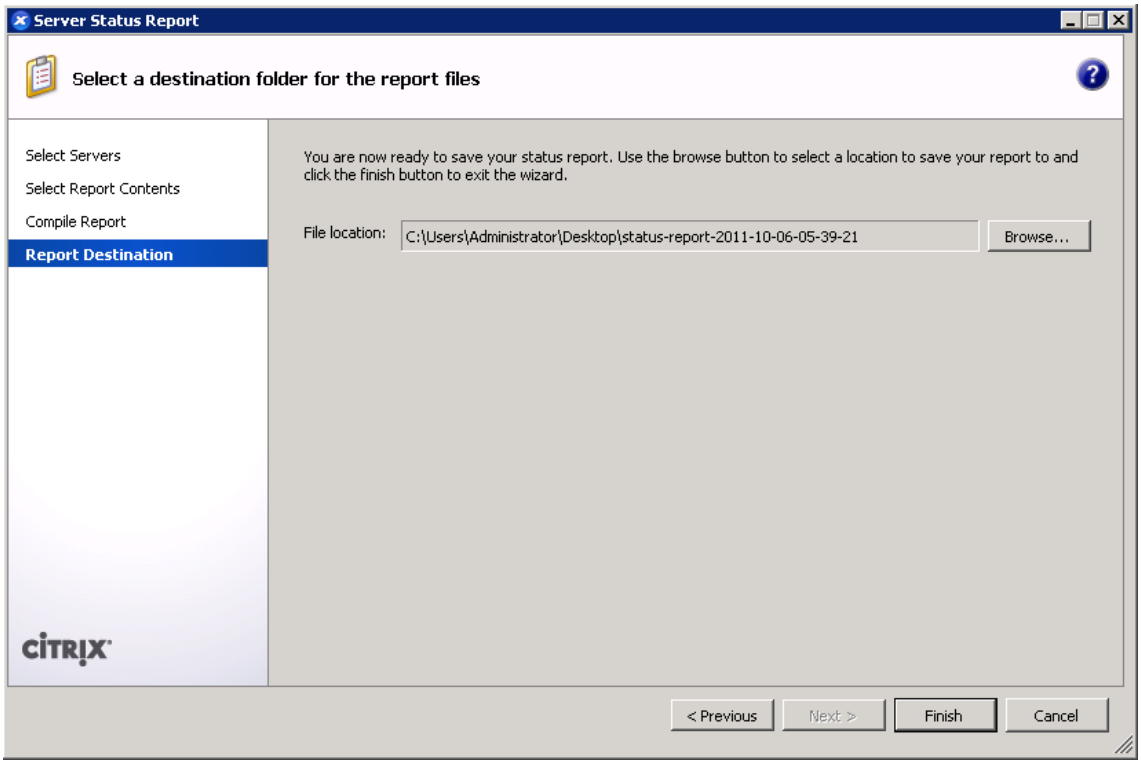
Estimated time to complete this lab: **15 minutes**.

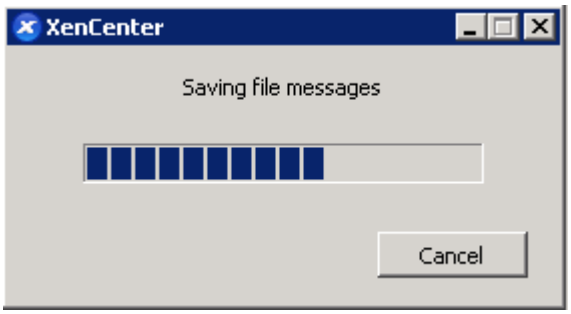
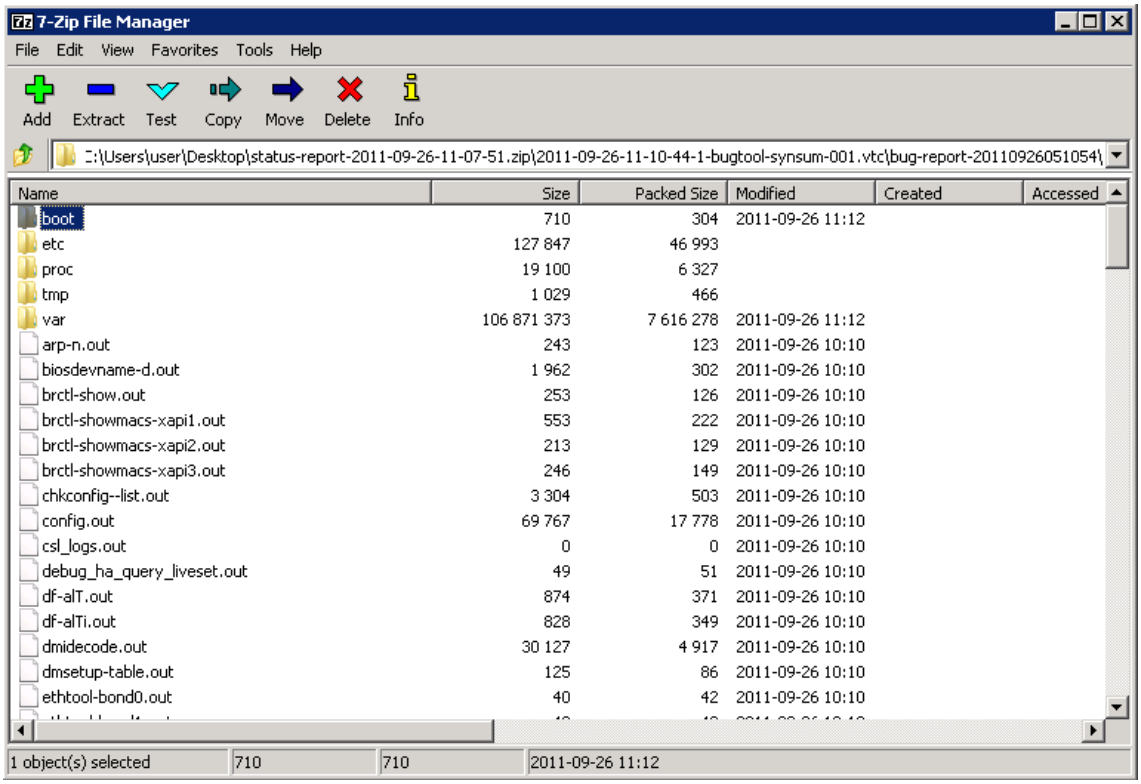
Step	Action
	Collect a Server Status Report via XenCenter:
1.	From your **Landing Desktop** launch **XenCenter** (if not already running) 

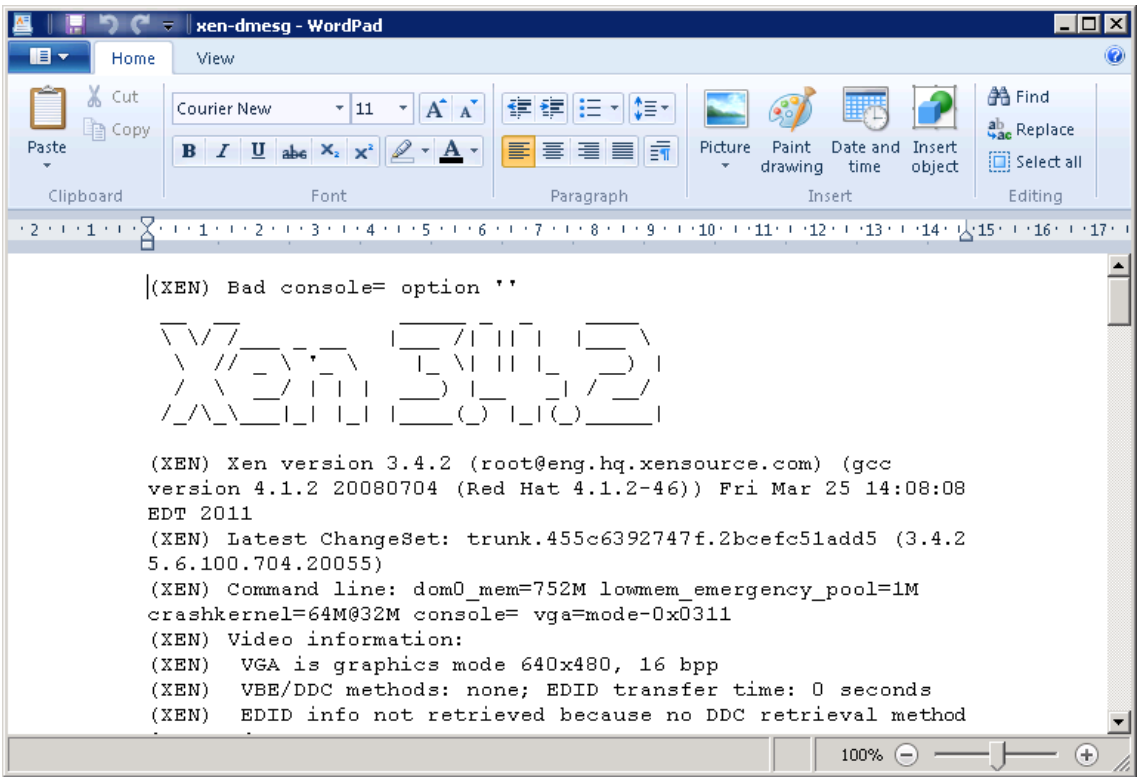
Step	Action
2.	Click **Tools** > **Server Status Report…** 
3.	Select the server to collect the status report from and click **Next**
4.	Review the list of Report Content. Use the **default** selections and click **Next** 

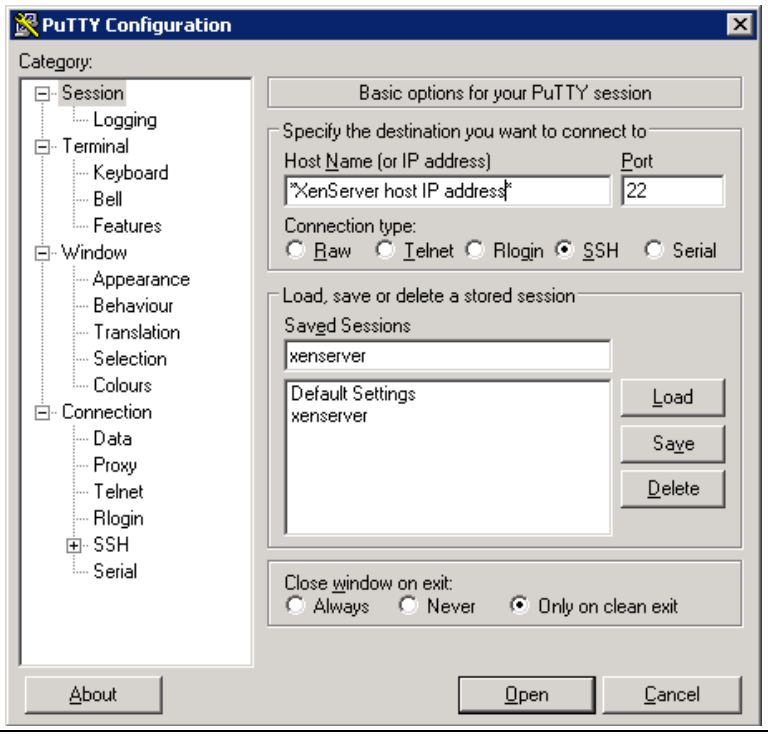
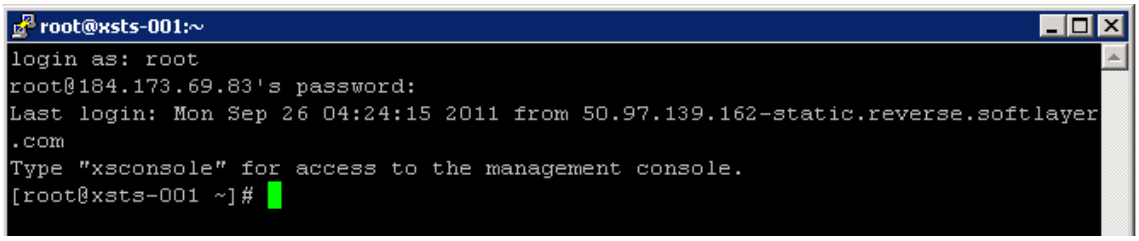
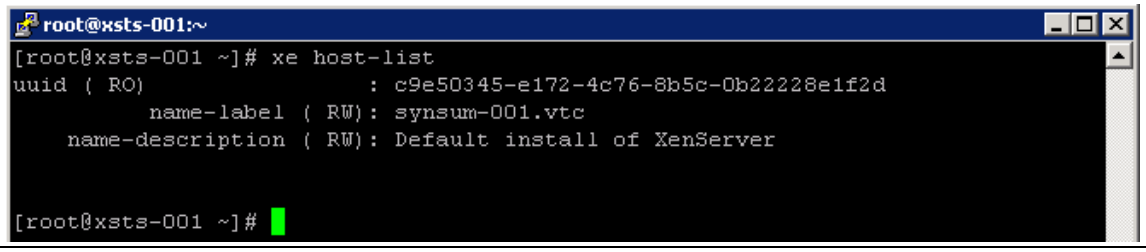
Step	Action
5.	After the report has been compiled and collected successfully click **Next**
6.	Browse to the desktop and click **Finish.**

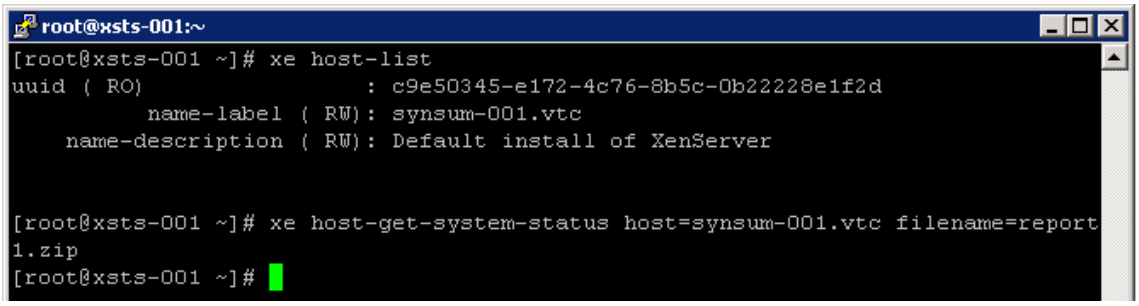
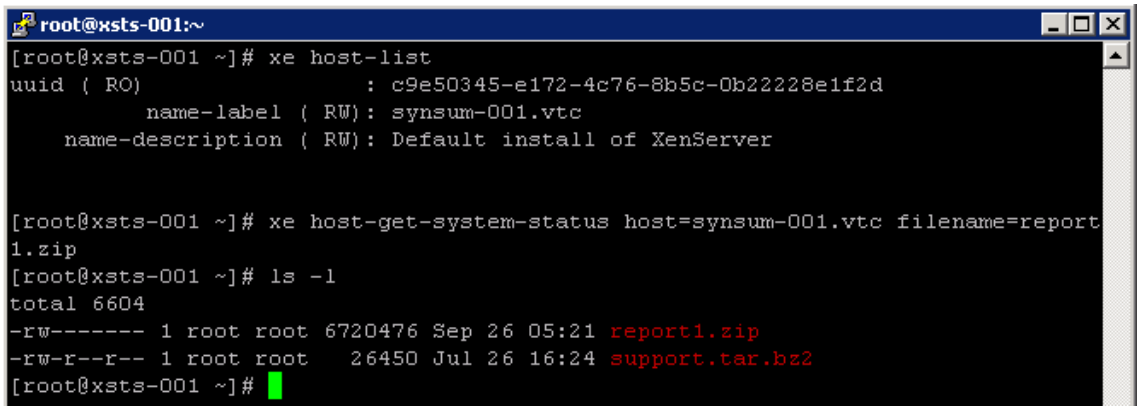


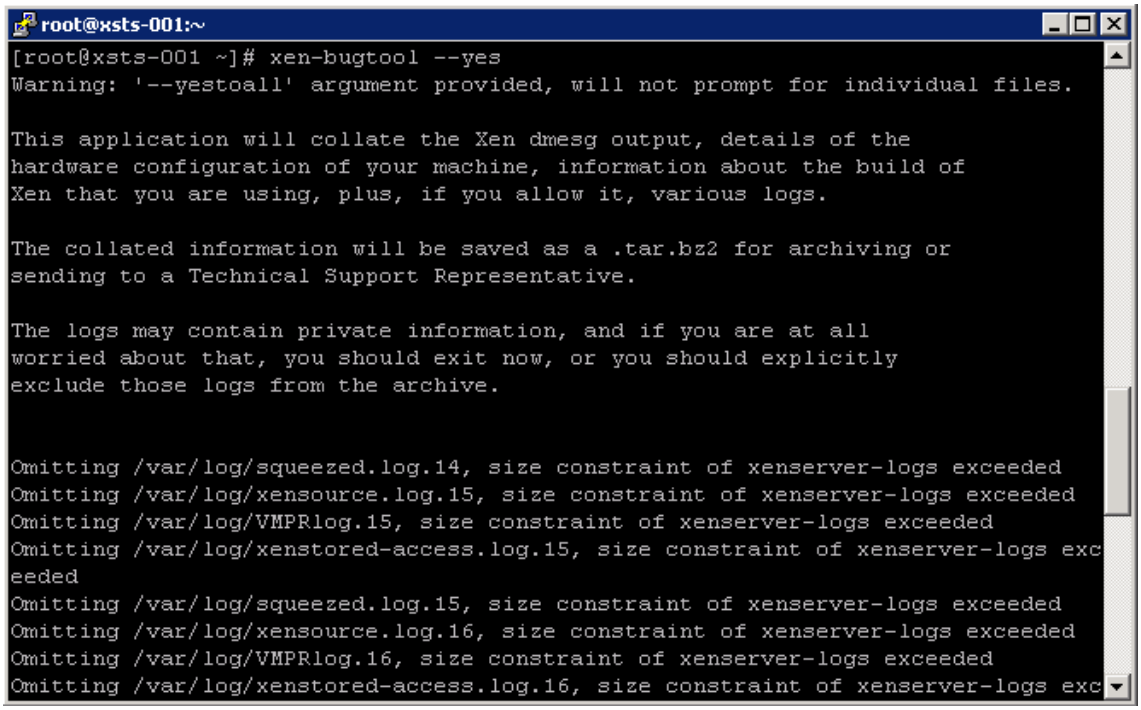
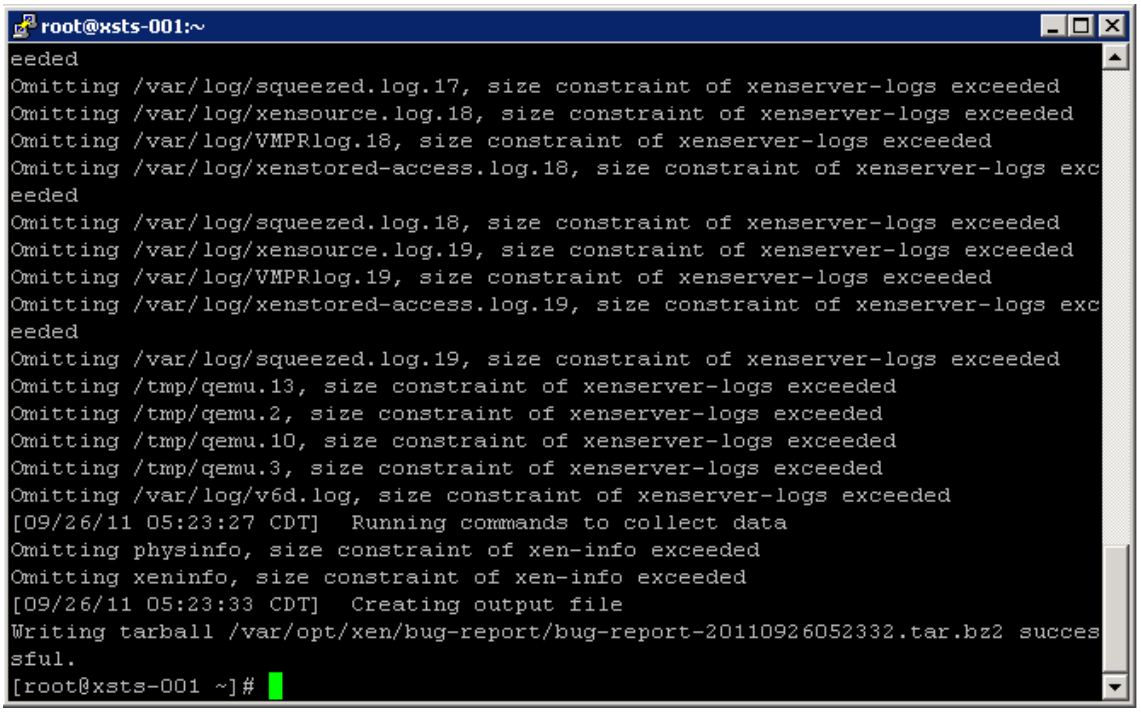


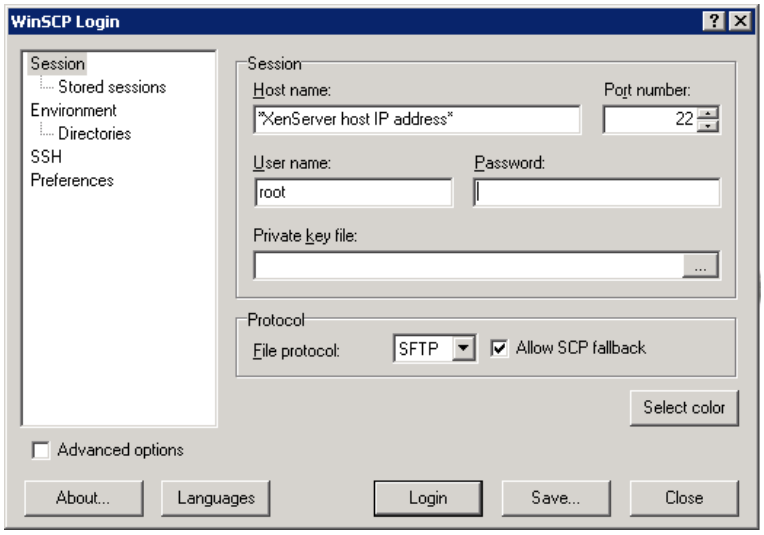
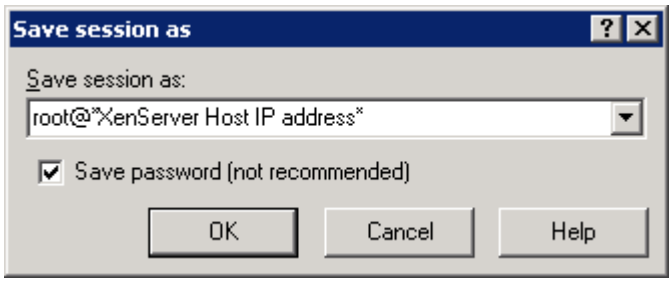
Step	Action
7.	The status report will be saved to your Landing Desktop 
	Open and review the content of the server status report:
8.	Open **.zip** file located on your Landing Desktop and browse through the folders to the **bug-report folder** 

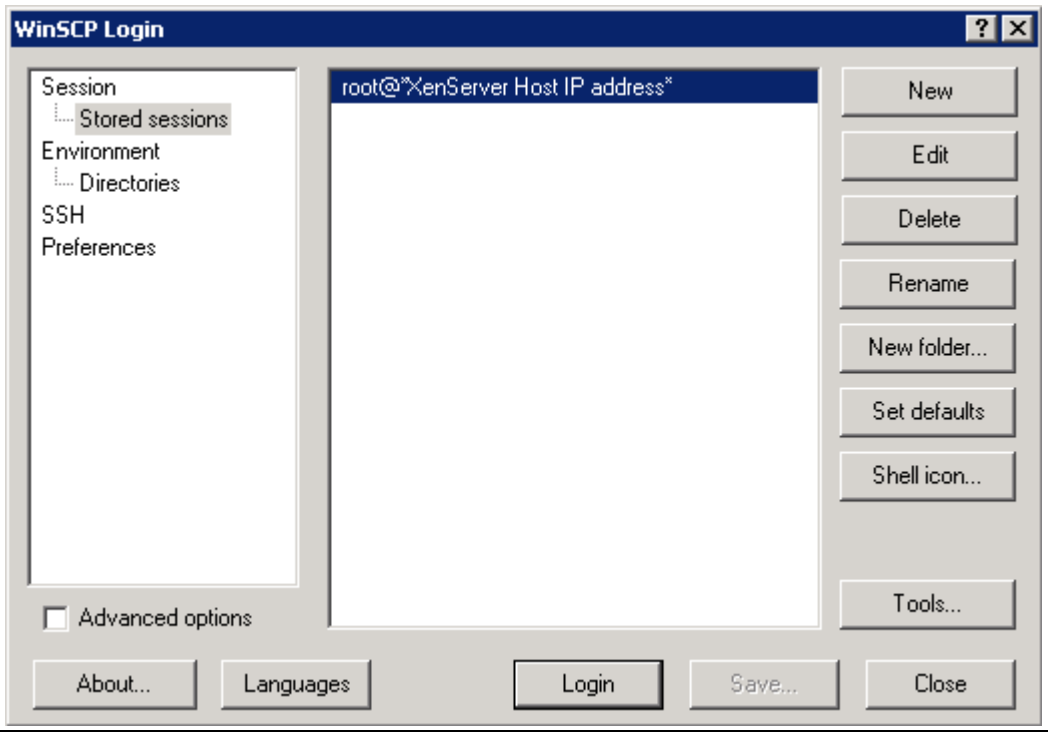
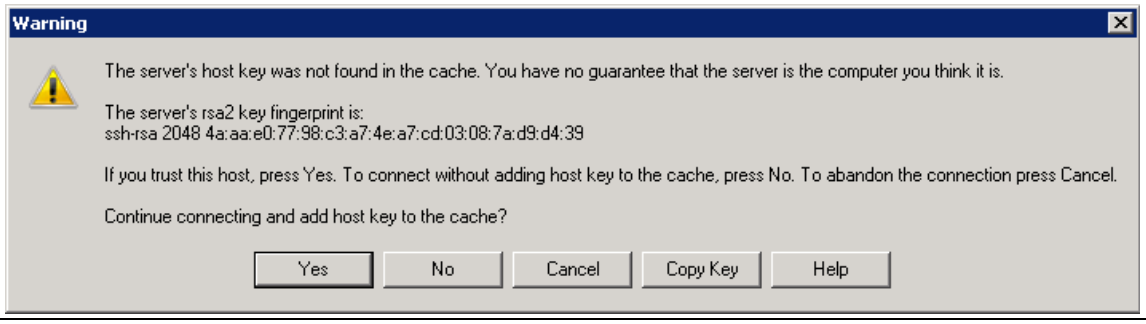
Step	Action
9.	Open the **xen-dmesg.out** file with WordPad and review  **Note:** This file contains information about the hypervisor. From this file we can confirm the **version** of the hypervisor i.e. 3.4.2, the **total amount of memory** detected, **CPU** information, even the control domain's/**dom0** creation parameters and much more.
	Collect a server status report via the CLI:

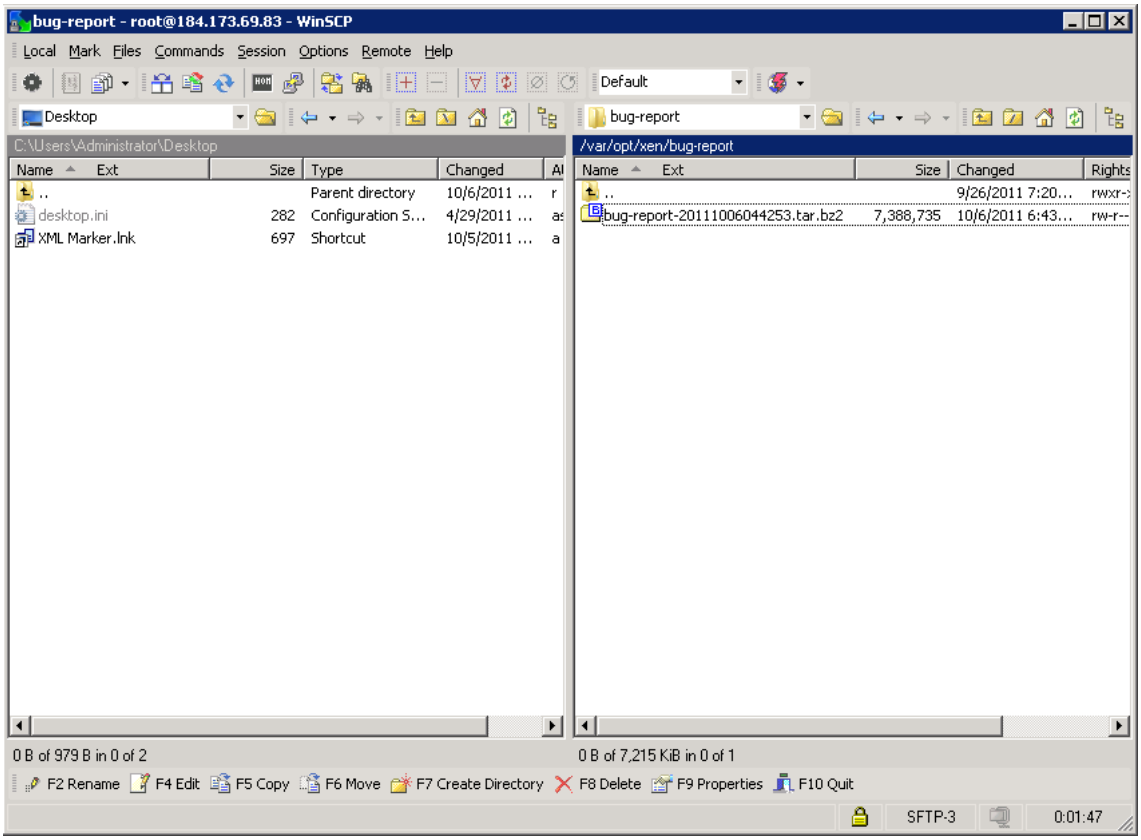
Step	Action
10.	Launch **PuTTY** from the Landing Desktop **OR** use an existing SSH session. 
11.	Login with the required credentials available from the Student Portal page. 
12.	Find the XenServer host information i.e. UUID, name label, etc. e.g. **xe host-list** 

Step	Action
13.	Collect the report using the **xe** command e.g. **xe host-get-system-status host=[server name] filename=[filename]**  **Note:** If no path has been designated in the **filename** parameter the file will be stored in the current folder. **Note:** The **xe** command requires that the **XAPI** service is running.
14.	List the folder contents with the **ls –l** command to locate the status report file i.e. **report1.zip**. e.g. **ls -l** 
	If the **xapi** service is not running or unable to start you can still collect a system report using the xen-bugtool:

Step	Action
15.	Run the xen-bugtool command to generate a server status report package e.g. **xen-bugtool --yes**  **Note:** The **--yes** parameter answers all prompts for confirmation with **yes**.
16.	When the package creation is complete the location of the package will be displayed in the console. The **default location** for the status reports is **/var/opt/xen/bug-report/** 
	Collect a system report from XenServer:

Step	Action
17.	Launch **WinSCP** from your Landing Desktop and connect to your designated XenServer by clicking **New** and entering the XenServer host IP address and credentials.  **Note:** Enter the credentials including Username and Password and click Save
18.	Save the connection information  **Note:** Tick the "Save password" box

Step	Action
19.	After saving the XenServer host credentials click **Login** 
20.	Accept any key exchange message 

Step	Action
21.	Browse to the default store location for the status report **(/var/opt/xen/bug-report)** and drag-n-drop the **.tar.bz2** file to your Landing Desktop.  **Note:** The contents of the status report is identical whether it is collected via the CLI or XenCenter
END OF EXERCISE	

Summary

Key Takeaways	The key takeaways for this exercise are: • You will be able to generate a system status report via XenCenter and CLI. • You will be able to collect a system status report using WinSCP.

Exercise 4: Collect and Review the Pool/Host Database

Overview

In this exercise we will locate the pool/host database and review the information stored within it.

In this version of XenServer the database is called state.db and is in XML format.

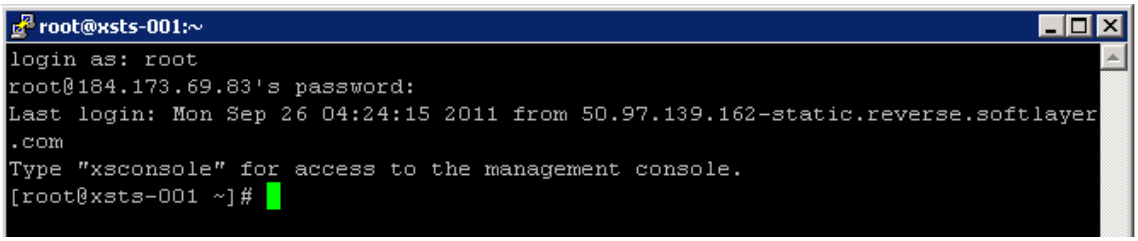
This database holds the pool/host configuration information which is critical to the functionality of the environment and should not be manually edited.

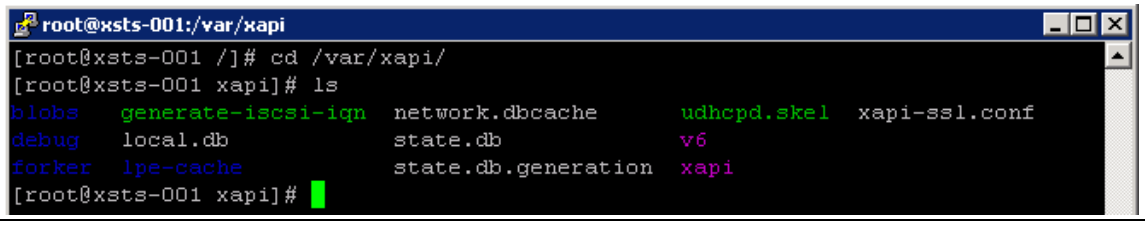
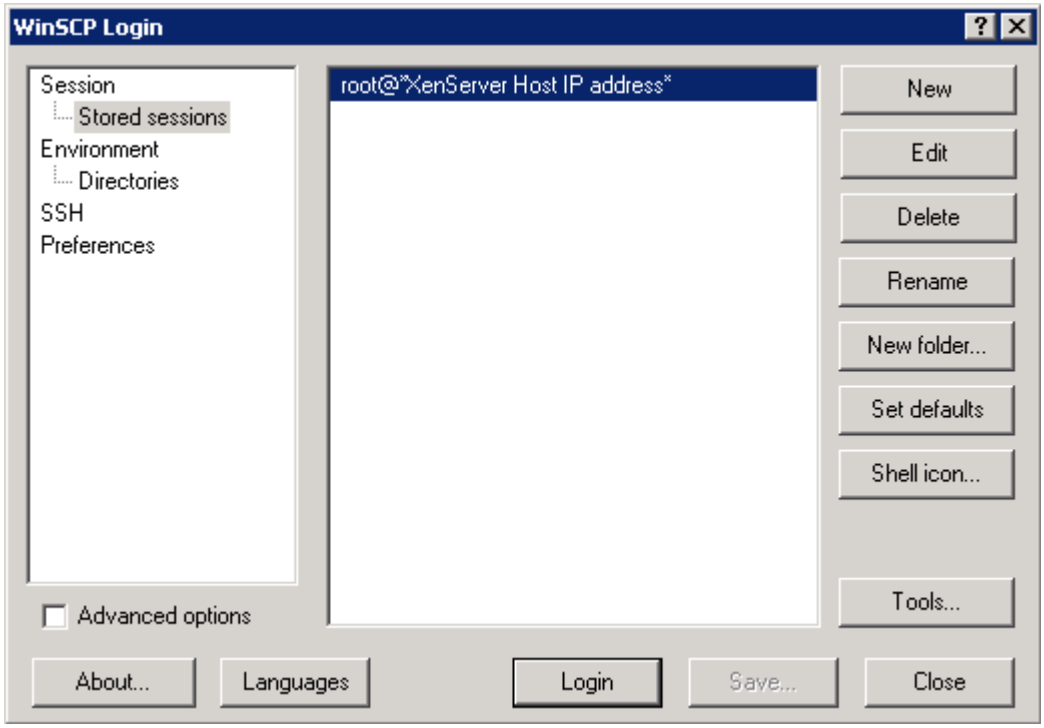
To complete this exercise, you must have the following:

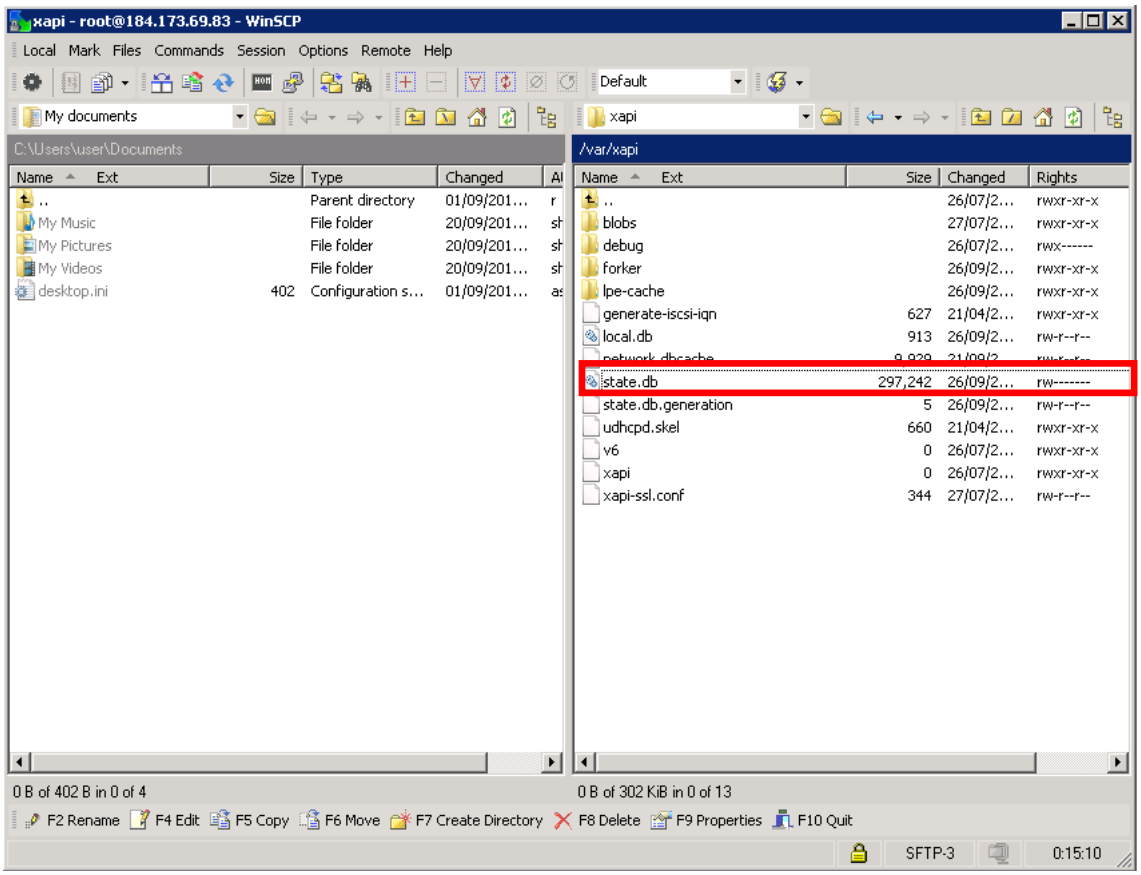
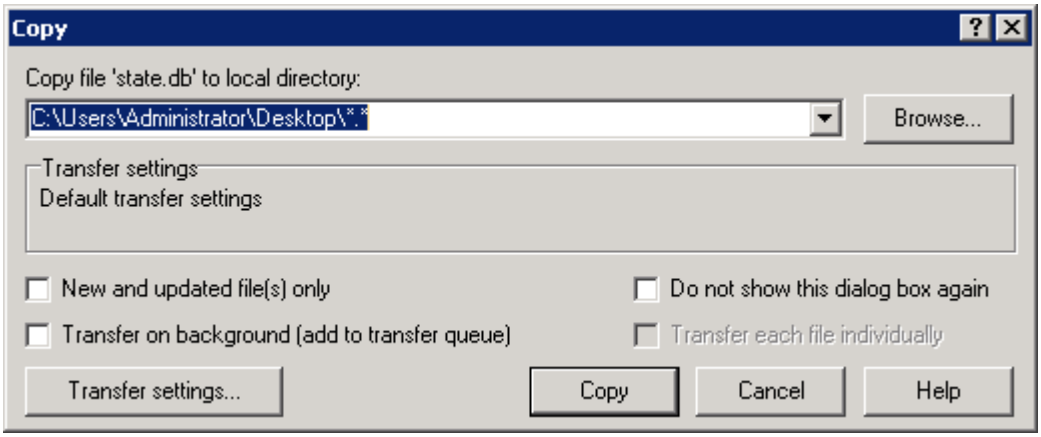
- XenCenter
- SSH client (PuTTY)
- WinSCP
- XML Marker

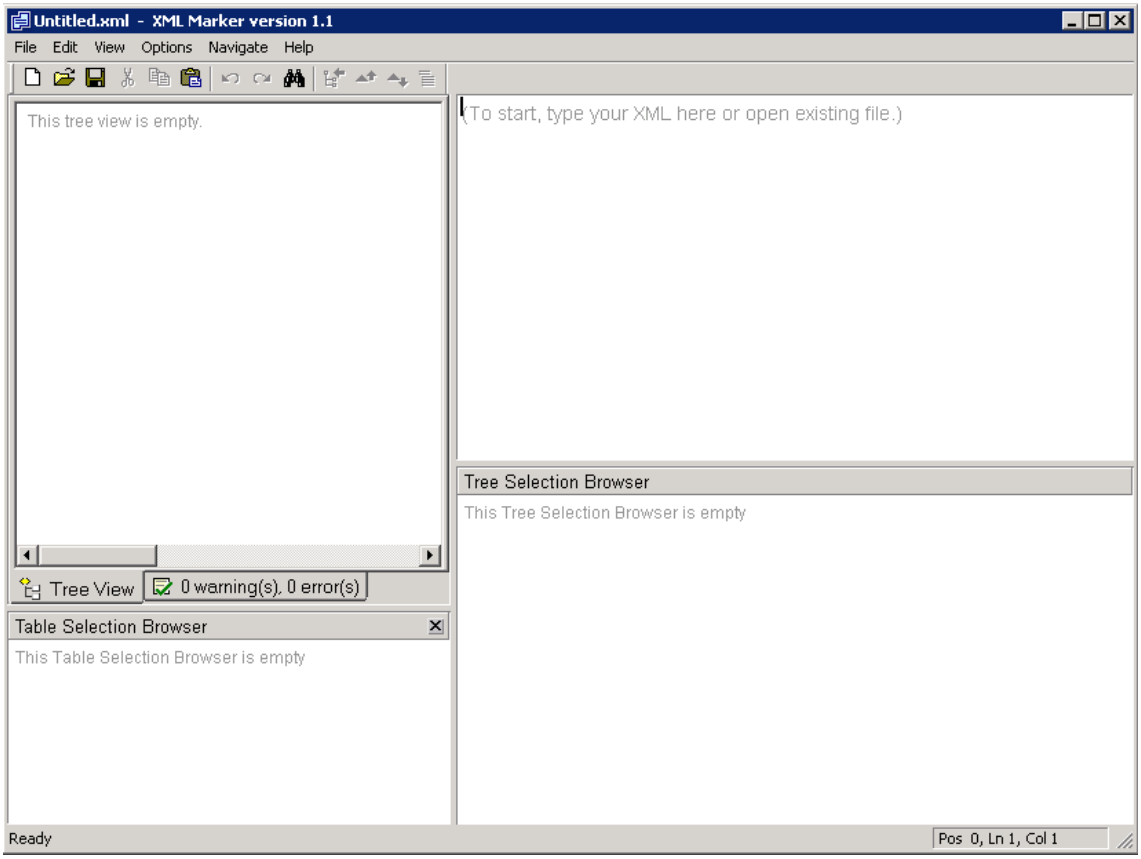
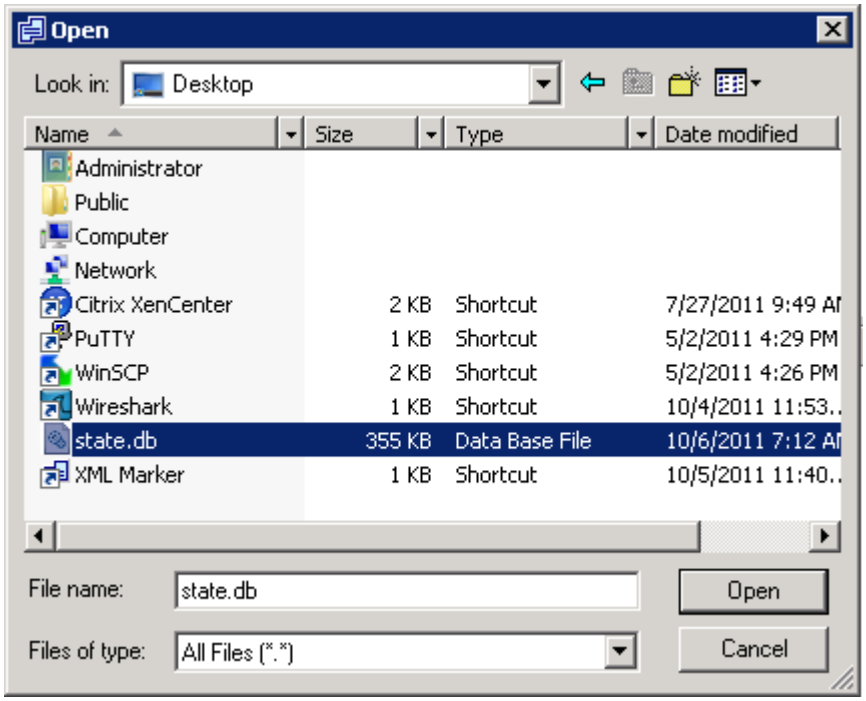
Step-by-step guidance

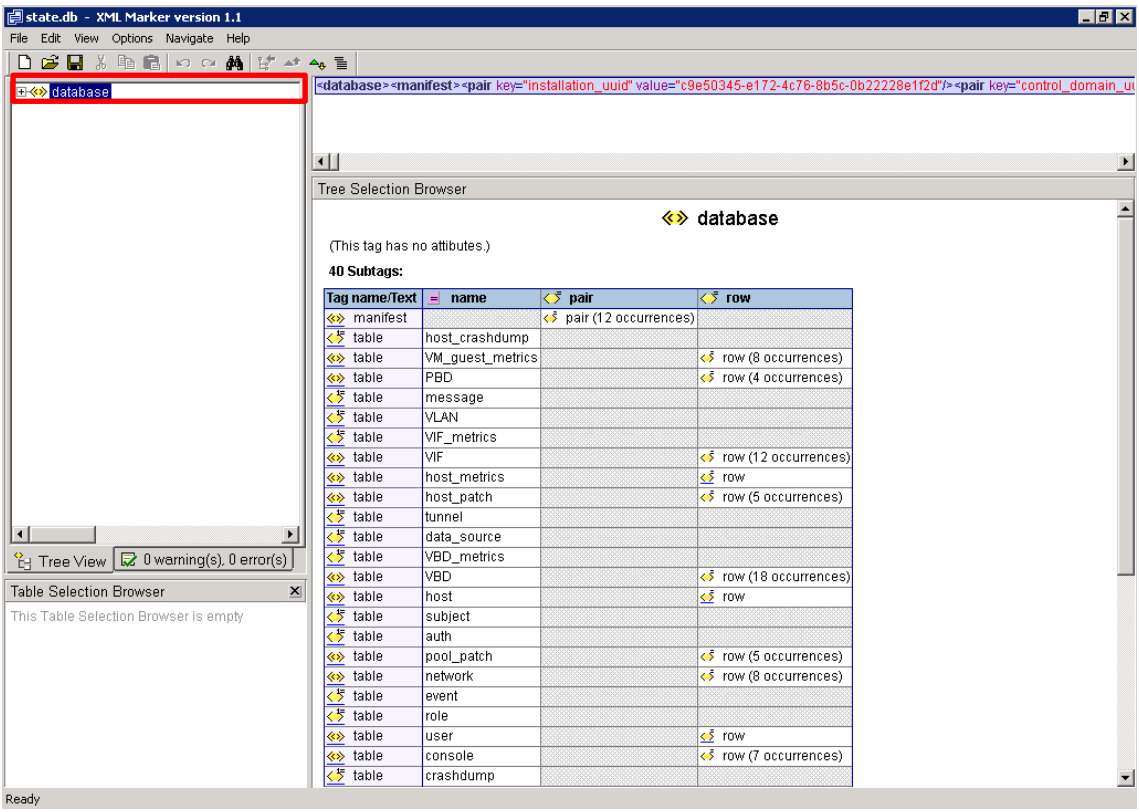
Estimated time to complete this lab: **15 minutes**.

Step	Action
	Locate the database file via the CLI:
1.	Launch a new SSH client **OR** duplicate an existing session of **PuTTY** from the Landing Desktop **OR** reuse an open session window. 
2.	Navigate to the folder location containing the database e.g. **cd /var/xapi**

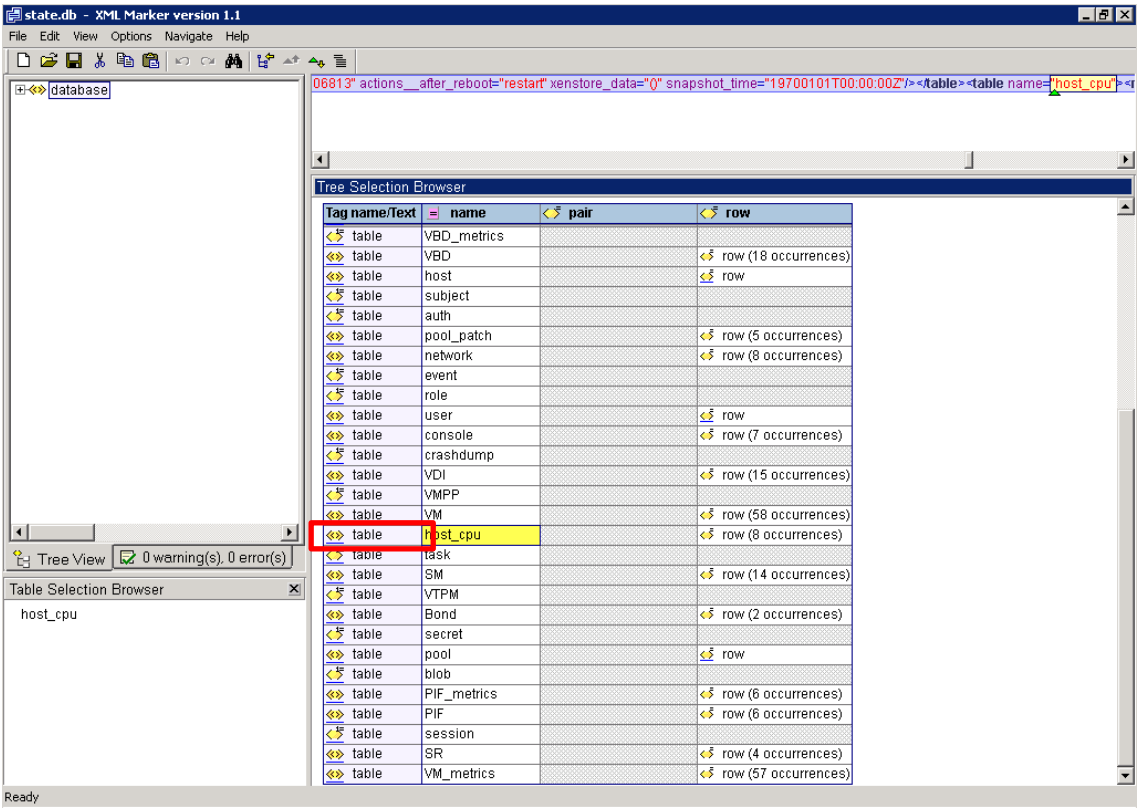
Step	Action
3.	List the contents of the /var/xapi folder e.g. **ls** 
4.	Confirm the presence of the **state.db** file **Note:** Running **xe pool-dump-database** command is the same as copying the state.db to another location. This command is covered in Exercise 5.
	Use WinSCP to collect a copy of this file:
5.	Use an existing **WinSCP** session or re-launch **WinSCP** from your Landing Desktop by selecting your saved session information and click **Login.** 

Step	Action
6.	Navigate to the **/var/xapi** folder location using WinSCP 
7.	Drag and drop a **copy** of the state.db file to the **Landing Desktop** 
	Review the contents of the **state.db** file:

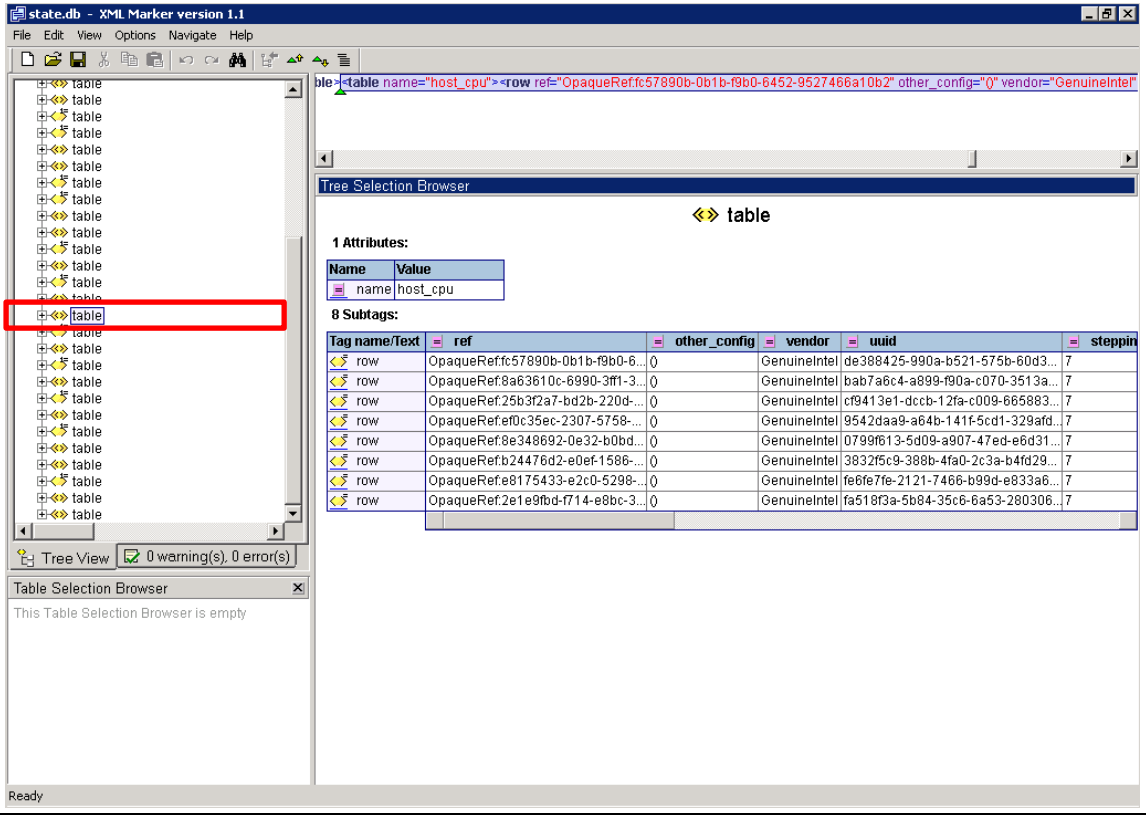
Step	Action
8.	Launch **XML Marker** from the **Landing Desktop** 
9.	Open the **state.db** file located on your Landing Desktop with **XML Marker**  **Note:** Ensure you select **All Files** from the Files of Type dropdown menu.

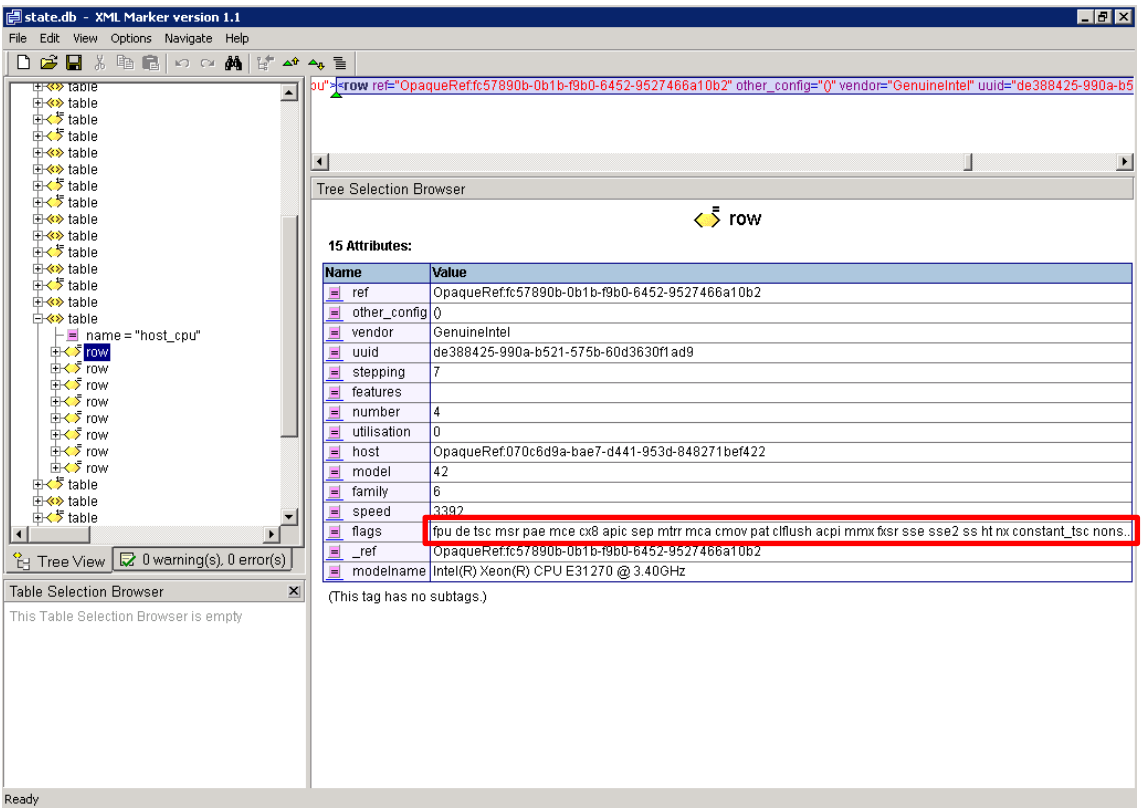
Step	Action
10.	Single click the **Database** object in the left column.  **Note:** Double clicking a database object in the bottom right panel (Tree Selection) will display the table/object rows and their description.

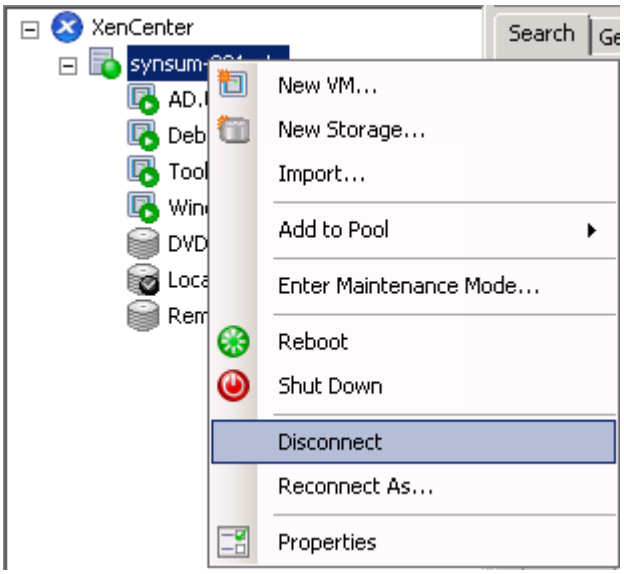
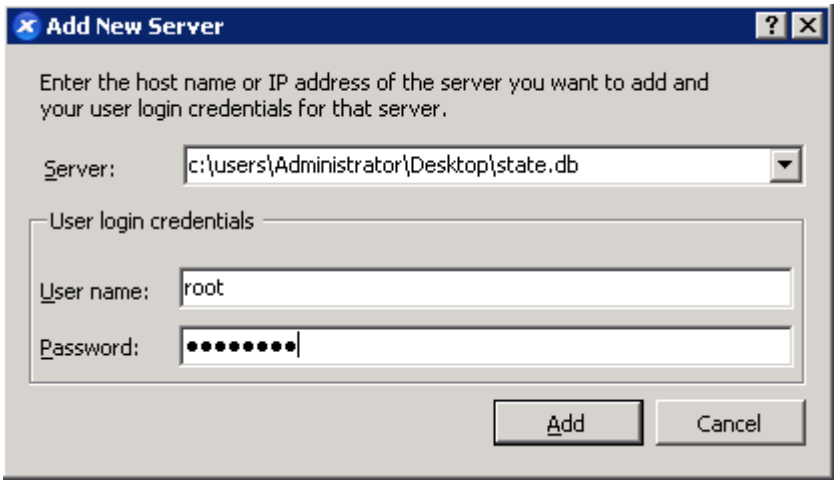
Step	Action
11.	In the right **Tree Selection Browser** pane click the table **icon** associated with the **host_cpu** entry.

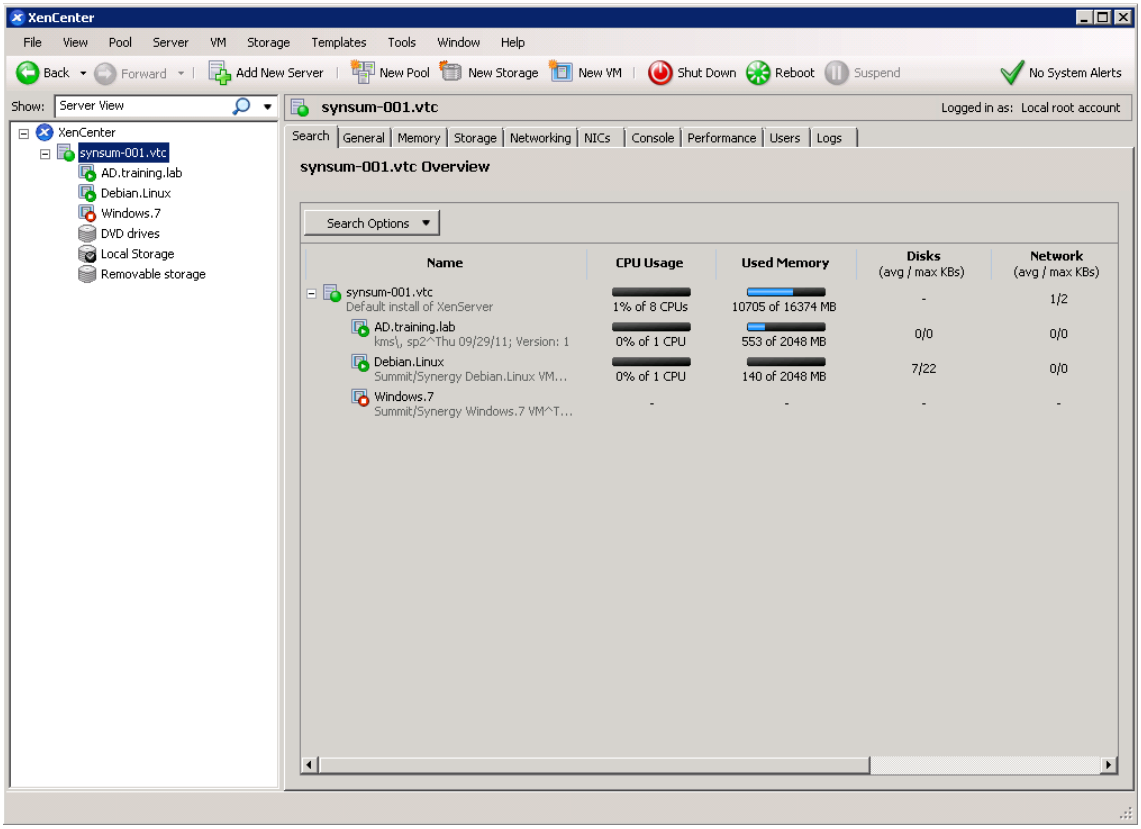


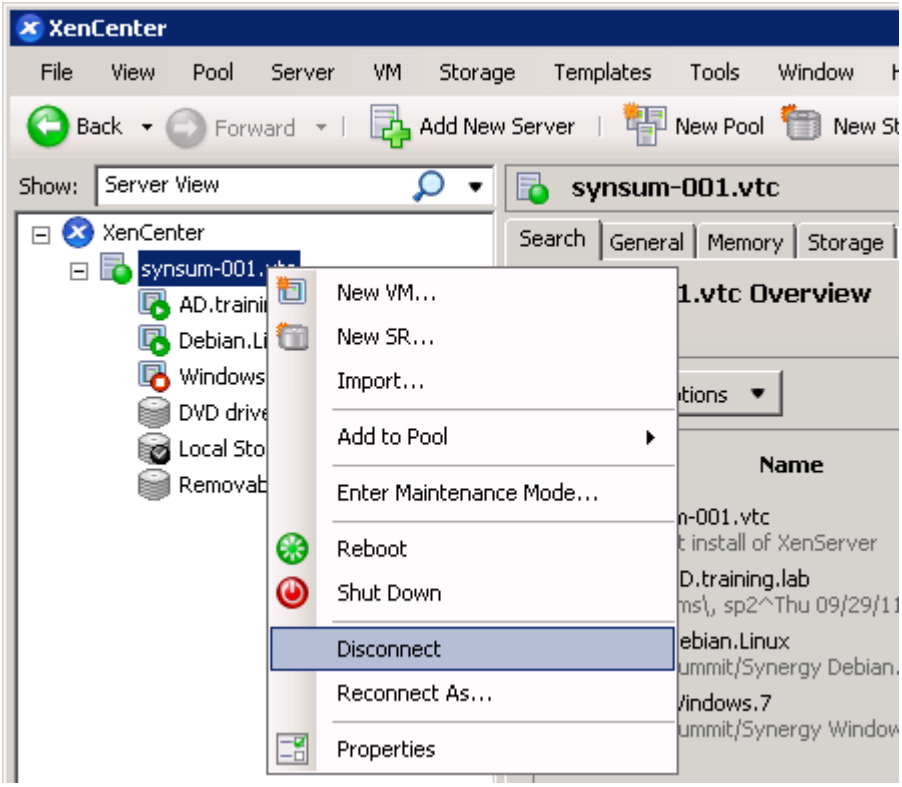
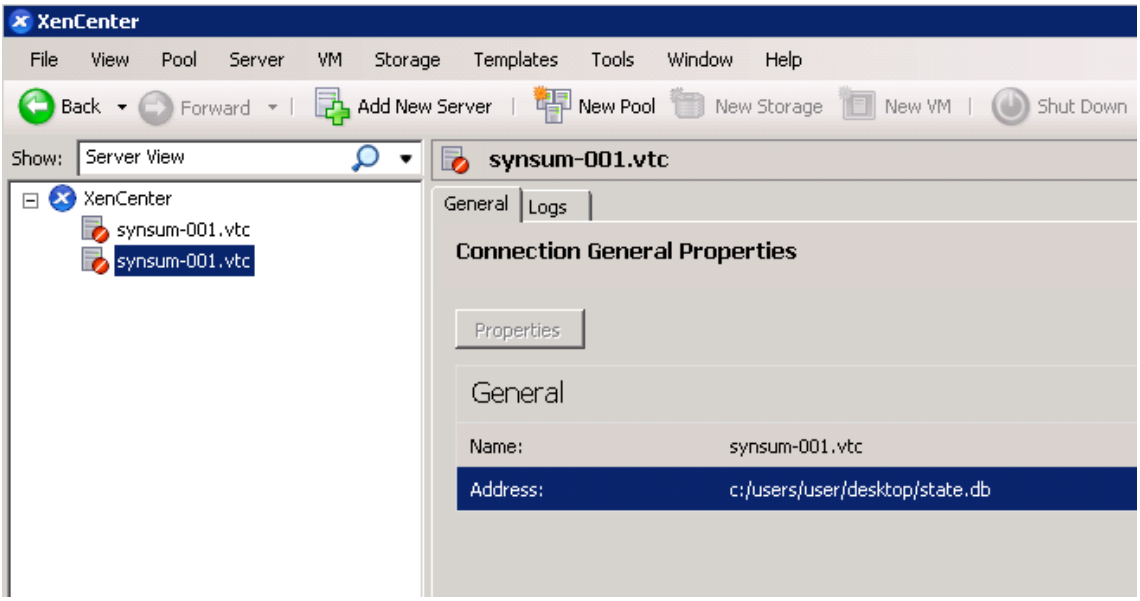
Step	Action
12.	Click the plus (+) sign for the highlighted table object and select the first row

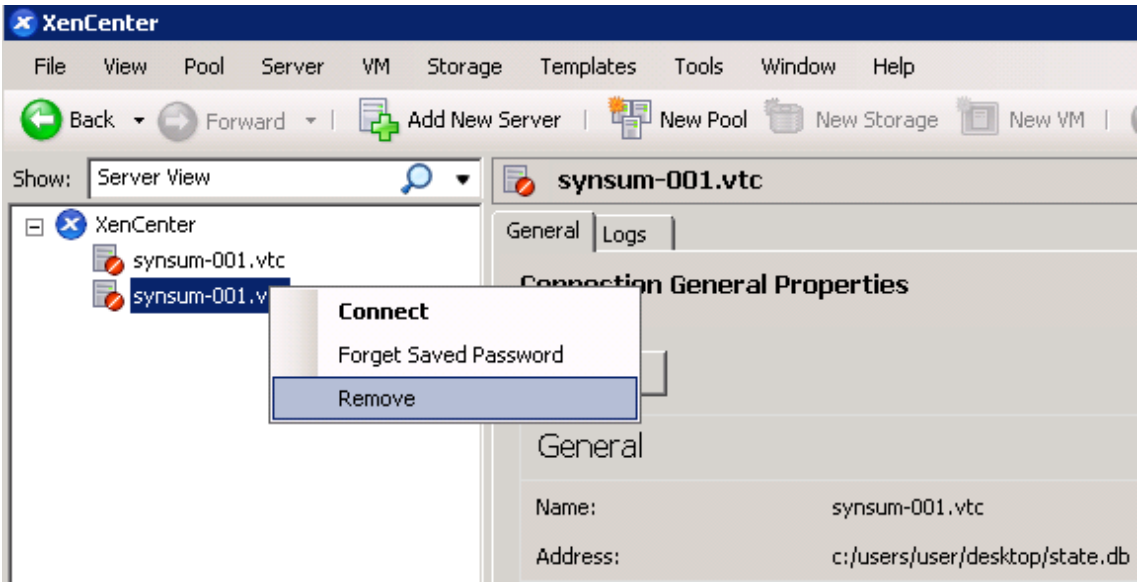


Step	Action
13.	**Review** the CPU flag information contained in the database  **Note:** This table contains the CPU information detected by the Control Domain (dom0). The **flags** section contains the CPU features/functions detected. **Warning:** Do not edit a live database as this can corrupt the configuration and affect your environment.
14.	Feel free to **explore** the database further to view the content contained within it
15.	Close the **XMLMarker** application
	Use XenCenter to open a copied database to display basic information about a pool/host configuration:

Step	Action
16.	Right click on your XenServer host and select **Disconnect** 
17.	In XenCenter click **ADD a Server** and enter the location of the copied state.db (**c:\users\Administrator\Desktop\state.db**) file instead of the IP address. 

Step	Action
18.	Navigate through the settings to review the host configuration  **Note:** The information displayed is static and represents the state of the pool/host when the state.db was copied.

Step	Action
19.	Disconnect from the "New Server" we added in the previous step. 
20.	Remove the newly added server connection information. Ensure that the correct entry is removed by verifying the **Address** parameter on the General tab in XenCenter. 

Step	Action
21.	Right click and select **Remove** 
END OF EXERCISE	

Summary

Key Takeaways	The key takeaways for this exercise are: • You will be able to locate, collect the pool/host database. • You will be able to view database information using 3rd party tools (XML Marker) or XenCenter.

Exercise 5: Backing up XenServer

Overview

In this exercise we will review possible backup options in XenServer. To mitigate the increased risks of failures in a virtual environment it is critical that a properly designed backup and recovery plan is in place.

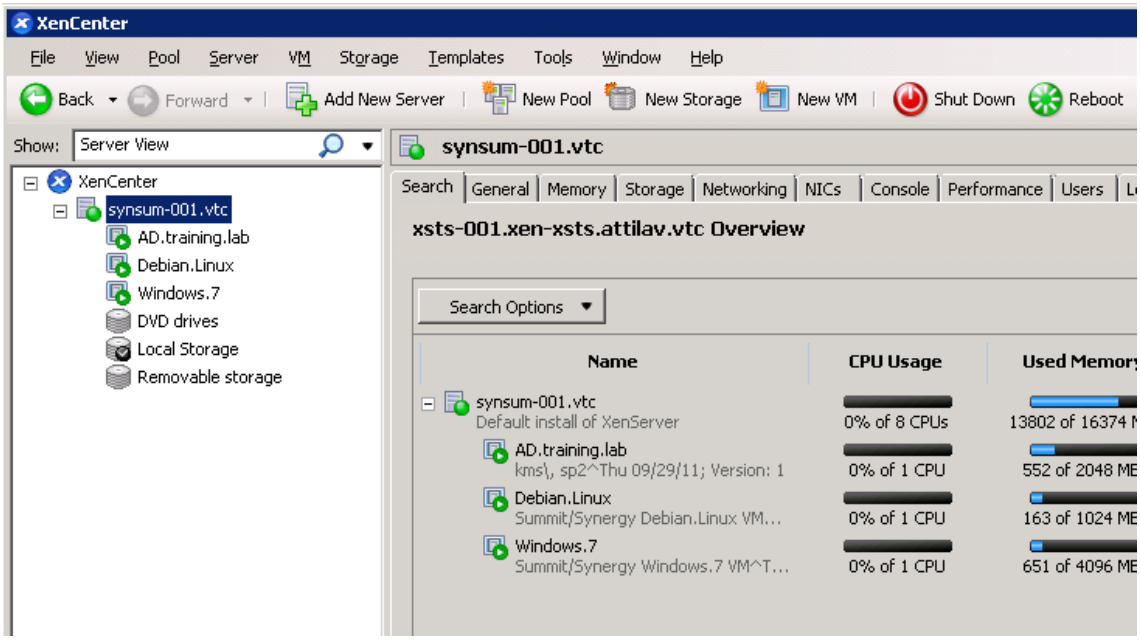
XenServer allows for the backup of three types of data i.e. Control Domain, VM and Pool/VM Metadata which we will review in this exercise.

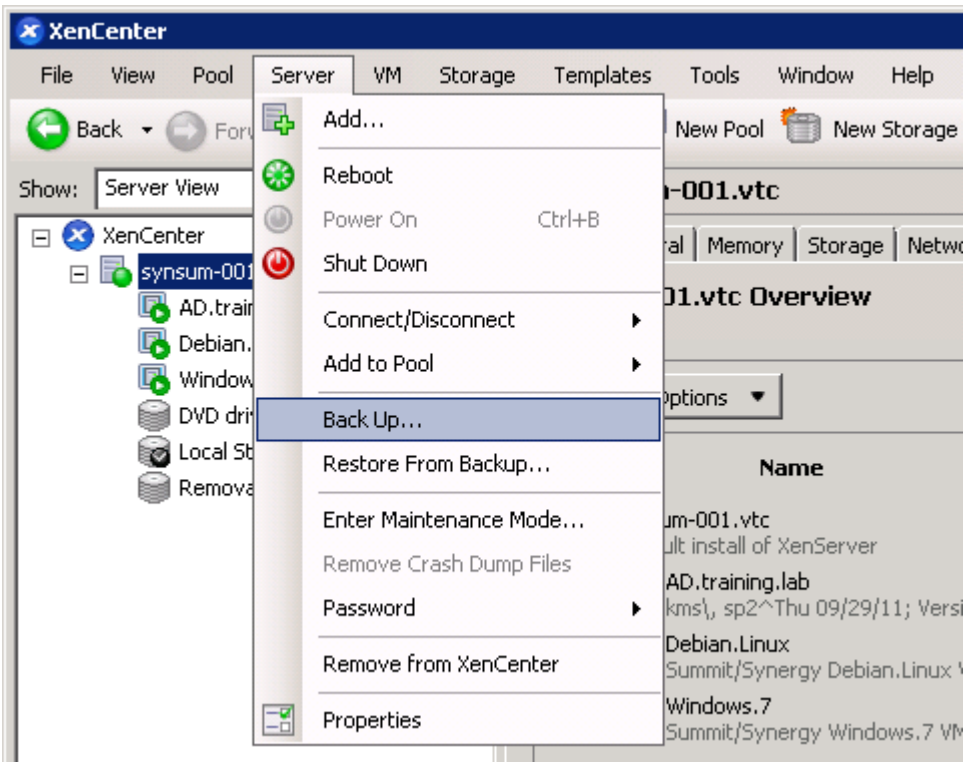
To complete this exercise, you must have the following:

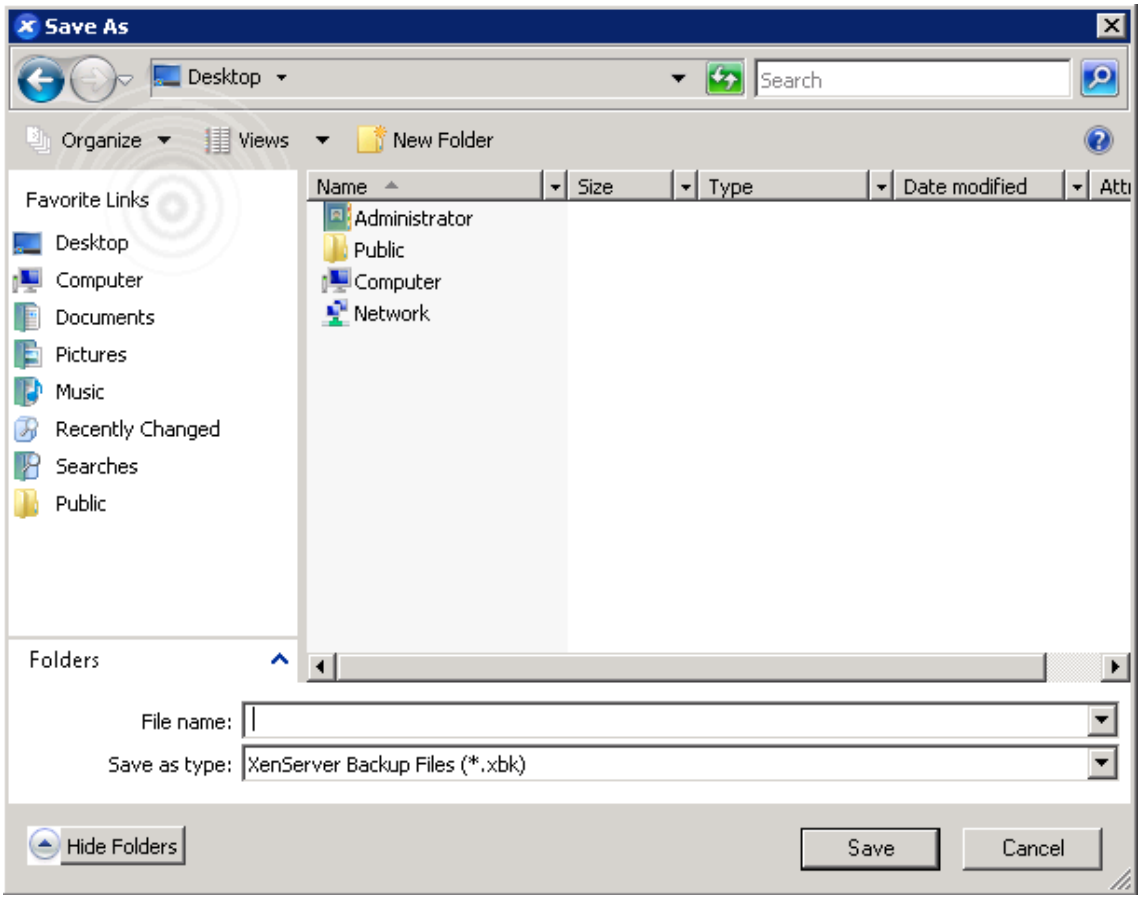
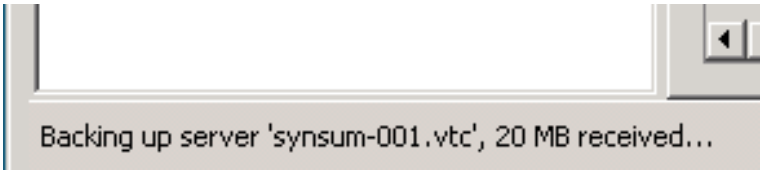
- XenCenter
- SSH Client (PuTTY)

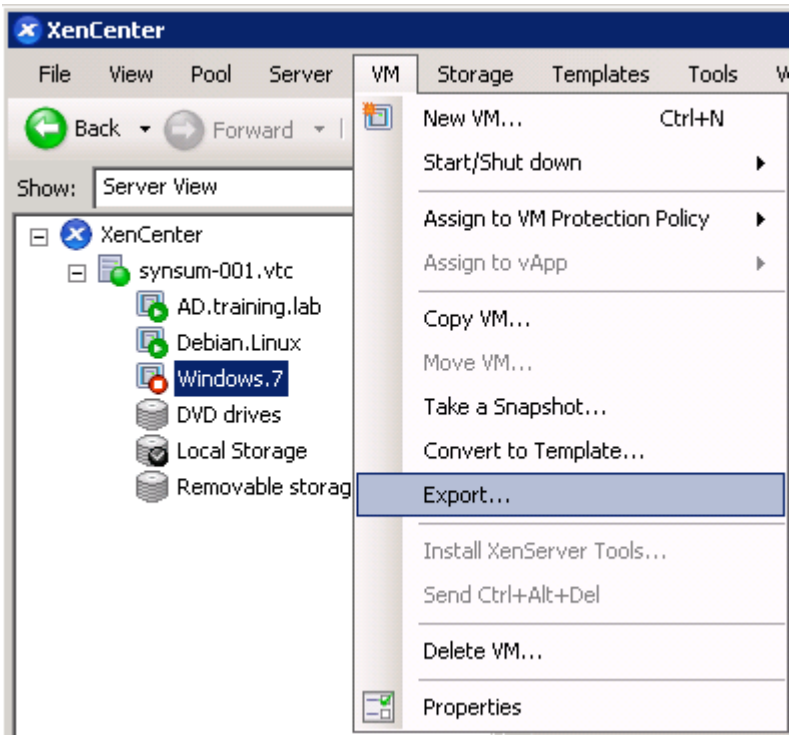
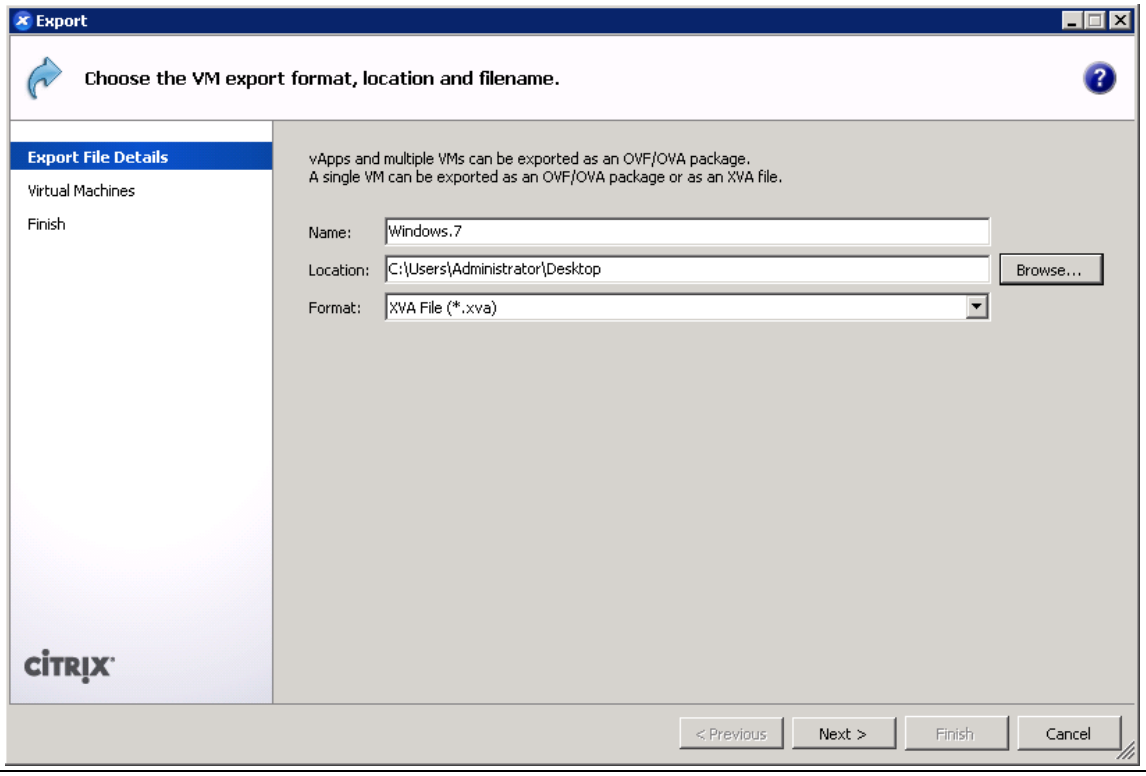
Step-by-step guidance

Estimated time to complete this lab: **15 minutes**.

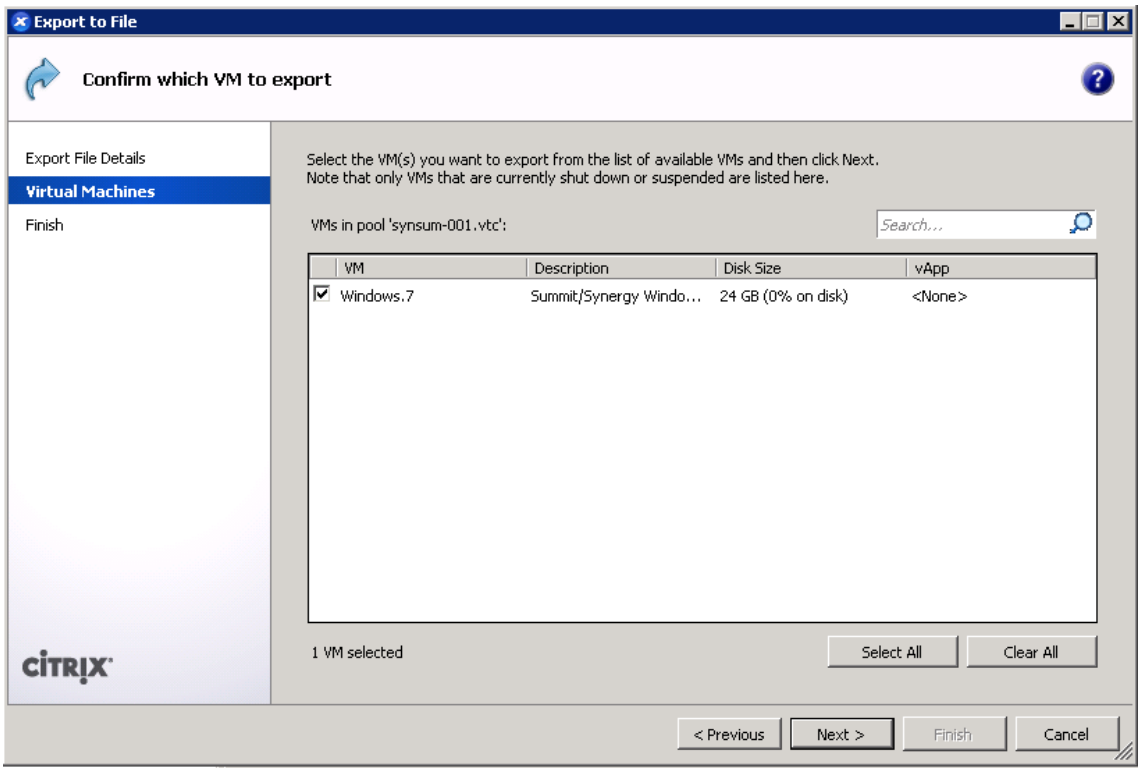
Step	Action
	Backup a XenServer Host via XenCenter:
1.	Launch XenCenter and connect to your designated XenServer (if required)
2.	Highlight the XenServer host which we want to backup. In your environment a single host will be available. 

Step	Action
3.	Click **Server > Back Up…** 

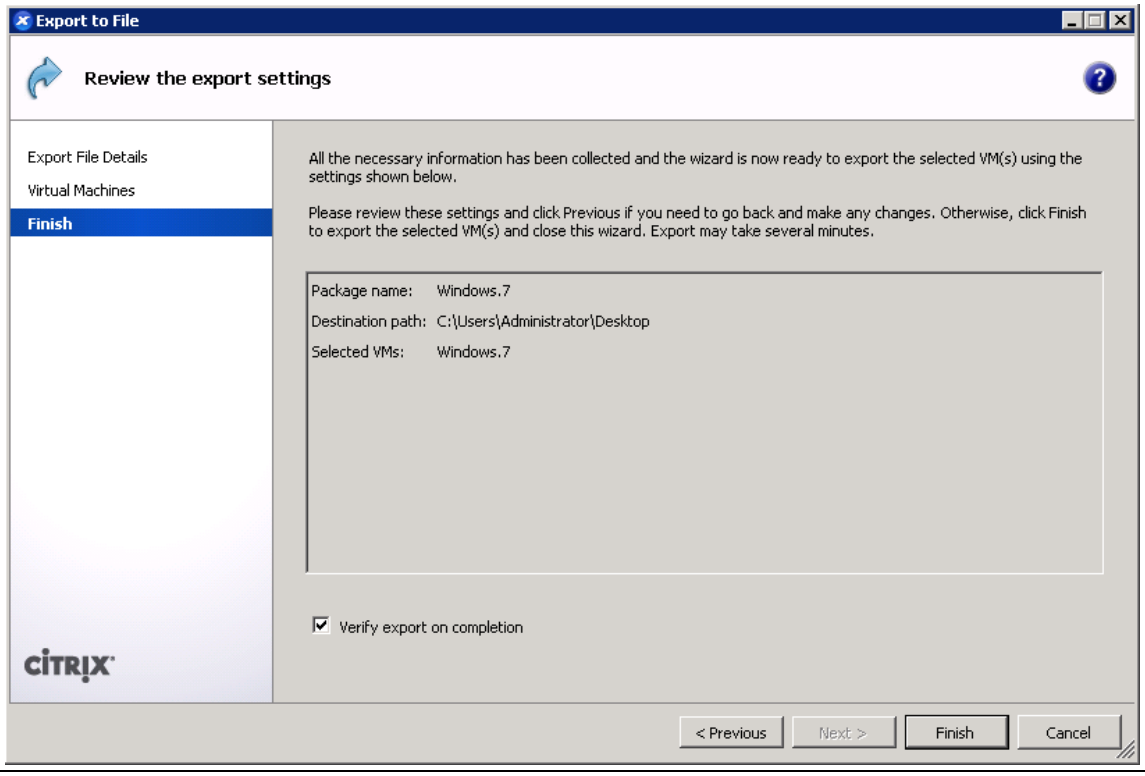
Step	Action
4.	Provide a **filename** for the backup file e.g. **host_backup.xbk** and save the file to your Landing Desktop.  **Note:** The backup should take a couple of minutes to complete
5.	**Verify** the backup process is running by reviewing the status bar at the bottom of the XenCenter console 
6.	The .xbk file will appear on the Landing Desktop when the backup is complete **Note:** The backup file is generally about 500MB in size
7.	Delete the **host_backup.xbk** file from the Landing Desktop
	Backup a virtual machine:

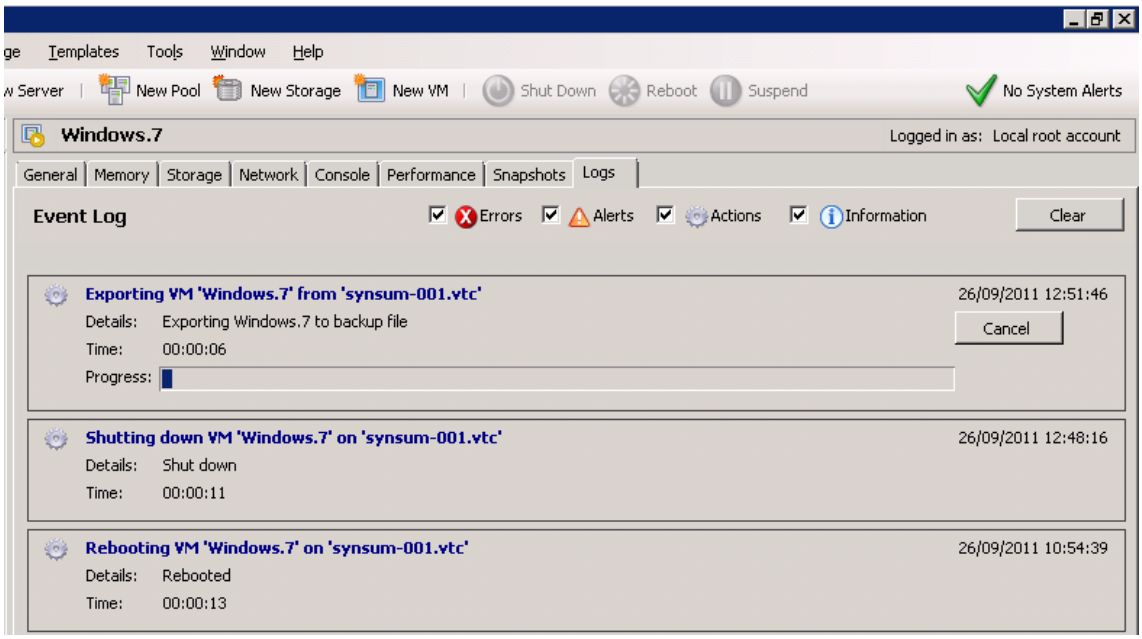
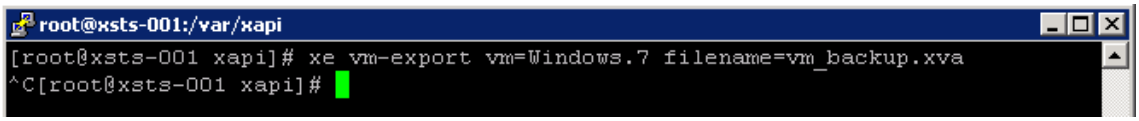
Step	Action
8.	Ensure the **Windows.7** virtual machine is in a stopped state before exporting. Highlight the Windows.7 virtual machine and click **VM > Export…** 
9.	Select the Landing Desktop as the save location and specify the format as XVA File (*.xva) and click **Next** 

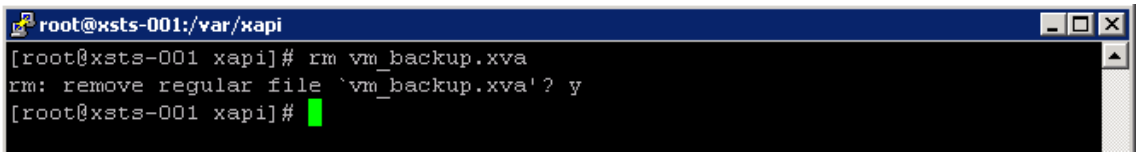
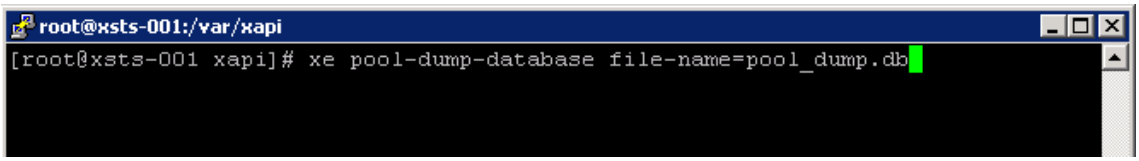
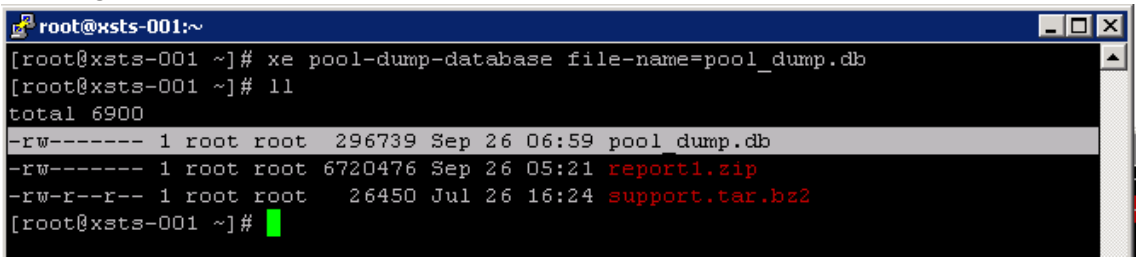
Step	Action
10.	Confirm the Windows.7 VM is selected and click **Next**

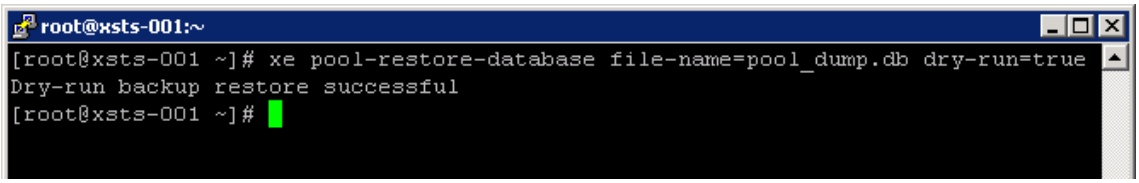
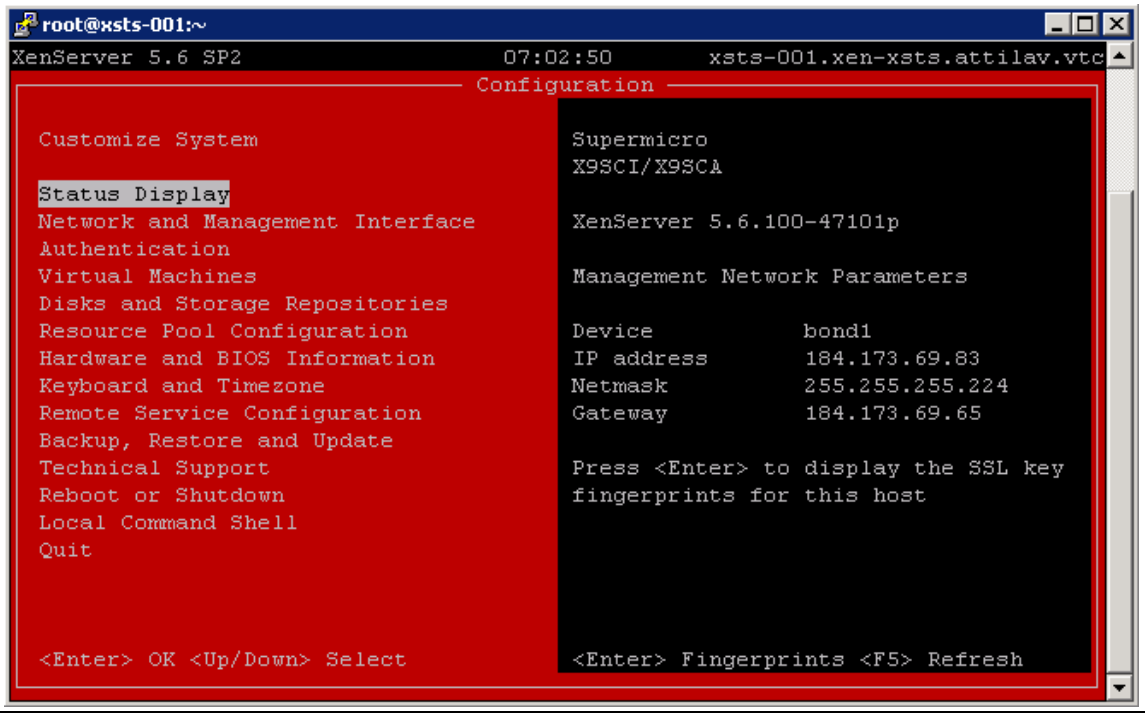


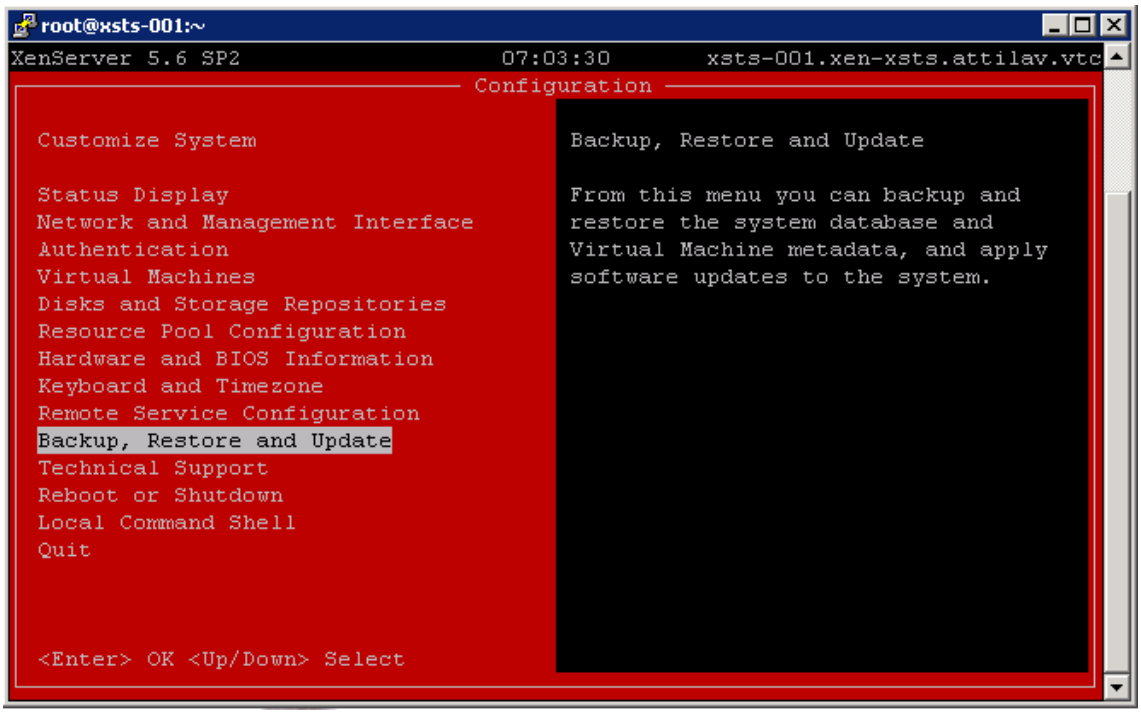
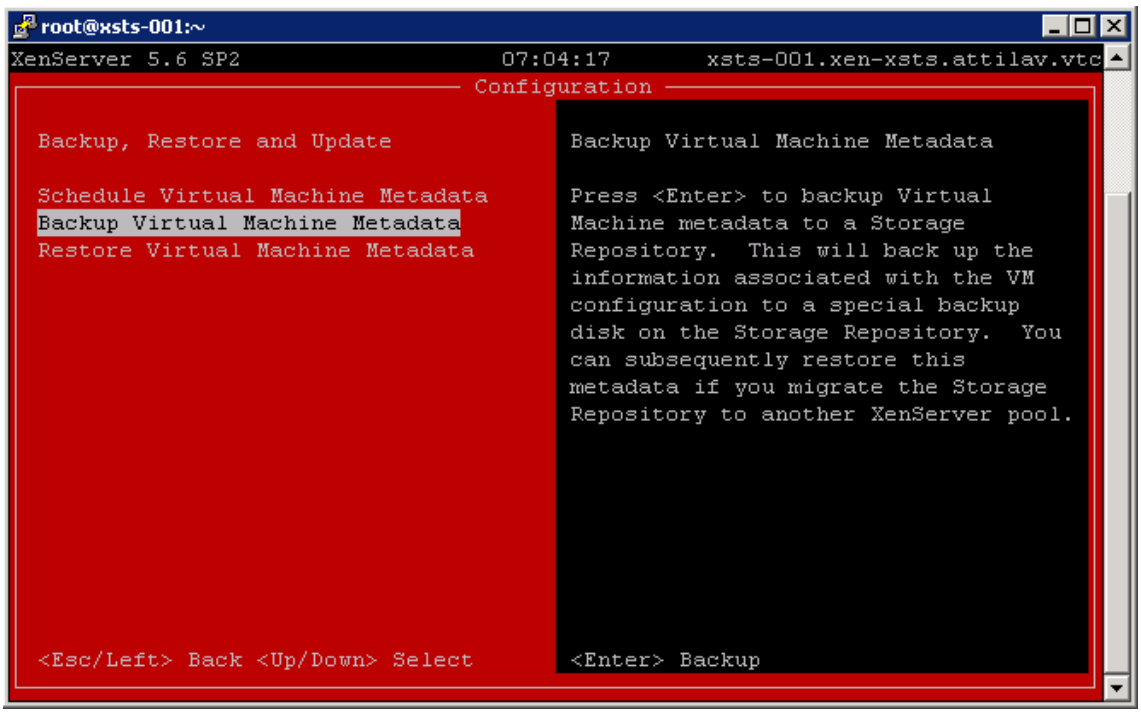
11.	Click **Finish** to start the export process

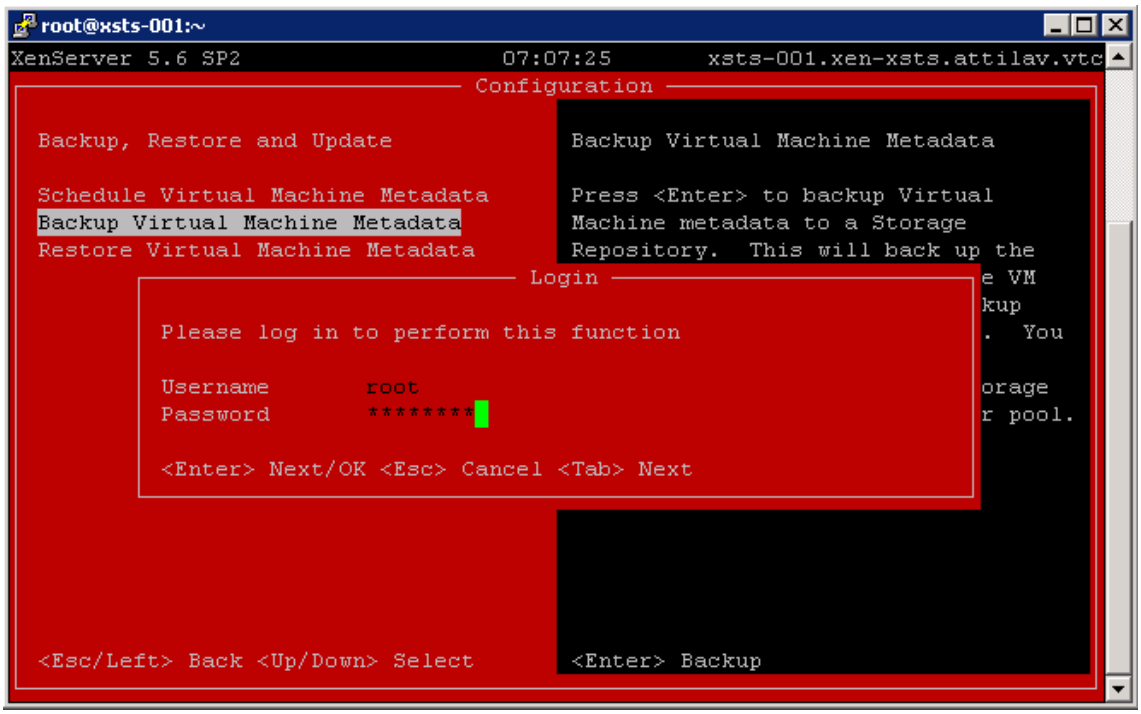
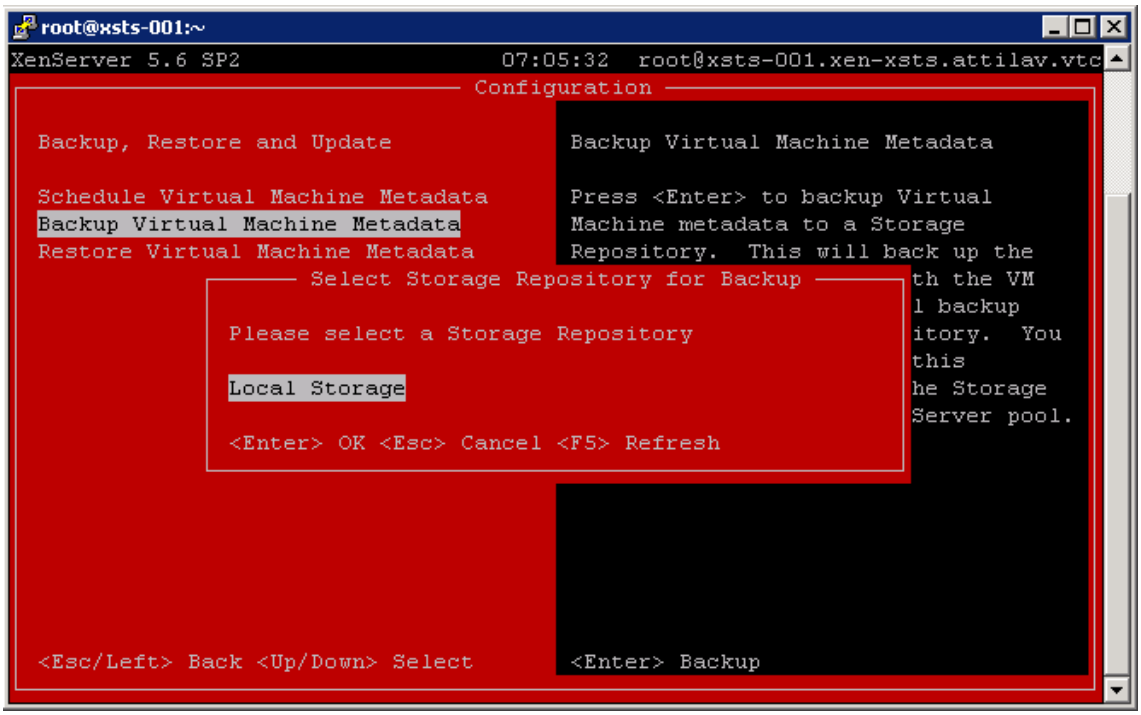


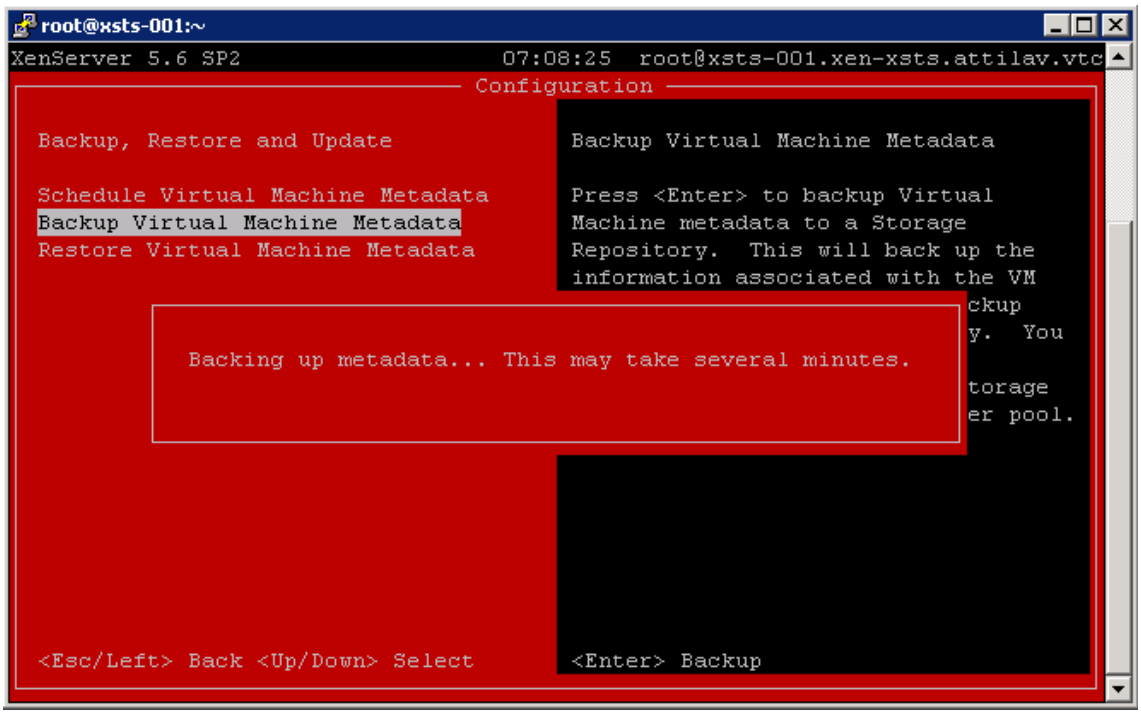
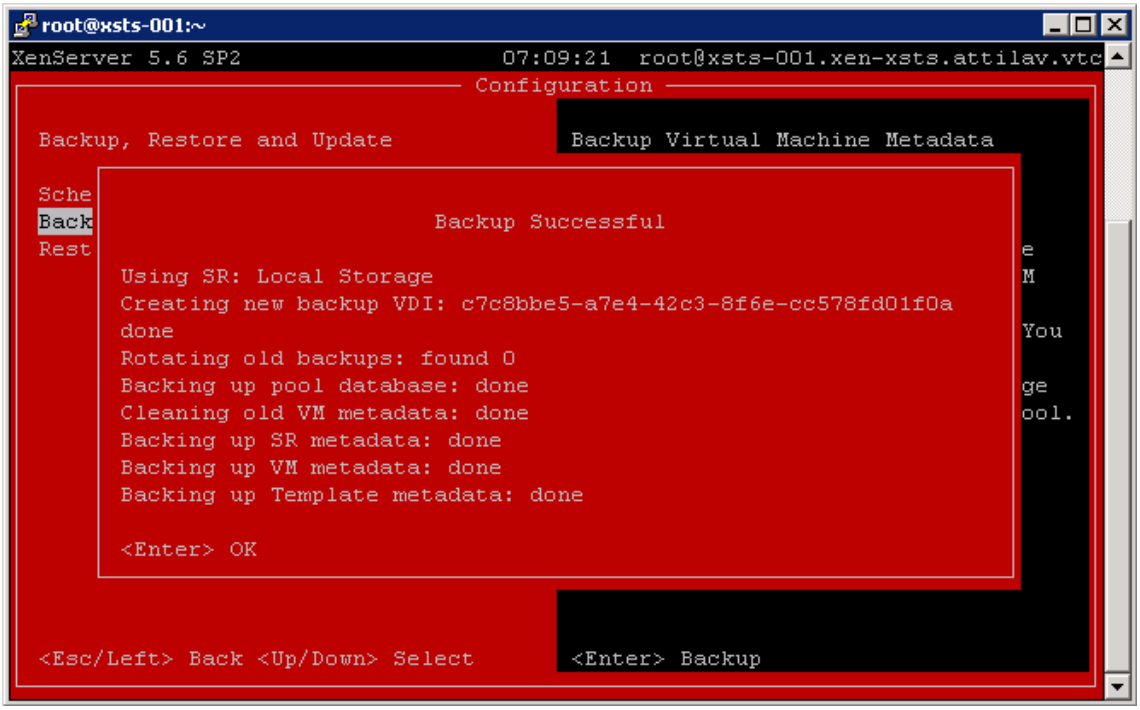
Step	Action
12.	Follow the backup process by clicking on Windows.7 VM and selecting the **Logs** tab 
13.	Click **Cancel** in the Log tab for the Windows.7 VM **Note:** For the purposes of this Learning Lab we will cancel the process as it can take some time for the process to complete.
14.	The above mentioned backup/export actions can also be complete via the CLI using the **xe** command e.g. **xe vm-export vm=Windows.7 filename=windows7.xva**  Press **CTRL+C** to cancel the process. **Note:** For the purposes of this learning lab we will cancel the process as it can take some time for the process to complete. **Note:** The export location will be the current folder unless otherwise specified **Note:** It is recommended to export VM to a share attached to the host/pool

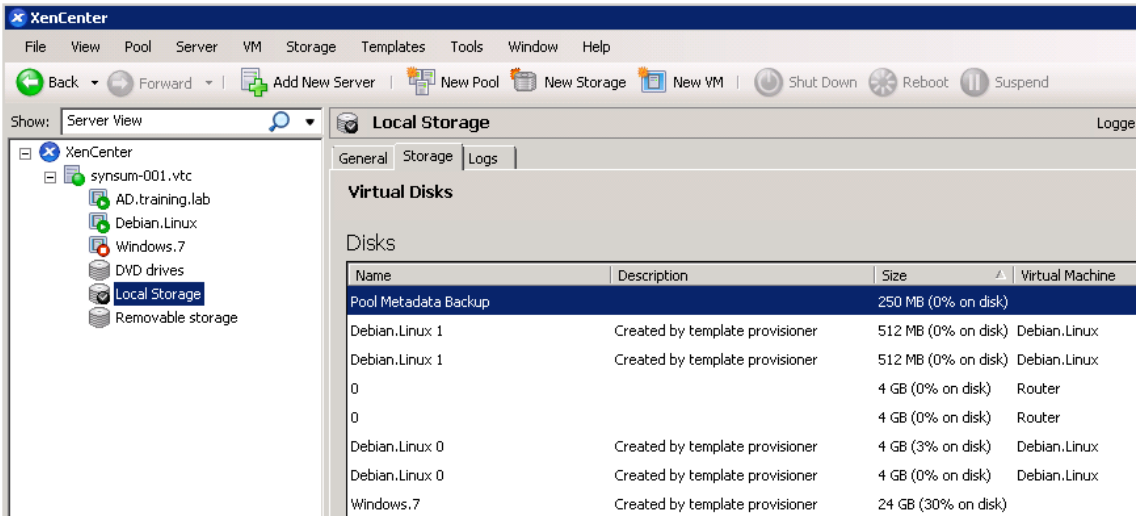
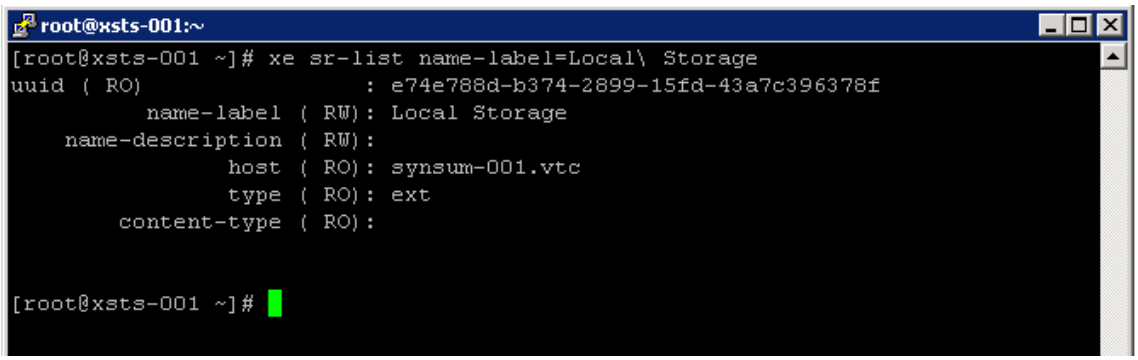
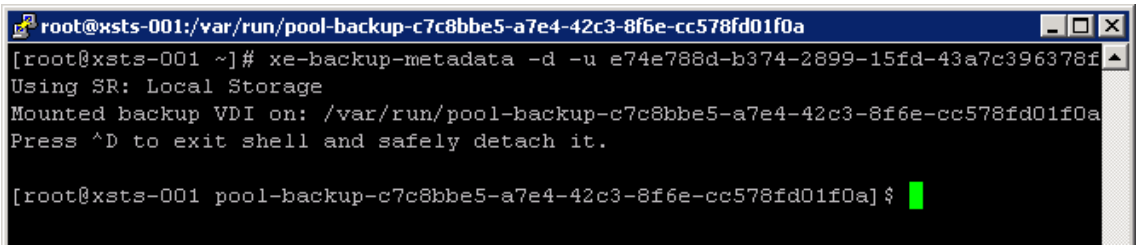
Step	Action
15.	Delete the exported VM file from Dom0 e.g. **rm vm_backup.xva**  **Note:** If the filesystem for dom0 is full the xapi service will be unable to start. To check the available space on dom0 (/dev/sda1) use the **df –h** command.
	Back up the host/pool configuration database:
16.	Launch a new SSH client **OR** duplicate an existing session of **PuTTY** from the Landing Desktop **OR** reuse an open session window.
17.	Use the xe command to generate a pool/host configuration backup e.g. **xe pool-dump-database file-name=[filename]**  **Note:** Every server in the pool will have a copy of this database however it is recommended to run this command on the master server.
18.	Confirm the backup has completed successfully by running **ls –l** and confirming the **pool_dump.db** file was generated. 

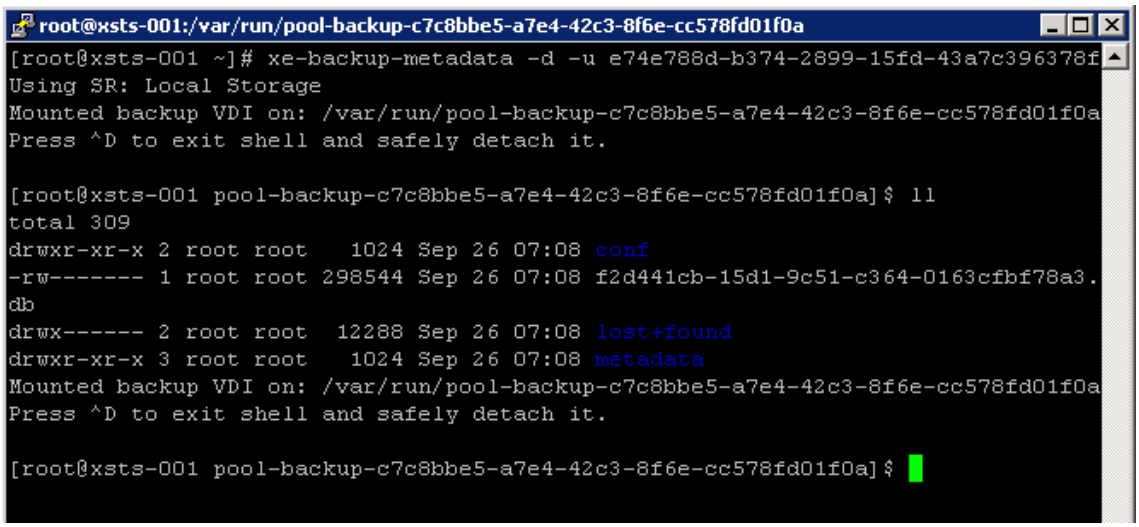
Step	Action
19.	To restore from a database backup use the xe command e.g. **xe pool-restore-database file-name=[filename] dry-run=true**  **Note:** It is highly recommended to do a dry-run of the restore before completing the process. This is accomplished by adding the **dry-run=** parameter to the restore command. **Note:** The xe toolstack needs to be restarted after a restore process is completed i.e. **xe-toolstack-restart**.
	Backup virtual machine metadata:
20.	From the SSH console session launch the **xsconsole** e.g. **xsconsole** 

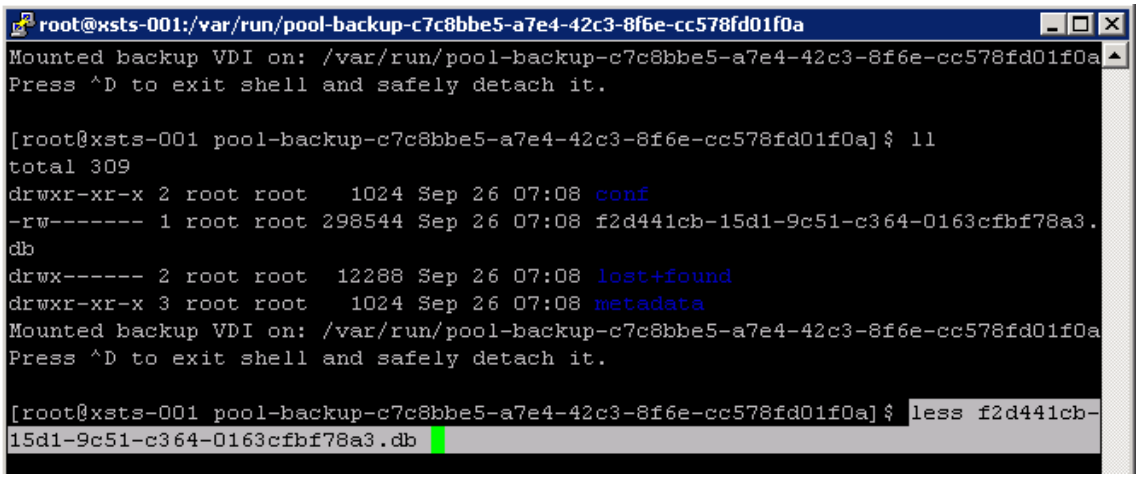
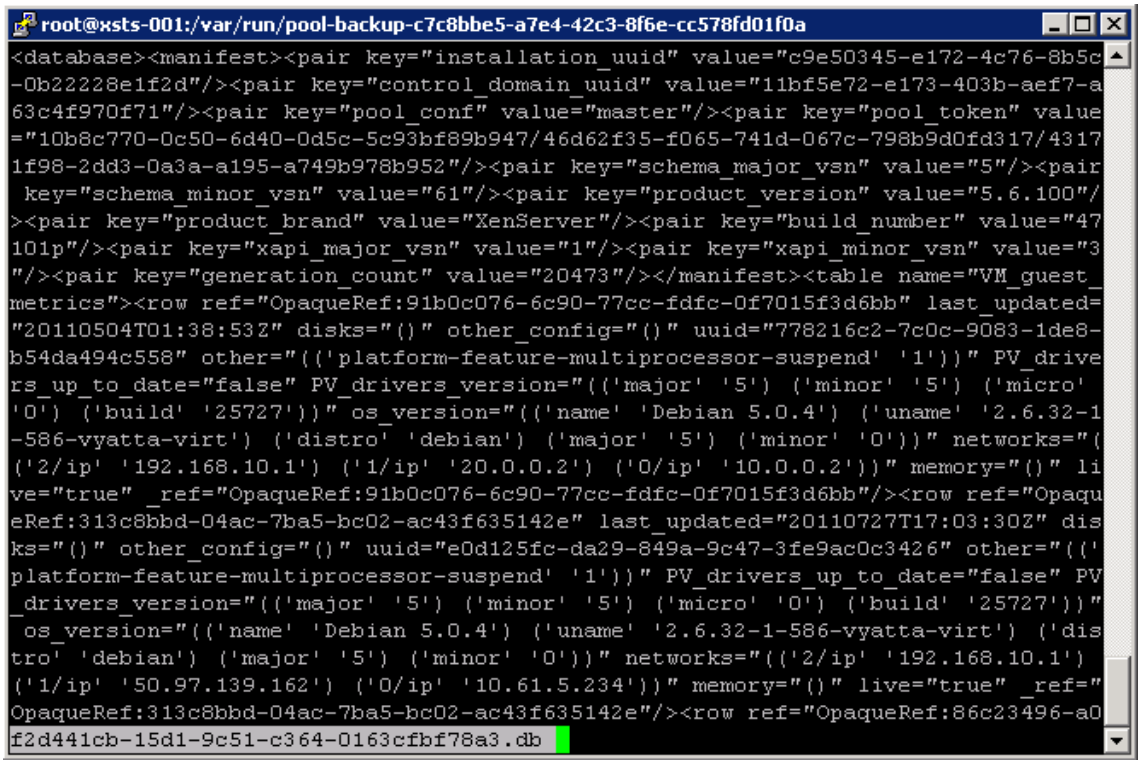
Step	Action
21.	Select **Backup, Restore and Update** 
22.	Select **Backup Virtual Machine Metadata** 

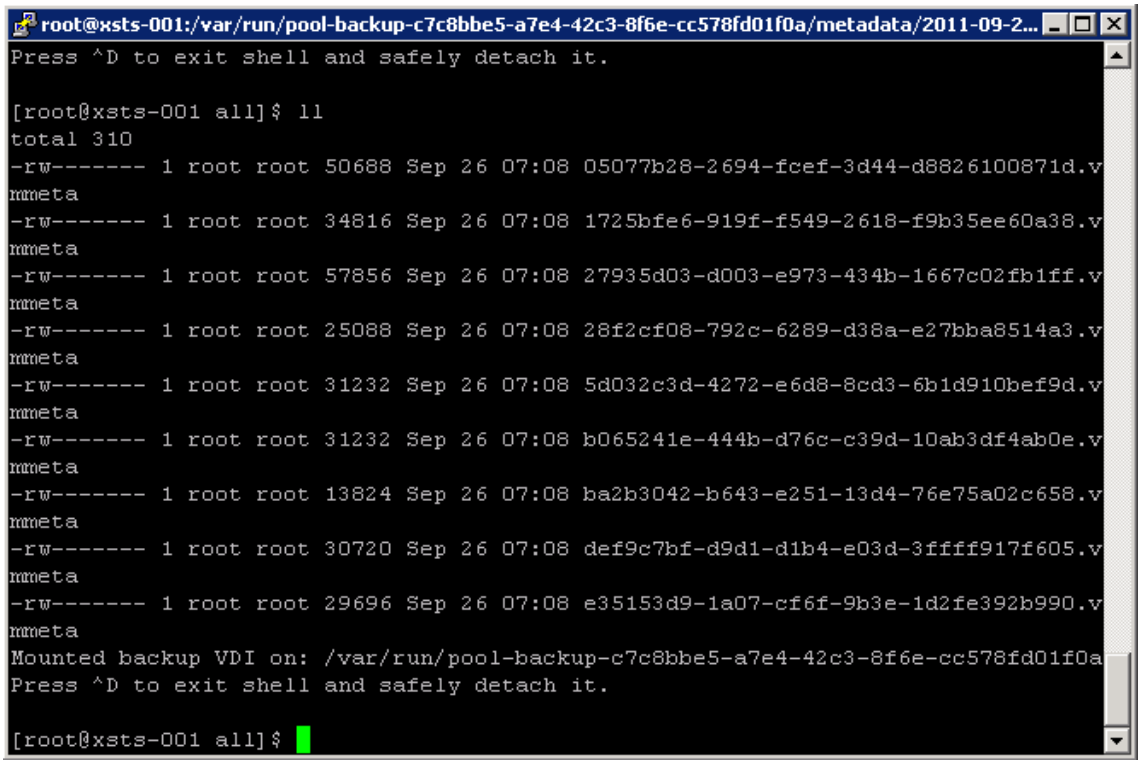
Step	Action
23.	Enter the root user **credentials** for your XenServer 
24.	Specify which **storage repository (SR)** should contain the metadata backup virtual disk (VDI)  **Note:** In this environment only a local SR is avail for the backup. Using local storage for a backup is not recommended in production environments.

Step	Action
25.	The metadata backup process will **initiate** 
26.	The process should complete with **information** about the backup 
27.	Accept the report **OK** and exit the **xsconsole** by pressing **ESC** and selecting **Quit.**

Step	Action
28.	Verify the metadata backup virtual disk by selecting the **Local Storage** and clicking the **Storage tab**.  **Note:** The Pool Metadata Backup VDI contains a copy of the pool database (state.db)
	Review the backup VDI created in the previous step via the CLI:
29.	Locate the local SR uuid e.g. **xe sr-list name-label=[SR name i.e. Local storage]** 
30.	Use the xe command to mount the VDI for our review e.g. **xe-backup-metadata -d –u [uuid of SR]** **Tip:** To copy the UUID in your console drag and select the UUID with your mouse and right click.  **Note: -d** mounts the vdisk via a script and **–u** indicates which SR to search for the metadata VDI

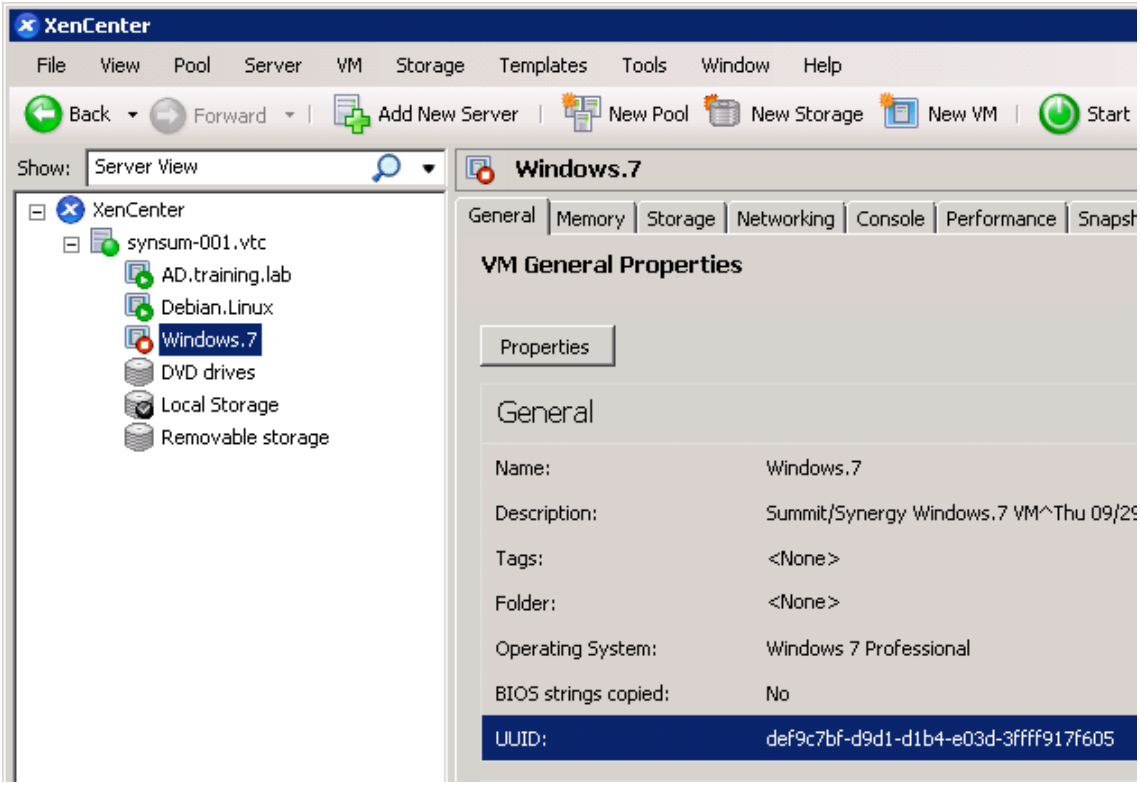
Step	Action
31.	Use the **ll** command to list the contents of the VDI 

Step	Action
32.	Use the less command to view the contents of the .db file. e.g. **less [filename.db]**   Press **q** to exit

Step	Action
33.	To review the specific VM metadata navigate to **cd metadata/[date folder]/all/** and list the contents using the **ll** command**.**  **Note:** Each file represents a virtual machine's meta/configuration data. The file names also correspond to the UUID of the VM.

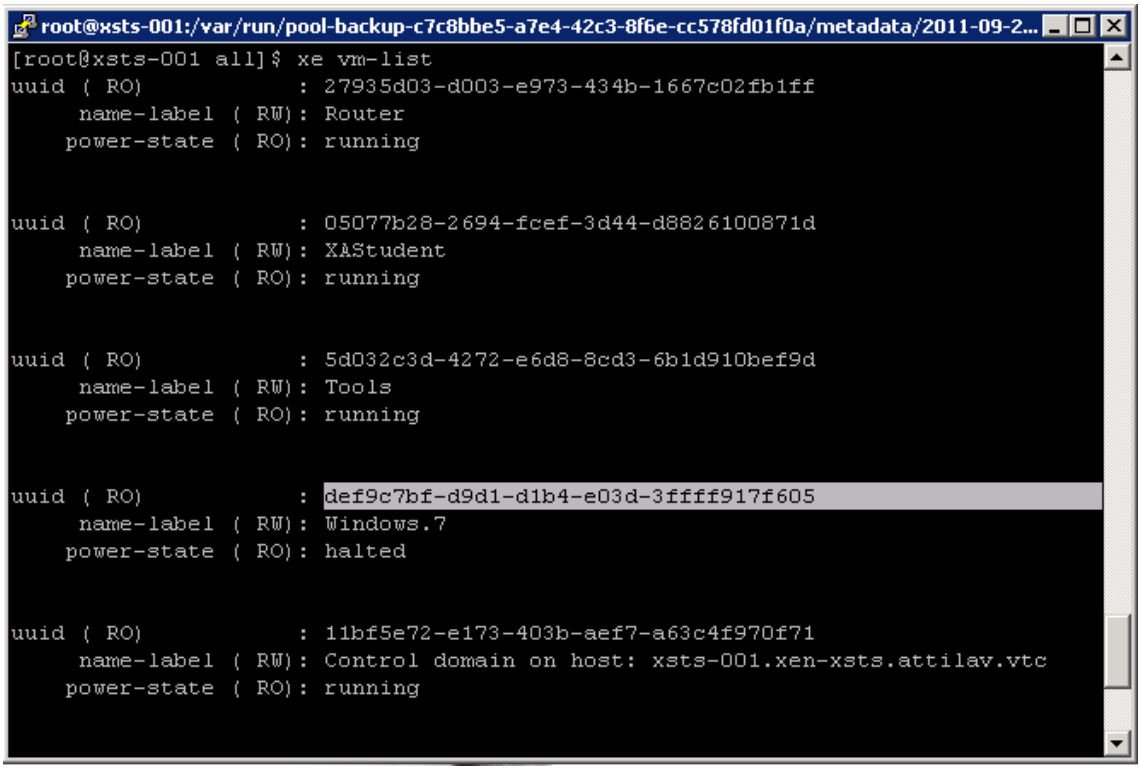
Step	Action
34.	Match the UUID listed in this folder with a UUID of a virtual machine. This can be done in XenCenter or the CLI

XenCenter:



CLI:

e.g. **xe vm-list**



Step	Action
35.	Press **CTRL+D** to exit the mount location and un-mount the backup VDI
END OF EXERCISE	

Summary

Key Takeaways	The key takeaways for this exercise are: • You will be able to create backups of pool configuration, virtual machine metadata and a XenServer host. • You will be able to view the contents of a backup VDI using the CLI.

Exercise 6: Capturing a Network Trace in XenServer

Overview

In this exercise we will capture a network trace on different network interfaces associated with a XenServer host and the virtual machines running on XenServer.

The first step is to identify the interface that you would like to trace on. Questions to ask would be if the issue is isolated to a virtual machine, a group of virtual machines or a specific XenServer. The answer will determine if you will collect a trace on a PIF, VIF or Bridge.

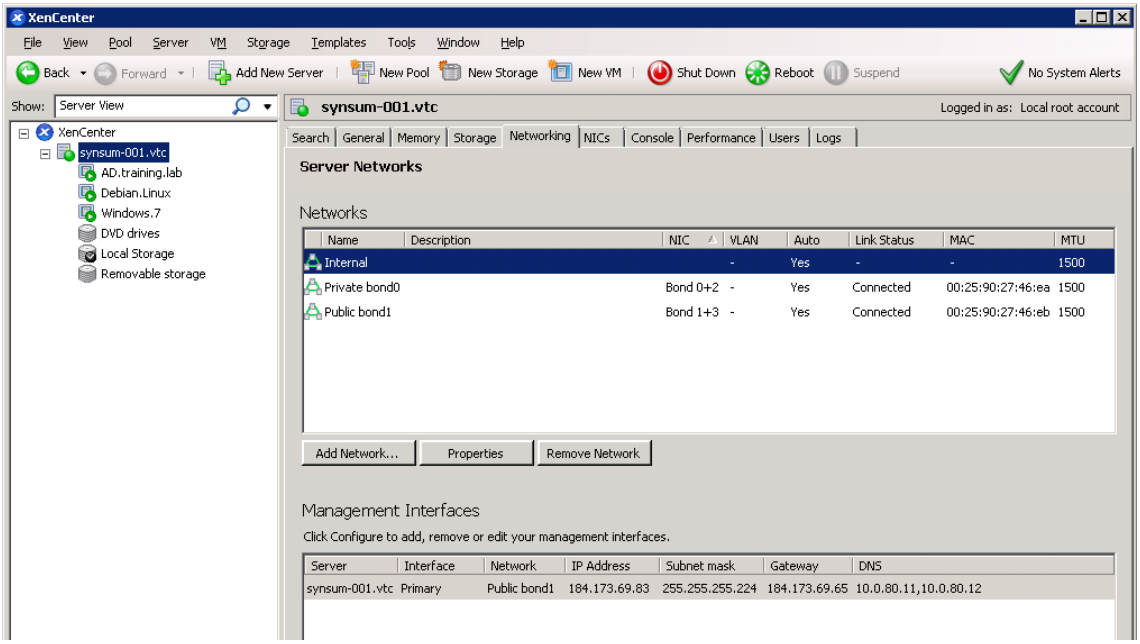
To complete this exercise, you must have the following:

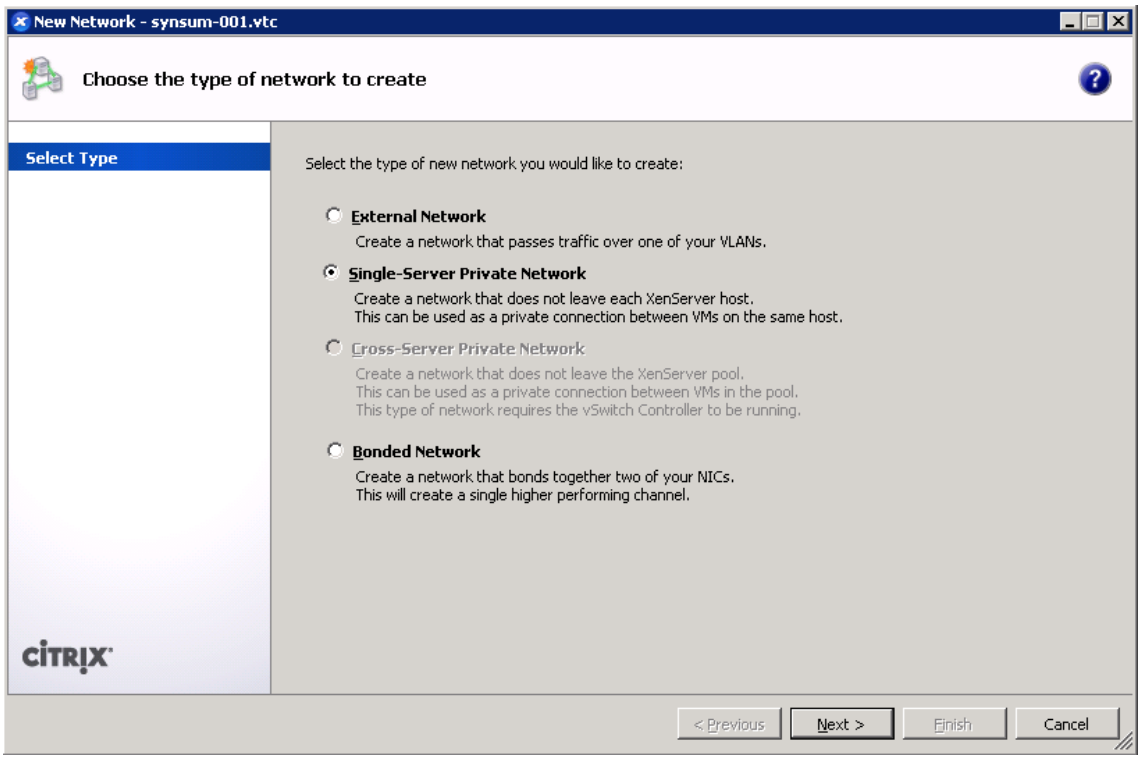
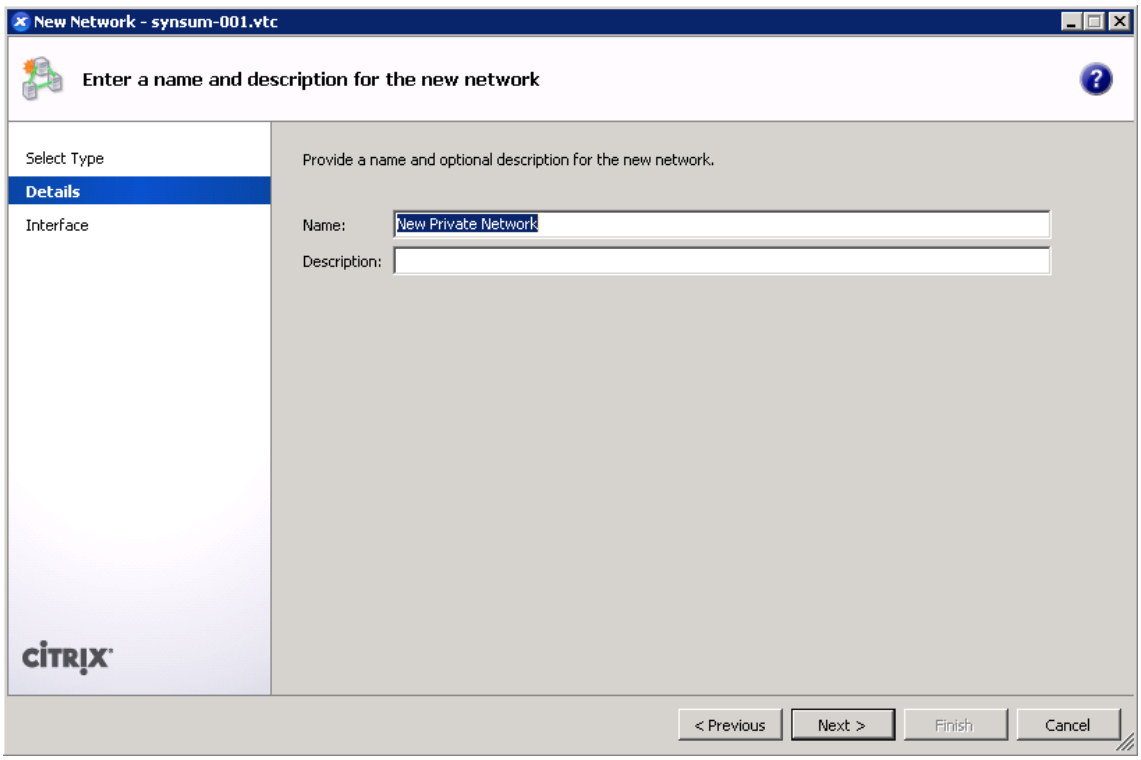
- SSH Client (PuTTY)
- WinSCP
- Network trace analysis tool (Wireshark)

Step-by-step guidance

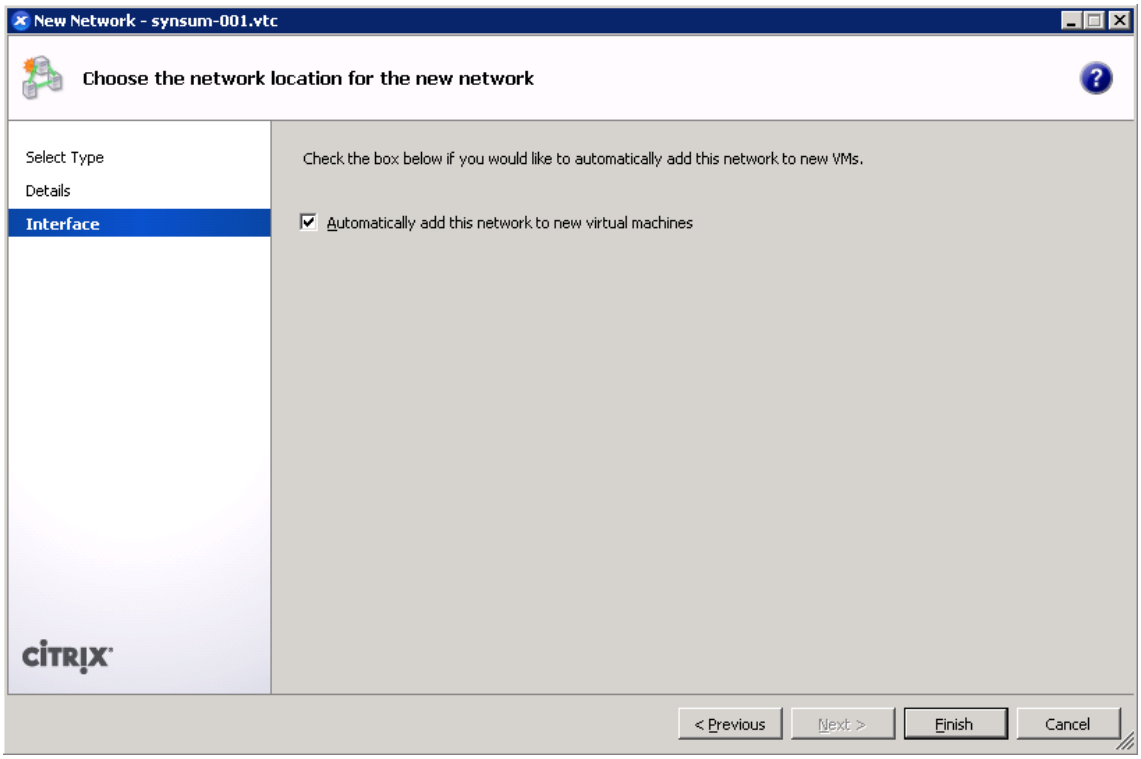
Estimated time to complete this lab: **15 minutes**.

Step	Action
	Create an isolated network and a VLAN using XenCenter:
1.	Start the **Windows.7** virtual machine
2.	Highlight the **host** and select the **Network** tab

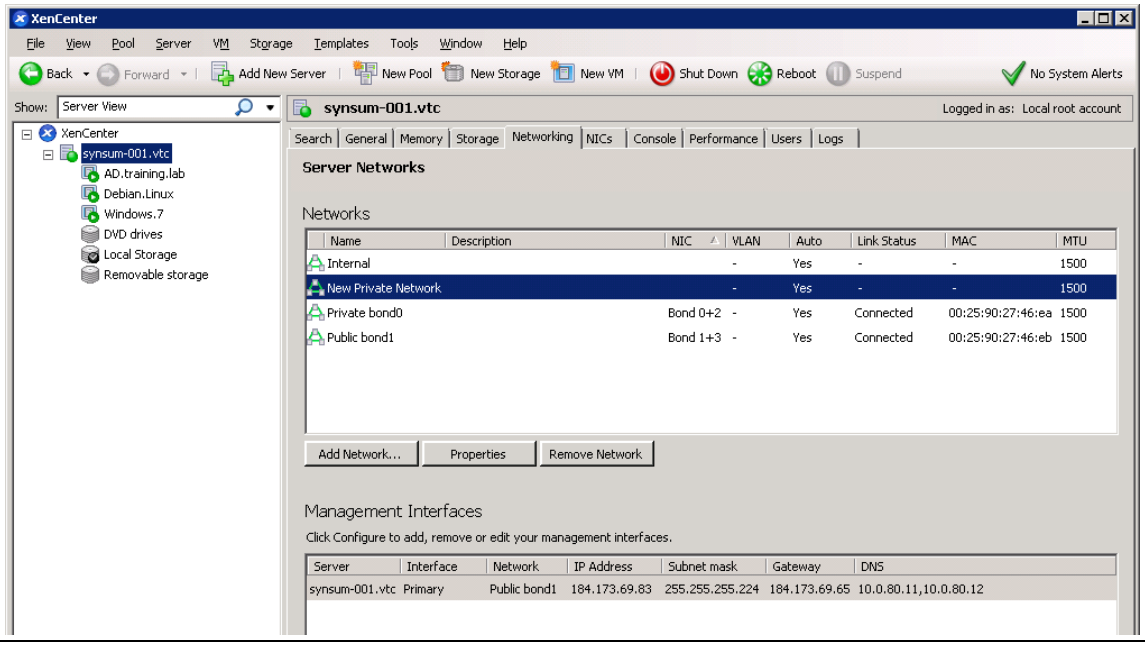


Step	Action
3.	Click **Add Network…** and select **Single-Server Private Network.** Click **Next.** 
4.	Leave the network name **default** and click **Next** 

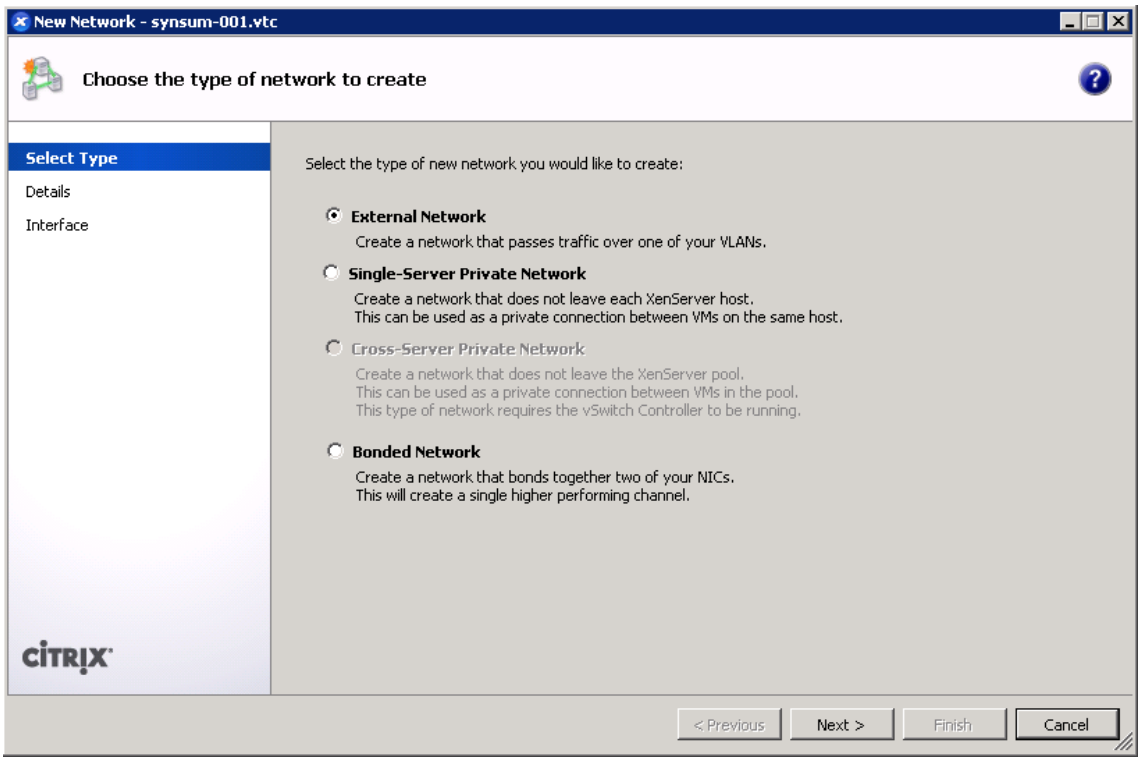
Step	Action
5.	**Tick** the option **to automatically add this network** to new virtual machines and click **Finish.**

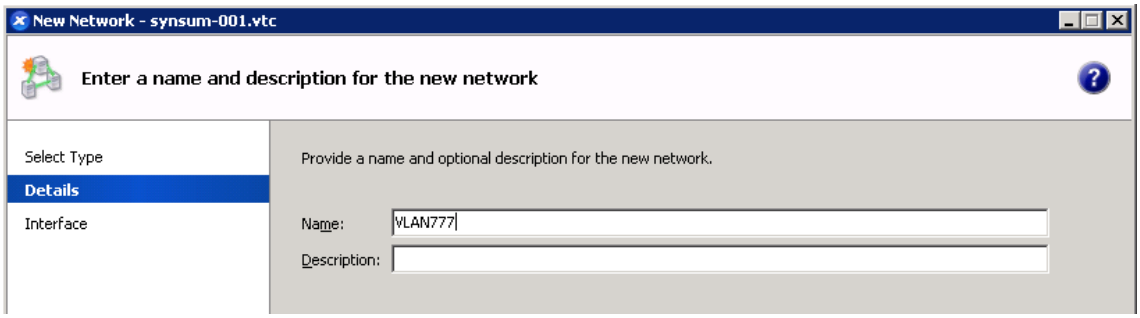


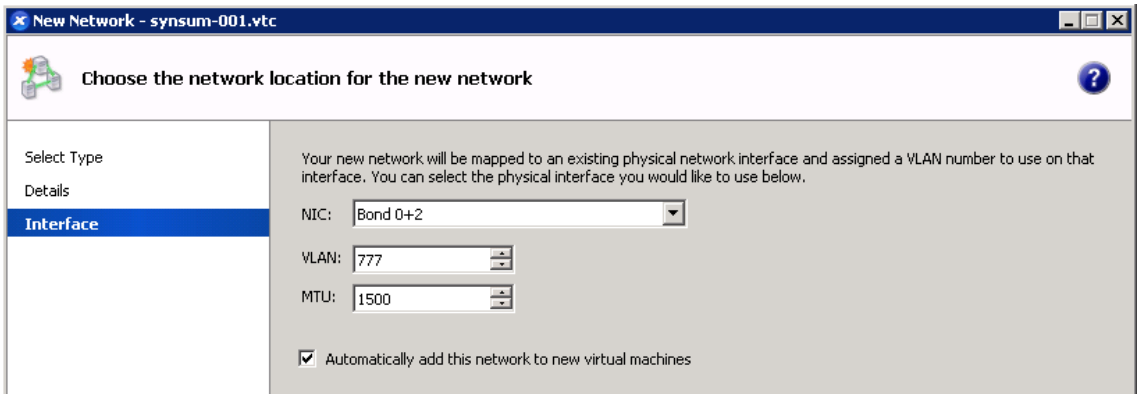
6.	The newly created internal network should now be listed in the networks tab.

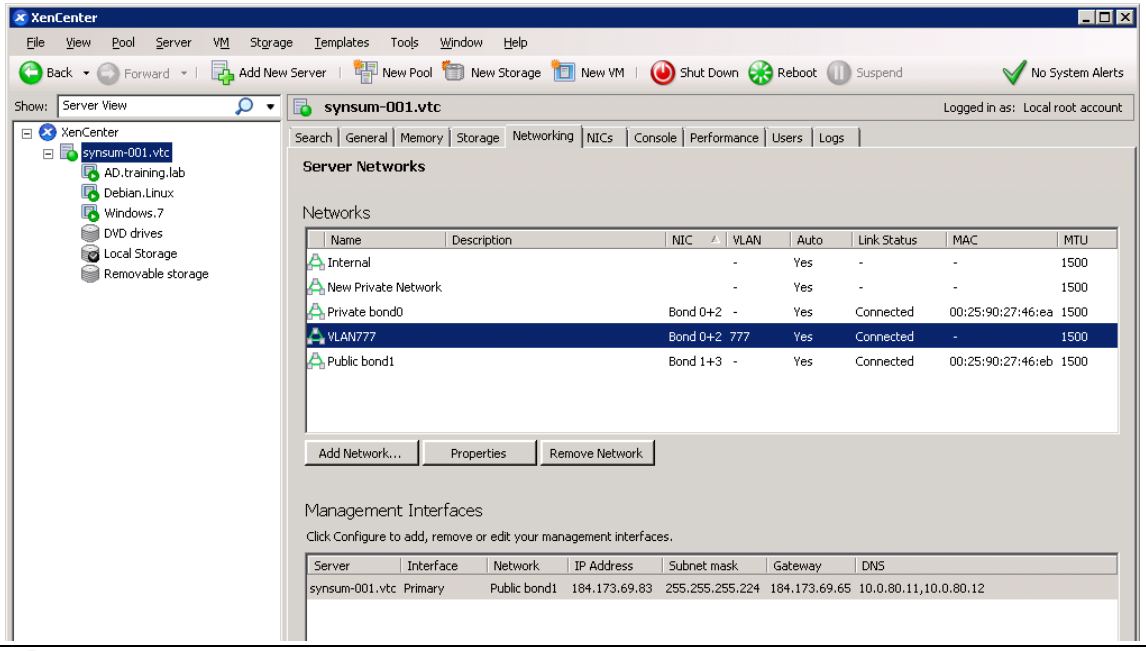
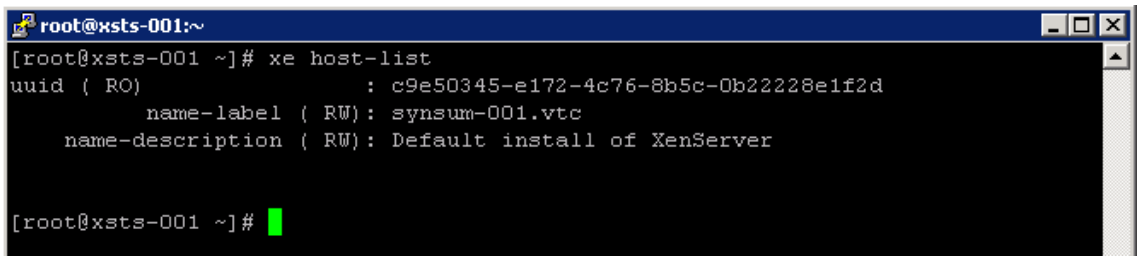


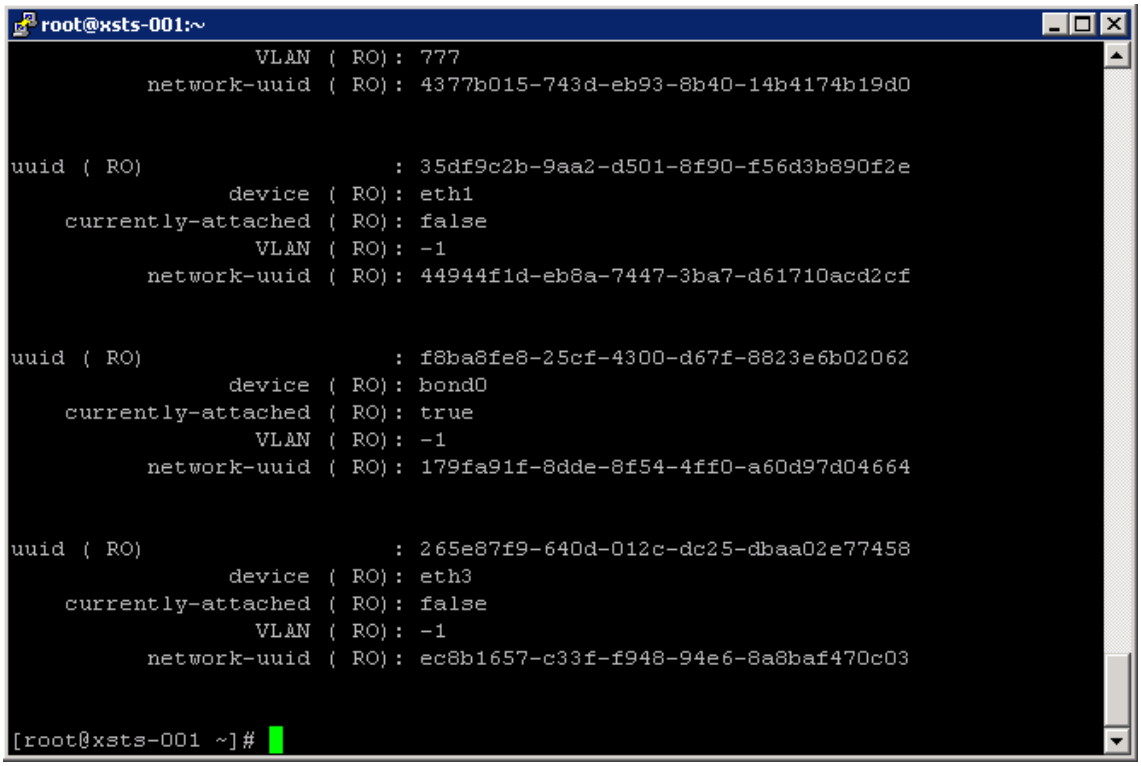
Step	Action
7.	Click Add Network… and select **External Network** and click **Next**
8.	Change the network name to **VLAN777** and click **Next**
9.	Select **Bond 0+2** and enter the VLAN number **777**. Tick the parameter to automatically add this network to new virtual machines. Click **Finish.**

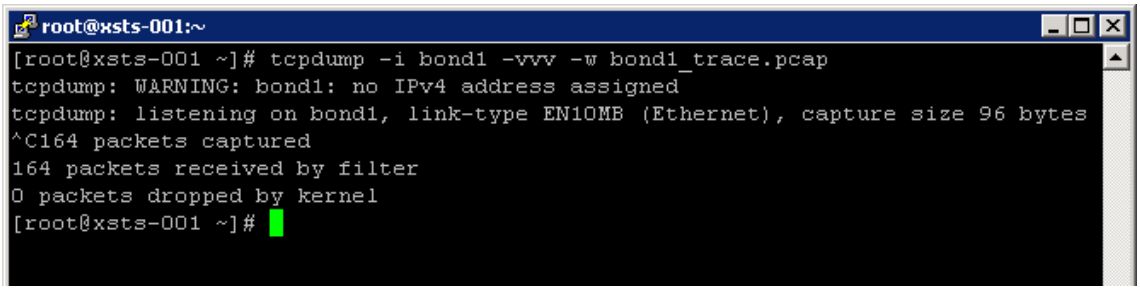
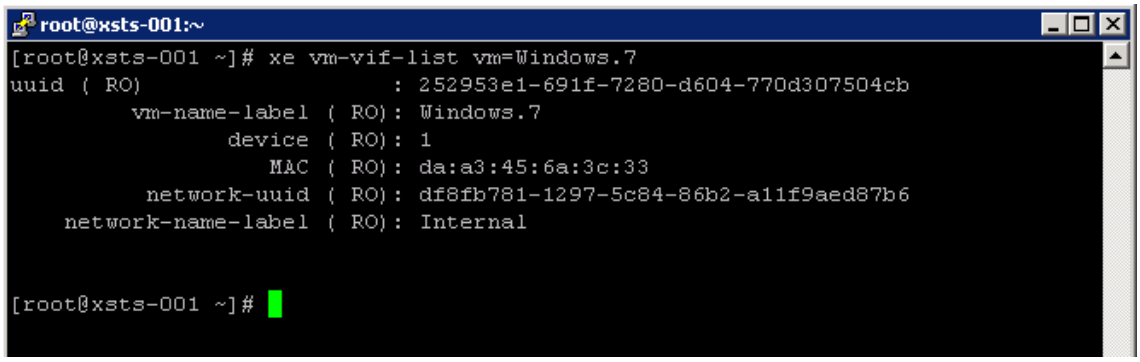


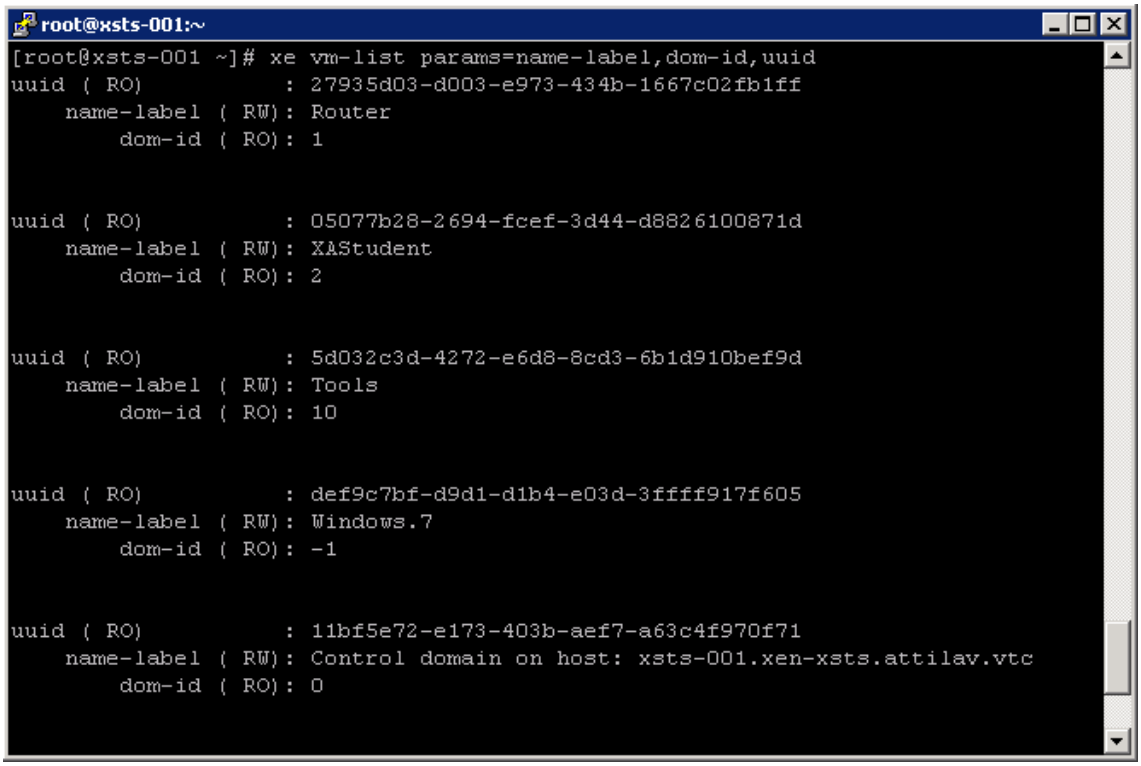
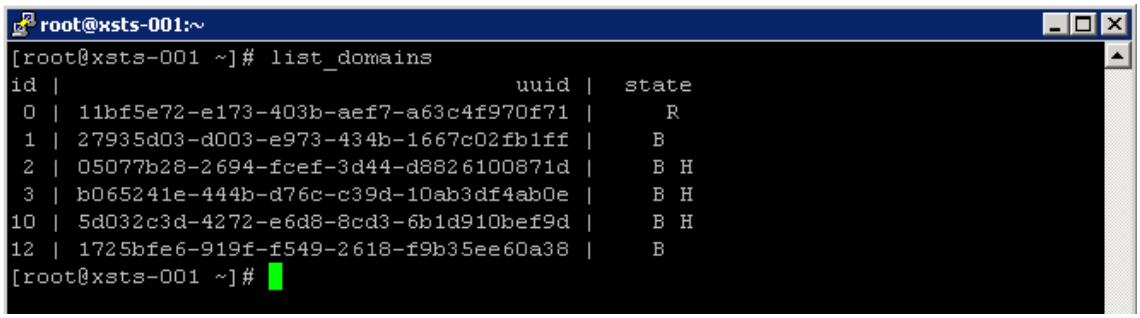


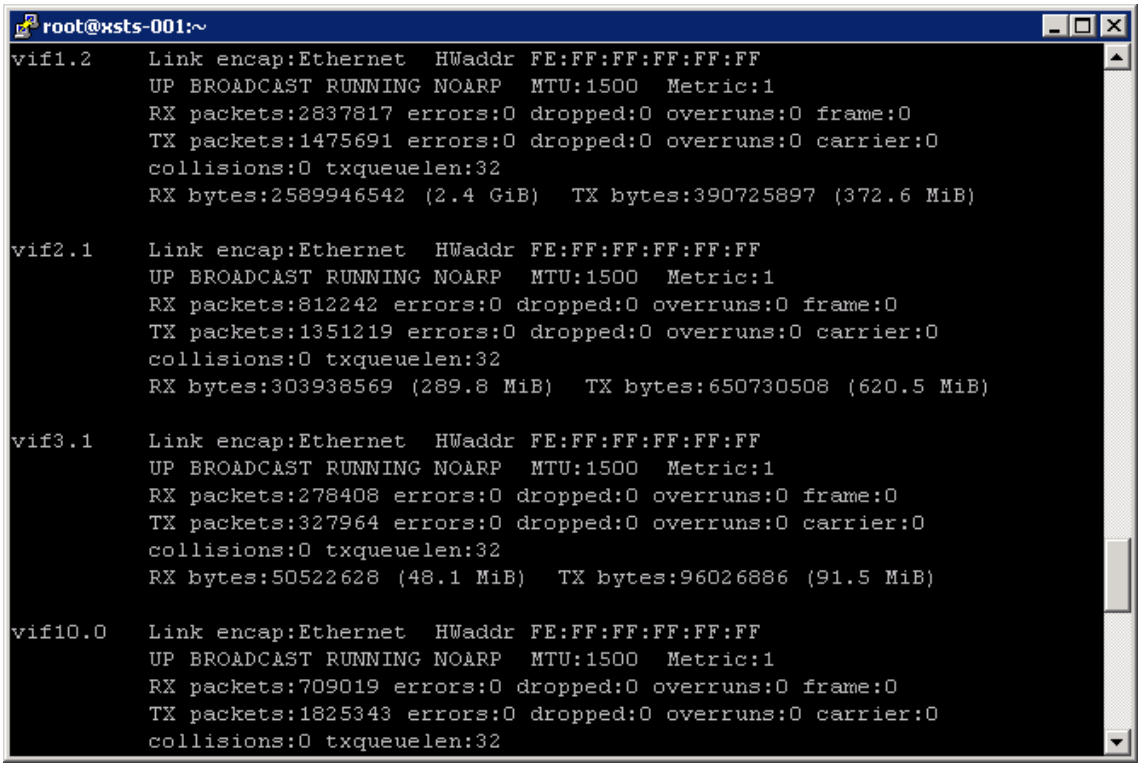
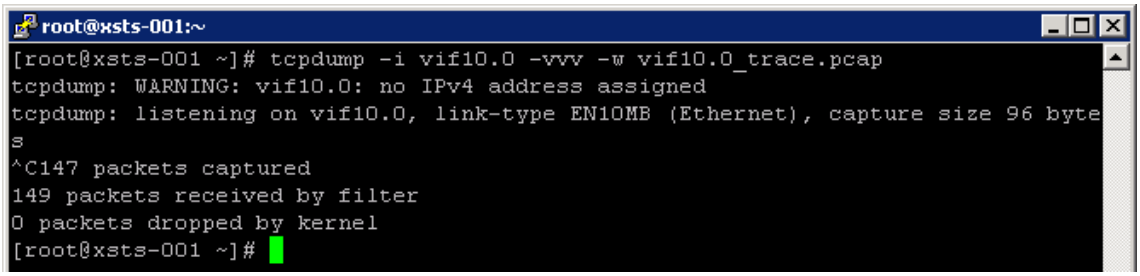


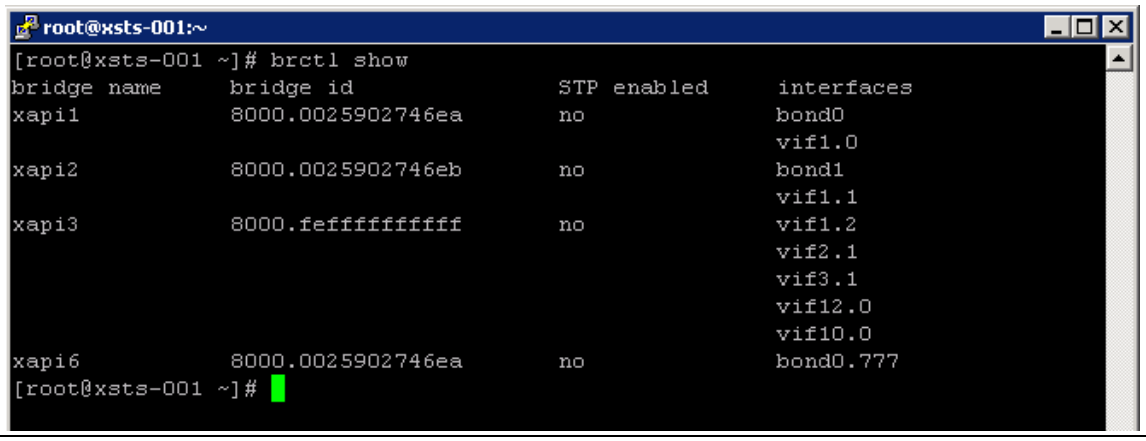
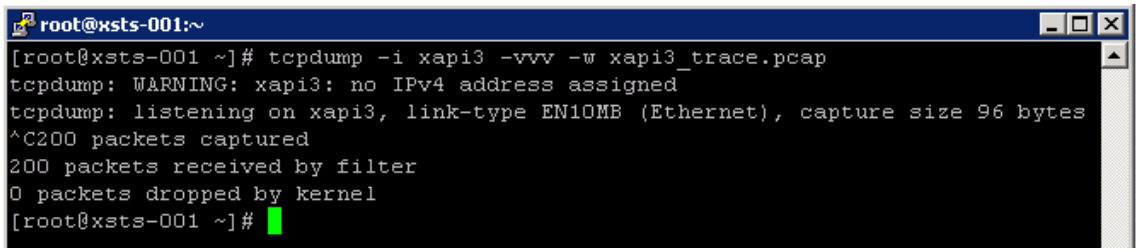
Step	Action
10.	Confirm that both **Internal Network** and **VLAN** have successfully been created. 
	Collect a network trace on a physical interface (PIF) used by XenServer via the CLI
11.	Launch a new SSH client **OR** duplicate an existing session of **PuTTY** from the Landing Desktop **OR** reuse an open session window.
12.	Identify the XenServer host which we will collect the network trace from e.g. **xe host-list**  **Note:** In our example only one XenServer host is available

Step	Action
13.	List the physical interfaces (PIF) detected by XenServer e.g. **xe pif-list host-name-label=[host name]** or **xe pif-list host-uuid=[host uuid]**  **Note:** In the above example the host has 4 NICs (**eth0, 1, 2, 3**) and a **VLAN 777** which is associated with **bond0** and seen as a PIF.

Step	Action
14.	Use tcpdump to collect a trace from a PIF e.g. **tcpdump –i [device] –vvv –w [filename.pcap]**  **Note:** To stop the trace press **CTRL+C** **Note:** In the above example we collected a network trace on **bond1** and wrote the output to a file called **bond1_trace.pcap**. **-i** = interface **-vvv** = very verbose mode **-w** = write to file **Note:** To capture the complete packed payload use the **–s 0** parameter when collecting a trace. **Note**: Use **.pcap** file extension to allow for file type **association** with network analyzing tools such as Wireshark.
	Collect a network trace on a virtual interface (VIF) used by a virtual machine: **Note**: VIF names are dynamically created on VM start. VIF names are constructed with the following structure; vif**x**.**y** where **x** is the domain id of the VM and **y** is the device number. The dynamic part of the name is the domain ID because it may change on VM start.
15.	List the VIFs device number associated with a VM e.g. **xe vm-vif-list vm=[vm name]**  **Note:** In the above example this VM has one VIF. **Device: 1** is connected to the **Internal** network**.**

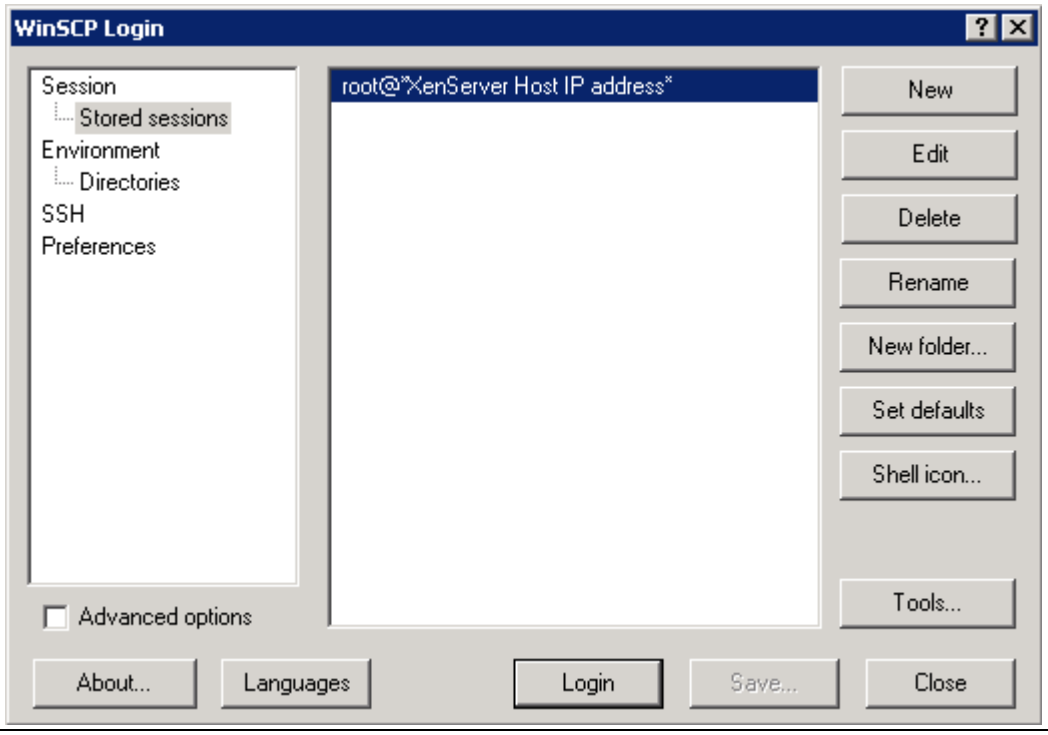
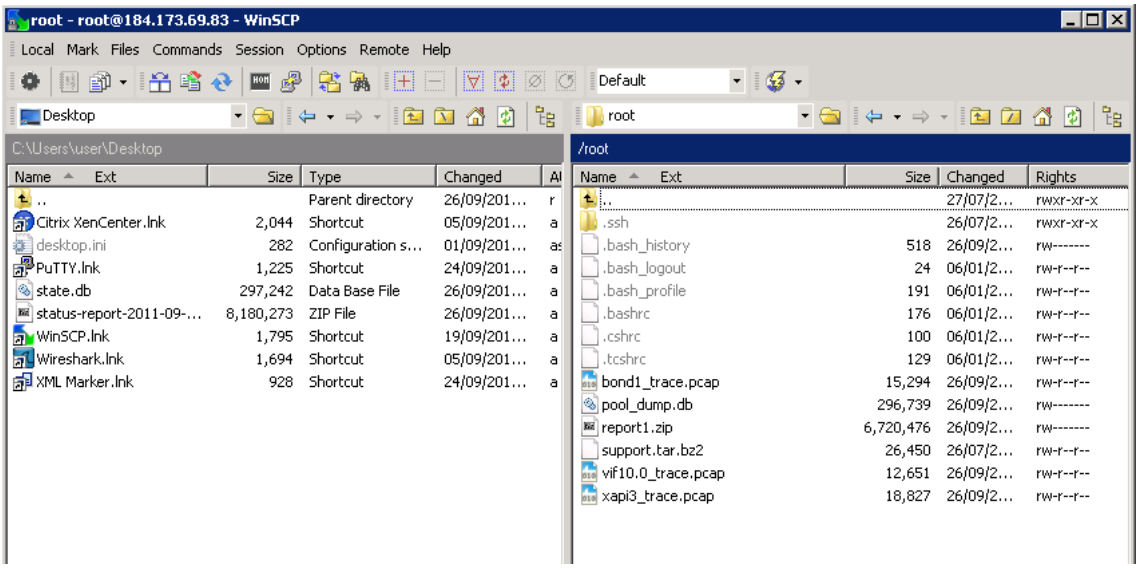
Step	Action
16.	Locate the domain identifier (domid) for a particular virtual machine using **xe** e.g. **xe vm-list params=name-label,dom-id,uuid** 
17.	An alternative method to list the **domid** of the current domains running on your XenServer is using the **list_domains** command. e.g. **list_domains**  **Note:** This command will list all running domains and their associated **domain identifiers (domid).** This command is also not dependent on **xapi**. **Note:** The additional domains listed are hidden virtual machines running on the host which provides the remote access infrastructure for this lab environment.

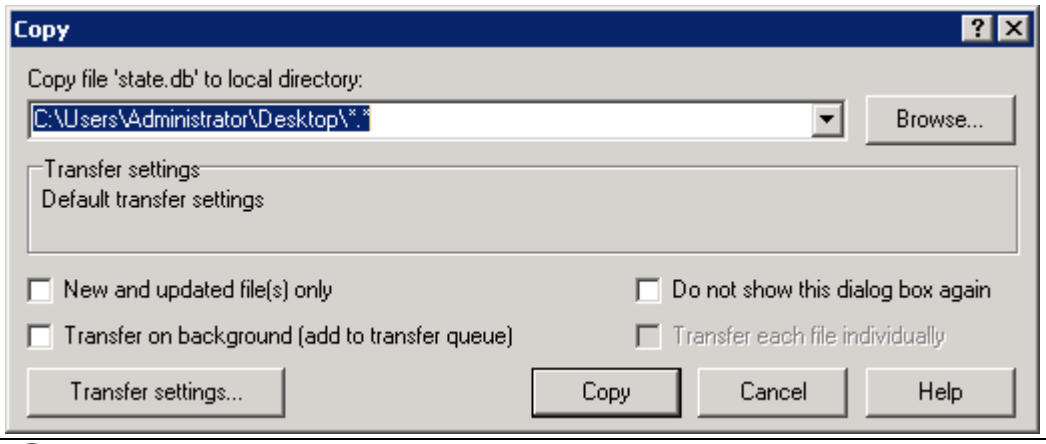
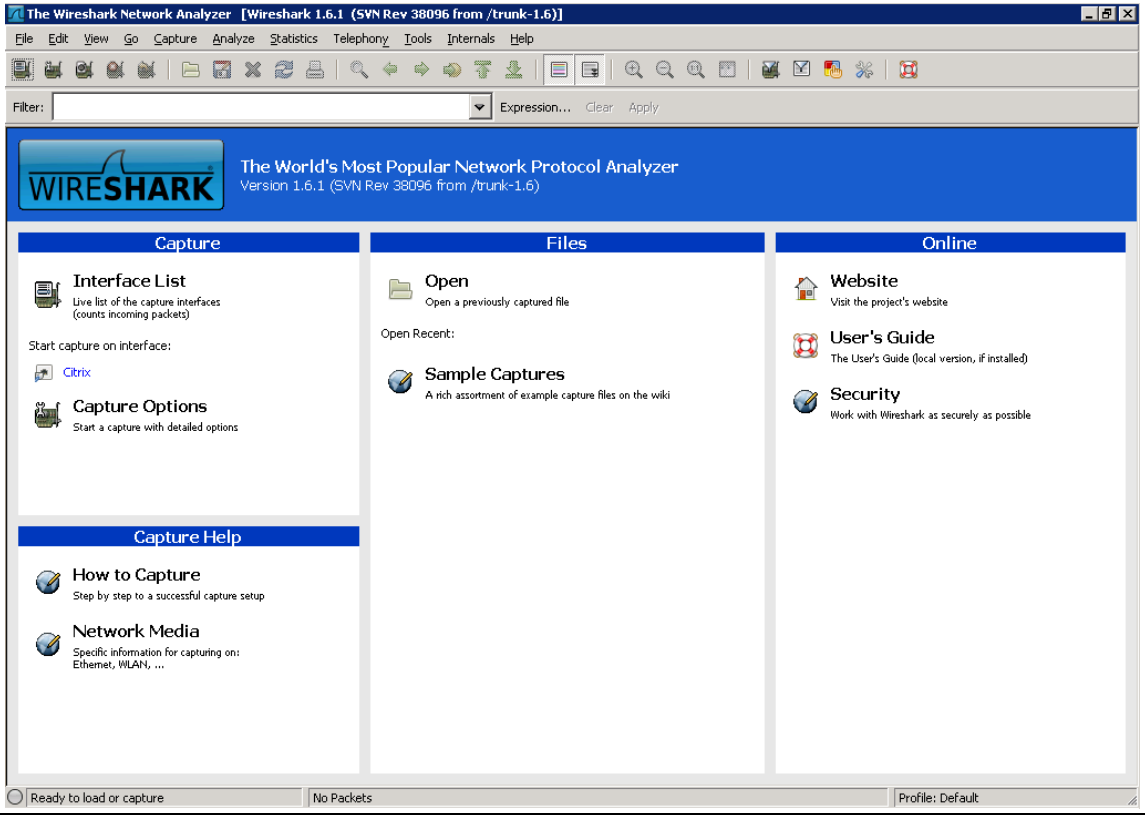
Step	Action
18.	List the current interfaces detected/managed by dom0 e.g. **ifconfig**  **Note:** If you scroll through the output you should see 4 **PIFs** (**eth0, 1, 2, 3**), the VLAN 777 (**bond0.777**) and **VIFs** associated with **domid 3** and **10** with device numbers **0** and **1** (vif3.1 and vif10.0)
19.	Collect a network trace from a VIF from the VM e.g. **tcpdump -i [interface] -vvv -w [filename]**  **Note:** In the above example a trace was collected from the **first interface (.0)** attached to the VM associated with **domid 10** i.e. **tcpdump -i vif10.0 -vvv -w vif10.0_trace.pcap** **Note:** To capture the complete packed payload use the **–s 0** parameter when collecting a trace.

Step	Action
	Collect a network trace on a virtual bridge (**xapiX/xenbrX**) used by a virtual machine: **Note:** This process will collect all traffic running over the bridge. Whether or not the data packet is leaving the host i.e. hitting the wire or not.
20.	List the current network bridge configuration e.g. **brctl show** 
21.	Trace network traffic on a bridge e.g. **tcpdump -i [bridge name] -vvv -w [filename]**  **Note:** i.e. **tcpdump -i xapi3 -vvv -w xapi3_trace.pcap** **Note:** To capture the complete packed payload use the **–s 0** parameter when collecting a trace.
	Collect the trace files from the XenServer for analysis:
22.	From the Landing Desktop connect to the XenServer host using **WinSCP**

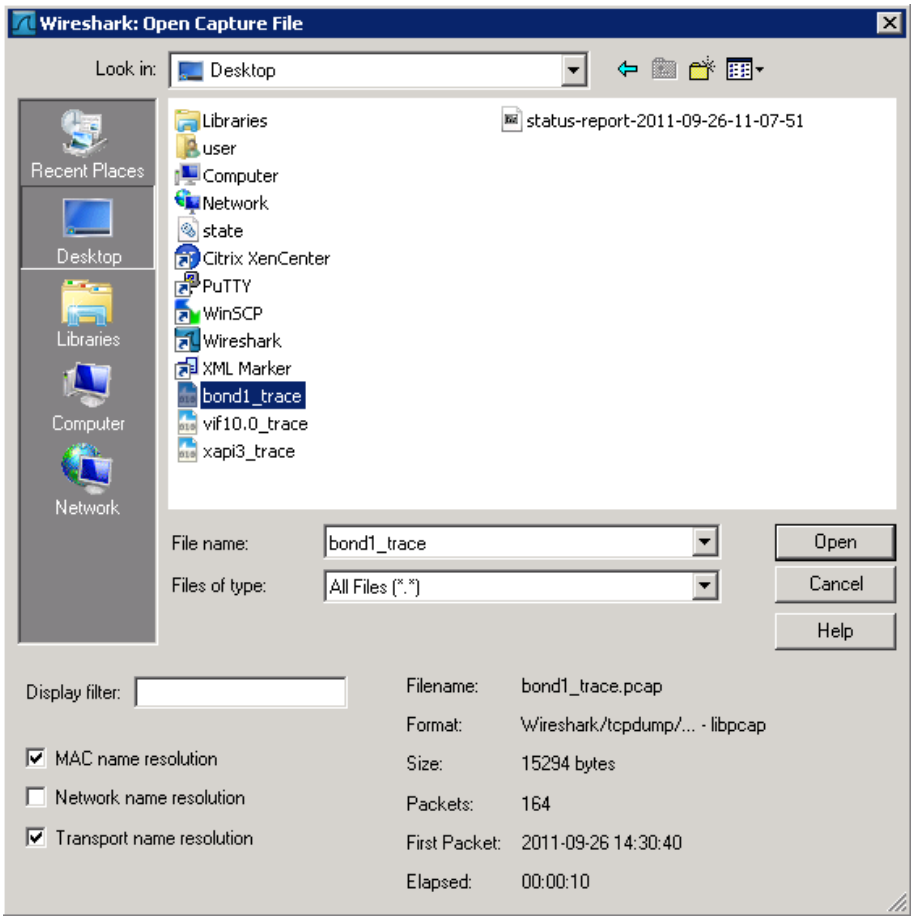
```
root@xsts-001:~
[root@xsts-001 ~]# brctl show
bridge name     bridge id               STP enabled     interfaces
xapi1           8000.0025902746ea       no              bond0
                                                        vif1.0
xapi2           8000.0025902746eb       no              bond1
                                                        vif1.1
xapi3           8000.feffffffffff       no              vif1.2
                                                        vif2.1
                                                        vif3.1
                                                        vif12.0
                                                        vif10.0
xapi6           8000.0025902746ea       no              bond0.777
[root@xsts-001 ~]#
```

```
root@xsts-001:~
[root@xsts-001 ~]# tcpdump -i xapi3 -vvv -w xapi3_trace.pcap
tcpdump: WARNING: xapi3: no IPv4 address assigned
tcpdump: listening on xapi3, link-type EN10MB (Ethernet), capture size 96 bytes
^C200 packets captured
200 packets received by filter
0 packets dropped by kernel
[root@xsts-001 ~]#
```

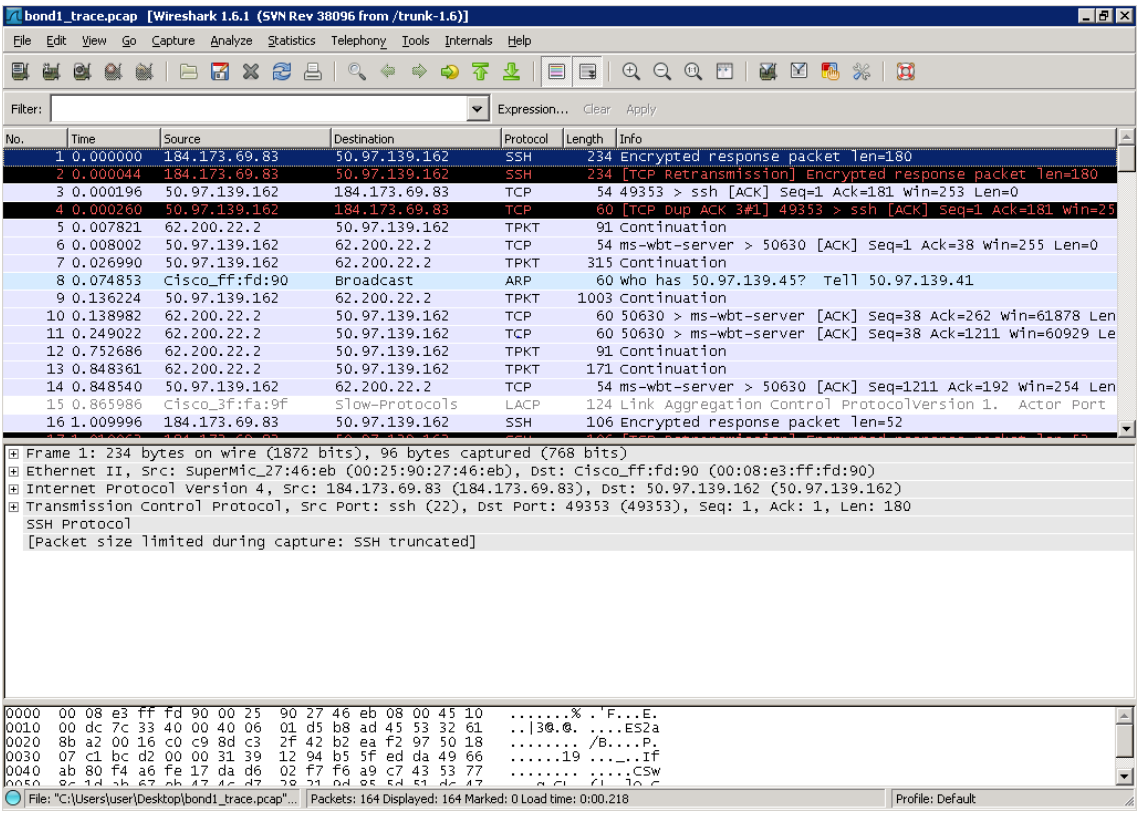
Step	Action
23.	Use an existing **WinSCP** session or re-launch **WinSCP** from your Landing Desktop by selecting your saved session information and click **Login.** 
24.	**Browse** to the trace files  **Tip:** To get to the root user's home folder click on the **home** button in the right column. **Note:** If the trace files are not displayed click the **refresh** button in the right column.

Step	Action
25.	**Select** all the trace files and **drag** them over to your Landing Desktop screen and click **copy** 
	Open the trace files with a trace analyzer i.e. Wireshark:
26.	Launch **Wireshark** from your client machine desktop 

Step	Action
27.	Click **Open** and browse to a trace file located on your Landing Desktop (copied earlier)



Step	Action
28.	**Open** the trace file



Note: In the above example we can see the SSH traffic running between the client (PuTTY) and the XenServer Host.

END OF EXERCISE

Summary

Key Takeaways	The key takeaways for this exercise are: • You will be able to identify network interfaces to trace. • You will be able to capture and collect network traces on different network interfaces associated with a XenServer host and the virtual machines.

Exercise 7: Monitoring in XenServer

Overview

In this exercise we will cover some common tools used to monitor performance related information about a XenServer environment.

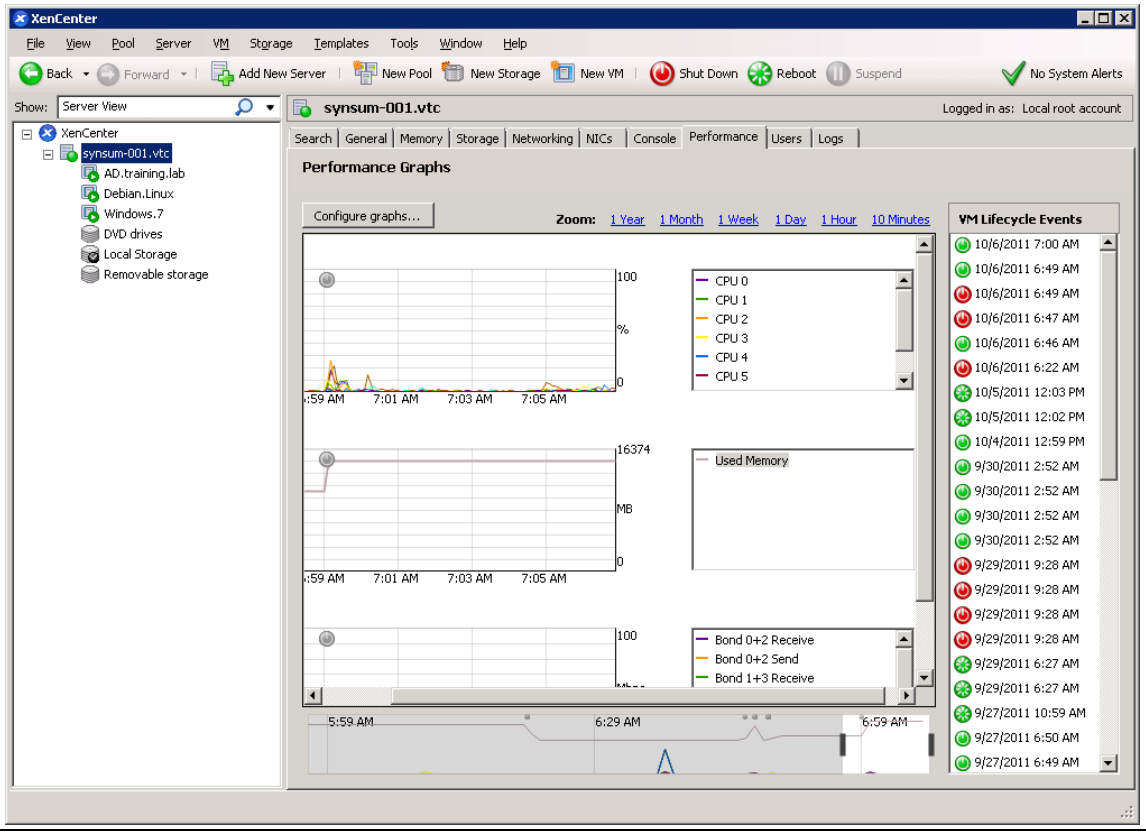
XenCenter provides a view of performance metrics for a XenServer host and virtual machine. However in some cases we use alternative tools to get another view of the performance and status of a host or VM.

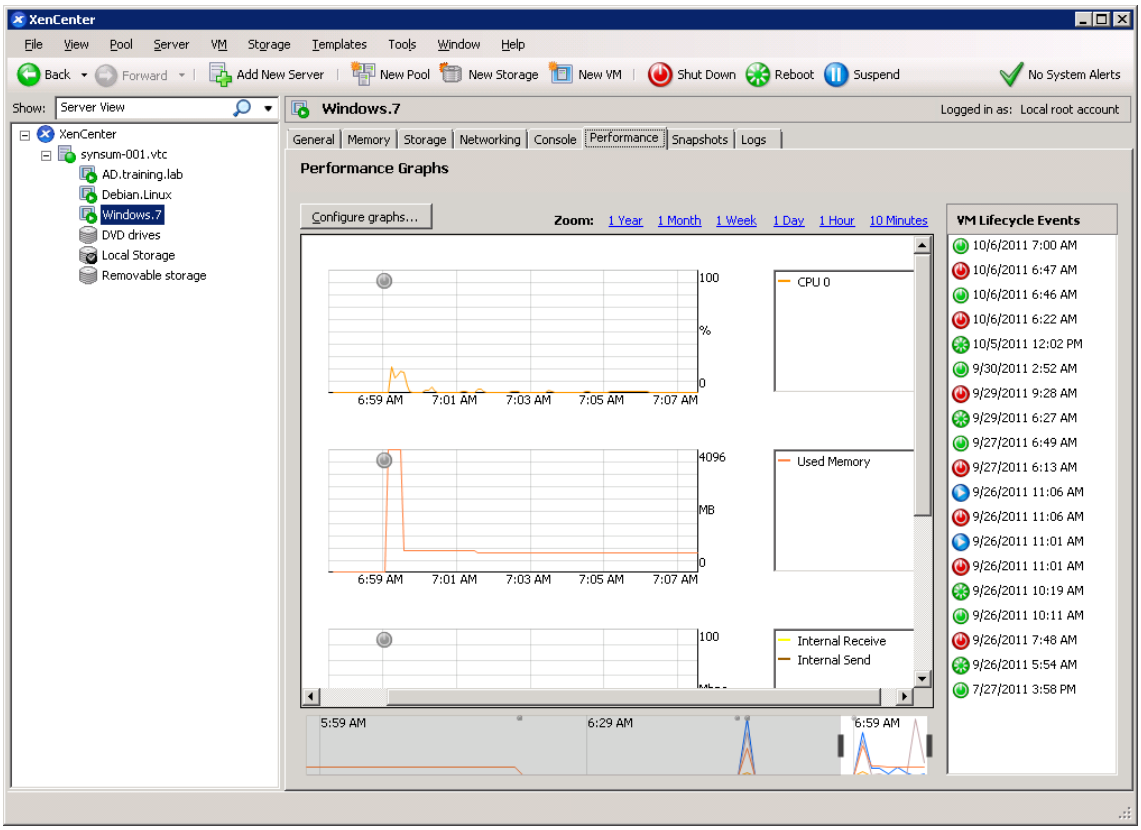
To complete this exercise, you must have the following:

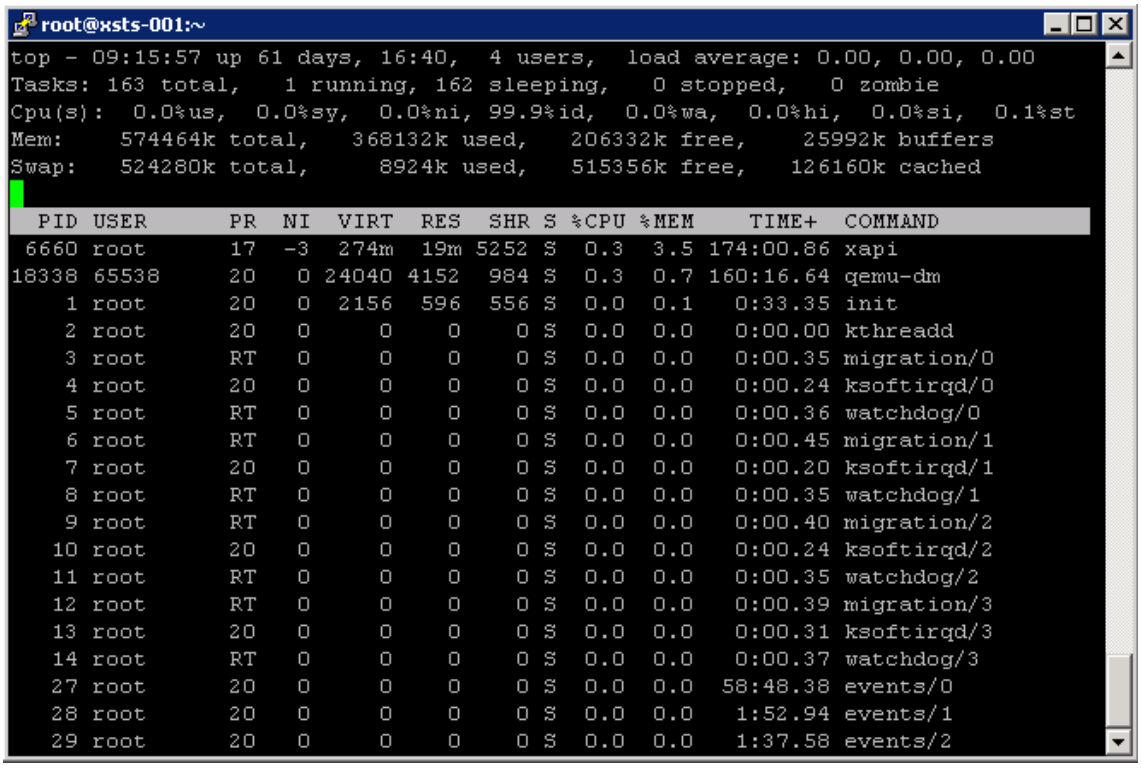
- XenCenter
- SSH client (PuTTY)

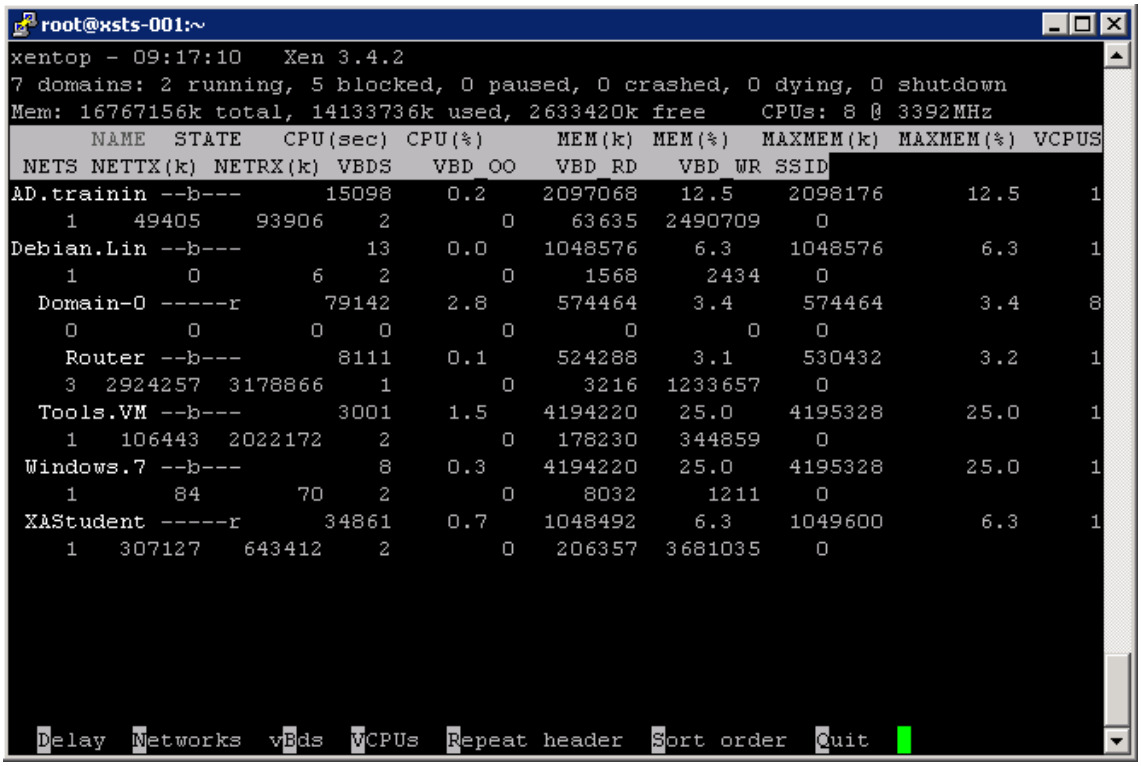
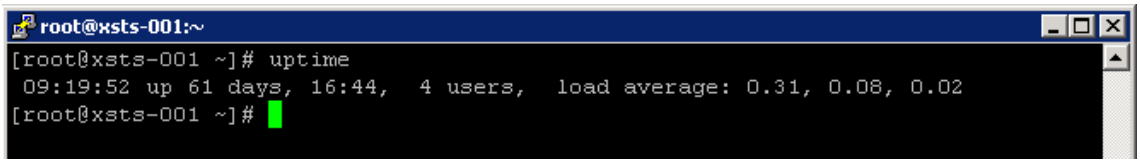
Step-by-step guidance

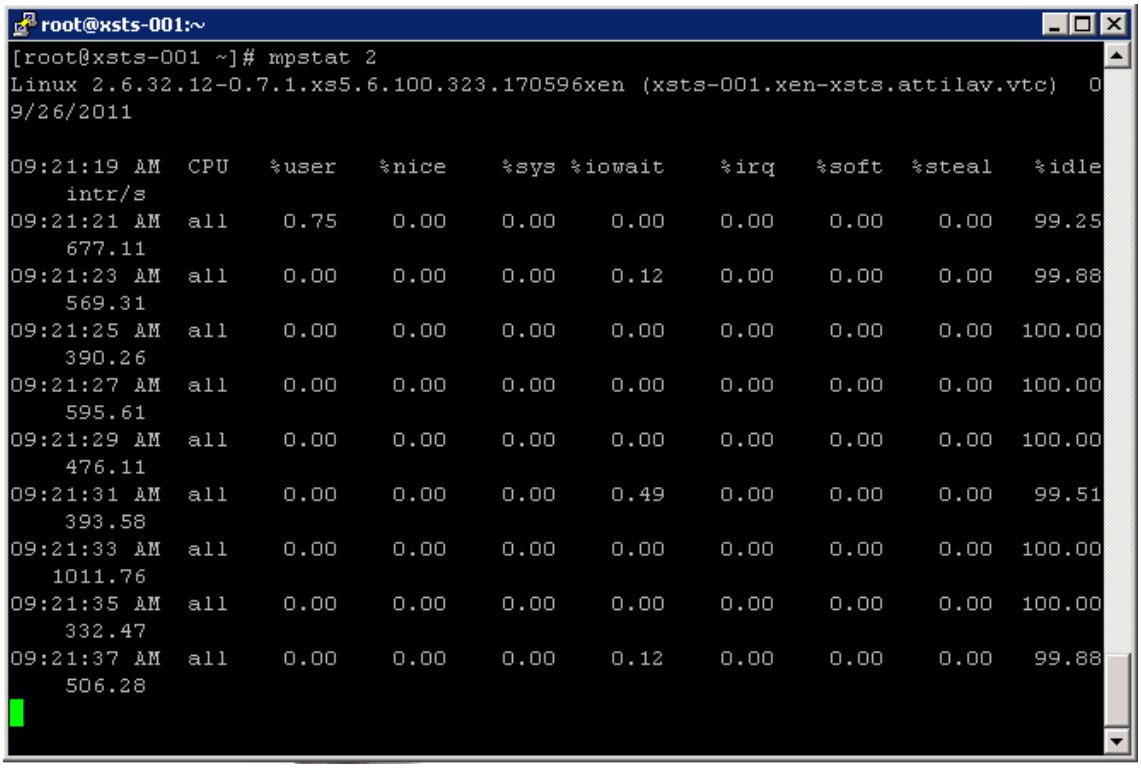
Estimated time to complete this lab: **15 minutes**.

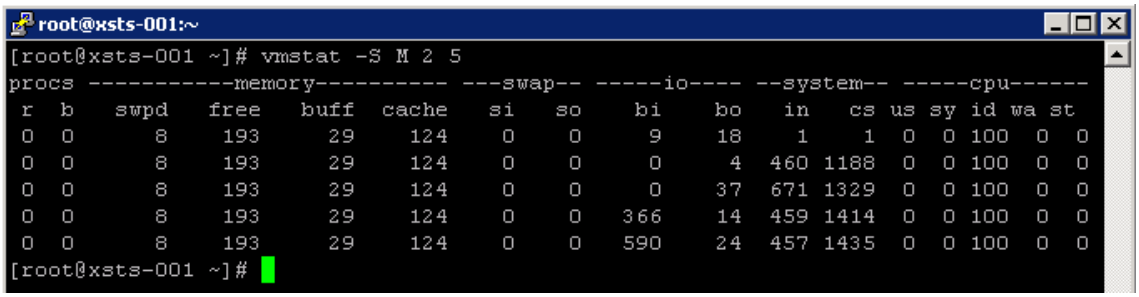
Step	Action
	Review the performance metric information available in XenCenter:
1.	Ensure all VMs are running to generate load on the XenServer host
2.	To monitor a XenServer host performance metric highlight the host and click on the **Performance** tab. 

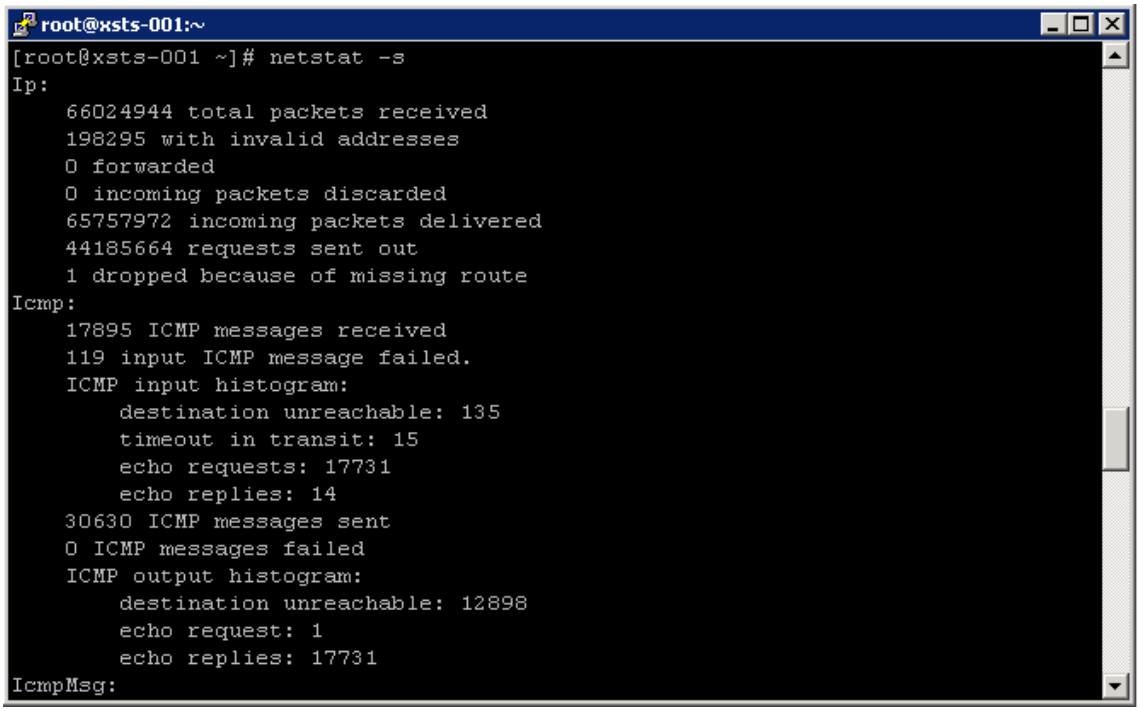
Step	Action
3.	To monitor a virtual machine performance metric highlight the VM and click on the **Performance** tab 
	Use the CLI to display performance and utilization information:
4.	Launch a new SSH client **OR** duplicate an existing session of **PuTTY** from the Landing Desktop **OR** reuse an open session window.

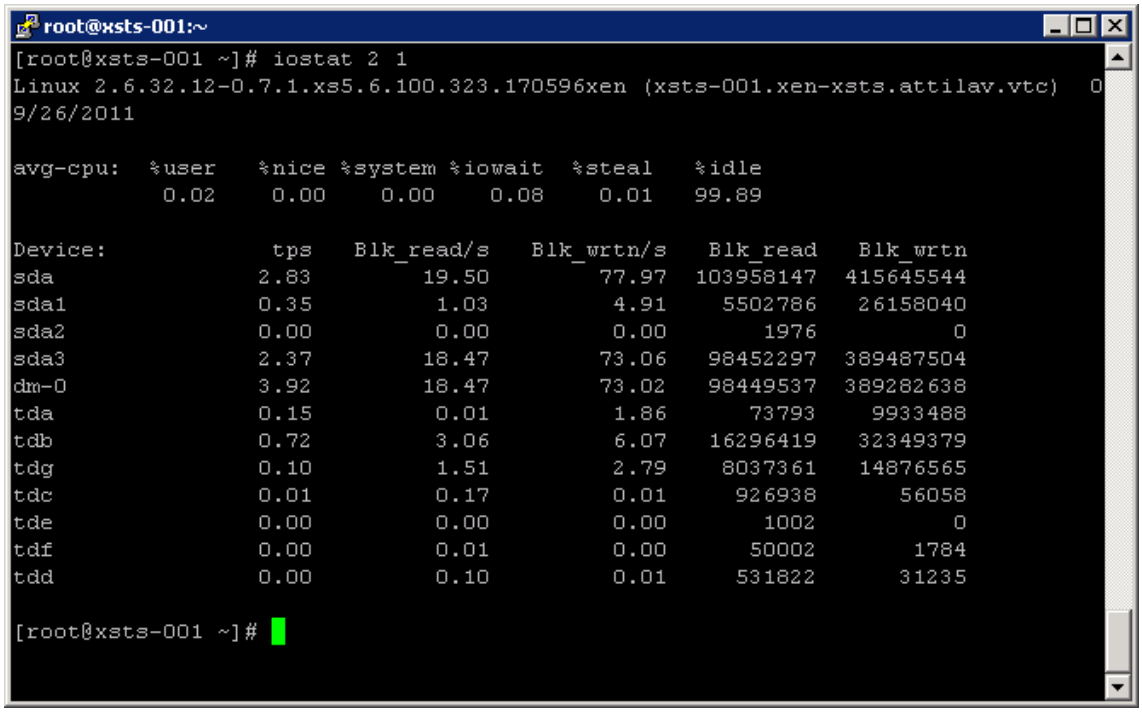
Step	Action
5.	Use the **top** command view the current tasks on dom0 e.g. **top**  Press **q** to quit **Tip:** • Press **h** to display interactive command options. Press **Enter** to return to the main screen. • Press **1** to view individual CPU information utilized by Dom0. Note that since XenServer 5.6 FP1 Dom0 has access to a maximum of 4 vCPUs by default. • Press **<** and **>** to scroll through the task columns. • Press **c** to display the command line name of the task. **Note:** For more information about the top command run **man top** for the manual page of this tool **Note: top** displays the information as seen from Dom0

Step	Action
6.	Use xentop to display the information of the hypervisor and domains. e.g. **xentop**  Press **q** to quit **Tip:** Press **N** to display network related information. **Tip:** Press **V** to display VCPU information. **Note: xentop** displays information as seen from the hypervisor. For more information about xentop type **man xentop.**
7.	Use the **uptime** command to display the average load on the server e.g. **uptime**  **Note:** The **uptime** command shows the average sum of the number of processes waiting in the run-queue plus the number currently executing over 1, 5, and 15 minute time periods i.e. **0.31** (1 min), **0.08** (5 min), **0.02** (15min). **Note:** If a system that has a load average significantly higher than the number of CPUs it could indicate a possible bottleneck.

Step	Action
8.	Use the **mpstat** command to display processor related information e.g. **mpstat 2**  Press **CTRL+C** to quit **Tip: mpstat (n)** will designate the interval at which metrics should be displayed i.e. **mpstat 5** **Tip: mpstat -P ALL 2 5** will display five reports of statistics for all processors at two second intervals **Note:** For more information about the mpstat command run **man mpstat** for the manual page of this tool

Step	Action
9.	Use the **vmstat** command to display virtual memory related information e.g. **vmstat –S M 2 5**  Press **CTRL+C** to quit **Tip: vmstat (n)** will designate the intervals at which metrics are displayed i.e. **vmstat 2** **Tip: vmstat** (n) **(n)** will designate the second intervals at which metrics are displayed and the count i.e. **vmstat 2 5** (every 2 seconds, 5 times). **Tip: -S** is used to specify units and **M** is to set the unit to Megabytes Columns of interest are: • **si**: memory swapped in from disk /s • **so**: memory swapped to disk /s • **us**: time running non-kernel code (user time/space) • **sy**: time running kernel code • **wa**: time waiting for CPU IO **Note:** For more information about the vmstat command run **man vmstat** for the manual page of this tool. This tool is generally used to highlight performance bottlenecks in a server.

Step	Action
10.	Use the **netstat** command to display network related information e.g. **netstat –s**  Press **CTRL+C** to quit **Tip: netstat –s –c** displays network statistics at 1 second intervals **Note:** For more information about the netstat command run **man netstat** for the manual page of this tool

Step	Action
11.	Use the **iostat** command to display input and output related information which could relate to CPU or devices e.g. **iostat 2 1**  **Tip: iostat 2 1** displays one report at two second intervals for all devices **Tip: iostat –d 2** displays a continuous device report at two second intervals **Tip: iostat –n** displays NFS directory statistic if mapped **Note:** For more information about the iostat command run **man iostat** for the manual page of this tool.

Step	Action
12.	Use the **sar** command to display processor queue related information e.g. **sar –q 2 10**

```
root@xsts-001:~
[root@xsts-001 ~]# sar -q 2 10
Linux 2.6.32.12-0.7.1.xs5.6.100.323.170596xen (xsts-001.xen-xsts.attilav.vtc)  0
9/26/2011

09:30:10 AM   runq-sz  plist-sz   ldavg-1   ldavg-5  ldavg-15
09:30:12 AM         0       299      0.01      0.02      0.00
09:30:14 AM         0       299      0.01      0.02      0.00
09:30:16 AM         0       299      0.01      0.02      0.00
09:30:18 AM         0       299      0.01      0.02      0.00
09:30:20 AM         1       299      0.01      0.02      0.00
09:30:22 AM         0       299      0.01      0.01      0.00
09:30:24 AM         0       299      0.01      0.01      0.00
09:30:26 AM         0       299      0.01      0.01      0.00
09:30:28 AM         0       299      0.01      0.01      0.00
09:30:30 AM         0       299      0.01      0.01      0.00
Average:            0       299      0.01      0.01      0.00
[root@xsts-001 ~]#
```

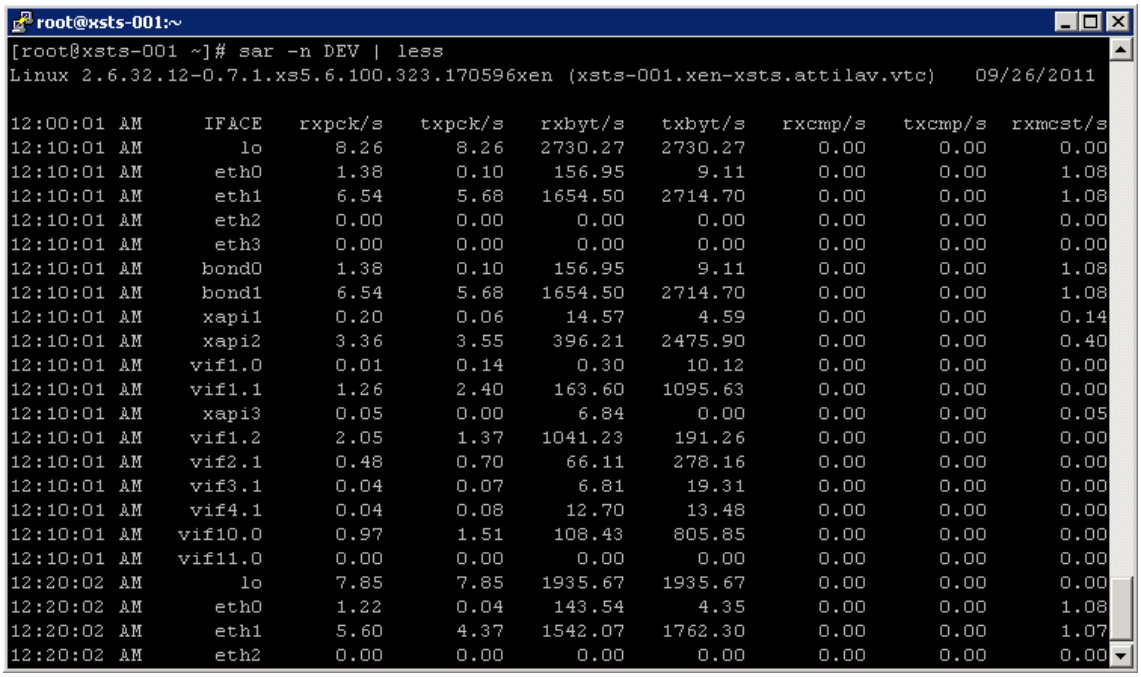
Note: In the above example we collect 10 reports in 2 second intervals.

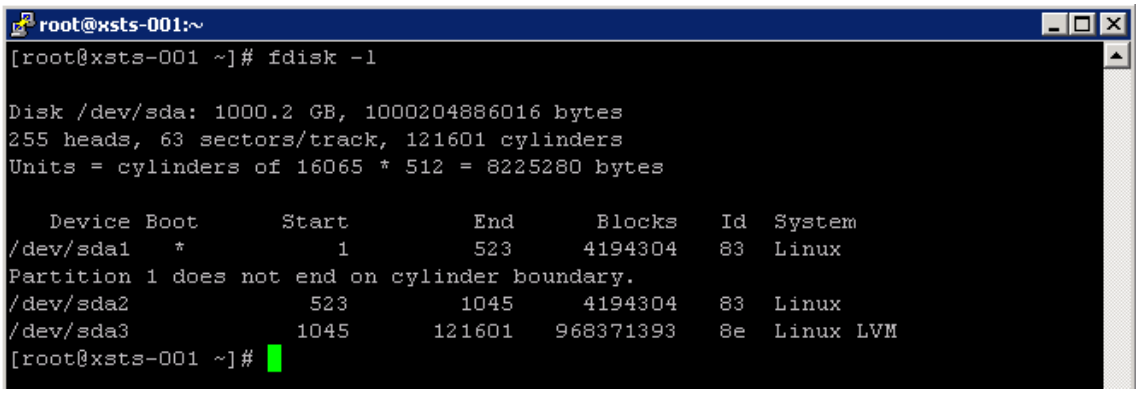
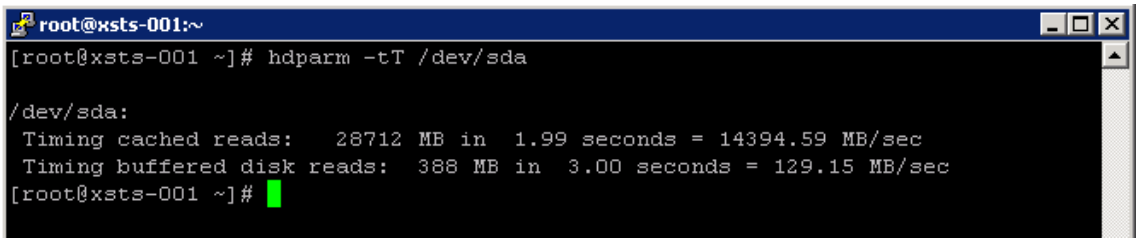
Also use the **sar** command
e.g. **sar –u**

```
root@xsts-001:~
[root@xsts-001 ~]# sar -u
Linux 2.6.32.12-0.7.1.xs5.6.100.323.170596xen (xsts-001.xen-xsts.attilav.vtc)   09
/26/2011

12:00:01 AM       CPU     %user     %nice   %system   %iowait    %steal     %idle
12:10:01 AM       all      0.02      0.00      0.01      0.08      0.01     99.89
12:20:02 AM       all      0.01      0.00      0.00      0.07      0.01     99.91
12:30:01 AM       all      0.01      0.00      0.00      0.07      0.01     99.90
12:40:01 AM       all      0.01      0.00      0.00      0.07      0.01     99.91
12:50:01 AM       all      0.01      0.00      0.00      0.08      0.01     99.90
01:00:01 AM       all      0.01      0.00      0.00      0.06      0.01     99.92
01:10:02 AM       all      0.02      0.00      0.00      0.07      0.01     99.91
01:20:01 AM       all      0.01      0.00      0.00      0.07      0.01     99.91
01:30:01 AM       all      0.01      0.00      0.00      0.06      0.01     99.92
01:40:01 AM       all      0.02      0.00      0.00      0.06      0.01     99.91
01:50:01 AM       all      0.01      0.00      0.00      0.06      0.01     99.92
02:00:01 AM       all      0.01      0.00      0.00      0.07      0.01     99.91
02:10:01 AM       all      0.02      0.00      0.00      0.06      0.01     99.91
02:20:01 AM       all      0.01      0.00      0.01      0.07      0.01     99.91
02:30:01 AM       all      0.01      0.00      0.00      0.08      0.01     99.91
02:40:01 AM       all      0.02      0.00      0.00      0.07      0.01     99.90
02:50:01 AM       all      0.01      0.00      0.00      0.07      0.01     99.91
03:00:01 AM       all      0.01      0.00      0.00      0.07      0.01     99.91
03:10:01 AM       all      0.02      0.00      0.00      0.06      0.01     99.91
03:20:01 AM       all      0.01      0.00      0.00      0.08      0.01     99.90
03:30:02 AM       all      0.01      0.00      0.00      0.07      0.01     99.92
```

Tip: These commands are useful to determine if your CPU is bound (is a bottleneck). If the run queue (**runq-sz**) from **sar –q** is consistently above 2 or 3 and the **idle CPU %** from **sar –u** is consistently below 5% then the CPU could be bound.

Step	Action
13.	Use the **sar** command to display network related information e.g. **sar –n DEV | less**  Press **q** to quit • **IFACE**: Name of the network interface for which statistics are reported. • **rxpck/s**: Total number of packets received per second. • **txpck /s**: Total number of packets transmitted per second. • **rxbyt/s**: Total number of bytes received per second. • **txbyt/s**: Total number of bytes transmitted per second. • **rxcmp/s**: Number of compressed packets received per second. • **txcmp/s**: Number of compressed packets transmitted per second. • **rxmcst/s**: Number of multicast packets received per second. **Note:** Scroll down to the bottom of the output to see the device averages.

Step	Action
14.	Use the **hdparm** command to collect disk transfer speeds: First list available device using fdisk. e.g. **fdisk –l**  Next display the transfer speeds of a disk device by using hdparm: e.g. **hdparm –tT [device name]**  **Note:** -t performs **device** read timings -T performs **cache** read timings
15.	Note that any of the above mentioned commands can redirect their output to a file using the **> [filename]** parameter
END OF EXERCISE	

Summary

Key Takeaways	The key takeaways for this exercise are: • You will be able to view and gather performance related data about your XenServer environment. • You will be able to analyze performance related data.

Exercise 8: Creating and Reviewing Snapshots

Overview

In this exercise we will create new virtual machine snapshots and also revert to these snapshots.

A virtual machine (VM) snapshot is a record of a running virtual machine at a point in time. When you take a snapshot of a VM, its storage information (the data on the hard drive) and metadata (configuration information) is saved.

XenServer 5.6 and above provides the functionality to save a VM's state (RAM). This can be useful if you are upgrading or patching software, or want to test a new application.

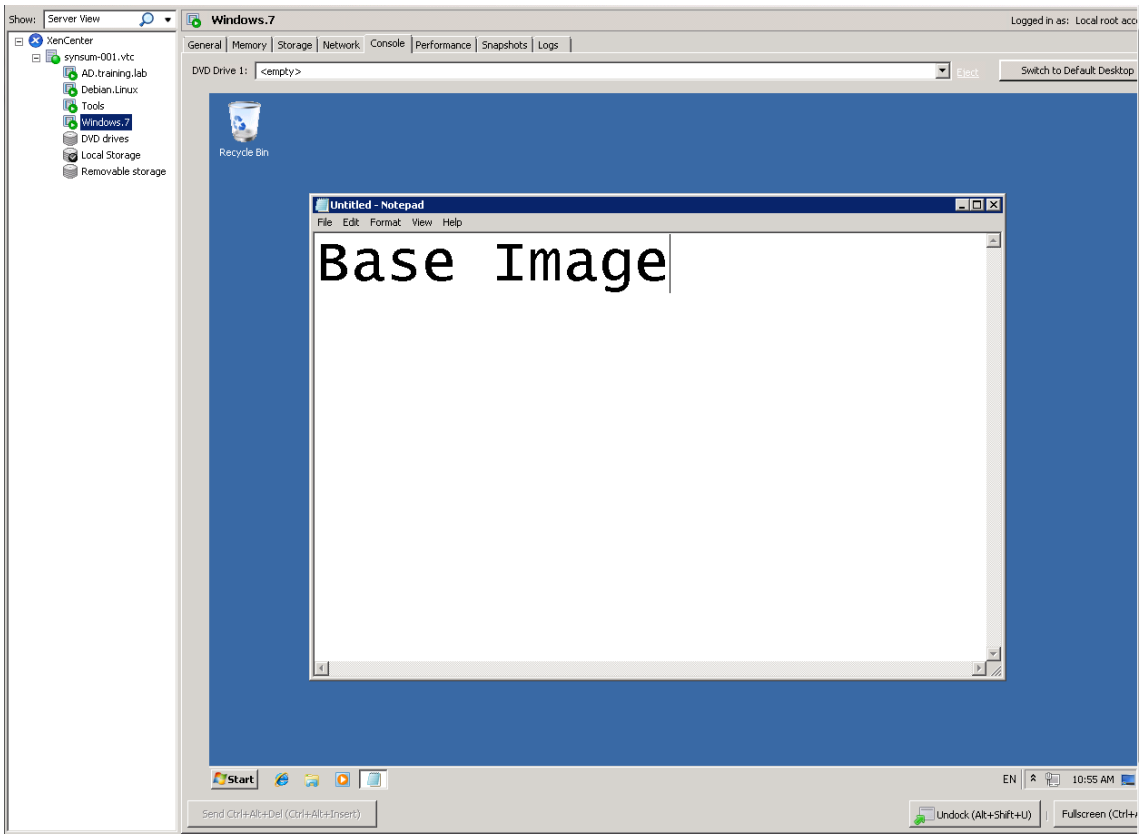
To complete this exercise, you must have the following:

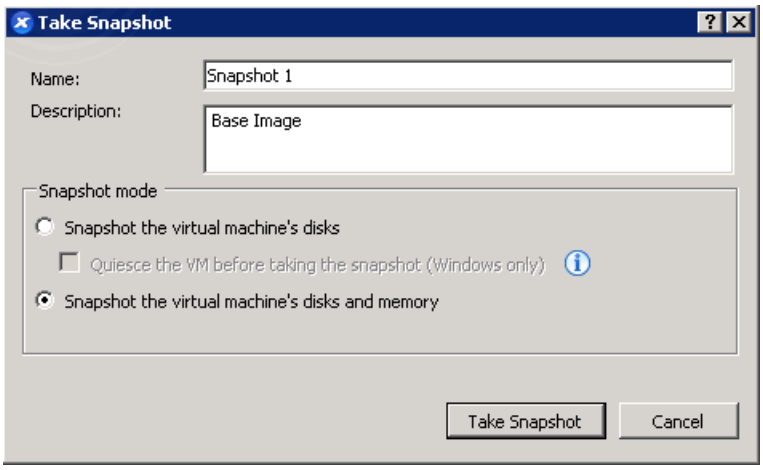
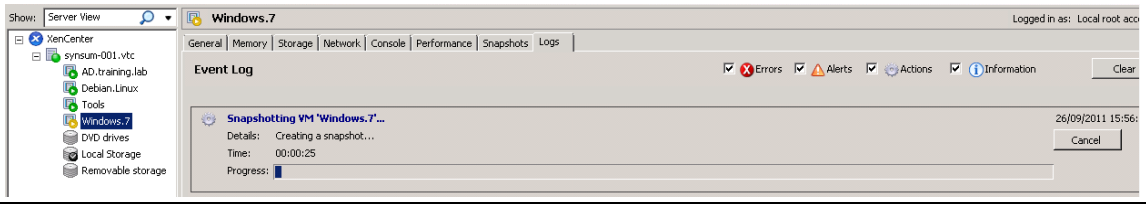
- XenServer 5.6 and above
- XenCenter
- SSH client (PuTTY)

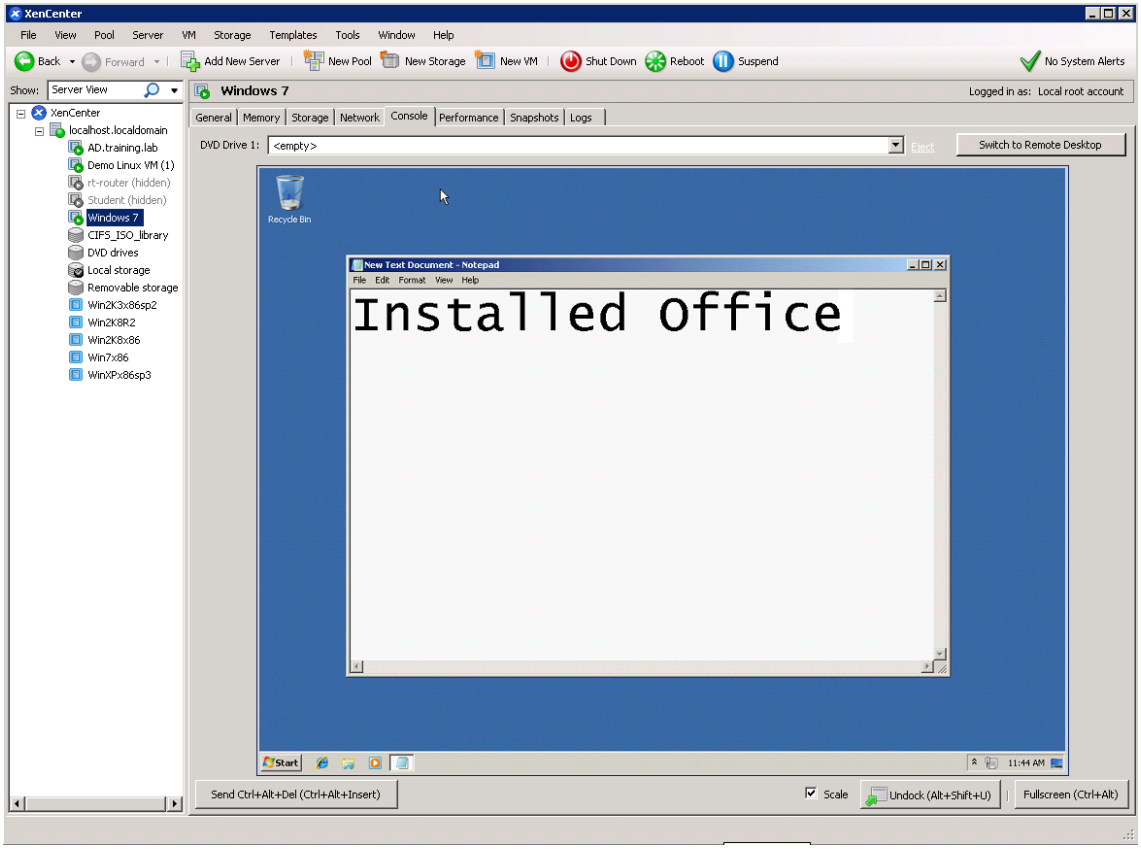
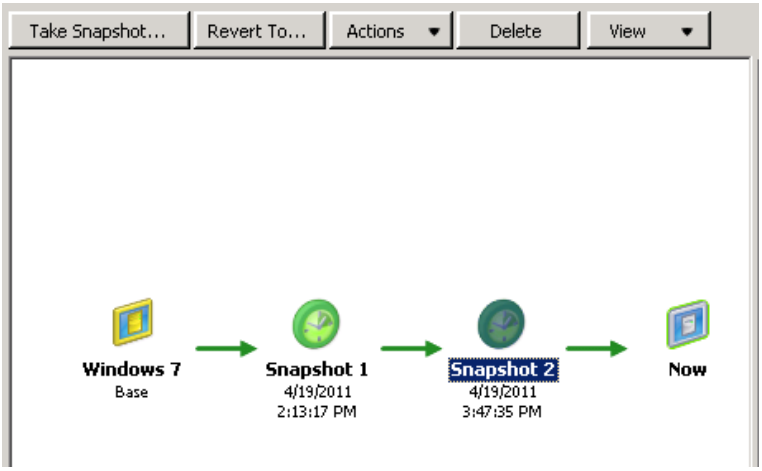
Step-by-step guidance

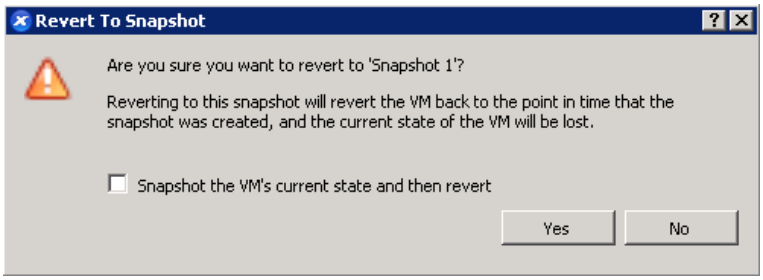
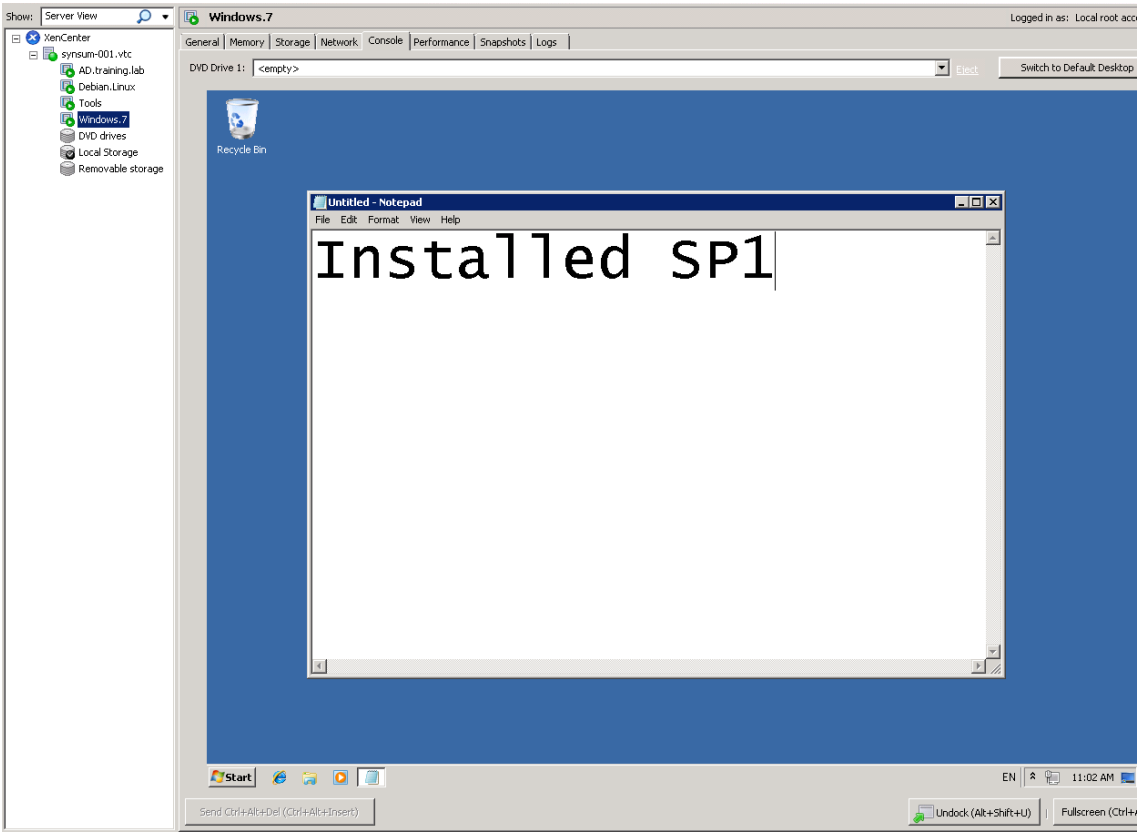
Estimated time to complete this lab: **15 minutes**.

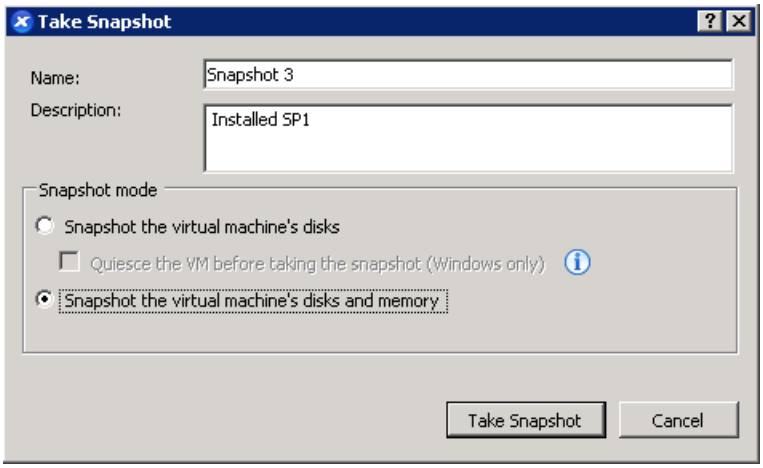
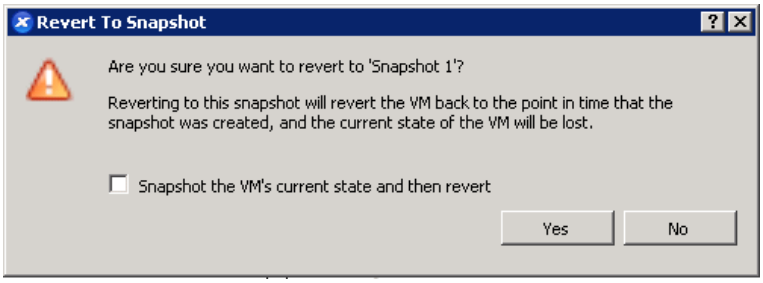
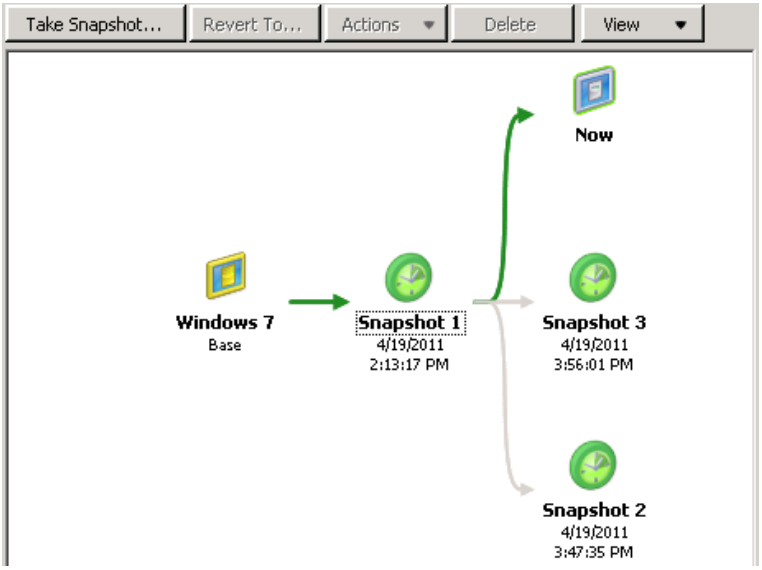
Step	Action
	Creating and Reverting VM Snapshots:
1.	Launch **XenCenter** and connect to your assigned XenServer if required
2.	Start or select the running **Windows.7** VM and click the **Console** tab

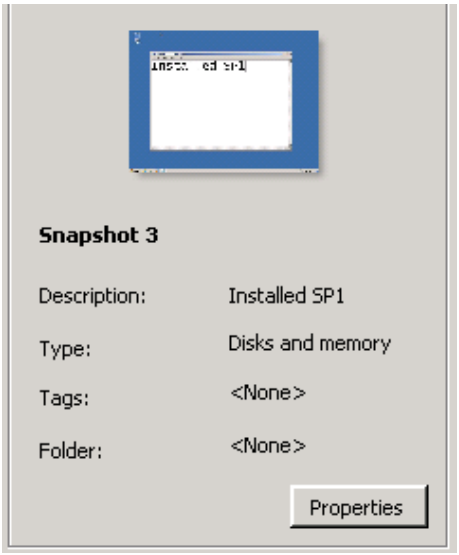
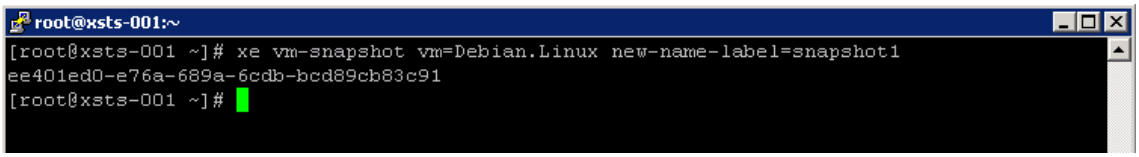
Step	Action
3.	Create a .txt file on the desktop and write "**Base Image**" in the file (leave file open). - The text will simulate the installation of software within the VM - We will be using this text to follow the snapshot state **Note:** Increase the font size to 48 if required. 
4.	Select the **Snapshots** tab

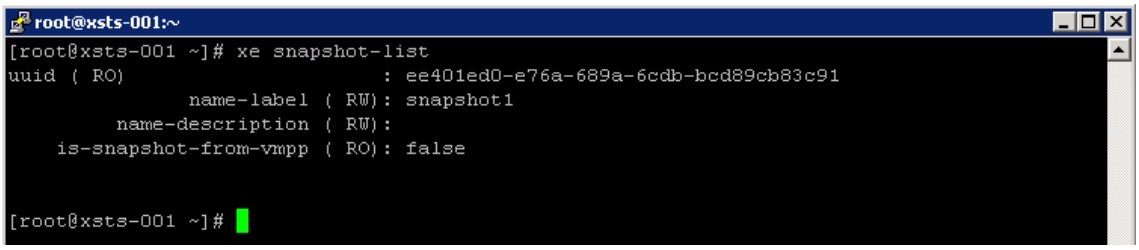
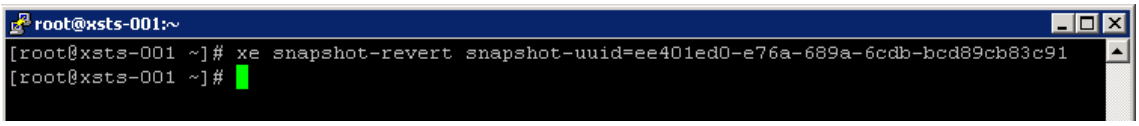
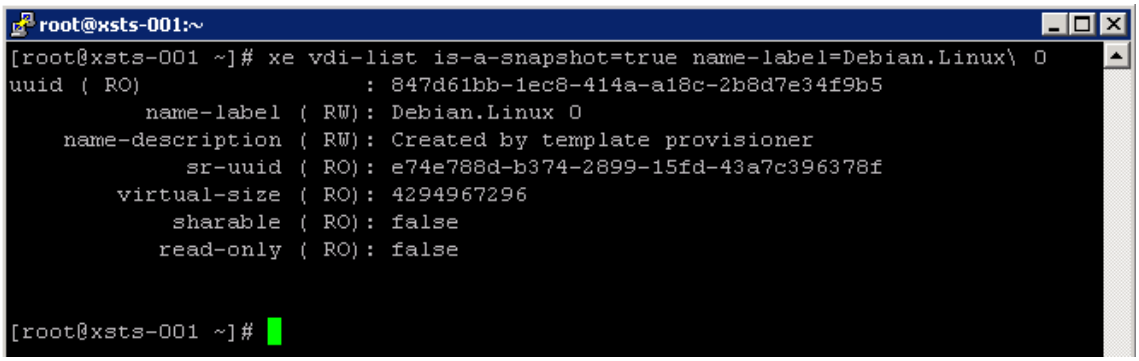
Step	Action
5.	Take **disk and memory** snapshot with a description of "**Base Image**"  **Note:** The running VM is temporarily suspended during the live snapshot process **Note:** Quiesce snapshots are only available for Windows VMs (Windows Server 2003 and Windows Server 2008 for both 32-bit and 64-bit variants) which utilizes the VSS service. The VSS plug-in needs to be installed within the virtual machine. For more information please refer to XenServer VM Installation Guide.
6.	Follow the snapshot process in the **Logs** tab. 

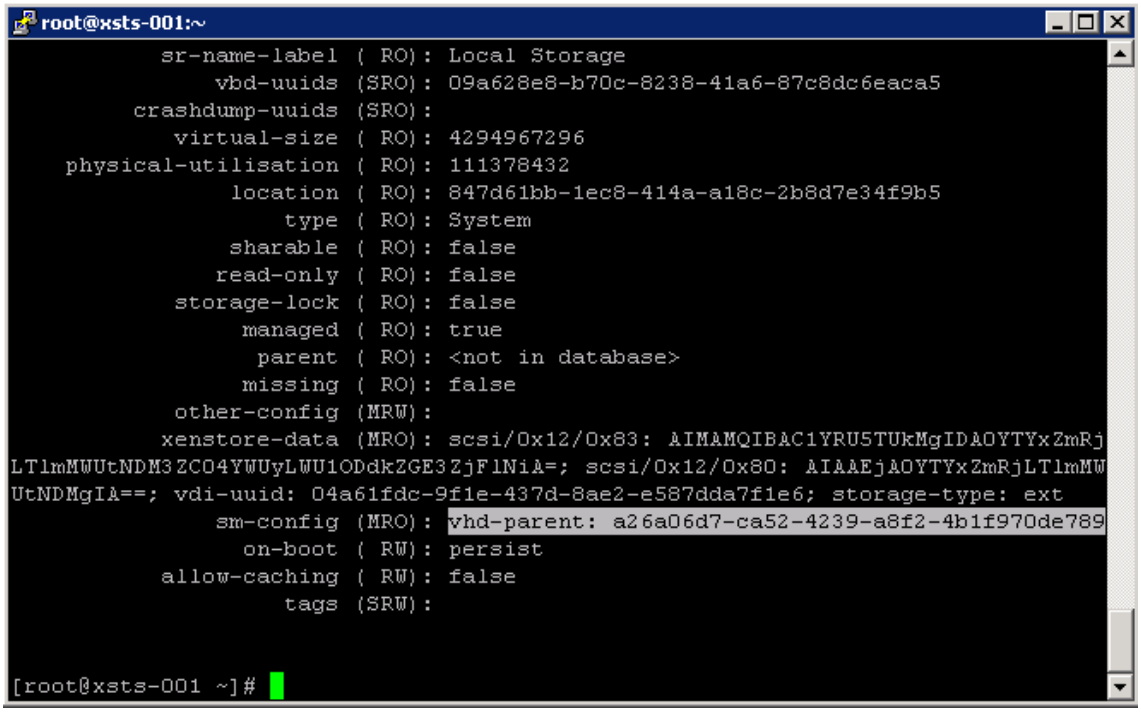
Step	Action
7.	Select the **Console** tab and change the text in the .txt file to read "**Installed Office**" 
8.	Create a **second** disk and memory **snapshot** with a description of "**installed office**" 

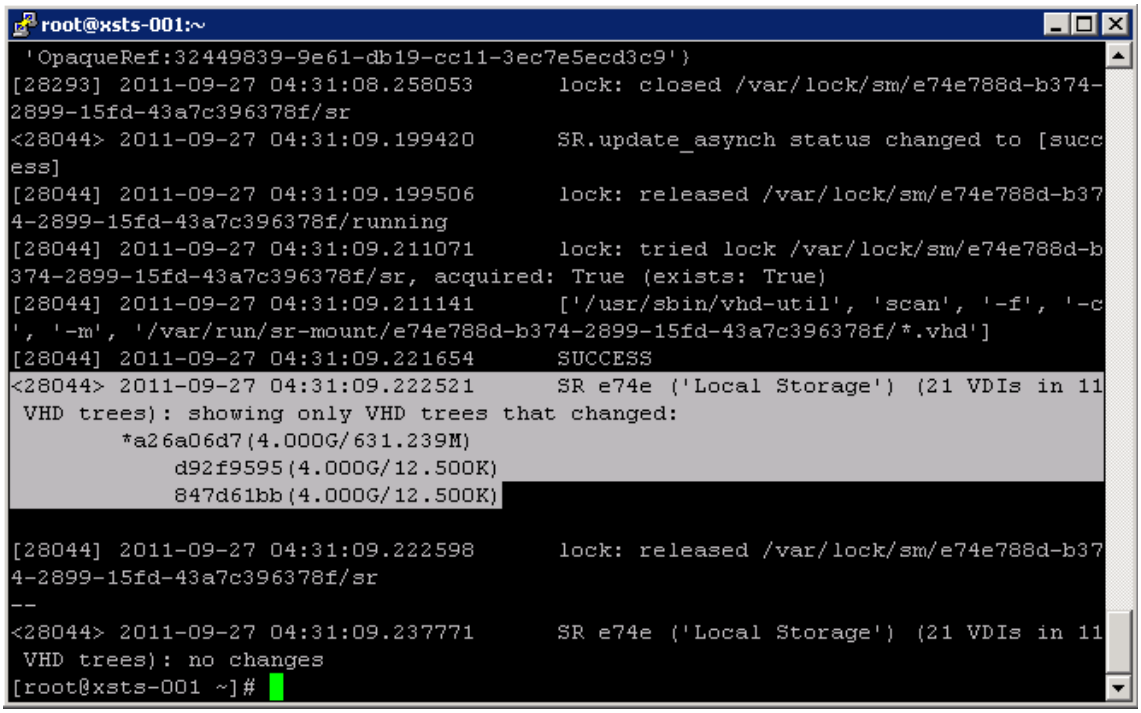
Step	Action
9.	Select **Snapshot 1** and click **Revert To…** - **Unselect** Snapshot the VMs current state - Click **Yes** 
10.	Click the **Console** tab and edit the .txt file to say "**Installed SP1**" 

Step	Action
11.	Select a **disk and memory** snapshot with a description of "**Installed SP1**" and take disk and memory snapshot 
12.	Select **Snapshot 1** from the Snapshot tab and click **Revert To…** - **Unselect** Snapshot the VMs current state - Click **Yes** 
13.	Review VM **Life Tree** 

Step	Action
14.	Select a **snapshot** and click on the screen **icon** in the **Details** pane to review the "state" of the VM based on the text file 
15.	Highlight all snapshots of the **Windows.7** VM by dragging your mouse over them and click **Delete**
	Connect to your XenServer host via an SSH client (PuTTY) and login to the console:
16.	Launch a new SSH client **OR** duplicate an existing session of **PuTTY** from the Landing Desktop **OR** reuse an open session window.
17.	Create a snapshot of your **Debian.Linux** VM by running following command: e.g. **xe vm-snapshot vm=Debian.Linux new-name-label=snapshot1**  **Tip:** Remember to use tab completion in the CLI
18.	**Confirm** snapshot has been taken correctly in XenCenter

Step	Action
19.	List snapshots via CLI by running the following command: i.e. **xe snapshot-list**  **Note:** This command will list all snapshots within a pool.
20.	Revert to a snap of your **Debian.Linux** VM by running following command: e.g. **xe snapshot-revert snapshot-uuid=[UUID of snapshot1]**  **Note:** Due to the disk-only snapshot taken previously the **Debian.Linux** VM will revert to a halted (crash consistent) state.
	Review VHD chain dependencies of a VM using the CLI:
21.	Find the VDI which you want to review by running following command: e.g. **xe vdi-list is-a-snapshot=true name-label=Debian.Linux\ 0** 

Step	Action
22.	Find out which VDI/VHD file is the parent of the VDI we want to review by running the following command: e.g. **xe vdi-param-list uuid=[UUID of snapshot VDI]**  **Note:** From the above command we can see which VDI/VHD file is the parent in a chain.

Step	Action
23.	To view the VHD tree/chain for a virtual disk we can use the **/var/log/SMlog** by running following command: e.g. **less /var/log/SMlog | grep SR –A 5**  **Note:** In the above example we use the **grep** command to output only the matching pattern **"SR"** and the following 5 lines. **Note:** In the above example the 3 VDIs are listed in relation to the Debian Linux VM: • ***a26a06d7(4.000G/631.239M)** = original parent disk • **d92f9595(4.000G/12.500K)** = current in-use R/W disk • **847d61bb(4.000G/12.500K)** = snapshot taken previously
END OF EXERCISE	

Summary

Key Takeaways	The key takeaways for this exercise are: • You will be able to create new and revert to VM snapshots. • You will be able to create, revert and view snapshots via the CLI. • You will be able to review VHD chain dependencies of a VM using the CLI.

Revision History

Revision	Change Description	Updated By	Date
1.0	Final Version	Dian Kotzé	10/2011

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is the leading provider of virtualization, networking and software as a service technologies for more than 230,000 organizations worldwide. Its Citrix Delivery Center, Citrix Cloud Center (C3) and Citrix Online Services product families radically simplify computing for millions of users, delivering applications as an on-demand service to any user, in any location on any device. Citrix customers include the world's largest Internet companies, 99 percent of Fortune Global 500 enterprises, and hundreds of thousands of small businesses and prosumers worldwide. Citrix partners with over 10,000 companies worldwide in more than 100 countries. Founded in 1989, annual revenue in 2008 was $1.6 billion.

http://www.citrix.com

© 2011 Citrix Systems, Inc. All rights reserved. Citrix®, Citrix Delivery Center™, Citrix Cloud Center™, XenApp™, XenServer™, NetScaler®, XenDesktop™, Citrix Repeater™, Citrix Receiver™, Citrix Workflow Studio™, GoToMyPC®, GoToAssist®, GoToMeeting®, GoToWebinar®, GoView™ and HiDef Corporate™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.