Palo Alto Networks Cybersecurity Essentials
Installation and Configuration Guide

Document Version: 2018-08-07

Installation of *Palo Alto Networks Cybersecurity Essentials* virtual pods as described in this guide requires that your *NETLAB+ VE* system is equipped with software version **18.4.2 or later**.
Contents

1 Introduction ................................................................................................................ 3
  1.1 Introducing the Palo Alto Networks Cybersecurity Essentials Pod ...................... 3
2 Planning ....................................................................................................................... 4
  2.1 Pod Resource Requirements ................................................................................ 4
  2.2 ESXi Host Server Requirements ............................................................................ 5
  2.3 NETLAB+ Requirements ....................................................................................... 5
  2.4 NETLAB+ Virtual Machine Infrastructure Setup ................................................... 5
    2.4.1 Software Requirements ................................................................................ 6
    2.4.2 Networking Requirements ............................................................................ 6
    2.4.3 Pod Internet Access ...................................................................................... 7
3 Software and Licenses ................................................................................................ 8
  3.1 Obtaining Palo Alto Networks Software Licenses ................................................ 8
  3.2 Completing the NETLAB+ Pod Internet Access and Use Agreement ............... 8
  3.3 Downloading OVF Files ......................................................................................... 8
4 Master Pod Configuration ......................................................................................... 10
  4.1 Get the Virtual Machines ready for NETLAB+ .................................................... 10
    4.1.1 Deploying Virtual Machine OVF/OVA Files ................................................. 10
    4.1.2 Modify Virtual Machines ............................................................................. 14
    4.1.3 NETLAB+ Virtual Machine Inventory Setup ................................................ 16
  4.2 Building the Master Palo Alto Networks Cybersecurity Essentials Pod ............. 18
    4.2.1 Enabling PAN8 Cybersecurity Essentials in Course Manager ..................... 18
    4.2.2 Create the Pod ............................................................................................ 18
    4.2.3 Assign Virtual Machines to the Pod ............................................................ 19
    4.2.4 Bring the Master Pod online ....................................................................... 24
  4.3 Make changes to the Master Pod ...................................................................... 24
    4.3.1 Virtual Machine Credentials ....................................................................... 24
    4.3.2 Create Class and Schedule the Master Pod ................................................ 25
    4.3.3 License the Firewall ..................................................................................... 25
    4.3.4 License the Client ........................................................................................ 25
    4.3.5 Shut down the Firewall and Client Machines ............................................. 26
    4.3.6 Reset the NIC to SAFETY NET ...................................................................... 27
    4.3.7 Create Snapshot on the Changed Master Virtual Machines ...................... 28
    4.3.8 End Reservation .......................................................................................... 28
5 Pod Cloning ............................................................................................................... 29
  5.1 Linked Clones and Full Clones ............................................................................ 29
  5.2 Creating User Pods ............................................................................................. 29
  5.3 Copying Your Master Pod to the Second Host ................................................... 31
  5.4 Creating User Pods on the Second Host ............................................................ 32
  5.5 Assigning Pods to Students, Teams, or Classes............................................... 32
1 Introduction

This document provides detailed guidance on performing the installation and configuration of the Palo Alto Networks Cybersecurity Essentials pod on the NETLAB+ VE system.

1.1 Introducing the Palo Alto Networks Cybersecurity Essentials Pod

The *Palo Alto Networks Cybersecurity Essentials* pod is a 100% virtual machine pod consisting of 4 virtual machines. Linked together through virtual networking, these 4 virtual machines provide the environment for a student or a team to perform the *Palo Alto Networks Cybersecurity Essentials* labs.
2 Planning

This guide provides specific information pertinent to delivering the Palo Alto Networks Cybersecurity Essentials 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 Palo Alto Networks Cybersecurity Essentials course will consume 39.3 GB of storage per each master pod instance.

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

<table>
<thead>
<tr>
<th>Virtual Machine</th>
<th>OVF/OVA</th>
<th>Initial Master Pod (Thin Provisioning)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>9</td>
<td>17</td>
</tr>
<tr>
<td>DMZ</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Firewall</td>
<td>7</td>
<td>17</td>
</tr>
<tr>
<td>vRouter</td>
<td>1</td>
<td>2.3</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>18</strong></td>
<td><strong>39.3</strong></td>
</tr>
</tbody>
</table>
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/

The deployment of the Palo Alto Networks Cybersecurity Essentials pod requires VMware ESXi Version of 6.0 or greater.

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 Palo Alto Networks Cybersecurity Essentials 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 Palo Alto Networks Cybersecurity Essentials 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.

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere ESXi</td>
<td>6.0</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>6.0</td>
</tr>
</tbody>
</table>

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

2.4.2 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.
2.4.3 Pod Internet Access

The pods for the Palo Alto Networks Cybersecurity Essentials course each require Internet access. This access is required for licensing the Master pod as well as the various lab objectives in the student pods.

This environment is designed to leverage one vSwitch per host that attaches to a network that has a DHCP server to assign IPv4 addresses that are routable to the Internet.

This lab environment is also designed to leverage the public DNS servers 8.8.8.8, and 4.2.2.2. This vSwitch must be able to access those servers, which may require adjustments in a firewall if applicable.
3 Software and Licenses

3.1 Obtaining Palo Alto Networks Software Licenses

To obtain licensing and access to the Palo Alto Networks Cybersecurity Essentials labs, your institution must be a Palo Alto Networks Authorized Academy Center (AAC).

You can find information about the Palo Alto Networks AAC at the following link: https://www.paloaltonetworks.com/services/education/academy

Once your membership in the Palo Alto Networks AAC is approved, you can request licenses for use with your pods from your Palo Alto Networks Academy representative or by e-mailing academy@paloaltonetworks.com.

3.2 Completing the NETLAB+ Pod Internet Access and Use Agreement

STOP You are required to complete the NETLAB+ Pod Internet Access and Use Agreement prior to obtaining access to the pod or content for this course.

Due to the security and legal implications regarding accessing the Internet from within the pod, we require that you agree to the terms contained within this online document prior to obtaining access to the pod or content for this course: https://www.netdevgroup.com/content/paloalto/agreement

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:

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 Get the Virtual Machines ready for NETLAB+

The following sub-sections deploy and prepare the virtual machines for use by NETLAB+.

4.1.1 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 datastore and click *Next*.

<table>
<thead>
<tr>
<th>VM Name</th>
<th>VM OS</th>
<th>Virtual Machine Deployment Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Windows 2012</td>
<td>PAN8_CE_Master_Client</td>
</tr>
<tr>
<td>DMZ</td>
<td>Linux</td>
<td>PAN8_CE_Master_DMZ</td>
</tr>
<tr>
<td>Firewall</td>
<td>Linux</td>
<td>PAN8_CE_Master_Firewall</td>
</tr>
<tr>
<td>vRouter</td>
<td>Linux</td>
<td>PAN8_CE_Master_VRouter</td>
</tr>
</tbody>
</table>

9. In the *Select Storage* section, select *Thin Provision* and choose the appropriate storage device. Click *Next*.

10. In the *Setup networks* section, select *SAFETY NET* as the destination and click *Next*.

    **STOP** 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*. 

8/7/2018
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.

13. The Firewall VM requires an extra step. First, deploy the VM from the OVA using the name *PAN8_210_FW_Init* and the instructions in the previous steps. Then, clone *PAN8_210_FW_Init*, naming it accordingly. Next, delete *PAN8_210_FW_Init*. This extra clone procedure is to resolve licensing with the PAN8 Firewall. You only need to perform this step with the Firewall VM.

### 4.1.2 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 of the virtual machines manually assign the **MAC** addresses for each **NIC**. The table below identifies the **MAC** addresses per **NIC**.

<table>
<thead>
<tr>
<th>Virtual Machine</th>
<th>NIC</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>1</td>
<td>00:50:56:8a:0d:49</td>
</tr>
<tr>
<td>DMZ</td>
<td>1</td>
<td>00:50:56:8a:92:db</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>00:50:56:8a:c6:2b</td>
</tr>
<tr>
<td>Firewall</td>
<td>1</td>
<td>00:50:56:8a:7c:78</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>00:50:56:8a:91:be</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>00:50:56:8a:91:c4</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>00:50:56:8a:54:c7</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>00:50:56:8a:84:17</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>00:50:56:8a:b3:fc</td>
</tr>
<tr>
<td>vRouter</td>
<td>1</td>
<td>(automatic)</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>00:50:56:8a:c8:55</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>00:50:56:8a:a6:88</td>
</tr>
</tbody>
</table>
3. Repeat the previous steps for each of the remaining virtual machines in the master pod.

4. For the vRouter virtual machine, change Network adapter 1 to the network that has DHCP Internet access available, see Pod Internet Access. Also, make sure the MAC address is set to automatic.
4.1.3 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+ VE system using the administrator account.
2. Select the Virtual Machine Infrastructure icon.

3. Click the Virtual Machine Inventory icon.

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

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.

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 (4) Virtual Machines](image)

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*. 
4.2 Building the Master Palo Alto Networks Cybersecurity Essentials Pod

This section will assist you in adding the *Palo Alto Networks Cybersecurity Essentials* pod to your *NETLAB+* system.

4.2.1 Enabling PAN8 Cybersecurity Essentials in Course Manager

Please refer to the *Course Manager* section of the *NETLAB+ VE Administrator Guide* on how to enable content. Please install the Palo Alto Networks Cybersecurity Essentials course.

4.2.2 Create the Pod

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

![Pods](image)

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

![Create New Pod](image)

4. On the *New Pod Wizard*, page click *Next*.
5. Then click on the *Palo Alto Networks Cybersecurity Essentials* pod entry.
6. On the New Pod window, input a value into the Pod ID and Pod Name fields and click Next.

![New Pod window]

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 (PAN8_CE) along with a host identifier (H45), the type and number of the pod (M11100).

7. To finalize the wizard, click OK.

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

4.2.3 Assign Virtual Machines to the Pod

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

![Pods]

2. Select the Palo Alto Networks Cybersecurity Essentials master pod from the pod list.
3. Click on the Action dropdown next to the virtual machine you are about to assign and select Attach VM.

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

4.2.3.1 Snapshot the Virtual Machine

1. In the pod list, click on the Palo Alto Networks Cybersecurity Essentials master pod you just assigned machines to.

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

4. In the Snapshot Manager window, click on the **Take** button. This will take a snapshot of the current state of the virtual machine.

   ![Snapshot Manager](image)

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

![Take Snapshot](image)

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

6. In the Snapshot Manager window, click the Dismiss button.

![Snapshot Manager](image)
4.2.3.2 Set the Revert to Snapshot

1. In the pod virtual machine view, click on the Settings button.

2. In the Settings window, click on the Revert to Snapshot dropbox and select GOLDEN_MASTER then click the Submit button.

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.


4.2.4 Bring the Master Pod online

In the pod view, click the drop arrow under State and select Online.

![Pod State](image)

4.3 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 Palo Alto Networks Cybersecurity Essentials master pod you will need to license the firewall. This process consists of:

- Scheduling the master pod
- Licensing the firewall
- Licensing the client
- Shutting down the firewall and client only (see *Shut down the Firewall and Client Machines*)
- Resetting the network interface cards to SAFETY NET
- Taking new snapshots
- Ending the reservation

4.3.1 Virtual Machine Credentials

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

<table>
<thead>
<tr>
<th>Machine</th>
<th>User name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>lab-user</td>
<td>Pal0Alt0</td>
</tr>
<tr>
<td>DMZ</td>
<td>root</td>
<td>paloalto</td>
</tr>
<tr>
<td>Firewall</td>
<td>admin</td>
<td>admin</td>
</tr>
<tr>
<td>vRouter</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>
4.3.2 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 Firewall and Client machines.

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.

4.3.3 License the Firewall

1. Log on to the Client machine in the pod.

The firewall may take a few minutes to load as the firewall will detect there is no activate license and reboot to clear any old settings. If you receive a “502 Bad Gateway” or Page Not Found” message, wait a few minutes and try again.

3. Click on the Device tab at the top.
4. Click on the Operations tab below.
5. Click on Load named configuration snapshot under Configuration Management.
6. Click the down arrow next to the Name field, and select pan8-ce-lab-06 and click OK.
7. Confirm the configuration loaded and click Close.
8. Click Commit in the upper-right.
9. Click Commit on the window.
10. When the configuration has committed successfully, click Close.
11. Scroll down in the window on the left-hand side. Click on Licenses.
12. Click on Activate feature using authorization code.
13. Enter the Authorization Code and click OK.
14. Click OK on the Warning window.

4.3.4 License the Client

1. Click on the Start icon in the lower left.
2. Right-click on This PC and select Properties.
3. Click on Activate Windows in the lower right.
4. Type the Product key.
5. Click Close.
4.3.5 Shut down the Firewall and Client Machines

1. In the Firewall web interface, make sure the Device tab is selected at the top and click Setup on the left side.
2. Click on Shutdown Device under Device Operations.
3. Click Yes on the Shutdown Device window.
4. Close the web browser.
5. From the Client dropdown in NETLAB+, select Send CTRL+ALT+DEL.

6. Click the Power symbol in the lower-right and select Shut down.

7. Leave the default reason and click Continue.
4.3.6 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 Client and Firewall virtual machines. Starting with the Client, right-click on the virtual machine and select Edit settings...
5. Change Network adapter 1 to SAFETY NET.

6. Click OK to confirm settings.
7. Repeat steps 4-6 for the Firewall virtual machine as well. Make sure all network adapters are set to SAFETY NET.
4.3.7 Create Snapshot on the Changed Master Virtual Machines

1. Right-click on the Client 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.
7. Repeat steps 1-6 for the Firewall virtual machine.

4.3.8 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. Click the Clone Pod button to create a new pod based on the settings and snapshots of this pod.
5. 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.
6. Enter a name for the cloned pod into the New Pod Name field. For example, PAN8_CE_H45_M11101. Click Next.
7. 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:**
- *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** is inputted.

8. When you are done changing settings, click **Clone Pod**. This should complete within a minute as we are creating linked virtual machines.

9. When the pod clone process is finished, click **OK**.
10. 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**.
11. 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. Click the `Clone` button to create a new pod based on the settings of this pod.
5. 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`.
6. Enter a name for the cloned pod into the `New Pod Name` field. For example, `PAN8_CE_H46_M11200`. Click `Next`.
7. 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:**
   - `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).
8. 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.

9. 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.