# ESXLab.com Sample Chapter

**Course:** ESXLab.com VMware vSphere 5.0 with ESXi and vCenter

Attached is a sample chapter from our *VMware vSphere 5.0 with ESXi and vCenter* 5 day class. This chapter is chapter 2 of 21 chapters that make up our 5 day introductory class.

In the attached chapter students install and configure ESXi from first principles. Not only do attendees learn the concepts and issues around installing ESXi, they get practical, hands-on skills that they can use at work including:

- Preparing a server for ESXi installation
- Performing installation and post installation tasks
- Installing the VMware vSphere Client
- Joining ESXi to a Windows domain
- Configuring the server for best performance while minimizing power draw
- Defining who can connect to the server and setting their permissions
- Configuring ESXi so that it provides accurate time to Virtual Machines

The attached chapter and lab are one of the longer chapters in our class. However, each chapter has the same level of detail, including detailed study notes. Each lab has easy-to-follow instructions that take attendees from first principles to successfully completing the required tasks. Our labs are designed so that attendees can perform essentially the same steps at their work – and accomplish the same result!

We also have a 4 day VMware vSphere Advanced class and a 5 day VMware vSphere Boot Camp class for attendees who want to take their VMware vSphere installation to the next level. We provide remote access servers and courseware as well.

For more information on aftermarket VMware training solutions and certification from ESXLab, please contact us:


Larry Karnis – ESXLab.com

Phone: 1 (905) 451-9488

Toll Free: 1 (888) 451-3131

E-mail: Larry.Karnis@esxlab.com

Web: Http://www.esxlab.com

# Chapter 2 – VMware ESXi






## Notes

# Stand Alone ESXi

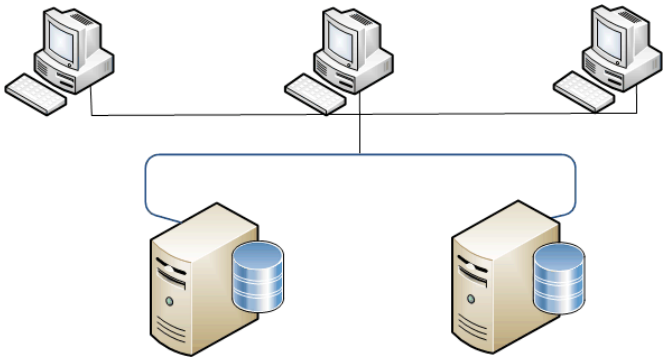
- ESXi Overview
- ESXi Installation Procedures
- Best Practices





## Notes

# Project Plan



- By the end of this chapter, we will have
  - Installed ESXi onto a stand alone server
  - Partitioned local storage for ESXi and VMs
  - Connected to ESXi using the vSphere Client and Secure Shell





## Notes

Our first step in this class is to install ESXi onto stand alone PC servers and then connect to those newly installed ESXi hosts using the vSphere Client and SSH. In future chapters we will add to our original implementation. Our ultimate objective is a scalable, highly redundant, load balanced Virtual Infrastructure implementation that supports a large community of Windows 2000, Windows 2003, Windows 2008, desktop and Linux VMs.

# Problems & Opportunities

- Problems
  - Server consolidation
    - DNS, DHCP, Web, File & Print, AD, DC
  - Reduce costs
    - Capital $
    - Hardware support $
    - IT staff admin time
  - Free up rack space
  - Increase server utilization rates
  - Position for future growth, flexibility
- Virtual Solution
  - ESXi or vSphere
    - unlimited physical RAM
    - unlimited core CPUs
    - Up to 32 GB NICs
    - Up to 8 10GB NICs
    - Local, shared storage volumes, file shares
  - Consolidate many workloads onto one ESXi host





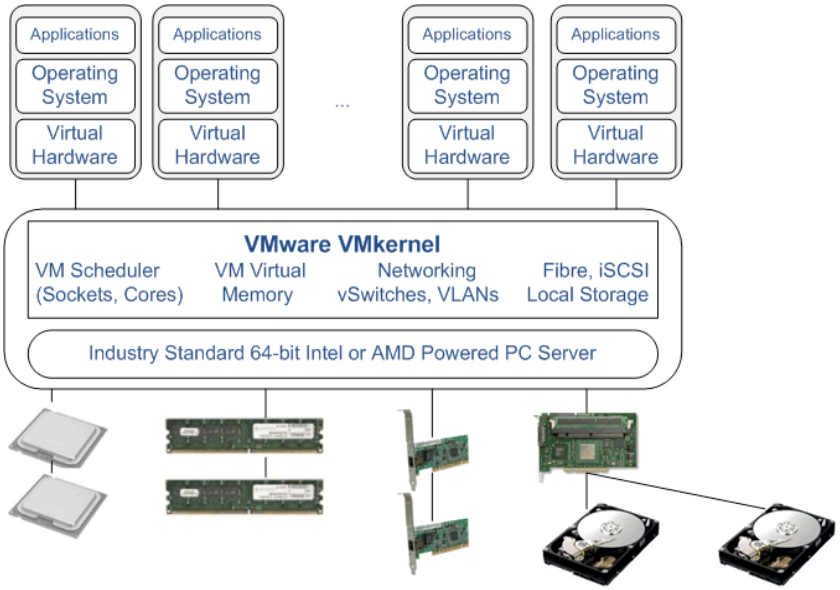

## Notes

vSphere Standard Edition is a low cost version of VMware ESXi especially intended for entry level virtualization deployments that offer the following hardware capabilities

- One or more physical CPUs
- 4 or 6 core CPUs supported (up to 12 core CPUs on vSphere Enterprise(+))
- Will use up all available physical memory up to 256GB
- Local disks or RAID volumes on supported SATA, SCSI or SAS controllers
- Up to 32, 1GB NICs including dual and quad NICs
- Up to 4, 10GB NICs
- iSCSI hardware and software initiators
- Fibre host bus adapter support and
- Use of NFS shares.

With the ability to run up to 8 light duty or 2-4 medium duty VMs per CPU core, ESXi or vSphere Standard Editions are excellent choices for entry level server consolidation projects.

# ESXi Block Diagram





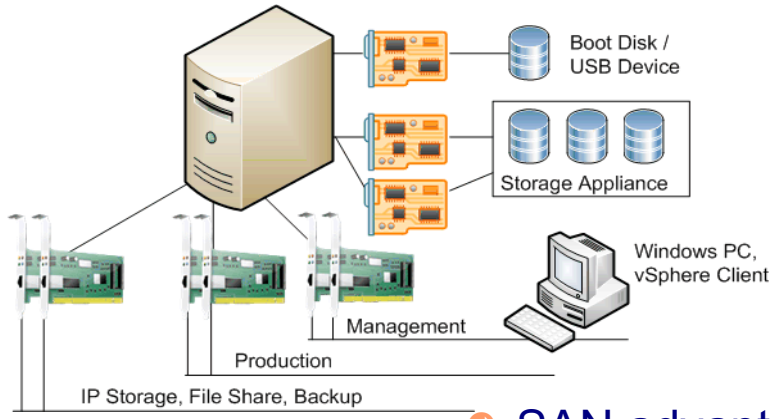



## Notes

VMware ESXi is a bare-metal virtualization hypervisor solution. As such, it must install on an industry standard PC server. Please check VMware's Hardware Compatibility Guide (portal on www.VMware.com web site) for the most up to date list of supported PC servers.

Because it owns the hardware, ESXi is in full control of resource assignments to running VMs. The VMkernel, allocates hardware resources on an as-needed basis. In this way, the VMkernel can prevent idling VMs from wasting CPU cycles that could otherwise be used by busy VMs. Likewise, the VMkernel keeps track of needed RAM, not just requested or allocated RAM. It can dynamically re-assign RAM to memory starved VMs, thereby ensuring that VMs get the memory they need to run.

# Scalable ESXi Deployment




- Local storage for
  - Boot, VMs, VM paging
- SAN LUNs
  - ESXi boot, swap, VMs

- SAN advantages
  - High performance
  - Higher availability
  - Capacity management
  - LUN Backup, replication
  - Disaster Recovery





## Notes

As your ESXi deployment matures (technically) you will want to introduce:

- Different LAN (virtual) segments to isolate network traffic. You could use different LAN segments for things like IP Storage, Management and production systems
- Shared storage solutions including iSCSI, Fibre SAN and NFS shares
- Hardware redundancy in the form of multipath storage solutions and teamed NIC configurations
- You may even wish to consider a Boot From SAN solution so you don't need to configure servers with local storage.

Boot from SAN is available on supported Fibre SAN controllers and also with iSCSI SAN controllers (using iSCSI hardware initiators).

# ESXi Server Hardware

- CPUs
  - 4, 6, 8, 10, 12 or 16 core physical CPUs
    - Max 160 cores/host
  - Intel 64-bit Xeon only
    - Hyperthreading
    - Not old EMT64 CPUs
  - AMD Opteron
    - NUMA local memory
    - All Opteron CPUs supported
  - Memory
    - Min 2GB to boot
    - All remaining physical RAM used for VMs
- Network
  - Up to 32 GB NICs
  - Up to 8 10GB NICs
  - VLAN, NIC Teams
- Storage
  - Local volumes
    - SCSI, SAS, SATA
    - RAID, non-RAID
    - SSD
  - iSCSI SANs
  - Fibre SANs
  - File Shares
    - NFS only
    - No SMB support




## Notes

ESXi is capable of using the largest PC server hardware platforms. Apart from what is stated above, ESXi is limited to:

- No more than 160 CPU cores (includes Hyperthreaded logical processors) for CPU scheduling purposes
- All available RAM

Furthermore the following implementation limitations need to be considered:

- Very limited selection of supported 10GB Ethernet controllers
- Jumbo Frames supported, which will dramatically improve software iSCSI performance.

# ESXi Embedded, Installable

- ESXi Embedded
  - Burned into flash on the motherboard
  - Host boots ESXi after POST
    - Boots from flash drive
  - ESXi configuration can be on local storage or retrieved from the network via PXE
- ESXi Installable
  - Local disks
    - RAID or JBOD
    - Can run on SSDs
  - USB boot
    - No RAID controller
    - No hard disks
    - Install and boot from low cost USB 2.0 device
    - Easy to duplicate
    - Most servers have internal USB stacks so USB drive cannot be accidentally removed




## Notes

JBOD – Just a Bunch of Disk. Physical disks in a non-RAID configuration.

VMware has officially retired ESX. That is, VMware will no longer release ESX for future releases of their software – just ESXi.

ESXi comes in two forms – Embedded and Installable. Embedded is baked into firmware on the motherboard of select PC servers. This lets you boot your server without any local storage.

ESXi Installable is a version of ESXi that can be installed onto local storage, USB memory keys or SAN storage. It is installed from CD media that you can download from www.vmware.com.

ESXi does away with the Service Console. This provides a smaller, leaner hypervisor than full ESX. It is also more secure because there is less software (to exploit) and fewer services running on ESXi than there is on ESX.

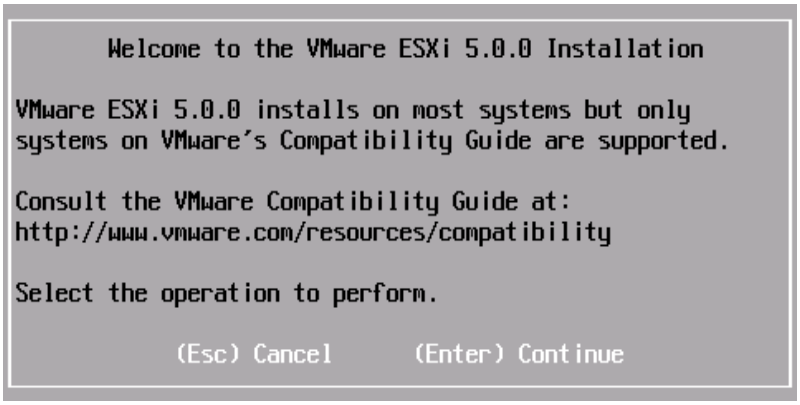
# ESXi Install Steps

- Install steps...
  - Boot your server from ESXi install media
  - Accept the EULA
  - Select target disk for installation
  - Select keyboard language
  - Set the root (administrator) password
  - Agree to partition and format disk
  - Reboot server when install complete
- Post install steps...
  - Log in and change root password




**Notes**

# ESXi Boot Screen




- To begin your ESXi install, boot from CD
  - Hit ENTER to launch the installer
- Customized installs
  - Serve media from HTTP or NFS
  - Scripted installs simplify deployment



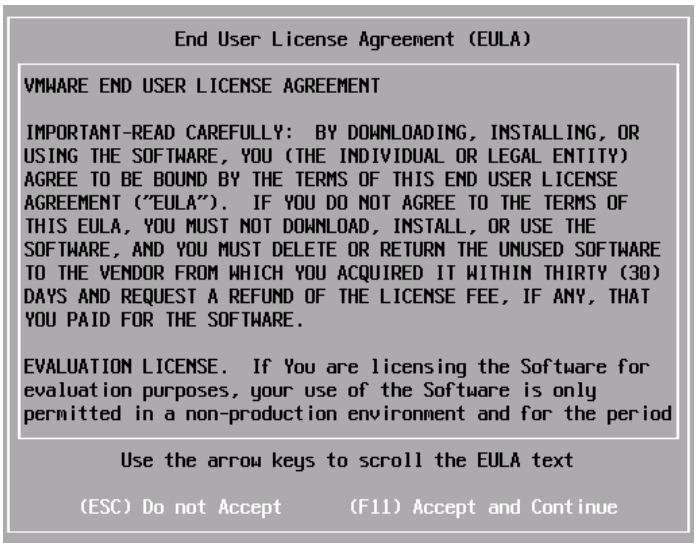

## Notes

ESXi is installed in text mode – so your PC server doesn't need to have graphics capability.

VMware makes it possible to set up an install server for ESXi so you can perform network based installs. Using Linux' KickStart capabilities, ESXi installations can be automated/scripted so you can install and configure new servers hands-off.

VMware also offers an ESXi automated deployment capability. This is part of the VMware vCenter Appliance that is new with vSphere 5.0.

# Accept the VMware EULA




- You must accept the VMware End User License Agreement before you install ESXi
  - Hit F11 to proceed to the next step




## Notes

The ESXi installer uses your Video Card's VESA mode for hardware independent graphics. The good news is that VESA is almost universally supported (and consequently should work). The bad news is that VESA is the slowest mode of operation.

The overall sluggishness of VESA mode is exacerbated by the use of remote management cards such as:

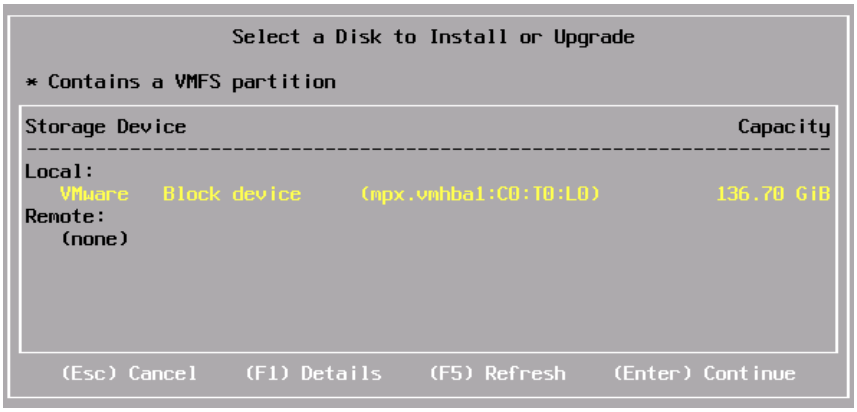
**HP** – Integrated Lights Out (iLo)
**IBM** – Remote Server Assistant (RSA)
**Dell** – Dell Remote Access Controller (DRAC)

While useful, remote graphics consoles over slower WAN links will require patience and a steady hand. To minimize the sluggish (drunk) mouse behavior, use key sequences like

**Tab** – move to the next clickable region
**Enter** – invoke a clickable action or
**Space** – select a clickable option.

In fairness to ESXi, graphics mode is only used during installation so graphics performance (or lack of it) is an installation time only issue.

# Select the Target Volume



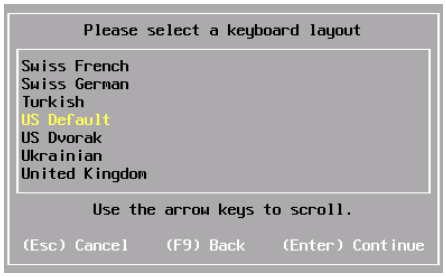

- Installer displays available storage volumes
  - Categorized as Local or Remote
  - Local volumes are visible to just your host and consist of local RAID or physical volumes
  - Remote volumes are visible SAN LUNs




## Notes

Normal ESXi installations occur in graphics mode. Consequently, the installer must get your preferences/settings for the install language, keyboard and mouse. These settings are used only during installation. Since, once it is in service, ESXi runs in text mode (with no native graphics capabilities), your language, keyboard and mouse preferences are discarded once the installation has completed.

# Keyboard, root Password



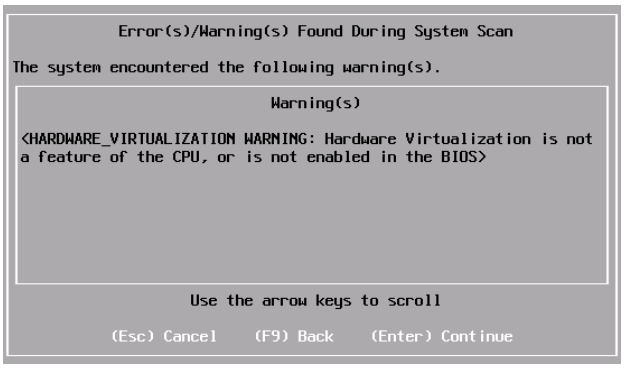


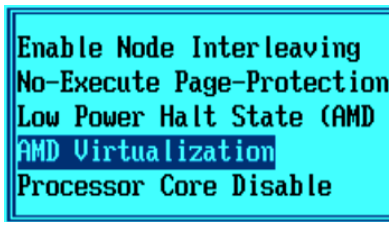
- Next, you specify:
  - The keyboard connected to your server
  - The password for the ESXi 5.0 root (local administrator) account
    - There is no password reset tool for ESXi 5.0 so do not forget your root password




**Notes**

# Hardware Virtualization Assist





- Modern CPUs have H/W virtualization assist capabilities
  - Intel VT technology and AMD-V
    - Significantly reduces VM overhead
  - Best Practice – Enable H/W virtualization features in the machine's BIOS if present




## Notes

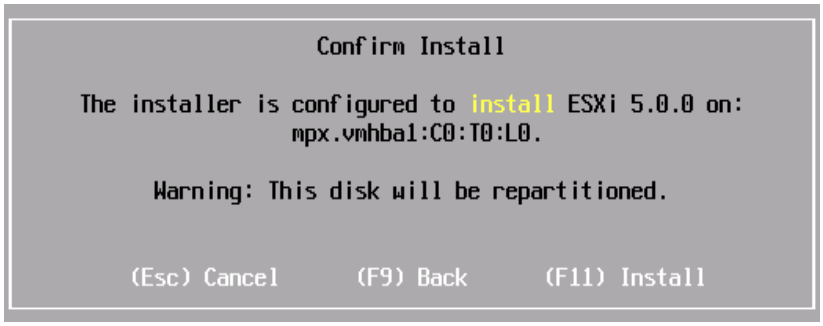
Virtualization abstracts the physical hardware to the VM. The VM guest operating system normally expects to own all hardware and also expects to be able to execute privileged CPU instructions that are not available to applications. If ESXi allowed guest operating systems full access to these instructions, then the guest OS could manipulate hardware directly, possibly interfere with virtual memory page translation tables and perform other operations that could compromise the ESXi host. To avoid this problem, VMware blocked guest OS' from privileged/dangerous instructions and CPU features through software that emulated (and controlled) what the guest OS could do. This worked but added significant overhead to some operations.

In 2006, both Intel and AMD introduced virtualization hardware assist technology in their updated CPUs. These new CPUs added sophisticated memory management capabilities, better hardware emulation features and other improvements that dramatically reduced the overhead of virtualization while maintaining compatibility with Guest OS'.

ESXi probes physical CPUs for Intel VT or AMD-V technology and attempts to use it if available (and warns if it isn't). Please be sure to turn on this feature in your machine's BIOS.

For more information see: http://en.wikipedia.org/wiki/X86_virtualization

# Ready to Install




- The installer is ready to proceed...
  - Selected volume is re-partitioned, formatted
    - All existing partitions on the selected volume are deleted
  - All local storage is used for ESXi
    - No partition customization options are available




## Notes

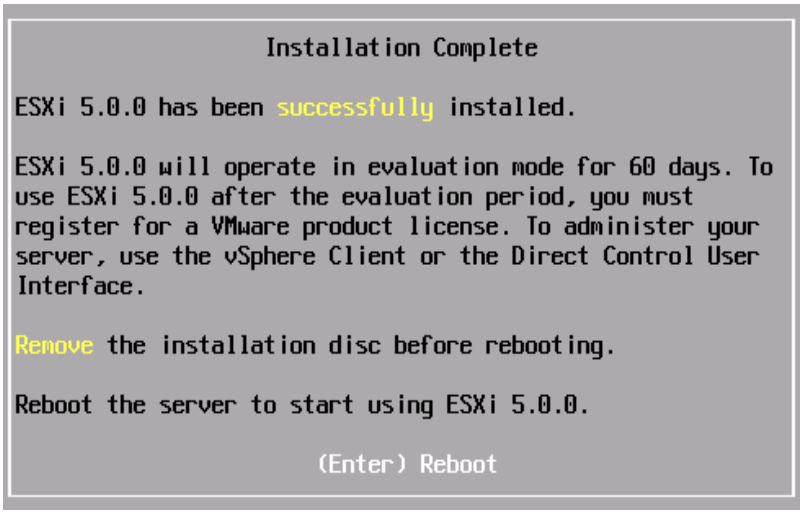
The installer will now install ESXi onto your selected storage volume. To do this, the installer:

- Wipes all partitions on the selected target storage volume
- Creates partitions as needed (normally 8 partitions are created)

Useful information about the installation disk:
- ESXi consumes about 6GB of disk space in overhead. The rest is for VM use
- partition 4 is the boot partition and is located at the front of the disk (behind the Master Boot Record and partition table)
- partitions 2 and 4, 5, 6 & 8 are for ESXi use and occupy the front of the disk
- partition 7 is a vmkcore partition (partition code 0xfc) and is a ESXi partition used to hold crash dumps
- partition 3 consumes all remaining disk space and is partitioned and formatted as a VMware File System (VMFS)

**Note**: ESXi 5.0 can now install on > 2TB volumes.

# Installation Completed

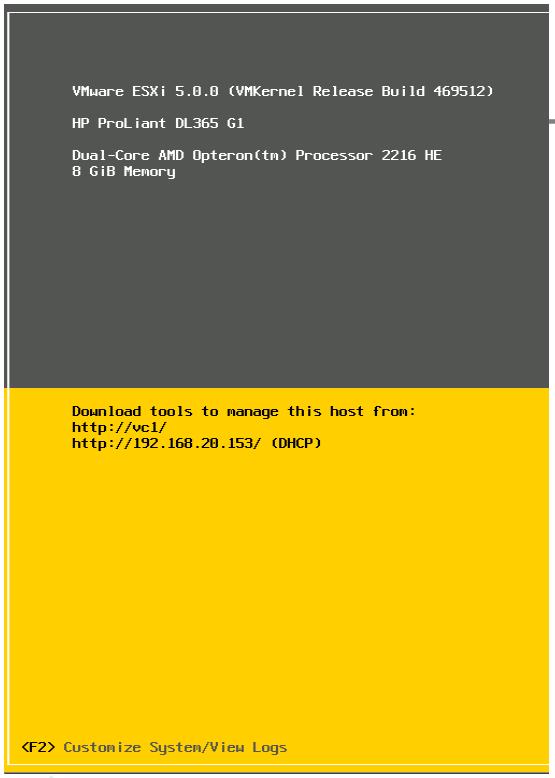



- Once your installation has completed, hit **Enter** to reboot to ESXi




## Notes

It only takes about 3-5 minutes to install ESXi 5.0 onto your PC server. The install proceeds non-interactively. A status indicator updates a percent completed horizontal bar.




# ESXi 5.0

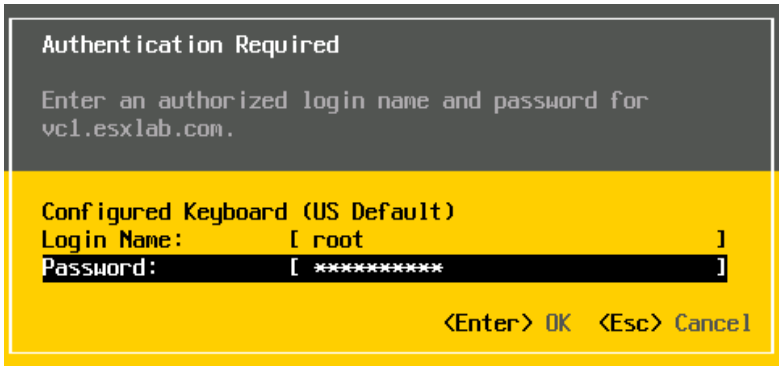
- ESXi is a small foot-print, bare metal hypervisor
  - Default – FQDN and IP properties acquired via DHCP
  - Use **F2** at the boot screen to set up your ESXi 5.0 host
  - Use **F12** to shutdown or reboot your host
  - Simple BIOS like interface




## Notes

ESXi has a simple, BIOS-like interface that makes it very easy to configure. To configure your ESX host, simply hit F2 at the greeter screen.

# Log In for the First Time




- The administrator account for ESXi is **root**
  - The root password is set during install
  - Do not lose the root password – there is no way to gracefully recover it!




## Notes

The ESXi administrator account is root (the traditional Linux administrator account). When you install ESXi, the system defaults to:

- The root password is set during installation
- IP properties set via DHCP
- No command line access (either locally or remotely)

In the next few slides, we will discuss how to change these values.

# ESXi Configuration Menu


- Configure ESXi through a simple text menu
  - Current menu item settings displayed on the right side of the screen
  - Hit **Enter** to activate a menu function

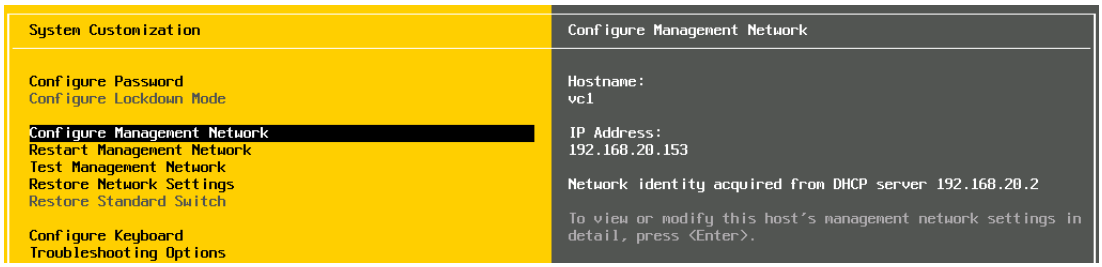



## Notes

The ESXi configuration menu is a simple text interface where you complete your server's customizations.

Use the up/down arrows to move to a function. When a function is highlighted, its properties and the command keys used to modify that function are displayed on the right.

# Default Management IP Settings




- By default your ESXi host uses DHCP
  - Host name, domain name and the IP address is assigned using an IP address out of your lease pool
    - Example above reclaims a desktop PC lease!
  - ESXi needs static IP properties




## Notes

You must set the IP properties of your ESXi host before you can manage it. Select **Configure Management Network** to set the:

- Fully Qualified Domain Name (FQDN)
- IP address
- Netmask
- Default Gateway

and other properties.

You can set these values statically or dynamically using DHCP. DHCP servers can send static properties to a host. To do this, configure your DHCP server with the MAC address of your ESXi host management NIC and then set the static properties to server whenever that NIC broadcasts for a DHCP lease.

Be sure to **Restart Management Network** after all changes to ensure your updates take effect.

# Configure Management Network


- The Configure Management Network sub-menu let's you set key network properties
  - Management NIC
  - IP V4 and IP V6 properties
  - DNS settings
  - DNS search domain list

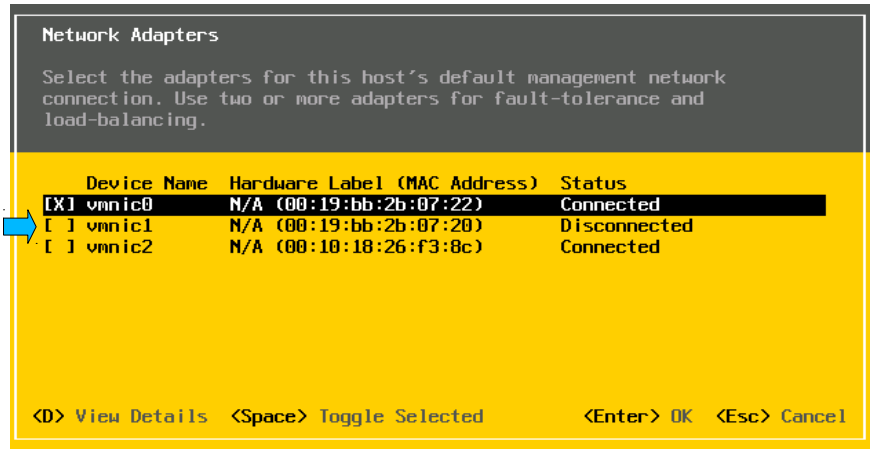



## Notes

It is a best practice to use static network settings for your ESXi host. To complete this task, you must:

1. Select the correct NIC for management networking
2. Set a static IP address and Netmask and Default Gateway values
3. Identify your local DNS server(s) and the default DNS search domains

# Select Management NIC(s)




- Physical NICs are used to carry mgt. traffic
  - Select **Network Adapters** to view/change NICs
  - Avoid disconnected NICs
    - Means they have no link to the network switch




## Notes

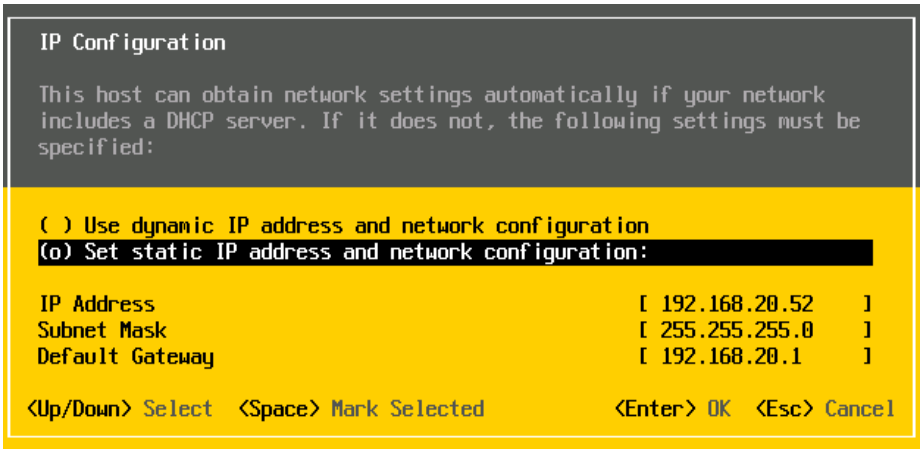
You manage your ESXi host through your network. To communicate with your ESXi host (using either the vSphere Client directly or vCenter indirectly), you must have network connectivity to it.

Since modern PC servers may have many NICs and these NICs may be connected into different physical and/or virtual LAN segments, you may have to select the correct physical NIC (rather than the default NIC) before you can manage your machine.

**NIC Teams**
The Network Adapters screen lets you review and select the NIC or NICs you wish to use to carry network traffic. If you select more than one physical NIC, you automatically create a NIC team. NIC teams afford better speed and redundancy.

**Tip**
It can be difficult (or impossible) to tell which RJ45 jack is associated with which MAC address. A simple way of selecting the correct physical NIC(s) is to unplug all NICs from their switch except for the NICs you wish to use for management. Then use the Status column (Connected means the NIC has a link to the switch) to determine which NICs you should for management.

# IP Configuration




- Best Practice - use Static IP properties
  - No chance your server could lose its IP lease and therefore it's IP address
  - Static IPs required for vCenter Management



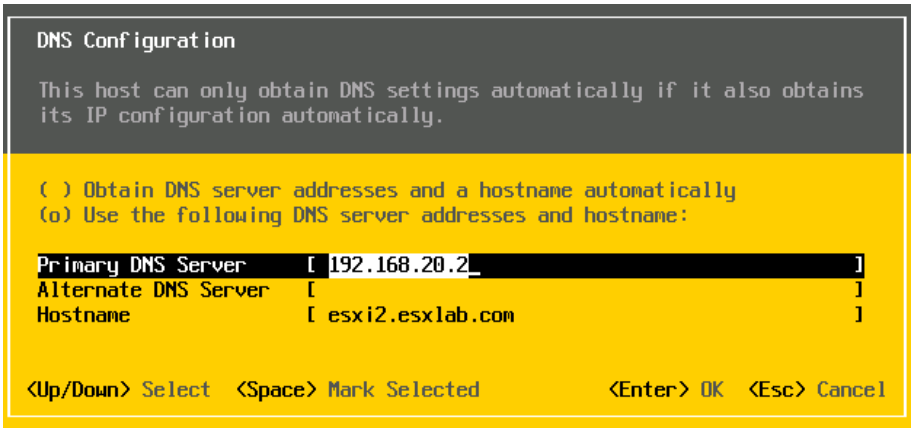

## Notes

Complete this form to set your ESXi host management NIC IP properties.

vCenter cannot manage an ESXi host whose IP address changes. For this reason it is best to give all of your ESXi, ESXi hosts fixed IP properties.

You must select **Set static IP addresses...** and complete all three fields to complete your static IP address properties assignment.

# DNS Configuration




- You must set DNS and FQDN properties
  - Enter the IP of your DNS server(s)
  - You MUST enter the FQDN of your ESXi host




## Notes

ESXi and vCenter require DNS services to function properly. So it is critical that you have DNS name servers set up and accessible from your local LAN segment.

It is a best practice to have both primary and secondary DNS servers available... but ESXi will function with just primary DNS.

You must set a fully qualified domain name for your ESXi host. The ESXi FQDN must be resolvable forward (host name → IP address) and backward (IP address → FQDN).

# Custom DNS Suffixes


- DNS suffixes help resolve host names
  - DNS look ups that contain only a host name append domain suffixes from this list, before a DNS look up is attempted
    - Use spaces, commas to separate multiple domains




## Notes

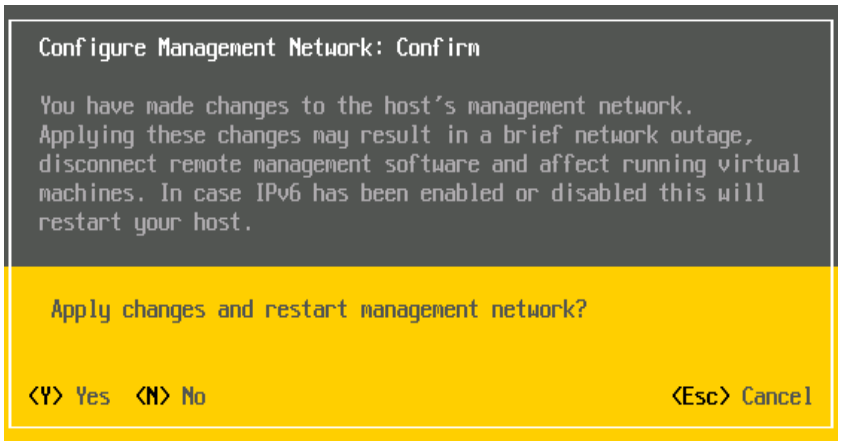
DNS Suffixes are used to enable DNS to look up the IP address of a host specified only by it's host name (and not qualified with a domain name). An example might be a look up request for a host called esxi5.

DNS needs a full domain name. Custom Suffixes will append domain names from the list set on this screen to simple host names and then perform a DNS query. This continues until either:

- a matching FQDN is found and it's IP address is returned
- no matching FQDN is found and all suffix Domain names have been tried

It is a good practice to add at last one domain name to this list!

# Apply Network Changes




- Network changes are applied en mass
  - NIC, IP and DNS changes are activated by restarting Management Network services

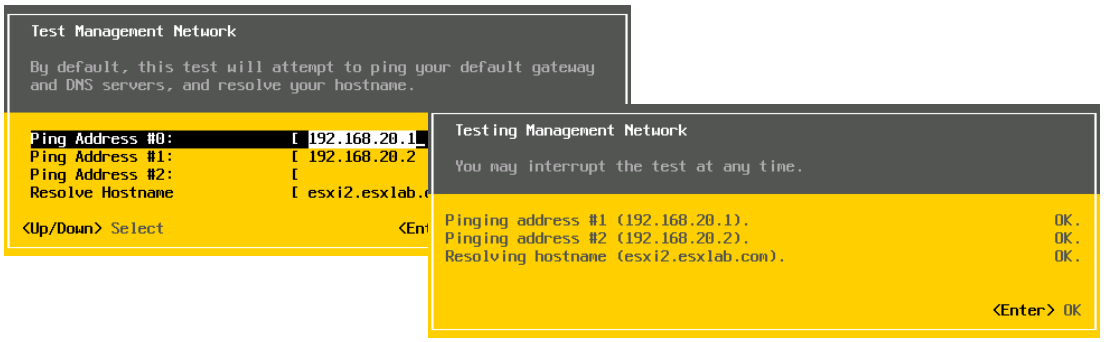



## Notes

All network changes are applied at one time when you leave the Configure Management Network sub-menu. First the new settings are applied to the appropriate configuration files and then the ESXi hosts' management network is brought down and back up again. For this reason it is best to be at the physical server's console when updating management networking properties.

You should be brought back to the System Customization menu. Your network changes should be visible.

# Test Management Network




- Basic connectivity test with Ping, DNS
  - Pings gateway, DNS server
  - Tries to resolve the server's FQDN
- Each test reports OK or Fail
  - Do not proceed until all tests pass!
  - Verify your DNS server is ping-able




**Notes**

# Local/Remote Tech Support


- Tech Support mode enables command line access to your ESXi host
  - **ESXi Shell** – Command line access from the physical server console
  - **SSH** – Secure Shell access to your server
  - Default is Disabled for both services
    - May need to turn on for VMware/partner access




## Notes

Tech Support Mode enables functions used by support providers who are comfortable working on the ESXi command line. By default, all local and remote command line access to your ESXi host is disabled – so you can only access your ESXi host through:

- the vSphere client pointed directly at your ESXi host
- vCenter if vCenter has management control over your ESXi host
- The VMware Management Assistant service (VMA), if installed

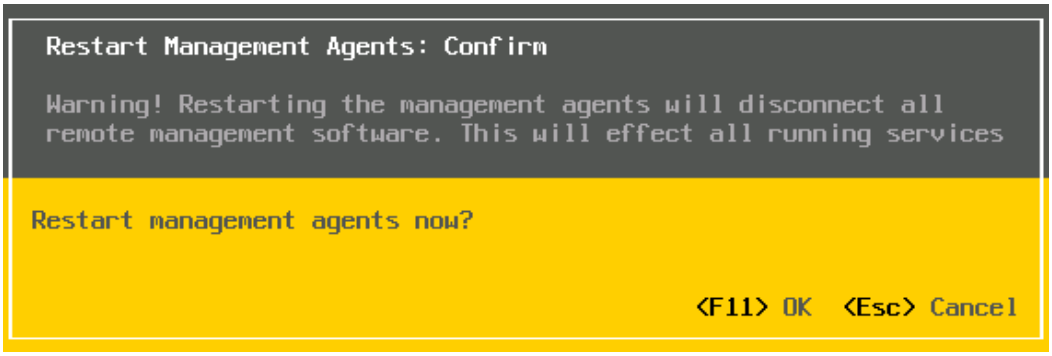
Enabling Local Tech Support allows physical console command line access. Support personnel who have access to the physical console (directly or via remote console services such as Dell DRAC, HP ILO or IBM RSA) would be able to log in to your server.

Enabling Remote Tech Support enables the Secure Shell Daemon (sshd) and supports network based administrator access to your box without the need for remote console services.

**Warning**
Enabling Remote tech support enables direct root access to your ESXi host through a TCP/IP connection. This is a potential security threat. Turn on this feature only if needed. If this feature is turned on, set a strong root password.

Never expose your machine to an untrusted network like the Internet if Remote Tech Support is turned on!

# Restart Management Agents




- ESXi uses agents (services) to communicate with vCenter and the vSphere client
  - If agents fail, your server is unmanageable
  - Use this feature to reset management agents
  - Does not interfere with running VMs



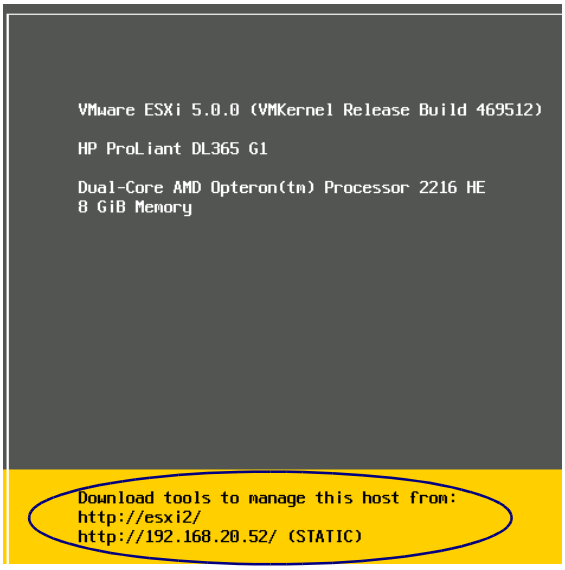

## Notes

It may happen that the management agents (services) on your ESXi host become unstable or crash. If this occurs, your ESXi host will not respond to vCenter or the vSphere client. In vCenter your host will grey out and report as disconnected.

You could reboot the ESXi host but that would bring down all running VMs. A more acceptable option is to simply restart the management agents on your ESXi host.

This function can be done at any time. Any connected vSphere Client sessions will be closed. Once this function completes, your host should become active in vCenter and should accept direct vSphere Client login requests.

# ESXi Ready for Service




- ESXi server is ready for use
  - Additional hot keys are active
    - Alt-F1 – command line access to your machine
    - Alt-F2 – this screen
    - Alt-F12 – VMkernel log records
  - Use the vSphere Client to manage ESXi



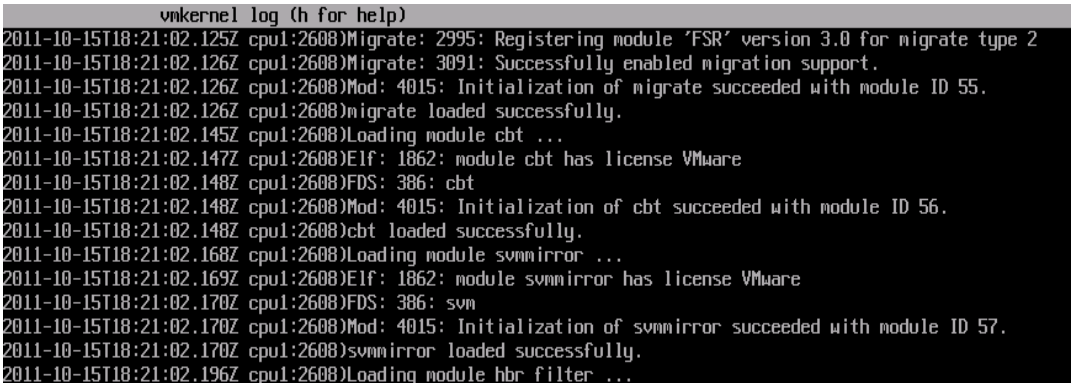

## Notes

Once ESXi has rebooted, it is managed through the web or via VMware's vSphere Client. You can download the vSphere Client from www.vmware.com/download.

There are additional hot keys active on the ESXi console:

Alt-F1 – first command line log in screen
Alt-F2 – the ESXi greeter screen (screen shot above)
Alt-F3 to Alt-F10 – no function
Alt-F11 – Grey scale status screen/greeter screen with no F-key prompts
Alt-F12 – VMkernel log dump

# Alt-F12 VMkernel Log Entries




- Hit Alt-F12 to view the VMkernel log file
  - Displays the most recent VMkernel log contents
    - Look here to see detailed error messages
  - File - /scratch/log/vmkernel.log on the command line




## Notes

The VMkernel records detailed log entries into a file called /var/log/messages. You can view this file by logging into the Local/Remote tech support prompts (as root) and issuing the command:

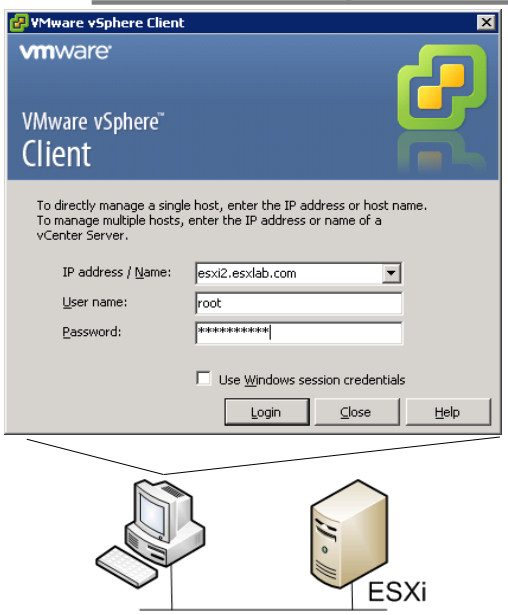
```
# less /var/log/messages
```

You can see the most recent entries by hitting the Alt-F12 keys on your machine's console. This display shows one screen full of the most current additions to the VMkernel log file. You should check this file if you are troubleshooting problems and need more information than is available in the vSphere client.

Hit Alt-F2 to go back to the ESXi greeter screen when done.

**Note**
All command line commands entered using Local or Remote tech support are logged to /var/log messages. In this way, it is possible to reproduce the activities of prior command line sessions.

# Login with vSphere Client




- Launch vSphere Client
  - Use ESXi IP or FQDN
    - ESXi User name (root)
    - ESXi Password
  - Chatty, but low band-width application
    - Runs well over corporate LAN, WAN
    - Can run over Internet
    - Selectable session time-out values




## Notes

You manage your ESXi host directly with the vSphere Client. This is a separate download and install available from VMware (http://www.vmware.com/download). Alternatively, you can just point your web browser over to your ESXi host and follow the vSphere Client download link found theter.

All VMware client to server connections are encrypted using strong encryption. The encrypted link is set up before any data is exchanged between the client and the back end server.

# Security Warning


- All VMware client/server connections use 256-bit AES symmetric key encryption
  - ESXi uses self-signed Digital Certificates
    - No Certificate Granting Authority to verify authenticity
- Since host is local, ignore warning
  - Check *Install this certificate...*




## Notes

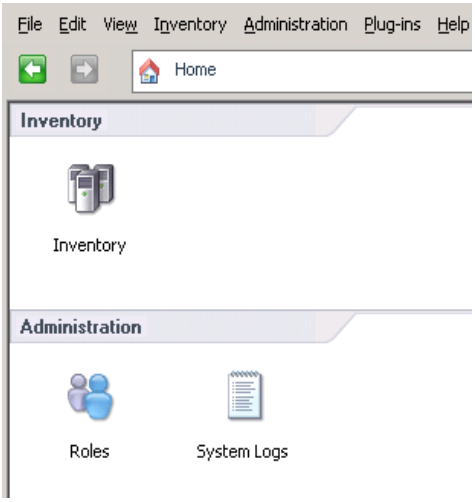
ESXi uses self-signed digital certificates to support end-to-end encryption. All communications between VMware client and VMware server software is encrypted using strong encryption.

Since the digital certificate cannot be independently verified by a 3rd party Certificate Granting Authority, a warning is issued. It is (usually) safe to permanently disregard this warning.

It is possible to purchase an SSL certificate from a Certificate Authority (CA) and then install that certificate onto your ESXi host. This would eliminate the warning messages because a trusted certificate can be used to verify that the host is who it says it is.

Normally trusted certificates are used on Internet facing hosts to ensure the integrity of web requests (e.g.: for secure banking/payment systems, etc.). Since your ESXi hosts won't be directly on the Internet, there is no need (and no benefit) to purchasing a trusted certificate for your machine.

# vSphere Client > ESXi Host

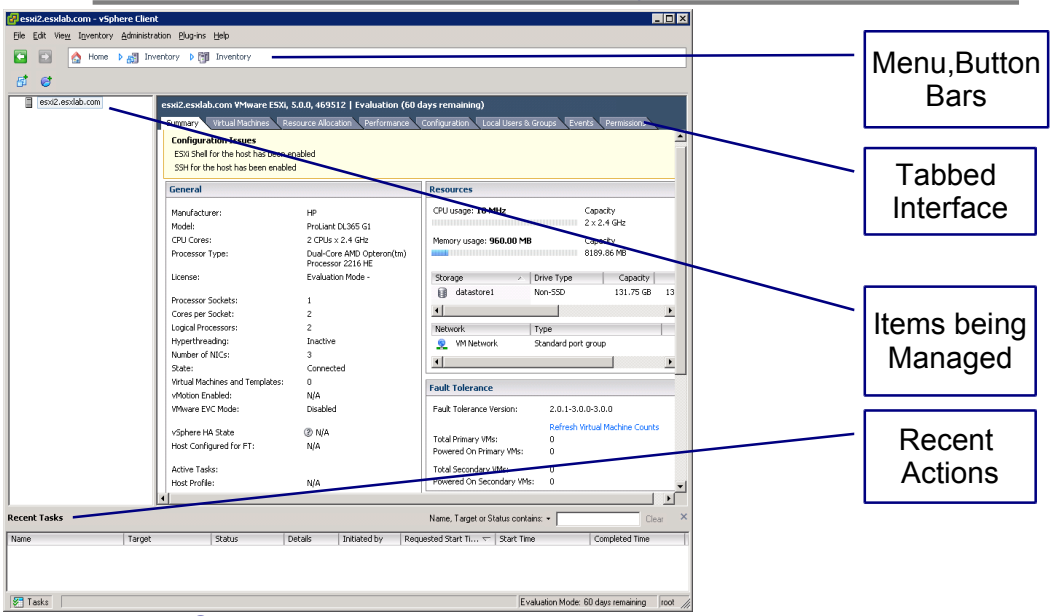



- vSphere Client presents a task launch page
  - **Inventory** – work with your ESXi host
  - **Roles** – define user categories
  - **System Logs** – review, save ESXi log files




**Notes**

# vSphere Client



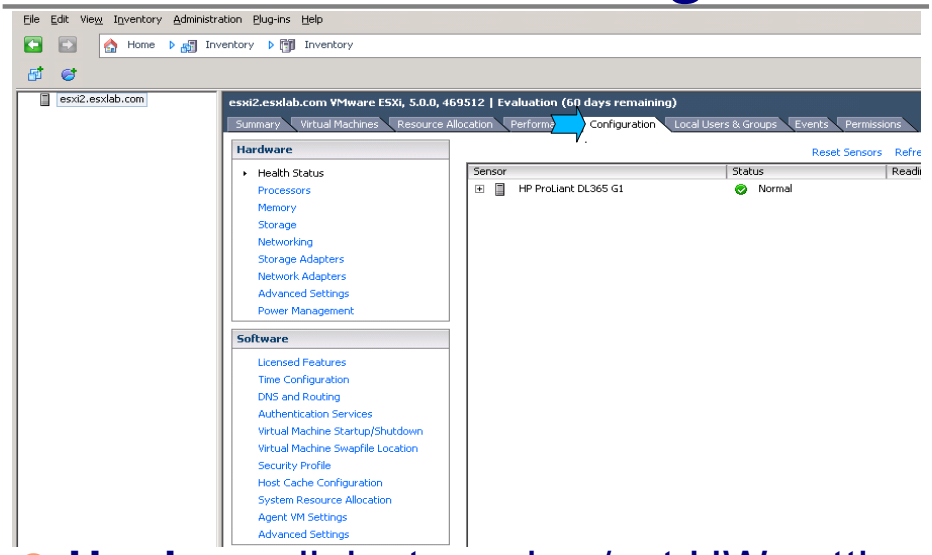

- 4 Sections: Menus, Inventory, Tabs, Recent Tasks





## Notes

# ESXi > Configuration




- **Hardware** links to review/set HW settings
- **Software** links to review/customize ESXi

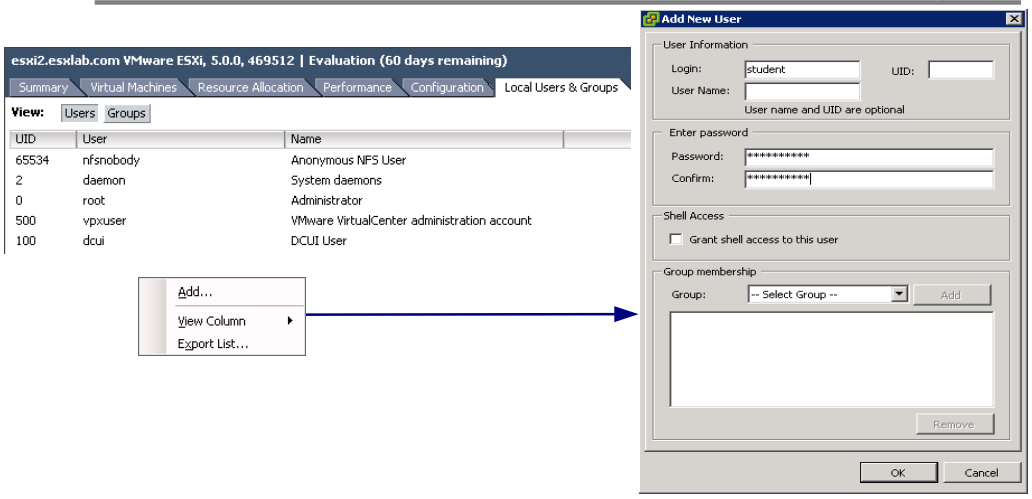



## Notes

Most ESXi hardware and software configuration is done using the vSphere Client.

Use the **Configuration** tab and the appropriate boxes (Hardware, Software) to review and/or configure your server.

# Local ESXi Users & Groups




- *Users & Groups* Tab – Define ESXi users
  - Right click on background, Select *Add...*
  - *Set user login, password and group (optional)*



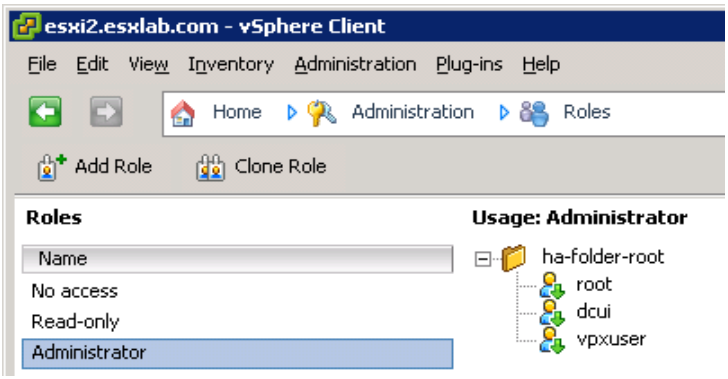

## Notes

You can create local ESXi user accounts with passwords to allow for local authentication (for both the vSphere client and Local/Remote Troubleshooting – if enabled). To do this click on the **Users & Groups** tab and then right-click the back ground and select Add.... You can make new groups by clicking the **Groups** button and then right-clicking the background.

**Best Practice**
You would create local accounts only if you do not have an Active Directory service available. Otherwise, it is a best practice to join an AD domain and use domain accounts.

**Tip**
To command line log into ESXi over the network (from Windows, ESXi Remote Troubleshooting Mode must be enabled) download the **putty** Secure Shell terminal emulator at http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html


# ESXi Host Roles



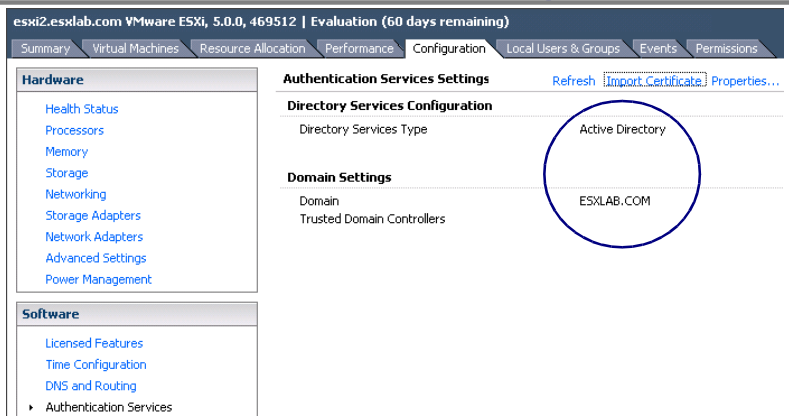

- Roles determine privileges by user, group
  - Default role: **No access** – no rights on ESXi host
  - **Read-only**: look but cannot modify
  - **Administrator**: full control of local ESXi host
    - root, dcui (local configuration) and vpxuser (for vCenter) hold the Administrator role





**Notes**

# Joining a Domain




- ESXi can join an Active Directory domain
  - Navigation: Software > Authentication Services > Properties...
  - Specify domain, then domain user/password with rights to add hosts to a domain

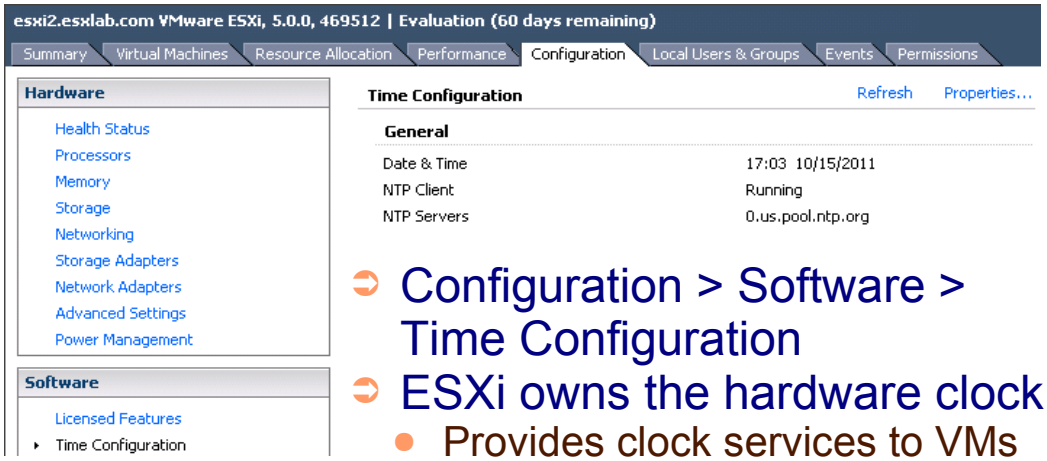



## Notes

ESXi 5.0 can now join an Active Directory domain. AD authentication allows you to set up access rules for ESXi login without having to create local user accounts on ESXi.

**FYI**
Joining an AD domain is the first step to allowing AD defined users to access ESXi directly. The second step is to select inventory items (your ESXi host, folders, VMs, Resource Pools) and assign these users rights on these items. Without specific permission assignments, AD based users will not be able to interact with ESXi.

# Review/Set Time Configuration




- Configuration > Software > Time Configuration
- ESXi owns the hardware clock
  - Provides clock services to VMs
  - Use Network Time Protocol to ensure a very accurate clock
    - Use Properties... to enable/configure NTP




## Notes

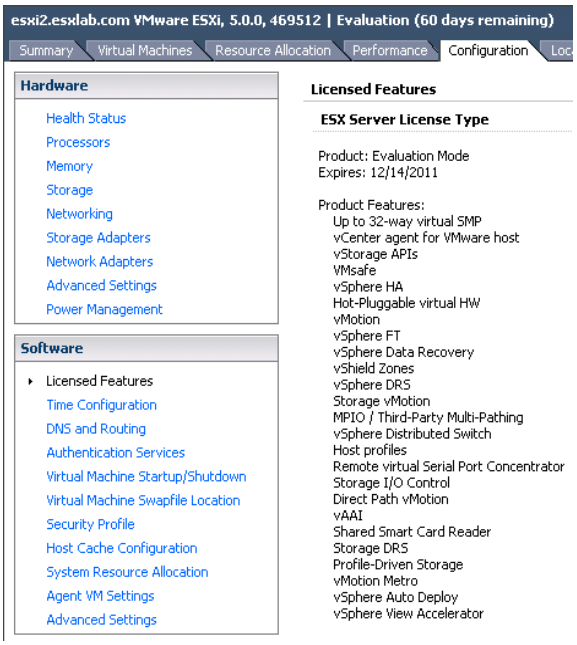
ESXi uses Network Time Protocol to ensure that it's clock remains accurate. This is important because the ESXi host provides clock services to all VMs it runs. So, any clock drift in the ESXi host will result in clock drift in VMs. If VM clocks drift by more than 5 minutes they may not be able to join or remain members of Active Directory domains.

Click the **Properties...** link to review and configure NTP.

**Best Practice**
Always set your server's BIOS clock to UTC and ensure you select Server Clock is UTC when you install ESXi. That way, VMs will get a UTC clock and can then set their local time zone to any region they like.

If you set the hardware clock to your local time, then VMs must all operate in your local time zone only (because they cannot calculate time zone offsets from any time zone other than UTC).

# Licensing ESXi 5.0




- License options
  - Evaluation Mode
    - 60-day evaluation
      - Cannot be extended
    - All features available
  - Serial Number
    - 25 character code
    - Get from VMware
    - Enables entitled licensed features
    - Click **Edit...** to add an ESXi license
  - License entitlements can also be obtained from vCenter

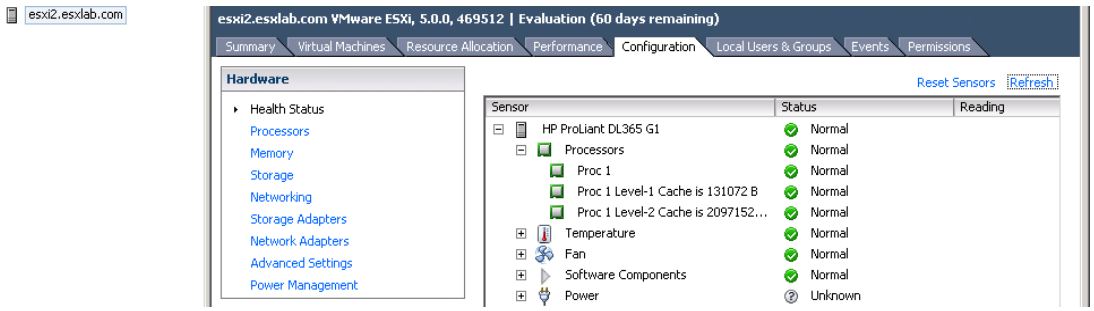



## Notes

ESXi now ships with an unrestricted use 60-day evaluation license. This eliminates the need to contact VMware for temporary evaluation licenses.

ESXi can be activated using a stand alone host license. A host license is issued on a host by host basis and unlocks access to feature entitlements purchased for that host. Alternatively, ESXi can draw a license entitlement for needed features from vCenter.

# System Health Status




- Click **Configuration** > **Health Status** to review host hardware health
  - Uses CIM to poll hardware
  - Reports back issues found
  - Issues propagate up to the host




## Notes

The vSphere Client can report on most aspects of your system's hardware health including:

- CPU sockets, cores and cache size
- Power supply, motherboard, CPU and add-on card temperatures
- Fan location, health and speed
- Hardware firmware and driver health including chipset, NIC, storage controller, BIOS functionality
- Power supply count and health (connected, disconnected, missing, etc.) and
- System boards.

Use this view to get a quick assessment of your server's physical health.

# Physical CPU Properties


- Click Configuration > Processors to review host CPU properties. Verify:
  - CPU socket, core and Hyperthreading status matches expectations
  - Click **Properties...** to enable Hyperthreading




## Notes

ESXi reports on the properties of the CPUs found in your server, including:

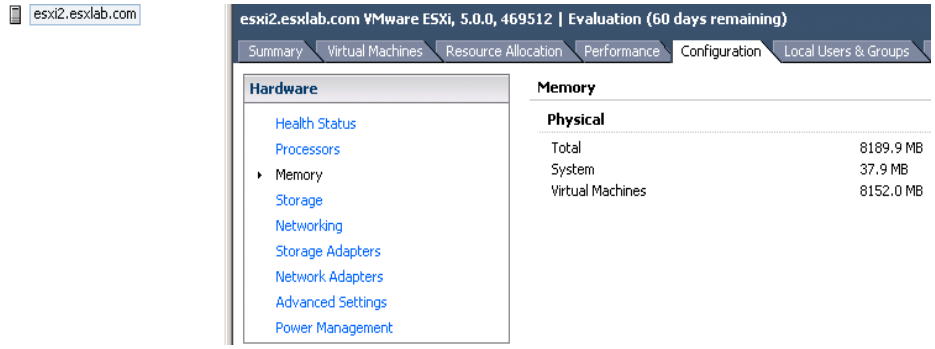
- The make/model of the machine
- Make/model and speed of the CPUs
- Number of populated sockets
- Number of cores in the CPU
- Number of Logical Processors (sockets * cores * HT logical processors)
- Presence/Absence of Hyperthreading (Intel CPUs only)
- Presence/Absence of power management capabilities (newer CPUs only)

If you have Intel CPUs and Hyperthreading is reporting N/A you should check to see if Hyperthreading is active. To do this, click:

Properties > Hyperthreading > Enabled

This will turn on Hyperthreading support even if the machine's BIOS is set to disable it. You will need to reboot ESXi for this change to take effect.

# Physical Memory Properties




- Click Configuration > Memory to review host RAM configuration. Note:
  - System (VMkernel) RAM is reserved
  - All remaining RAM available for VM use




## Notes

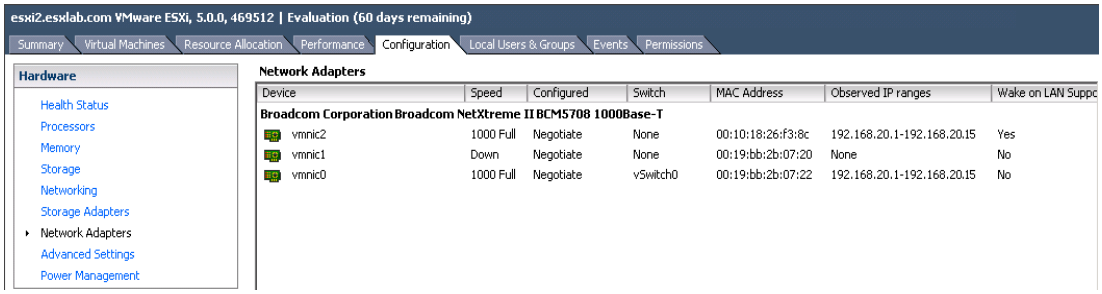
ESXi uses memory in 2 ways:

1. For the VMkernel hypervisor (approximately 400MB), and
2. For virtual machines (all remaining RAM).

ESXi needs a minimum of 2GB of RAM or it will refuse to run. Adding more RAM means more room for VMs to run which should result in good performance as your VM population and RAM requirements grow.

ESXi is very frugal and hands out memory to VMs only when needed and only for as long as needed. We will explore ESXi memory scavenging techniques later in this class.

# Network Adapters




- All recognized NICs displayed in the Network Adapters view
  - Speed, Assigned vSwitch, physical MAC address and Observed IP ranges reported
  - Observed IP range - helps you determine which sub-net a physical NIC can see – and consequently what traffic is should carry




## Notes

**Observed IP Ranges**
This value displays the IP address range observed by ESXi as frames flow through each physical NIC. Here's what it's used for.

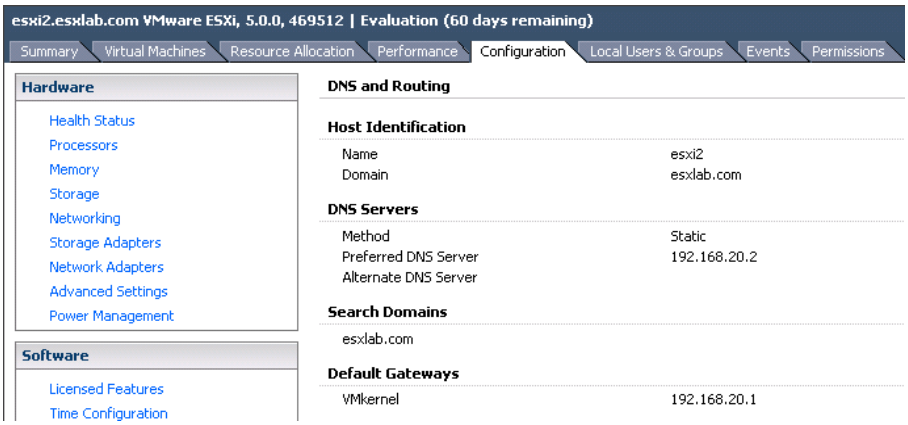
In most corporate networks, different physical LAN segments are used to isolate different types of traffic such as Production traffic, storage traffic, management traffic, back up traffic, etc. It is a common practice to use different sub-net address blocks for each physical segment.

For example, your company may subnet its network traffic as follows:

10.1.0.0/16 – Production traffic including servers
10.2.0.0/16 – Desktop PCs and printers
172.16.0.0/16 – Management LAN segment for direct PC server management
192.168.50.0/24 – Back Up LAN
192.168.100.0/24 – IP Storage LAN (for iSCSI servers)

In the above scheme, if a physical NIC reported Observed IPs in the 10.1/16 range, you would know it was physically connected to the management LAN. If another physical NIC reported Observed IPs in the 192.168.100/24 range, then it should be used to carry back up traffic.

# Network Properties




- Click Configuration > DNS and Routing to review ESXi management settings:
  - Verify Host, Fully Qualified Domain Name, IP address, DNS IP and Gateway
    - Click Properties... to make any changes



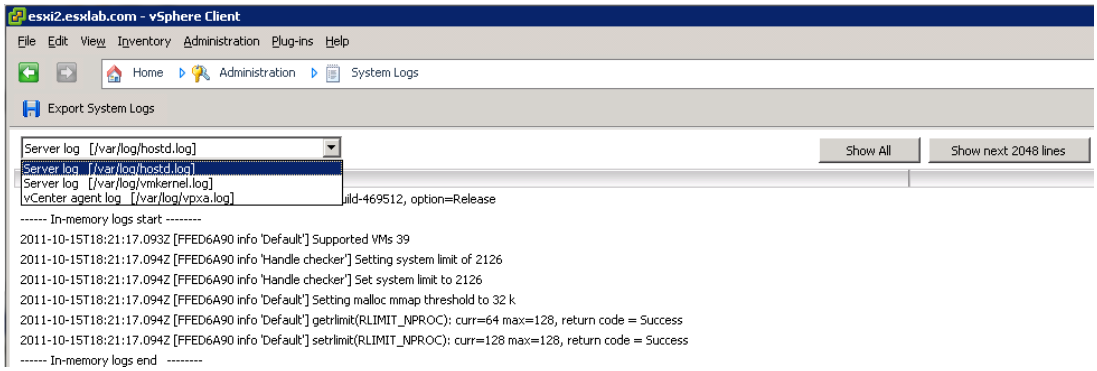

## Notes

It is important that your Service Console OS network settings are correct. After installation, it is a good idea to review these settings and fix any errors you find.

Click Properties... to edit network settings for the Service Console. You will need to reboot your ESXi host before these changes take effect.

System Logs

# ESXi System Logs




- Review, save ESXi system logs
  - Home > Administration > System Logs
  - hostd.log: host management service log
    - Licensing, cluster mgt., vCenter mgt., etc.
  - Use Export System Logs to save log files locally as text files





## Notes

# Sizing ESXi CPU, Memory

- Physical CPUs service Virtual CPUs
  - About 2-5% CPU virtualization overhead
    - Plan for between 2-8 vCPUs per physical CPU core
  - Maximize CPU cores, speed & cache size
    - Don't expect Intel Hyperthreading to help
    - Physical core restrictions removed vSphere 5
- Memory
  - Must have 2GB RAM to install/boot ESXi
    - Once booted, the VMkernel uses 40+MB of RAM
    - All remaining RAM free for VM use
  - VMs given RAM as needed, not declared
    - 1.2-1.4x memory over commit is reasonable




**Notes**

# Sizing ESXi Storage, NICs

- Storage Controllers
  - ESXi is inherently multipath aware
    - Vendor supplied multipath drivers now supported
    - Better I/O performance to LUNs
    - Improved reliability through path redundancy
- NICs
  - Virtual Switches use physical NICs
    - Physical NIC uplinks vSwitch to physical LAN segments
  - Virtual NIC traffic consumes CPU cycles
    - Faster ESXi CPUs give faster virtual network speed
    - Benchmark network performance before deploying network heavy production workloads




**Notes**

# Lab 2 – Install ESXi 5.0

- In this lab we will perform an install of ESXi 5.0 onto a physical PC server
  - Install onto dedicated HP DL360/5 servers
    - Use RDP to access our kit central server
    - From there, use Remote ILO console to power on and install ESXi
- Our server pod
  - Is located in a remote Class-A data center
  - Accessed by Microsoft Terminal Services
  - Has one server/student
  - Uses real PC server hardware
    - Not simulation, emulation or PCs running ESXi in a VM




**Notes**

# Review & Questions

- VMware ESXi 5.0
  - Enterprise class server virtualization
  - Installs on bare hardware
  - ESXi is managed through vSphere Client
    - Simple Menu/Item/Tab interface
  - Needs Windows PC with MS .Net framework
  - For best results:
    - Size ESXi to your expected VM needs
    - Plan, perform ESXi installs with care
    - Expect growth in VM population






**Notes**

## Notes

# Lab 2 – Install ESXi

## *ESXi Server Configuration*

In this lab, you will install VMware ESXi 5.0 onto a dedicated server. If you are using ESXLab.com remote access servers, your machine is an HP/Compaq DL365 enterprise class server and is fully supported by VMware. Your server has a minimum of the following hardware (some may have more)

- 1 AMD Quad/Dual Core Opteron 64-bit CPU or 1 Intel Dual Core 64-bit CPU
- 5-8 GB RAM
- HP Smart Array Controller with 36-300+GB of local disk
- ILO – Integrated Lights Out Remote Management Card
- 3 x 1gb NICs

## *Objectives:*

In this lab, you will:

- Install ESXi 5.0 onto a physical server using remote console services
- Set fixed IP address properties for management
- Install the vSphere Client on our remote desktop
- Access your ESXi host via the vSphere Client application
- Review your servers hardware and default configuration
- Create a non-privileged account for local access
- Connect to Active Directory and enable an AD account
- Configure your server to synchronize its time with an NTP time server
- Review and adjust power management policies

## *ESXi Installation – Needed Information*

Please refer to the information below when installing and configuring your ESXi server:

| | |
|---|---|
| ESXi Service Console IP Address | **192.168.20.50 + #** |
| ESXi Service Console Host Name (FQDN) | **esxi#.esxlab.com** |
| Netmask | **255.255.255.0** |
| Gateway | **192.168.20.1** |
| DNS 1 | **192.168.20.2** |
| DNS 2 | **- leave blank -** |
| Root Password | **esxlab.com** |
| FQDN of NTP time source | **0.us.pool.ntp.org** ('zero'.us.pool.ntp.org) |

# Part 1 - Install ESXi

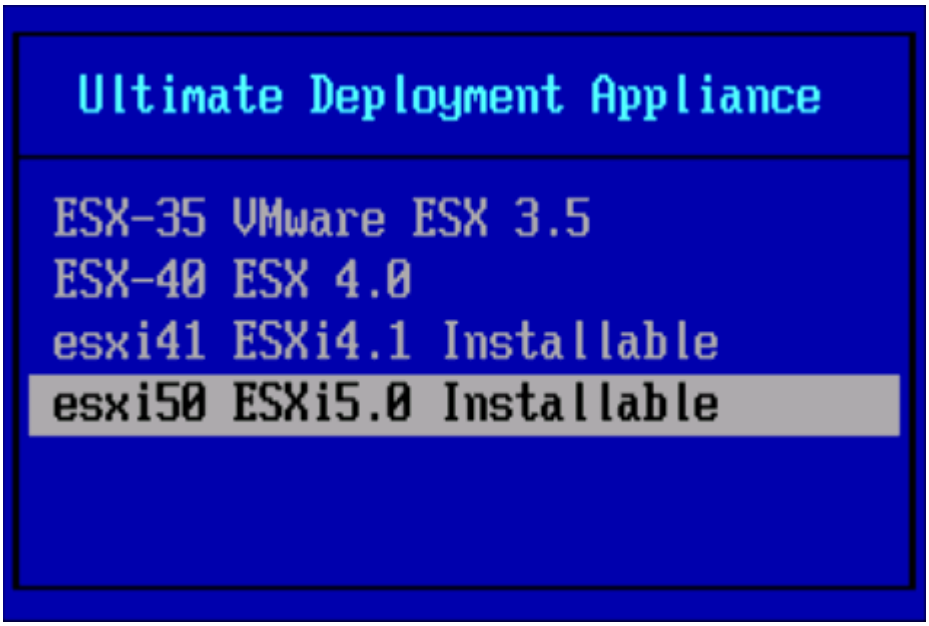
**Boot ESXi using ESXLab.com Remote Access Servers**
Your server has been set with the following boot device order:

- Local Hard Disk
- Ethernet (PXE)

Because our servers are off site, we must install ESXi without using the CD/DVD reader. We will use PXE (**P**re-boot e**X**ecution **E**nvironment, pronounced *pixie*) network boot services.

Once you install ESXi onto your local hard disk, your machine will boot from local disk. In preparation for your class, your server's hard disk array has been wiped, destroying any MBR and partition table information on the drive. So, when your machine boots it will attempt a Hard Disk boot and fail. Next, it will attempt a PXE network boot, which will succeed.

Once your machine completes its POST, you should get a PXE network boot menu:




Please ensure that **esxi50 ESXi5.0 Installable** item is highlighted, then hit **ENTER** to network boot from ESXi 5.0 install media.

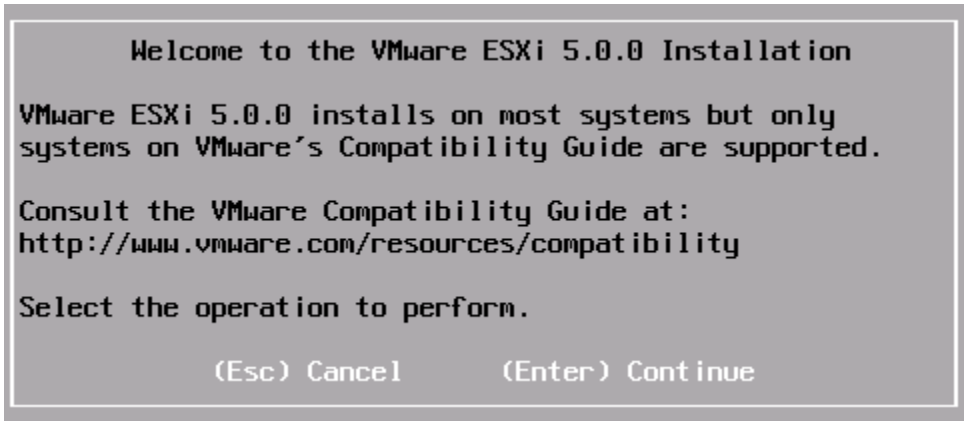
Note: If you accidentally select some other option, please:

- Switch to your main ILO session > Power Management Tab
- Click the Reset button and let the machine reboot
- Watch the machine run its power on self test and wait for the above menu to appear

**Optional** - *Boot ESXi from Other Media*
If you are using local servers (not ESXLab.com remote servers), simply power on the ESXi host and follow the instructions provided by your trainer on how to boot ESXi.

## *Welcome to the VMware ESXi 5.0 Installation*

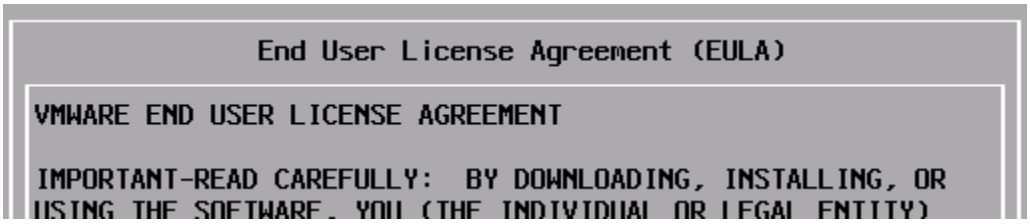
The ESXi 5.0 installer will boot and run. The machine will initialize and then launch the installer:




Please hit **ENTER** to continue.

## *End User License Agreement*

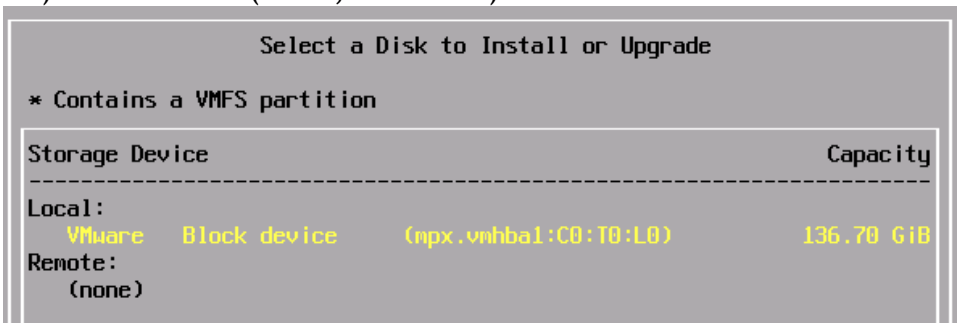
You must accept the EULA before continuing the install:




Hit **F11** to accept the EULA and continue

## *Select a Disk*

The installer then presents you with a roster of visible storage volumes, organized into **Local** (SAS RAID) and **Remote** (Fibre, iSCSI SAN) volumes.



Please hit **Enter** to give the installer permission to wipe and use the local storage volume.

**Note:** The ESXi installer uses 100% of the selected disk (and does not give you the chance to change/edit partitions on the selected volume)

## *Keyboard Layout*

ESXi 5.0 can work with international keyboards... but we will use the default US keyboard

- Please hit **Enter** to accept the **US default** keyboard layout.

**Note**: Do not change your keyboard even if you are using something else locally

## *Root Password*

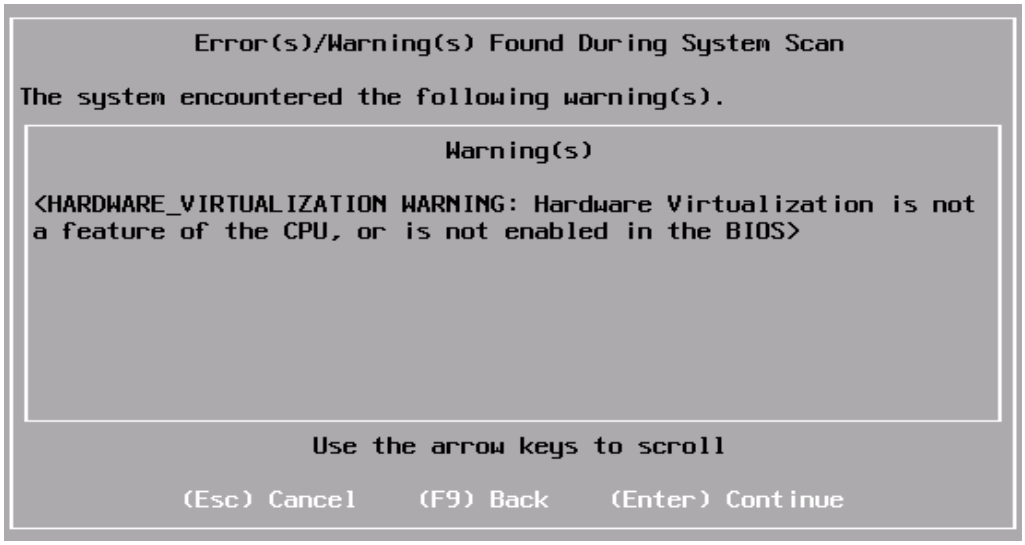
Next, you need to set the root (administrator) password:

- Type **esxlab.com** as your root password
- Arrow down
- Type **esxlab.com** again to confirm your password
- Look for the message below that says the passwords match
- Hit **Enter** to continue

**Note**: Be sure to use the suggested password above.

**Warning**: Do not deviate from the suggested password. If you use something else and you forget your password, you will have to re-install ESXi and you will lose all of your work!

**Hardware Virtualization Warning (May not Be Present on Your Machine)**
At this point, you may see the following warning:



If you don't see this warning, please skip to **Confirm Install**

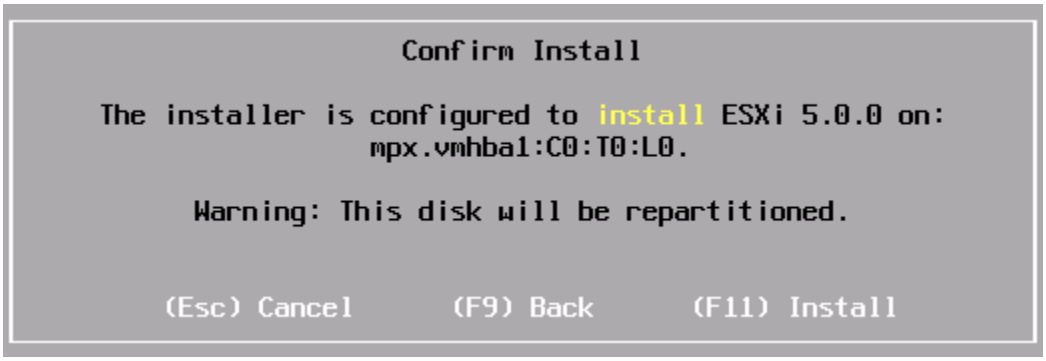
The installer is advising you that the CPU(s) in your server either lack modern hardware virtualization assist technology, or your server's BIOS has these features turned off.

**Note**: ESXI will not install/run ff the CPUs in your server are not 64-bit, or if it uses early Intel Xeon EMT/64 processor. Dual core processors that incorporate Intel VT or AMD-V virtualization assist technology will function (and produce the warning above). Quad-core processors (and higher) should just work without producing the above message.

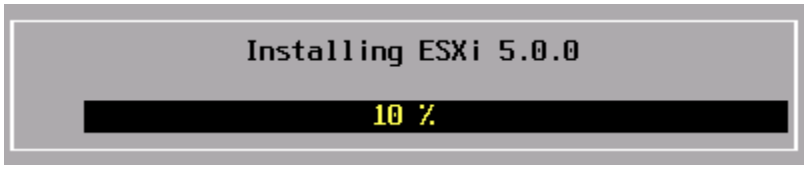
- If you see this message, just hit **Enter** to ignore the message and continue

## *Confirm Install*

ESXi will now install on your local server...



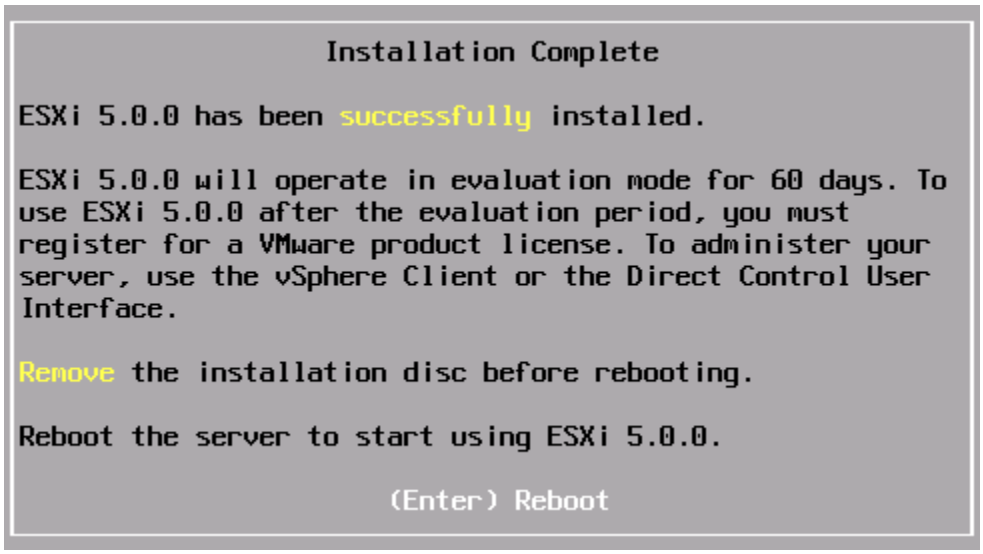

Please hit **F11** to proceed with the install. The installer downloads and installs ESXi onto your server. Progress is displayed as the install proceeds:



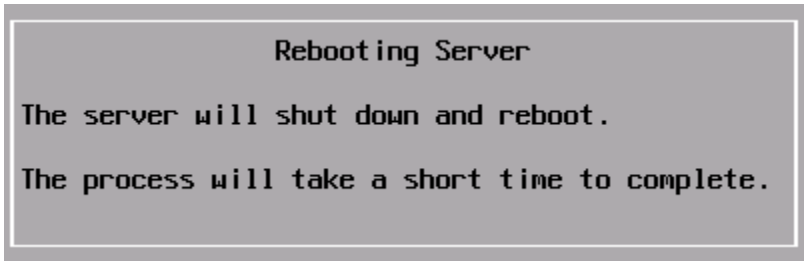

It should take no more than 3-5 minutes to install ESXi.

### *Installation Complete*

When your ESXi installation has finished you will see the following:

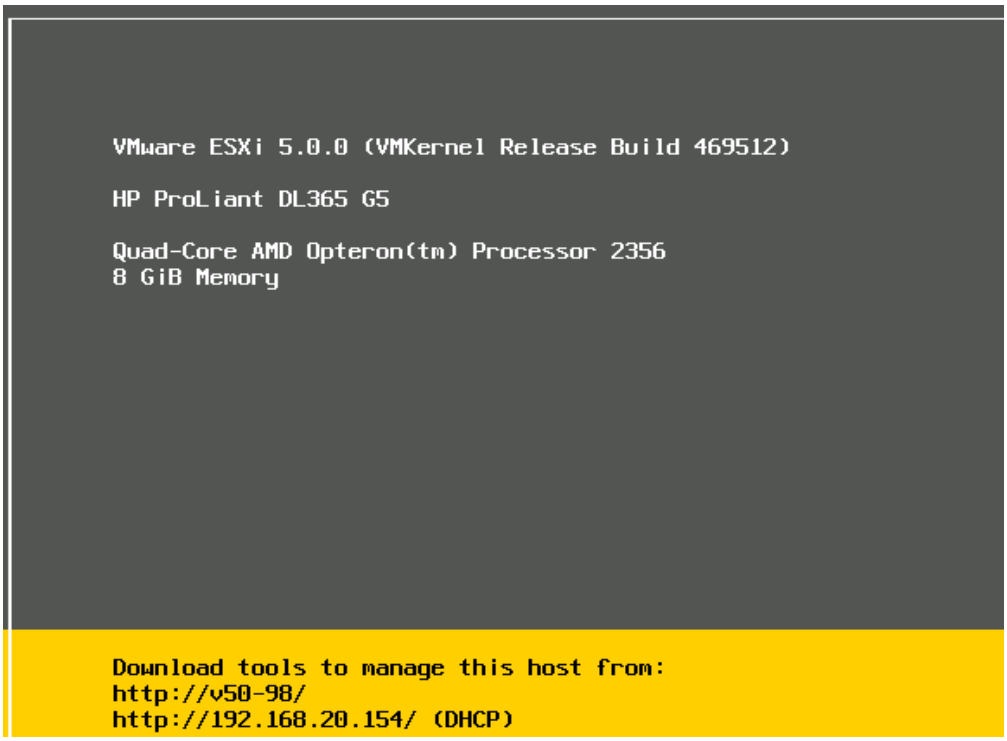



Please hit **Enter** and wait for your server to reboot...



# Part 2 – Configure ESXi

Once your server reboots, it presents you with an ESXi 5.0 greeter screen:

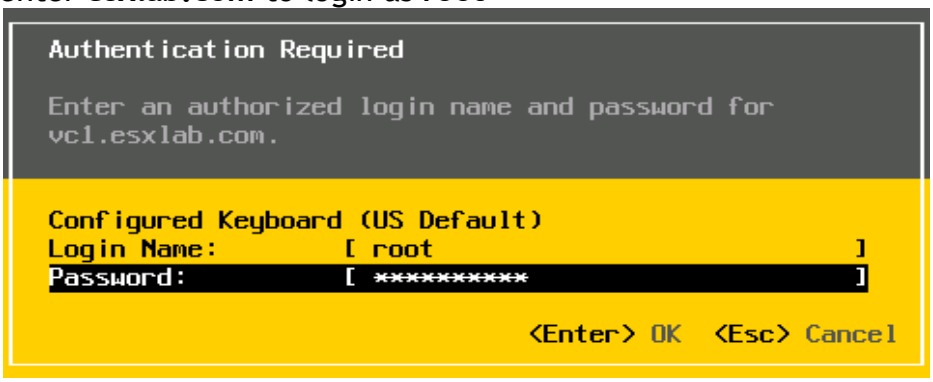



Your server acquired it's name and IP address from DHCP. Let's change that now.

## *Customize ESXi*

Let's customize your server now. Please hit **F2** to proceed (you may have to hit F2 a 2nd time if you screen has gone black). You must authenticate with the local administrator (root) ID and password

- Please hit **Enter** to accept the default Login Name (root)
- Please enter **esxlab.com** to login as **root**



## *System Customization – Configure Management Network*

Next, let's set static IP properties for your ESXi server... Please complete the following:

- Continuing where you left off (above), arrow down to *Configure Management Network* and hit **Enter**
- Highlight *Network Adapters* and hit **Enter**
- Verify that all of the NICs in your physical server are connected (note if your server has 4 NICs, its OK if the last NIC is disconnected). If any of vmnic0, vmnic1 or vmnic2 on your server are disconnected, please inform your instructor!
- Hit **ESC** to leave the *Network Adapters* screen
- **Arrow down** to *IP Configuration* and hit **Enter**
- **Arrow down** to *Set static IP address and network configuration* and hit the **Space** bar
- **Arrow down** to the IP Address field and **enter your server's IP address**. Your server's management IP address for our server pod is set according to the following formula

  **192.168.20.(50 + #)** (where **#** is your instructor assigned server #)

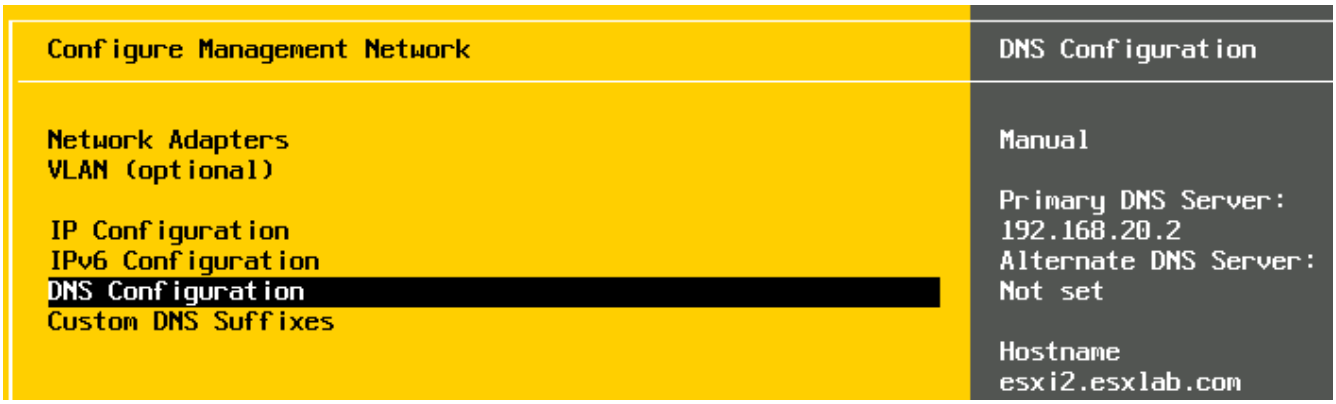
  E.g.: if you were assigned server 11, your server's IP is 192.168.20.61
- Arrow down to the *Subnet Mask* field and enter **255.255.255.0**
- Arrow down to the *Default Gateway* field and enter **192.168.20.1**
- Hit **Enter** to apply these properties

Verify your settings. Please ensure that your server uses static IP addressing following the formula and values above. Your server should look similar to the screen shot below:


Now, let's configure DNS...

- **Arrow down** to the *DNS Configuration* option and hit **Enter**
- In the *Primary DNS Server* field, enter **192.168.20.2**
- Verify that the *Alternate DNS Server* field is **blank**
- **Arrow down** to the *Hostname* field. Please enter **esxi#.esxlab.com** (where **#** is your unique server number. E.g.: If you are assigned server 5, you FQDN would be esxi5.esxlab.com)
- Hit **Enter** to apply these properties

You are now placed back at the *Configure Management Network* menu, with *DNS Configuration* highlighted. Review the *DNS Configuration* details (right side of the screen). You should see something similar to:




Please fix any/all errors before continuing.

Next, let's set/verify DNS search suffixes. These suffixes are a list of domains to try whenever the ESXi host is attempting to resolve a hostname that lacks a domain (i.e.: trying to resolve esx5 rather than esx5.esxlab.com).

- **Arrow down** to *Custom DNS Suffixes* and hit **Enter**
- Enter **esxlab.com** in the *Suffixes* field.
- Hit **Enter** to accept this value and return to the *Configure Management Network* menu.

**Note**: If this were a production environment, you could enter a space delimited list of domains that you want DNS to search when attempting to resolve a host name.

It is now time to apply your IP addressing and DNS changes...

- Please hit **ESC** to leave the *Configure Management Network* menu
- You should see a *Confirm* pop up asking you to apply these changes. Hit **Y** to apply changes

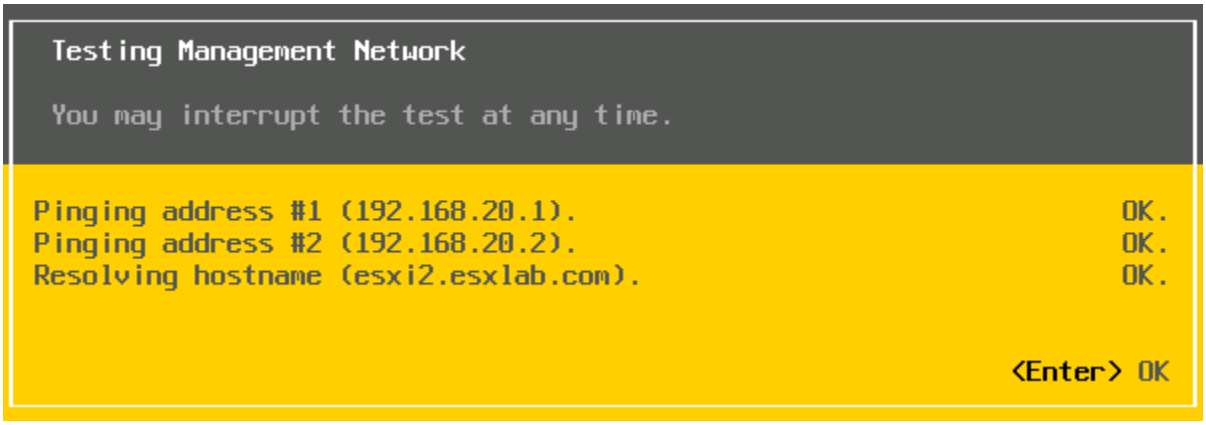
## *System Customization > Test Management Network*

Before we continue, let's test our management network settings to ensure they are correct:

- **Arrow down** to *Test Management Network* and hit **Enter**

The *Testing Management Network* pop up appears and launches ping tests of both the default gateway and the configured DNS server. It also performs a DNS look up of the Fully Qualified Domain Name (FQDN) of your ESXi host.

Hit **Enter** to run the tests. Results appear as follows




Please fix any issues reported by this test before continuing.

- Hit **Enter** to dismiss this window.

## *Enable Local, Remote Troubleshooting*

Troubleshooting Mode is command line access to your ESXi host. There are two versions:

- *ESXi Shell* – direct command line access from your machine's console
- *SSH* – Secure Shell (ssh) network command line access to your host

Normally, you would leave these disabled unless you actually needed them. We will turn on both troubleshooting options to facilitate support...

Please arrow down to *Troubleshooting Options* and hit **Enter**

- If necessary, hit **Enter** on the **Enable ESXi Shell** menu option to permit local command line access
- **Arrow down**
- If necessary, hit **Enter** on the **Enable SSH** menu option to permit secure shell access
- Hit **ESC** to leave the *Troubleshooting Options* sub-menu

Please hit **ESC** to log out of the *Direct Console User Interface* (DCUI).

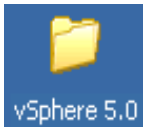
Close the Internet Explorer *Remote Console* window

Log out of ILO and close the ILO IE window.

## Part 3 - Install/Use the vSphere Client

The *vSphere Client* is a VMware supplied GUI tool used to manage both stand alone ESXi hosts and vCenter. The vSphere Client is included in the vCenter 5.0 install bundle. You can also download the vSphere client directly from VMware's download site (www.vmware.com/download).

We have pre-copied the vCenter 5.0 install bundle to your remote access desktop. To install the vSphere Client, please complete these steps:

| Step | Directions |
|---|---|
|  | • Please minimize all programs on your remote session desktop.<br>• Locate the **vSphere 5.0** folder and double click it.<br>• Double click **autorun.exe**<br>• When the vCenter Installer application starts, click the **vSphere Client** link > **Install** |
| Choose Setup Language | • Leave at **English (United States)**<br>• Click **OK** |
| Welcome to the Installation Wizard for the vSphere Client 5.0 | • Click **Next >** |
| End User Patents | • Click **Next >** |
| License Agreement | • Click **I agree to the terms of the license agreement**<br>• Click **Next >** |
| Customer Information | • User Name: **admin**<br>• Organization: **esxlab.com**<br>• Click **Next >** |
| Destination Folder | • Click **Next >** |
| Ready to install the program | • Click **Install** |
| Installation Completed | • Click **Finish** |
|  | The vSphere Client icon should appear on your desktop<br><br>• Close the VMware *vCenter Installer* window<br>• Close the *Windows Explorer* window |

# Part 4 - Connect to and Configure Your ESXi 5.0 Server

We will now use the vSphere Client to connect to our ESXi host.

- Double click the **VMware vSphere Client** on your desktop
- Enter the following credentials when prompted:

  IP Address / Name **esxi#.esxlab.com** (where # is your server number)

  User name **root**

  Password **esxlab.com**

- Click **Login**
- You will see a *Security Warning* window... Click **Install this certificate and do not display any security warnings...**
- Click **Ignore** to log into your ESXi host
- When the *VMware Evaluation Notice* window pops up, click **OK**

## *Review Your Server*

Let's explore your ESXi host...


Inventory

- Double click the **Inventory** icon in the *Inventory* pane
- Click the **Summary** tab for hardware specific information about your server
- Click the **Configuration** tab for detailed hardware information.

There are two main views to the *Configuration* tab... **Hardware** and **Software**.

Please use the vSphere Client (using the indicated Tab or Function) to locate the following information:

| **Property** | **Location Tab / Function** | **Values** |
|---|---|---|
| CPU Make, Model | Configuration > Hardware box > Processors | |
| Processor Cores per Socket | Configuration > Hardware box > Processors | |
| Processor Speed (Ghz) | Configuration > Hardware box > Processors | |
| Server Manufacturer | Summary Tab | |
| Server Model | Summary Tab | |
| Total RAM | Configuration > Hardware box > Memory | |
| System (RAM) | Configuration > Hardware box > Memory | |

| | | |
|---|---|---|
| Virtual Machines (RAM) | Configuration > Hardware box > Memory | |
| Number of Physical NICs | Configuration > Hardware box > Network Adapters | |
| Local Storage Make/Model (see Note below) | Configuration > Hardware box > Storage Adapters > vmhba1 | |
| Storage Volume Name(s) | Configuration > Hardware box > Storage | |

**Note**: If you are running on ESXLab.com servers, your storage adapter should be either an HP Smart Array E200i or a Smart Array P400i. If you are running on other hardware your instructor will help you identify the local storage adapter.

Let's look at your default network configuration in more detail. Follow these steps:

- Click the **Configuration** tab
- In the *Hardware* box, click **Networking**
- You will see one virtual switch (vSwitch0). Click the **Properties...** link beside vSwitch0
- To see the properties of the NIC bound to this vSwitch, click the **Network Adapters** tab

The *PCI Hardware Address* of this NIC is found in the *Adapter Details* box to the right of the Location label: Enter the PCI Hardware Address here - **PCI** ___:___.____

Click **Close** to close the *vSwitch0* Properties window.

## *Host Licensing*

ESXi comes with a 60-day unlimited use evaluation license built in. This eliminates the need to obtain a trial license from VMware. Let's review the capabilities of your ESXi box while it is running under evaluation mode.

- Click the **Configuration** tab
- In the *Software* box, click **Licensed Features** in the *Software* box

| | |
|---|---|
| How many days remain in your evaluation?<br>(**hint**: just above the *Configuration* tab) | |
| What is the maximum number of virtual CPUs available to a VM<br>(Up to __-way virtual SMP)? | |
| Is **vMotion** available? | |
| Is **vSphere DRS** available? | |

| | |
|---|---|
| Is **Storage VMotion** available? | |
| Are **vSphere HA** (High Availability) Cluster services available? | |
| Is **vSphere Distributed Switch** available? | |

**Note**: You would simply click the **Edit...** link (upper right hand corner) to assign a permanent license code to your ESXi host.

## Rename Your Datastore

By fault, the local VMFS storage volume created when you install ESXi is called **datastore1**. Since we will (eventually) be adding multiple ESXi hosts to vCenter, it's nice to create unique names for our storage volumes. Let's do that now:

- Click **Configuration** tab > **Storage**
- Find your *datastore1* volume. Right click it and select **Rename**
- Change the name to **esxi#-datastore1** (where # is your server number)

## *Add a Local User*

If your ESXi host will not be managed by vCenter, it is a good idea to add local users. This is done from the *Local Users & Groups* tab. Let's add a local user now.

- Click the **Local Users & Groups** tab now
- The default is a *Users* view. Click the **Groups** button to review the default groups
- Click the **Users** button to go back to the *Users* view

There is hidden functionality throughout the vSphere Client. In this case, a root (background) menu is available.

- **Right-Click** the background and select **Add...**
- Use these values to complete the *Add New User* pop up

| | | |
|---|---|---|
| Login | **_____** | (your first name in lower case) |
| UID | Leave blank | |
| User Name | Leave blank | |
| Enter Password | **esxlab.com** | |
| Confirm | **esxlab.com** | |
| Grant shell access to this user | Leave unchecked | |
| Group | Leave default | |

- Click **OK** to continue. Look for your newly added user on the user list.

Before we can use the new, local user, we must grant them access to our ESXi host. Right-click your ESXi host (**esxi#.esxlab.com**) in the inventory pane (upper left, below the menus). Click **Add Permission...**

The *Assign Permissions* pop up appears. Please complete this wizard as follows:

- In the *Users & Groups* box, click the **Add...** button
- Scroll through the *Users & Groups* list. Find and click the **student#** user
- Click the **Add** button
- Click **OK** and the *Select Users & Groups* pop up will dismiss

Now, let's assign the user *student* a role. Continuing in the *Assigned Permissions* pop up:

- In the *Assigned Role* box, click the drop down field
- Select **Read-only**
- Leave all other settings at their default value
- Click **OK** to dismiss the *Assigned Permissions* pop up window

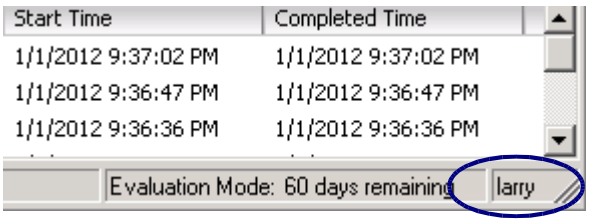
Click the **Permissions** tab. You should see *your* user name appear (along with users *root*, *vpxuser* and *dcui*) as an authorized user. You should also see you hold the *Read-only* role on our ESXi host.

We have just created a new, local user and assigned them *Read Only* permissions. Let's test the new local user account. Please complete these steps:

- **Close** your vSphere Client session
- Double click on the **vSphere Client** icon on your remote desktop
- Log in with ID **<your Name>** and Password **esxlab.com**

Navigate through the vSphere client. Note that many of the links and menu options that were active for the root account are inactive (greyed out or black) for the **<your Name>** user.

Your log in user name is displayed at the bottom right of the vSphere client. Please verify that you are operating as <*your Name*> and not *root*. You should see the following:




Please close the vSphere Client and log in again as user **root** with password **esxlab.com**

## *Connect to Active Directory*

ESXi can connect to Microsoft's Active Directory. This means that you can configure ESXi to authenticate AD managed accounts (rather than creating new local user accounts as we just did). Before your AD users can log in, we must join a domain, and grant domain users access to our ESXi system.

ESXLab.com remote access server pods run an AD service with one predefined domain: *esxlab.com*. We have created users with user names **user1** through **user12.**

To have your ESXi host join a domain, complete the following steps:

- Ensure that you are are logged in as the **root** user. If not, close the vSphere client and log in again as **root** with password **esxlab.com**
- Click the **Configuration** tab
- Click **Authentication Services** in the *Software* box
- Note that the *Directory Services Type* field is set for **Local Authentication** only
- Click the **Properties...** link (upper right hand corner).

Complete the *Directory Services Configuration* pop up as follows:

- Click the drop down field and click **Active Directory**
- The *Domain:* field activates. Enter **esxlab.com**
- Click the **Join Domain** button
- Complete the *Join Domain ESXLAB.COM* pop up with the following values:

| | |
|---|---|
| User name: | **user#@esxlab.com** (where # is your server number) |
| Password: | (Password found on your Kit Access document) |

- Click the **Join Domain** button

If all goes well, the *Directory Services Configuration* box should grey out all fields. This means that you have successfully joined the ESXLAB.COM domain. If you get an error message, please try again.

- Click **OK** to dismiss the pop up window

Now, let's grant *Read-only* permission for our AD based user (student#) to access our ESXi host. **Right click your ESXi host** (**esxi#.esxlab.com**) in the inventory pane (upper left, below the menus). Click **Add Permission...**

The *Assign Permission* pop up appears. Please complete this wizard as follows:

- Click the **Add** button

- In the *Select Users & Groups* box, click the **Domain:** drop down and click the **ESXLAB** domain
- Click the **Name** column header to sort users by their name
- Scroll through the *Users & Groups* list. Find and click the **student#** user
- Click the **Add** button. You should see the *Users:* field populate with **ESXLAB\student#**
- Click **OK** and the *Select Users & Groups* pop up will dismiss

Now, let's assign the user *ESXLab\student#* user a role. Continuing in the *Assigned Permissions* pop up:

- In the *Assigned Role* box, click the drop down field
- Select **Read-only**
- Leave all other settings at their default value
- Click **OK** to dismiss the *Assigned Permissions* pop up window

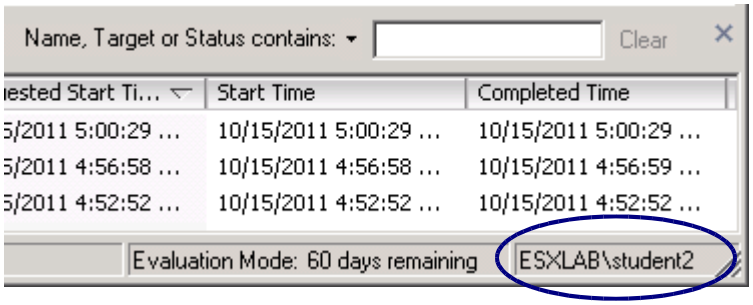
Click the **Permissions** tab. You should see the ***ESXLAB\student#*** user appear (along with users <*your Name*>, *root, dcui* and others) as an authorized user. You should also see that user *ESXLAB\student#* holds the *Read-only* role on our ESXi host.

We have just created a new, AD based user permission with *Read Only* rights. Let's test the access. Please complete these steps:

- Close your vSphere Client session
- Double click on the **vSphere Client** icon on your remote desktop
- Log in with ID **ESXLAB\student#** with the same password as your **ESXLAB\user#** account

Navigate through the vSphere client. Note that many of the links and menu options that were active for the *root* account are inactive (greyed out or black) for the *ESXLAB\user#* user.

Your log in user name is displayed at the bottom right of the vSphere client. Please verify that you are operating as *ESXLAB\user#* and not *root*. You should see the following:




Please close the vSphere Client and log in again as **root** with password **esxlab.com.**

## *Configure ESXi's Clock Services*

ESXi can synchronize all VM clocks to the server's hardware clock – so it is critical that the hardware clock is correct. To ensure accurate time, ESXi uses the Network Time Protocol service to synchronize the local hardware clock to an Internet based, ultra accurate time source. An up to date list of available NTP time servers can be found at

http://support.ntp.org/bin/view/Servers/NTPPoolServers

NTP is not automatically configured when ESXi is installed. Let's set up NTP now (note, you can skip this step if your servers are not connected to the Internet or if advised by your instructor):

- Click the **Configuration** tab
- Click **Time Configuration** in the *Software* box
- Note that the *NTP Servers* field is empty (contains '--')

Let's configure NTP. Click the **Properties...** link (upper right hand corner). The *Time Configuration* pop up window appears. Complete this pop up as follows:

- In the *NTP Configuration* box, click the **Options** button
- The *NTP Daemon (ntpd) Options* window appears. Click **NTP Settings** (left side)
- Click the **Add...** button to add an NTP server
- In the *Add NTP Server* pop up window, enter **0.us.pool.ntp.org** (zero.us.pool.ntp.org)
- Click **OK** to dismiss the *Add NTP Server* pop up. Your NTP server should automatically populate the NTP Servers box
- Check the **Restart NTP service to apply changes** box
- Click **OK** to dismiss the *NTP Daemon (ntpd) Options* pop up
- Click **OK** to dismiss the *Time Configuration* window

Your changes should be applied immediately. Please verify that:

- NTP is running (*NTP Client* field)
- The correct NTP time server is configured (*NTP Servers* field)

If *NTP Client* field does not display as *Running*, click **Properties...** and fix the problem. Ask your instructor for help if you encounter difficulties.

Note the information at the bottom of your screen... The vSphere client translates ESXi time into the correct time for the local machine (our servers are located at a facility in the Eastern Standard Time so the time displayed may not be correct for your local time zone).

## Balanced Power Use

**Note**: This lab section may not work with all ESXLab server pods. Please skip this step if the **Properties...** link (below) is not active.

ESXi can be configured to balance power consumption vs. performance. By default, all power management capabilities of your server are turned off. It is a simple matter to enable power management and thereby saving power while not compromising server performance... Let's do that now:

- Click the **Configuration** tab
- Click **Power Management** in the *Hardware* box
- Click the **Properties...** link. The *Edit Power Policy Settings* pop up should appear.
- Click **Balanced**. This will allow ESXi to use all available hardware power management features (e.g.: slow down unneeded CPU cores when CPU load is light) to reduce power consumption without impacting CPU performance
- Click **OK**
- The screen may not update immediately, click the **Refresh...** link (upper right)

Modern PC servers let you actually review server power consumption over time. On ESXLab.com's HP servers, this feature is built into ILO. You can review your server's power consumption by following these steps:

- Open **Internet Explorer** on your remote desktop
- Point IE at your server's management card: **esx#ilo.esxlab.com** (where **#** is your server number)
- Accept any browser security warnings (if any) and proceed to the web site
- Log in with ID: **admin**, password: **letmein!**
- Click the **Power Management** tab

The BIOS of your server must be configured to allow ESXi to take advantage of hardware power management. Let's review how our server is configured:

- On the left side, click the **Settings** link
- Note the value of the *Power Regulator* for ProLiant field. It should be set to **OS Control mode**. Other settings are *Static Low Power* mode (sacrifice performance for power savings) or *Static High Power* mode (sacrifice power savings for performance). Your server must be in **OS Control mode** for your ESXi power adjustment to make a difference

Now let's look at power consumption. Click the **Power Meter** link (left side). Please scroll down and complete this table:

| | |
|---|---|
| 24hr Average Power | watts |
| 24hr Maximum Power | watts |
| 24hr Minimum Power | Watts |

- Please click the **Log out** link (upper right hand corner) to log out of ILO
- Please close **Internet Explorer**

**Note**: You may wish to log back in to ILO in a few hours to see if your changes have reduced the power draw of your server.

## Working With ESXi Log Files

In this lab step, we will review your ESXi host system logs.

- Back at the vSphere Client menu bar, click **View** > **Home**
- Double click the **System Logs** icon
- Note that the currently selected log file is **/var/log/hostd.log** (the standard log file)
- Click the **Show All** button to display all log file entries
- Click the **Export System Logs** icon (floppy icon). This launches the Export System Logs wizard
- On the Select System Logs step, click Next >
- On Download Location step, browse to your desktop and click Next >
- On Ready to Complete, click Finish

The **Downloading System Log Bundles** pop up appears. Please wait for this task to finish. It will take 1-2 minutes to complete. Click Close when done.

- Minimize all tasks
- On your desktop, there should be a new folder called **VMware-vCenter-Support-yyyy-mm-dd@hh-mm-ss**
- Double click this folder to open it
- Double click the **smaller** of the two .ZIP files
- If you like, review the contents of the various log files. Right click a file and select **View with Notepad**
- When you are finished close all log file windows
- Remove the **VMware-vCenter-Support...** folder from your desktop
- Restore your vSphere Client window

## Server Health

ESXi actively monitors the health status of your server. Monitored items include hardware and ESXi itself. Hardware includes:

- Processors
- Temperature sensors
- Fans
- Software (ESXi 5.0 itself)
- Power Supplies

Monitored software includes all ESXi hardware and component drivers.

Server health monitoring can inform you when a component has degraded or failed completely. It does this by putting yellow warning or red error triangles on the icon representing the component. By default, these warnings propagate up the device hierarchy so a component alert will be visible as a server alert.

Server health monitoring also provides feedback on processor temperatures, component temperatures, fan speed, power supply redundancy, etc. It is useful to browse the component hierarchy to review these values.

Click the **Configuration** tab > **Health Status**

Look through the hierarchy (expanding branches and possibly widening columns) to find the values for the following properties:

| | |
|---|---|
| Proc 1 Level-1 Cache (bytes) | |
| Processor 2 Temperature 2 (Degrees C) | |
| External Environment 1 Temp 1 (Degrees C) | |
| Memory Module 1 Fan Block 3 (Percent) | |
| Power Supply 2 | |

ESXi relies on CIM (Common Information Model) to acquire server hardware information. CIM is defined by DMTF (Distributed Management Task Force). DMTF defines many object profiles. The SMASH (Systems Management Architecture for Server Hardware) profile set is used by VMware to define how to harvest data from hardware sensors.

**Note:** Tier-1 server manufacturers work closely with VMware to ensure their hardware is correctly recognized and that many hardware properties can be monitored and reported.

# Part 6 – Troubleshooting (Optional)

ESXi contains only a minimal command line interface. By default, all access to the local command line is disabled. You can enable command line access from either the server console only or from the network. This can be helpful when diagnosing problems, reviewing log files or performing tasks not available through the vSphere Client.

Enabling command line access to your ESXi host will allow your instructor (and ESXLab) to access your system to help fix problems.

If you haven't already done so, let's enable command line access now:

- Please launch Internet Explorer on your remote access desktop
- In the IE address bar, enter **esx#ilo.esxlab.com** (where # is your server number)
- IE will warn you that there is a potential problem with the web site's security certificate. Please click **Continue to this website (not recommended)**. This occurs because HP ILO uses self signed digital certificates
- For *Login name*, please enter: **admin**
- For *Password*, please enter: **letmein!** and click **Log In** to continue
- On the *System Status* tab, please click the **Launch** button. This launches a console window to your physical server's remote console
- Accept any warnings by clicking **Yes** or **OK**
- Click your remote console window.
- Hit **F2** to log on (Note you may have to hit **F2** a second time)
- Log on with Login name **root** and Password **esxlab.com**
- Arrow down to *Troubleshooting Options* and hit **Enter**
- Arrow to *Enable Local Tech Support* (this allows root logins on the ESXi console). If necessary, hit **Enter** to activate this feature
- Arrow to *Enable Remote Tech Support* (this allows direct root logins over the network). If necessary, hit **Enter** to activate this feature

**Note**: Enabling *Local Tech Support* permits command line access only from the server's physical console. Enabling *Remote Tech Support* permits command line administrator access from any PC on your network (using an SSH client such as the freely available putty).

**Leaving Remote Tech Support enabled is a major security concern!**

Normally, you should only enable *Remote Tech Support* under the following conditions:

1. You are comfortable working on a Linux server as root
2. You have installed a strong (unguessable) password for the root account
3. Your ESXi host is not available from an untrusted network (such as the Internet)
4. Your root password is closely held. That is, you don't give it out to junior

administrators who could do damage with it
5. You were asked to perform these functions by VMware or your local support partner

## *Restarting Management Agents*

ESXi uses Management Agents (software) to interact with the vSphere Client and with vCenter. These agents may occasionally get into an inconsistent state. If that happens, your host becomes unmanageable (using the vSphere client).

If this occurs, you could reboot your server – but that would make the owners and users of VMs on that host very unhappy. Fortunately, it is a simple matter to restart the Management Agents on your ESXi host.

Let's restart the Management Agents now:

- You should still be logged into your ESXi host console. If not, please launch Internet Explorer on your remote access desktop and repeat the steps at the beginning of Part 6 (previous page)
- Arrow down to *Troubleshooting Options* and hit **Enter**
- Arrow down to **Restart Management Agents** and hit **Enter**
- Hit **F11** to confirm that you want to restart the Management Agents
- Watch as the agents are stopped and then restarted
- Hit **Enter** to close this pop up
- Hit **ESC** twice to log out of ESXi

**Note**: You should only take these steps when you cannot login in to or manage your ESXi host using the vSphere Client.

**Note**: Restarting Management Agents does not harm running VMs.

**Congratulations. You have successfully completed Lab 2**