Remote PC Guide for VMware Implementation Using ESXi Version 3.5/4.01

Document Version: 2010-10-22

This guide is a primer for adding remotely accessible PC or servers into your NETLAB Academy Edition® or NETLAB Professional Edition® equipment pods using the VMware Inc. virtualization product ESXi.

This guide covers features available in NETLAB+ version **2010.R5** and later. The details of this guide are specific to **VMware ESXi.**

Documentation for interfacing with other versions of VMware virtualization products can be found in their respective *Remote PC Guide for VMware Implementation* guides.

Part 1 Background 6
1.1 What is a Remote PC? 6
1.2 What Can Users Do With a Remote PC? 7
1.3 What is a Virtual Machine? 8
1.4 What Does ESXi Provide? 9
1.5 How Do NETLAB+ and ESXi Servers Work Together? 11
Part 2 Planning 13
2.1 What Software Is Required? 13
2.1.1 Product Licensing 14
2.1.2 VMware Hosting Product Comparison 15
2.1.3 NETLAB+ Support Summary for ESXi 16
2.1.4 NETLAB+ Known Issues for ESXi 17
2.1.4.1 NETLAB+ Does Not Currently Integrate with vCenter 17
2.1.4.2 No Built-In USB Support For Virtual Machines 17
2.1.4.3 Continuous High CPU Utilization Causes Timeouts 17
2.1.4.4 NETLAB+ Not Tested With All Guest Operating Systems 17
2.1.4.5 NETLAB+ Does Not Support Novell Netware 18
2.1.4.6 Mouse Cursor and VMware Tools 18
2.1.4.7 Installing an Operating System on a Virtual Machine using the NETLAB+ Remote PC Viewer 18
2.1.5 Upgrading From VMware Server To ESXi 18
2.2 ESXi Host Hardware Requirements 19
2.3 How Many ESXi Server Host Systems Do I Need? 22
2.4 Management Station Requirements 27
2.4.1 VMware Infrastructure Client (VI Client) Requirements 27
2.4.2 vSphere Client Requirements 28
Part 3 ESXi Host System Setup 29
3.1 Installing ESXi Server 29
3.2 Setup Using the ESXi Management Console 32
3.2.1 Configuring the Administrative Password 32
3.3 ESXi Host Connectivity Using the IMAN Networking Model 32
3.4 Configuring the Outside Interface 35
3.5 Verifying and Managing the ESXi Host Using VI Client 35
3.5.1 Entering the ESXi License Key 38
3.6 Configuring the Inside Interface 39
3.6.1 Understanding VLAN 1 and Bridged VLANs 40
3.6.2 Adding a Virtual Switch 41
3.6.2.1 Selecting the VMkernel Connection Type 41
3.6.2.2 Selecting the Network Adapter 42
3.6.2.3 Selecting Connection Settings 42
3.6.2.4 Finishing the Configuration of the Virtual Switch 44
3.6.3 Adding a VLAN3 Placeholder 45
3.6.3.1 Selecting the Network Connection Type 45
3.6.3.2 Selecting the Network Adapter 45
3.6.3.3 Selecting Connection Settings 46

3.6.3.4 Finishing the Configuration of the VLAN3 Placeholder 47
3.6.4 Establishing the Inside Connection 48
3.6.4.1 Allocating a Reserved Port on Control Switch for Inside Connection 48
3.6.4.2 Configuring a Reserved Control Switch Port for Inside Connection 49
3.6.4.3 Configuring Trunking Between Multiple Control Switches 49
3.6.4.4 Connecting the Inside Interface and Verify Link 50
3.7 Creating a NETLAB+ User Account 51
3.8 Creating the NETLAB VM Role 52
3.9 Assigning Permissions to the NETLAB+ User Account 53
Part 4 Adding Virtual Machines 56
4.1 Creating a New Virtual Machine Using the VI Client 56
4.1.1 Selecting the Custom Configuration Option 57
4.1.2 Providing a Name for Your Virtual Machine 58
4.1.3 Selecting a Datastore 59
4.1.4 Selecting the Guest Operating system 59
4.1.5 Selecting the Number of Processors 60
4.1.6 Configuring the Memory Size 61
4.1.7 Choosing Network Connections 62
4.1.8 Selecting the I/O Adapter Types 63
4.1.9 Creating a Virtual Hard Disk 63
4.1.10 Specifying Advanced Options 64
4.1.11 Verifying the Settings 65
4.2 Installing a Guest Operating System 66
4.3 Editing the Virtual CD/DVD Device 66
4.4 Installing VMware Tools 68
4.5 Setting the Virtual Machine Display Properties for Remote Access 70
4.6 Adjusting Visual Effects 72
4.7 Disabling the Desktop Background 73
4.8 Adding Software Applications 74
4.9 Taking a Snapshot of Your Virtual Machine and Managing Snapshots 74
4.10 Remote PC Settings (for New Pods) 78
4.11 Modifying PC Settings 82
4.12 Configuring Remote Display Options 83
4.13 Verify the Virtual Machine 86
Part 5 Connecting Virtual Machines to Real Lab Devices 90
5.1 Determining Which VLAN Numbers Are Used by Your Pod 91
5.1.1 Determining VLANs Example 1 – Cuatro Router Pod 92
5.1.2 Determining VLANs Example 2 – Cuatro Switch Pod 94
5.2 Creating VLAN Adapters using VI Client 96
5.2.1 Selecting the Virtual Machine Connection Type 96
5.2.2 Selecting the Network Adapter 97
5.2.3 Selecting Connection Settings 98
5.2.4 Finishing the Configuration of the VLAN Adapter 98
5.3 Configuring Virtual Machines to use the correct VLAN Adapter 100
5.4 Deleting the Placeholder VLAN 3 102

Part 6 Verifying Connectivity and Troubleshooting 104
6.1 Verifying Connectivity Between Virtual Machines and Lab Gear 104
6.2 Review and Modify VM Settings For an Existing Virtual Machine 109
6.3 The Most Frequently Encountered ESXi Issues 112
Appendix A Copying VMDK File to Clone Virtual Machines 116
Appendix B Contacting NDG for Technical Support 127
Appendix C Upgrading from VMware Server 1.x, 2.x, or GSX to VMware ESXi 128

OBJECTIVES

PART 1 - Background

- What is a remote PC?
- What can users do with a remote PC?
- What is a virtual machine?
- What does ESXi provide?
- How does NETLAB+ integrate with ESXi?

PART 2 – Planning

- What software is needed?
- What hardware is needed?
- How many ESXi host servers do I need?

PART 3 – VMware Server Setup

- Install ESXi
- Create NETLAB+ management account
- Configure physical networks
- Install VMware Infrastructure Client
- Prepare for virtual networking

PART 4 – Adding Virtual Machines

- How do I add a virtual machine to my ESXi server?
- How do I make a virtual machine accessible to NETLAB+ users?

PART 5 – Connecting Virtual Machines to Real Lab Devices

- Connecting to an External Network
- Creating VLAN interfaces

PART 6 – Verifying Connectivity and Troubleshooting

- Verifying Connectivity Between Virtual Machines and Lab Gear
- Identify and resolve the most frequently encountered issues.

Part 1 Background

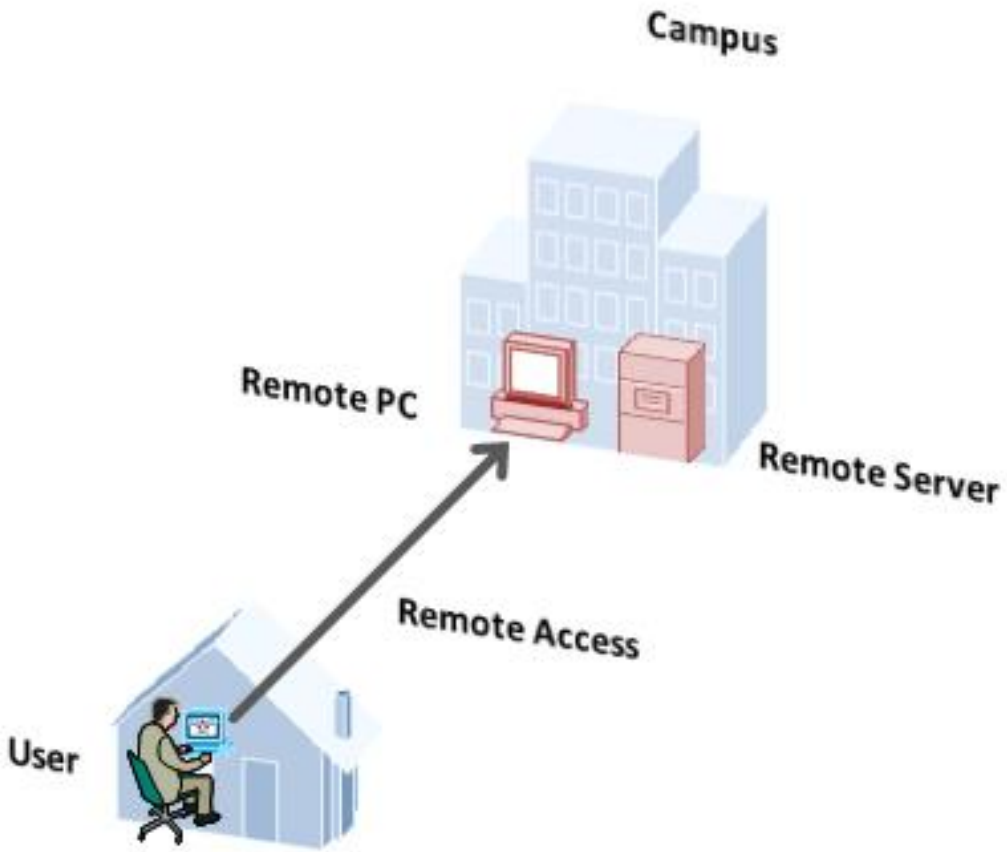
This section builds a fundamental understanding of how remote PCs, virtualization and NETLAB+ work together.

Objectives

- What is a remote PC?
- What can users do with a remote PC?
- What is a virtual machine?
- What does ESXi provide?
- How does NETLAB+ integrate with ESXi?

1.1 What is a Remote PC?

A *remote PC* is a personal computer or server that can be remotely accessed from another PC. *Remote access* allows a user to have full access to the keyboard, video, and mouse of the remote PC. NETLAB+ provides built-in client software for remote access, which is loaded automatically via the user's web browser.



1.2 What Can Users Do With a Remote PC?

Users can remotely access the keyboard, video, and mouse of a virtual machine. NETLAB+ also provides special features such as shared simultaneous access, interfacing with real lab equipment (routers, switches, and firewalls), remotely powering a PC on or off, and restoring the PC to a clean state. This offers a wide range of possibilities. Here are a few scenarios that are being used today.

- **Application Service**. Provides students with access to real operating systems and application software, without distributing software or licenses.

- **Distance Learning.** Provides remote instructor-led training by allowing simultaneous shared access to remote PCs and remote servers. Several users can connect to and share the remote PC's graphical user interface at the same time. Using NETLAB+, students can observe what the instructor is doing on the remote PC, and vice-versa.

- **Resource Scheduling.** Provides controlled, scheduled usage to limited hardware resources.

- **License Management.** Limits the number of licensed operating systems or software applications that can be used at the same time.

- **Online General IT Training**. Provides on-line access to real operating systems and real application software. Using NETLAB+, remote PCs can be completely isolated from production networks, providing a safe environment for instructors and students to do things that are not typically allowed on production networks. Students can safely experience administrative privileges in complex computing environments. You can now provide labs that are not practical for students to set up at home, or scenarios that would be too difficult to set up by new IT students.

- **Online Lab Delivery.** Provides remote delivery of student assignments and lab work.

- **Online Network Training.** Provides online delivery of network training. Remote PCs can be interface with real lab equipment, such as routers, switches, and firewalls, all of which can be accessed remotely using NETLAB+.

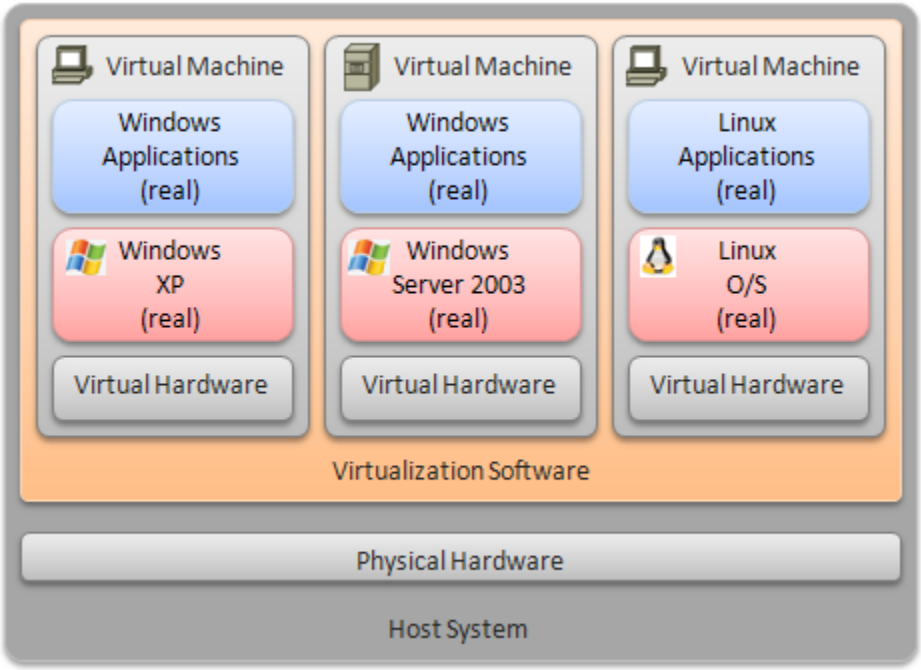
- **Online Security Training.** Provides online delivery of security training. Using NETLAB+, remote PCs can be completely isolated from production networks, providing a safe environment for instructors and students to do things that are not typically allowed on production networks. This might include configuring PCs and lab devices using administrator privileges, installing new software, capturing

network traffic, experimenting with firewalls and VPNs, running malicious software, and scanning networks. At the end of the lab reservation, NETLAB+ will undo any changes.

1.3 What is a Virtual Machine?

In NETLAB+, a *virtual machine* is a remote PC or remote server that runs on virtualized hardware. Although the hardware is virtualized, real operating systems and real application software can still be used; virtual hardware appears to be real as far as the software is concerned. In fact, the software running on a virtual machine is allowed to execute instructions directly on the real CPU. This provides relatively good performance, comparable to actual hardware in most cases. A special process known as the *hypervisor* manages workload among virtual machines to ensure that each application has time to execute.

The result is that virtualization allows you to host real operating systems and real application software with fewer hardware resources.



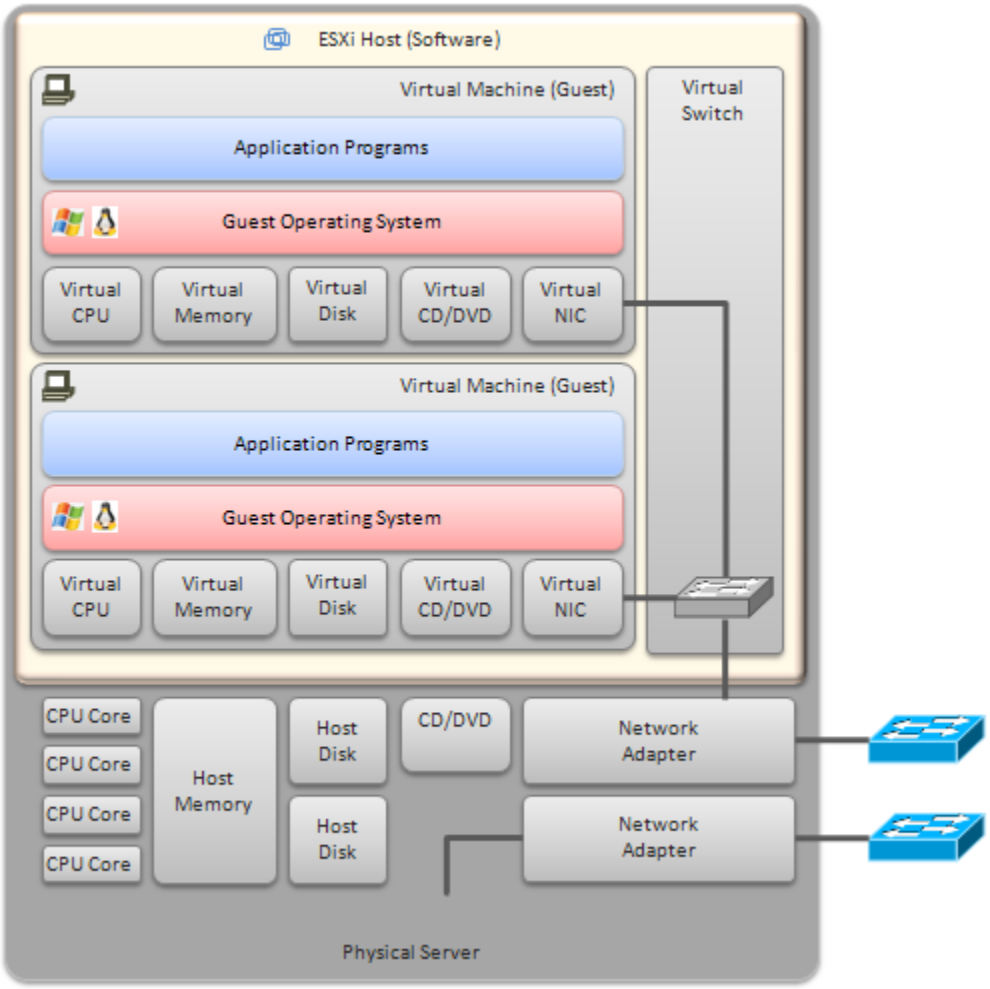
To implement virtual machines, the NETLAB+ software interfaces with third party virtualization products that run on separate servers (not on the NETLAB+ server). This guide is specific to ESXi, from VMware Inc.

NETLAB+ provides remote PC access solutions for both virtual machines and real *standalone* PCs. However, due to the rapid progress of virtualization technology and the numerous benefits it provides, NDG recommends that all new remote PCs be implemented using virtual machines. New development and support for standalone PC interfacing is no longer provided by NDG.

1.4 What Does ESXi Provide?

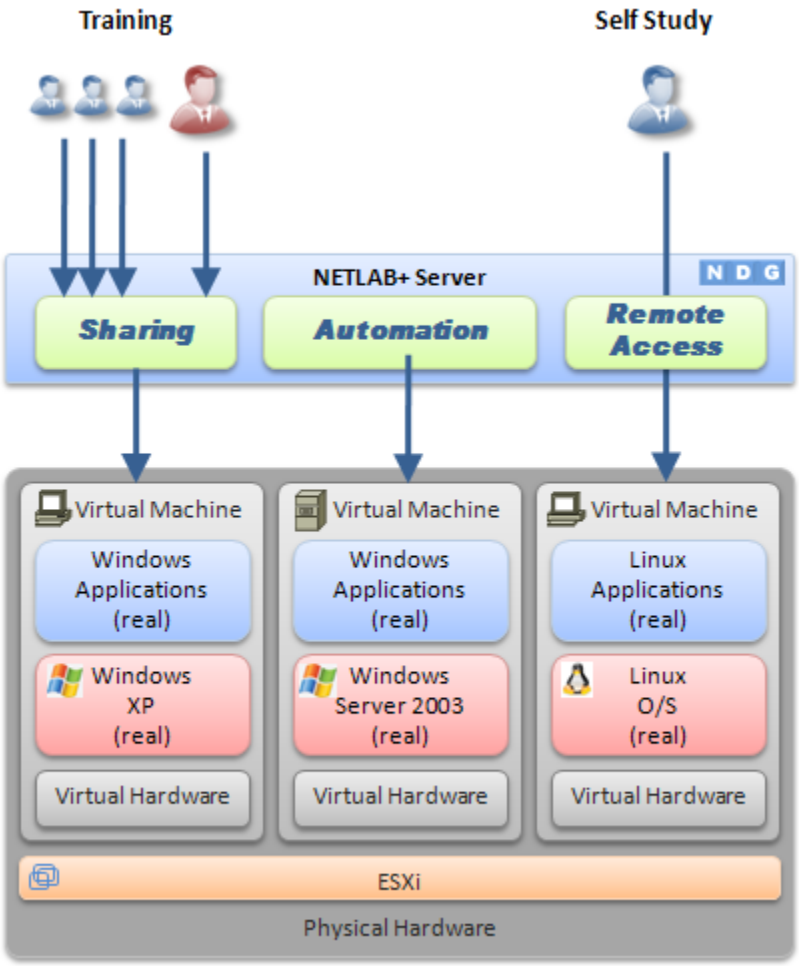
VMware ESXi provides *virtualization server* software. The software abstracts computing resources so that several PCs or servers can run on the same physical server.

Each NETLAB+ remote PC or remote server runs inside of a virtual machine. ESXi provides virtual CPU, virtual memory, virtual disk drives, virtual networking interface cards, and other virtual hardware for each virtual machine. ESXi also provides the concept of a virtual networking switch. Virtual switches can be connected to real networks via host network adapters, allowing virtual machines to connect to real networks.


ESXi Host (Software)
Virtual Machine (Guest)
Application Programs
Guest Operating System
Virtual CPU
Virtual Memory
Virtual Disk
Virtual CD/DVD
Virtual NIC
Virtual Switch
Virtual Machine (Guest)
Application Programs
Guest Operating System
Virtual CPU
Virtual Memory
Virtual Disk
Virtual CD/DVD
Virtual NIC
CPU Core
CPU Core
CPU Core
CPU Core
Host Memory
Host Disk
Host Disk
CD/DVD
Network Adapter
Network Adapter
Physical Server

1.5 How Do NETLAB+ and ESXi Servers Work Together?

NETLAB+ interfaces with ESXi virtualization servers using protocols and application programming interfaces (API) to incorporate virtual machines (PCs and servers) into the lab environment, and make them remotely accessible in an easy-to-use, intuitive way. It also facilities sharing so that multiple users can access the keyboard, video and mouse of a virtual machine simultaneously.



Here is list of features and benefits provided by NETLAB+, working in conjunction with VMware virtualization servers.

- The keyboard, video and mouse of each virtual machine can be accessed without a “backdoor” network or interface on the virtual machine. Access to a virtual machine is proxied through NETLAB+ and the virtualization host system, similar to KVM-over-IP hardware solutions.

- No special client software (other than Java) is required on the user’s computer. NETLAB+ will download its remote PC access application to the client whenever the user clicks on a PC.

- Multiple users can share access to a virtual machine simultaneously.

- NETLAB+ *multiplexes* virtual machine traffic using a single IP address and two TCP ports. It also provides a front-end to the virtual machine environment, so that virtualization servers and virtual machines do not have to be placed on production networks. This significantly increases security and eases firewall administration.

- If the user has a valid lab reservation, NETLAB+ will proxy client access to the keyboard, video and mouse of the virtual machine. This access is terminated when the lab reservation completes, ensuring that users of different reservations do not interfere with each other.

- NETLAB+ supports *revert to snapshot*. Changes to a virtual machine can be discarded at the end of a lab reservation, returning the PC to a clean state.

- Users can have administrative privileges on a virtual machine without risk.

- Users may power on, power off, and revert to clean state (scrub) from the NETLAB+ web interface.

- Users can shutdown and reboot a virtual machine during the lab, without losing changes.

- Virtual network interfaces on a virtual machine can be tied to real networks in the lab. NETLAB+ provides the framework to separate lab networks from real networks in a secure manner.

Virtualization using ESXi is performed on separate physical servers, not included with NETLAB+. You can interface with multiple ESXi servers if necessary.

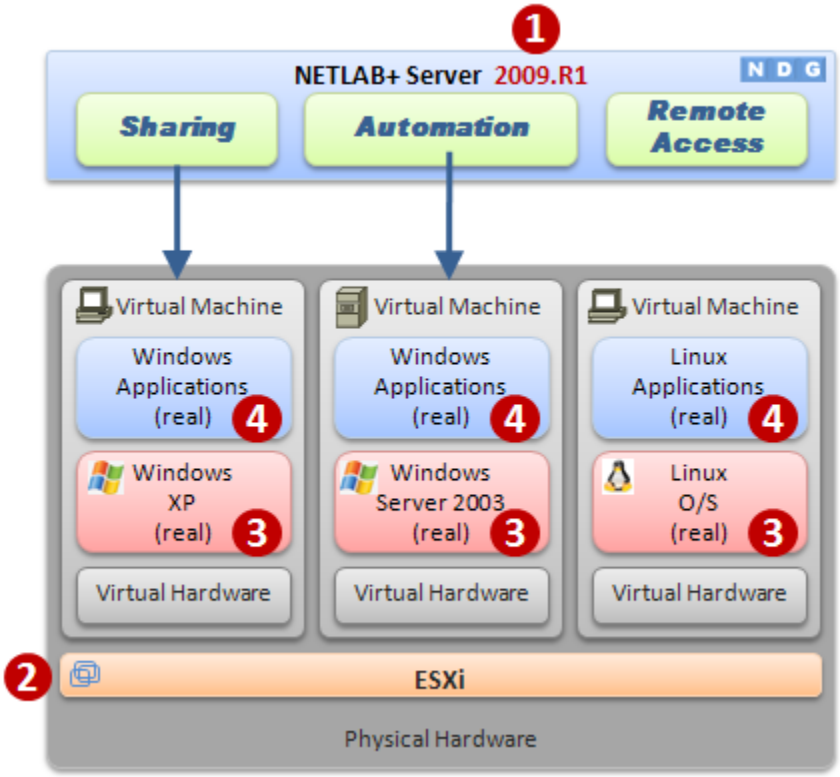
Part 2 Planning

This section discusses the software and hardware requirements for planning a remote PC deployment using ESXi.

Objectives

- What software is required?
- What hardware is required?
- How many ESXi host servers do I need?

2.1 What Software Is Required?



Refer to the numbered diagram above.

(1) Your NETLAB+ server must be running version **2009.R1** or later to interface with ESXi.

(2) Each virtualization server requires either VMware ESXi Installable (software downloadable from http://www.vmware.com) or VMware ESXi Embedded (software pre-installed in flash memory by a PC hardware vendor). Other

VMware products are supported (see the table below). All examples and procedures in this guide are specific to ESXi.

(3) Each virtual machine requires a copy of a supported operating system. In ESXi and NETLAB+ terms, this is called a *guest operating system.* Please refer to the ESXi documentation to determine which operating systems versions are currently supported. NETLAB+ has been tested with Microsoft Windows and Linux operating systems.

Novell Netware is known to have problems with cursor updates, and is therefore not supported at this time.

(4) Each virtual machine can run application programs. These are installed on each virtual machine the same way you install software on a real PC.

2.1.1 Product Licensing

For the purpose of software licenses, each virtual machine is treated as an independent real PC or server. Please refer to the specific vendor license agreements (and educational discount programs, if applicable) to determine licensing requirements for your virtual machine's software, server software, operating systems, and application programs.

2.1.2 VMware Hosting Product Comparison

The following table compares NETLAB+ support and features for selected VMware hosting products. This guide is specific to **ESXi.** Should you decide to use one of the other listed products with NETLAB+, please switch to the respective *NETLAB+ Remote PC Guide* specific to the VMware product.

VMware ESXi 4.1 is not supported. Please do not upgrade your systems to VMware ESXi 4.1. NDG is working to resolve known issues concerning the use of ESXi 4.1 and plans to support this version in a future software release.

Product	VMware ESXi		VMware Server		VMware GSX
VMware Version	**3.5 U3/U4/U5**	**4.01**	**2.x**	**1.x**	**3.x**
NETLAB+ Support	Supported	Supported	Supported	Deprecated	Deprecated (2)
Minimum NETLAB+ Version	2009.R1	2009.R1	2009.R1	4.0.11	3.7.0
Architecture	Hypervisor	Hypervisor	Hosted	Hosted	Hosted
Minimum VMware Version Required	3.5 U3	4.01	2.0	1.0.3	3.1
VMware Versions Tested by NDG	3.5 U3/U4/U5	4.01	2.0	1.0.3 1.0.6 1.0.7	3.1 3.2
Host Operating System Required	No	No	Windows	Windows	Windows
Windows Server O/S Versions Tested	n/a	n/a	2003	2003 2000	2003 2000
Linux Server O/S Versions Tested	n/a	n/a	n/a (1)	n/a (1)	n/a (1)
NETLAB+ Feature Support:					
• Remote PC Viewer	Yes	Yes	Yes	Yes	Yes
• Power On / Off	Yes	Yes	Yes	Yes	Yes
• Revert to Snapshot (scrub)	Yes	Yes	Yes	Yes	Yes
USB Support within VM	No	No	Yes	Yes (USB 1.1)	

(1) VMware Server for Linux or VMware GSX for Linux is not currently supported or documented by NDG. However, you may run Linux as a *guest operating system* on virtual machines.

(2) VMware GSX has been replaced by VMware Server 1.x and VMware Server 2.x.

2.1.3 NETLAB+ Support Summary for ESXi

	VMware ESXi 3.5	VMware ESXi 4.01
NETLAB+ Support Status	Supported	Supported
Minimum NETLAB+ Version Required	NETLAB+ 2009.R1	NETLAB+ 2009.R1
ESXi Minimum Version Required	ESXi version 3.5 U3	ESXi version 4.01
ESXi Versions Tested	ESXi version 3.5 U3/U4/U5	ESXi version 4.01
Guest Operating Systems Tested (1, 2)	Windows XP (x86, 32-bit)	Windows XP (x86, 32-bit)
Maximum Number of Running Virtual Machines (on each ESXi server host)	**Varies with CPU and Hardware[3]**	**Varies with CPU and Hardware[4]**
NETLAB+ Supported Features	Remote PC Viewer Power On Power Off Revert to Snapshot (scrub)	Remote PC Viewer Power On Power Off Revert to Snapshot (scrub
USB Support for Virtual Machines	**No** (a separate USB-over-IP solution is required to support USB devices)	**No** (a separate USB-over-IP solution is required to support USB devices)

(1) Please refer to the VMware Guest Operating System Installation Guide for specific product support, installation instructions and known issues.

(2) Older 32-bit processors will only support 32-bit guest operating systems. A 64-bit processor is required for 64-bit guest operating systems.

(3) NDG currently recommends no more than 4 running VMs per CPU core. VMware configuration maximums can be found at http://www.vmware.com/pdf/vi3_35/esx_3/r35u2/vi3_35_25_u2_config_max.pdf. CAUTION: The numbers within this document are absolute maximums, not recommended values.

(4) NDG currently recommends no more than 8 running VMs per CPU core. VMware configuration maximums can be found at http://www.vmware.com/pdf/vsphere4/r40/vsp_40_config_max.pdf CAUTION: The numbers within this document are absolute maximums, not recommended values.

2.1.4 NETLAB+ Known Issues for ESXi

In this section, we will discuss several known issues encountered when ESXi with NETLAB+.

2.1.4.1 NETLAB+ Does Not Currently Integrate with vCenter

NETLAB+ communicates directly with VMware ESXi hosts. Integration with vCenter and other VI Infrastructure components is planned.

2.1.4.2 No Built-In USB Support For Virtual Machines

A separate USB-over-IP solution is needed for virtual machines to access physical USB devices. Alternatively, VMware Server 2.0 supports USB 2.0 pass-through from host to virtual machine.

2.1.4.3 Continuous High CPU Utilization Causes Timeouts

Continuous high CPU utilization at or near capacity on all processor cores may cause API connection timeouts. This in turn may cause automated operations performed in NETLAB+ to fail.

Causes. Running too many active virtual machines on one server, and/or using a server with inadequate hardware resources.

Workaround #1. Add additional ESXi servers and divide the workload.

Workaround #2. Upgrade server CPU and memory. Additional CPU speed, processor cores and memory are usually helpful. See the hardware discussion in the later section for additional guidance.

2.1.4.4 NETLAB+ Not Tested With All Guest Operating Systems

VMware provides a *Guest Operating System Installation Guide* that contains a list of supported guest operating systems and the known issues for each. Not all operating systems in this document have been tested with NETLAB+.

We recommend that you thoroughly test each unique guest operating system in the NETLAB+ environment prior to production deployment. In particular, you should install the VMware Tools on the guest operating system, and then use the NETLAB+ Remote PC

Viewer to test for proper functioning of the keyboard, mouse, mouse cursor, and screen updates.

2.1.4.5 NETLAB+ Does Not Support Novell Netware

Novell Netware as a guest operating system is not supported by NETLAB+ at this time. There are known issues with cursor updates, making remote access unusable.

2.1.4.6 Mouse Cursor and VMware Tools

To use the mouse of a virtual machine from NETLAB+, VMware Tools must be installed and running on the virtual machine.

2.1.4.7 Installing an Operating System on a Virtual Machine using the NETLAB+ Remote PC Viewer

Normally you install an operating system and VMware Tools on a virtual machine using the VI or vSphere client before making the virtual machine available to NETLAB+ users.

In some cases you may wish to allow NETLAB+ users to install the operating system as part of a training exercise using the NETLAB+ Remote PC Viewer Application. In this case, the operating system installation must be performed using keyboard commands and shortcuts. The mouse cursor will not work properly during operating system installs because VMware Tools is not installed during the process (see 2.1.4.6).

2.1.5 Upgrading From VMware Server To ESXi

The management interfaces, APIs, and virtual machine settings for ESXi are significantly different from VMware Server 1.x and VMware Server 2.x, which has required NDG to develop this separate guide.

Configuration changes to both NETLAB+ and virtual machine settings are required when upgrading from VMware Server to ESXi. Appendix C documents the necessary changes.

2.2 ESXi Host Hardware Requirements

At this point, you have decided that ESXi is the appropriate product to host your virtual machines. (If not, please switch to the respective NETLAB+ guide that matches the specific VMware product.)

Henceforth, a reference to **"ESXi"**, **"ESXi host system"** and **"ESXi server"** in this document refers to a server running VMware's ESXi virtualization software.

Next, we will explore hardware requirements. The *VMware Hardware Compatibility Guide* provides a convenient reference to review hardware compatibility for your specific version of ESXi.

- If you are using VMware ESXi version 3.5, you may also consult the Requirements section of the *ESX Server 3i Installable Setup Guide* or the *ESX Server 3i Embedded Setup Guide*, depending on the version you have chosen. This is important, particularly if you wish to run 64-bit guest operating systems. (Be aware that VMware has made some recent changes to product names; some VMware documentation refers to ESXi by its old product name, ESX Server 3i).

- If you are using VMware ESXi 4.01, you may refer to the requirements section of the ESXi Installable and vCenter Server Setup Guide or the ESXi Embedded and vCenter Server Setup Guide depending on the version you have chosen. This is important, particularly if you wish to run 64-bit guest operating systems.

Remote PCs are implemented on one or more ESXi host systems (separate from the NETLAB+ server). The table below contains a list of recommended hardware for an ESXi server.

Servers that do not meet the minimum requirements listed may work, but may encounter performance issues and/or lack support for certain guest operating systems.

VMware ESXi only supports hardware RAID. If you are upgrading from VMware Server to VMware ESXi, be sure the RAID controller is supported by ESXi. Please note that the "on-board" RAID in many motherboards is actually software RAID (or "fake" RAID), because the actual RAID functions are performed by device drivers running on the host operating system. You can ***potentially*** run your SATA drives in a non-RAID configuration. More information regarding limitations is available in the VMware Knowledge Base. These options should only be considered by those seeking to make use of existing equipment. If you are purchasing new equipment, following the requirements in the current test platform section is your best option.

	Recommended Minimum / Features	Notes
Processor(s)[1, 2]	x86-64 compatible (Intel, AMD) • 4 or more cores • 2.33 Ghz per core Intel-specific features: • Intel 64 (formerly EM64T)[1,2] • Intel VT-x (Vanderpool) AMD-Specific Features: • AMD64 revision D or later[1,2] • AMD-V (virtualization)	Examples that meet the minimum: • Intel Xeon E5520 (Quad core)[5] • Intel Xeon E5410 (Quad core)[4] Please search *the* *VMware Hardware Compatibility Guide* for supported processors.
Memory	Up to 6TB	Install enough memory the maximum number of running virtual machines and the host.
Disk[3]	3TB RAID1	See note 3 below concerning RAID. VMware ESXi also supports external iSCSI and NAS storage arrays. Please search the *VMware Hardware Compatibility Guide* for supported processors.
Network Interfaces	Dual (2) 100/1000 Ethernet with 802.1q Supported Interfaces: • **Intel** server adapter (825XX chipset) with Advanced Network Support (ANS) features	Please search the *VMware Hardware Compatibility Guide* for supported processors.

(1) x86-64 should not be confused with the Intel Itanium (formerly *IA-64*) architecture, which is not compatible on the native instruction set level with the x86 or x86-64 architecture.

(2) VMware provides a standalone utility that you can use without ESXi to perform the same check and determine whether your CPU is supported for ESXi virtual machines with 64-bit guest operating systems. You can download the 64-bit processor check utility from http://www.vmware.com/download.

(3) VMware ESX/ESXi only supports hardware RAID. If you are upgrading from VMware Server to VMware ESXi (or ESX in the future), be sure the RAID controller is supported by ESX/ESXi. Please note that the "on-board" RAID in many motherboards is actually software RAID (or "fake" RAID), because the actual RAID functions are performed by device drivers running on the host operating system. You can ***potentially*** run your SATA drives in a non-RAID configuration. More information regarding limitations is available in the VMware Knowledge Base. These options should only be considered by those seeking to make use of

existing equipment. If you are purchasing new equipment, following the requirements in the current test platform section is your best option.

[4]This hardware was used by NDG as the 2009 test platform.

[5]This hardware was used by NDG as the 2010 test platform. In the future, the E5520 will be the minimum processor that may be used to support the VMware IT Academy Program ICM course.

2.3 How Many ESXi Server Host Systems Do I Need?

The number of ESXi host systems and memory requirements vary based on the lab topologies and number of pods you want to implement.

As a general planning and budget guideline, NDG recommends no more than 10 to 12 virtual machines per server with hardware meeting the requirements in section 2.2. More virtual machines may be possible for certain workload types and/or high-end hardware.

Each virtual machine uses CPU cycles and memory on the server. The table below shows a hypothetical allocation of processor cores for virtual machines and other system tasks. You do not actually configure this; ESXi will do this dynamically based on workload.

CPU Core #1 (2.33 GHz)	VM1 VM2 VM3 VM4
CPU Core #2 (2.33 GHz)	VM5 VM6 VM7 VM8
CPU Core #3 (2.33 GHz)	VM9 VM10 VM11 VM12
CPU Core #4 (2.33 GHz)	ESXi and API processes

 If you have more than one ESXi host server, consider spreading the VMs from each pod across all of host servers. This will evenly spread the load on critical system resources for each ESXi host (processing and memory).

Running too many virtual machines may starve the host and/or ESXi Server APIs. This may lead to timeouts and task automation failures in NETLAB+.

 If a single ESXi host is shared among multiple pods and the ESXi host does not meet the requirements from section 2.2, users from one pod may notice a substantial delay when the reservation begins/ends from another shared pod. When a reservation begins, NETLAB+ instructs the ESXi host server to power on or resume all Virtual Machines represented in that lab topology. When this occurs, the ESXi host may experience a high CPU load for several minutes. This can result in sub-optimal and even unresponsive communications for those NETLAB+ users logged in from a different pod, accessing virtual machines hosted by the same ESXi server.

Step-By-Step Guidance

Step 1. Carefully study your lab topologies and determine the number of virtual machines required by each pod. The requirements for several NETLAB$_{AE}$ pods shown below assume that you are implementing all PCs supported by the pod.

The following table shows some of the pods that support virtual machines in NETLAB$_{AE}$. For an updated list of NETLAB$_{AE}$ topologies, please view the lab topologies page.

	Maximum Virtual Machines
Multi-purpose Academy Pod(MAP)	**3**
Basic Router Pod v2 (BRPv2)	**4**
Basic Switch Pod v2 (BSPv2)	**3**
Cuatro Router Pod (CRP)	**5**
Cuatro Switch Pod (CSP)	**4**
LAN Switching Pod (LSP)	**4**
Network Fundamentals Pod (NFP)	**5 required** **2 optional**
Network Security Pod 2.0 (NSP)	**7**

Step 2. Add up the number of virtual machines used by each pod you are implementing. For example:

Pod Name	Type	Virtual Machines
POD 1	Basic Router Pod Version 2	4
POD 2	Basic Router Pod Version 2	4
POD 3	Basic Router Pod Version 2	4
POD 4	Basic Router Pod Version 1	0 (n/a)
POD 5	Basic Switch Pod Version 2	3
POD 6	Network Security Pod (2.0)	7
Total		**22**

Step 3. Assign each pod that supports PCs to an ESXi host server. Note, POD4 does not support PCs and uses no ESXi host resources.

ESXi Host #1 – Example		
Pod	**Type**	**Virtual Machines**
POD 1	Basic Router Pod Version 2	4
POD 2	Basic Router Pod Version 2	4
POD 3	Basic Router Pod Version 2	4
Total		**12**

ESXi Host #2 - Example		
Pod	**Type**	**Virtual Machines**
POD 5	Basic Switch Pod Version 2	3
POD 6	Network Security Pod (2.0)	7
Total		**10**

Step 4. Based on the pod type and curriculum requirements, determine which guest operating system you will use on each virtual machine. Tabulate the operating system and memory requirements for the virtual machines. You should allocate the same amount of memory as you would if standing up a real PC. The following would represent typical choices for ESXi Host 1 in the previous example.

VMware Host System #1 - Example			
Pod	**PC Name**	**Operating System**	**Memory (MB)**
POD 1	PC1a	Windows XP	128
POD 1	PC1b	Windows XP	128
POD 1	PC2	Windows XP	128
POD 1	PC3	Windows XP	128
POD 2	PC1a	Windows XP	128
POD 2	PC1b	Windows XP	128
POD 2	PC2	Windows XP	128
POD 2	PC3	Windows XP	128
POD 3	PC1a	Windows XP	128
POD 3	PC1b	Windows XP	128
POD 3	PC2	Windows XP	128
POD 3	PC3	Windows XP	128
Total			**1536 (2GB) ***

* At least 4GB per server is now recommended to support recent mainstream operating system requirements with greater memory requirements.

Step 5. Translate the requirements from steps 1 through 4 into an itemized list for each server. The two VMware host systems in the previous examples would require the following items.

VMware Host System #1 - Example		
Quantity	**Item**	**Role**
1	Server • Intel Core i7 920 (2.93 GHz X 4 cores) • 4GB (recommended) • 2 x 320GB Hard Disks with RAID1 support • Dual (2) Intel Network Interfaces with 802.1q VLAN tag support	server hardware
1	ESXi	virtual machine software
12	Windows XP (Home or Pro)	guest operating systems

VMware Host System #2 - Example		
Quantity	**Item**	**Role**
1	Server • Intel Core i7 920 (2.93 GHz X 4 cores) • 4GB (recommended) • 2 x 320GB Hard Disks with RAID1 support • Dual (2) Intel Network Interfaces with 802.1q VLAN tag support	server hardware
1	ESXi	virtual machine software
5	Windows XP (Home or Pro)	guest operating systems
3	Windows 2000 Server	guest operating systems
2	Linux	guest operating systems

2.4 Management Station Requirements

It is also necessary to have at least one other computer to act as a management station. This computer must be running Windows, have network access to the ESXi server, and have Internet access.

The management software you use will depend upon the version of ESXi you have selected:

- If you are using VMware ESXi 3.5, the VMware Infrastructure Client software will be installed on this machine (see section 3.5). In this guide, the majority of screenshots show the use of the VMware Infrastructure Client. Please refer to the requirements in section 2.4.1.

If you are using VMware ESXi 4.01, the VMware vSphere Client will be installed on this machine. Since the majority of screenshots in this guide depict the use of the VMware Infrastructure Client, you will see minor differences between your system and the screenshots in this guide. Please refer to the requirements in section 2.4.2.
The functionality is the same for both software versions. References to the VMware Infrastructure Client (VI Client) throughout this guide apply to both the VMware Infrastructure Client (ESXi 3.5) and the VMware vSphere Client (ESXi 4.01) except where indicated otherwise.

2.4.1 VMware Infrastructure Client (VI Client) Requirements

If you are using VMware ESXi 3.5, you will install VMware Infrastructure Client software as your management station on a machine meeting the following requirements:

Hardware Requirement

- **Processor** – 266MHz or higher Intel or AMD x86 processor (500MHz recommended).
- **Memory** – 256MB RAM minimum, 512MB recommended.
- **Disk Storage** – 150MB free disk space required for basic installation. You must have 55MB free on the destination drive for installation of the program, and you must have 100MB free on the drive containing your %temp% directory.
- **Networking** – Gigabit Ethernet recommended.

Software Requirements

- The VMware Infrastructure Client (VI Client) is designed for 32-bit versions of the Windows operating systems.

- The VI Client requires the Microsoft .NET 2.0 Framework, which will be automatically installed if it is not present on the system.

2.4.2 vSphere Client Requirements

If you are using VMware ESXi 4.01 you will install vSphere Client software as your management station on a machine meeting the following requirements:

Hardware Requirements

- **Processor** – 266MHz or faster Intel or AMD processor (500MHz recommended).
- **Memo**ry – 200MB RAM
- **Disk Storage** – 1GB free disk space is required for a complete installation, which includes the following components:
  - Microsoft .NET 2.0
  - Microsoft .NET 3.0 SP1
  - Microsoft Visual J#
  - vSphere Client 4.0
  - vSphere Host Update Utility 4.0

- You must also have 400MB free on the drive that has your %temp% directory.

- If all of the prerequisites are already installed, 300MB of free space is required on the drive that has your %temp% directory, and 450MB is required for the vSphere Client 4.0.

- Networking – Gigabit connection recommended.

Software Requirements

- The vSphere Client requires the Microsoft .NET 3.0 SP1 Framework. If your system does not have it installed, the vSphere Client installer installs it.

- For a list of supported operating systems, see the *Compatibility Matrixes* on the VMware vSphere documentation Web site. Getting Started with ESXi Installable VMware,

Part 3 ESXi Host System Setup

This section describes the initial preparation of an ESXi host system. After ESXi is installed and configured, virtual machines can be added (as *guests*) and integrated into the overall NETLAB+ system.

Objectives

- Install ESXi Server
- Become Familiar with the ESXi management console
- Learn about the IMAN networking model.
- Configure the Outside Interface
- Install VMware Infrastructure Client software
- Configure the Inside Interface

All tasks in this section are performed on **separate dedicated servers** that you provide. Do not perform any of the tasks in this section on the NETLAB+ server appliance, as this will delete the NETLAB+ software, requiring you to return it to the factory for re-installation.

3.1 Installing ESXi Server

ESXi is available embedded in server hardware, or may be installed from a CD. When downloading ESXi, it is important to select a version that is compatible with NETLAB+. **Currently, the latest supported version is 4.01.**

Please do not upgrade your systems to VMware ESXi 4.1. NDG is working to resolve known issues concerning the use of ESXi 4.1 and plans to support this version in a future software release.

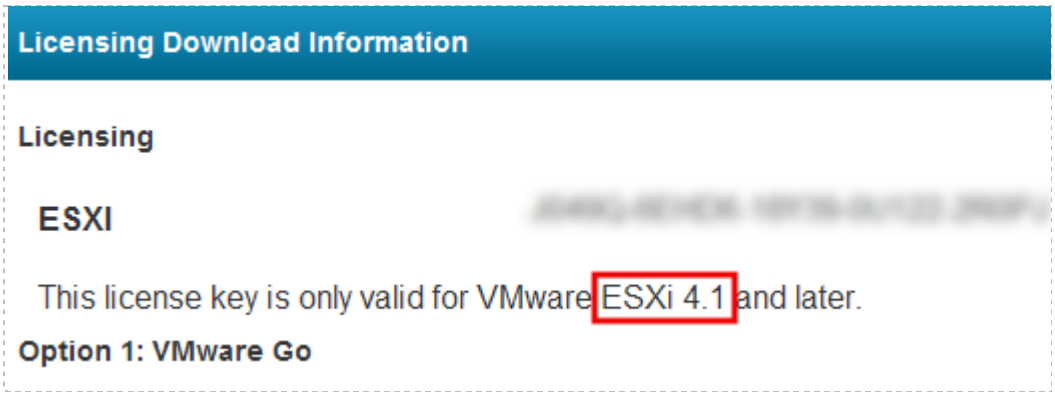
Instructions for downloading ESXi:

1. Please visit VMware's page for registration of VMware vSphere Hypervisor. This will include access to ESXi: https://www.vmware.com/tryvmware/

2. In order to obtain a free download, you must register. Login if you already have a VMware account.

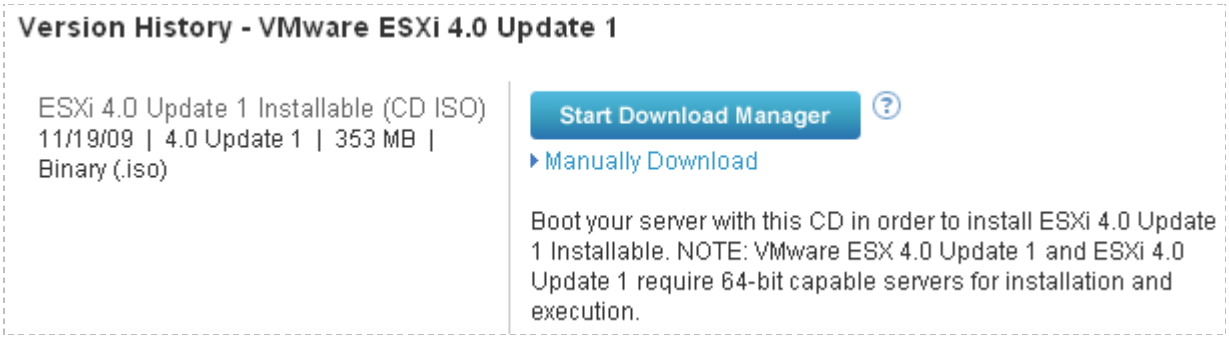
3. After accepting the license agreement, you will receive a link via email that will bring you to the VMware vSphere Hypervisor Product License and Download page.

4. The page includes your license key for ESXi. Please make note of your license key, as you will need it in order to continue using ESXi beyond the evaluation period (see section 3.5.1).



Although it is indicated that the license key is valid for 4.1 and later, the license key is valid for use with your download of 4.01.

5. Scroll down the page to locate the download for **ESXi 4.0** and follow the download procedure.



6. To patch from 4.0 U1 to U2, use the Host Update Utility, which is packaged with the vSphere client. For more information, refer to VMware's vSphere Upgrade Guide for details: http://www.vmware.com/pdf/vsphere4/r40/vsp_40_upgrade_guide.pdf

If you are using VMware ESXi 4.01, please review the information in the *Getting Started with ESXi Server Installable* guide. You may use this guide as a reference for ESXi 4.01 Installable and ESXi 4.01 Embedded versions, with the exception that using **ESXi Installable requires performing the installation procedure detailed on page 7, *Install ESXi 4.0.***

If you are using VMware ESXi 3.5, please review the information in the *Getting Started with ESX Server 3i Installable* guide. You may use this guide as a reference for ESXi 3.5 Installable and ESXi 3.5 Embedded versions, with the exception that using **ESXi Installable requires performing the installation procedure detailed on page 4, *Installing ESX Server 3i*.**

3.2 Setup Using the ESXi Management Console

Following installation, power on the ESXi host (with a keyboard and monitor connected). When the ESXi host is powered on for the first time, it enters a boot-up phase during which system network and storage devices are configured with defaults. After the host completes the boot-up phase, the direct console appears on the attached monitor. In the subsection below, details are provided on configuring the administrative password. Additional setup tasks needed in order to configure the outside interface will be discussed in section 3.4.

3.2.1 Configuring the Administrative Password

The administrative username for the ESXi host is **root**. By default, the administrative password is *null*.

To configure a password for the ESXi server:

1. Press F2 to display the default configuration of the host.
2. Press F2 again, to display options to customize system options.
3. Select the **Configure Root Password** option.
4. When prompted for the old password, press enter.
5. Enter a new password.
6. Confirm the new password.
7. Make note of the password for future use.

3.3 ESXi Host Connectivity Using the IMAN Networking Model

Several types of network communication occur to and from the ESXi host system.

- **KVM.** Provides remote Keyboard/Video/Mouse access to virtual machines, via the NETLAB+ server.

- **API.** Provides an interface for NETLAB+ to query and control virtual machines (status, power on, power off, and revert to snapshot).

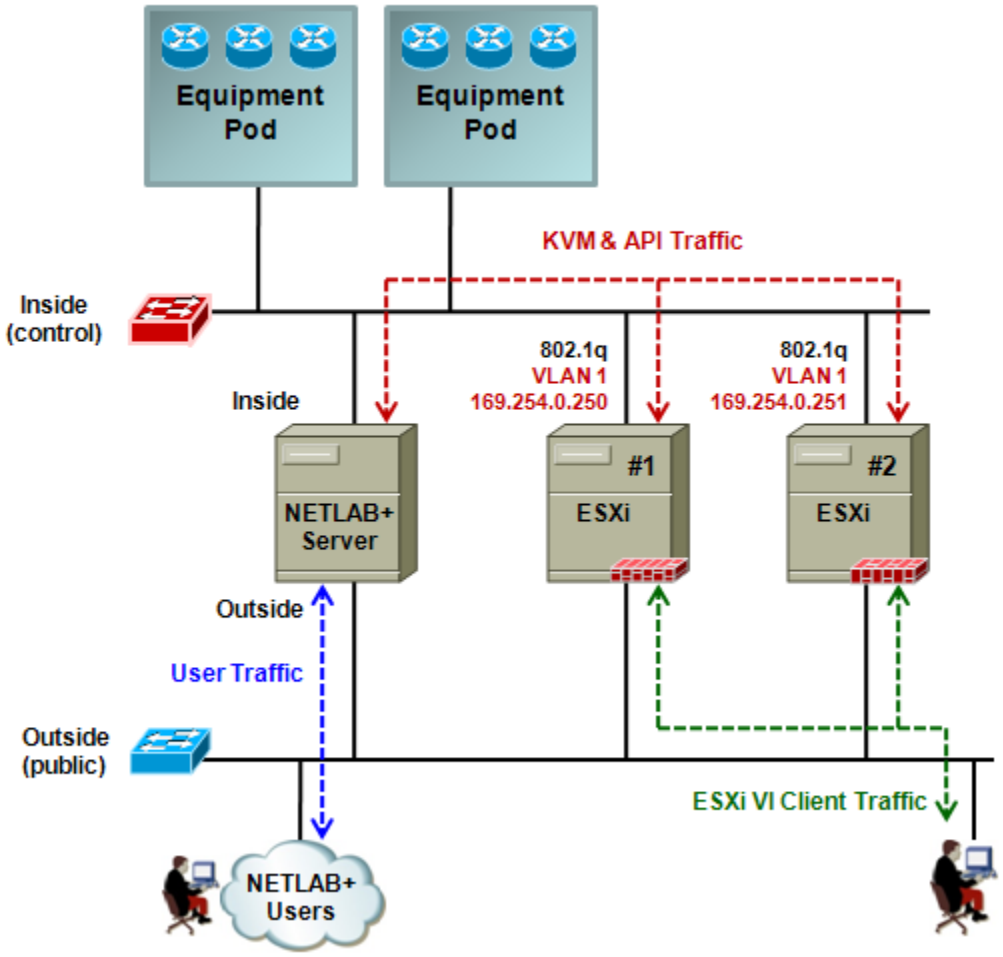
- **Bridging (optional).** Allows virtual machines to connect to real lab devices such as routers, switches, and firewalls. This is accomplished by connecting ESXi virtual machines to a virtual switch, then connecting the virtual switch to Virtual LANs (VLAN) behind NETLAB+ control switches. Although not documented in this guide, physical network adapters (NICs) on the VMware host system may be directly connected to lab devices as an alternative to VLANs, for special applications that require a more direct path between a virtual machine and external lab device.

- **Remote Management.** The ESXi host server and virtual machines are managed using the VMware infrastructure client, which you will install (see section 3.5).

NDG has developed a networking model, *Inside Networking with External Management* (IMAN) to facilitate this communication. IMAN is the only networking model recommended for use with ESXi. If you are upgrading from VMware Server 2.x or VMware Server 1.x, you may be familiar with the *Inside Networking with High Security* (ISEC) and *Outside Networking with External Management* (OMAN) models. These models are not recommended for use with ESXi.

Networking Model	IMAN Recommended for ESXi	ISEC	OMAN
Security	Very Good	Excellent	Good, with proper diligence in firewall configuration
Manage VMware hosts and virtual machines from VI Client	Yes	No	Yes
Required number of Ethernet ports in each VMware server	2	1	2
Requires 802.1q VLAN support on inside interface	Yes	Yes	Yes
Requires 802.1q support on outside interface	No	n/a	No
Requires native (untagged) VLAN 1 support on inside interface	Yes	Yes	No
KVM and API traffic flow	Inside network (control switches)	Inside network (control switches)	Outside network (user LAN)

The Inside Networking model with External Management (IMAN) provides a balance between security and manageability. All virtual machine traffic (Bridging), KVM, and automation traffic (API) remain behind the NETLAB+ inside interface (i.e. the control switches). The outside interface on each ESXi server provides a path for remote management of the VMware host system and virtual machines (via VI Client).



IMAN Features

- Provides a practical method for managing ESXi host systems and virtual machines, while keeping most NETLAB+ and lab communication safely on a private network.

IMAN Requirements

- Each ESXi Server requires two Ethernet interfaces.

3.4 Configuring the Outside Interface

In this section, we will perform tasks required to enable connectivity through the outside interface. The outside interface is used for external management of the ESXi server. This interface is referred to as the *Management Network* in VMware documentation.

To provide network access through the outside interface to your ESXi host, you have two options:

- Use the default DHCP (Dynamic Host Configuration Protocol) configured IP settings
- Configure a static IP address.

Use of a static IP address is highly recommended so that references to the IP address can be made without concern of future changes.

If you are using ESXi 3.5, the *Configuring Management Network* section of the *Getting Started with ESX Server 3i Installable* guide includes details on configuring static IP settings.

If you are using ESXi 4.01, the *Configuring IP Settings for ESXi* section of the *Getting Started with ESXi Server Installable* guide includes details on configuring static IP settings.

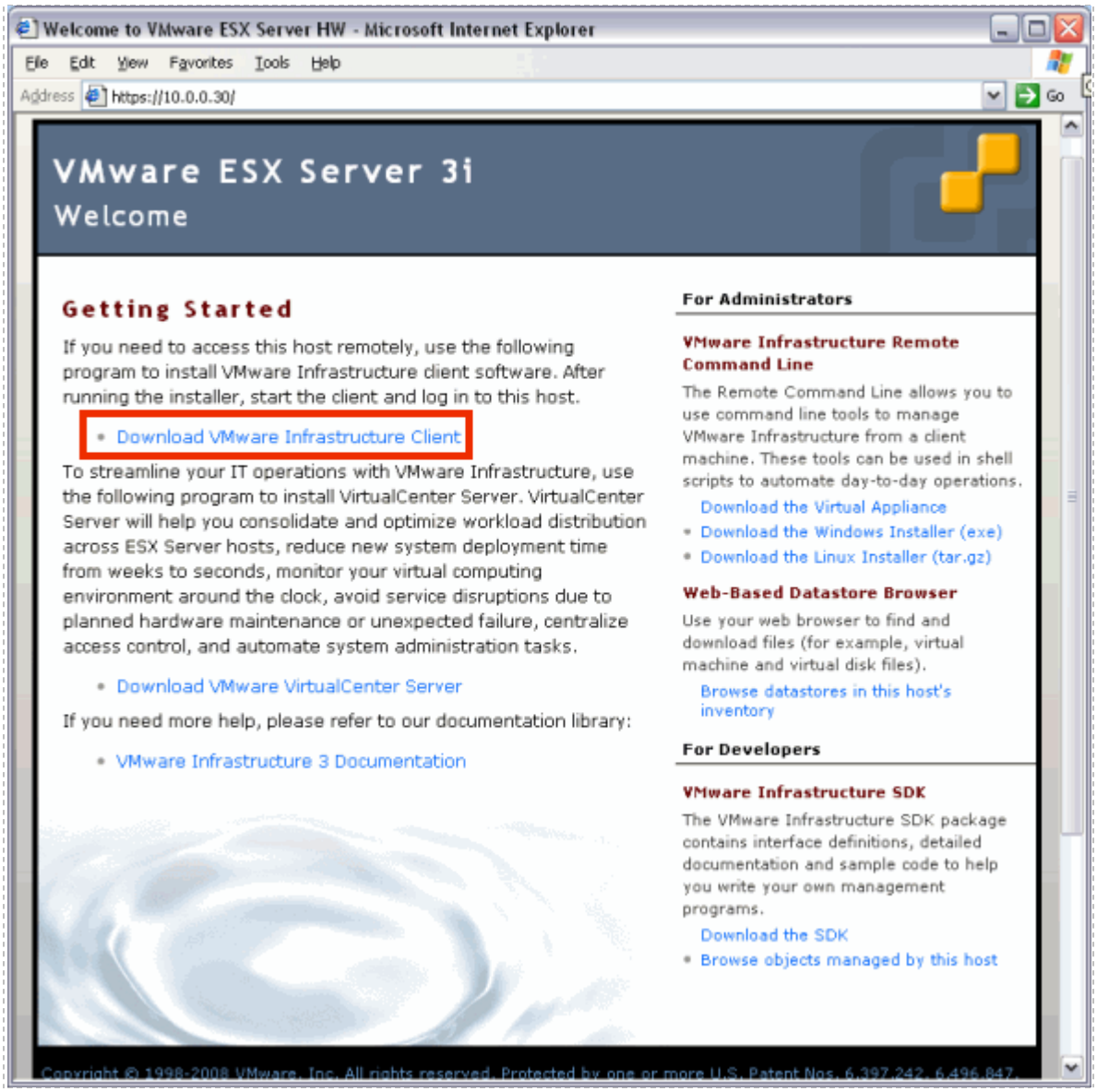
3.5 Verifying and Managing the ESXi Host Using VI Client

As discussed in section 2.4, if you are using ESXi 4.01, you will use the vSphere client, instead the VMware Infrastructure Client (VI Client) as described this section. The functionality is the same for both software versions.

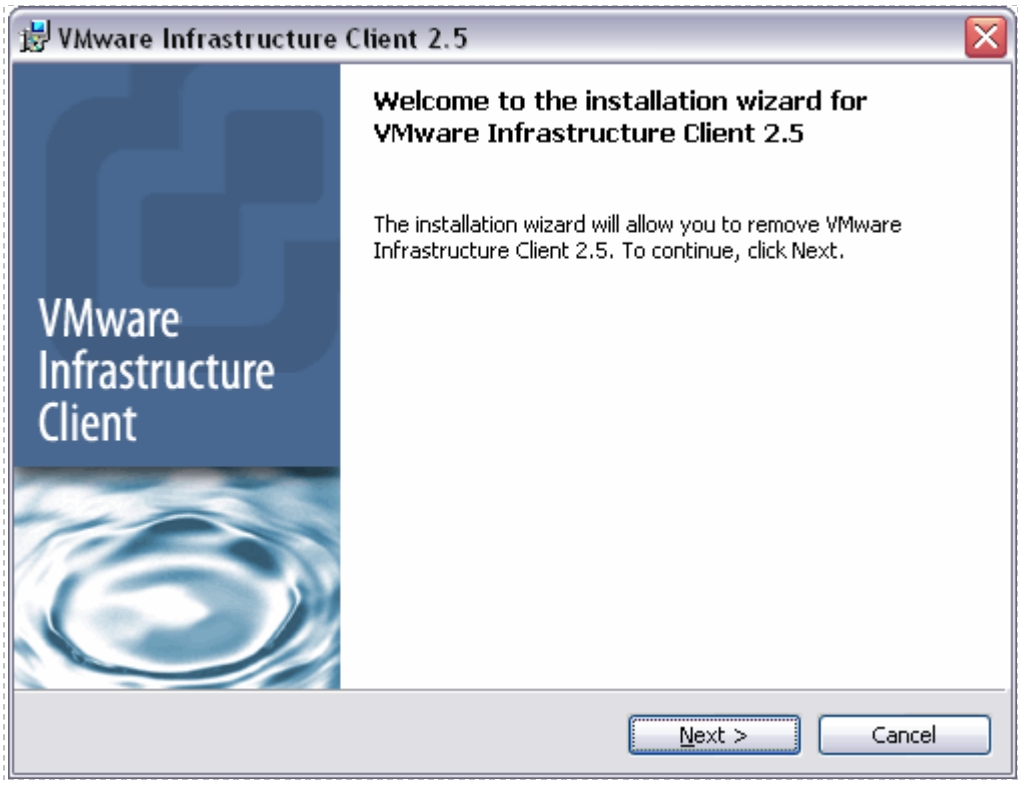
For details on installing the vSphere client, please refer to the *Install the vSphere Client* section of the *Getting Started with ESXi Server Installable* guide.

You will manage your ESXi host using the VMware Infrastructure Client (VI Client). This client software may be installed on any windows based computer on your network that has access to your ESXi server through the outside interface (see section 3.4).

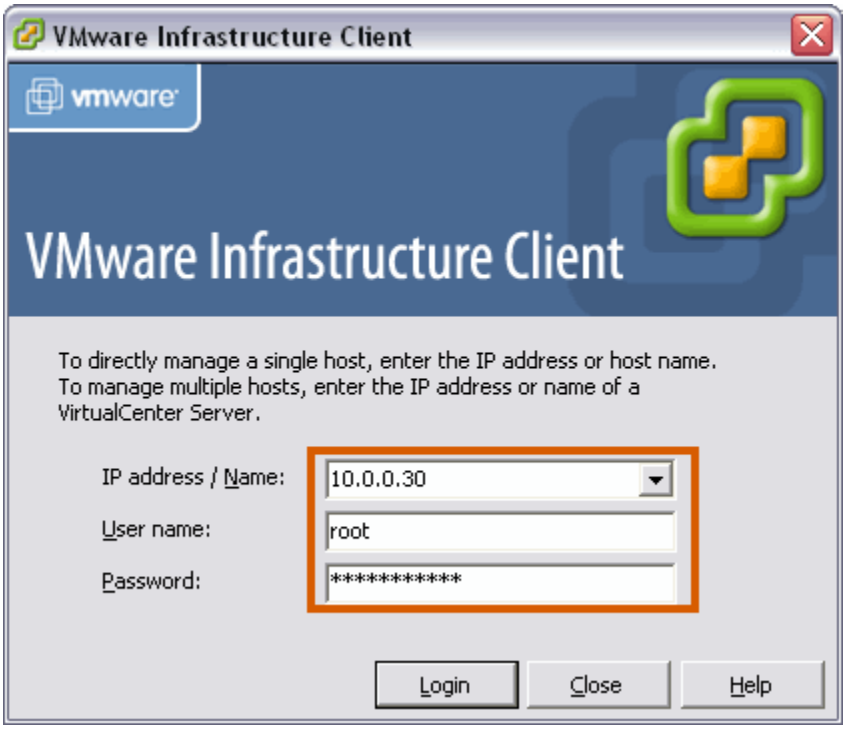
Open a web browser and enter the IP address of your ESXi server. If you have properly configured your outside interface, you will view the ESXi server's static web page.



Select the **Download VMware Infrastructure Client** link to download the client software. Download and run the executable file on your local machine. The installation wizard will guide you through the installation process.



Enter the outside network address of the host, **root** as the user name, and password (if configured) to login to VMware Infrastructure Client (VI Client). The inside interface tasks in section 3.6 will be completed using the VI Client.



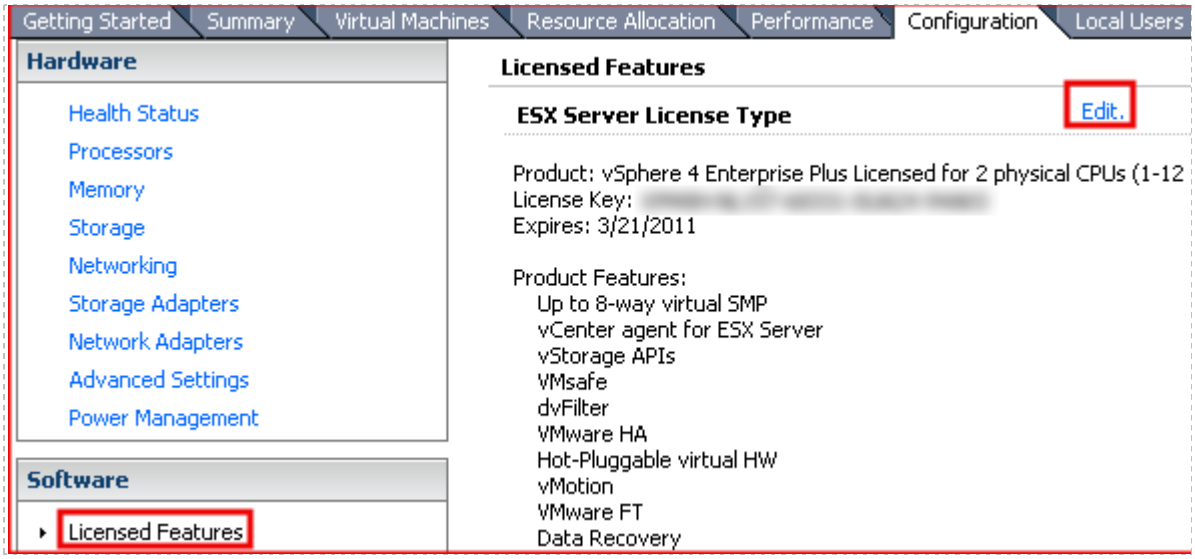
During initial login, a security warning may be displayed. This security-warning message occurs because the VI Client detected a certificate signed by the ESXi host itself (default setting). For highly secure environments, certificates generated by trusted third-party are recommended. You can set up third party certificates later if you choose.

3.5.1 Entering the ESXi License Key

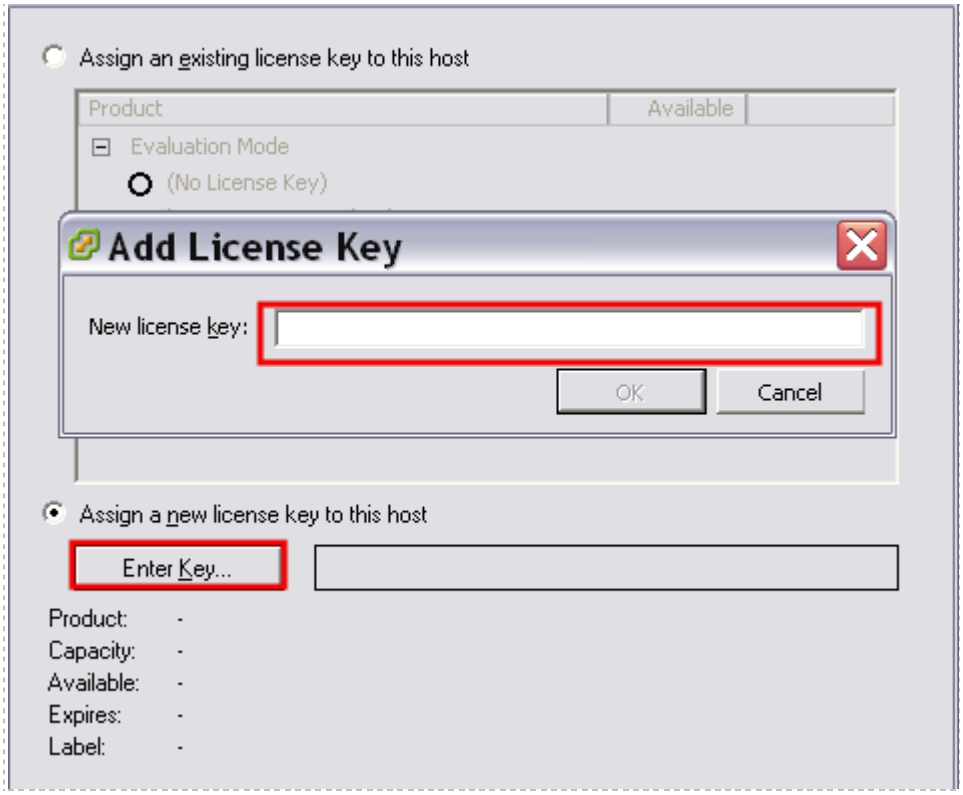
It is necessary to enter a license key in order to continue using ESXi beyond the evaluation period. If the key is not entered, you will be unable to use ESXi when the evaluation period is over. See section 3.1 for details on obtaining a license key.

The screen-shots shown here may vary slightly from your system, depending on the version of ESXi you are using.

1. Using the vSphere Client, select **Configuration > Licensed Features** and click **Edit** next to **ESX Server License Type**.



2. Select the option to **Assign a New License Key to this host**, enter the license key, and select OK.



3.6 Configuring the Inside Interface

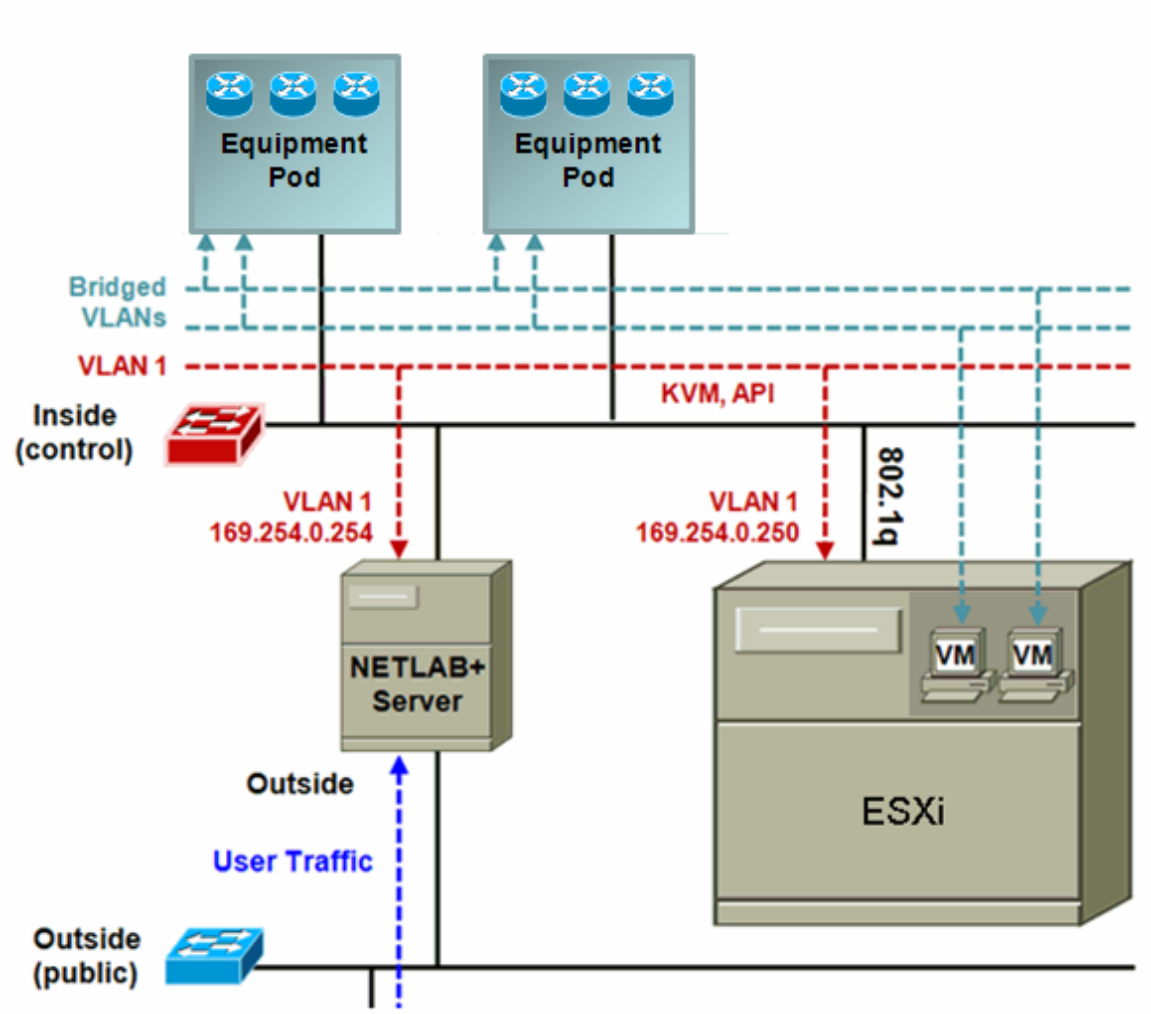
All virtual machine traffic (Bridging), KVM, and automation traffic (API) will take place through the inside interface using the IMAN networking mode. The Inside Interface is configured using VI Client.

- ESXi 3.5 users, please use the *ESX Server 3i Configuration Guide*, chapter 2, *Networking*, as a reference to aid in understanding the concepts and terminology involved.

- ESXi 4.01 users, please use the *ESXi Configuration Guide*, chapter 2, *Networking*, as a reference to aid in understanding the concepts and terminology involved.

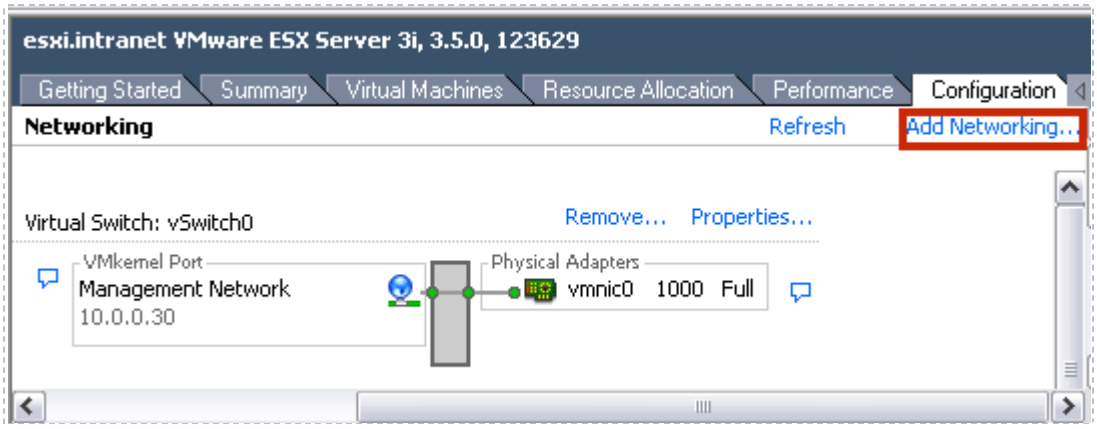
3.6.1 Understanding VLAN 1 and Bridged VLANs

The number of physical adapters required is greatly reduced by using VLANs. In the IMAN model, *VLAN 1* is used to transport KVM and API traffic between NETLAB+ and the ESXi host. *Bridged* VLANs are used to transport network data between virtual machines and real lab equipment. The Inside Physical Interface runs 802.1q and acts as container for VLANs. VLAN 1 corresponds to the native (untagged) VLAN on the control switch.



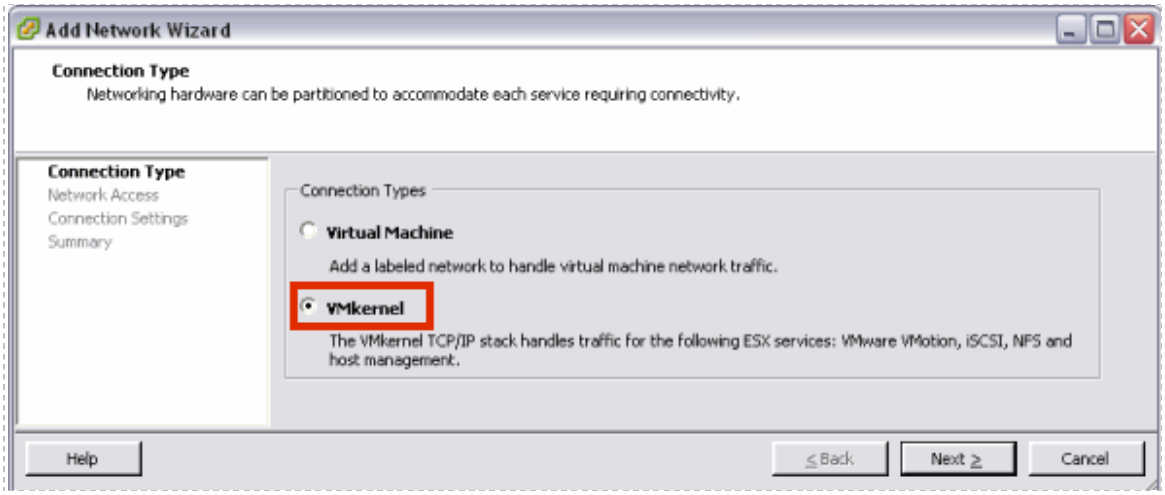
3.6.2 Adding a Virtual Switch

Select the Configuration tab on VI Client and click on the **Networking** section. You will see that your first virtual switch has been assigned a VMkernel Port, **Management Network**. This represents the connection you have established through the outside interface to allow you to use VI Client to manage your ESXi server. A virtual switch must be added for the inside connection. Select **Add Networking** to start the **Add Network Wizard**.



3.6.2.1 Selecting the VMkernel Connection Type

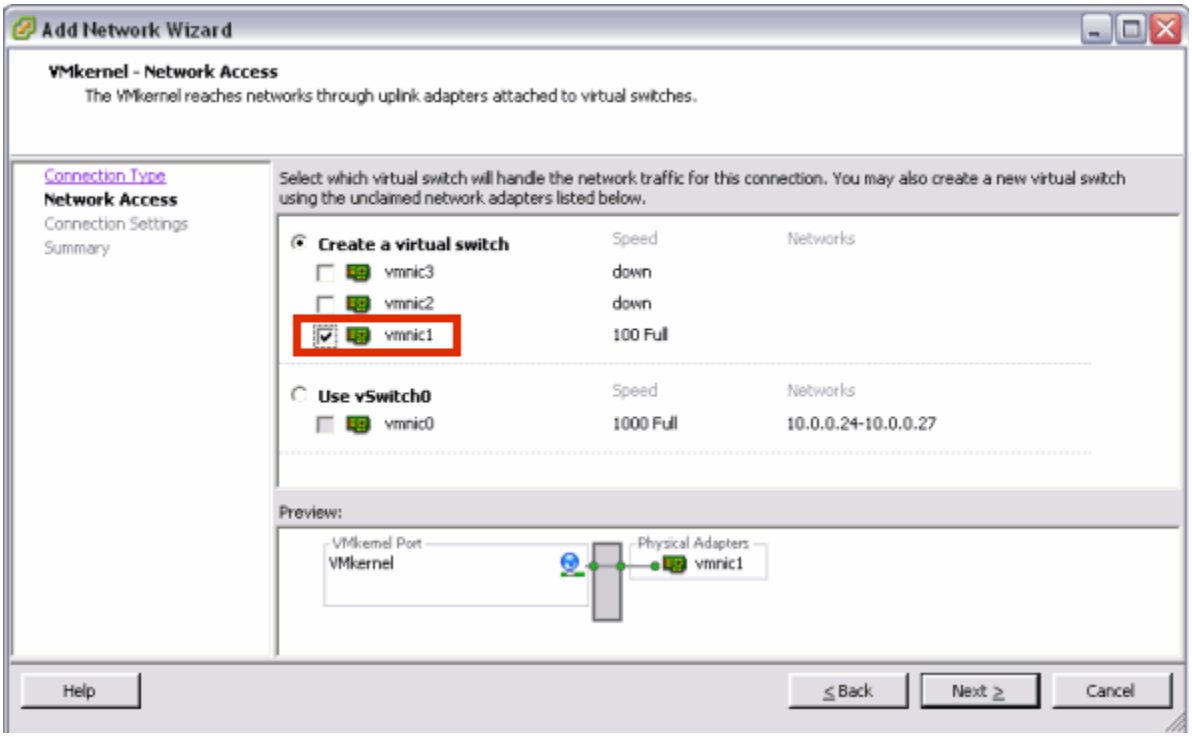
Use the **VMkernel** connection type for the Inside Interface.



3.6.2.2 Selecting the Network Adapter

As noted in the hardware requirements (section 2.2), your server must have at least 2 NIC cards. The Inside Interface and Outside Interface must be on different virtual switches. In this example, vmnic1 has been selected for the inside interface, (the outside interface is on vmnic0, as shown in section 3.4).

The selection and number of network adapters on your system will vary depending on your hardware selections.

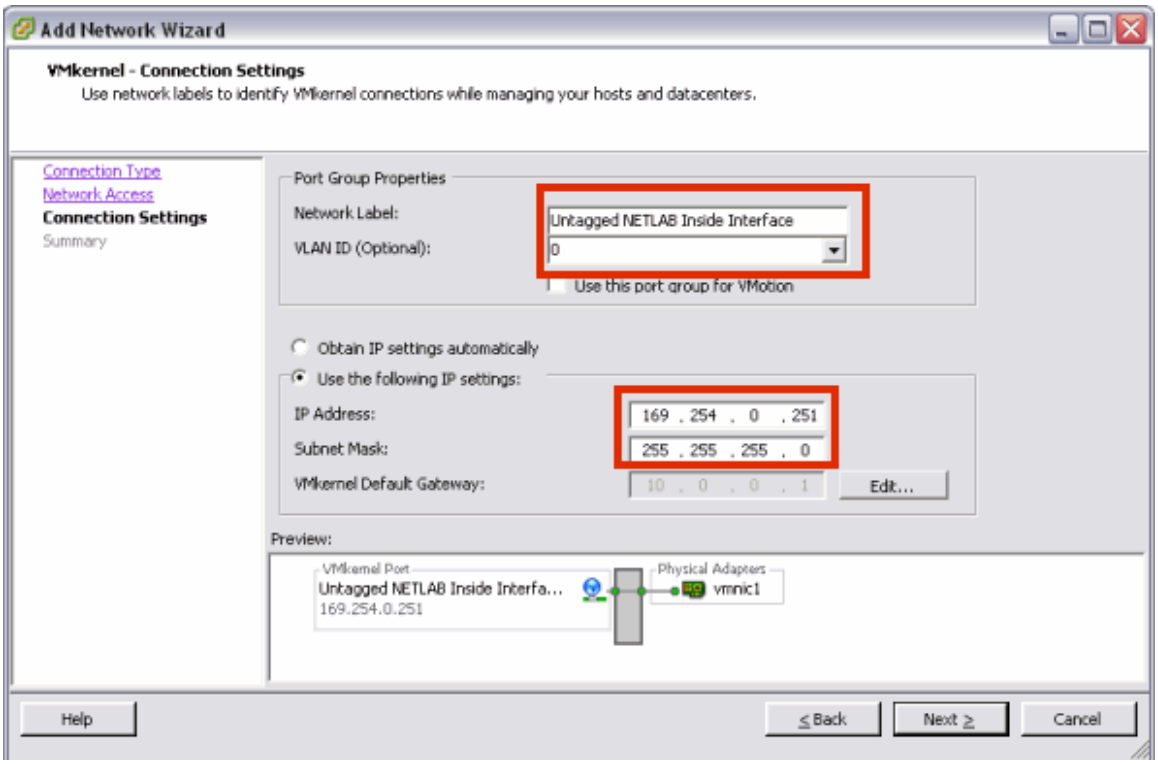


3.6.2.3 Selecting Connection Settings

Enter **"Untagged NETLAB Inside Interface"** as the Network Label. The **VLAN ID** should be set to **"0"**.

Configure the TCP/IP settings for the Inside Interface using the table on the next page.

- Do not use the same IP address on more than one server.
- Do not use 169.254.0.254 (this is assigned to the NETLAB+ server)

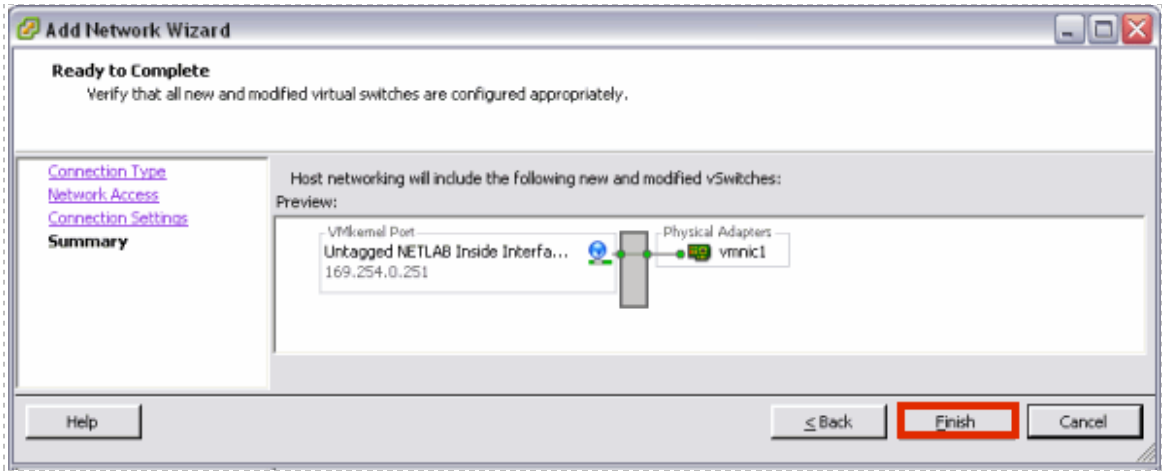


Use this table to select the appropriate IP settings.

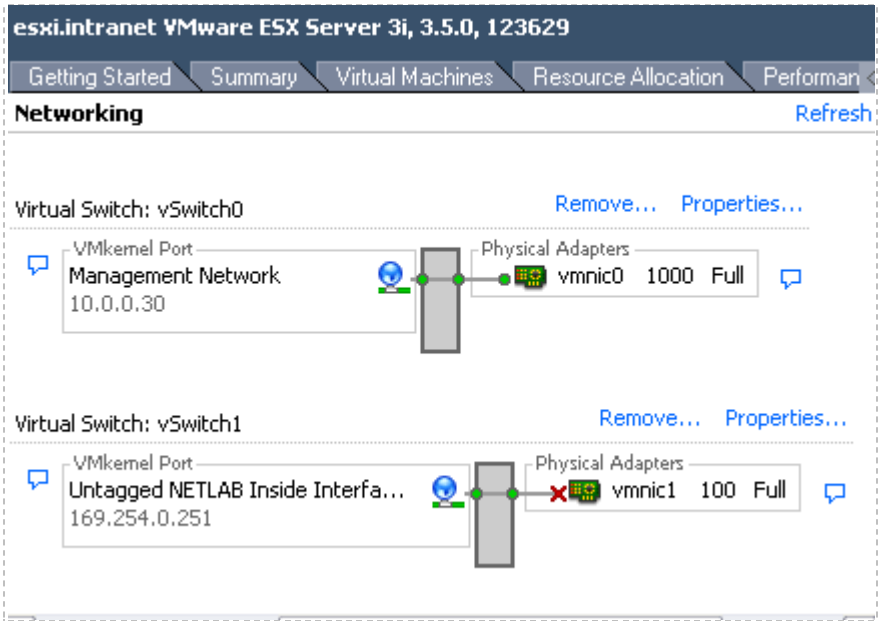
ESXi Host Server > Untagged NETLAB Inside Interface > TCP/IP Properties		
IP Configuration Interface	**VLAN 1** (untagged VLAN sub-interface)	
IP Address	**169.254.0.250**	1st server
	169.254.0.251	2nd server
	169.254.0.252	3rd server
	169.254.0.253	4th server
	169.254.0.254	**NETLAB+ … DO NOT USE**
	169.254.0.240 … **169.254.0.249**	5th server … 14th server
Subnet Mask	**255.255.255.0**	
Default Gateway	**None** (leave blank)	
Preferred DNS Server	**None** (leave blank)	
Alternate DNS Server	**None** (leave blank)	

3.6.2.4 Finishing the Configuration of the Virtual Switch

Select **Finish** to complete the configuration process.



Your new virtual switch is now displayed on the networking page. Notice the ✖ mark displayed near vmnic1, this indicates that the connection has not yet been physically cabled. Cable your connection and the ✖ will be removed.



3.6.3 Adding a VLAN3 Placeholder

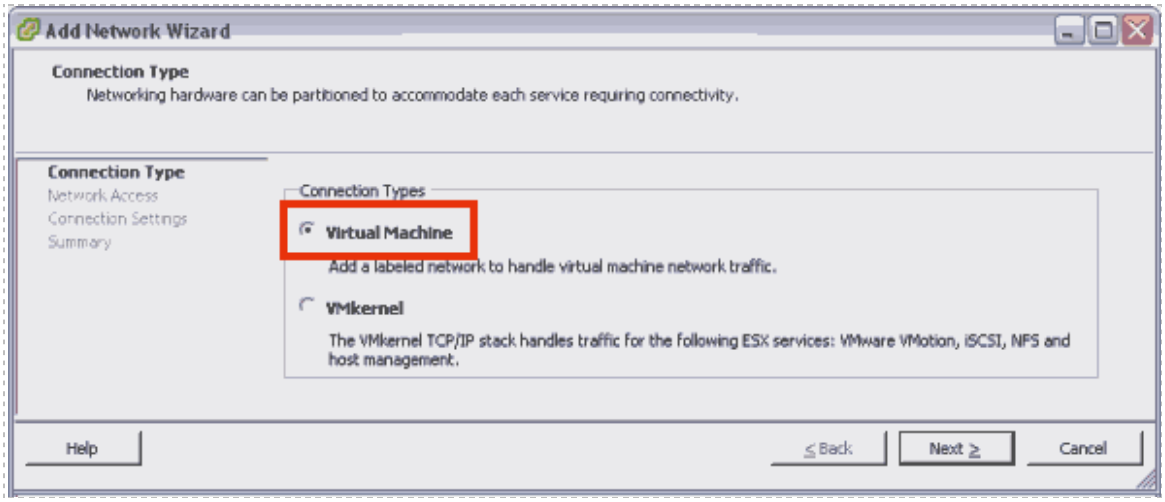
Add a VLAN3 placeholder, which will serve as the first virtual machine network connection type. This placeholder is necessary since at least one VM network connection type must be present prior to adding your first virtual machine (see Part 4). It will not be possible to create a virtual network adapter for your virtual machines without this placeholder.

Placeholder VLAN3 also serves as an example of how you will later add VLAN adapters for your pod VMs (section 5.2). After you have added VMs and pod VLANs to the Inside Interface, you may delete this placeholder (section 5.4).

Begin by selecting **Add Networking** to start the **Add Network Wizard**.

3.6.3.1 Selecting the Network Connection Type

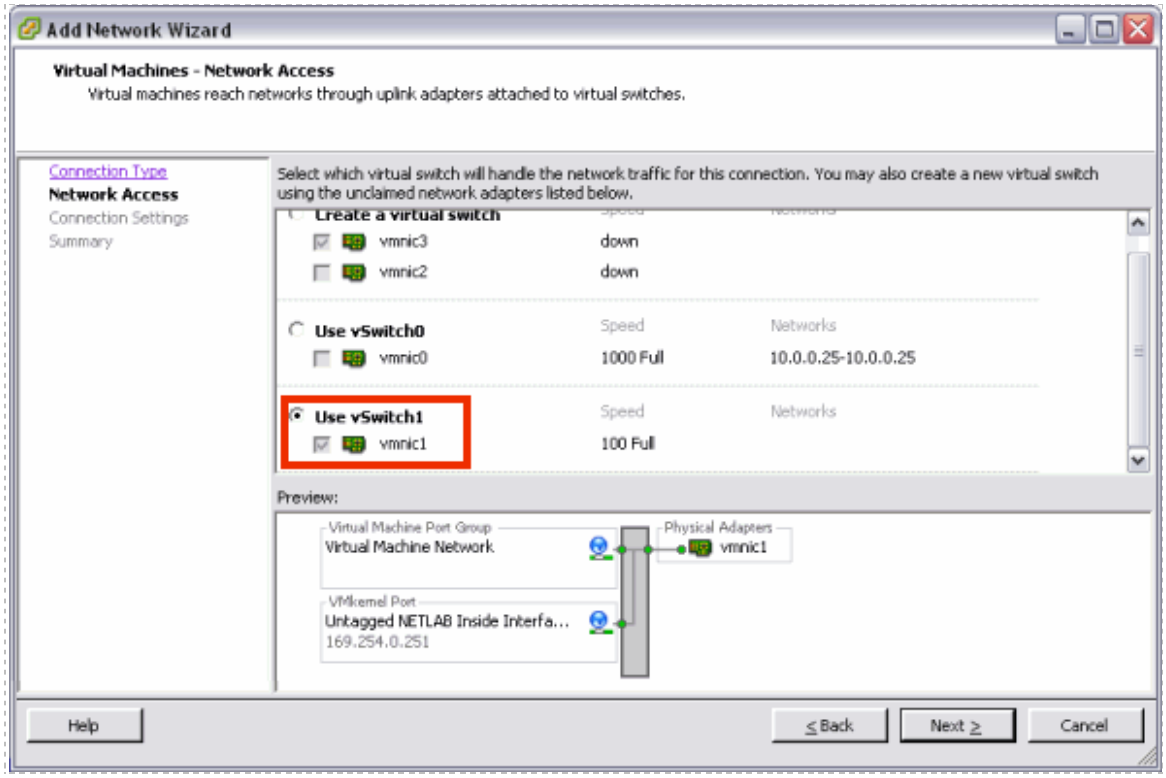
Use the **Virtual Machine** connection type for VLAN3.



3.6.3.2 Selecting the Network Adapter

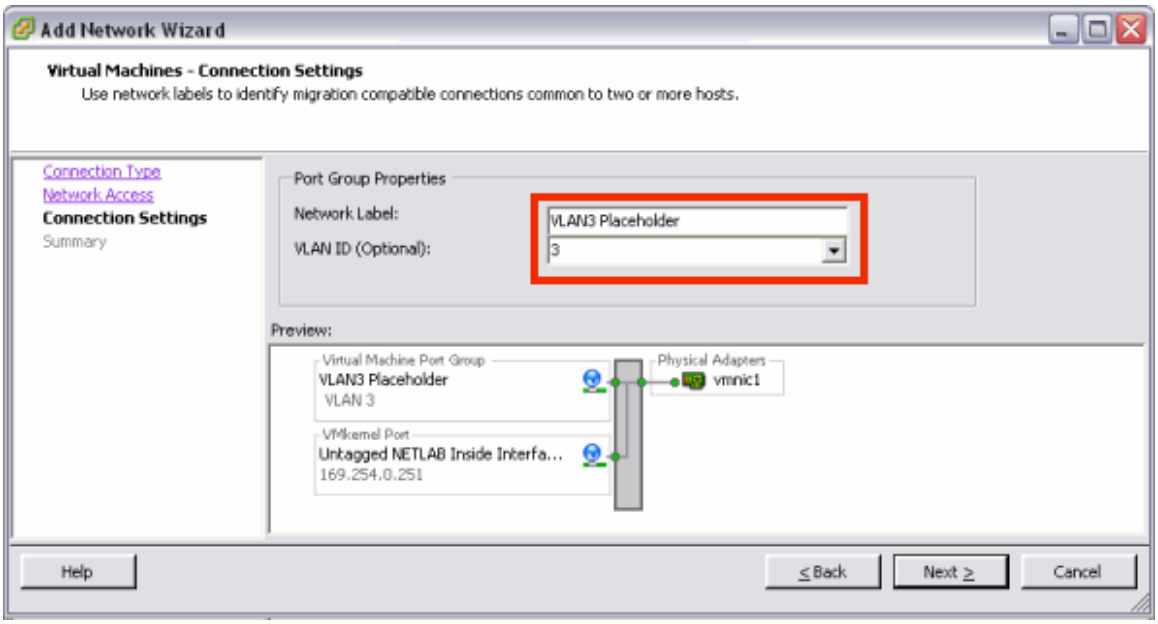
Placeholder VLAN3 must be assigned to use the same virtual switch as the Inside Interface. In this example, vmnic1 was selected for the Inside Interface (see section 3.6.2.2); therefore, the VLAN3 placeholder must also be assigned to vmnic1.

The selection and number of network adapters on your system will vary depending on your hardware selections.



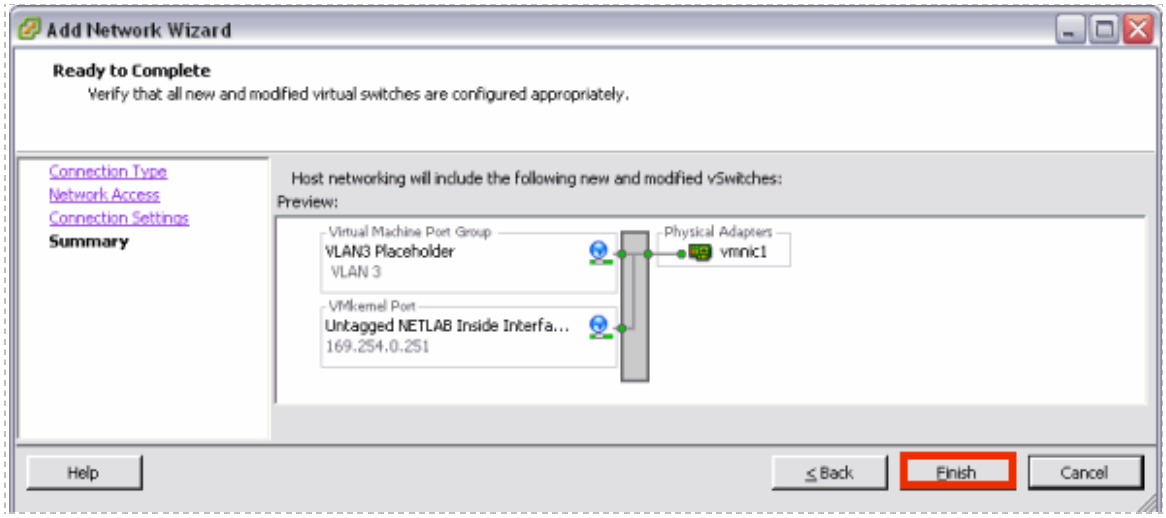
3.6.3.3 Selecting Connection Settings

Assign **"VLAN3 Placeholder"** as the **Network Label**. Enter **"3"** as the **VLAN ID**.

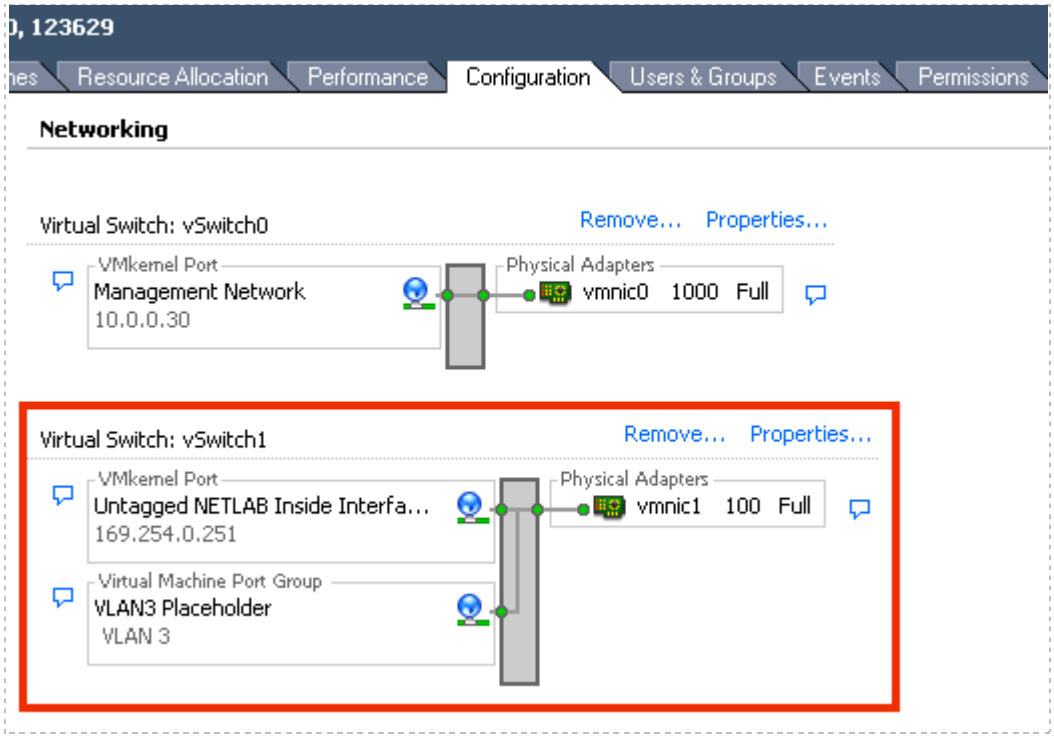


3.6.3.4 Finishing the Configuration of the VLAN3 Placeholder

Select **Finish** to complete the configuration process.



The **VLAN3 placeholder** is now displayed on the networking page. Note that VLAN3 is on the same virtual switch as the Inside Interface.



3.6.4 Establishing the Inside Connection

In this section, you will establish a connection between the ESXi host inside port and NETLAB+ server.

Objectives

- Select a reserved control switch and port.
- Configure the control switch port.
- Bring up the link.
- Verify ESXi host system can connect to NETLAB+ using VLAN 1.

3.6.4.1 Allocating a Reserved Port on Control Switch for Inside Connection

There are several issues to keep in mind when selecting a reserved port. Remember that reserved ports operate in VLAN 1, so there are no consecutive port requirements. Typically, when installing control devices, it is desirable to connect NETLAB+, access servers, switched outlet devices, and all other control switches to Control Switch 1, in a hub and spoke fashion. Please refer to the *Installing the Control Plane* section of the *NETLAB+ Installation Guide* for detailed discussion of reserved ports and control devices.

For each ESXi server you install, the inside connection may be located on any reserved port that is available on a control switch. In most cases, you may have more than one control switch and ESXi server. If this is the case, you should try to select a reserved port from the same control switch where the pods associated with the ESXi server reside. In some circumstances, your ESXi server may be hosting several pods. Consequently, the reserved port may be located on a different control switch, if all links between control switches are also configured as 802.1q trunks and all VLANs are allowed. The most important factor would be keeping the pod gear communication and ESXi server communication located on one or two control switches.

3.6.4.2 Configuring a Reserved Control Switch Port for Inside Connection

One reserved port on the control switch connects to an 802.1q NIC card on the ESXi server. This allows devices in the pod to communicate with virtual machines. The reserved port should be configured as an 802.1q trunk port.

Once you have allocated a reserved port on the control switch, connect the ESXi server inside NIC using a straight through CAT5 cable. Configure the switch port as a trunk.

Example switch port configuration. Interface number will vary.

```
interface FastEthernet0/23
 description inside connection for ESXi Server #1
 switchport mode trunk

 switchport nonegotiate
 no switchport access vlan
 no shutdown
```

The control switch console password is **router**. The enable secret password is **cisco**. These passwords are used by NETLAB+ automation and technical support - please do not change them.

3.6.4.3 Configuring Trunking Between Multiple Control Switches

If the reserved port selected for your ESXi server is on a different control switch than the lab equipment pods it is serving, you must ensure that inter-switch links between control switches are configured in trunking mode. Some switch models will automatically form trunks. However, it is recommended that both sides be manually configured as trunk ports per the configuration commands below.

Example switch port configuration. Interface number will vary.

```
interface FastEthernet0/24
 description Trunk to control switch #2
 switchport mode trunk

 switchport nonegotiate
 no switchport access vlan
 no shutdown
```

3.6.4.4 Connecting the Inside Interface and Verify Link

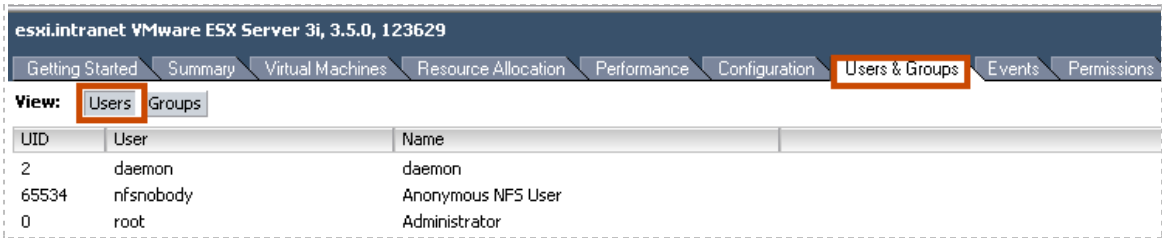
After you have configured the reserved the port as described in the previous section, verify your cabling between the reserved port and the ESXi server inside NIC. Check the interface status of the reserved port:

```
netlab-cs1#show interfaces FastEthernet 0/23
FastEthernet0/23 is up, line protocol is up (connected)
```

3.7 Creating a NETLAB+ User Account

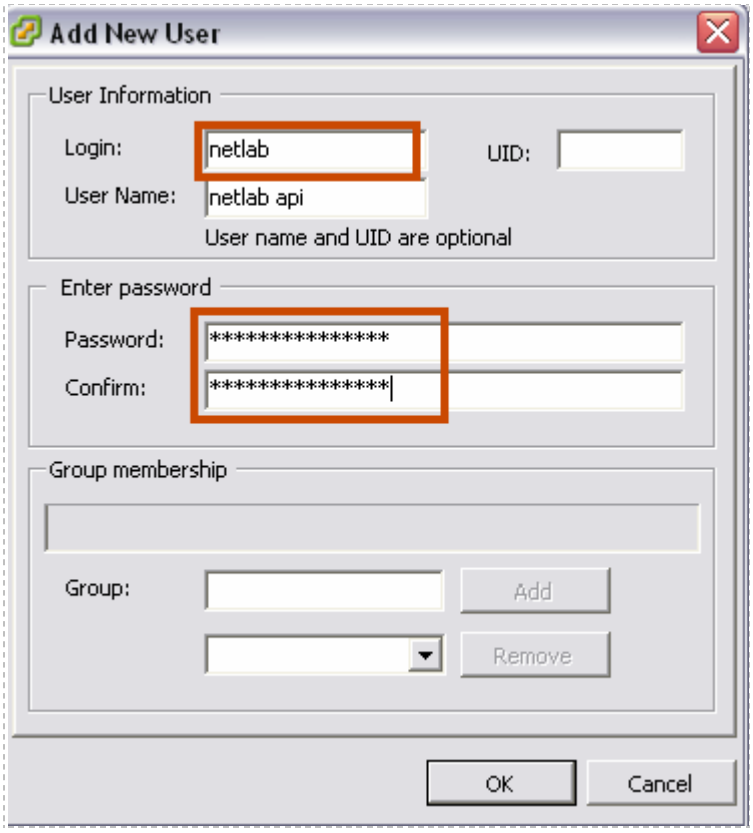
A NETLAB+ user account must be created on the ESXi host, using VI Client. NETLAB+ will use this account to control virtual machines through the VMware API.

Users & Groups → View **Users** → ***Right-Click*** on the page→ **Add**



The recommended login is **netlab**. You may also enter a user name (optional). You must enter a password for this account. We recommend choosing a strong password.

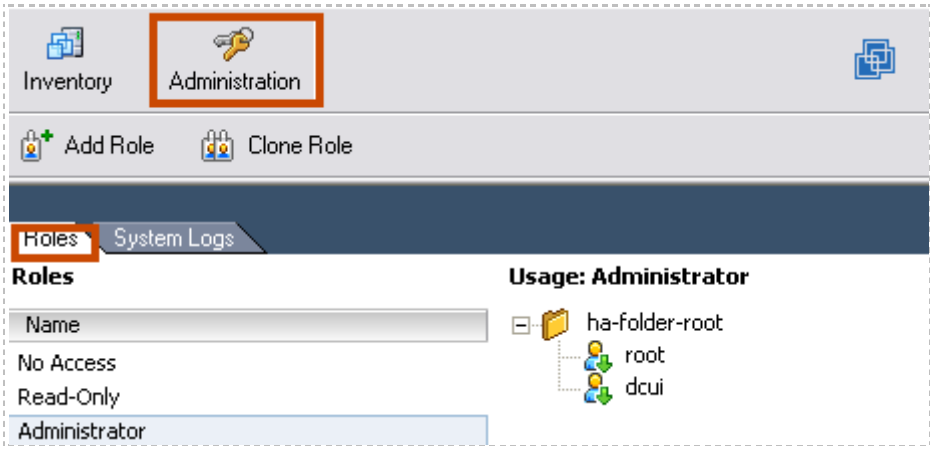
Make note of the login and password you assign to this user account. You will need to enter this information as PC configuration settings in section 4.10.



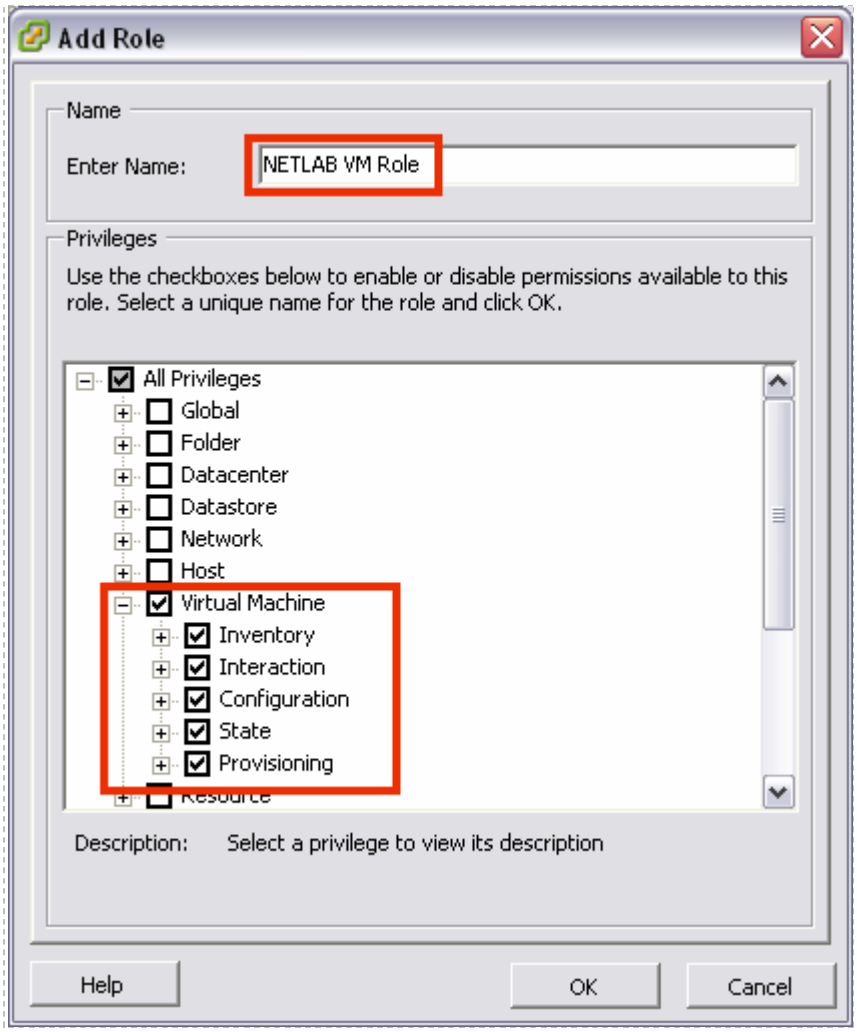
3.8 Creating the NETLAB VM Role

Roles are a combination of access permissions that can be assigned to a user or group. VI Client includes several preconfigured roles, including Administrator. You will create a role that will be assigned to your NETLAB+ user account (section 3.7). Assigning this role, with the proper access permissions configured, will allow NETLAB+ to access virtual machines through the VMware API.

Administration → **Roles** → ***Right-Click*** on the page→ **Add**

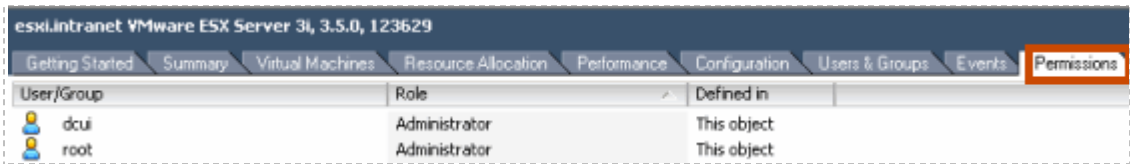


Add the **"NETLAB VM Role"** role and select the **Virtual Machine** checkbox. This will enable permissions for the **NETLAB VM Role** for all virtual machine permission subcategories.

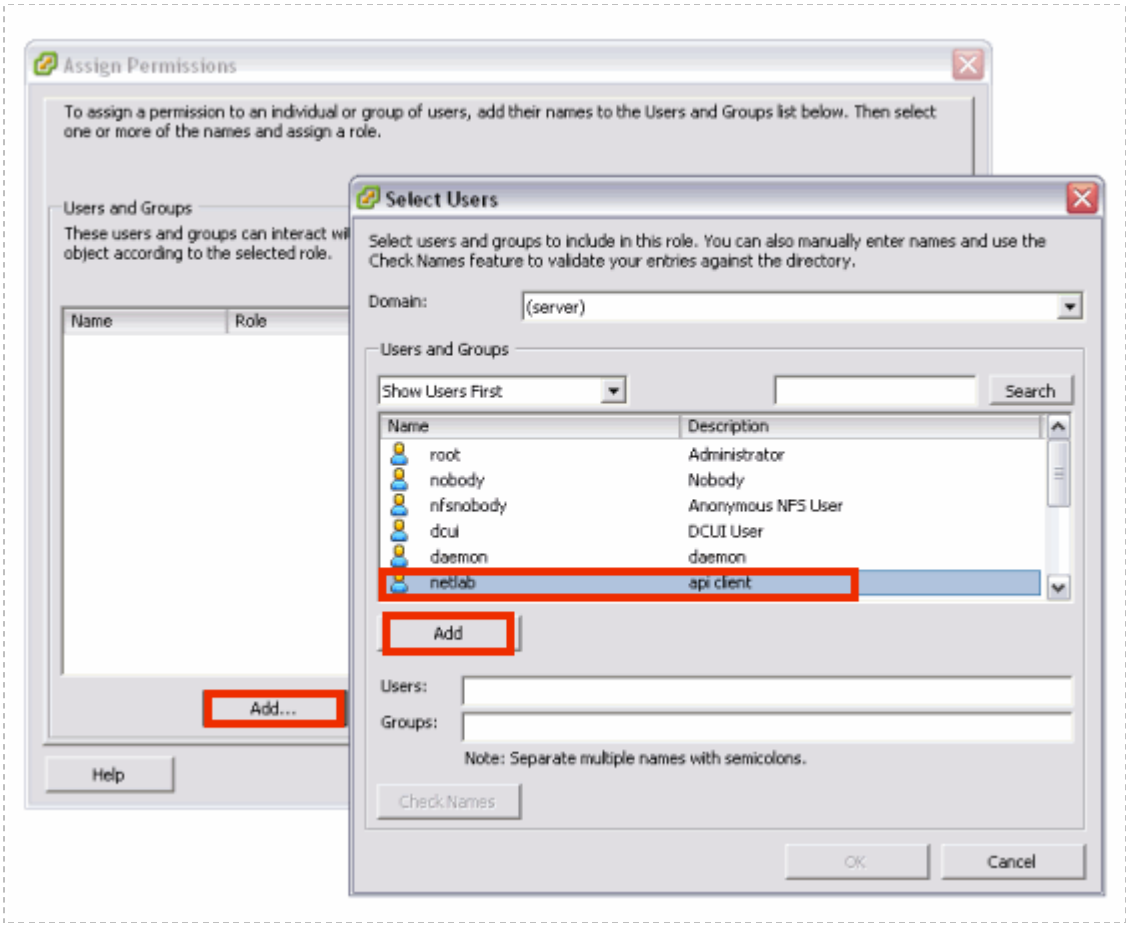


3.9 Assigning Permissions to the NETLAB+ User Account

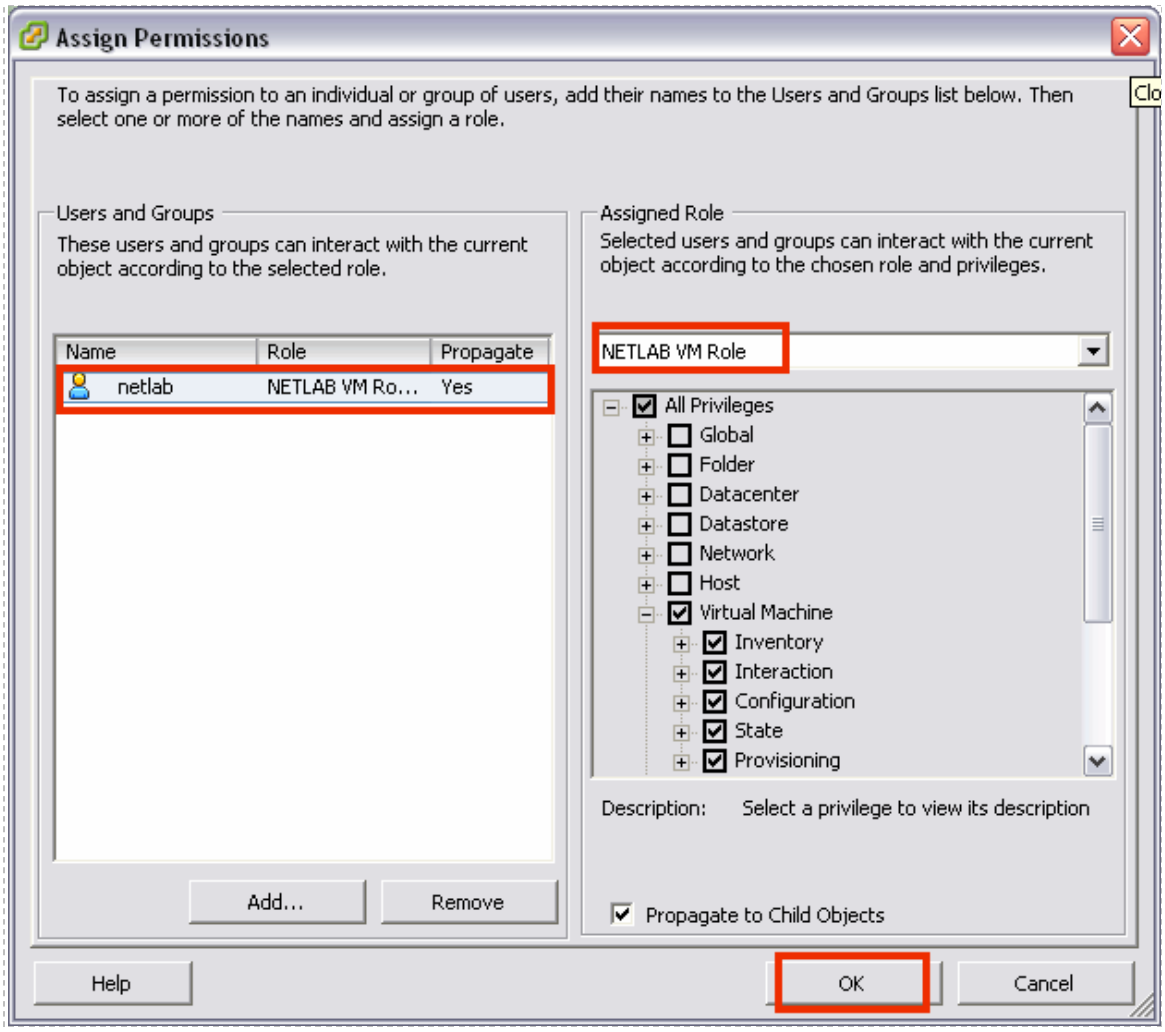
Assign virtual machine permissions to the NETLAB+ user account created in section 3.7 by assigning it to the role created in section 3.8.



- **Permissions** → ***Right-Click*** on the page → **Add Permission** → **Add** → select **netlab** user



The **netlab** user name will now appear in the users and groups list of the assign permissions page. Select the **NETLAB VM Role**, which has all virtual machine permissions, as defined in section 3.8.



Select **OK** to assign the **NETLAB VM Role**. You will see the User/Role assignment displayed.

Part 4 Adding Virtual Machines

This section explains how to configure a new ESXi virtual machine and the proper settings required for NETLAB+. Repeat this process for each new virtual machine.

After completing preparation of each host server as described in Part 3, virtual machines can be added (as *guests*) and integrated into the overall NETLAB+ system.

Objectives

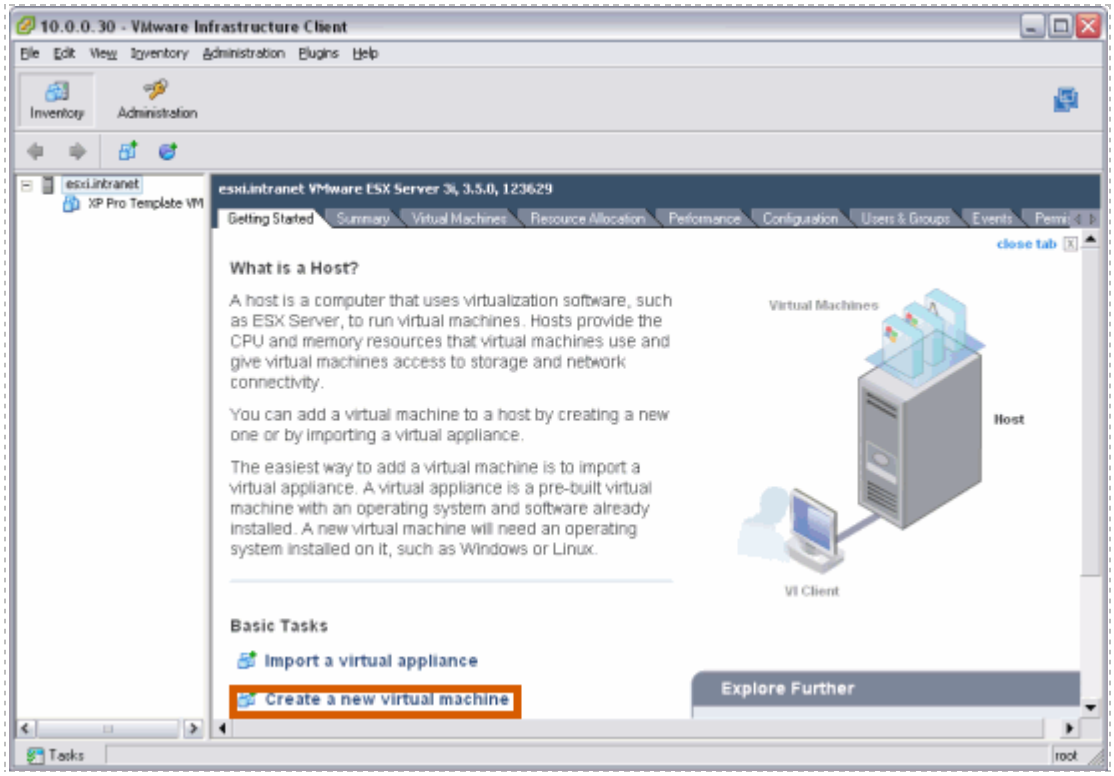
- Add virtual machines to the ESXi server host system.
- Make virtual machines accessible to NETLAB+ users.

The process outlined in this section must be followed for each virtual machine added to the system.

4.1 Creating a New Virtual Machine Using the VI Client

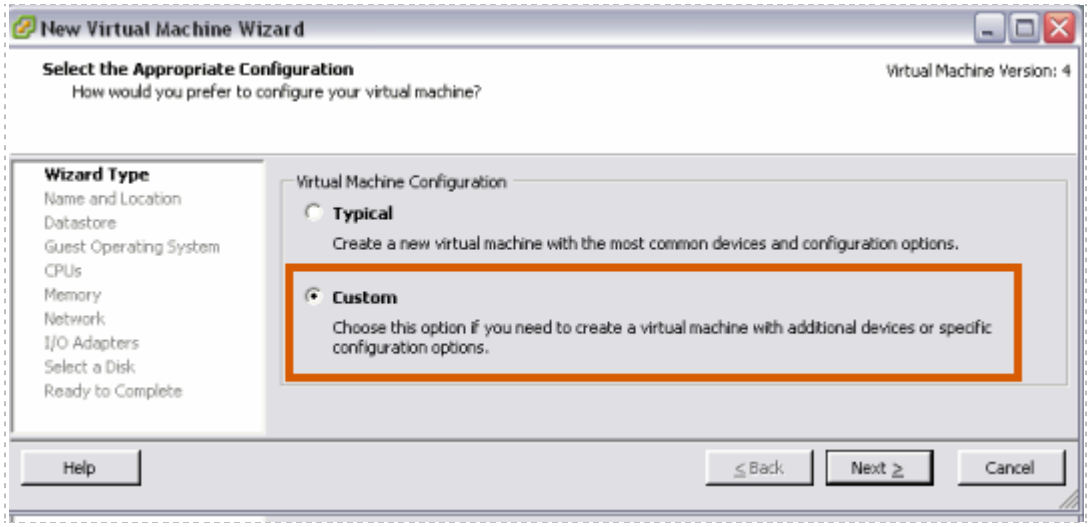
In section 3.5, you downloaded the VMware Infrastructure client to a machine connected to your outside interface. Enter the outside network address of the host, use **root** as the user name, and password (if configured).

The **Getting Started** tab includes a **Basic Tasks** section. Select the **Create a new virtual machine** option. The subsections below will provide information on each step you will need to follow using the **New Virtual Machine Wizard.**



4.1.1 Selecting the Custom Configuration Option

Select the **Custom** option for your virtual machine configuration.



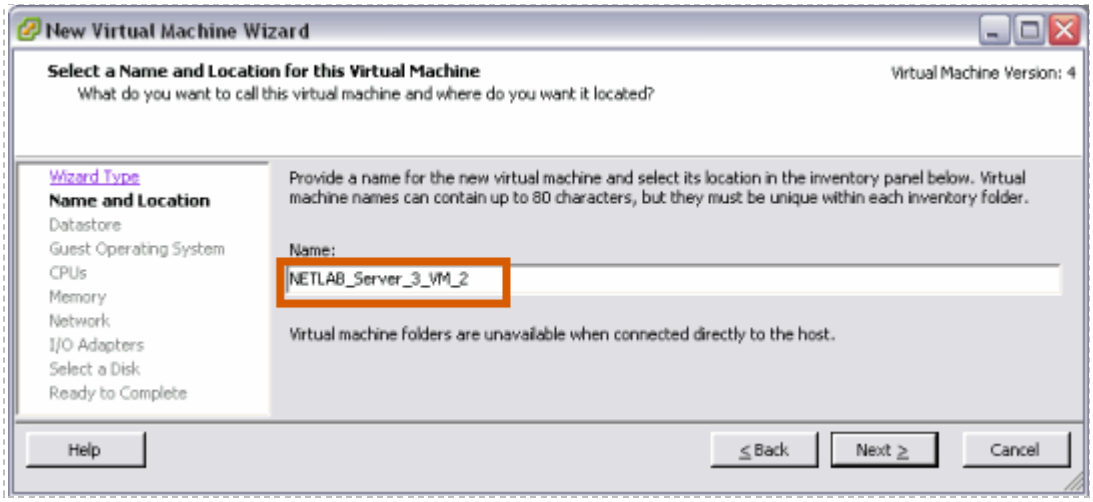
4.1.2 Providing a Name for Your Virtual Machine

You will be prompted to enter a name for your new virtual machine.

Choose a name for the virtual machine very carefully. Here are two recommended naming conventions to consider:

- [VM NAME] = [POD_*X*_ PC_*Y*]: If you do not plan on moving virtual machines from one pod to another, we recommend that you include the NETLAB+ pod number and/or PC ID in the name.

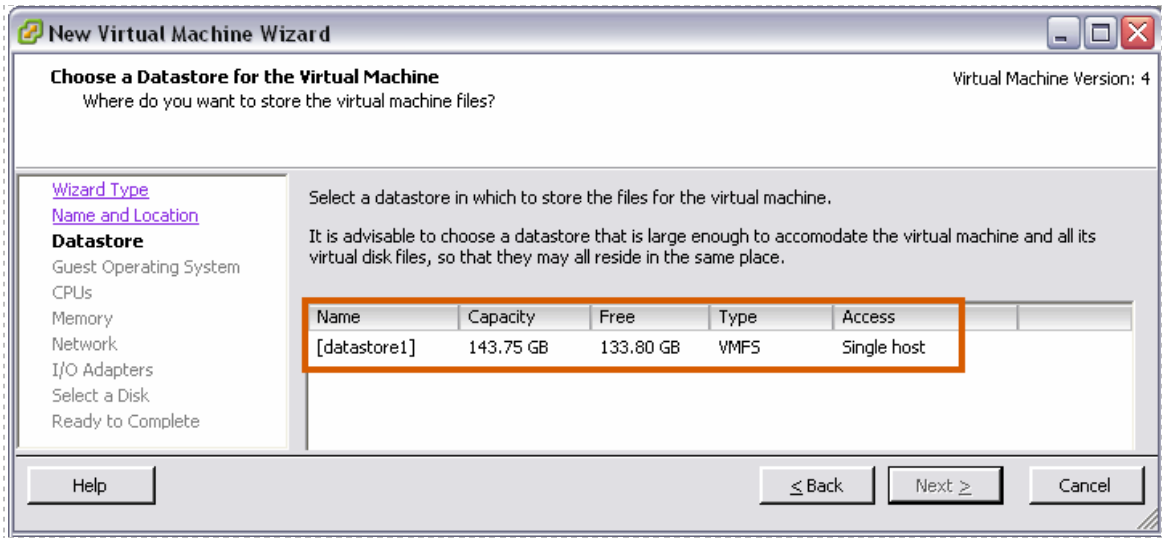
- [VM NAME] = [SERVER_*X* _VM_*Y*]: Another, more flexible naming convention would include the ESXi server number and virtual machine number. This method would be useful if you are going to be moving virtual machines from one pod type to another.



Since we have established a direct connection to the host, we will not be prompted to enter an inventory location. Select **Next** to continue.

4.1.3 Selecting a Datastore

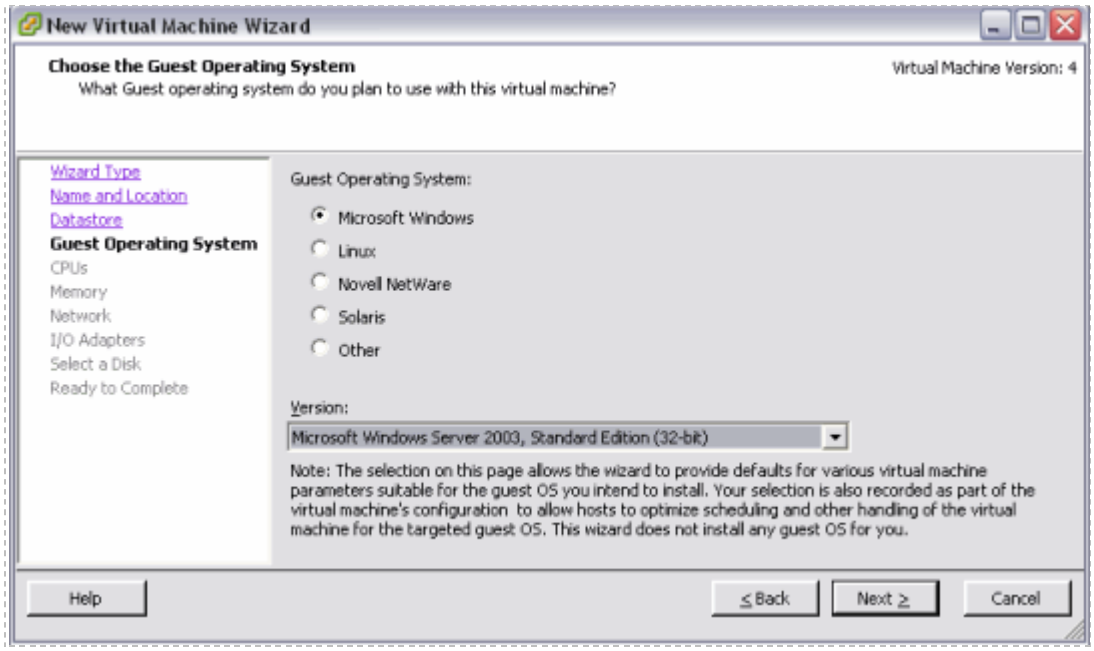
Virtual machine files are stored in a *datastore.* Select a datastore for the virtual machine that will be adequate to store the guest operating system and all of its software applications for pod labs.



4.1.4 Selecting the Guest Operating system

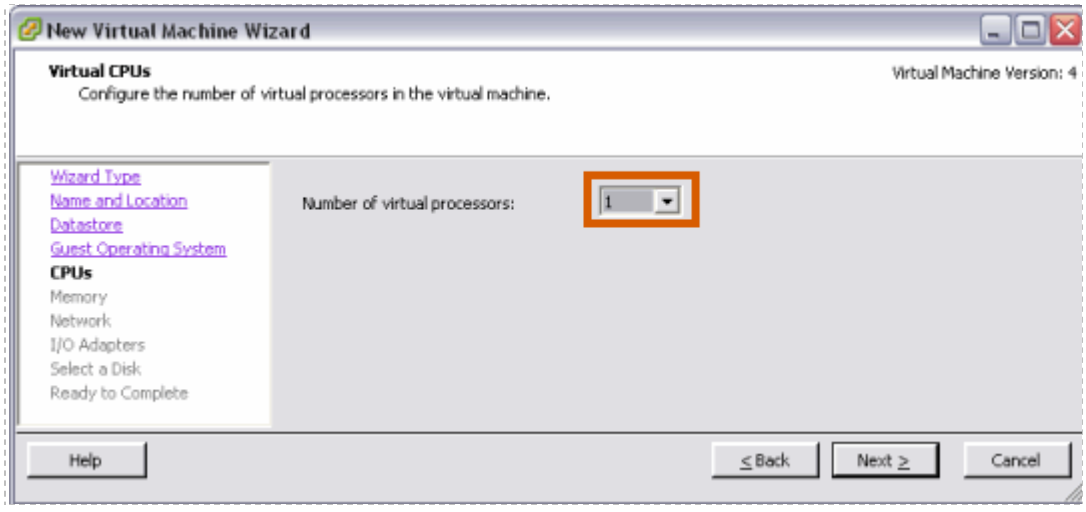
The Guest Operating system and version of your choice that you will install on the virtual machine must be selected.

In this example, Microsoft Windows Server 2003 is selected as the Guest Operating System.



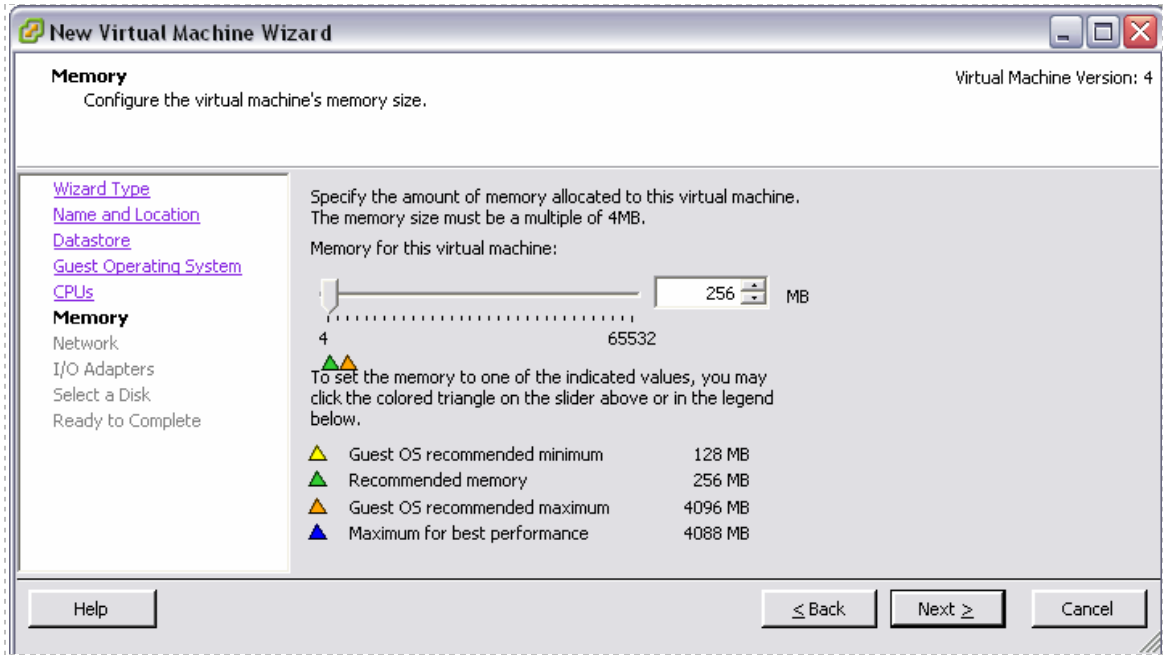
4.1.5 Selecting the Number of Processors

Selecting the default value of **1** for number of processors in the virtual machine is typically sufficient, depending on the applications you will run on the virtual machine.



4.1.6 Configuring the Memory Size

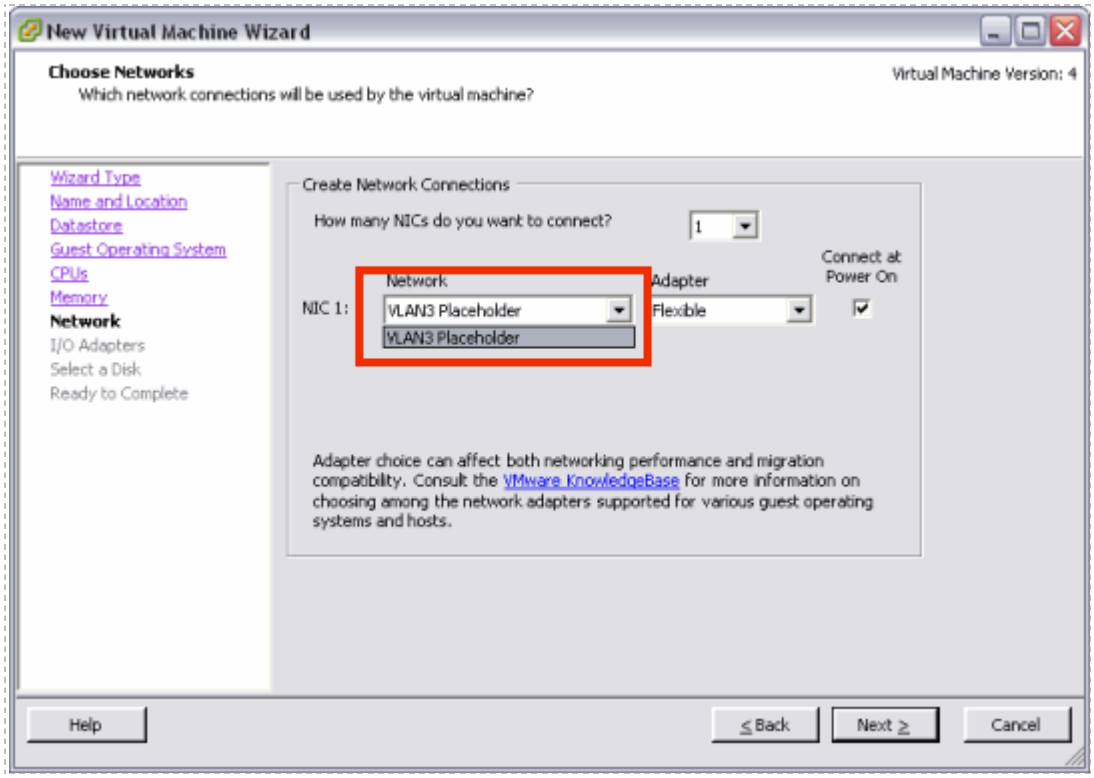
Choose the amount of physical memory that will be allocated to the virtual machine. In most cases, you may use the default settings for memory. If memory space is a concern, you may need to select a value closer to the recommended minimum. Please make sure you do not oversubscribe system resources (see section 2.1.4.3)



4.1.7 Choosing Network Connections

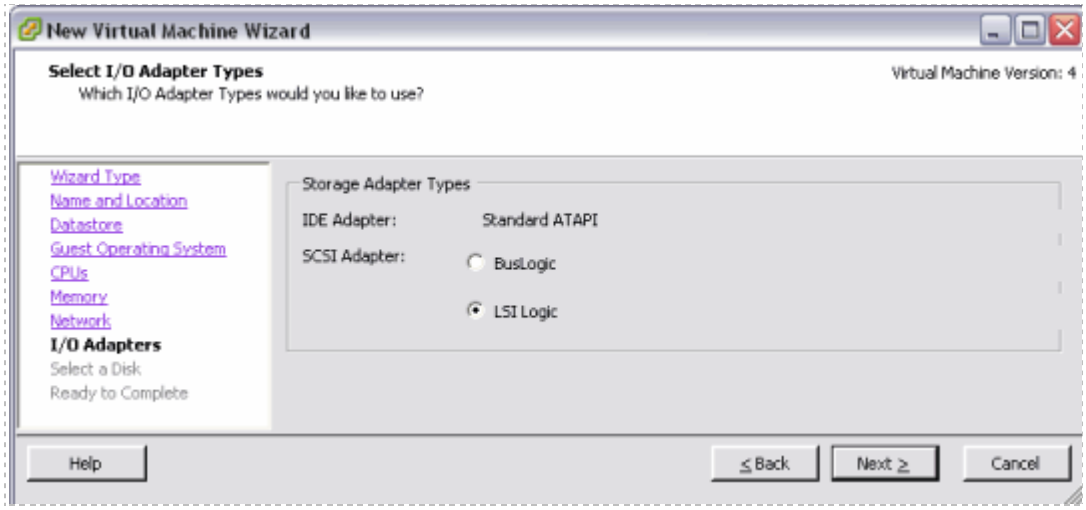
In most cases, it will be necessary to connect a Network Interface Card (NIC) to the virtual machine. (If your equipment pod will consist of only one individual PC, a Network Adapter is not necessary and number of NICs may be set to "None").

Establishing networking connections will be handled as a separate task in Part 5. For now, use the VLAN3 placeholder as your selection.



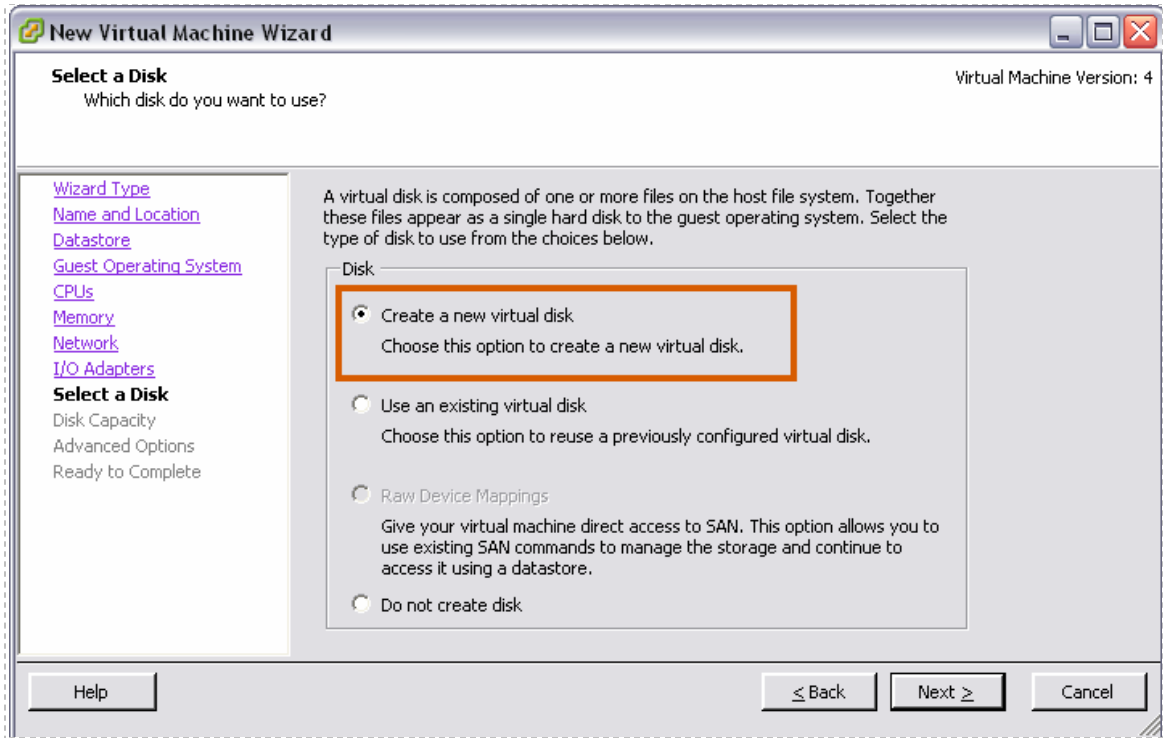
4.1.8 Selecting the I/O Adapter Types

In most cases, you may use the default setting for I/O adapter types. Be aware also of any requirements due to your selection of guest operating system (section 4.1.4).

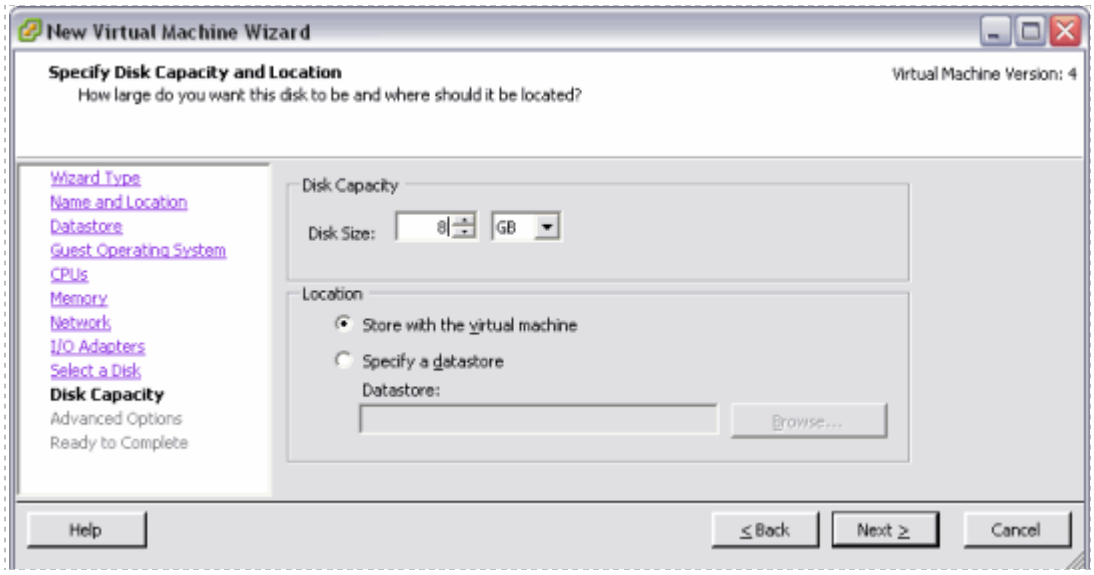


4.1.9 Creating a Virtual Hard Disk

Use the default settings to **Create a new virtual disk** for your virtual machine.



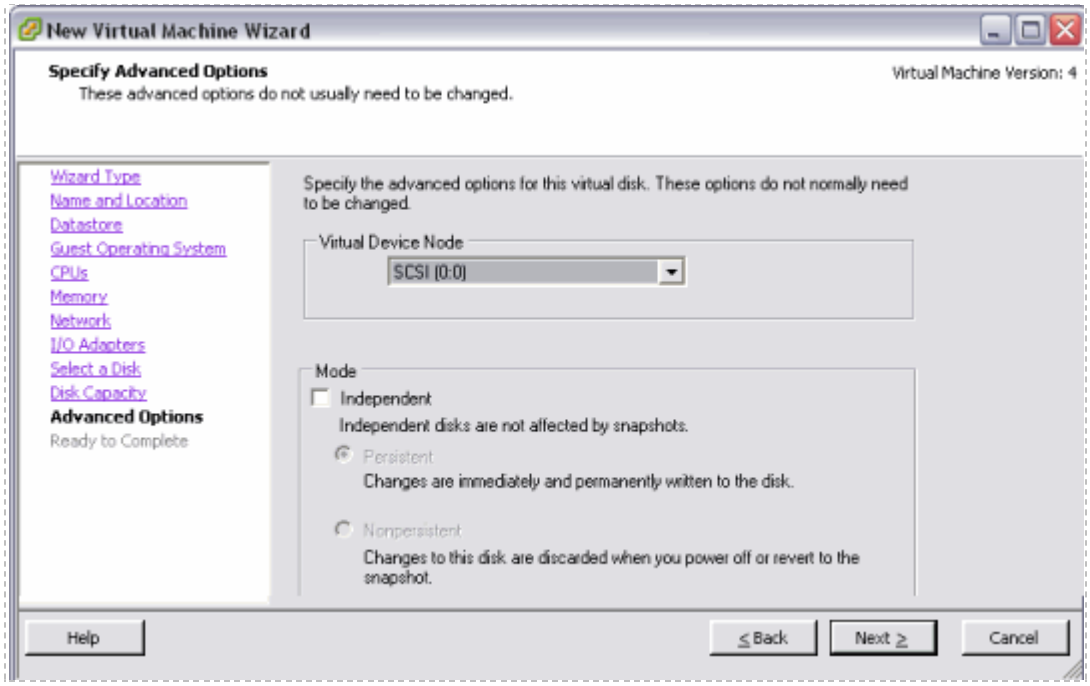
Specify the disk capacity for this virtual machine. Select a disk size that will be adequate to store the guest operating system and all of its software applications for pod labs. The example below shows a selection of 8GB; your requirements may vary.



4.1.10 Specifying Advanced Options

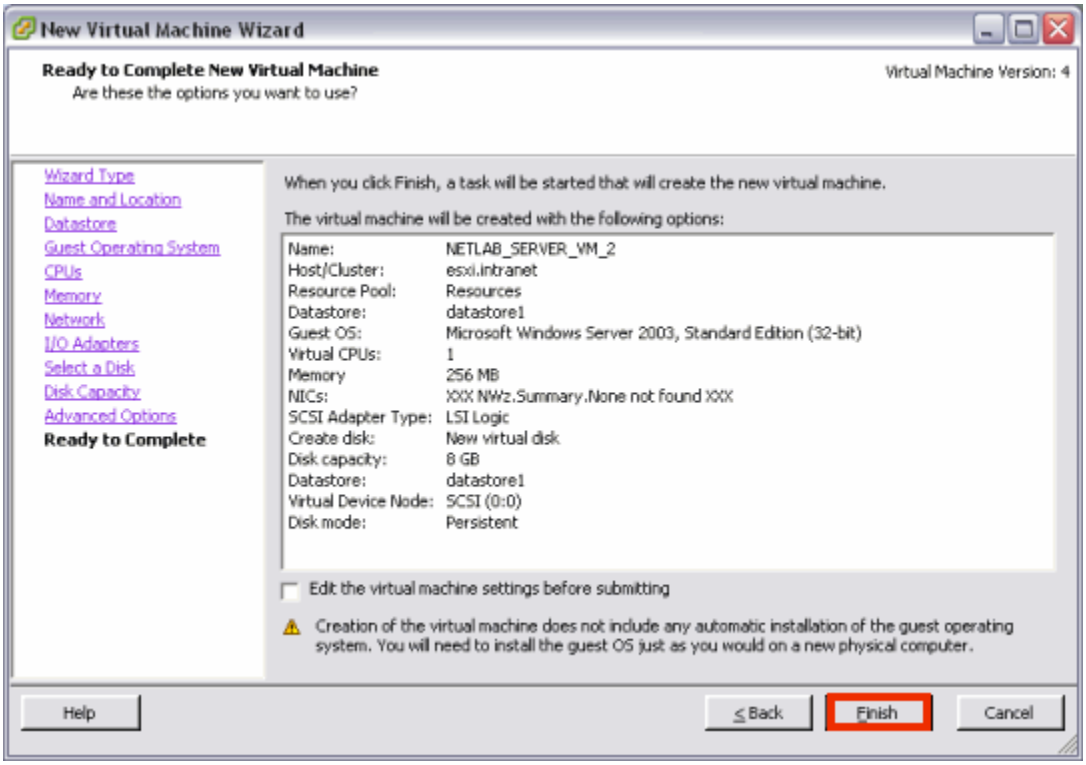
In most cases, you may use the default settings for the **Advanced Options**.

The use of SCSI drivers in a Windows XP or Windows Server 2003 virtual machine requires a special SCSI driver. You may download the driver from the VMware website.

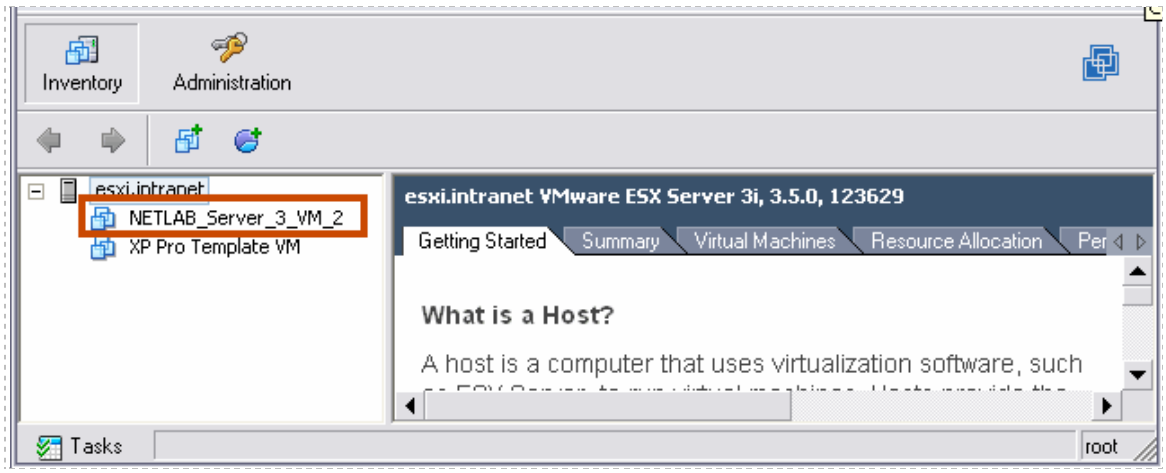


4.1.11 Verifying the Settings

Review the configuration settings displayed on the page and select **Finish.**



Your virtual machine will now be listed in the virtual machine inventory.



4.2 Installing a Guest Operating System

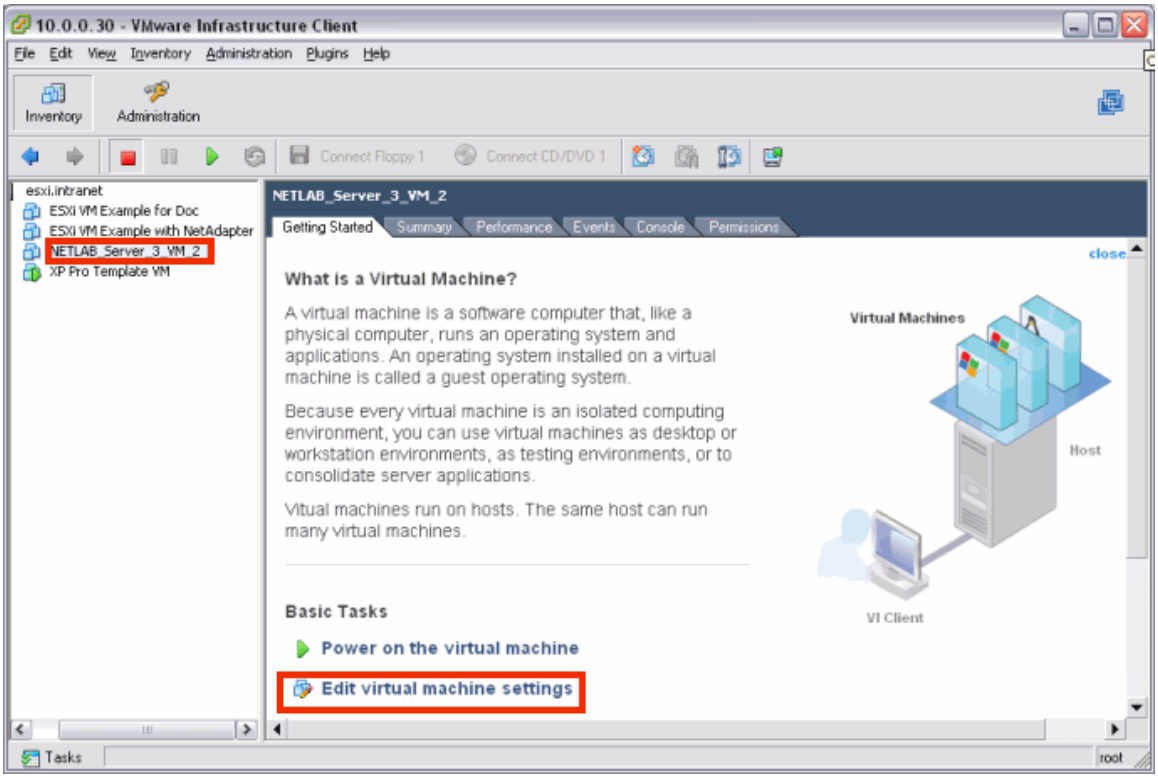
After you have configured the virtual machine settings, you must install an operating system on the virtual machine. Refer to VMware's *Basic System Administration Guide for ESXi*, *Chapter 10, Creating Virtual Machines*, for details on the procedure to install a guest operating system.

4.3 Editing the Virtual CD/DVD Device

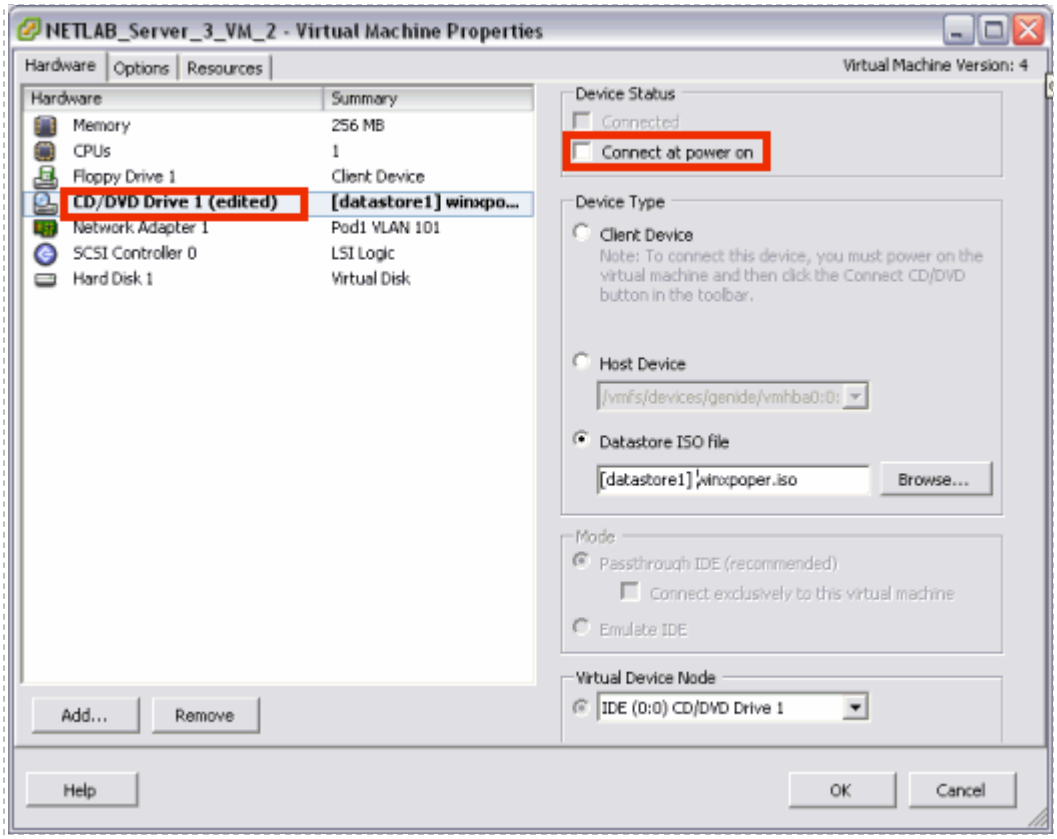
You may have configured your virtual machine to access a physical CD/DVD drive or access an ISO image in order to install the guest operating system. In the process, you may have enabled the **Connect at Power On** setting. For optimal pod performance, please verify the **Connect at Power On** option is ***Unchecked.***

This setting must be edited **after** installing the guest operating system.

1. From the VI Client, **Getting Started** tab, select the virtual machine from the inventory list and select **Edit virtual machine settings.**



Select the CD/DVD drive in the hardware list. ***Uncheck*** the **Connect at power on** box. This is necessary to prevent the virtual machine from attempting to connect to the ESXi host's CD/DVD device, which could result in undesired properties or boot errors. You may also point the CD/DVD device connection to a unique ISO image on the local ESXi host. If you choose this option, make sure each VM you create does not point to the same ISO file. Otherwise, you may see some undesired properties or boot errors.

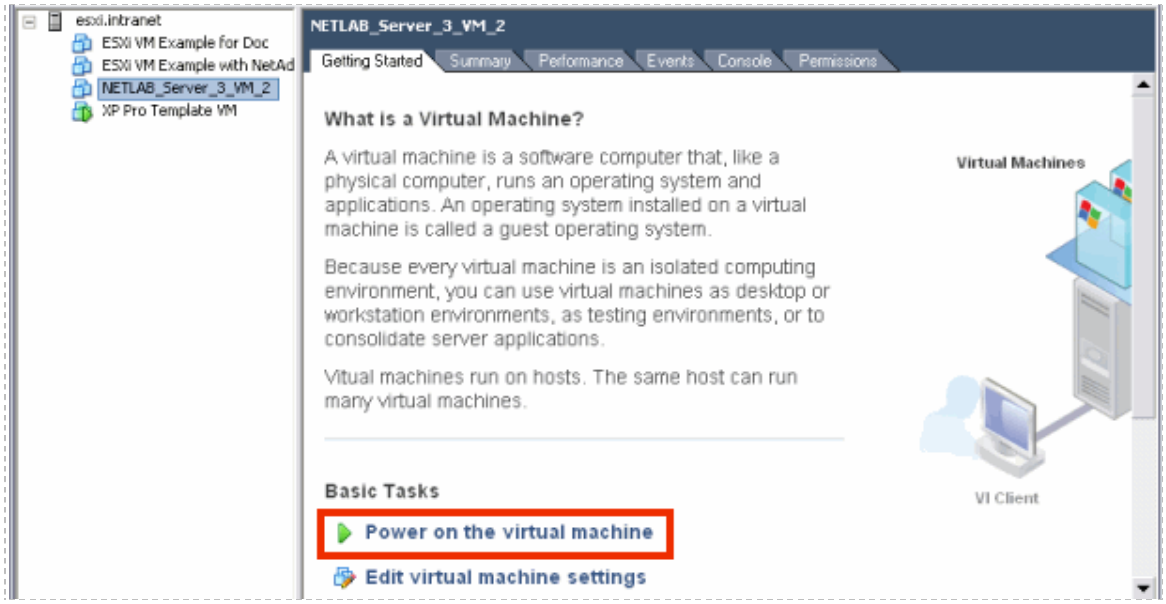


4.4 Installing VMware Tools

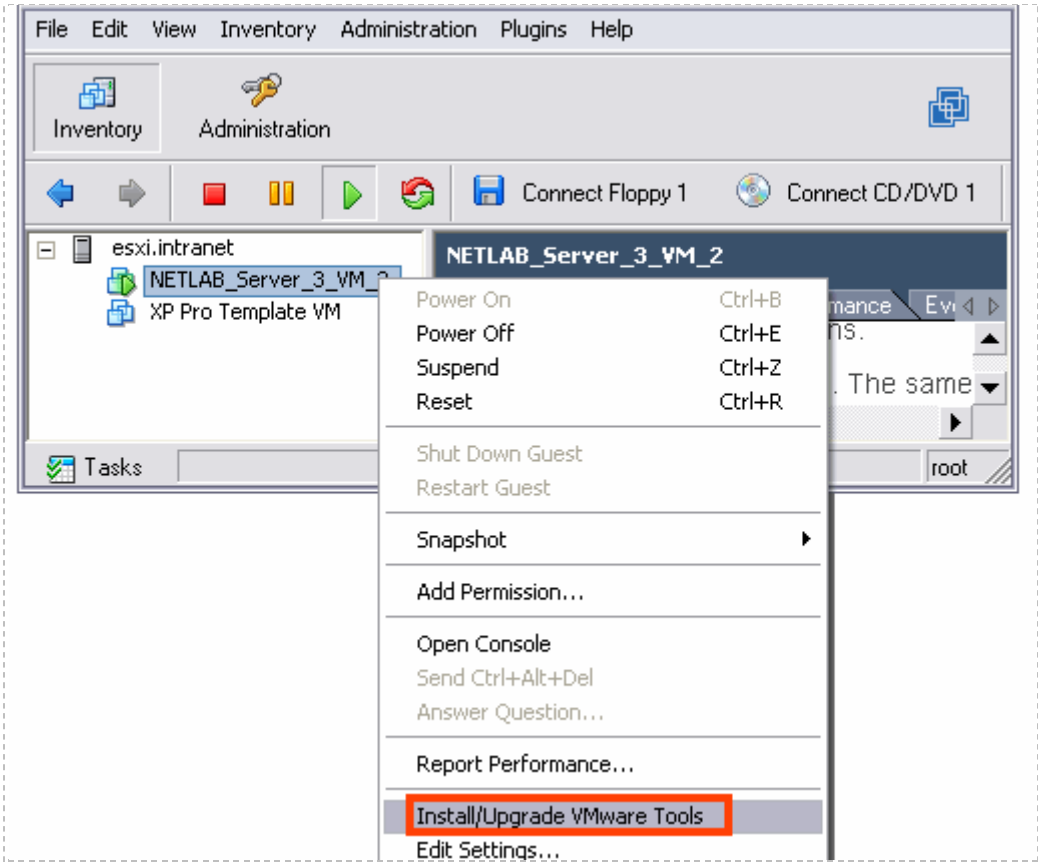
Installation of VMware Tools is required to ensure optimal performance and proper NETLAB+ operation.

VMware Tools must be installed **after** installing the guest operating system (see section 4.2).

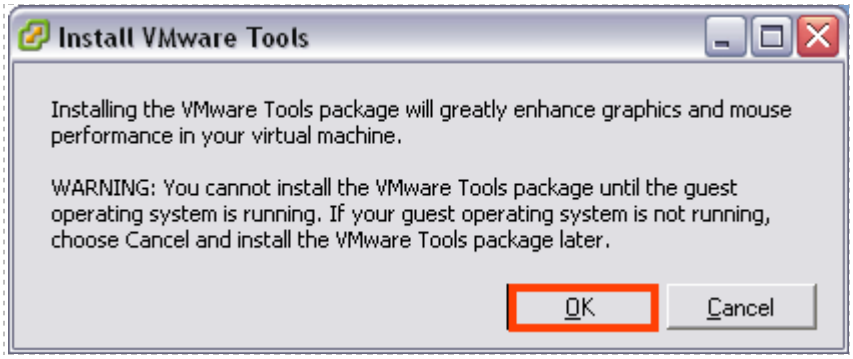
Your virtual machine must be powered on to install VMware Tools. Select the virtual machine in the inventory list, and click **Power on the virtual machine** on the **Getting Started** tab.



The option to install VMware tools will now be available. Select the virtual machine in the inventory list, ***right-click*** on the page, and select **Install/Upgrade VMware Tools.**



Assuming you have completed the installation of the guest operating system as described in section 4.1.4, you may proceed with the install of VMware Tools.



4.5 Setting the Virtual Machine Display Properties for Remote Access

For optimal performance and minimal bandwidth consumption, we recommend using the lowest possible resolution setting. The use of **800 x 600** provides a good fit on a typical laptop screen without the need to scroll the display.

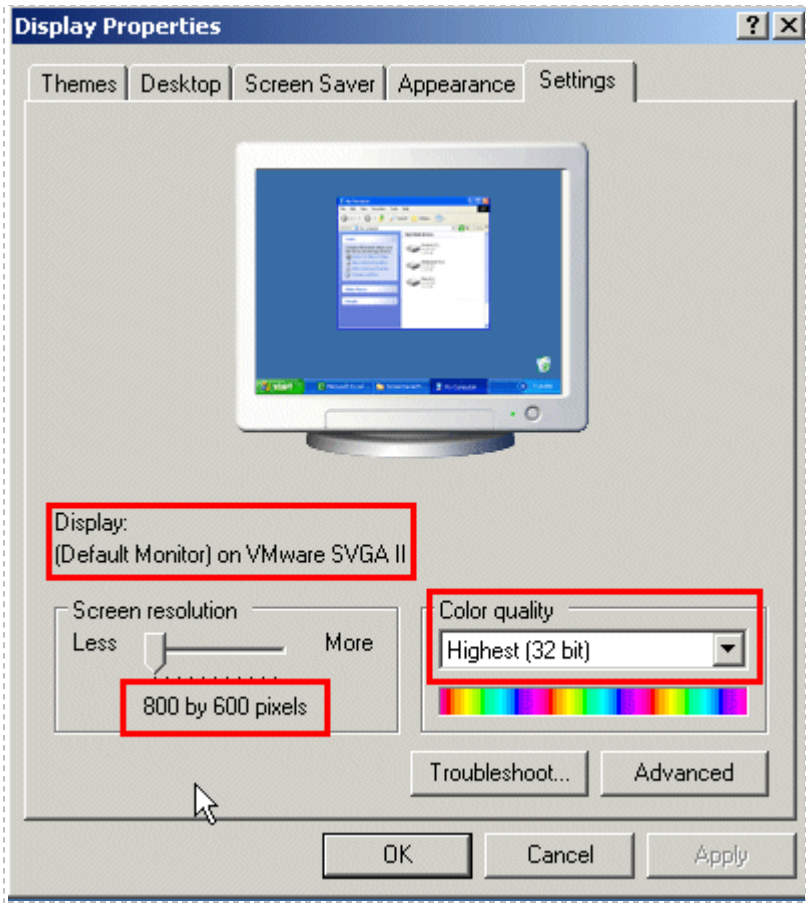
It is possible, however, that your applications may require a higher resolution, such as 1024 x 768.

32-bit color is required. Display update problems have been observed with the 16-bit setting.

The following task assumes a virtual machine running a Windows XP operating system. Adjust accordingly for other operating systems.

To set the screen resolution and color quality:

- Boot the virtual machine.
- ***Right-click*** on the display and select **Properties**.
- Click on the Desktop tab.
- Click on the **Settings** tab.
- Set screen resolution to your desired resolution (800 x 600 is used in this example).
- Set color quality to **32-bit** (required).


Display Properties
Themes
Desktop
Screen Saver
Appearance
Settings
Display:
(Default Monitor) on VMware SVGA II
Screen resolution
Less
More
800 by 600 pixels
Color quality
Highest (32 bit)
Troubleshoot...
Advanced
OK
Cancel
Apply

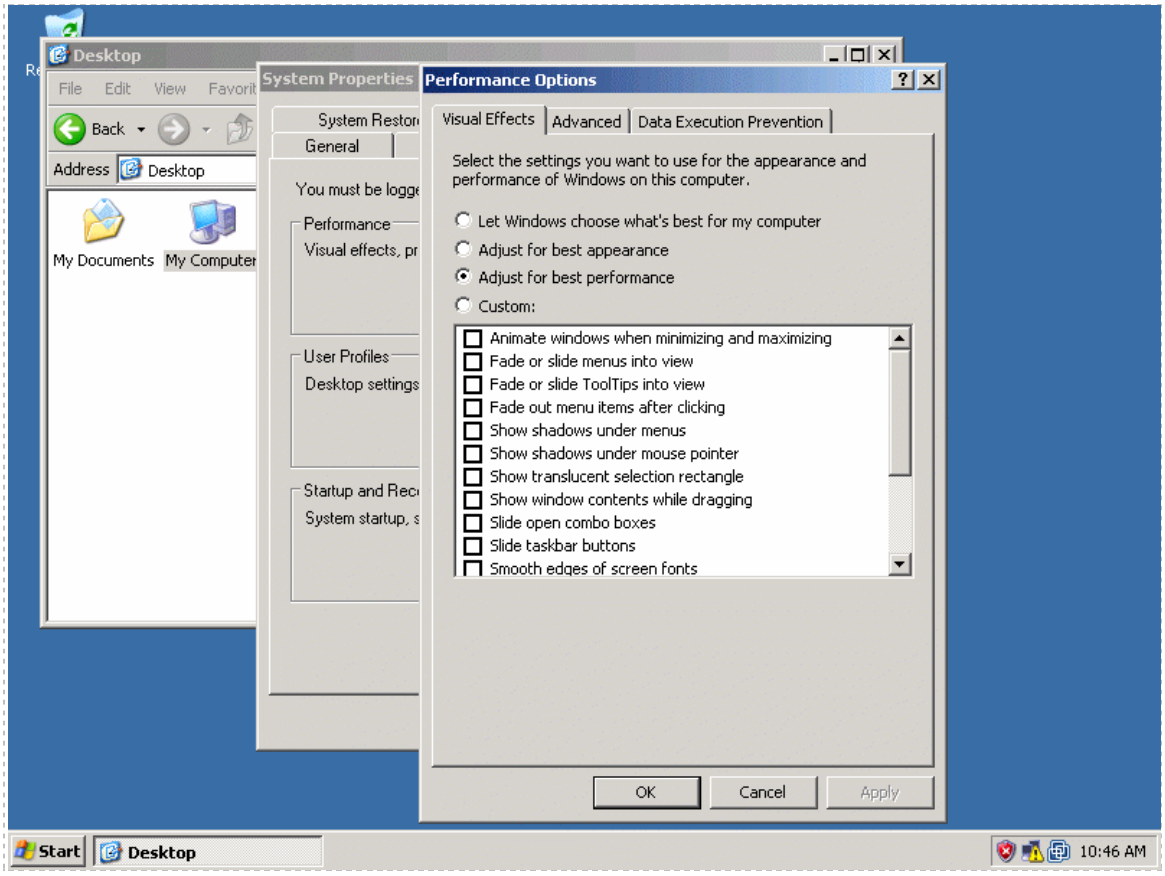
4.6 Adjusting Visual Effects

Visual effects must be adjusted to provide minimal bandwidth utilization and to ensure the responsiveness of the remote experience.

The following task assumes a virtual machine running a Windows XP operating system. Adjust accordingly for other operating systems.

Adjust the visual effects:

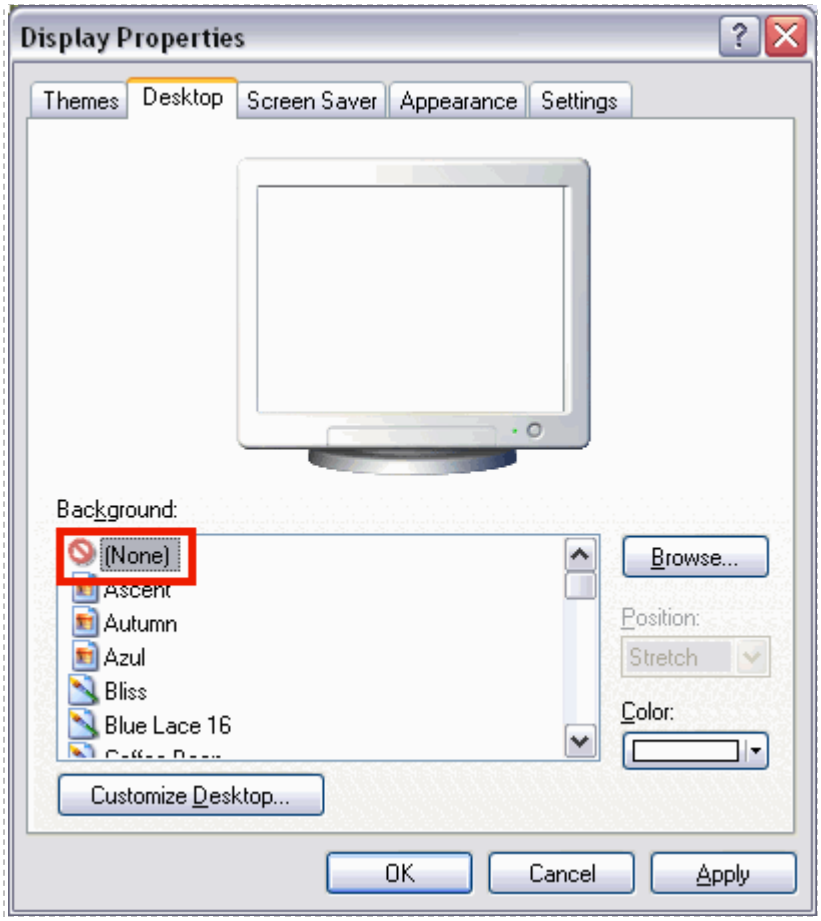
- ***Right-click*** on **My Computer** and select **Properties.**
- Click on the **Advanced** tab.
- Click the **Settings** button for **Performance.**
- Click the **Visual Effects** tab.
- Select the radio button to **Adjust for best performance.**
- Click **Ok** to accept changes.



4.7 Disabling the Desktop Background

The desktop background must be set to **None** to provide minimal bandwidth utilization and to ensure the responsiveness of the remote experience.

- Boot the virtual machine.
- ***Right-click*** on the display and select **Properties**.
- Click on the **Desktop** tab.
- Select **None** for the Background.



4.8 Adding Software Applications

You may now add new software to your virtual machine as required by the lab exercises you plan to use on your pods.

4.9 Taking a Snapshot of Your Virtual Machine and Managing Snapshots

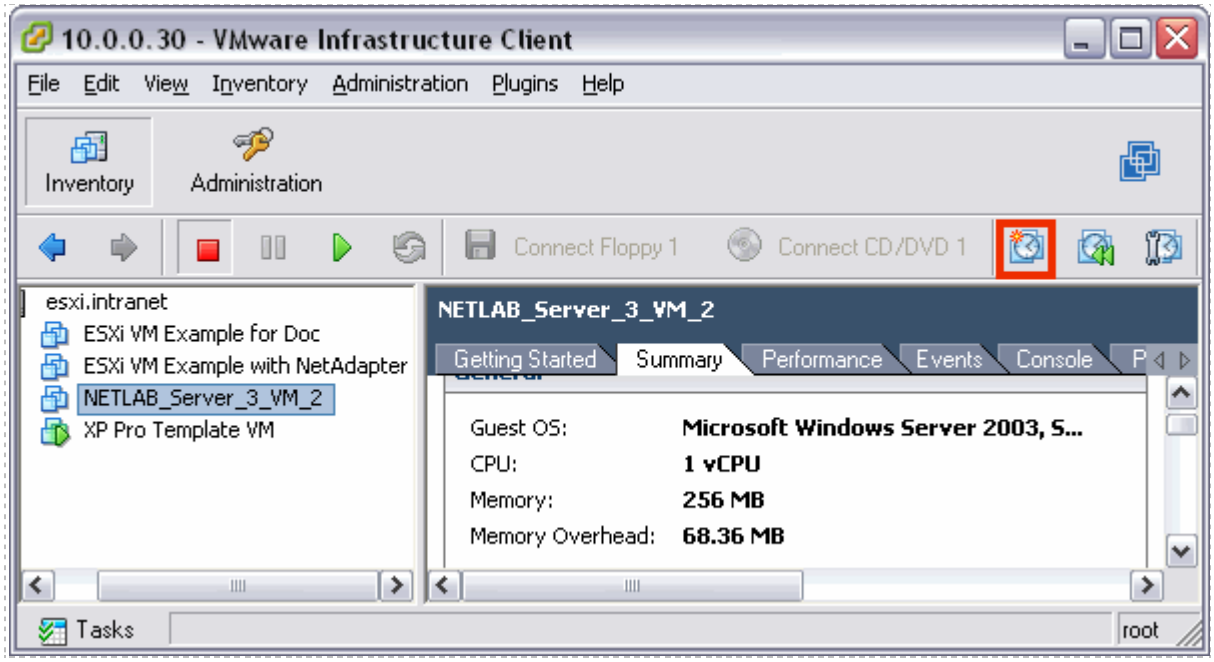
Each time you make changes or install new applications on a virtual machine, be sure to take a new *Snapshot*. Any changes made to the virtual machine by lab users will be lost when the virtual machine guest operating system reverts to the snapshot:

- At the end of a lab reservation.
- When a user selects Scrub from the NETLAB+ Action tab.

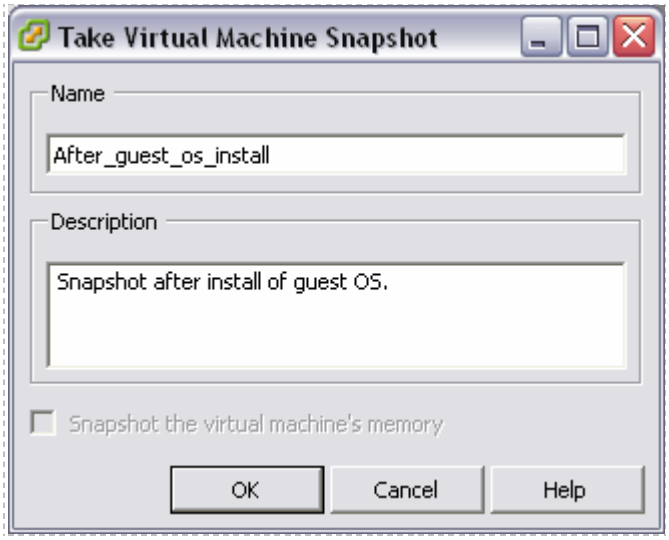
If you do not take a new snapshot after modifying the configuration file, your changes will be lost the next time the snapshot reverts. Your changes will also be lost if the virtual machine is not powered off when the configuration file is edited.

DO NOT take a Snapshot of a Virtual Machine when it is either turned on or suspended. Make sure VM is powered off each time you take a new Snapshot.

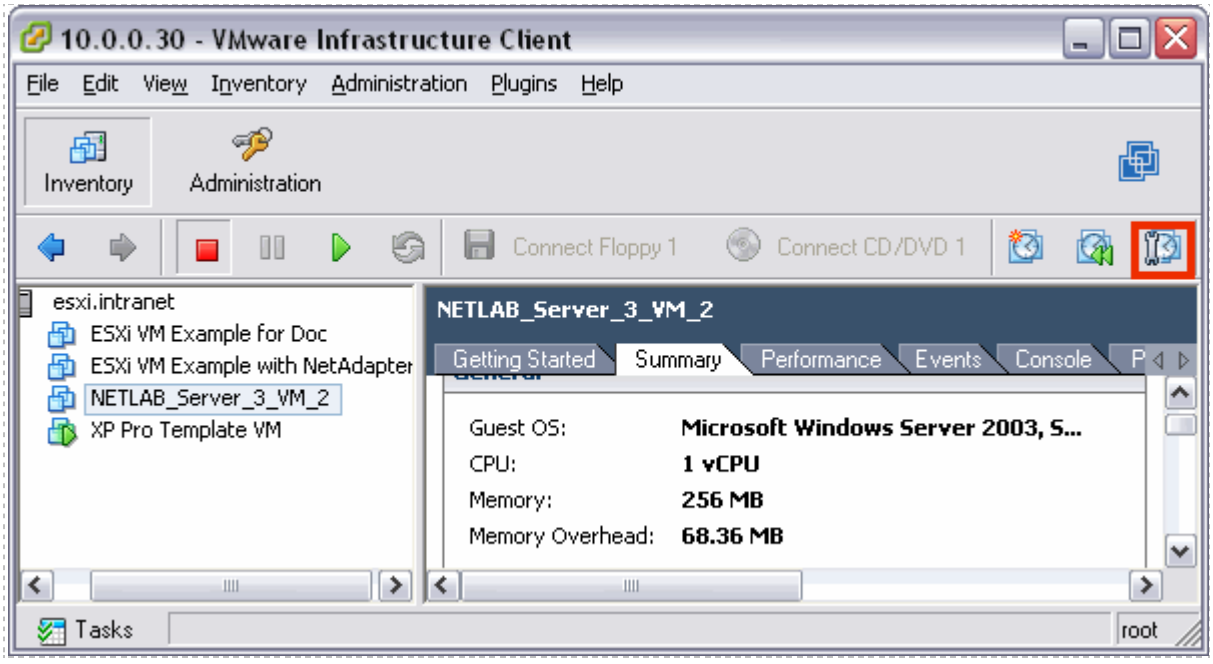
With the virtual machine powered off, select the virtual machine in the inventory list and select the **Take Snapshot** toolbar button.



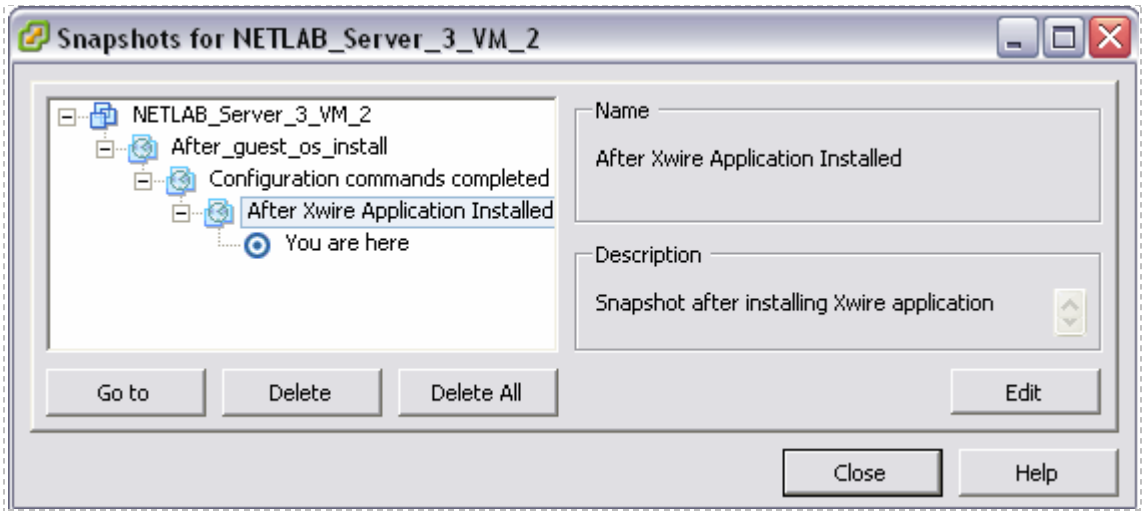
Enter a **Name** and **Description** for your snapshot.



ESXi can maintain multiple snapshots of your virtual machine. Use the **Snapshot Manager** to manage snapshots.



In this example, we see that three snapshots have been taken of this virtual machine (after installing the guest operating system, after configuring the remote display commands, and after installing an application).



Be aware of features available using the Snapshot Manager.

- The **You Are Here** icon represents the current operational state of the virtual machine. Each time you take a new snapshot, the Current Snapshot state is updated. NETLAB+ will revert to the current snapshot.

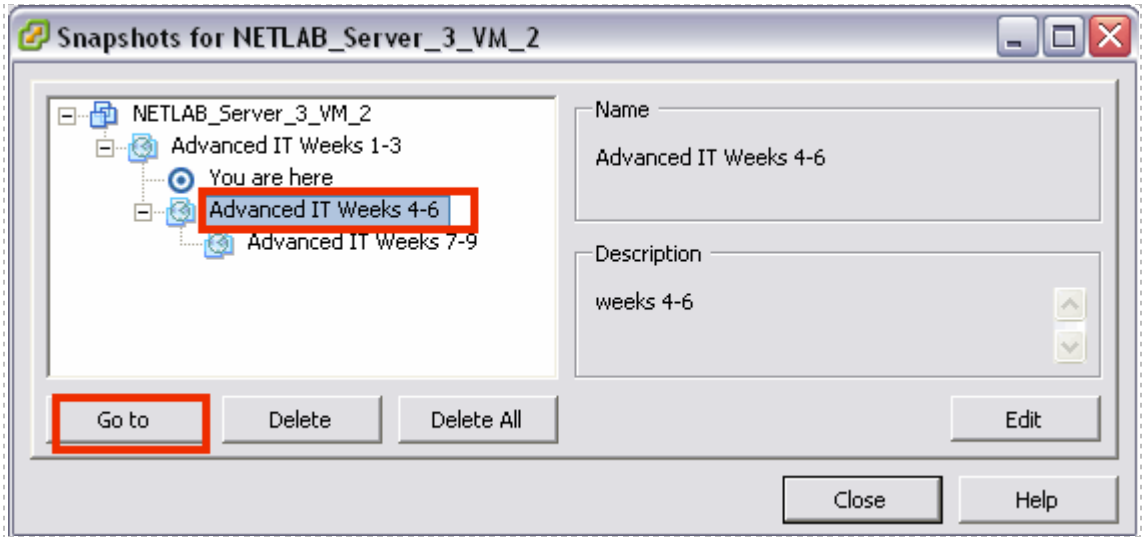
- **Delete** commits the snapshot data to the parent and removes the selected snapshot.

- **Delete All** commits all the immediate snapshots before the **You Are Here** current active state to the base disk and removes all existing snapshots for that virtual machine.

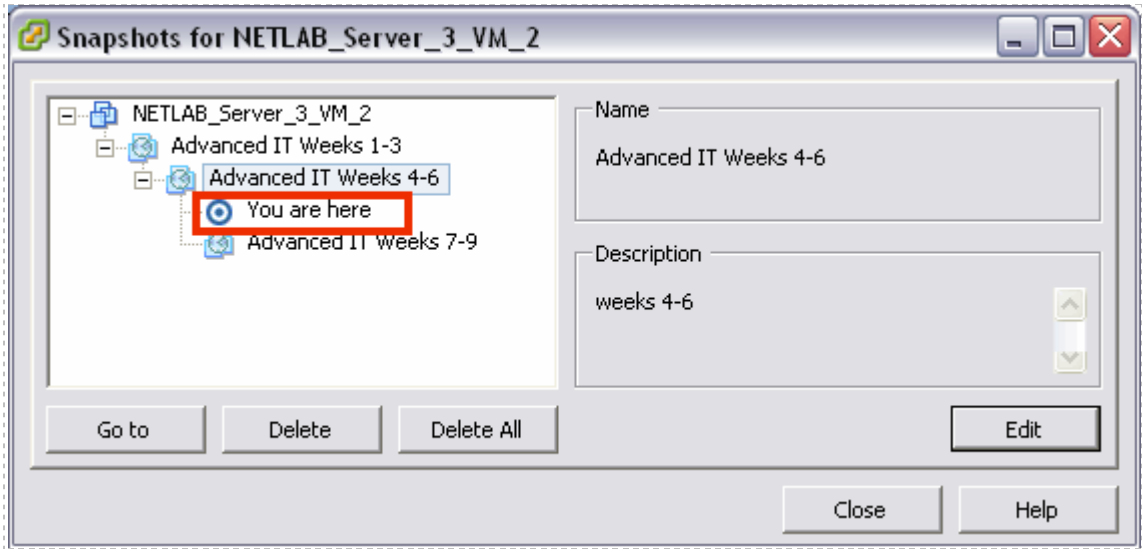
- **Go To** allows you to select the position of the current operational state of the virtual machine. You may maintain multiple snapshots and control which snapshot NETLAB+ will use by using **Go To** in order to modify the position of **You Are Here**, which indicates the current operational state of the VM.

Example:
*A nine-week Advanced IT course is taught where the files and applications required are different for each 3-week period. Snapshots are created with the appropriate configuration for each 3-week period. The **You Are Here** icon is placed at the snapshot for Weeks 1-3 at the beginning of the course.*

*At the end of the first three weeks, the **Go To** command is used to select the snapshot for Weeks 4-6.*



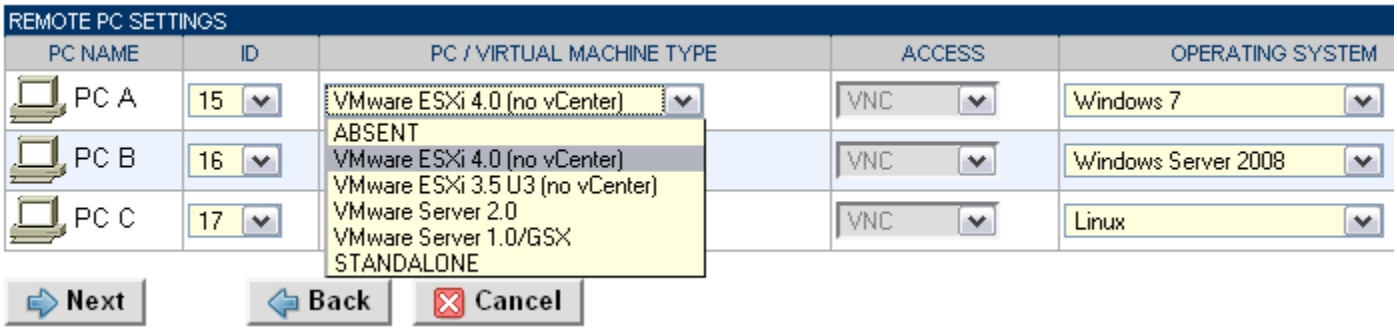
The position of the You Are Here indicator has been changed. NETLAB+ will now use the snapshot created for Weeks 4-6.



4.10 Remote PC Settings (for New Pods)

Remote PCs are part of a lab topology, so they must be configured in NETLAB+ when a new equipment pod is added. All settings (except ID) can be modified later. Remote PCs are only available in pods where the network topology indicates the existence of lab PCs.

Remote PC settings will appear in the New Pod Wizard when you add an equipment pod that supports remote PCs. Each PC has an ID, type, access method, and operating system setting. All settings (except ID) can be modified later. To modify existing PCs, skip ahead to section 4.11.

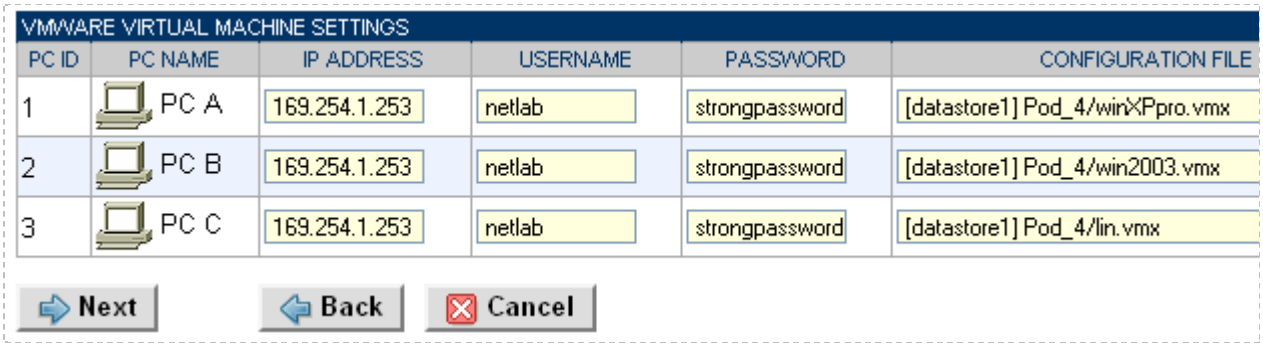


For **PC/Virtual Machine Type**, use the **VMware ESXi 3.5 U3 (no vCenter)** or **VMware ESXi 4.0 (no vCenter).** The 4.0 setting is available in NETLAB+ version 2010.R3. If you do not see this setting (because you are using an earlier version NETLAB+) please select the ESXi 3.5 U3 setting, even when using ESXi 4.01..

The **Access** setting, VNC, allows direct access to the PC's keyboard, video and mouse using the VNC protocol. This setting cannot be altered when ESXi has been selected as the PC/Virtual Machine Type.

The **Operating System** setting specifies an OS for this PC. The availability of a selection does not guarantee compatibility with all labs.

NETLAB+ will prompt for additional settings on the next page.



Each virtual machine requires four ESXi-specific settings.

- The **IP Address** setting is used to connect to the ESXi host system. This is the IP address used for KVM and API traffic flow. Use the inside network address of the VMware server.

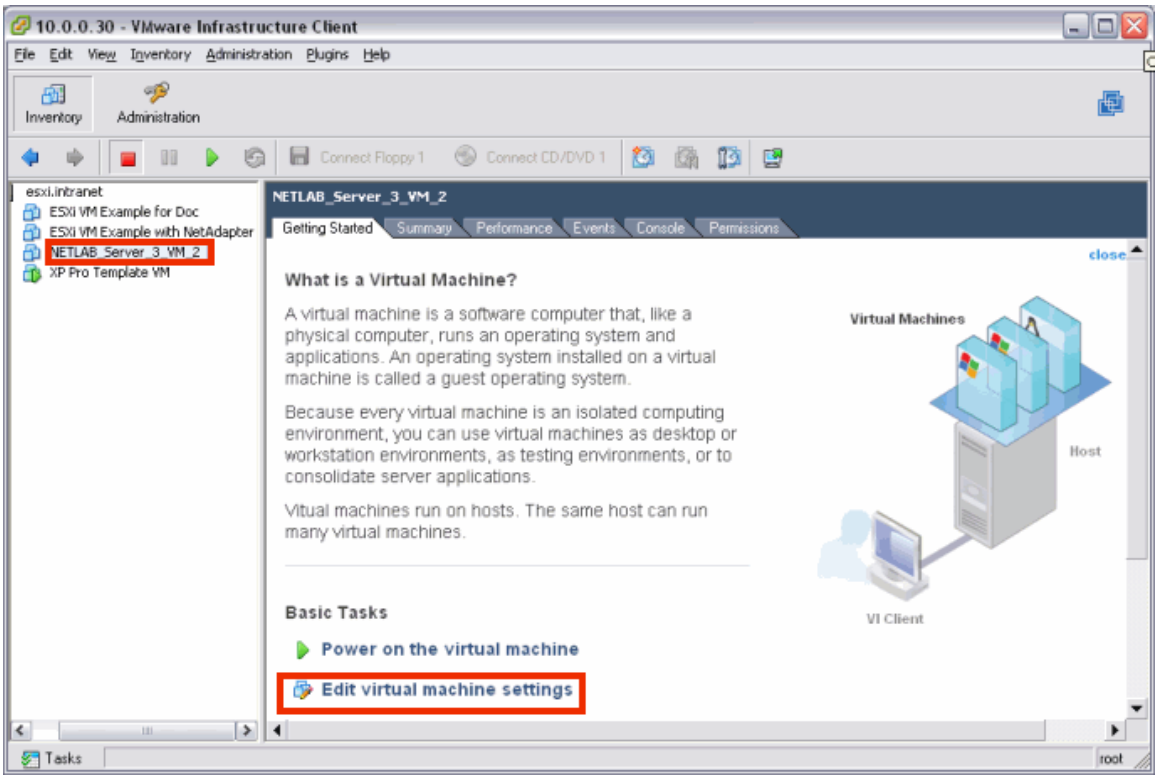
- **Username** specifies an operating system account on the ESXi host system. NETLAB+ will use this account to login to the ESXi host and control virtual machines through the VMware API (see section 3.7).

- **Password** specifies the password associated with the host account (see section 3.7).

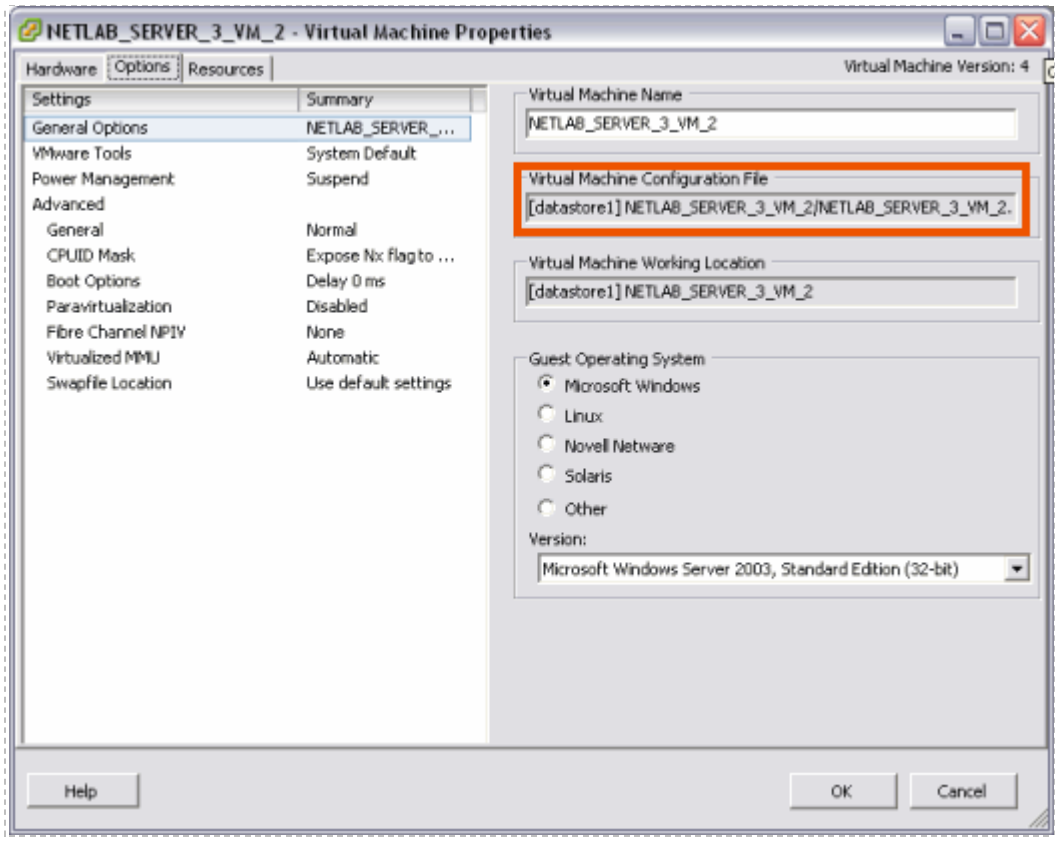
- **Configuration File** Enter the relative path of the virtual machine configuration file on the ESXi host, including datastore. This file name is typically in the form of [datastore] <*pc name*>/<*operating system*>.vmx.

To find the name of a virtual machine configuration file:

1. From the VI Client, **Getting Started** tab, select the virtual machine from the inventory list and select **Edit virtual machine settings.**



2. Select the **Options** tab to display the **Virtual Machine Configuration File**.



You can copy and paste the full pathname of a VM Configuration file from the VM configuration screen into the NETLAB+ virtual machine settings **Configuration File Name** field.

The use of relative path names is specific to ESXi and VMware Server 2.x. VMware server 1.0 and GSX require absolute path names. If you are upgrading from VMware Server 1.0 or GSX, you must change your configuration file path names to use relative path names, as shown in the example above. Please refer to Appendix C for details on upgrading to VMware ESXi.

4.11 Modifying PC Settings

To modify PC settings, or convert an existing PC to use ESXi:

1. Take the pod offline.
2. Select the PC from the Pod Management page.

POD 1 - PCs AND SERVERS (click the GO buttons to reconfigure)

GO	NAME	PC ID	STATUS	TYPE	ACCESS	CONTROL IP	OPERATING SYSTEM
	PC1a	200	ONLINE	VMWARE Server 1.0/GSX	VNC	10.0.0.26	Windows XP
	PC1b	201	ONLINE	VMWARE Server 2.0	VNC	169.254.0.250	Windows XP
	PC2	202	ONLINE	ABSENT	NULL		
	PC3	203	ONLINE	VMWARE ESXi 3.5 U3	VNC	10.0.0.30	Windows XP

3. Change Type to **VMWARE ESXi 3.5 U3** (if it is not the current setting).
4. Specify the VMware settings (described in section 4.10).

POD 1 - PC 203

PC ID	203
PC Name	PC3
Type	VMWARE ESXi 3.5 U3
VMware Host IP Address	10.0.0.30
VMware Host Username	netlab
VMware Host Password	strongpassword
VMware Guest Configuration File	[datastore1] XP Pro Template VM/XP Pro Template VM.vn
VMware Guest Operating System	Windows XP
VMware Guest VNC Settings	RemoteDisplay.vnc.enabled = "true" RemoteDisplay.vnc.port = "6103"
Access Method	VNC
Admin Status	ONLINE
Options	revert to snapshot during scrub operation

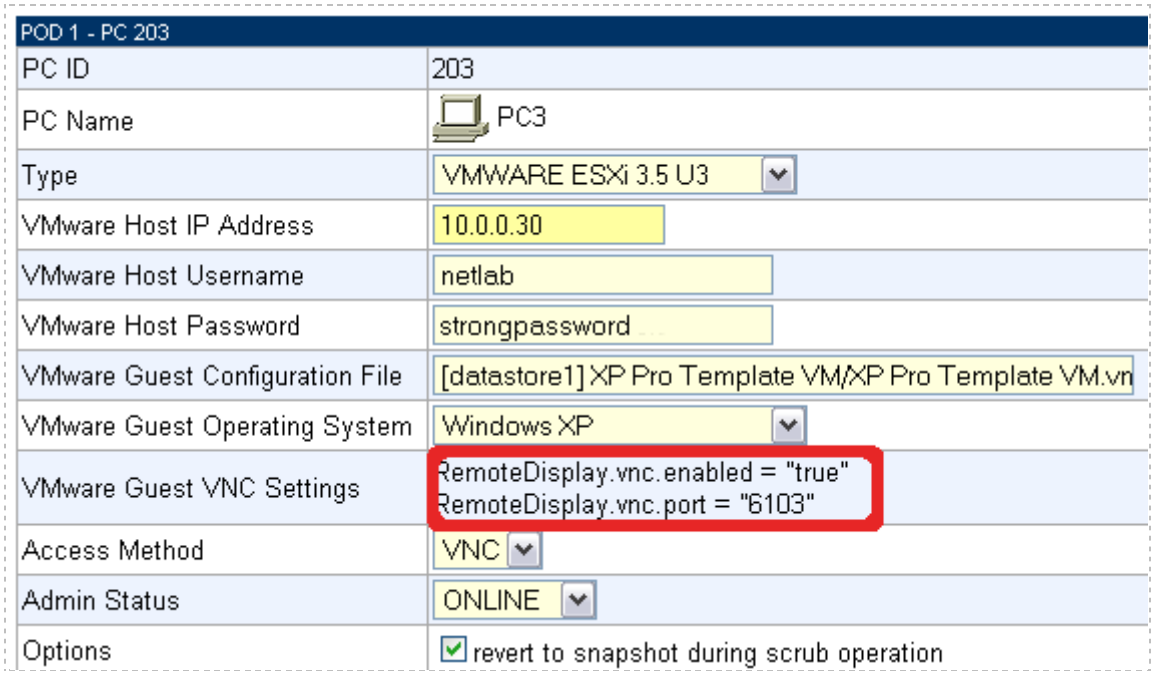
If you want NETLAB+ to return the PC to a clean state after a lab reservation, make sure “revert to snapshot” is checked.

4.12 Configuring Remote Display Options

To allow NETLAB+ users to access the keyboard, video, and mouse of a virtual machine, you must add two **RemoteDisplay** statements to the virtual machine's configuration file.

1. Access the detailed remote PC settings from the NETLAB+ Pod Management page (as described in section 4.10).

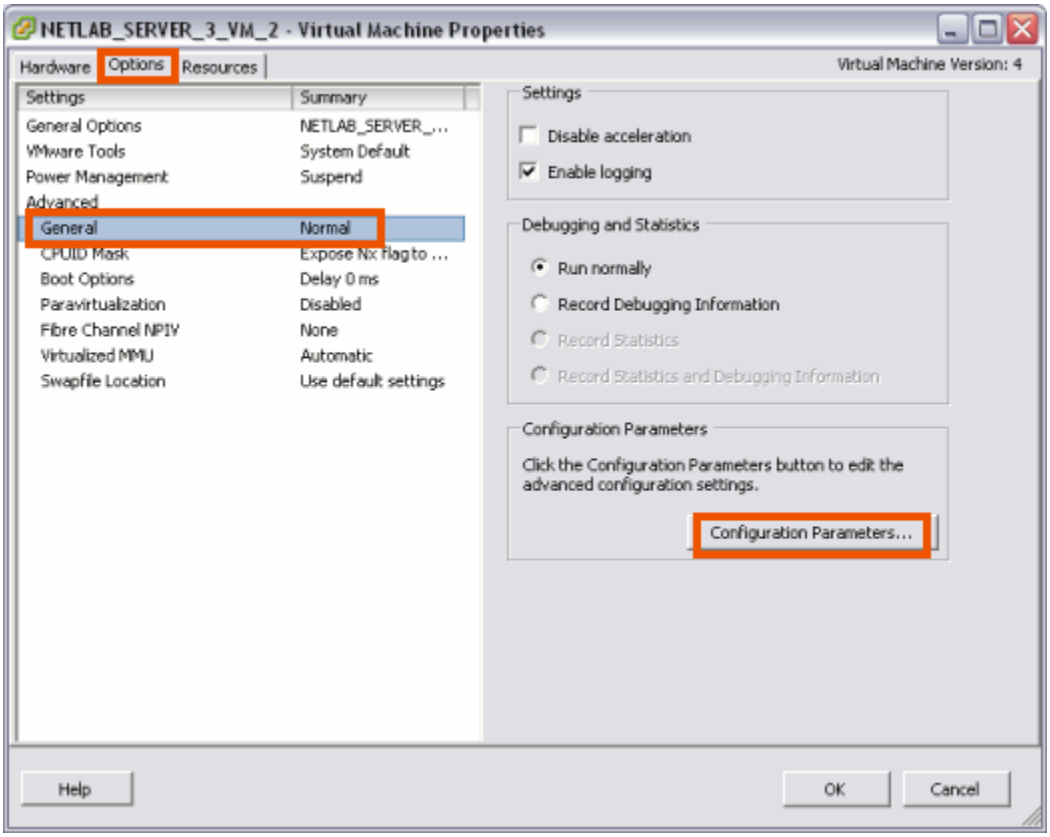
2. Obtain the **VMware Guest VNC Settings** (automatically computed by NETLAB+). The settings for this example are highlighted in the picture below (your settings will vary).



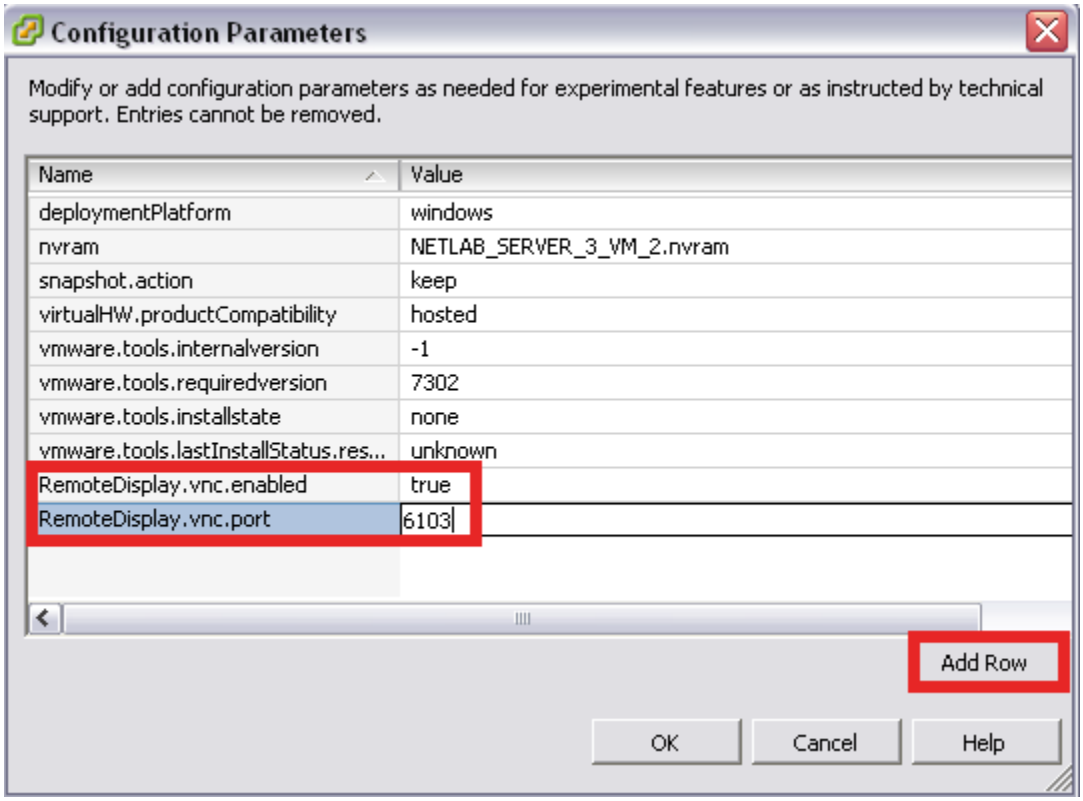
3. From the VMware management console, make sure the PC is powered **OFF or suspended**.

4. Access the Edit Settings for the virtual machine. On the Options tab in the Advanced section, select General. The **Configuration Parameters** button will be displayed.

5. Select Configuration Parameters.



6. Add the two VMware guest VNC settings as configuration parameters.



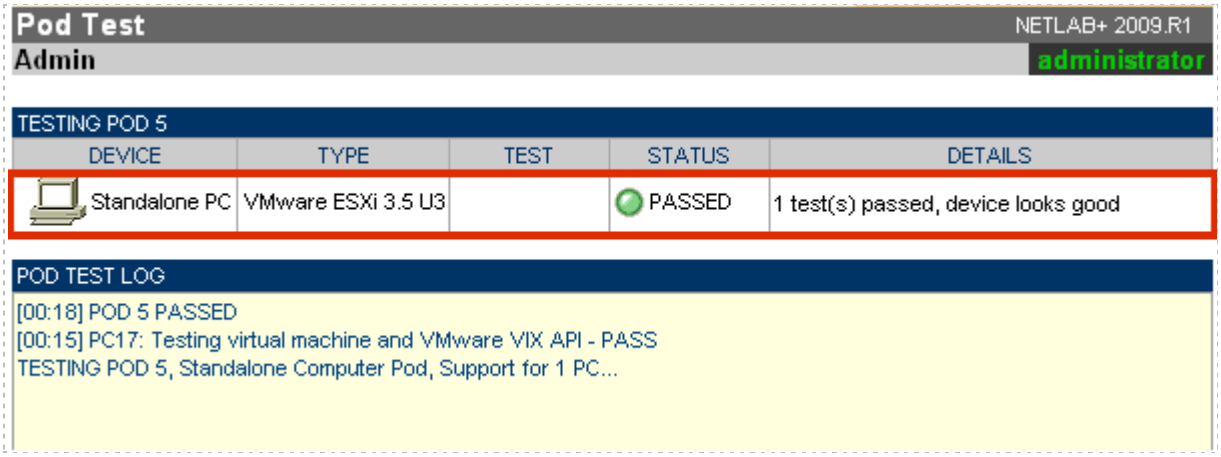
7. Take a new snapshot of your virtual machine (see section 4.9).

If you do not take a new snapshot after modifying the configuration file, your changes will be lost the next time the snapshot reverts. Your changes will also be lost if the virtual machine is not powered off when the configuration file is edited.

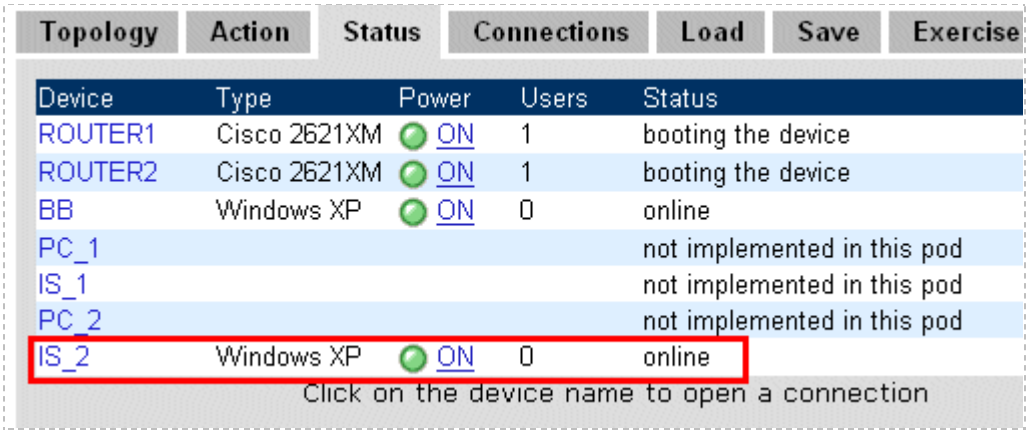
4.13 Verify the Virtual Machine

After your virtual machine is configured, perform the following tasks to verify the API is functioning.

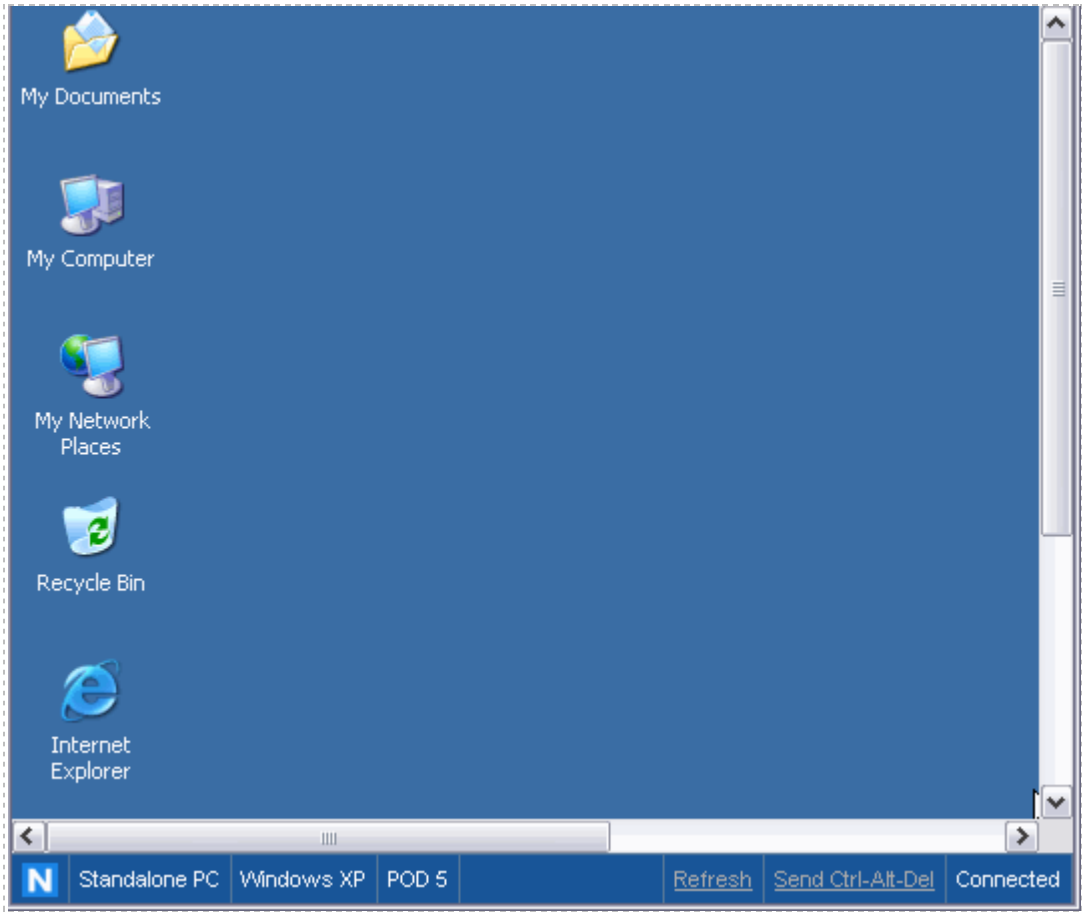
The Pod Test only verifies the remote display parameters and the function of the VMware API. The Pod Test does not test network connectivity to networking gear such as routers, switches and firewalls. The process required to bridge your virtual machines to real networks and real lab equipment (such as routers, switches, and firewalls) is described in detail in Part 5.



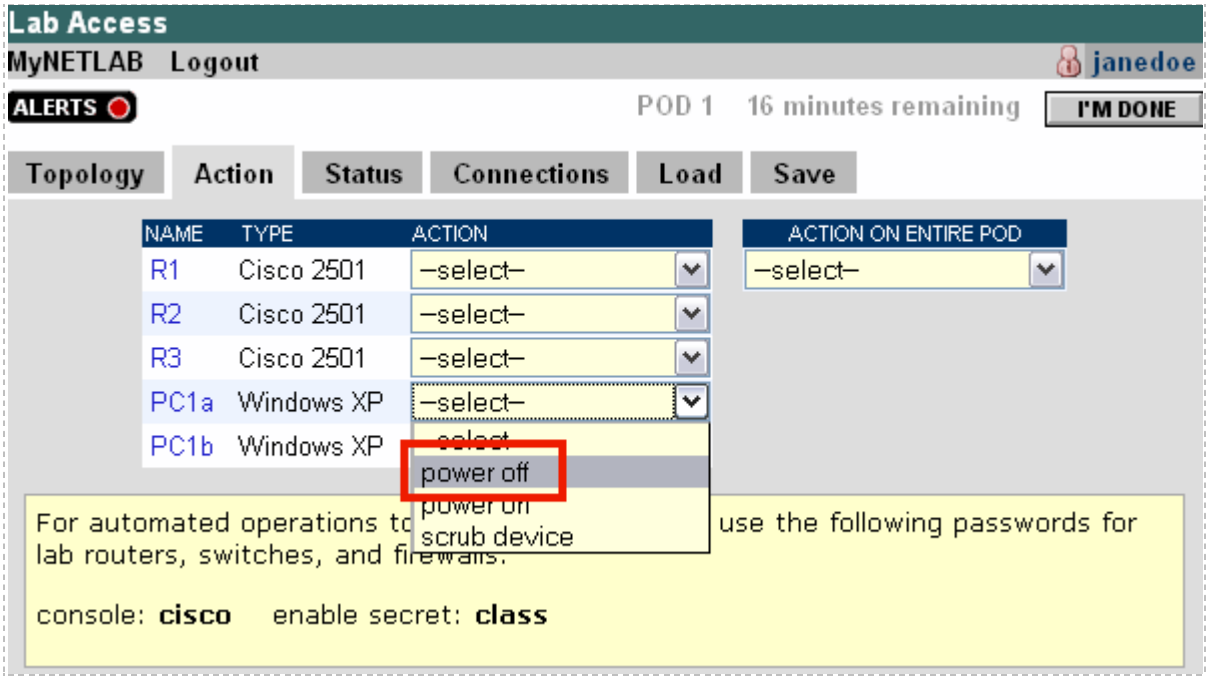
1. Run a pod test. NETLAB+ will check your settings and verify that the API is working.
2. Bring the pod back online.
3. Login to an instructor account and create a lab reservation to test your virtual machine(s).
4. On the **Status** tab, your virtual machines should be online.



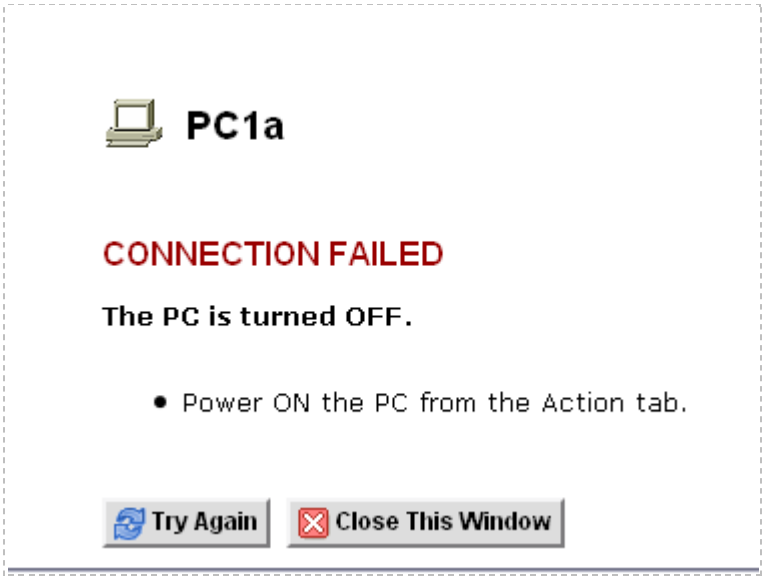
5. Open a connection to the PC by clicking on the device in the topology tab, status tab, or connections tab. This will bring up the NETLAB+ Remote PC viewer (assuming you have Java installed).



6. Test the VMware API. **Power off** the machine from the **Action** tab.



If you had a connection open, it should drop. If you reconnect, NETLAB+ should know the PC is powered off (by obtaining the status of the virtual machine via the VMware API).



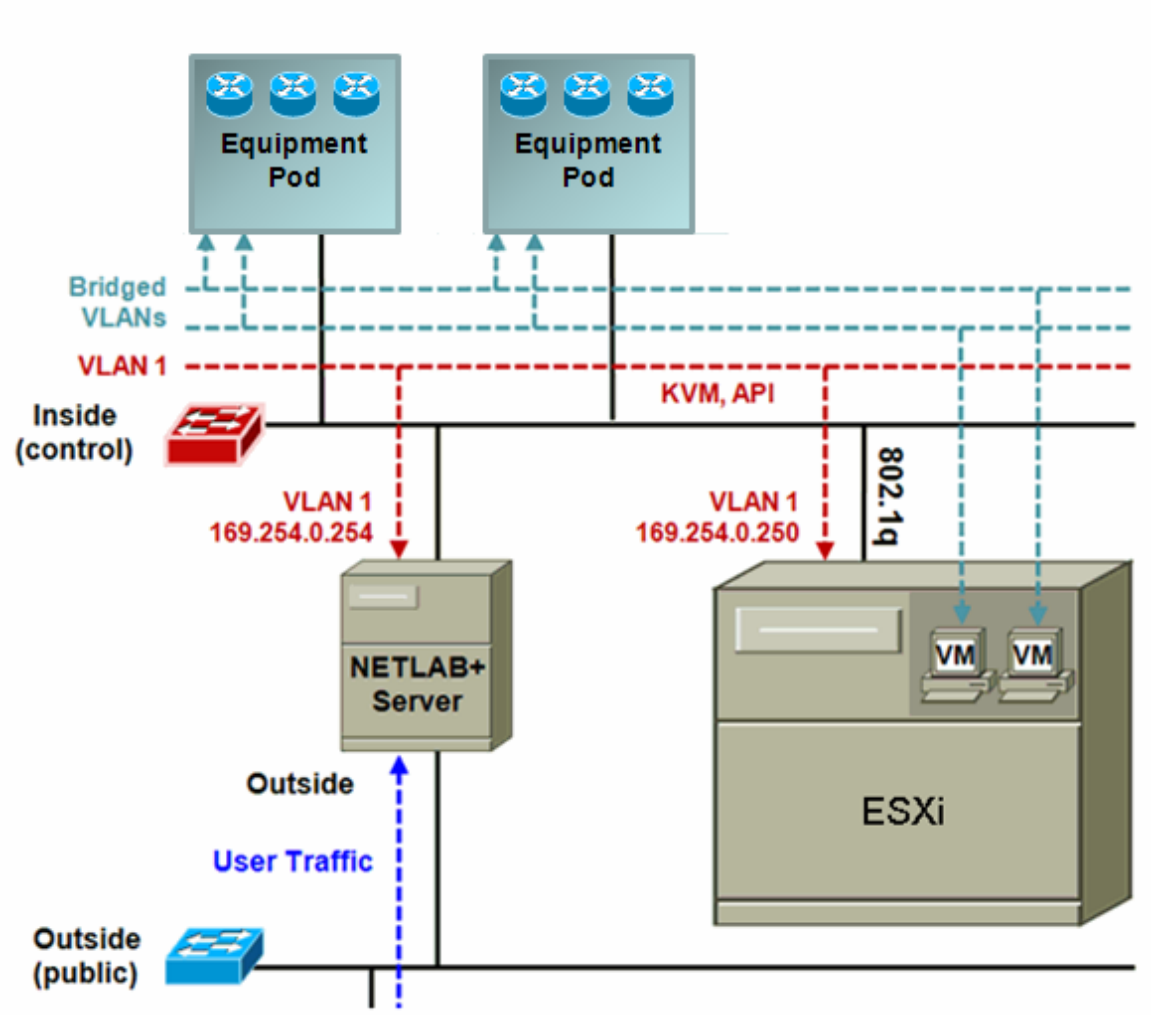
7. From the **Action tab**, power the virtual machine back **ON**. Wait a minute for the machine to startup. You should now be able to reconnect.

8. Test the scrub device/snapshot feature. Make some changes to the PC (i.e. move some icons around and create some files). Select **Scrub Device** on the Action tab. The PC will reboot and your connection will drop (this is normal). Wait a minute for the machine to restart. You should now be able to reconnect, and your previous changes should be gone.

Part 5 Connecting Virtual Machines to Real Lab Devices

This section focuses on the establishing communication between virtual machines and lab devices in the topology. You can skip this section if your virtual machines do not need to communicate with lab equipment and/or external networks on separate VLANs.

Virtual LANs (VLANs) are used to bridge your virtual machines to real lab equipment (such as routers, switches, and firewalls). These VLANs are implemented on control switches and managed by the NETLAB+ software.



The following objectives will make more sense after you have added a new equipment pod.

Objectives

- Determine which VLAN numbers are used by your pod.
- Create the proper VLAN adapter.
- Bind each VLAN adapter to the Inside Interface.
- Take a final snapshot to save changes made to the VM configuration.

5.1 Determining Which VLAN Numbers Are Used by Your Pod

The VLAN adapters you must create for you virtual machines will vary based on which pods you have added to your NETLAB+ server.

A *VLAN Pool* is the consecutive range of VLANs used by NETLAB+. Each pod has a unique *VLAN pool* and the actual VLAN numbers will be unique for each pod. **You must determine which VLAN numbers used by NETLAB+ must be trunked to the VMware host.**

There are resources available to assist you in determining which VLAN numbers are used:

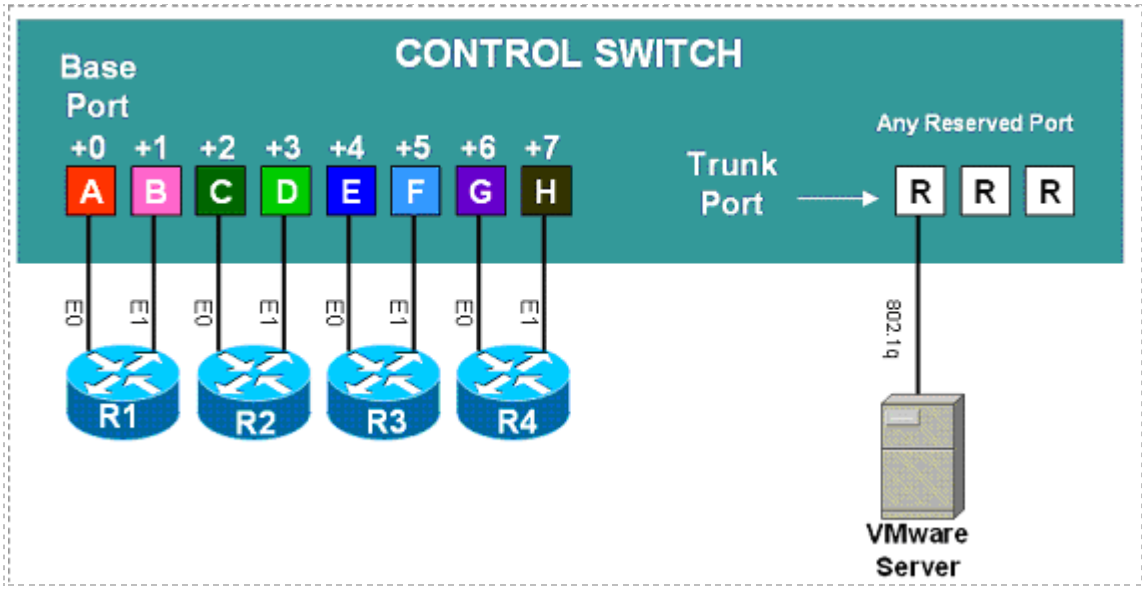
- If you are implementing a standard NETLAB+ Academy Edition® pod, you may refer to the *Configuring VMware and Virtual Machines* section of the appropriate pod-specific guide to obtain this information, including the VLAN Offset Reference Table specific to your pod. The examples in the subsections below provide more detail regarding this process.

- If you are implementing a custom pod design, consult with the individual who created the pod design and refer to the *Pod Design Theory* section of the *NETLAB+ Pod Design Guide* for additional information.

ESXi virtual network adapters and virtual LAN adapters are used to connect virtual machines to the pod. Each VLAN adapter will be connected to the virtual switch configured for the inside interface. Depending on the pod design, some virtual machines may share the same VLAN.

5.1.1 Determining VLANs Example 1 – Cuatro Router Pod

In this example, we see that a Cuatro Router Pod requires **8 consecutive ports** on a supported control switch.



Ports are labeled **+0** to **+7** in the diagram and are relative to the *base port*. Using SNMP, $NETLAB_{AE}$ will automatically setup VLANs and configure ports on the control switch. These VLANs are depicted as letters "A" through "H" and represent one subnet in the topology. Each $NETLAB_{AE}$ pod has a unique *VLAN pool* and the actual VLAN numbers will be unique for each $NETLAB_{AE}$ pod.

Step 1. Determine the Base VLAN for the pod.

The base VLAN and VLAN pool numbers are displayed on the Pod Management page in the Control Switch table. Please see the *Verifying Your Settings* section of the *NETLAB+ Administrator Guide* for details on accessing the Pod Management page to find the base VLAN number for your pod.

An example of the VLAN pool information available on the Pod Management page. In this example, pod 7 uses VLANs 160-167. The base VLAN is 160. Your VLAN numbers will vary.

POD 7 - CONTROL SWITCH

SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL
2	1-8	160	160-167

Step 2. Determine the actual VLAN number for each virtual network.

Add the base VLAN to the offsets in the table below. In this example, the **VLAN Offset Reference Table** from the *NETLAB$_{AE}$ Cuatro Router Pod Guide* is used. Consult the appropriate pod-specific guide to obtain the information for your pod.

Using ESXi, all VLAN adapters will be connected to a single virtual switch. The information in the Virtual Switch (VMnet) column is relevant only when using VMware Server 1.0/GSX and VMware Server 2.0.

The base VLAN value used below (160) is an example, the base VLAN of your pod will vary.

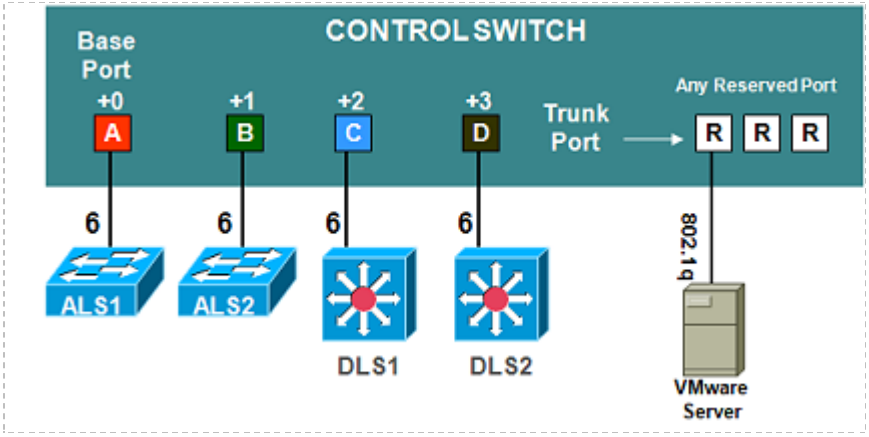
VLAN Offset Reference Table – Cuatro Router Pod

Virtual Machines	Virtual Switch (VMnet)	Offset (add to base VLAN)	Actual VLAN	Example
PC1a PC1b	R1 VMnet	+ 0	= _____	160 + 0 = 160
PC2	R2 VMnet	+ 2	= _____	160 + 2 = 162
PC3	R3 VMnet	+ 4	= _____	160 + 4 = 164
PC4	R4 VMnet	+6	=_____	160 + 6 = 166

In this example, we have determined that we must create VLAN adapters for VLANs 160, 162, 164, and 166.

5.1.2 Determining VLANs Example 2 – Cuatro Switch Pod

In this example, we see that a Cuatro Switch Pod requires **4 consecutive ports** on a supported control switch.



Ports are labeled **+0** to **+3** in the diagram and are relative to the *base port*. Using SNMP, $NETLAB_{AE}$ will automatically setup VLANs and configure ports on the control switch. These VLANs are depicted as letters "A" through "D" and represent one subnet in the topology. Each $NETLAB_{AE}$ pod has a unique *VLAN pool* and the actual VLAN numbers will be unique for each $NETLAB_{AE}$ pod.

Step 1. Determine the Base VLAN for the pod.

The base VLAN and VLAN pool numbers are displayed on the Pod Management page in the Control Switch table. Please see the *Verifying Your Settings* section of the *NETLAB+ Administrator Guide* for details on accessing the Pod Management page.

An example of the VLAN pool information available on the Pod Management page, your VLAN numbers will vary.

POD 10 - CONTROL SWITCH

SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL
2	9-12	190	190-193

In this example, Pod 10 uses VLANs 190-193. The base VLAN is 190.

Step 2. Determine the actual VLAN number for each virtual network.

Add the base VLAN to the offsets in the table below. In this example, the **VLAN Offset Reference Table** from the *NETLAB$_{AE}$ Cuatro Switch Pod Guide* is used. (Consult the appropriate pod-specific guide to obtain the information for your pod).

Using ESXi, all VLAN adapters will be connected to a single virtual switch. The information in the Virtual Switch (VMnet) column is relevant only when using VMware Server 1.0/GSX and VMware Server 2.0.

The base VLAN value used below (190) is an example, the base VLAN of your pod will vary.

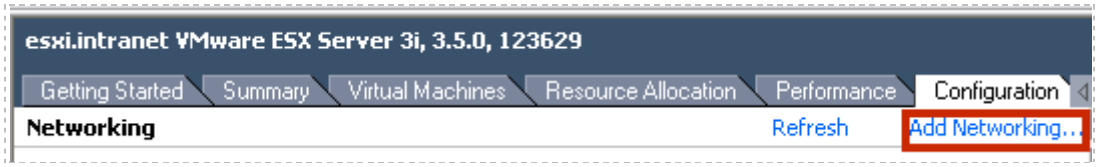
VLAN Offset Reference Table – Cuatro Switch Pod

Virtual Machines	Virtual Switch (VMnet)	Offset (add to base VLAN)	Actual VLAN	Example
Host A	ALS1 VMnet	+ 0	= _____	190 + 0 = 190
Host B	ALS 2 VMnet	+ 1	= _____	190 + 1 = 191
Host C	DLS 1 VMnet	+ 2	= _____	190 + 2 = 192
Host D	DLS 2 VMnet	+ 3	= _____	190 + 3 = 193

In this example, we have determined that we must create VLAN adapters for VLANs 190, 191, 192, and 193.

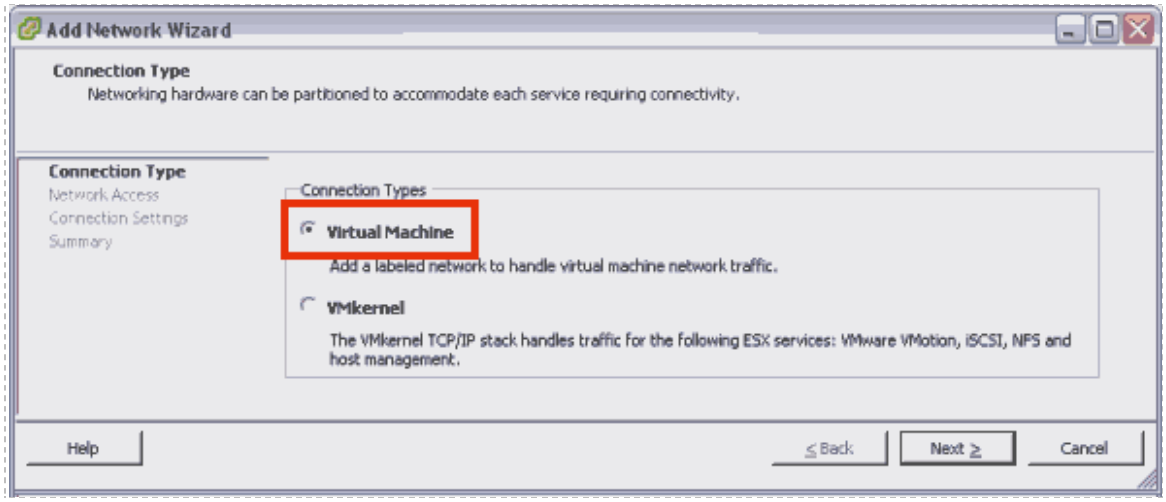
5.2 Creating VLAN Adapters using VI Client

Based on the VLAN numbers identified in the previous section, follow the steps described in the subsections below to create each of the VLAN adapters required. You will create a VLAN sub-interface on the **Inside Physical Interface** (container interface). Begin by selecting **Add Networking** to start the **Add Network Wizard**.



5.2.1 Selecting the Virtual Machine Connection Type

Use the **Virtual Machine** connection type for your VLAN adapter.

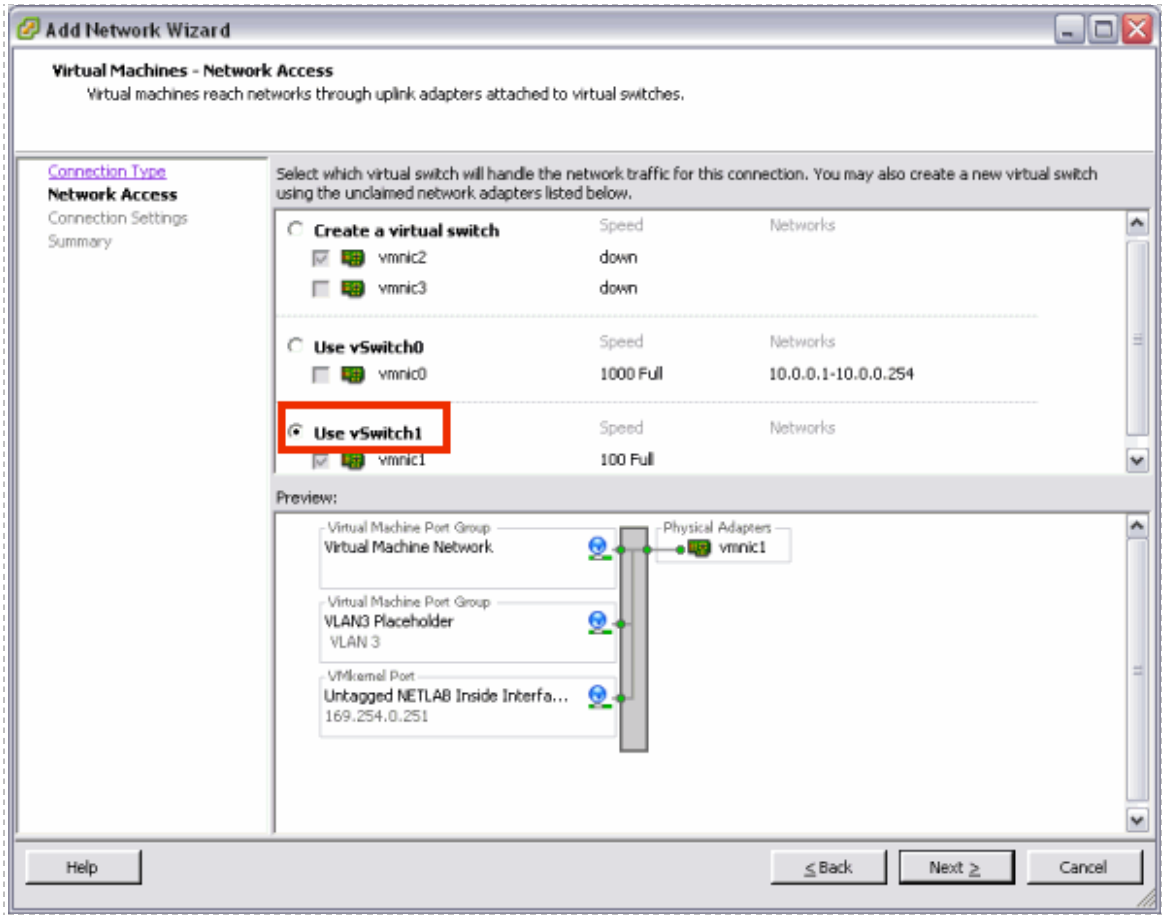


5.2.2 Selecting the Network Adapter

The VLAN adapter must be assigned to use the same virtual switch as the Inside Interface (section 3.6.2.2) and placeholder VLAN3 (section 3.6.3.3). In this example, vmnic1 was selected for the Inside Interface.

Using ESXi, all VLAN adapters are added to the same virtual switch as the Inside Interface.

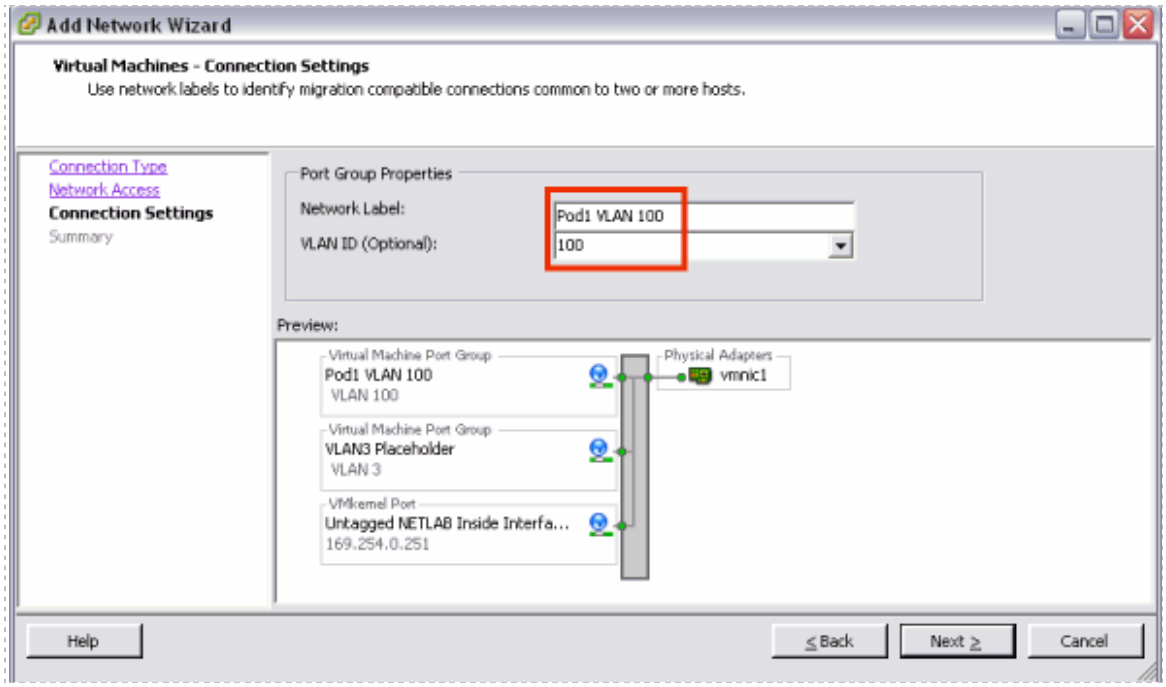
The selection and number of network adapters on your system will vary depending on your hardware selections.



5.2.3 Selecting Connection Settings

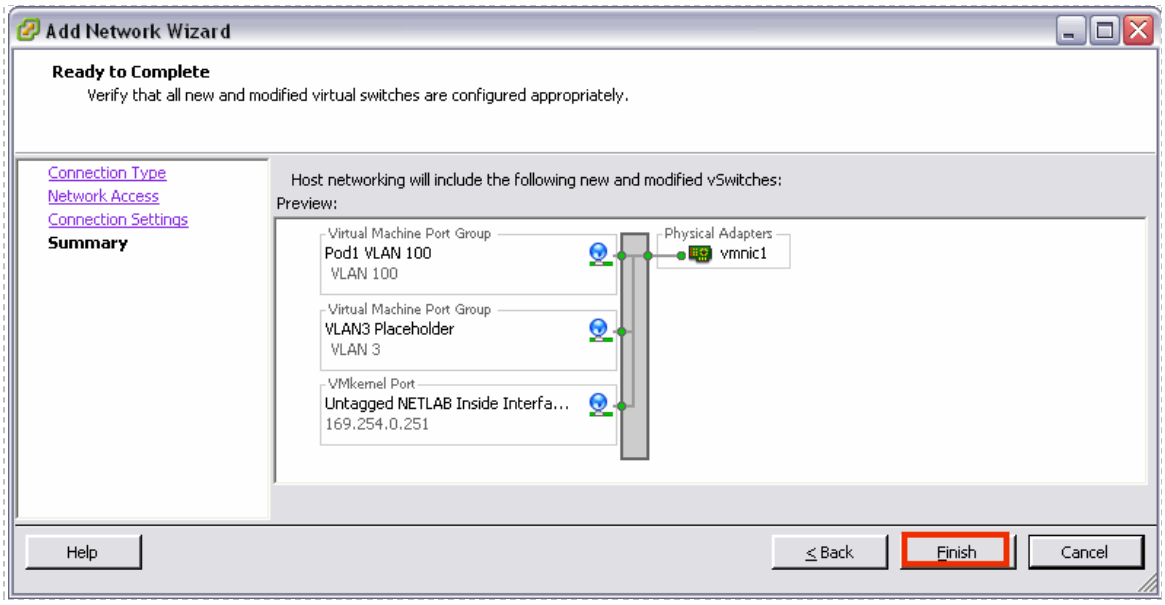
Use a descriptive name such as ***Pod id + VLAN number*** as the **Network Label**. Enter the **VLAN number** as the **VLAN ID**.

In this example, the network adapter was assigned a Network Label of Pod 1 VLAN 100.

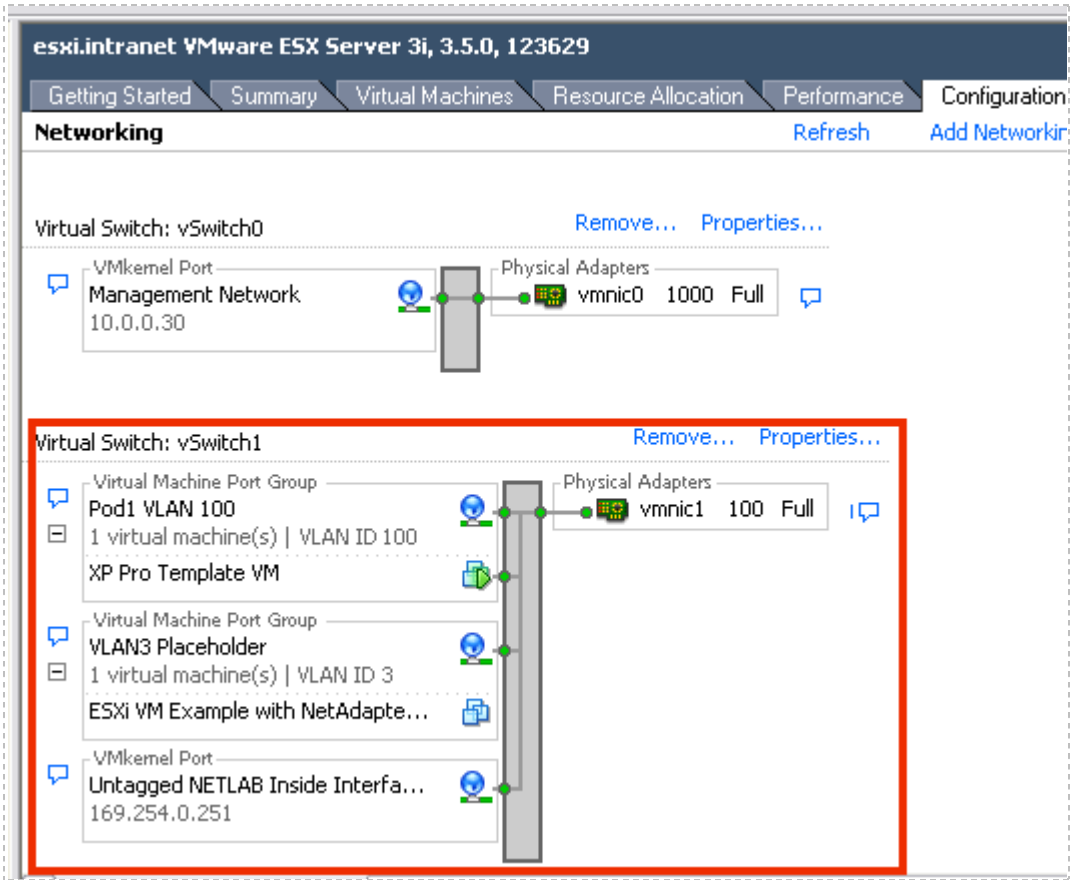


5.2.4 Finishing the Configuration of the VLAN Adapter

Select **Finish** to complete the configuration process.



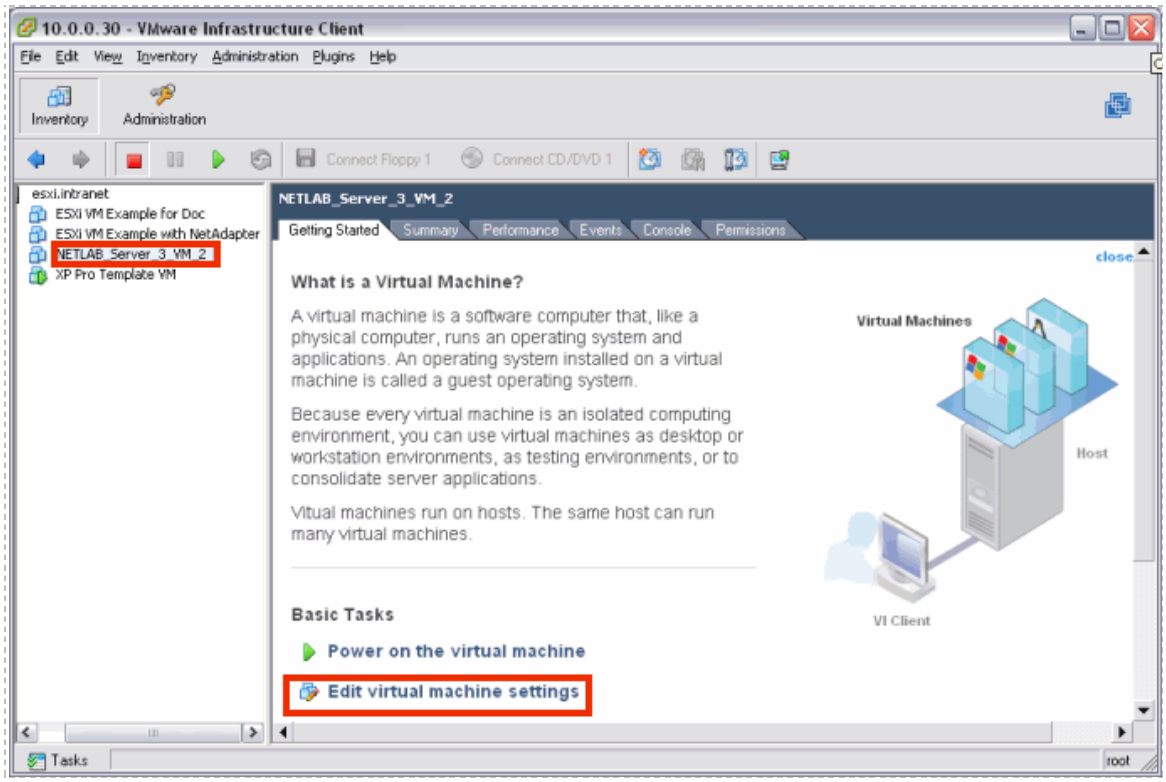
The VLAN adapter is now displayed on the networking page, on the same virtual switch as the Inside Interface and placeholder VLAN3. Return to section 5.2 and repeat this process for each VLAN adapter necessary for your system.



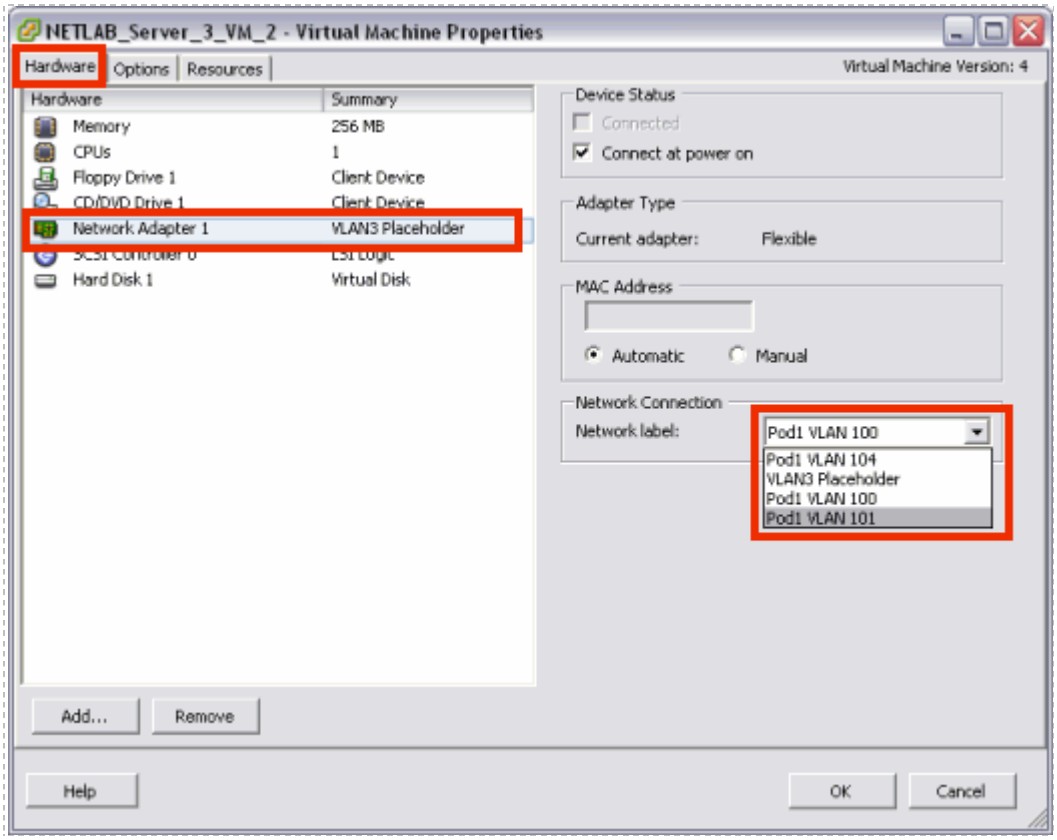
5.3 Configuring Virtual Machines to use the correct VLAN Adapter

Each virtual machine must be configured to use the appropriate VLAN adapter. Recall from section 4.1.7 that virtual machines were initially assigned placeholder VLAN3 as a network adapter. This setting must be edited for each VM, from the selection of VLAN adapters created in section 5.2.

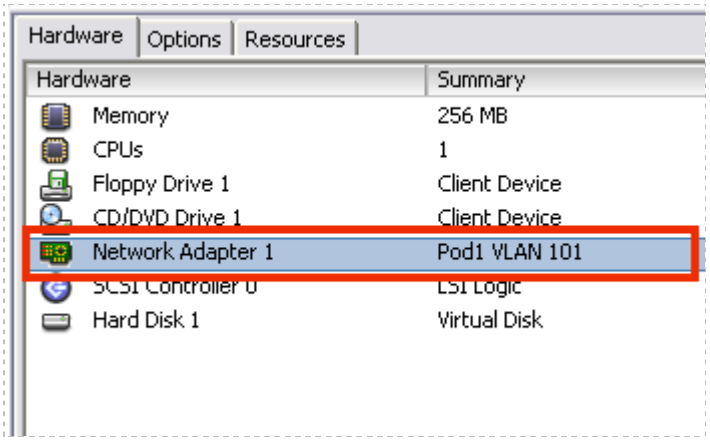
1. From the VI Client, **Getting Started** tab, select the virtual machine from the inventory list and select **Edit virtual machine settings.**



2. On the **Hardware** tab, select **Network Adapter 1**. Replace the current **Network Connection** of VLAN3 Placeholder with the appropriate VLAN adapter for this VM. Refer to section 5.1 to verify the appropriate VLAN adapter selection for the VM.



3. Your VLAN adapter selection is now shown on the Hardware tab.

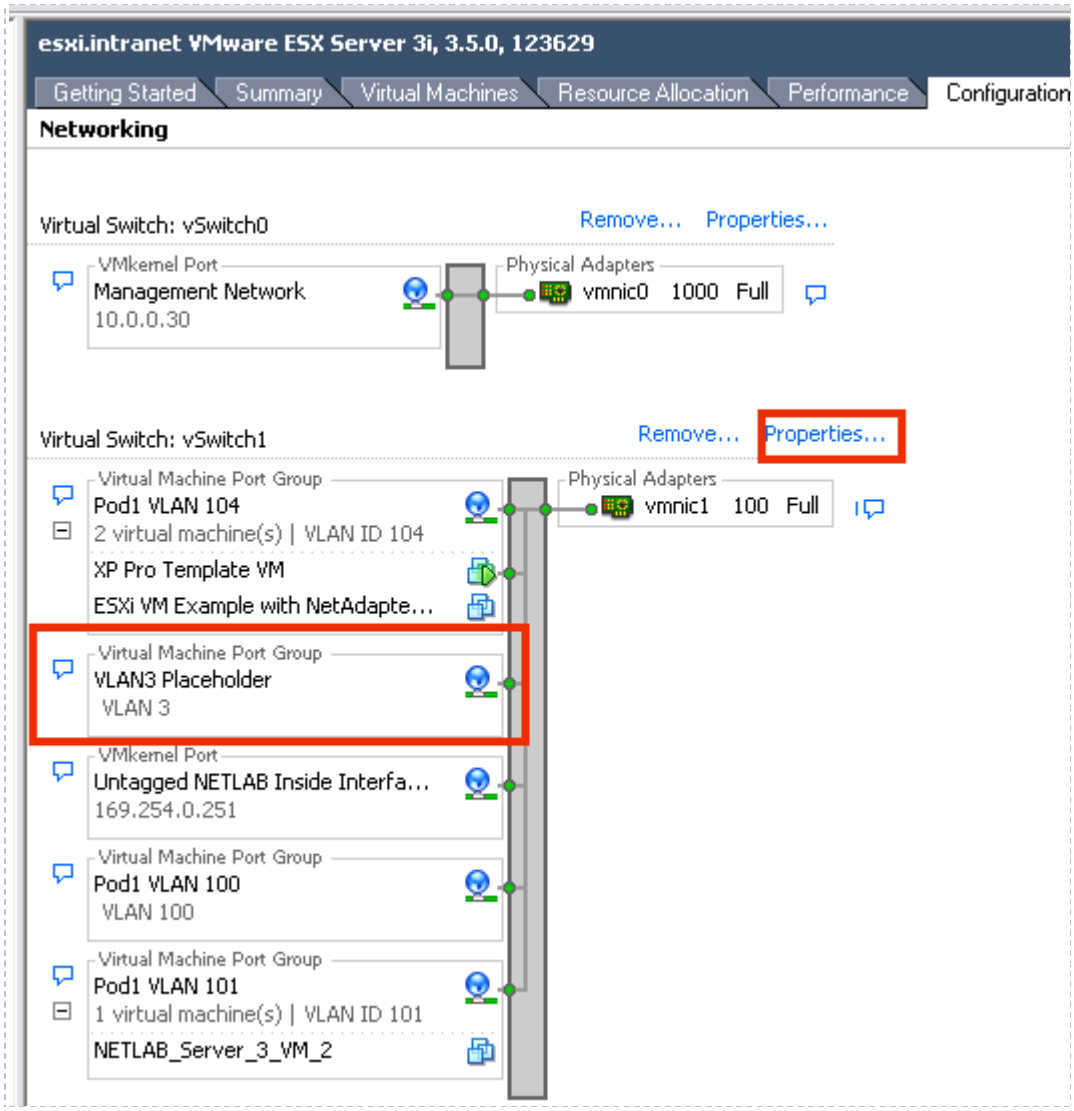


4. Take a final snapshot of your virtual machine (see section 4.9).

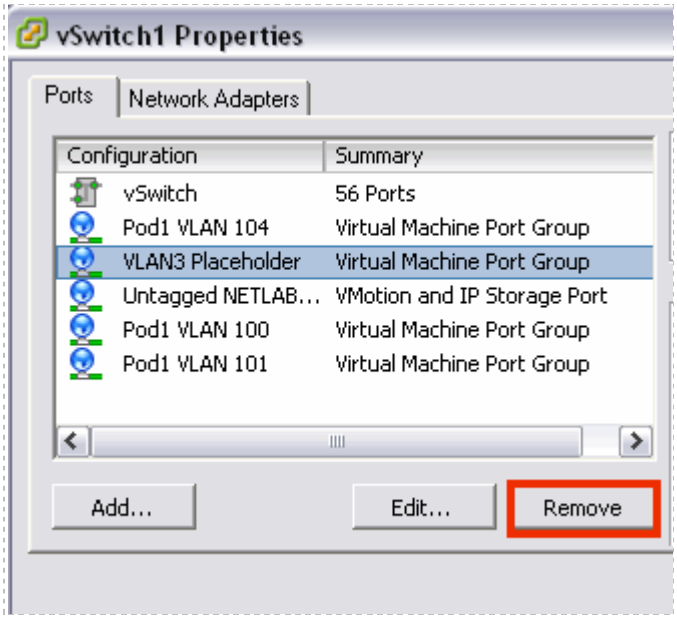
5.4 Deleting the Placeholder VLAN 3

Recall from section 3.6.3 that VLAN 3 was created as a temporary placeholder. This placeholder was necessary since at least one VM network connection type must be present prior to adding your first virtual machine. In section 5.3, each virtual machine was configured to use the appropriate VLAN adapter. Placeholder VLAN3 is no longer in use and may now be deleted.

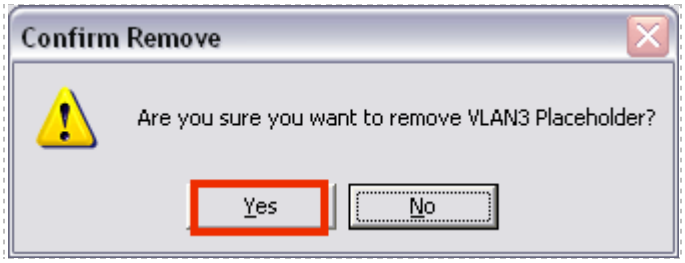
1. Select the option to display the **Properties** for the virtual switch of your Inside Interface.



2. Select **VLAN3 Placeholder** from the list displayed on the **Ports** tab and click **Remove.**



3. Select **Yes** to confirm the deletion.



Part 6 Verifying Connectivity and Troubleshooting

This section provides guidance on common troubleshooting issues associated with the implementation of ESXi with NETLAB+ and guidance on verifying connectivity after installation. Please review the material in this section prior to contacting NDG for customer support (see Appendix B).

Objectives

- Verifying connectivity between virtual machines and lab gear.
- Reviewing and/or modifying virtual machine settings for existing virtual machines.
- Identify and resolve the most frequently encountered issues.

6.1 Verifying Connectivity Between Virtual Machines and Lab Gear

We strongly encourage verifying the connectivity between your virtual machines and lab gear after completing the processes outlined in Part 5, using the method described in this section.

The troubleshooting methods shown here can also aid you in determining why a remote PC in a NETLAB+ pod is having network connectivity problems.

Verify that your pod is online (see the *Equipment Pods* section of the *NETLAB+ Administrator Guide*) and that the pod passes the pod test (see section 4.13).

The example below illustrates a NETLAB$_{AE}$ BRPv2 topology installed as Pod #5 on Control Switch #4:

BRPv2 Lab Device	Device Port	Control Switch #4 Port	NETLAB+ Pod VLAN
Router 1	fa 0/0	fa 0/1	140
	fa 0/1	fa 0/2	141
PC1a	virtual NIC	fa 0/23	140
PC1b	virtual NIC	fa 0/23	140
Router 2	fa 0/0	fa 0/3	142
	fa 0/1	fa 0/4	143
PC2	virtual NIC	fa 0/23	142
Router 3	fa 0/0	fa 0/5	144
	fa 0/1	fa 0/6	145
PC3	virtual NIC	fa 0/23	144

In order to test the connectivity between remote PCs and neighboring lab devices, using the above example, you may follow these steps, using an Instructor Account (see the *Manage Accounts* section of the NETLAB+ Administrator Guide).

1. Make a lab reservation.

2. Configure IP addresses on the remote PCs and neighboring lab devices you will be testing.

3. In the example above, PC1a and PC1b should share the same VLAN adapter, so they should be able to ping each other. If they cannot ping each other, then you should review the following:

    - What VLAN adapter are PC1a and PC1b using? (refer to 5.3).

    - Is there a firewall installed or enabled on the virtual machine?

4. To verify the connectivity between remote PCs and neighboring lab devices, you should test the following:

    - Ping from PC1a to R1 and vice versa.

    - Ping from PC1b to R1 and vice versa.

    - Ping from PC2 to R2 and vice versa.

    - Ping from PC3 to R3 and vice versa.

5. If you can ping from a remote PC to a neighboring lab device, but cannot ping from the lab device to the remote PC, then you may want to determine if there is a firewall installed or enabled on the virtual machine.

6. If any of the tests from step 4 completely fail (you cannot ping from remote PC to neighboring lab device and vice versa), then you will need to analyze the network traffic on the control switch. Using the above example, perform the following steps:

    - Connect a PC or terminal to the console port of the control switch.

    - Type **"show vlan"** or **"show vlan brief"** to view the VLAN status on the control switch.

The control switch console password is **router**. The enable secret password is **cisco**. These passwords are used by NETLAB+ automation and technical support - please do not change them.

```
Connected to 169.254.1.14.
Escape character is '^]'.


User Access Verification

Password:
netlab-cs4>en
Password:
netlab-cs4#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------
1    default                          active    Fa0/14, Fa0/15, Fa0/
                                                Fa0/18, Fa0/19, Fa0/
                                                Fa0/22, Fa0/24, Gi0/
3    NETLAB_3                         active
11   NETLAB_11                        active
12   NETLAB_12                        active
13   NETLAB_13                        active
140  NETLAB_140                       active    Fa0/1
141  NETLAB_141                       active    Fa0/2
142  NETLAB_142                       active    Fa0/3
143  NETLAB_143                       active    Fa0/4
144  NETLAB_144                       active    Fa0/5
145  NETLAB_145                       active    Fa0/6
```

During a lab reservation, you will notice the active lab ports and their VLAN assignments. From the example above, Pod #5 is a BRPv2 installed on ports fa0/1 through fa0/6 on Control Switch #4. The base VLAN for this pod is 140.

- On the control switch, type **"show interfaces trunk"** to view the trunk information.

```
netlab-cs4#show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/23      on           802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/23      140,142,144

Port        Vlans allowed and active in management domain
Fa0/23      140,142,144

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/23      140,142,144
```

This command will reveal whether or not you have properly configured the control switch port that connects to the VMware trunking port. The following shows the proper configuration for the example above on port 23 of Control Switch #4.

```
netlab-cs4#show running-config interface fastEthernet 0/23
Building configuration...

Current configuration : 252 bytes
!
interface FastEthernet0/23
 description trunk to VMware 10.0.0.25
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 140,142,144
 switchport trunk pruning vlan none
 switchport mode trunk
 switchport nonegotiate
 no ip address
end
```

- On the control switch, type “show mac-address-table dynamic”. Use the MAC address table to verify: 1) whether the MAC addresses of the remote PCs are in the table and 2) if these MAC addresses are in the correct VLANs.

```
netlab-cs4#show mac-address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 140    0000.0c5d.150e    DYNAMIC     Fa0/1
 140    000c.291d.6ee8    DYNAMIC     Fa0/23
 140    000c.292f.57f2    DYNAMIC     Fa0/23
 142    000c.291f.6542    DYNAMIC     Fa0/23
 142    0010.7b81.aae0    DYNAMIC     Fa0/3
 144    0000.0c76.bd12    DYNAMIC     Fa0/5
 144    000c.29c1.1bc7    DYNAMIC     Fa0/23
   1    000d.60f3.1757    DYNAMIC     Fa0/24
   1    0050.5000.1109    DYNAMIC     Fa0/24
   1    00c0.b763.c4ce    DYNAMIC     Fa0/24
   1    00c0.b7a3.1def    DYNAMIC     Fa0/24
Total Mac Addresses for this criterion: 11
```

7. If any of the tests from step 4 completely fail (you cannot ping from the remote PC to a neighboring lab device and vice versa), and the MAC address of a remote PC is either:
   a. Not in the correct VLAN or
   b. Does not show up in the control switch MAC address table, then please review the VLAN and settings for your NETLAB+ pod very carefully. Refer to Part 5 for complete details.

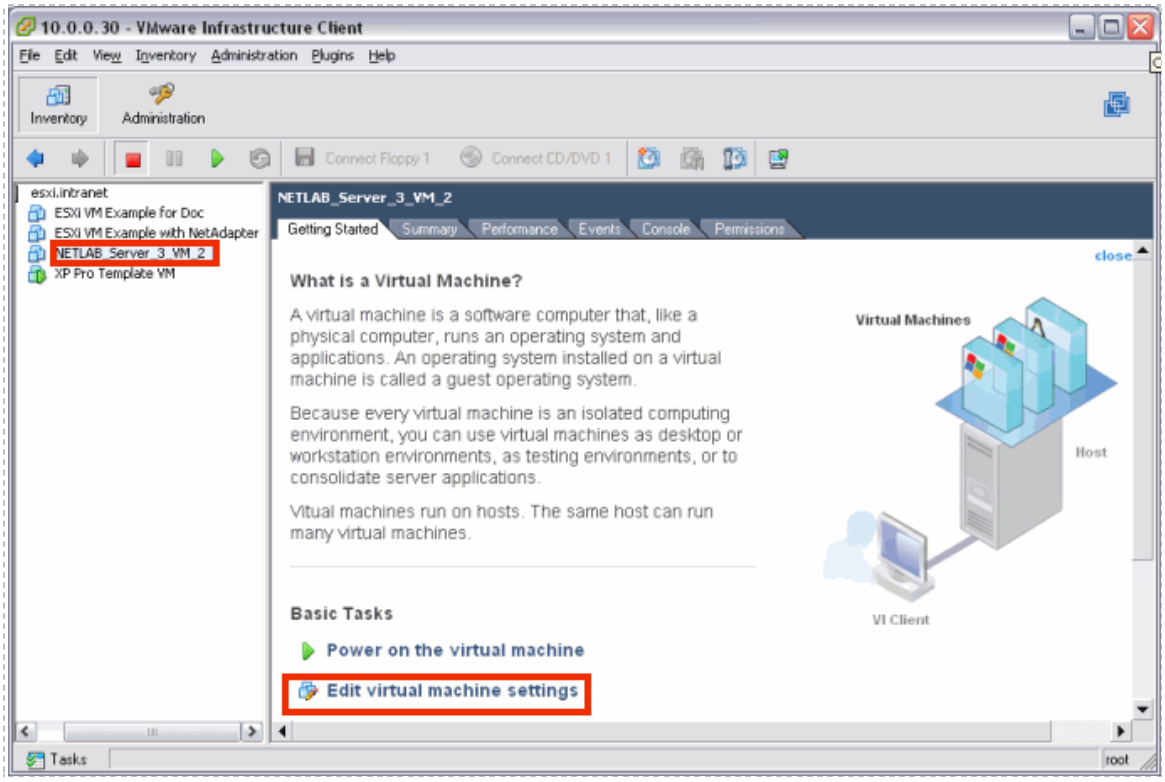
   Possible error conditions include:
   - An incorrect VLAN ID was entered when creating a VLAN interface.
   - No VLAN or an incorrect VLAN was mapped using VI Client
   - The control switch port (for the Inside Connection) is not trunking or not allowing the correct VLANs.

If you are in the process of installing a new NETLAB$_{AE}$ pod on your NETLAB+ system, please return now to the respective pod-specific guide for your pod. The final chapters, *Testing the Pod*, and *Finishing Up* provide details that will allow you ensure your pod is installed properly and ready for use.

6.2 Review and Modify VM Settings For an Existing Virtual Machine

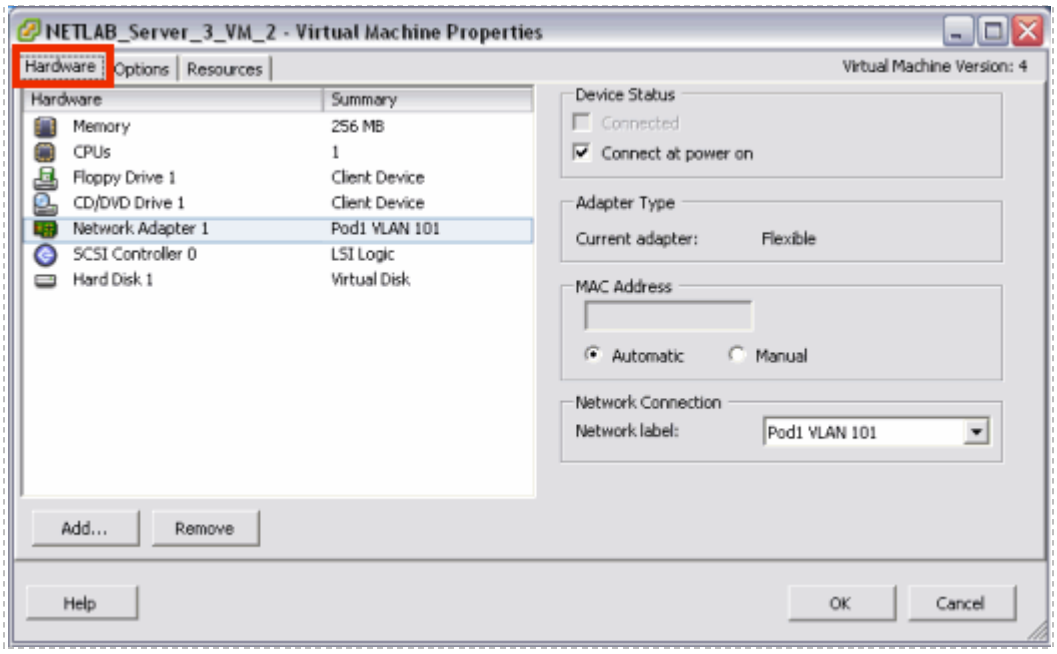
Section 4.1 outlined the creation of new virtual machines using the VI Client. This section describes how to verify and/or modify the VM settings of an existing virtual machine for integration with NETLAB+.

From the VI Client, **Getting Started** tab, select the virtual machine from the inventory list and select **Edit virtual machine settings.**

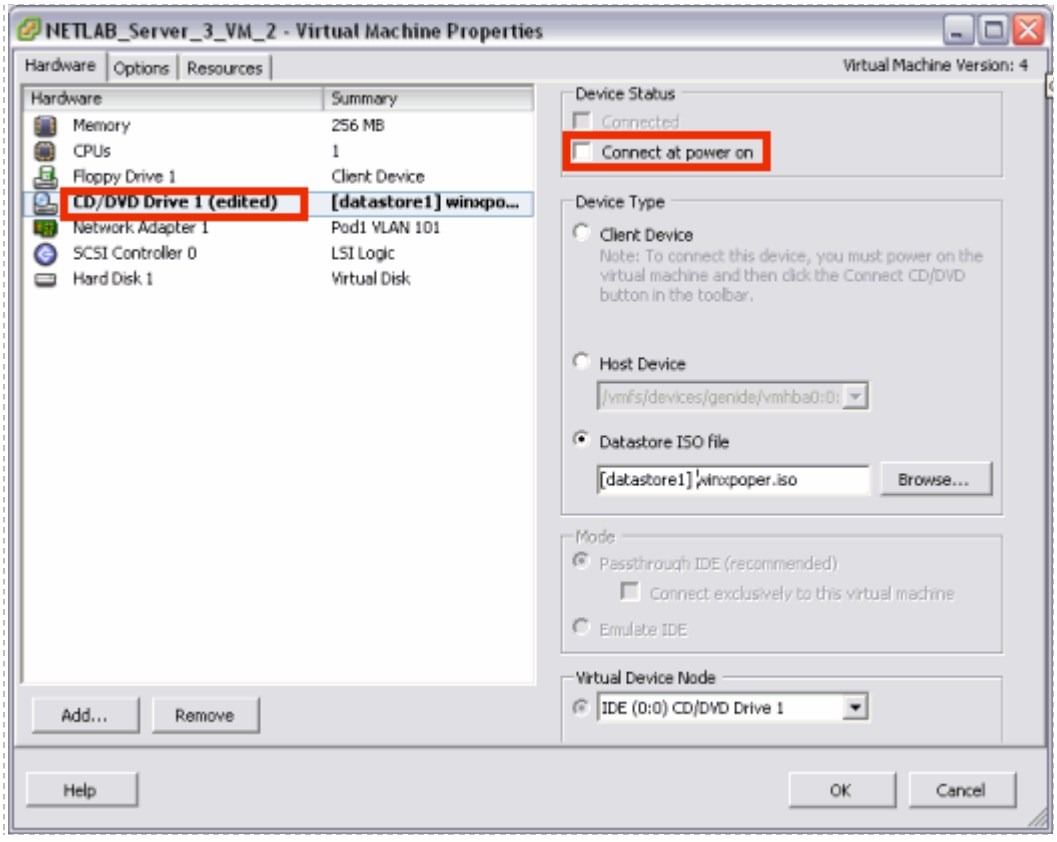


The current hardware settings, including the Network Adapter are available on the **Hardware** tab. See section 5.3 for details on selecting the network adapter.

The settings shown are for example purposes only, your settings will vary.

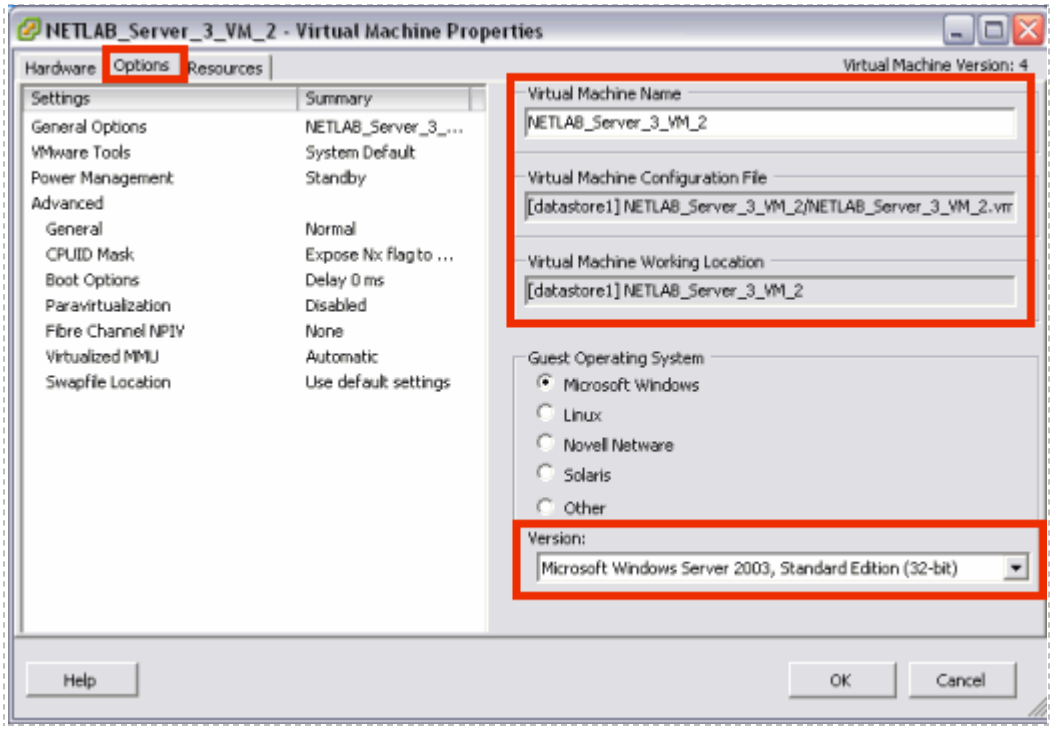


Verify that the Connect at Power on setting of the CD/DVD drive is ***Unchecked***. You may also point the CD/DVD device connection to a unique ISO image on the local ESXi host. If you choose this option, make sure each VM you create does not point to the same ISO file. Otherwise, you may see some undesired properties or boot errors.



The settings on the Options tab include the Virtual Machine Name, Configuration File, and your selection of guest operating system.

The file names shown here are for example purposes, your selections may vary.

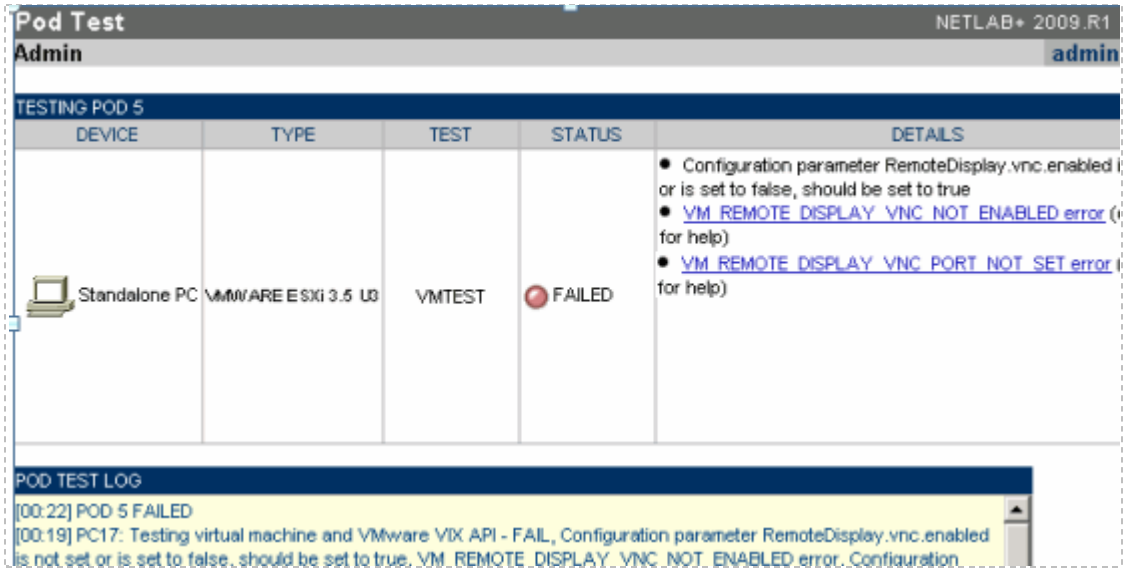


6.3 The Most Frequently Encountered ESXi Issues

If you are experiencing problems with your virtual machines or they are not passing the pod test, please review the following symptoms and resolutions carefully:

1. **Symptom:** The user runs a pod test and the results indicate that the remote display settings are missing or misconfigured.

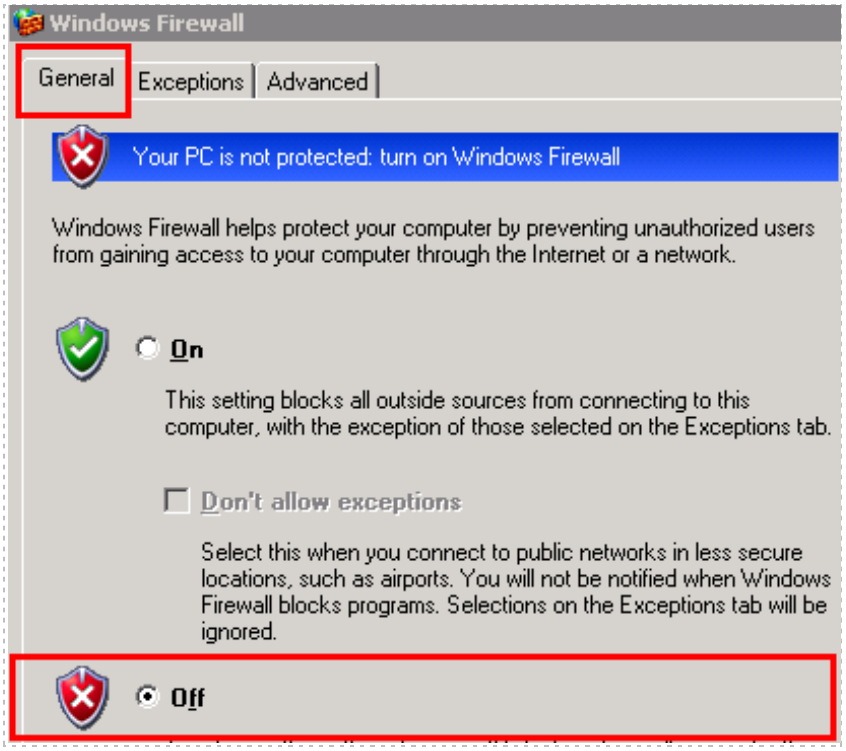
Additional information regarding error conditions is available by selecting the hyperlinked text within the details section of the pod test results.



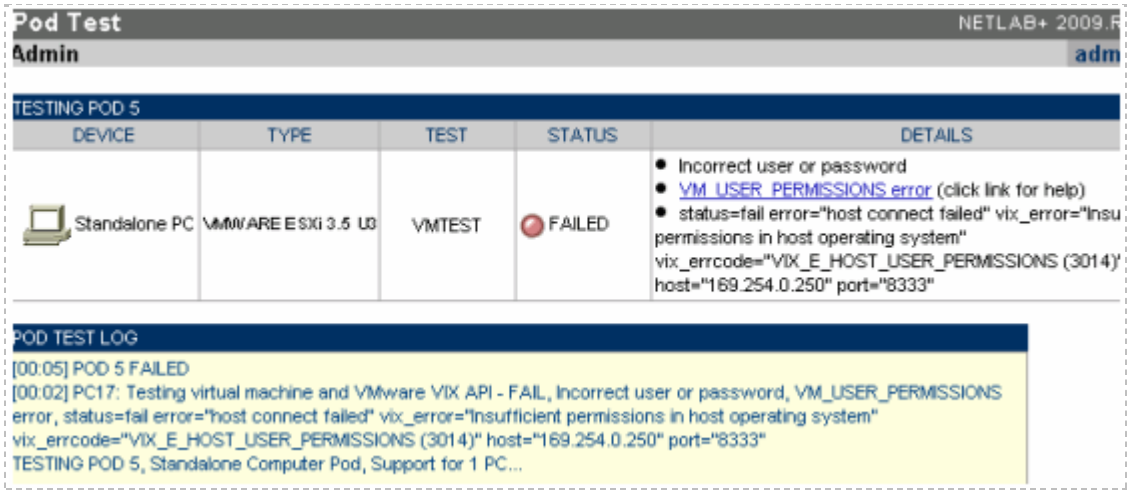
Resolution: Each virtual machine allocated for a NETLAB+ pod for remote PC access should have the VNC settings saved into the VMX file. This procedure is described in section 4.12.

2. **Symptom:** You are unable to ping lab gear from the virtual machine.

   Resolutions: See section 6.1 for an example of a troubleshooting scenario.
   a. Each virtual machine should be mapped to the proper VLAN adapter. Reference section 5.3 for full details.
   b. Disable built-in firewalls on the virtual machine (Windows firewall, for example).



3. **Symptom:** A Pod test failure indicates API-Fail incorrect user or password.



Resolution: Make certain you have created the management account (section 3.7) and you added to proper permissions (section 3.9).

4. **Symptom:** My keyboard and/or mouse are behaving very erratically (sub as, double letters, or the mouse is very jumpy) when using the NETLAB+ Remote PC viewer.

   Resolution: Each virtual machine should have **VMware Tools** installed. Refer to section 4.4 for details.

5. **Symptom:** I am using a non-Windows guest operating system, and I cannot get the mouse to behave properly.

   Resolution: Some guest operating systems, such as Linux, require very specific steps to install VMware Tools properly. For example, most Linux VMs require you to run a configuration script to complete the VMware Tools installation. Do not assume that VMware Tools is properly installed without reviewing the guidelines as per the VMware documentation: http://kb.vmware.com/selfservice/dynamickc.do?externalId=340&sliceId=2&command=show&forward=nonthreadedKC&kcId=340.

6. **Symptom:** You are in a NETLAB+ reservation and the Remote PC viewer is slightly sluggish in performance.

   Resolution: Each virtual machine should be adjusted for optimum remote display access (see section 4.5):

   a. Minimal screen resolution with 32-bit color quality (see sections 4.5).

   b. Do not use a graphical background. The desktop background should be plain or none (see section 4.7).

   c. Adjust the visual effects for best performance (each O/S may have different settings, see section 4.6).

7. **Symptom:** Your virtual machines are giving an "UNKNOWN" status from the Status tab of a lab reservation in NETLAB+.

   Resolution: Review the following potential causes:

   a. We recommend no more than 10 to 12 virtual machines, per server that meets the minimum requirements in section 2.2. Each virtual machine uses CPU cycles and memory on the server. As a simple rule of thumb, divide the processor clock speed by the number of virtual machines to determine the speed of each virtual machine in a heavily loaded environment (i.e. all pods are running at the same time and users are working on the PCs). For example, a 3GHz processor could run 10 virtual machines at 300MHz each.

   If your VMs are running in a heavily loaded environment, the VMware daemon process may stall, hang, or become unresponsive. This could cause requests from the NETLAB+ server to be ignored. This would give an "UNKNOWN" status for your remote PCs from the Status tab of a lab reservation in NETLAB+.

   b. Each virtual machine should have their virtual CD/DVD device disabled, (section 4.3).

   c. Verify each VM setting from section 6.2.

Appendix A Copying VMDK File to Clone Virtual Machines

Once you have successfully created a single virtual machine, you may clone this VM to create new VMs as a short cut. This would essentially save the time it takes to install a new guest operating system and VMware Tools.

Each guest operating system is fully functional and must meet the vendor's licensing requirements (see section 2.1.1).

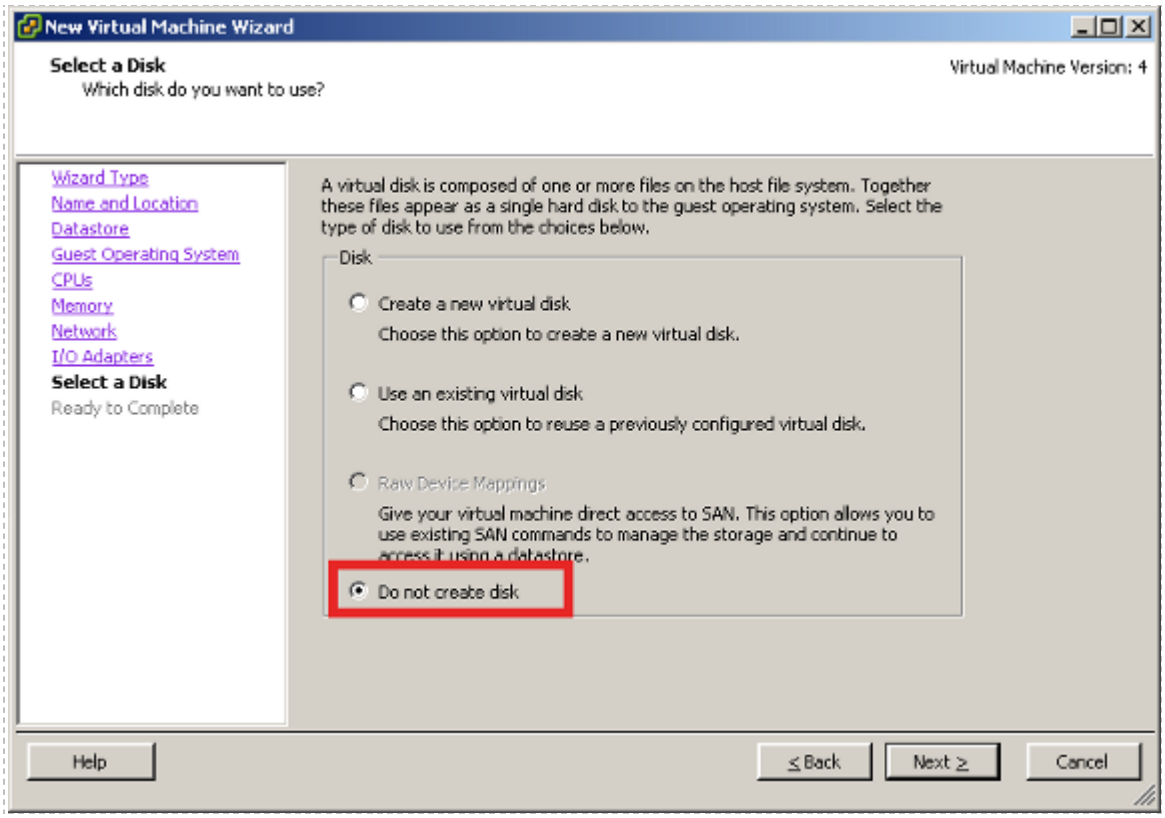
This short cut is useful only if your NETLAB+ pod VMs will have similar virtual machine settings:

- VM memory size (can be adjusted easily after new copy is created)
- VM hard disk size (**cannot** be adjusted easily)
- VM Operating System (this must be the same if you are cloning)

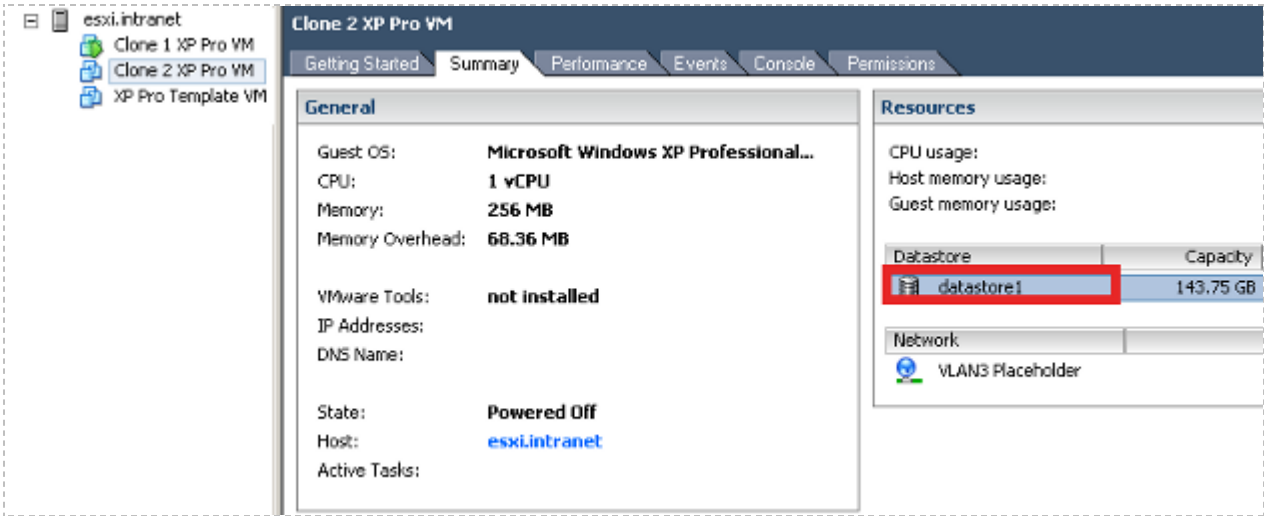
 Make sure to copy the first VM's VMDK after you have added VMware tools, and all other applications that you want on the VM. This will allow you to avoid making multiple changes on every VM.

The following steps highlight the procedure for cloning your virtual machine to create new VMs. It is assumed you have successfully created a single VM as per Part 4.

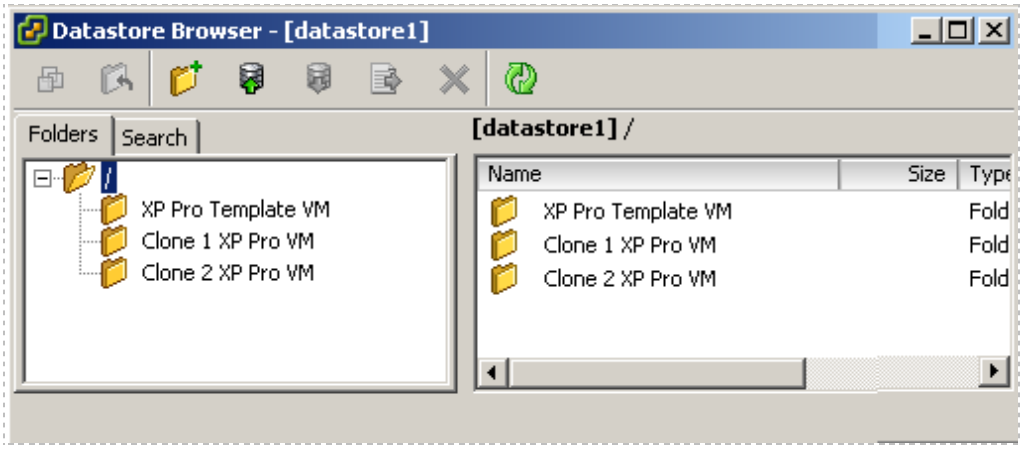
1. Proceed through the steps outlined in section 4.1 to create a new virtual machine, with the exception of the option selected in step 4.1.9. Instead, use the **Do not create disk** option for this clone virtual machine. This option is used since we are going to copy and paste the first VM's VMDK file into the new VM datastore directory.



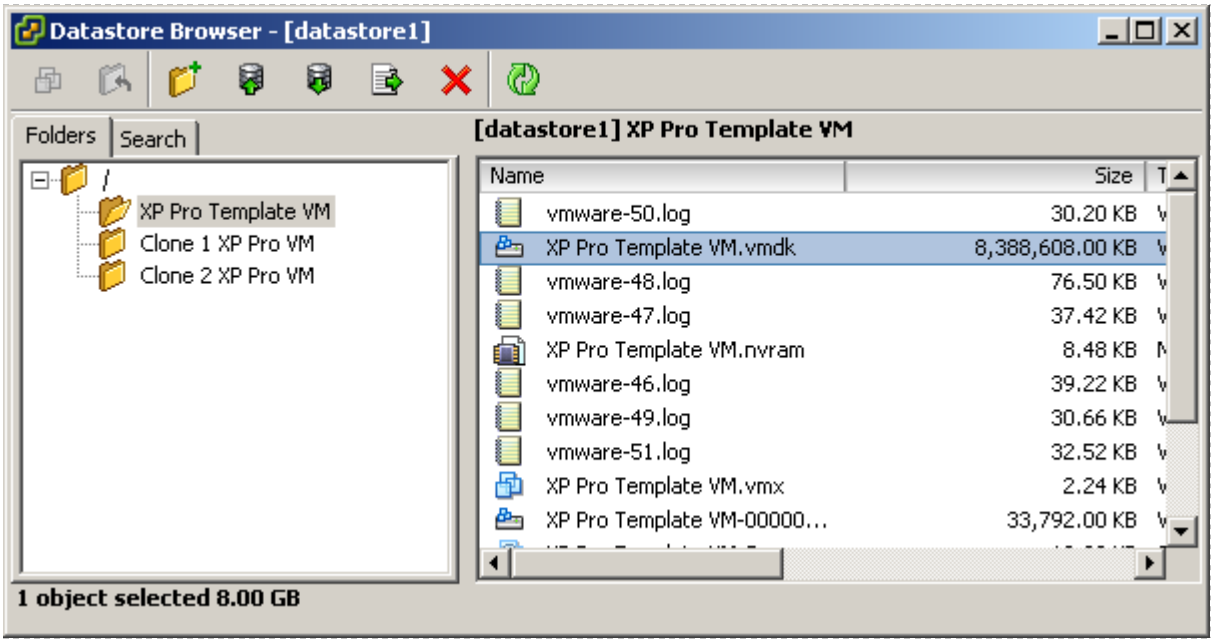
2. Locate the **datastore** of the clone virtual machine on the **Summary** tab.



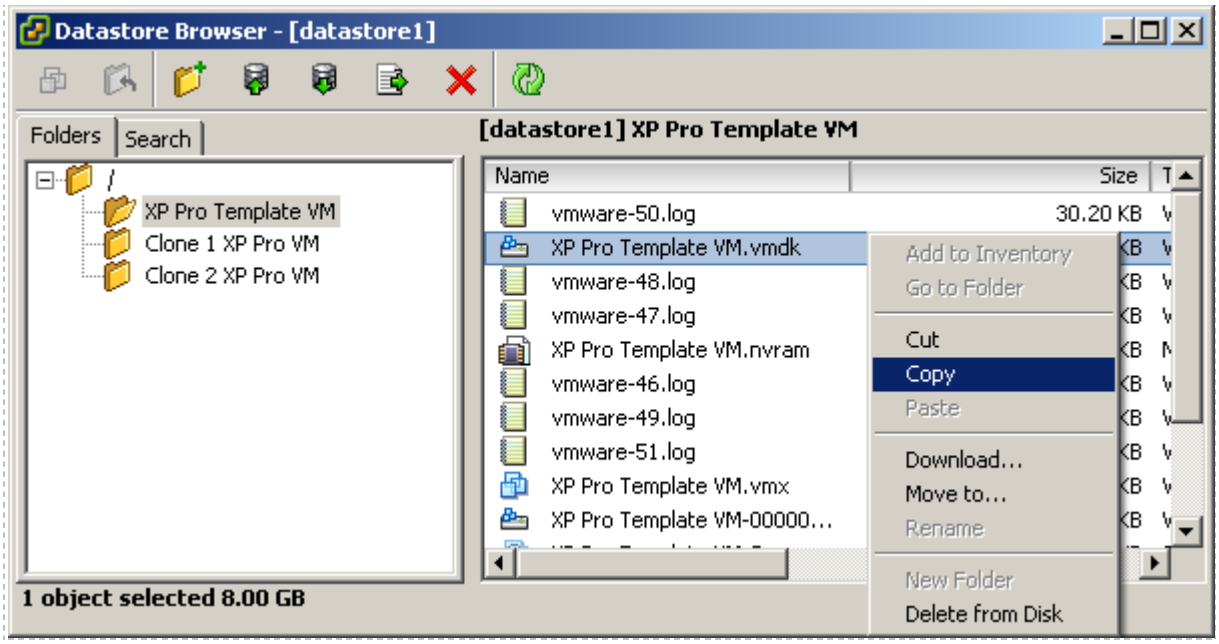
3. Double-click to open the **Datastore Browser**



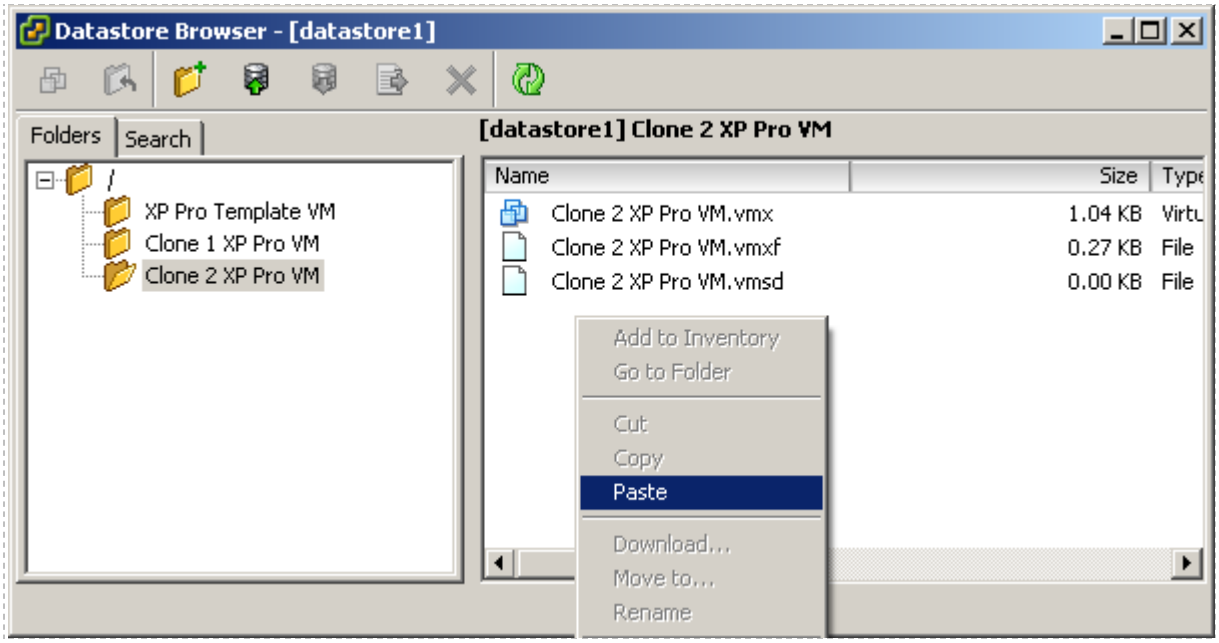
4. Navigate to the first VM that was installed and locate the VMDK file.



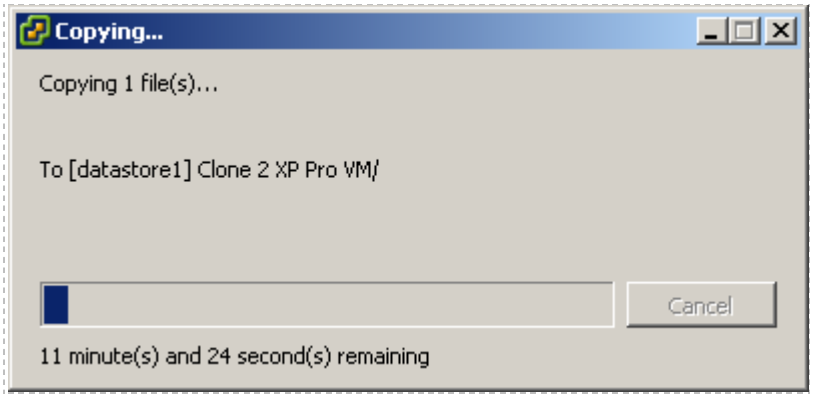
5. Copy the VMDK file.



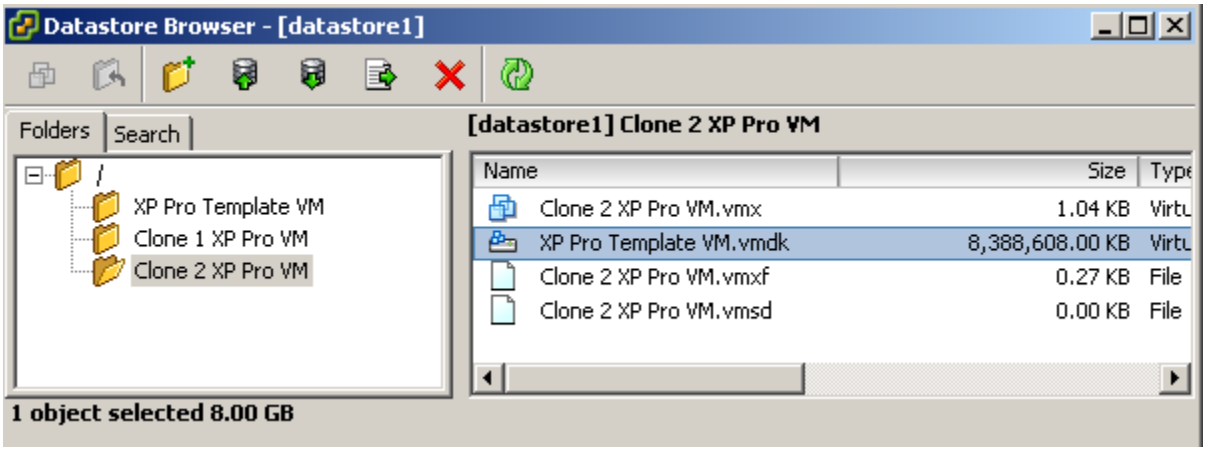
6. Navigate to the clone VM directory. Notice there is no VMDK file (because in step 1 we did not create a disk). Paste the VMDK file into this directory.



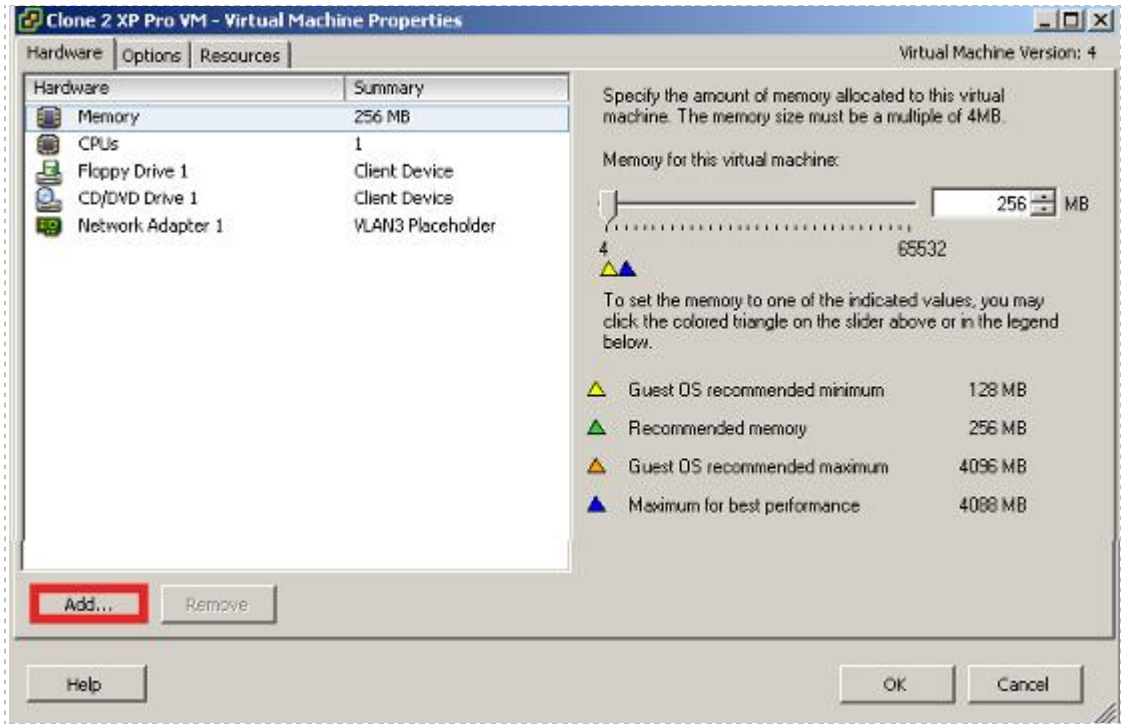
It may take several minutes to copy and paste this file.



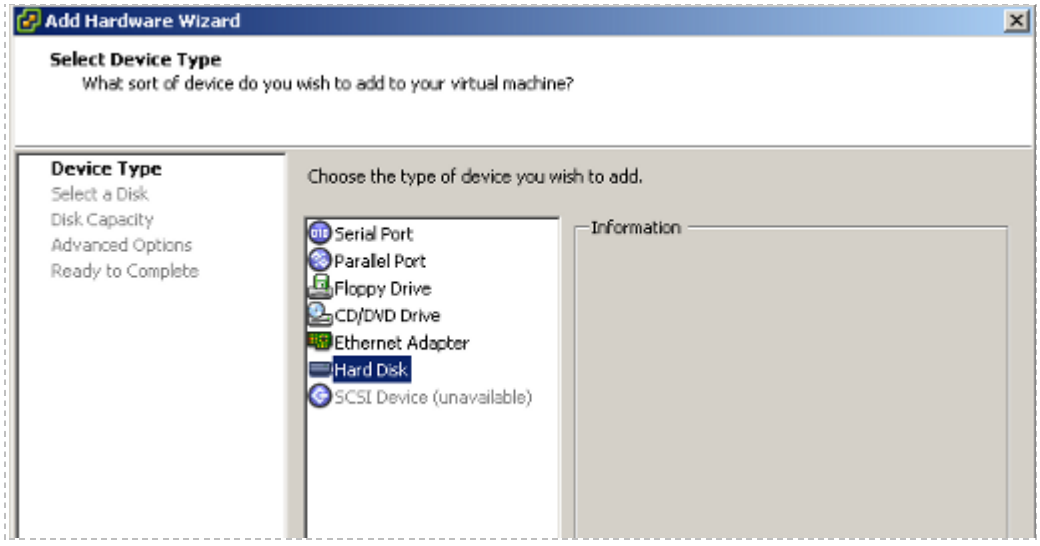
The file will be listed in the directory when the copy/paste is complete.



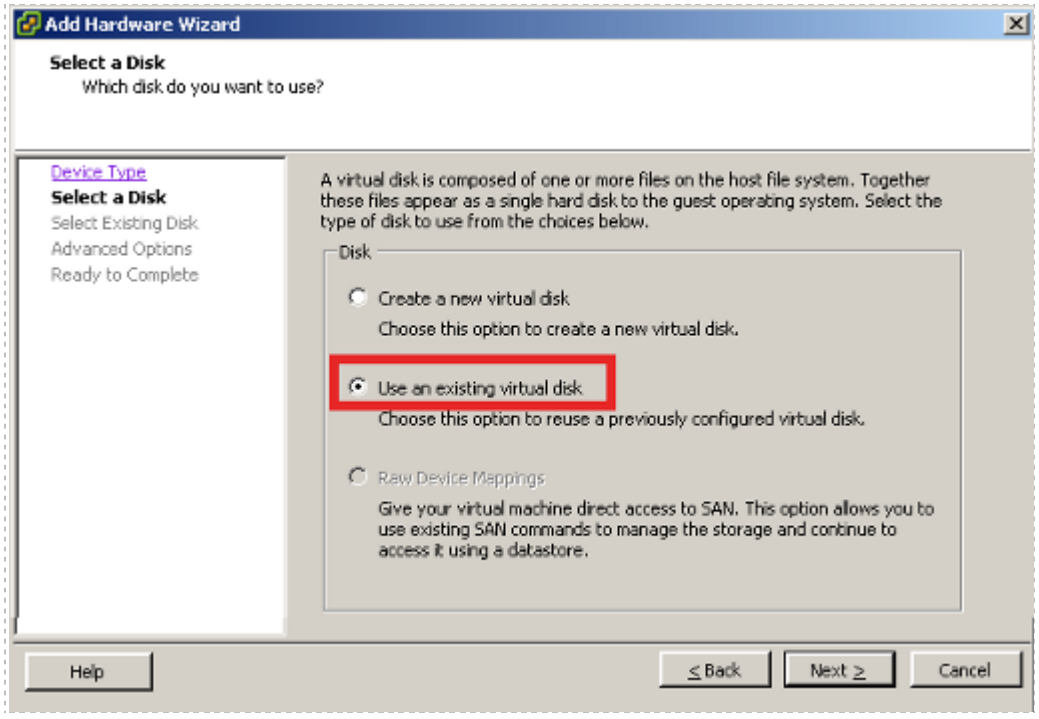
7. Navigate to the clone VM properties and click on **Add hardware**.



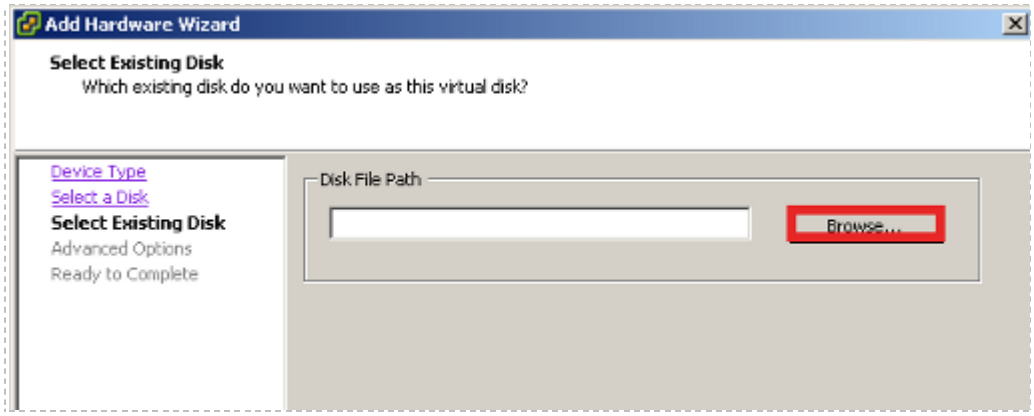
8. We will now add a hard disk.



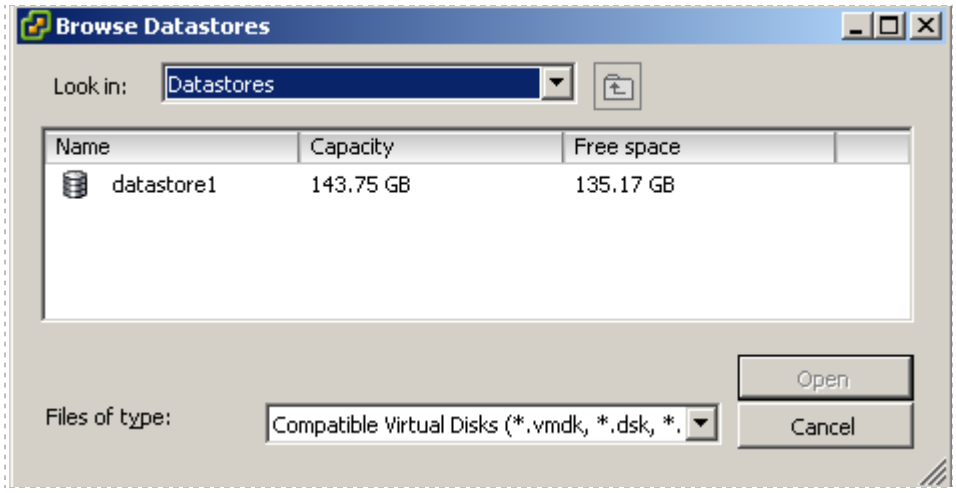
9. Select the **Use an existing virtual disk** option, since we will select the VMDK file that was pasted as the virtual disk for this clone.



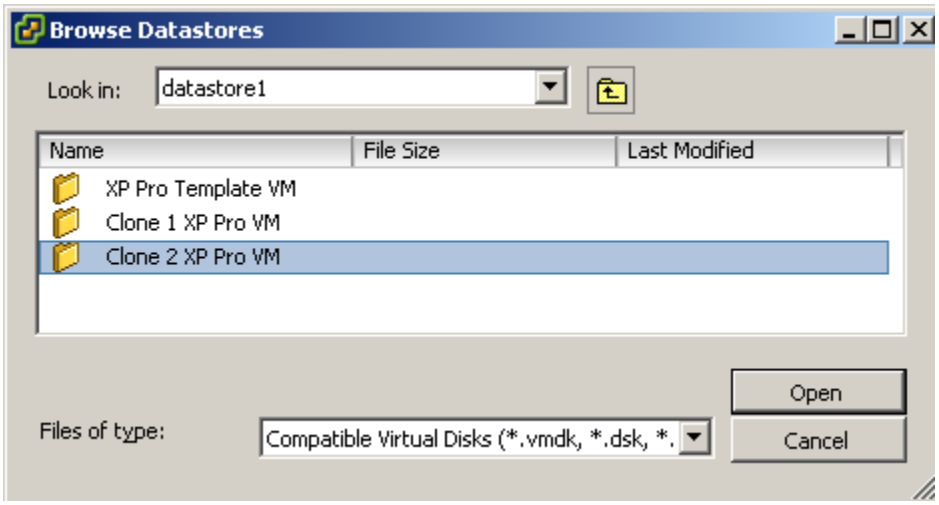
10. Browse to the VMDK file that was pasted into the clone directory.



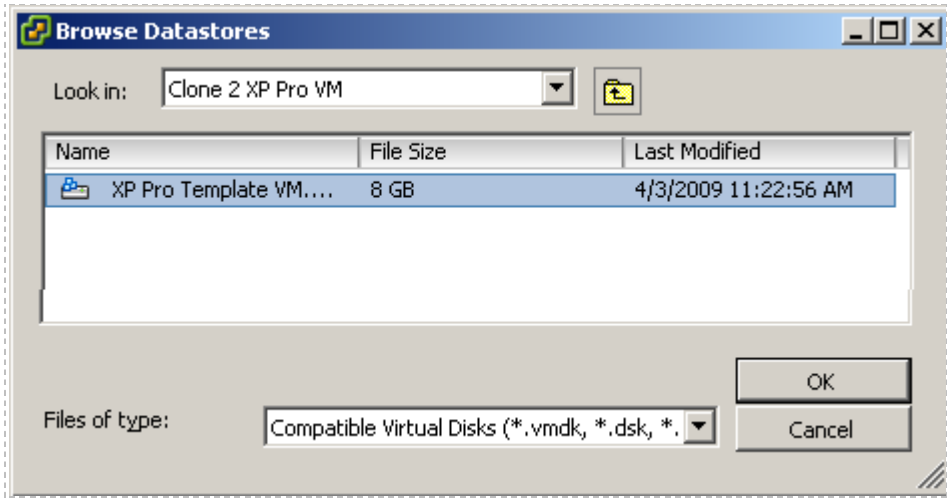
11. Selecting browse will display the **Browse Datastores** page.



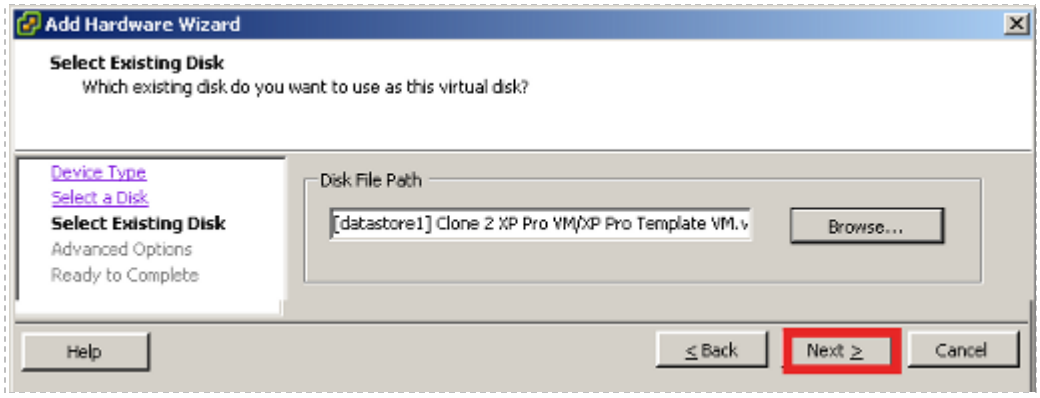
12. Make sure to pick the correct directory.



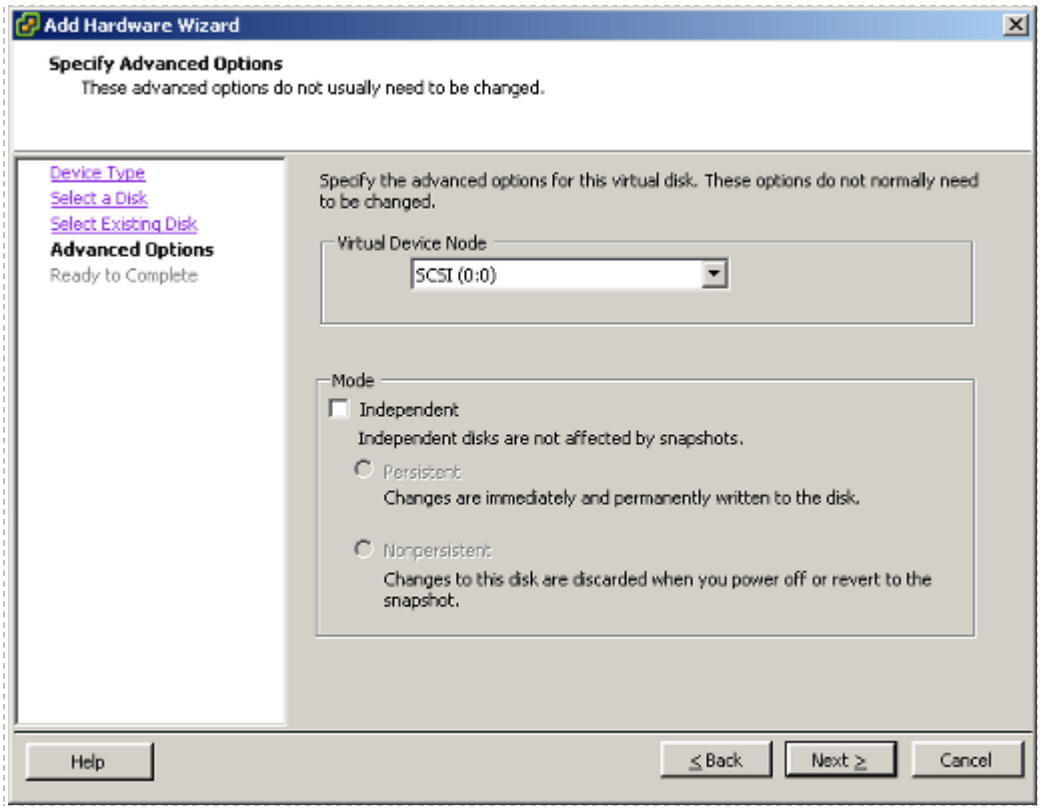
13. Select the VMDK file.



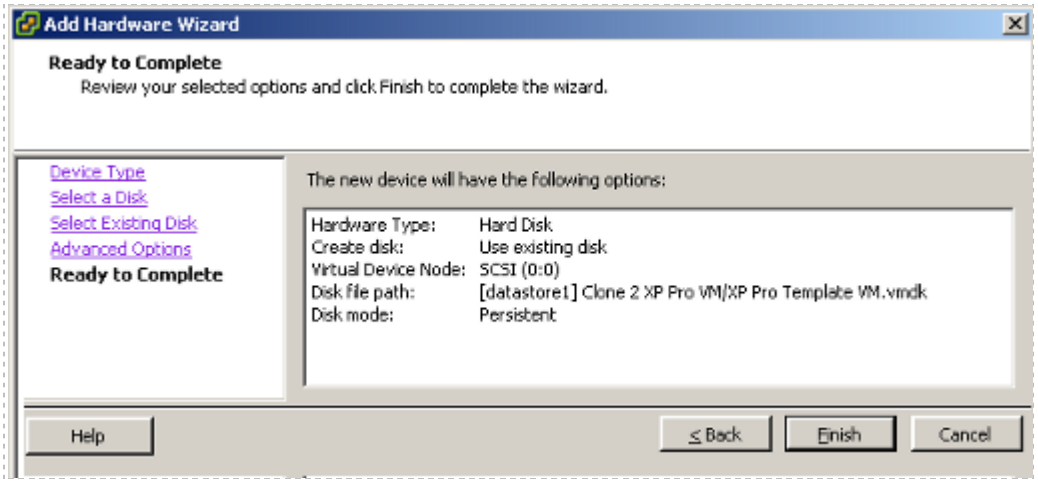
14. Select **Next** to continue with the **Add Hardware Wizard**.



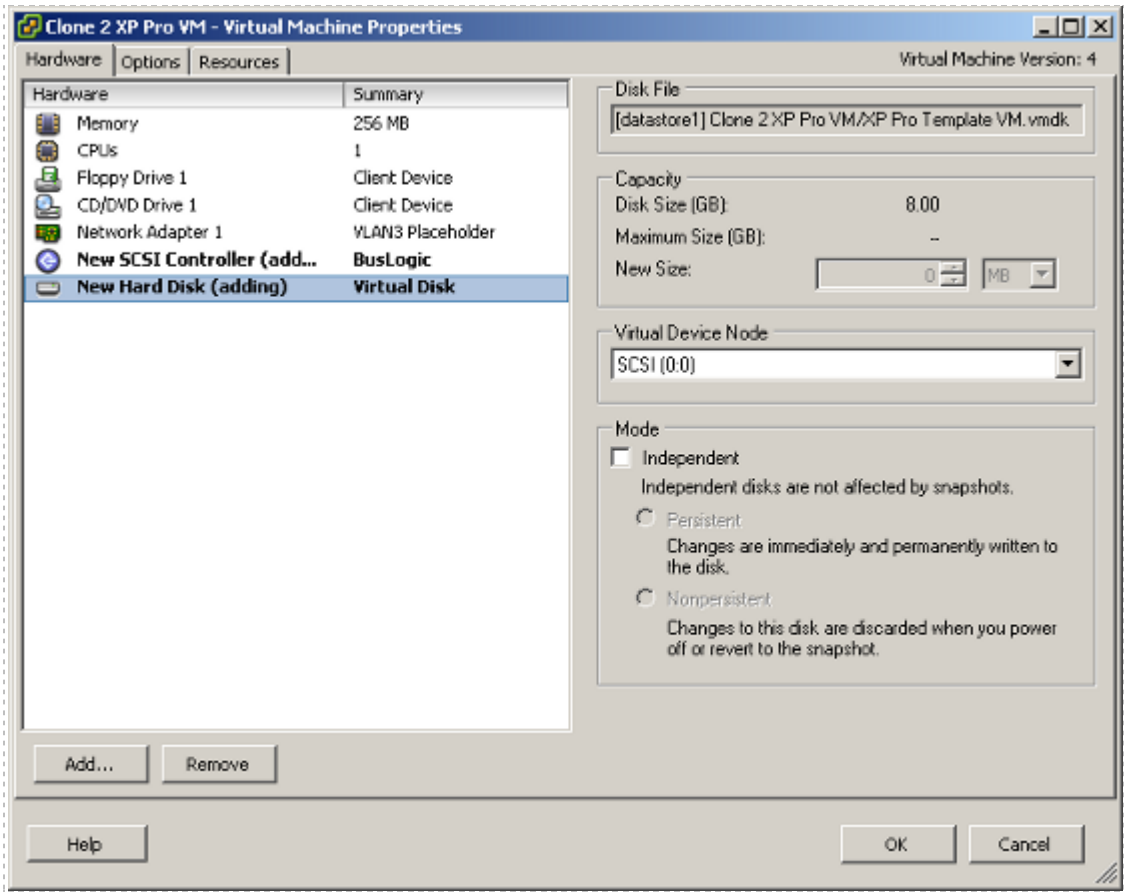
15. Keep the default **Advanced Options** (these should match the first VM). The following screenshot is an example and may be different for your ESXi server (depending on the hardware platform used).



16. Click on **Finish** to complete clone VM.



17. The hard disk and controller will now appear on the hardware list.



18. Your new clone VM should now boot immediately into the same state as the first VM (depending on what stage you copied the VMDK).

Appendix B Contacting NDG for Technical Support

If you need to contact NDG for support, please be aware that VMware ESXi is a third party product. NDG cannot transfer a customer to the VMware help desk, but we will do our best to help you setup and operate a remotely accessible PC or server using supported VMware virtualization products on your NETLAB+ system under the following guidelines:

1. The NETLAB+ administrator has thoroughly studied the NDG documentation including this guide, and attempted to install Virtual Machines (VMs) based on NDG recommendations.

2. Remote access to both the VMware ESXi and NETLAB+ server provides the most effective way for NDG to assists customers.

    a. NDG provides up to 2 hours of support assistance for customers with current NETLAB+ support agreements if remote access is enabled.

    b. Remote access to the NETLAB+ server is provided via SSH (preferred) or Telnet. Please reference the NDG CSS whitepaper for port details.

    c. We request that the NETLAB+ administrator be present while NDG is providing assistance.

Appendix C Upgrading from VMware Server 1.x, 2.x, or GSX to VMware ESXi

1. Modify the **PC Type** setting to **VMware ESXi 3.5 U3**. This value is must be set for each virtual machine that you are upgrading to VMware Server 2.x. Please refer to 4.11 for details.

POD 1 - PC 203	
PC ID	203
PC Name	PC3
Type	VMWARE ESXi 3.5 U3
VMware Host IP Address	10.0.0.30
VMware Host Username	netlab
VMware Host Password	NETLAB.API.10.0.0.30
VMware Guest Configuration File	[datastore1] XP Pro Template VM/XP Pro Template VM.vm
VMware Guest Operating System	Windows XP
VMware Guest VNC Settings	RemoteDisplay.vnc.enabled = "true" RemoteDisplay.vnc.port = "6103"
Access Method	VNC
Admin Status	ONLINE
Options	revert to snapshot during scrub operation

2. If you are upgrading from VMware Server 1.0 or GSX you must modify the value of the VMware Guest Configuration file to the format of a relative path name. This file name is typically in the form of [datastore]<*pc name*>/<*operating system*>.vmx. Example: [standard] POD_1 PC_3/winXPpro.vmx. Please refer to 4.11 for details.

   The use of relative path names is specific to VMware Server 2.x and ESXi. VMware server 1.0 and GSX require absolute path names. If you are upgrading from VMware Server 1.0 and GSX, you must change your configuration file path names to use relative path names, as shown in the example above.

3. Run at pod test to verify the function of the API, see section 4.13.