NDG NETLAB+®

NISGTC
The National Information, Security & Geospatial Technologies Consortium

POD INSTALLATION AND CONFIGURATION GUIDE

Forensics

Document Version: 2016-05-05

Contents

1   Introduction

This document provides detailed guidance on performing the installation and configuration of the Forensics pod on the NETLAB+ system.

1.1   Introducing the Forensics Pod

The Forensics pod is a 100% virtual machine pod consisting of 7 virtual machines. Linked together through virtual networking, these 7 virtual machines provide the environment for a student or team to perform the Forensics labs. The following image is the pod topology for this lab series.
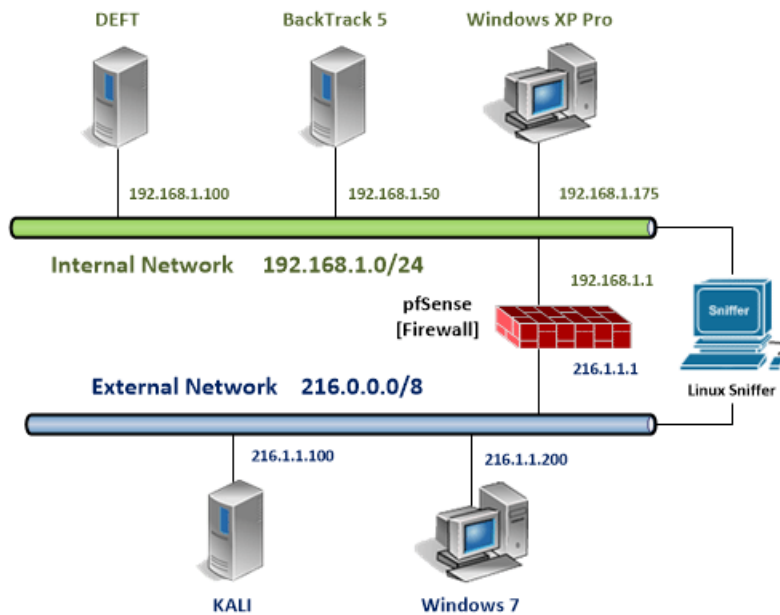
2   Planning

This guide provides specific information pertinent to delivering the Forensics course. The _NETLAB+ Remote PC Guide Series_ provides the prerequisite guidance for setting up your VMware infrastructure, including:

- An introduction to virtualization using NETLAB+.
- Detailed setup instructions for standing up VMware vCenter and VMware ESXi.
- Virtual machine and virtual pod management concepts using NETLAB+.

This document assumes that you have set up virtual machine infrastructure in accordance with the _NETLAB+ Remote PC Guide Series_. The planning information below refers to specific sections in the Remote PC Guide when applicable.

2.1   Pod Creation Workflow

The following list is an overview of the pod setup process.

1. Obtain the master virtual machine images required for the pod.
2. Deploy the master virtual machine images to a master pod.
   a. Deploy virtual machines using Thin Provisioning to reduce storage consumption.
   b. Make necessary adjustments to each virtual machine in the environment.
      i. Insert manual MAC addresses.
      ii. Change default network to SAFETY NET.
3. Import the virtual machines deployed to the NETLAB+ Virtual Machine Inventory.
4. Activate or license the required software on each virtual machine.
5. Take a snapshot of each virtual machine in the master pod labeled GOLDEN_MASTER. The GOLDEN_MASTER snapshot is used to clone virtual machine images for the user pods.
6. Create copies of the virtual machines in the master pod on VMware host using the NETLAB+ Pod Cloning feature.
7. If multiple hosts are used in the NETLAB+ environment, make a full clone of the master pod on the initial host (Host A) to the subsequent host (Host B), using the NETLAB+ Pod Cloning Feature.

2.2 Pod Resource Requirements

The Forensics course will consume 57.1 GB of storage per each user pod instance.

The following table provides details of the storage requirements for each of the virtual machines in the pod.

Virtual Machine	Initial Master Pod (Thin Provisioning)
Deft	5.5
Backtrack	15.11
Windows XP Pro	2.6
pfSense	.2
Linux Sniffer	7.6
Kali	11.2
Windows 7	9.6
Total Recommended	51.81

2.3 ESXi Host Server Requirements

Please refer to the NDG website for specific ESXi host requirements to support virtual machine delivery: http://www.netdevgroup.com/content/vmita/requirements/

The number of **active** pods that can be used simultaneously depends on the NETLAB+ product edition, appliance version and the number of VMware ESXi host servers meeting the hardware requirements specifications below.

For current ESXi server requirements and active pod count, refer to the following URL:

http://www.netdevgroup.com/support/remote_pc.html#vm_host_server_specifications.

2.4   NETLAB+ Requirements

Installation of Forensics pods, as described in this guide, requires that your NETLAB+ system is equipped with NETLAB+ version 2011.R5 or later.

Previous versions of NETLAB+ do not support the use of VMware ESXi 5.1 on the physical host servers, which is required to support the installation and use of Forensics Pods on NETLAB+.

> Please verify that your NETLAB+ system is running NETLAB+ version **2011.R5** or later, prior to upgrading your VMware ESXi servers to version 5.1.

2.5   Software Requirements

For the purpose of software licensing, each virtual machine is treated as an individual machine, PC or server. Please refer to the specific vendor license agreements (and educational discount programs, if applicable) to determine licensing requirements for your virtual machines' software, operating system and applications.

The following tables list the software that is required for virtual machines inside the Forensics pod.

Pod Software Requirements		
Software	**Version**	**Source**
Windows XP	Professional	Dreamspark
Windows 7	Professional	Dreamspark

2.6   Networking Requirements

To accommodate the movement of large VMs, OVF/OVAs and ISO disk images from one host to another, Gigabit Ethernet or better connectivity is recommended to interconnect your NETLAB+, vCenter Server system and ESXi host systems.

Two standard networking models recommended to interconnect your servers are described in detail in the *Networking Models* section of the *Remote PC Guide Series – Volume 1*.

3   Obtaining Software and Licenses

3.1   Downloading OVF Files

The virtual machines are made available as Open Virtualization Format (OVF) or Open Virtualization Archive (OVA) files. These files are available for download from CSSIA.

To request access to the preconfigured virtual machine templates from CSSIA:

1. Go to the CSSIA Resources page: http://www.cssia.org/cssia-resources.cfm.
2. Select **VM Image Sharing Agreement – Image Sharing Agreement**.
3. Select **VM Image Sharing Agreement** to open the request form.
4. Complete and submit your access request by following the instructions on the request form.
5. CSSIA will email a link, along with a username and password to access the download server. Access to the download server is provided only to customers who are current with their NETLAB+ support contract and are participants in the appropriate partner programs (i.e. Cisco Networking Academy, VMware IT Academy, and/or EMC Academic Alliance).
6. Once access to the download server has been established, the virtual machines can be deployed directly to the vCenter Server by clicking on File > Deploy OVF Template in the vClient window and copying the link into the location field.
7. The deployment will start after the username and password are entered.
8. Each virtual machine is deployed individually.

4   Master Pod Configuration

4.1   Deploying Virtual Machine OVF/OVA Files

Deploy on your host server the pod virtual machine OVF/OVA files you have downloaded.

1. Open the vClient on your administration machine where you downloaded the files from NDG. Connect to your vCenter Server.
2. Select **Hosts and Clusters** in the address bar.
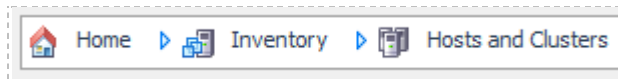
3. Click on the first ESXi Host Server.
4. Click on **File -> Deploy OVF Template.**
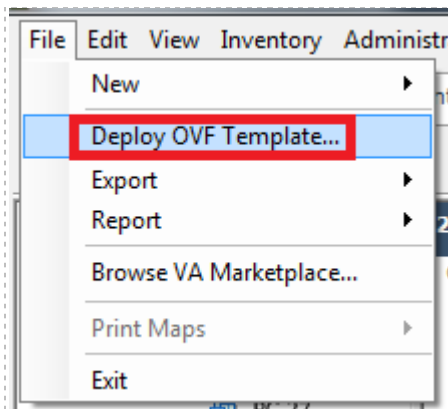
5. Click on **Browse** and locate the OVF/OVA file you downloaded. Click **Next** to continue.
6. On the OVF Template Details window, click **Next.**
7. On the Name and Location window, change the name of the virtual machine to something that is easy to manage. You can use the names provided in the list below as names for the virtual machines if you do not have a set naming convention. Click **Next**.

Virtual Machine Topology Name	Virtual Machine Deployment Name
Deft	Forensics_Master_Deft
Backtrack	Forensics_Master_Backtrack5
Windows XP Pro	Forensics_Master_WindowsXP
pfSense	Forensics_Master_pfSense
Linux Sniffer	Forensics_Master_LinuxSniffer
Kali	Forensics_Master_Kali
Windows 7	Forensics_Master_Windows7

8. On the Datastore window, select the appropriate datastore and click **Next**.
9. On the Disk Format window, select **Thin provisioned format** and click **Next.**
10. On the Network Mapping window, leave the default networks. Click **Next**.

> Network mapping is handled automatically by the NETLAB+ system during pod creation.

11. On the Ready to Complete window, confirm the information and click **Finish**.
12. vCenter will begin deploying the virtual machine. This may take some time depending on the speed of your connection, HDDs, etc.
13. When completed, click on **Close**.

4.2 Modify and Activate Virtual Machines

The following tasks must be performed prior to taking snapshots or assigning the virtual machines to pods.

4.2.1 Modify Network Interface Cards

Once the virtual machines are imported onto the host, change the Network Interface Cards (NIC's) MAC address via the VMware vSphere Client interface. The following steps will guide you through the process.

1. In the vSphere Web Client interface, right-click on the imported virtual machine and select **Edit Settings**.
2. Right-click on each virtual machine and change the MAC addresses from automatic to manual then set the corresponding MAC address to the address listed in the table below.

Virtual Machine	NIC	MAC
Deft	1	00:50:56:9c:86:22
Backtrack	1	00:50:56:1f:98:ae
Windows XP Pro	1	00:50:56:9c:8c:96
pfSense	1	00:50:56:9c:c0:c2
	2	00:50:56:9c:28:e5
Linux Sniffer	1	00:50:56:9c:7c:02
	2	00:50:56:9c:01:86
Kali	1	00:50:56:9c:2f:ce
Windows 7	1	00:50:56:9c:40:7b
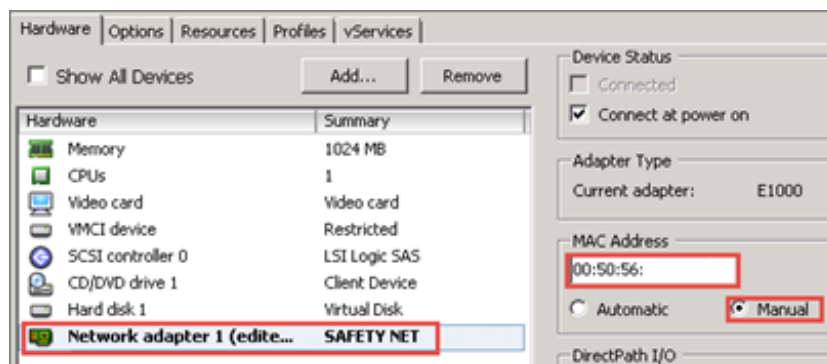
3. **Repeat Steps 1 – 2** for each of the virtual machines in the pod.

4.2.2   Modify BIOS Setup

Once the virtual machines are imported onto the host, you will need to verify or change the boot order of the Windows XP and Windows 7 virtual machines.

First, we must make the virtual machine boot into BIOS. Right-click on the virtual machine and select **Edit Settings**. Then check the Force BIOS Setup in the Boot Options section of the Virtual Machine Properties Options. Once finished, click **OK** to save the configurations.
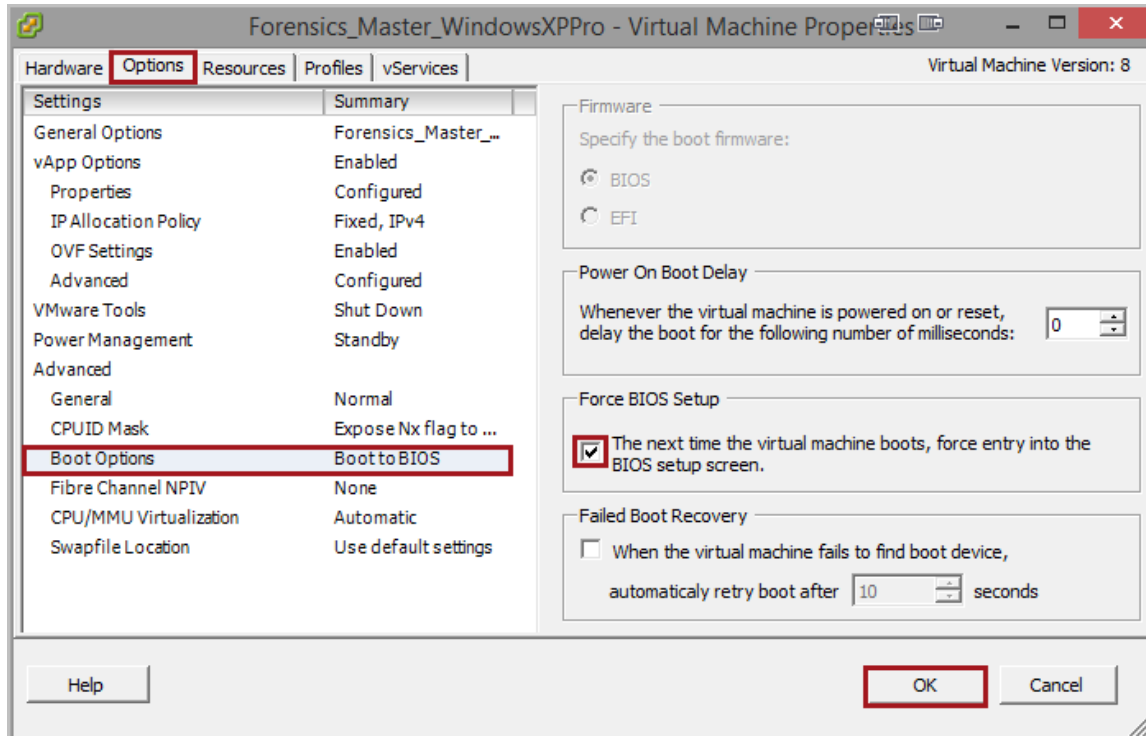
In the next section, you will need to use the keyboard to navigate the BIOS menu system.

4.2.2.1 Windows XP Boot Order

1. **Power On** the Windows XP virtual machine within the vSphere Client.
2. Select **Open Console**.

In the Windows XP BIOS, use the keyboard to navigate to the **Boot** tab. Verify that the boot order is similar to the order shown below. If not, you will need to select the hard drive using the arrow keys and change its position either up or down by using the <+> or <-> keys as noted in the help section on the right.

Once the order is correct, you can save the BIOS setting and exit BIOS by depressing the **F10** key.

```
                    PhoenixBIOS Setup Utility
    Main      Advanced     Security     Boot     Exit

                                              Item Specific Help
        +Removable Devices
        CD-ROM Drive
        -Hard Drive
             Bootable Add-in Cards           Keys used to view or
             VMware Virtual IDE Hard-(PM)    configure devices:
             VMware Virtual IDE Hard-(PS)    <Enter> expands or
        Network boot from AMD Am79C970A      collapses devices with
                                             a + or -
                                             <Ctrl+Enter> expands
                                             all
                                             <+> and <-> moves the
                                             device up or down.
                                             <n> May move removable
                                             device between Hard
                                             Disk or Removable Disk
                                             <d> Remove a device
                                             that is not installed.


    F1   Help    ↑↓  Select Item   -/+   Change Values      F9    Setup Defaults
    Esc  Exit    ↔   Select Menu   Enter  Select ▶ Sub-Menu  F10   Save and Exit
```
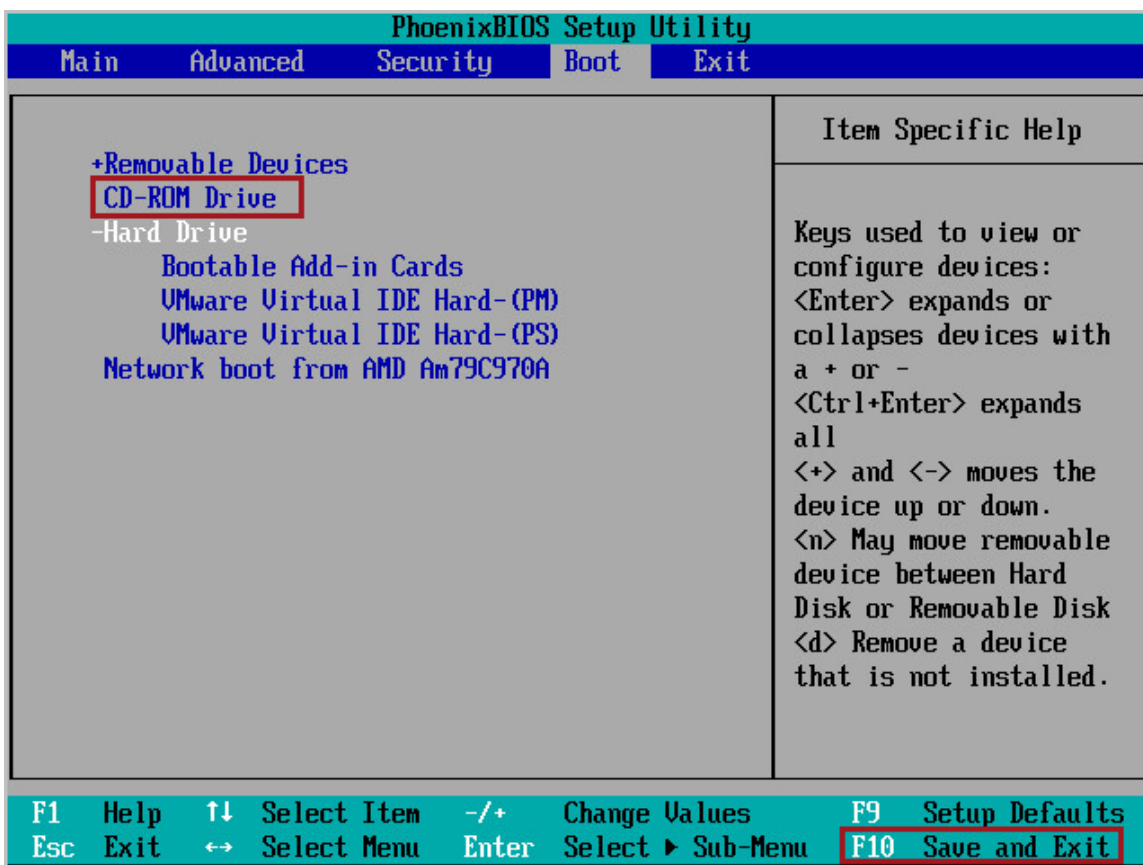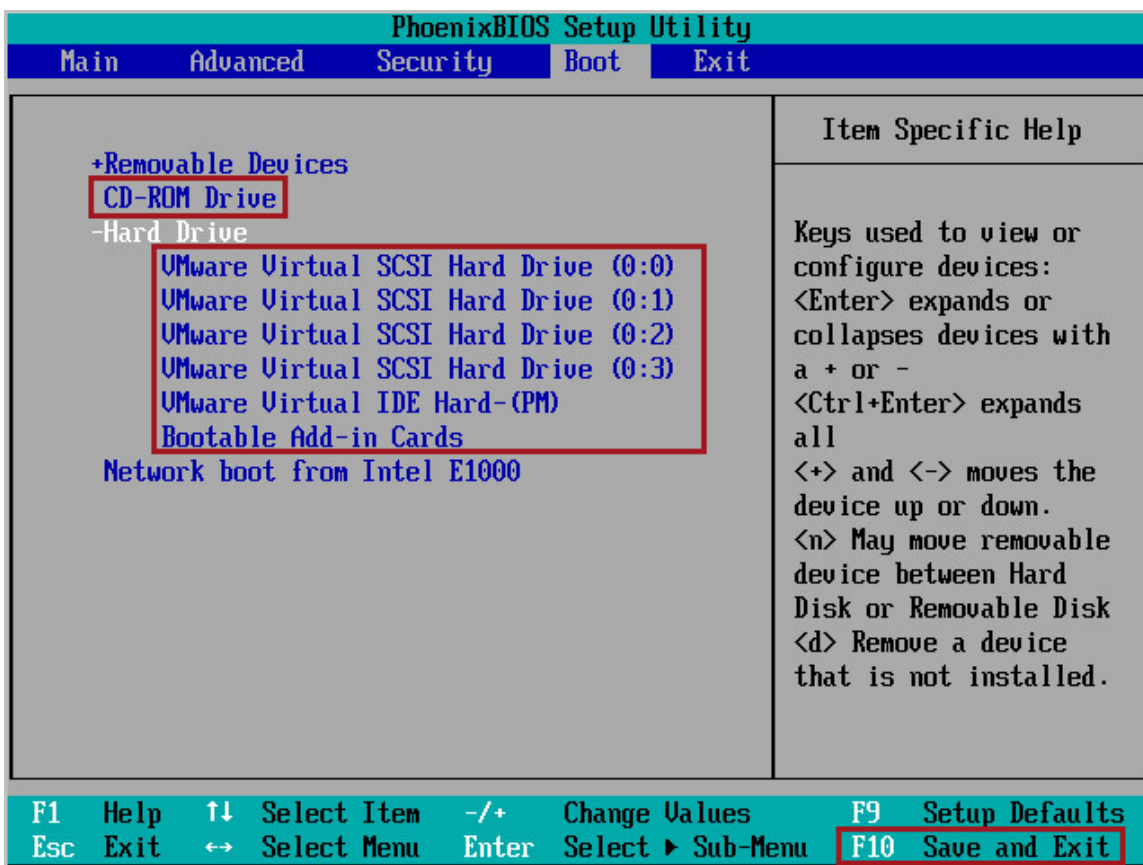
Once the settings are configured, gracefully shut down the VM and navigate your way back into Virtual Machine Properties Options (Section 4.2.2). Uncheck the checkbox under Force BIOS Setup and click **OK**.

4.2.2.2 Windows 7 Boot Order

1. **Power On** the Windows 7 virtual machine within the vSphere Client.
2. Select **Open Console**.

In the Windows 7 BIOS, use the keyboard to navigate to the **Boot** tab. Verify that the boot order is similar to the order shown below. If not, you will need to select the hard drive using the arrow keys and change its position either up or down by using the <+> or <-> keys as noted in the help section on the right.

Once the order is correct, you can save the BIOS setting and exit BIOS by pressing the **F10** key.

```
                    PhoenixBIOS Setup Utility
   Main      Advanced      Security      Boot      Exit

                                                  Item Specific Help
      +Removable Devices
       CD-ROM Drive
      -Hard Drive                            Keys used to view or
         VMware Virtual SCSI Hard Drive (0:0)   configure devices:
         VMware Virtual SCSI Hard Drive (0:1)   <Enter> expands or
         VMware Virtual SCSI Hard Drive (0:2)   collapses devices with
         VMware Virtual SCSI Hard Drive (0:3)   a + or -
         VMware Virtual IDE Hard-(PM)           <Ctrl+Enter> expands
         Bootable Add-in Cards                  all
       Network boot from Intel E1000           <+> and <-> moves the
                                               device up or down.
                                               <n> May move removable
                                               device between Hard
                                               Disk or Removable Disk
                                               <d> Remove a device
                                               that is not installed.


   F1    Help    ↑↓  Select Item   -/+    Change Values    F9   Setup Defaults
   Esc   Exit    ↔   Select Menu  Enter   Select ▶ Sub-Menu F10  Save and Exit
```

Once the settings are configured, gracefully shut down the VM and navigate your way back into Virtual Machine Properties Options (Section 4.2.2). Uncheck the checkbox under Force BIOS Setup and click **OK**.

4.2.3   Activate Virtual Machines

You will need to activate Microsoft Windows on the Windows-based virtual machines. This needs to be done prior to snapshot, pod assignment and cloning.

Virtual machine password list:

Machine	User name	Password
Deft	root	<No Password>
Backtrack	root	toor
Windows XP Pro	student	<No Password>
pfSense	admin	pfsense
Linux Sniffer	root	toor
Kali	root	password
Windows 7	Student	password

You will need to turn on each of the Windows machines. Accessing the machines via remote console, you can follow the steps offered in the Microsoft KB articles listed below:

- How to activate a Microsoft product by using Microsoft Product Activation Center: http://support.microsoft.com/kb/950929
- Windows 7: http://technet.microsoft.com/en-us/library/ee355153.aspx

4.3   Create Snapshots for the Master Virtual Machines

In order to proceed with pod cloning, snapshots must be created on each of the pods virtual machines.

Verify that all VMs are powered off before taking snapshots.

1. Open the vClient on your management workstation. Connect to your vCenter Server.
2. Select **Hosts and Clusters** in the address bar.
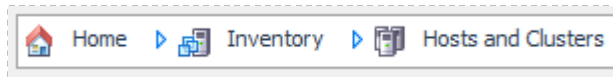
3. Right-click on each virtual machine and select **Snapshot -> Take Snapshot**.
4. Enter **GOLDEN_MASTER** as the Snapshot Name.
5. Enter a description. It is a good idea to include the date in the description for later reference.
6. Click **OK**.
7. Repeat Steps 3-6 for the remainder virtual machines in the pod.
8. When all tasks are complete, continue to the next section.

4.4   NETLAB+ Virtual Machine Infrastructure Setup

The NETLAB+ Virtual Machine Infrastructure setup is described in the following sections of the *Remote PC Guides for NETLAB+:*

- *Registering a Virtual Datacenter in NETLAB+*
- *Adding ESXi hosts in NETLAB+*
- *Proactive Resource Awareness*

 It is important to configure Proactive Resource Awareness to maximize the number of active pods per physical ESXi host.

4.5   NETLAB+ Virtual Machine Inventory Setup

This section will guide you in adding your templates to the Virtual Machine Inventory of your NETLAB+ system.
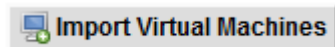
1. Login into your NETLAB+ system using the administrator account.
2. Select the **Virtual Machine Infrastructure** link.

Virtual Machine Infrastructure

3. Click the **Virtual Machine Inventory** link.

Virtual Machine Inventory
Import, clone, and manage the inventory of virtual machines to be used with NETLAB+.
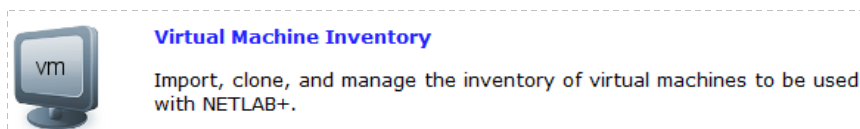
4. Click the **Import Virtual Machines** button.
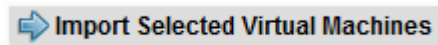
Import Virtual Machines

5. Select the check box next to the virtual machines you had just deployed and click **Import Selected Virtual Machines**.

Import Selected Virtual Machines
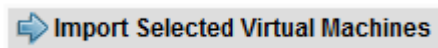
6. When the Configure Virtual Machines window loads, you can set your virtual machine parameters.
   a. Check the drop down box for the correct operating system for each imported virtual machine.
   b. Add any comments for each virtual machine in the box to the right.
   c. Verify your settings and click **Import Selected Virtual Machines**.

Import Selected Virtual Machines

   d. Click **OK** when the virtual machines have finished loading.
   e. Verify that your virtual machines show up in the inventory.

For additional information, please refer to the *NETLAB+ Remote PC Guide - Volume 3*.
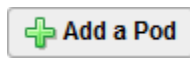
4.6   Create the Master Forensics Pod

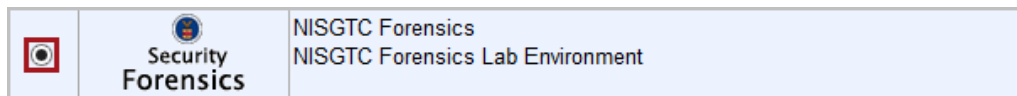This section will assist you in adding the Forensics Pod to your NETLAB+ system.

1. Login into NETLAB+ with the administrator account.
2. Select the **Equipment Pods** link.

3. Create a new pod by scrolling to the bottom and clicking the **Add a Pod** button.

4. On the New Pod Wizard page, click **Next**.
5. Then select the **Forensics** pod radio button and click **Next**.

6. Select a Pod ID and click **Next**.

> It is best practice to use a block of sequential ID numbers for the number of pods you are going to install. The Pod ID number determines the order in which the pods will appear in the scheduler.

7. Type in **Forensics_Master** for the Pod Name and click **Next**.
8. To finalize the wizard click **OK**.

For additional information, please refer to the *NETLAB+ Administrator Guide*.
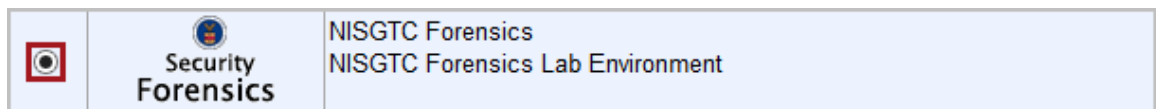
4.7   Update Master Pod

We need to update the master pod to associate the virtual machines that we deployed on the host with the pod we created.

1. Update the master pod on your NETLAB+ system.
    a. Login into NETLAB+ with the administrator account.
   b. Select the **Equipment Pods** link.


2. Select the Forensics master pod.

3. Click on the Magnifying Glass icon next to the first VM. Please note that your PC IDs will not match the graphic below.

| GO	NAME	PC ID	STATUS	TYPE / VM	OPERATING SYSTEM
🔍	DEFT	4100	ONLINE	ABSENT	
🔍	Backtrack5	4101	ONLINE	ABSENT	
🔍	WindowsXPPro	4102	ONLINE	ABSENT	
🔍	pfSense	4103	ONLINE	ABSENT	
🔍	Kali	4104	ONLINE	ABSENT	
🔍	Windows7	4105	ONLINE	ABSENT	
🔍	Linux Sniffer	4106	ONLINE	ABSENT	

4. Click on Modify PC Settings.
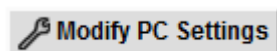
5. Change the PC Type drop-down box to **Use Virtual Machine Inventory**.
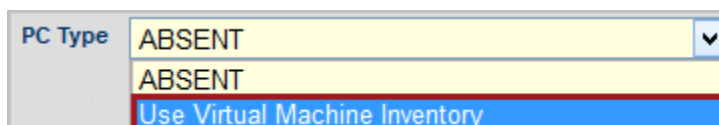
6. In the Base Virtual Machine window, select your virtual machine to associate with the spot held for it in the pod.
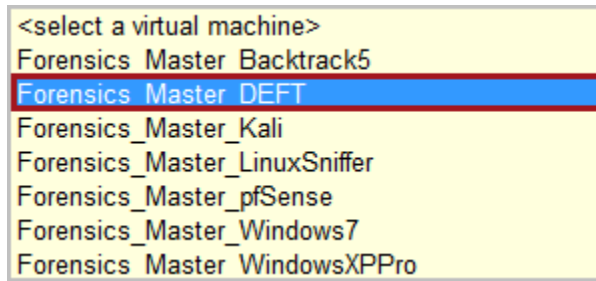
7. Update **Base Snapshot** to your *GOLDEN_MASTER* snapshot.
8. Review the information on the screen and click **Update PC Settings**.
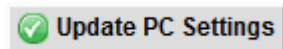
9. Click on **Show Pod**.
10. Repeat Steps 3-9 for the remaining virtual machines.

Make sure the pod status is **Offline** prior to continuing. The cloning process requires the pod be offline, and since this is our master pod used for cloning other pods with, we will keep it offline to create the instructor and student pods from.

5   Pod Cloning

This section will help you create multiple student pods. The following sections describe the NETLAB+ pod-cloning feature used to create student pods on one or two host systems.

5.1   Linked Clones and Full Clones

NETLAB+ can create *linked clones* or *full clones*.

A **linked clone** (or linked virtual machine) is a virtual machine that shares virtual disks with the parent (or master) virtual machine in an ongoing manner. This conserves disk space, and allows multiple virtual machines to use the same software installation. Linked clones can be created very quickly because most of the disk is shared with the parent VM.

A **full clone** is an independent copy of a virtual machine that shares nothing with the parent virtual machine after the cloning operation. Ongoing operation of a full clone is entirely separate from the parent virtual machine.

5.2   Creating User Pods on the First Host

The following section describes how to create user pods on the same VMware Host system that holds your master pod's virtual machines. In this scenario, we will create linked virtual machines using the NETLAB+ pod cloning utility.

1. Login into NETLAB+ with the administrator account.
2. Select the **Equipment Pods** link.

Equipment
Pods

3. Click on your master pod.
4. Click the **Clone** button to create a new pod based on the settings of this pod.
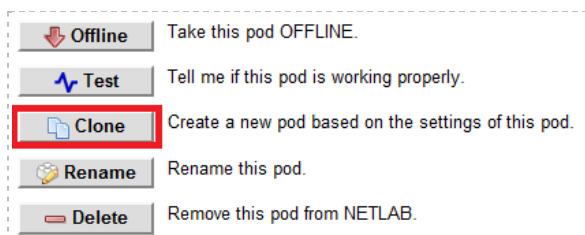
5. Select the New Pod ID. It is advised to keep the pods in numerical order. If the pod IDs are not in numerical order, they will not show up in the scheduler in numerical order.
6. Click **Next**.
7. Enter a New Pod Name. For example, **Forensics_Pod_01**. Click **Next**.
8. When the action has finished processing, a settings screen will be present.

PC Name	Source Virtual Machine	Source Snapshot	➡	Clone Name	Clone Type	Clone Role	Runtime Host or Group	Clone Datastore	Storage Allocation
DEFT	Forensics_Master_DEFT	GOLDEN_MASTER		Forensics_Pod_01 DEFT	Linked	Normal	Host 192.168.0.12	NFS	On Demand
Backtrack5	Forensics_Master_Backtrack5	GOLDEN_MASTER		Forensics_Pod_01 Backtrack5	Linked	Normal	Host 192.168.0.12	NFS	On Demand
WindowsXPPro	Forensics_Master_WindowsXPPro	GOLDEN_MASTER		Forensics_Pod_01 WindowsX	Linked	Normal	Host 192.168.0.12	NFS	On Demand
pfSense	Forensics_Master_pfSense	GOLDEN_MASTER		Forensics_Pod_01 pfSense	Linked	Normal	Host 192.168.0.12	NFS	On Demand
Kali	Forensics_Master_Kali	GOLDEN_MASTER		Forensics_Pod_01 Kali	Linked	Normal	Host 192.168.0.12	NFS	On Demand
Windows7	Forensics_Master_Windows7	GOLDEN_MASTER		Forensics_Pod_01 Windows7	Linked	Normal	Host 192.168.0.12	NFS	On Demand
Linux Sniffer	Forensics_Master_LinuxSniffer	GOLDEN_MASTER		Forensics_Pod_01 Linux Sniff	Linked	Normal	Host 192.168.0.12	NFS	On Demand

9. The three key columns for this master pod clone are Source Snapshot, Clone Type and Clone Role. The following settings should be applied to all 3 virtual machines:
    a. Source Snapshot should be set to the **GOLDEN_MASTER** snapshot you created previously.
    b. Under Clone Type, verify that **Linked** is selected.
    c. Under Clone Role, verify that **Normal** role is selected.
10. When you are done changing settings, Click **Clone Pod**. This should complete within a minute as we are creating linked virtual machines.
11. When the pod clone process is finished, click **OK**.
12. If you want to dedicate this pod to a particular class, team, or student, use the Pod Assignment feature. For details, see the *Pod Assignment Guide*.
13. Click the **Online** Button in the Pod Management page to activate the pod.

The user pod can now be reserved. When the reservation becomes active, NETLAB+ will automatically configure virtual machines and virtual networking for your new pod.

The GOLDEN_MASTER snapshot is the starting point for all pods. We recommend that you reserve the 1st pod and conduct some labs to make sure the snapshot images work correctly. If there are defects, make corrections to the images to the master pod and retake the GOLDEN_MASTER snapshot before creating additional pods.

Time Saver: If you clone the 1st user pod instead of the master pod, the defaults will all be set correctly, and you will not have to change the Clone Type or Clone Role each time. NETLAB+ will still assume you want to link to the master VMs as masters are ranked higher than normal or persistent VMs in the default pod cloning selections.
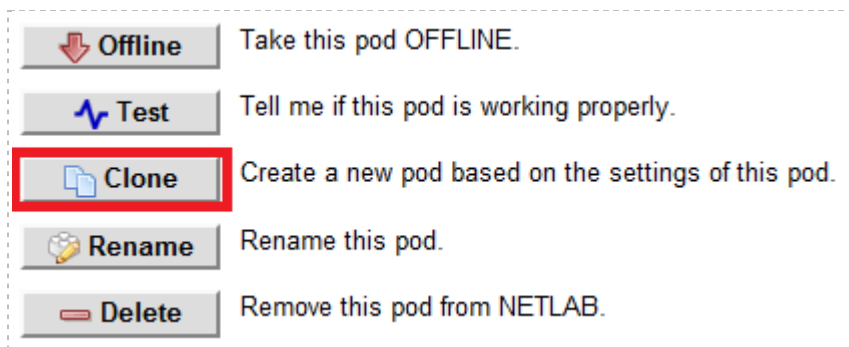
5.3   Copying Your Master Pod to the Second Host

For this task, we will use the pod cloning utility to copy our master pod to the 2nd host.

1. Login into NETLAB+ with the administrator account.
2. Select the **Equipment Pods** link.

3. Click on the master pod that was created on the 1st VMware host server.
4. Click the **Clone** button to create a new pod based on the settings of this pod.

5. Select the New Pod ID.

> It is advised to keep the pods in numerical order. If the pod IDs are not in numerical order, they will not show up in the scheduler in numerical order.

6. Click **Next**.
7. Enter a New Pod Name. For example, **CourseName_Master_Pod_2** then Click **Next**.
8. When the action has finished processing, a settings screen will be present.

PC Name	Source Virtual Machine	Source Snapshot	➡	Clone Name	Clone Type	Clone Role	Runtime Host or Group	Clone Datastore	Storage Allocation
DEFT	Forensics_Master_DEFT	GOLDEN_MASTER		Forensics_Pod_01 DEFT	Linked	Normal	2nd Host	NFS	On Demand
Backtrack5	Forensics_Master_Backtrack5	GOLDEN_MASTER		Forensics_Pod_01 Backtrack5	Linked	Normal	2nd Host	NFS	On Demand
WindowsXPPro	Forensics_Master_WindowsXPPro	GOLDEN_MASTER		Forensics_Pod_01 WindowsX	Linked	Normal	2nd Host	NFS	On Demand
pfSense	Forensics_Master_pfSense	GOLDEN_MASTER		Forensics_Pod_01 pfSense	Linked	Normal	2nd Host	NFS	On Demand
Kali	Forensics_Master_Kali	GOLDEN_MASTER		Forensics_Pod_01 Kali	Linked	Normal	2nd Host	NFS	On Demand
Windows7	Forensics_Master_Windows7	GOLDEN_MASTER		Forensics_Pod_01 Windows7	Linked	Normal	2nd Host	NFS	On Demand
Linux Sniffer	Forensics_Master_LinuxSniffer	GOLDEN_MASTER		Forensics_Pod_01 Linux Sniff	Linked	Normal	2nd Host	NFS	On Demand

9. The four key columns for this master pod clone are Source Snapshot, Clone Type and Clone Role, and Runtime Host.
   a. Source Snapshot should be set to the **GOLDEN_MASTER** snapshot you created previously.
   b. Under Clone Type, click the dropdown menu and verify that **Full** is selected.
   c. Under Clone Role, click the dropdown menu and select **Master**.
   d. Under Runtime Host, select the 2nd host system (which should be different than the system you are cloning from).
10. When you are done changing settings, Click **Clone Pod**. This may take up to 30 minutes as full copies are being made. You may navigate away from the cloning progress screen, and then later return to the pod to check progress.

> The NETLAB+ software does not automatically create the snapshots on the virtual machines. It is necessary to create the snapshots manually as you did in a previous section.

11. When the cloning process is complete, you should create a GOLDEN_SNAPSHOT on each virtual machine in the 2nd master pod.

5.4 Creating User Pods on the Second Host

To create user pods on the second host, repeat the steps to create User pods on the first host (Section 5.2), substituting the 2nd master pod (created in the previous section) as the cloning source.

6   Assigning Pods to Students, Teams , or Classes

Please refer to the *Pod Assignment Guide* for details on using the Pod Assignment feature.