Cisco CCNA Cyber Ops

Pod Installation and Configuration Guide

Document Version: 2018-06-05

⚠️ Installation of *Cisco CCNA Cyber Ops* virtual pods as described in this guide requires that your *NETLAB+ VE* system is equipped with software version **17.3.11 or later**.

Contents

1   Introduction

This document provides detailed guidance on performing the installation and configuration of the Cisco CCNA Cyber Ops pod on the NETLAB+ VE system.

1.1   Introducing the Cisco CCNA Cyber Ops Pod

The *Cisco CCNA Cyber Ops* pod is a 100% virtual machine pod consisting of five virtual machines. Linked together through virtual networking, these five virtual machines provide the environment for a student or a team to perform the *Cisco CCNA Cyber Ops* labs.
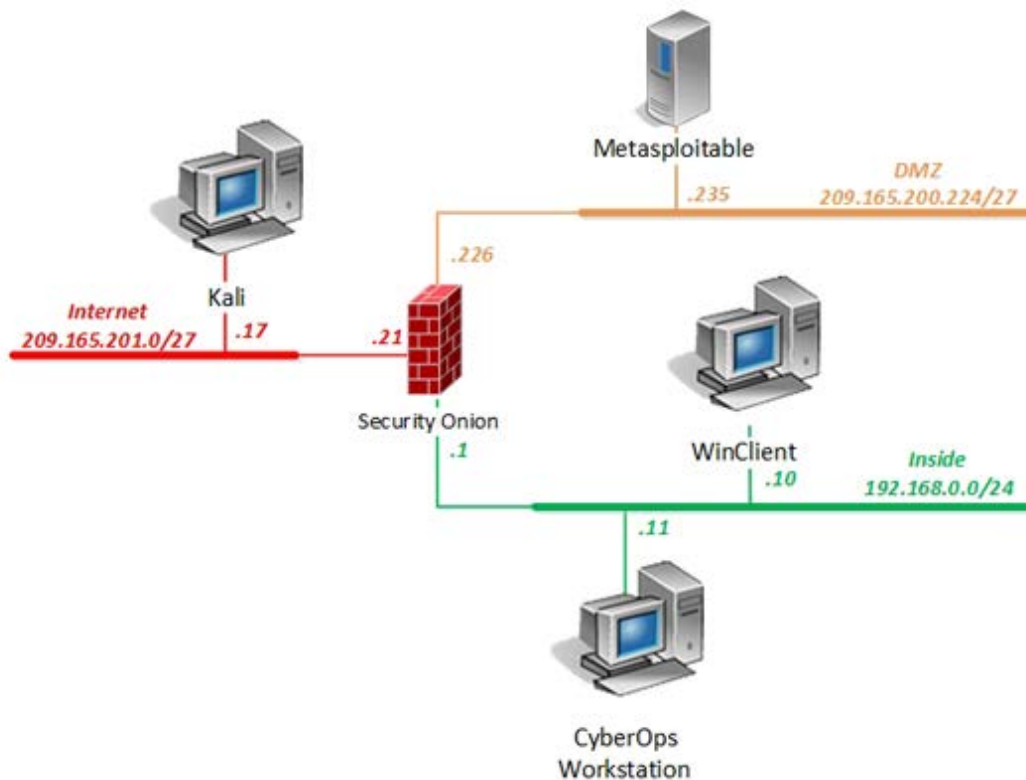
2   Planning

This guide provides specific information pertinent to delivering the *Cisco CCNA Cyber Ops Administration* pod. 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 Resource Requirements

The *Cisco CCNA Cyber Ops* course will consume 37.1 GB of storage per each master pod instance.

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

Virtual Machine	OVF/OVA	Initial Master Pod (Thin Provisioning)
CyberOps Workstation	2.4 GB	5.7 GB
Kali	3.6 GB	8.3 GB
Metasploitable	900 MB	1.8 GB
Security Onion	3.2 GB	9.7 GB
WinClient	6 GB	11.6 GB
Total	**16.2**	**37.1**

2.2   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/

> **Please Note**
>
> The number of **active** pods that can be used simultaneously depends on the *NETLAB+* product license and the number of *VMware ESXi* host servers meeting the hardware requirements specifications.

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.

2.3   NETLAB+ Requirements

Installation of *Cisco CCNA Cyber Ops* pods, as described in this guide, requires that your *NETLAB+* system is equipped with *NETLAB+ VE* version **17.3.11 or later**.

Previous versions of *NETLAB+* do not support requirements for the *Cisco CCNA Cyber Ops* course on the physical host servers.

Please refer to the *NETLAB+ Remote PC Guide Series*.

2.4   NETLAB+ Virtual Machine Infrastructure Setup

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

- *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.

2.4.1   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 minimum virtual infrastructure software required for standing up this pod is in the following table.

Virtual Infrastructure Requirements	
Software	Version
vSphere ESXi	6.0
vCenter Server	6.0

Please refer to the *Software and Licenses* section regarding the software requirements for virtual machines in pod.

2.5   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.

The 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 - Introduction and Planning*.

3   Software and Licenses

3.1   Obtaining Windows Software Licenses

The following table lists the software that is required for the virtual machines inside the *Cisco CCNA Cyber Ops* pod. Your organization needs to be a member of the vendor programs listed in the *Source* column to obtain and use the licenses.

Pod Software Requirements		
Software	**Version**	**Source**
Windows Server	2016 Standard (64-bit)	Microsoft Imagine or Visual Studio

To enable all features of the *Windows*-based virtual machines, licensing will be required, followed through with activations for the master virtual machines only. This needs to be done before cloning.

There are two options for institutions to access *Microsoft* licenses. The first option is through the *Visual Studio Subscription Portal*. The second option is by accessing your institution's *Kivuto WebStore* via *Microsoft Imagine*.

> For more information about *Visual Studio Subscriptions*, you may visit their FAQ page: https://www.visualstudio.com/my/myvsfaq.
>
> For more information regarding the *Microsoft Imagine* program, you may visit their FAQ page: https://imagine.microsoft.com/en-us/institutions/faq.
>
> It is recommended to acquire the *Multiple Activation Key* (*MAK*) lab key license for a specified *Windows* product. This type of key enables you to activate multiple installations of a product with the same key.

Please note that activating licenses is only required on master pods. Doing a *Link Clone* of the master pod will preserve the activation on the cloned VMs in the user pods. It is important to note that when activating *Windows*, that the VMs have temporary Internet access so that they can contact *Microsoft Licensing Servers*. There are multiple ways of providing temporary Internet access for VMs in a *vSphere* environment. The most common way is to temporarily assign the *vNIC* of the desired VM to connect to the virtual switch that is connected to an outside facing physical *NIC*.

3.2   Obtaining Cisco Networking Academy Access

To obtain access to the *Cisco CCNA Cyber Ops* labs, your institution must be a Cisco Networking Academy member.

You can find information about the Cisco Networking Academy at the following link: https://www.netacad.com/get-started/educators/.

3.3   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, Red Hat Academy, Palo Alto 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 client 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. Navigate to your **vSphere Web Client** using your management workstation, ensure that your downloaded *OVA/OVF* files are accessible on this machine and then connect to your **vCenter Server**.
2. From the *vSphere Web Client* dashboard, select **Hosts and Clusters**.
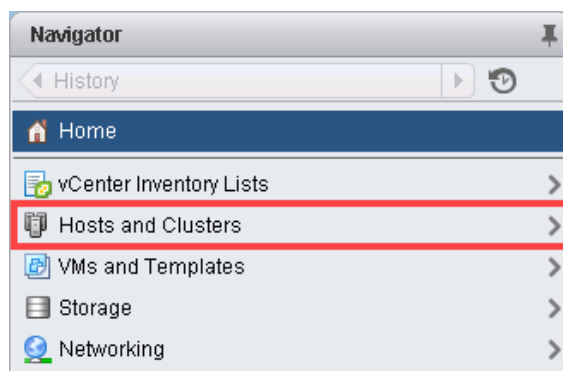
3. Right-click on the target **ESXi Host Server** and select **Deploy OVF Template**.
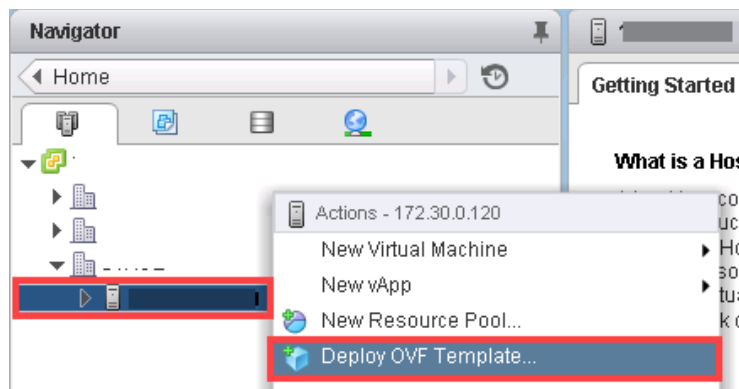
4. In the *Deploy OVF Template* window, on the *Select source* section, select the **Local File** radio button and click **Browse**.
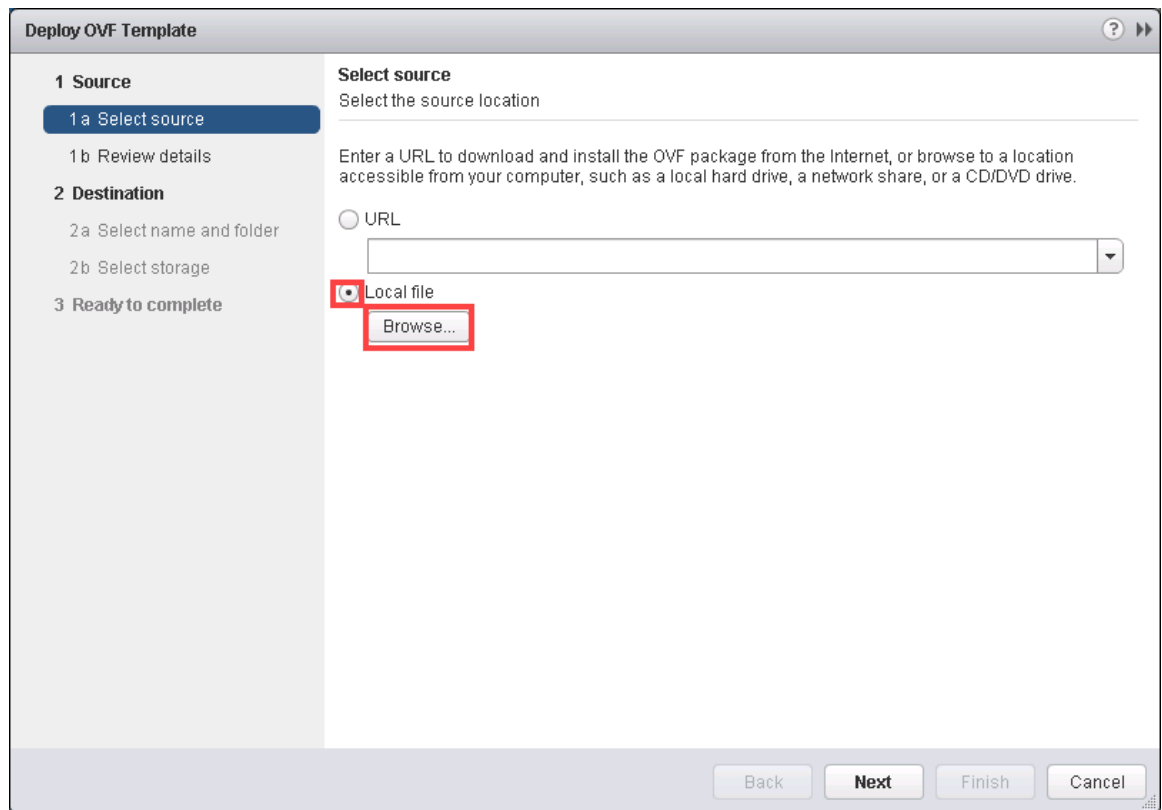
5. Locate and select one of the VMs for the pod, click **Open**.

> **Please Note** Only one VM can be selected using this wizard. The process will have to be repeated for the remaining VMs.

6. Verify that the VM file path and name appears next to the *Browse* button and click **Next**.

7. In the *Review details* section, make sure to fill the checkbox for **Accept extra configuration options** (*if present*) and click **Next**.

8. In the *Select name and folder* section, 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. Select the appropriate **datacenter** and click **Next**.

VM Name	VM OS	Virtual Machine Deployment Name
CyberOps Workstation	Linux	Cisco_CCNA_CyberOps.Workstation
Kali	Linux	Cisco_CCNA_CyberOps.Kali
Metasploitable	Linux	Cisco_CCNA_CyberOps.Metasploitable
Security Onion	Linux	Cisco_CCNA_CyberOps.Security_Onion
WinClient	Windows Server 2016 Standard	Cisco_CCNA_CyberOps.WinClient
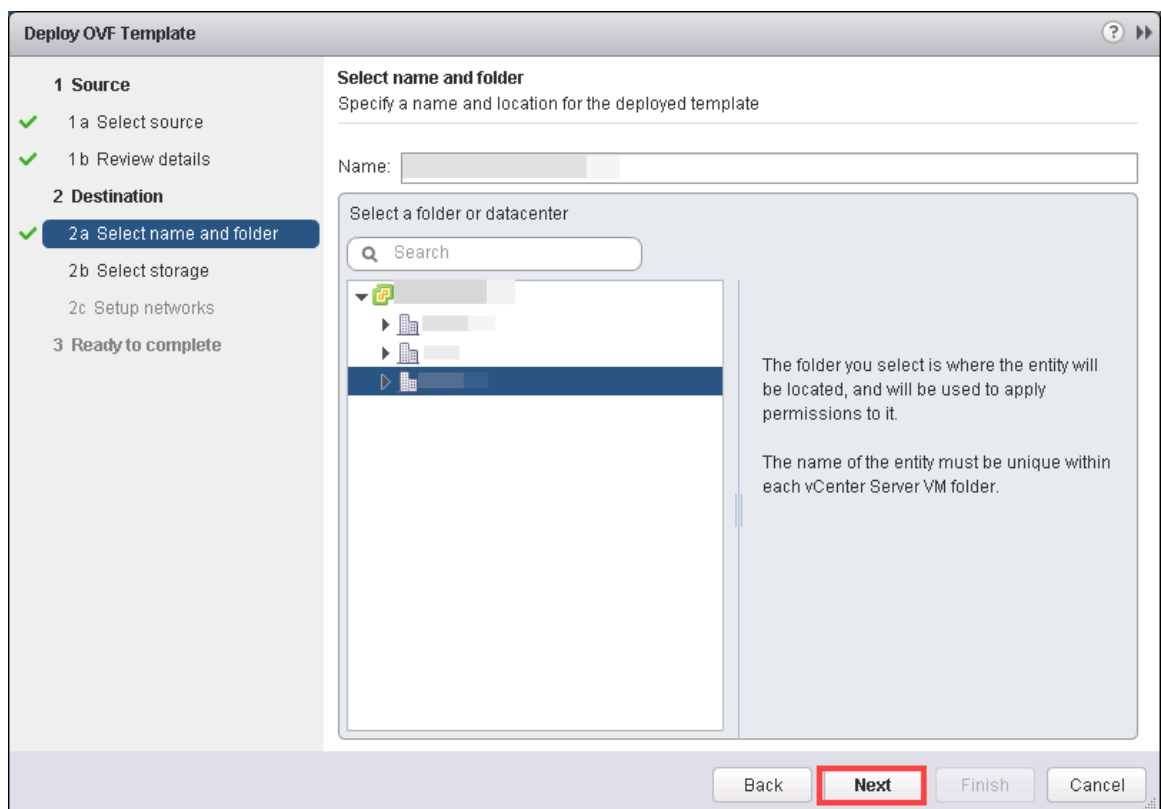
9. In the *Select Storage* section, choose the appropriate storage device and make sure that **Thin Provision** is selected. Click **Next**.
10. In the *Setup networks* section, select **SAFETY NET** as the destination and click **Next.**

> 🛑 If *SAFETY NET* is not available, refer to the *Create a Safe Staging Network* section in the *Remote PC Guide Series – Volume 2*.

11. In the *Ready to complete* section, make sure **Power on after deployment** is **unchecked** and confirm the settings. Click **Finish**.
12. *vCenter* will begin deploying the virtual machine. This may take some time depending on the speed of your connection, HDDs, etc. Repeat the previous steps for each remaining virtual machine in the master pod.

4.1.1   Modify Virtual Machines

Once the virtual machines are imported onto the host, verify the configurations. 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. For all the virtual machines manually assign the *MAC* addresses for each *NIC*. The table below identifies the *MAC* addresses per *NIC*.

Virtual Machine	NIC	MAC
CyberOps Workstation	1	08:00:27:23:B2:31
Kali	1	08:00:27:CA:70:C6
Metasploitable	1	08:00:27:AB:84:07
	2	08:00:27:DE:6E:B0
Security Onion	1	08:00:27:8c:29:85
	2	08:00:27:2b:22:6e
	3	08:00:27:a8:ab:b6
	4	08:00:27:44:6c:a0
WinClient	1	00:50:56:82:da:48
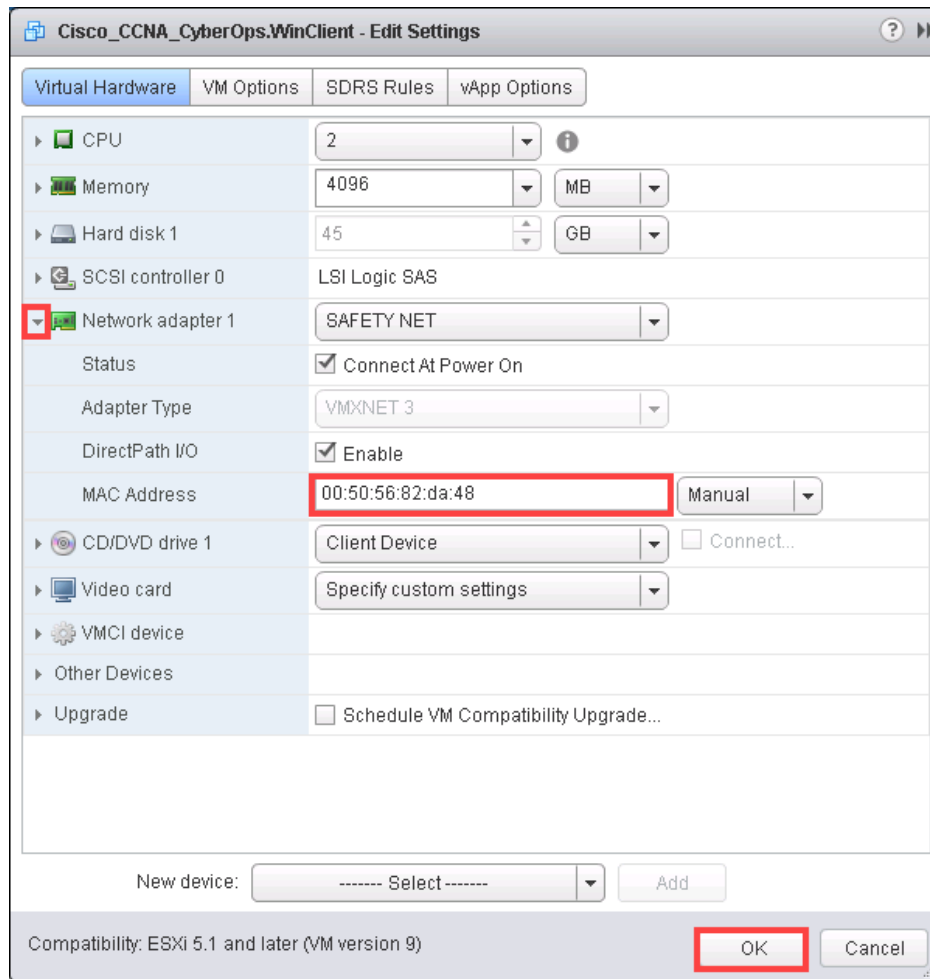
3. Repeat the previous steps for each of the remaining virtual machines in the master pod.

4.2   NETLAB+ Virtual Machine Inventory Setup

This section will guide you in adding your templates to the *Virtual Machine Inventory* of your *NETLAB+ VE* system.

1. Login into your *NETLAB+ VE* system using the administrator account.
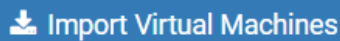2. Select the **Virtual Machine Infrastructure** icon.
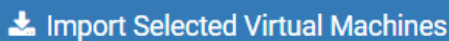
3. Click the **Virtual Machine Inventory** icon.

Virtual Machine Inventory

Import, clone, and manage the inventory of virtual machines to be used with NETLAB+.

4. Click the **Import Virtual Machines** button located at the bottom of the list.

Import Virtual Machines

5. Select the appropriate datacenter from the list where your master VMs reside.
6. Select the check box next to the virtual machines you had just deployed and click **Import Selected Virtual Machines**.

Import Selected Virtual Machines

7. When the *Configure VMs* 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. Change *Role* to **Master** for each VM.
   c. Add any comments for each virtual machine in the last column.

   > It is advised to leave the *Version* and *Build* numbers for reference when requesting *NDG* support.

   d. Verify your settings and click **Import (X) Virtual Machines** (notice the number in parenthesis is dynamic, depending on the amount of VMs selected).

   Import (5) Virtual Machines

   e. Verify all *Import Statuses* report back with **OK** and then click on the **Dismiss** button.
   f. Verify that your virtual machines show up in the inventory.

For additional information, please refer to the *NETLAB+ VE Administrator Guide*.

4.3   Building the Master Cisco CCNA Cyber Ops Pod

This section will assist you in adding the *Cisco CCNA Cyber Ops* pod to your *NETLAB+* system.

4.3.1   Enabling Cisco CCNA Cyber Ops in Course Manager

Please refer to the *Course Manager* section *of the NETLAB+ VE Administrator Guide* on how to enable content. Please install the *Cisco CCNA Cyber Ops* course.

4.3.2   Create the Master Pod

1. Log into **NETLAB+ VE** with the *administrator* account.
2. Select the **Pods** icon.

3. Create a new pod by scrolling to the bottom and clicking the **Create New Pod** button.
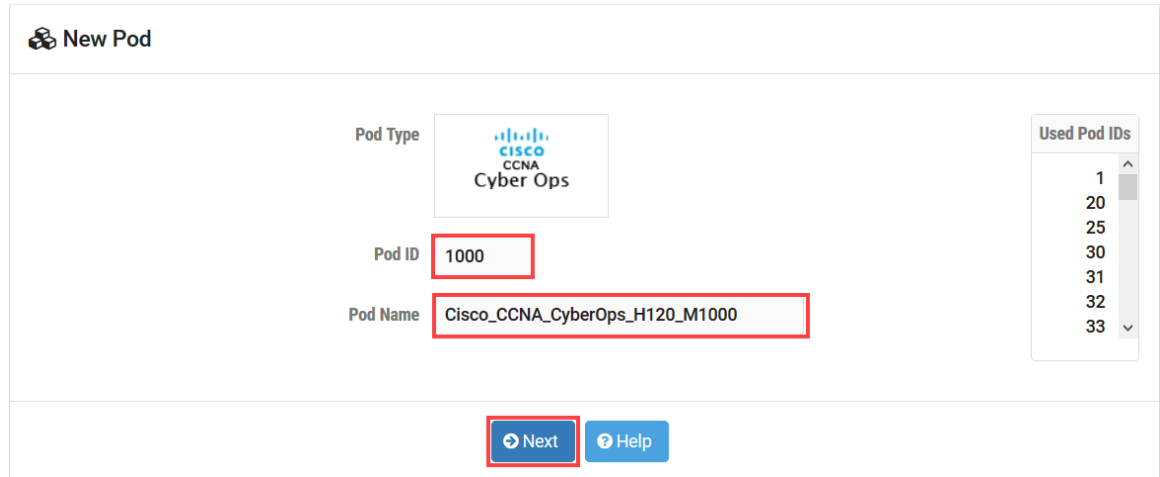
4. Then click on the **Cisco CCNA Cyber Ops** pod entry from the list of installed pod types.

	Cisco CCNA Cyber Ops The CCNA Cyber Ops training prepares candidates to begin a career working with associate-level cybersecurity analysts within security operations centers. 2018 Copyright (C) Network Development Group, Inc. https://www.netdevgroup.com/support/tech_support.html	NDGTK NDG

5. On the *New Pod* window, input a value into the **Pod ID** and **Pod Name** fields. Click **Next**.

> The *Pod ID* determines the order in which the pods will appear in the scheduler. It is best practice to use a block of sequential ID numbers for the *Pod Id* that allows for the number of pods you are going to install.
>
> The *Pod Name* identifies the pod and is unique per pod. Here we used the name of the lab set or course in a shortened form along with a host identifier (H120), the type and number of the pod (M1000).

6. To finalize the wizard, click **OK**.

For additional information, please refer to the [NETLAB+ VE Administrator Guide](#).

4.3.3   Assign Virtual Machines to the Master Pod

Update the master pod to associate the virtual machines with the newly created pod.

1. To assign virtual machines to the master pod on your *NETLAB+* system, select the **Pods** icon.

2. Select the **Cisco CCNA Cyber Ops** master pod from the pod list.

1000	Cisco CCNA Cyber Ops	Cisco_CCNA_CyberOps_H120_M1000	Persistent	IDLE	⭕ OFFLINE	▼	☐

3. Click on the **Action** dropdown next to the virtual machine you are about to assign and select **Attach VM**.

Remote PC ⑤					
	PC Name	**VM**	**Operating System**	**VM Role**	**Runtime Host**	**Action**
🖥	CyberOps Workstation	ABSENT				▼
🖥	Kali	ABSENT				👁 View
🖥	Metasploitable	ABSENT				⚙ Settings
🖥	Security Onion	ABSENT				⊕ Attach VM
🖥	WinClient	ABSENT				⊖ Remove VM From...
						📷 Snapshots

4. Select the corresponding virtual machine from the inventory list.

🖳 Cisco_CCNA_CyberOps.Kali	Linux	Master	QA	
🖳 Cisco_CCNA_CyberOps.Metasploitable	Linux	Master	QA	
🖳 Cisco_CCNA_CyberOps.Security_Onion	Linux	Master	QA	
🖳 Cisco_CCNA_CyberOps.WinClient	Windows 10	Master	QA	
🖳 Cisco_CCNA_CyberOps.Workstation	Linux	Master	QA	

5. Repeat the previous steps for the remaining virtual machines.

4.3.4   Snapshot the Virtual Machine

1. In the pod list, click on the **Cisco CCNA Cyber Ops** master pod you just assigned machines to.

1000	Cisco CCNA Cyber Ops	Cisco_CCNA_CyberOps_H120_M1000	Persistent	IDLE	⭕ OFFLINE	▼	☐

2. In the pod view, click on a virtual machine in the list to view the properties of that machine in *NETLAB+*. You will need to do this for each of the virtual machines in the list.

| Remote PC 5					
PC Name	**VM**	**Operating System**	**VM Role**	**Runtime Host**	**Action**
CyberOps Workstation	Cisco_CCNA_CyberOps.Workstation	Linux	MASTER	172.30.10.43	▾
Kali	Cisco_CCNA_CyberOps.Kali	Linux	MASTER	172.30.10.43	▾
Metasploitable	Cisco_CCNA_CyberOps.Metasploitable	Linux	MASTER	172.30.10.43	▾
Security Onion	Cisco_CCNA_CyberOps.Security_Onion	Linux	MASTER	172.30.10.43	▾
WinClient	Cisco_CCNA_CyberOps.WinClient	Windows 10	MASTER	172.30.10.43	▾

3. In the pod virtual machine view, click on the **Snapshots** button to open the *Snapshot Manager*.

⟳ Dismiss   ⚙ Settings   🖥 Manage VM   🔧 Change VM   📷 Snapshots
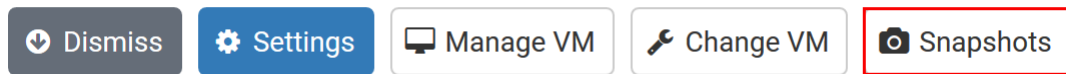
4. In the *Snapshot Manager* window, click on the **Take** button. This will take a snapshot of the current state of the virtual machine.

⚠ Any changes made after this will require a new snapshot or those changes will not reflect in the reset state of the pod or its clones.

Snapshot Manager

PAN8_210_Master_Client
  ⦿ You Are Here!

Name:

Description:

🖫 Take   📋 Delete All   ⦿ Go To   📝 Edit   🗑 Delete

⟳ Dismiss

5. In the *Take Snapshot* window, type `GOLDEN_MASTER` in the *Name* field then click the **OK** button.

Take Snapshot

Name:

GOLDEN_MASTER

Description:

OK   Cancel

⚠️ It is recommended to use *GOLDEN_MASTER* as the snapshot name when working with normalized pod types.

6. In the *Snapshot Manager* window, notice the snapshot is created. Click the **Dismiss** button.

Snapshot Manager

Cisco_CCNA_CyberOps.Workstation
 GOLDEN_MASTER
  🔴 You Are Here!

Name:
 GOLDEN_MASTER

Description:

📷 Take   📷 Delete All   🔴 Go To   📝 Edit   📷 Delete

⬇ Dismiss

⚠️ At this point it is good to verify that you have only one snapshot on the virtual machine. Multiple snapshots increase the likelihood of having problems, especially if the snapshots are named the same.

6. Click the **Dismiss** button to return to the pod view page and repeat the previous steps for the remaining virtual machines.

4.3.5 Set the Revert to Snapshot

1. In the pod view, click on a virtual machine in the list to view the properties of that machine in *NETLAB+*. You will need to do this for each of the virtual machines in the list.

2. In the pod virtual machine view, click on the **Settings** button.
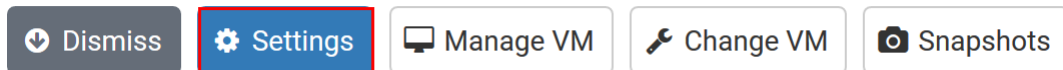
3. In the virtual machine's *Settings* window, click on the *Revert to Snapshot* drop box and select **GOLDEN_MASTER** then click the **Submit** button.

> This sets the snapshot on the virtual machine that will get reverted to each time the pod is scheduled.

4. Click **OK** to confirm.
5. Click the **Dismiss** button to return to the pod view page and repeat the previous steps for the remaining virtual machines.

4.3.6 Bring the Master Pod online

In the pod view, click the drop arrow under *State* and select **Online**.
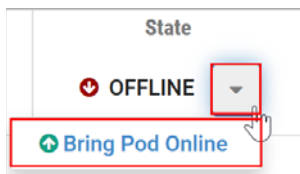
4.4 Create Class and Schedule the Master Pod

Create a class as identified in *Add Classes* section of the [NETLAB+ VE Instructor Guide](#) then schedule the *Master Pod* to license the *WinClient* machine.

> ⚠️ When scheduling the *Master Pod*, it is important to schedule the pod for enough time to complete the following steps. Failure to complete the steps prior to taking the final snapshot could mean redeploying necessary virtual machines.

4.5 Make changes to the Master Pod

Some pods have software that needs to be altered on the host machine before it can be used properly. This normally happens when software requires licenses to function.

If there are changes that need to be made to the master pod prior to link cloning either student pods or full cloning other master pods on other hosts, you will need to follow this set of instructions to ready your master pod.

For the Cisco CCNA Cyber Ops master pod you will need to license the WinClient machine. This process consists of:
- Scheduling the master pod
- Providing temporary internet access to the *WinClient* machine
- Licensing/Activating the *WinClient*
- Shutting down the *WinClient* only
- If necessary, resetting the network interface cards to *SAFETY NET*
- Taking a new *GOLDEN_MASTER* snapshot for *WinClient*
- Ending the reservation

4.5.1 Virtual Machine Credentials

For your reference, the following table provides a list of the credentials for the systems in the pod:

Machine	User name	Password
CyberOps Workstation	analyst	cyberops
Kali	root	cyberops
Metasploitable	msfadmin	msfadmin
Security Onion	analyst	cyberops
WinClient	administrator	cyberops

4.5.2 Provide Temporary Internet Access to the WinClient

1. Outside the *NETLAB+* interface, navigate to your **vSphere Web Client** using your management workstation, and then connect to your **vCenter Server**.
2. From the *vSphere Web Client* dashboard, select **Hosts and Clusters**.
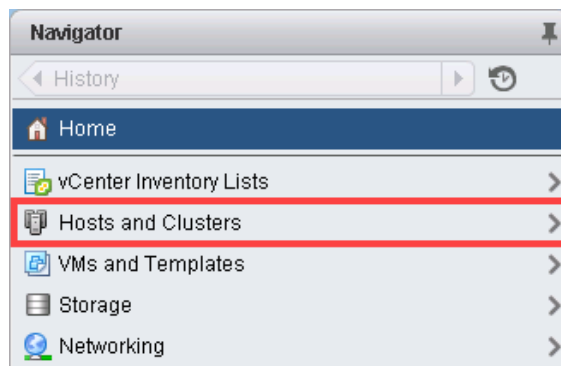
3. Select your host under the **NETLAB** datacenter.
4. Locate the *WinClient* virtual machine. Right-click on the virtual machine and select **Edit settings**.
5. Change *Network adapter 1* to a virtual machine port group that is linked to an internet accessible physical adapter.
6. Click **OK** to confirm settings.

4.5.3 License and Activate the WinClient

1. Log on to the **WinClient** machine in the pod. If necessary, click the drop-down arrow and select **Send CTRL+ALT+DEL**.
2. Log in as `Administrator` with `cyberops` as the password.
3. Once logged in, make sure the *IP/TCP* settings are temporarily configured correctly so that the Internet is reachable. This can vary depending on how your environment is set up.
4. Right-click on the **Start** menu and select **System**.

5. In the *Windows activation* pane, click the **Activate Windows** link.
6. Click **Change product key**.
7. Enter the product key and then click **Next**.
8. Windows should now be activated. If your received an error, make sure that the key entered is valid and click the **Troubleshoot** link from the *Activation Settings*.

4.5.4   Shut down WinClient

1. Click the **Start** menu followed by clicking the **Power** icon.
2. Click **Shut down**.
3. When prompted, choose **Other (Planned)** and click **Continue**.

4.5.5   Reset the NIC to SAFETY NET

1. Outside the *NETLAB+* interface, navigate to your **vSphere Web Client** using your management workstation, and then connect to your **vCenter Server**.
2. From the *vSphere Web Client* dashboard, select **Hosts and Clusters**.
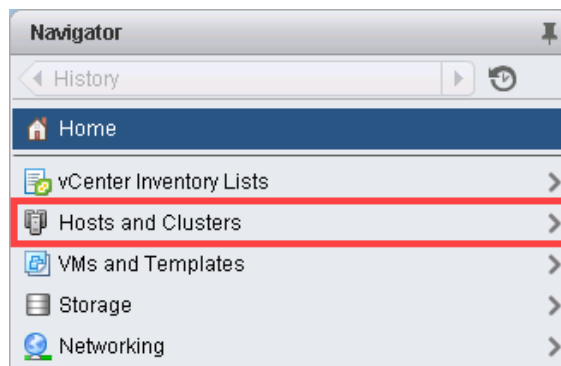
3. Select your host under the **NETLAB** datacenter.
4. Locate the *WinClient* machine. Right-click on the virtual machine and select **Edit settings**.
5. Change *Network adapter 1* to **SAFETY NET**.
6. Click **OK** to confirm settings.

4.5.6 Create Snapshot on the Changed Master Virtual Machines

1. Right-click on the **WinClient** virtual machine and select **Snapshots-> Manage Snapshots...**

2. Click **Delete** to delete the current snapshot. Remember the name of this snapshot as the new snapshot will need to have the exact same name.
3. Click **Yes** on the *Confirm Delete* window.
4. Click **Close** on the *Manage Snapshots* window.
5. Right-click on the Client virtual machine and select **Snapshots-> Take Snapshot...**
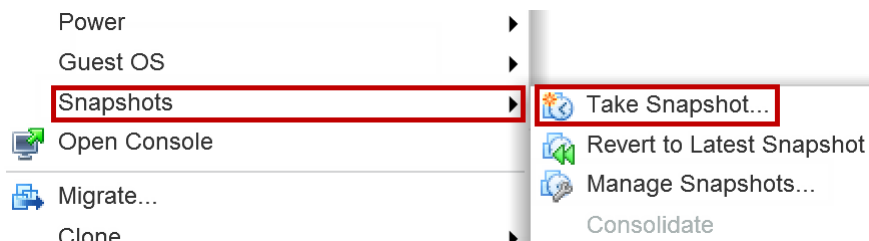
6. In the *Take Snapshot* window, type `GOLDEN_MASTER` or whatever prior snapshot name the virtual machine had from step 2. Click **OK** to take snapshot.

4.5.7 End Reservation

You may now end the reservation of the master pod.

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

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+ VE** with the *administrator* account.
2. Select the **Pods** icon.

3. Click on your master pod.
4. Make sure the pod is offline by selecting **Take Pod Offline**.
5. Click the **Clone Pod** button to create a new pod based on the settings and snapshots of this pod.
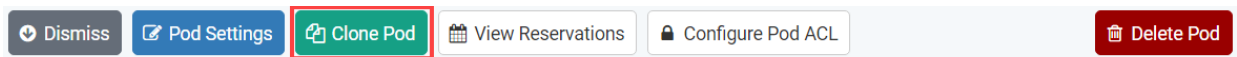
6. Input a new ID value into the **New Pod ID** field. It is advised to keep the pods in numerical order. If the pod IDs are not in numerical order, they will not show up in the scheduler in numerical order. Click **Next**.
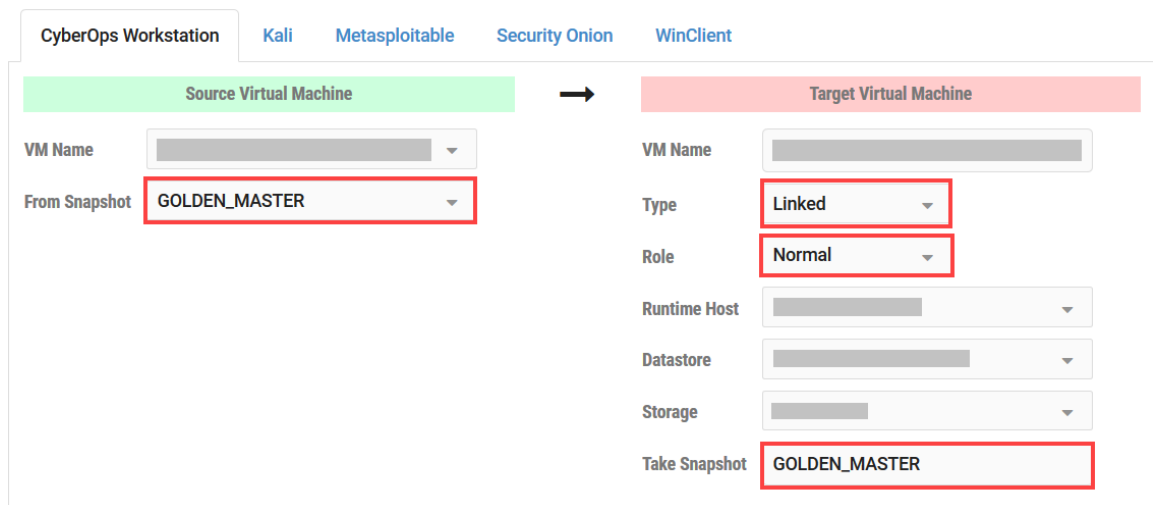
7. Enter a name for the cloned pod into the **New Pod Name** field. For example, **Cisco_CCNA_CyberOps_Pod1**. Click **Next**.

8. When the action has finished processing, you are presented with a settings screen. Notice each VM has its own tab. Go through each tab and verify the following:

   Source Virtual Machine:
   a. *From Snapshot* should be set to the **GOLDEN_MASTER** snapshot you created previously.
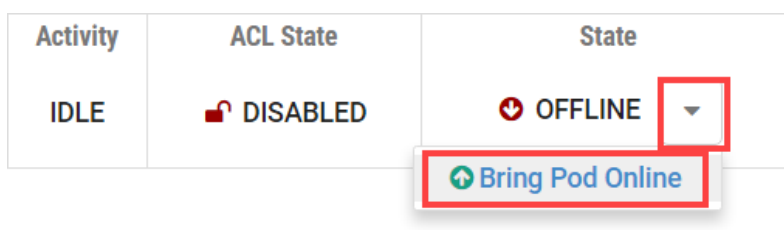
   Target Virtual Machine:
   a. For *Type*, verify that **Linked** is selected.
   b. For *Role*, verify that **Normal** role is selected.
   c. For *Take Snapshot*, verify that **GOLDEN_MASTER** s inputted.

9. When you are done changing settings, click **Clone Pod**. This should complete within a minute as we are creating linked virtual machines.
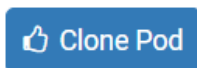
10. When the pod clone process is finished, click **OK**.
11. If you want to dedicate this pod to a particular class, team, or student, use the *Pod ACLs* feature. For details, see the [NETLAB+ VE Instructor Guide](#).
12. Click the **Online** Button in the *Pod Management* page to activate the pod.

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.

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 second host.

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

3. Click on the master pod.
4. Make sure the pod is offline by selecting **Take Pod Offline**.
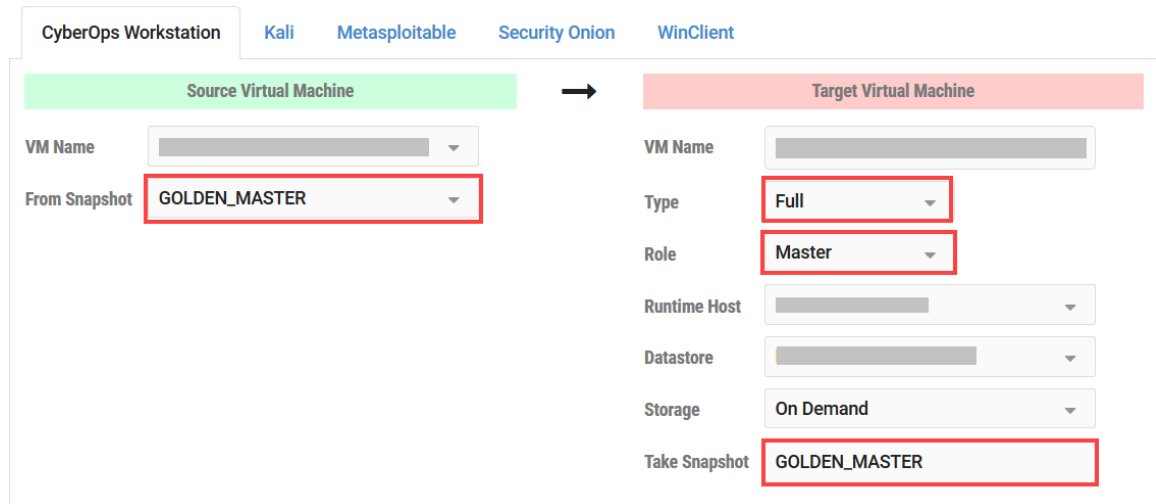5. Click the **Clone** button to create a new pod based on the settings of this pod.
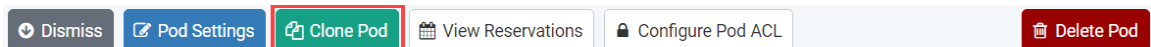
6. Input a new ID value into the **New Pod ID** field. It is advised to keep the pods in numerical order. If the pod IDs are not in numerical order, they will not show up in the scheduler in numerical order. Click **Next**.
7. Enter a name for the cloned pod into the **New Pod Name** field. For example, **Cisco_CCNA_CyberOps_Master2**. Click **Next**.
8. When the action has finished processing, you are presented with a settings screen. Notice each VM has its own tab. Go through each tab and verify the following:

   Source Virtual Machine:
   a. *From Snapshot* should be set to the **GOLDEN_MASTER** snapshot you created previously.

Target Virtual Machine:
- a. For *Type*, verify that **Full** is selected.
- b. For *Role*, verify that **Master** role is selected.
- c. For *Take Snapshot*, verify that **GOLDEN_MASTER** is inputted.
- d. For *Runtime Host*, select the second host system (which should be different than the system you are cloning from).

9. 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.
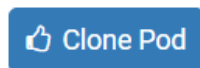
10. When the pod clone process is finished, click **OK**.

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 (see *Creating User Pods*), substituting the second master pod (created in the previous section) as the cloning source.

5.5   Assigning Pods to Students, Teams, or Classes

Please refer to the *NETLAB+ VE Instructor Guide* for details on using the *Pod ACLs* feature.