



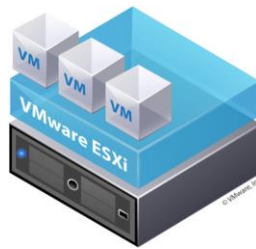
This support document is intended for users with an active VMware vSphere license. If you do not have a VMware vSphere license, you will need to purchase one to operate NETLAB+ until our team releases a version utilizing Proxmox.



## Remote PC Guide Series - Volume 2

### Installing and Configuring VMware vSphere 6.0

Document Version: **2019-02-25**



This guide will lead you through the process of adding remotely accessible PC or servers into your NETLAB+ equipment pods using the [VMware](#) ESXi and vCenter virtualization products.

This guide is part of a multi-volume series, designed to provide you with the guidance needed to implement remote PCs on your NETLAB+ system. [Learn more about the Remote PC Guide Series.](#) See the [Documentation Library](#) for a list of all NETLAB+ guides.



The details of this guide are specific to **VMware ESXi version 6.0 with vCenter.**

Copyright © 2019 Network Development Group, Inc. [www.netdevgroup.com](http://www.netdevgroup.com)

NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

VMware is a registered trademark of VMware, Inc. Cisco, IOS, Cisco IOS, Networking Academy, CCNA, and CCNP are registered trademarks of Cisco Systems, Inc.

1	Background .....	3
2	VMware Infrastructure Planning .....	4
2.1	VMware ESXi Host Requirements .....	5
2.2	VMware vCenter Server Requirements .....	6
3	VMware Infrastructure Software and Licenses .....	7
3.1	Downloading ESXi software for the Dell R630 .....	7
3.2	Gaining access to VMware Licenses for your Infrastructure .....	8
3.3	Obtaining VMware vCenter and ESXi Software and Licenses.....	8
3.4	Obtaining the VMware vCenter Server Appliance .....	12
4	Network Planning.....	13
5	VMware Infrastructure Setup .....	15
5.1	Preparing the ESXi Server .....	15
5.2	Installing ESXi on a Host Server .....	16
6	Basic Network Configuration .....	17
7	Management Console .....	18
8	vCenter Server Appliance Deployment.....	19
8.1	Configure Automatic Startup for vCenter .....	19
9	vCenter Server Appliance Configuration .....	21
9.1	Create NETLAB+ datacenter in vCenter .....	21
9.2	Adding ESXi hosts to the NETLAB+ datacenter .....	21
9.3	Allowing Remote PC Viewer sessions in ESXi firewall.....	23
9.4	Modifying Password Policies.....	25
9.4.1	Modifying the SSO Configuration Password Policy .....	25
9.4.2	Modifying the root Password Policy .....	27
10	vSwitch Configuration .....	28
10.1	Verifying vSwitch0 Configuration .....	29
10.2	Inside Network Configuration .....	29
10.3	Creating vSwitch1 and Binding to Physical NIC .....	33
10.4	Create a Safe Staging Network .....	36

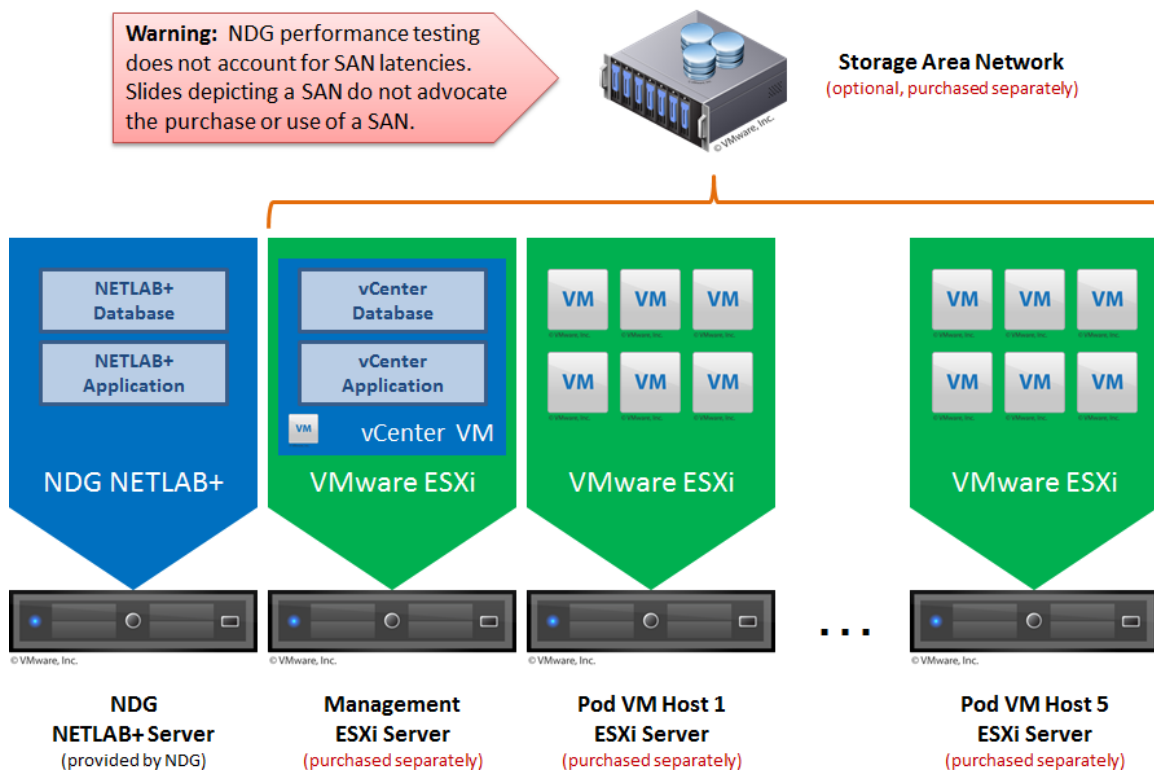
## 1 Background

NETLAB+ pod remote PCs and servers can be implemented using virtual machines running on VMware vSphere 6.0. This guide is designed to help you set up your virtual machine infrastructure for use with NETLAB+.

- This guide assumes you are familiar with the Remote PC concept behind NETLAB+. Please review the [Remote PC Guide Series - Volume 1, Introduction and Planning for Remote PC Implementation with NETLAB+](#).
- This guide is designed to help you install and configure vSphere 6.0 for use with NETLAB+. You will be installing VMware ESXi 6.0 and a VMware vCenter 6.0 Server Appliance.
- This guide also assumes that you have configured the NDG supported servers, the Dell R630 or SuperMicro 1028U-TR4+.

Dell R630 users: Please refer to the [Remote PC Guide Series - Volume 2c - Dell R630 BIOS and RAID Configuration](#) for details.

The basics of a NETLAB+ infrastructure consist of a NETLAB+ Appliance, Management Server, vCenter Appliance, and ESXi Host Server. The following image illustrates how these all work together:



## 2 VMware Infrastructure Planning

There are two components to the VMware Infrastructure: (1) Physical VMware ESXi servers host the virtual machines in your pods (2) VMware vCenter Server enables you to manage the resources of multiple ESXi hosts and allows you to monitor and manage your physical and virtual infrastructure.

Virtualization using ESXi is performed on separate physical servers, not included with NETLAB+. You can interface with multiple ESXi servers for larger deployments. NETLAB+ integrates with VMware vCenter Server to assist the administrator with installing, replicating and configuring virtual machine pods.



NETLAB+ is compatible with VMware ESXi version 6.0 and vCenter Server version 6.0.

## 2.1 VMware ESXi Host Requirements

Please refer to our host server specifications page for the latest information on recommended ESXi Host servers. Use the following link to get detailed requirements: [http://netdevgroup.com/support/remote\\_pc.html#vm\\_host\\_server\\_specifications](http://netdevgroup.com/support/remote_pc.html#vm_host_server_specifications)

Please search the VMware Compatibility guide to ensure your ESXi host hardware is compatible with the VMware version you wish to use: <http://www.vmware.com/resources/compatibility/search.php>

### NDG Equipment Selection Disclaimer

NDG offers no warranties (expressed or implied) or performance guarantees (current or future) for third-party products, including those products NDG recommends. Due to the dynamic nature of the IT industry, our recommended specifications are subject to change at any time.

NDG recommended equipment specifications are based on actual testing performed by NDG. To achieve comparable compatibility and performance, we strongly encourage you to utilize the same equipment, exactly as specified and configure the equipment as directed in our setup documentation. Choosing other hardware with similar specifications may or may not result in the same compatibility and performance. The customer is responsible for compatibility testing and performance validation of any hardware that deviates from NDG recommendations. NDG has no obligation to provide support for any hardware that deviates from our recommendations, or for configurations that deviate from our standard setup documentation.

Hardware Assisted Virtualization (Intel VT-x) is **REQUIRED** on any host you use.

Virtualization courses, such as the VMware IT Academy labs, have not been tested on server platforms using AMD processors and are not supported on server platforms using AMD processors. VMs available from CSSIA were created on the Intel platform. As such, they may not work as intended on a server platform utilizing AMD processors.

## 2.2 VMware vCenter Server Requirements

As of vSphere 5.1, NDG only supports the VMware vCenter Appliance. The physical server where the vCenter appliance resides should be a dedicated "management server" to provide ample resources. It is strongly recommended you follow our server recommendations listed below to provide ample resources now and in the future.

[http://www.netdevgroup.com/support/remote\\_pc.html#vcenter\\_server\\_specifications](http://www.netdevgroup.com/support/remote_pc.html#vcenter_server_specifications)



NDG does not support configurations where vCenter is running on a heavily loaded ESXi host and/or an ESXi host that is also used to host virtual machines for NETLAB+ pods. Such configurations have exhibited poor performance, API timeouts, and sporadic errors in NETLAB+ operations.

The vCenter server must have network access to your ESXi servers. You will use the VMware vSphere Web Client to access vCenter Server. As of vSphere 5.1, there is a vSphere Web Client.

Below is a list of reasons why NDG will only support the VMware vCenter Server Appliance:

- Starting with vCenter 5.1, the appliance now uses Postgres databases. This allows the appliance to be able to handle multiple VMs and multiple ESXi hosts compared to the 5 ESXi hosts and 50 VM limit that the vCenter 5.0 Appliance had.
- The vCenter Appliance is a standalone VM that runs on SUSE Linux, instead of Microsoft Windows Server. This eliminates the need for Microsoft licensing for both Microsoft Windows Server and SQL Server.
- The Windows version of vCenter 5.1 now requires multiple databases. It also requires an Active Directory setup in order to work with the VMware Single Sign-On feature that is embedded in the appliance. Because of the complexity of configuring an Active Directory and multiple databases, NDG no longer recommends nor supports the Windows version. Based on our research, VMware is migrating to the appliance version in the future.
- The quick and easy deployment of the vCenter Appliance makes the infrastructure configuration much easier to deploy for NETLAB+ administrators.
- NDG strongly recommends and only supports the use of the vCenter Appliance on a separate Management Server. NDG has Management Server recommendations that will support not only the vCenter Appliance but also future versions of the NETLAB+ software.

### 3 VMware Infrastructure Software and Licenses

In order to continue, you must have received an email from Kivuto Solutions with your login information for your school's web store.

#### 3.1 Downloading ESXi software for the Dell R630



If you are not using the Dell R630, please skip to section [3.2](#).

**Dell R630 Users: It is very important that you download the software from Dell, as they have customized the installer ISO with drivers for the server platform, including networking and storage adapters.**

The following procedure assumes you are using a Dell R630 server:

1. Go to Dell's website at <http://www.dell.com>.
2. Hover your mouse over **Support** below the Search text box and click on **Support by Product**.
3. The easiest way is to enter your Dell Service Tag, usually found on the front of your Dell Server. It can be found on a plastic pullout tab on the front of the server. Enter your service tag and click **Submit**.
4. If you cannot locate your Dell Service Tag, choose **View products** in the Browse for a product window and select **Servers, Storage, & Networking** under *Select a product*. Select **PowerEdge** and select your server model.
5. Click on **Drivers and Downloads** from the tabs listed in the middle of the page.
6. Under *Optimize your system with drivers and updates*, click on **Change OS**.
7. Select **VMware ESXi 6.0** from the list of operating systems. The list name should change to **View all available updates for VMware ESXi 6.0**.
8. In the list of categories below, select **Enterprise Solutions (2 files)**.
9. Click on **Download File** under VMware ESXi 6.0 Update 1.
10. Under *Other file formats*, click on **Download File** beneath the ISO file.
11. Select **Save File** and click **OK** to begin the download.
12. The above steps should point you to the following link. However, it is strongly recommended that you use the steps above to make sure you are getting the latest copy: [http://downloads.dell.com/FOLDER03374484M/1/VMware-VMvisor-Installer-6.0.0.update01-3073146.x86\\_64-Dell\\_Customized-A01.iso](http://downloads.dell.com/FOLDER03374484M/1/VMware-VMvisor-Installer-6.0.0.update01-3073146.x86_64-Dell_Customized-A01.iso)

### 3.2 Gaining access to VMware Licenses for your Infrastructure

Licensing considerations will vary, depending on your school's participation in the [VMware IT Academy Program \(VITA\)](#) program and/or the [VMware Academic Subscription \(VMAS\)](#).

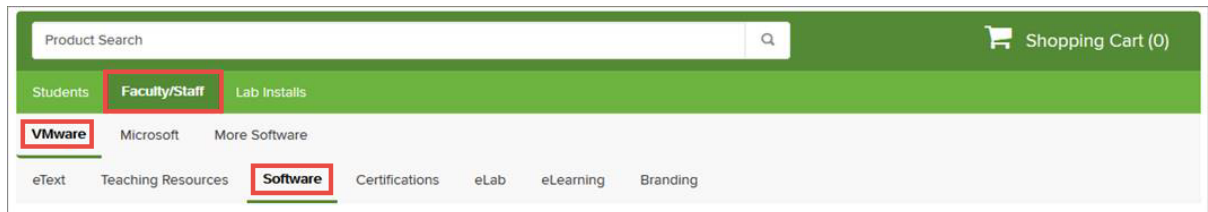


Guidance on navigating licensing is available on the [VMware Product Licensing Through VMware Academic Subscription \(VMAS\)](#) chart.

### 3.3 Obtaining VMware vCenter and ESXi Software and Licenses

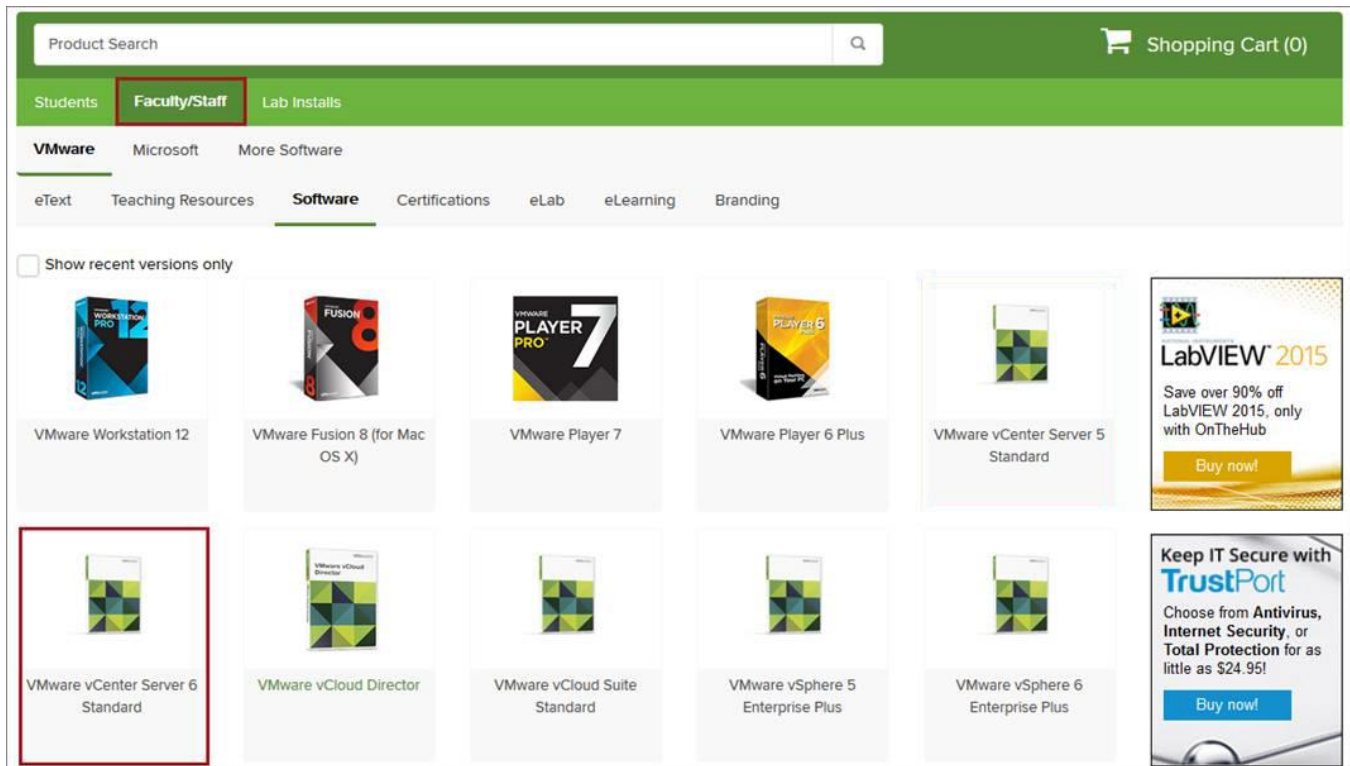
When downloading VMware vCenter and ESXi, it is important to select a version that is compatible with NETLAB+. NETLAB+ is compatible with VMware vCenter and ESXi version 6.0.

1. Follow the link provided to you by VMware when you registered in the VMware Academic Subscription. This will take you to the academic software store.
2. Sign in with your registered login.
3. Click on **Faculty/Staff** at the top followed by **VMware** and then **Software** to see the available downloads. You must be a registered Faculty/Staff user. For more information, contact the VMware Academy contact at your school.

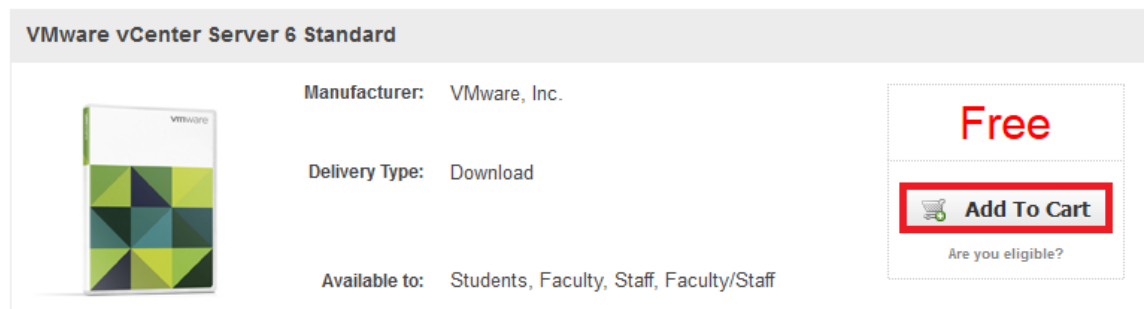




- Click on **VMware vCenter Server 6 Standard**. This is the first of two software items you will obtain from your school's webstore. The correct item is marked with a red box in the picture below.

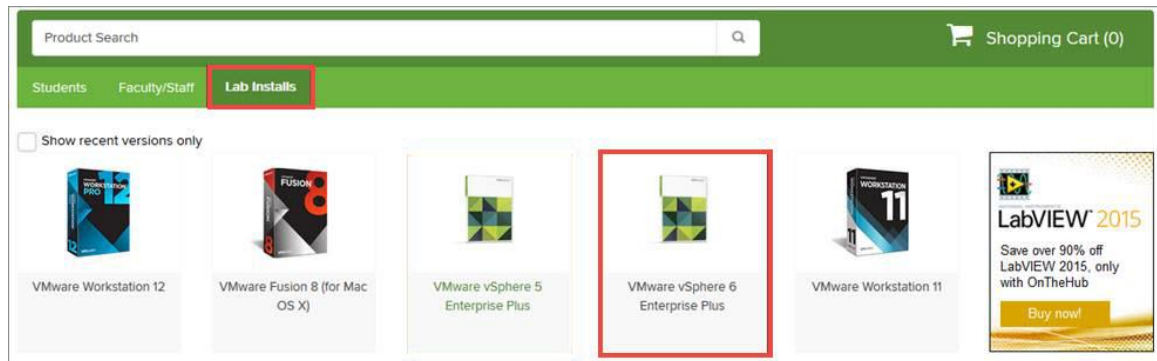


- Click on **Add to Cart**.

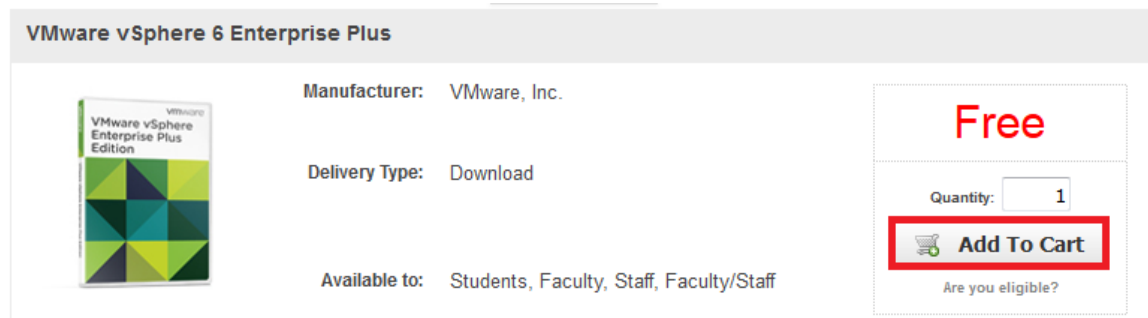


- Click on **Continue Shopping**.
- Click on **Lab Installs** located at the top panel.

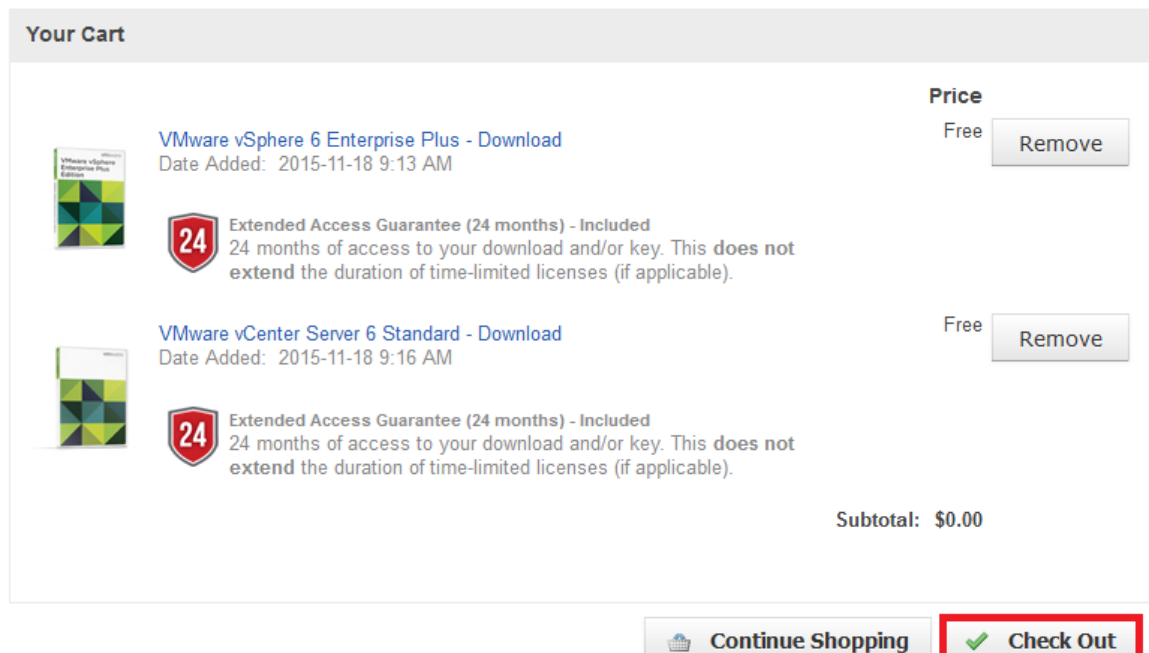
- Click on **VMware vSphere 6 Enterprise Plus**. This is the second of two software items you will obtain from your school's webstore. The correct item is marked with a red box in the picture below.



- Click on **Add to Cart**.







- Click on **Check Out** to continue.



11. Read and accept the **EULA**.
12. On the confirmation page, click on **Proceed With Order**.
13. On the receipt page, record the serial numbers found under **Items**. **You will need these serial numbers for the installation later.**

**Items** All prices are in US Dollars Start Download

	Amount
 VMware vSphere 6 Enterprise Plus - Download	\$0.00
 Extended Access Guarantee (24 months) - Included 24 months of access to your download and/or key. This does not extend the duration of time-limited licenses (if applicable). Expires 2017-11-18	
Serial Number: M12A3 [REDACTED] C1R40	
Messages: <ul style="list-style-type: none"><li><a href="#">VMware EULA</a></li></ul>	
 VMware vCenter Server 6 Standard - Download	\$0.00
 Extended Access Guarantee (24 months) - Included 24 months of access to your download and/or key. This does not extend the duration of time-limited licenses (if applicable). Expires 2017-11-18	
Serial Number: HJ03J [REDACTED] 8R2P4	
Messages: <ul style="list-style-type: none"><li><a href="#">VMware EULA</a></li></ul>	
Subtotal: \$0.00	
Taxes: \$0.00	
Total: \$0.00	

14. Stay on the **Items** page and continue following the instructions in the next section.

### 3.4 Obtaining the VMware vCenter Server Appliance

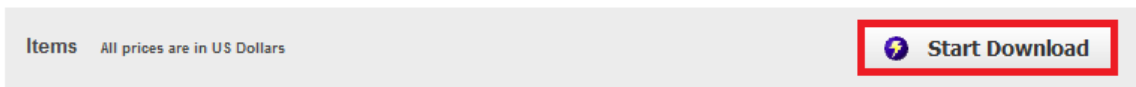


If you are using the Dell R630 please go to section 3.1 for guidance specific to the Dell R630 for obtaining VMware ESXi and licenses.

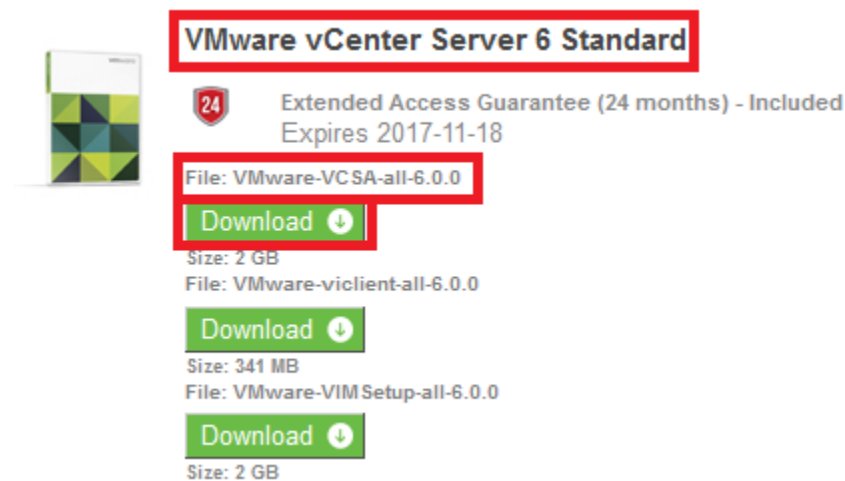
If you are using any other server, including the SuperMicro 1028U-TR4+, please contact your vendor to find out if a customized version of VMware ESXi needed for your hardware. Otherwise, follow the instructions below to access the generic VMware vCSA executable installation file(s).

The following information will point you to the generic VMware vCSA executable installation file(s).

1. You may download the necessary software by clicking on **Start Download**.



2. Under VMware vCenter Server 6 Standard, click the **Download** link for **VMware-VC SA-all-6.0.0**.



3. Select **Save File** when prompted and then click **OK**.
4. Click on the **Download** link under **VMware vSphere 6 Enterprise Plus**.
5. Select **Save File** when prompted and then click **OK**.

## 4 Network Planning

This section is designed to help you plan your networking infrastructure. Please review the "Networking Models" section of the [Remote PC Guide Series - Volume 1, Introduction and Planning for Remote PC Implementation with NETLAB+](#).



Remember, dual-homed is only necessary and required if you plan to use real physical lab devices, such as physical equipment pods for the Cisco Networking Academy.

The IP addressing and DNS servers will be dictated by the model you select. Please fill out the appropriate table below to help assist you with configuration.



It is strongly recommended that you print out your table in order to have it available for easy reference throughout the installation and configuration of your Virtual Machine Infrastructure.

Single-Homed Model	
vCenter Outside IP Address	
ESXi Management Server Outside IP Address	
ESXi Host Server 1 Outside IP Address	
ESXi Host Server 2 Outside IP Address	
ESXi Host Server 3 Outside IP Address	
ESXi Host Server 4 Outside IP Address	
Subnet Mask	
Default Gateway	
Primary DNS Server	
Secondary DNS Server	

	NETLAB+		vCenter Appliance		ESXi Management Server		ESXi Host 1 Server	
	Outside	Inside	Outside	Inside	Outside	Inside	Outside	Inside
IP Address	Campus		Campus		Campus		Campus	
Subnet Mask	Campus		Campus		Campus		Campus	
Gateway	Campus		Campus		Campus		Campus	
vSwitch			vSwitch0		vSwitch0		vSwitch0	
Management Path			*		*		*	

Dual-Homed Model – Real Equipment Pods	
vCenter Outside IP Address	
ESXi Management Server Outside IP Address	
ESXi Host Server 1 Outside IP Address	
ESXi Host Server 1 Inside IP Address	169.254.0.241
ESXi Host Server 2 Outside IP Address	
ESXi Host Server 2 Inside IP Address	169.254.0.242
ESXi Host Server 3 Outside IP Address	
ESXi Host Server 3 Inside IP Address	169.254.0.243
ESXi Host Server 4 Outside IP Address	
ESXi Host Server 4 Inside IP Address	169.254.0.244
Outside Subnet Mask	
Inside Subnet Mask	255.255.255.0
Outside Default Gateway	
Inside Default Gateway	None
Primary DNS Server	
Secondary DNS Server	

	NETLAB+		vCenter Appliance		ESXi Management Server		ESXi Host 1 Server	
	Outside	Inside	Outside	Inside	Outside	Inside	Outside	Inside
IP Address	Campus	169.254.0.254	Campus		Campus		Campus	169.254.0.241
Subnet Mask	Campus	255.255.255.0	Campus		Campus		Campus	255.255.255.0
Gateway	Campus	not set	Campus		Campus		Campus	not set
vSwitch			vSwitch0		vSwitch0		vSwitch0	vSwitch1
Management Path			*		*		*	

## 5 VMware Infrastructure Setup

This section describes the software installation on a VMware ESXi host server.



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

There should be a minimum of two (2) ESXi servers. One will be used for management, referred to, as the Management Server, and the other will be your ESXi Host Server, which will hold the virtual machines for the pods. You may have one or more ESXi Host servers depending on the courses you plan to teach.

NDG supports the Dell R630 or SuperMicro 1028U-TR4+ for use as a Management Server or as an ESXi Host Server. Please refer to the NDG requirements website for the latest supported server configurations:

[http://www.netdevgroup.com/support/remote\\_pc.html#vm\\_host\\_server\\_specifications](http://www.netdevgroup.com/support/remote_pc.html#vm_host_server_specifications)

### 5.1 Preparing the ESXi Server

NDG recommends the Dell R630 or SuperMicro 1028U-TR4+ server platforms. If you are using non-supported servers, please contact your vendor for assistance in configuring the BIOS and RAID options.



Dell R630 Users: For instructions on BIOS and RAID configuration please refer to [\*Remote PC Guide Series - Volume 2c - Dell R630 BIOS and RAID Configuration\*](#).

## 5.2 Installing ESXi on a Host Server

This section will refer you to the appropriate documentation on VMware's Website to install the ESXi host software. This will need to be performed on the Management Server and on each ESXi Host Server. The PDF for the installation document can be found at the following link: [vSphere Installation and Setup](#).



Please let us know if the above link to VMware's documentation does not work so that we can update it accordingly.

Special Instructions for installing ESXi when using the above-linked document:

1. Use section 4 - Installing ESXi for the installation.
2. The subsection is Installing ESXi interactively, pp. 55-57.
3. Important information regarding the Direct Console ESXi Interface can be found in section 5, pp. 162-166.



## 6 Basic Network Configuration

This section will refer you to the appropriate documentation on VMware's Website to configure the network settings on your servers. This will need to be performed on the Management Server and on each ESXi Host Server. The PDF for the installation document can be found at the following link: [vSphere Installation and Setup](#).



Please let us know if the above link to VMware's documentation does not work so that we can update it accordingly.

Special Instructions for installing ESXi when using the above-linked document:

1. Use section 5 - Setting Up ESXi for configuration.
2. You can skip subsection, Set the VLAN ID (p. 169).
3. The subsection is Configuring IP Settings for ESXi (pp. 169-172).
  - a. Use the table you filled out in section 4 for your IP addressing and DNS setup.
  - b. If you are not using IPv6, it is strongly recommended that you disable it to prevent possible networking issues in a production environment.

## 7 Management Console

The VMware vCenter Server Appliance can be managed through any web browser or the vSphere client. This configuration requires a “management console” in order to configure the vCenter Server appliance, ESXi Host Servers, and virtual machines. The management console can be either a virtual machine or a physical host like a workstation or laptop. The management console will need to be on the same network as the ESXi hosts and vCenter Server Appliance.

The management console will also be where you want to download any virtual machine images for pod deployment. As such, it is strongly recommended that you have plenty of storage available to this virtual machine.

## 8 vCenter Server Appliance Deployment

This section will refer you to the appropriate documentation on VMware's Website to deploy the vCenter Server Appliance. The PDF for the installation document can be found at the following link: [Deploying the VMware Server Appliance](#).



Please let us know if the above link to VMware's documentation does not work so that we can update it accordingly.



NDG does not support configurations where vCenter is running on a heavily loaded ESXi host and/or an ESXi host that is also used to host virtual machines for NETLAB+ pods. Such configurations have exhibited poor performance, API timeouts, and sporadic errors in NETLAB+ operations.

Special Instructions for installing vCSA when using the above-linked document:

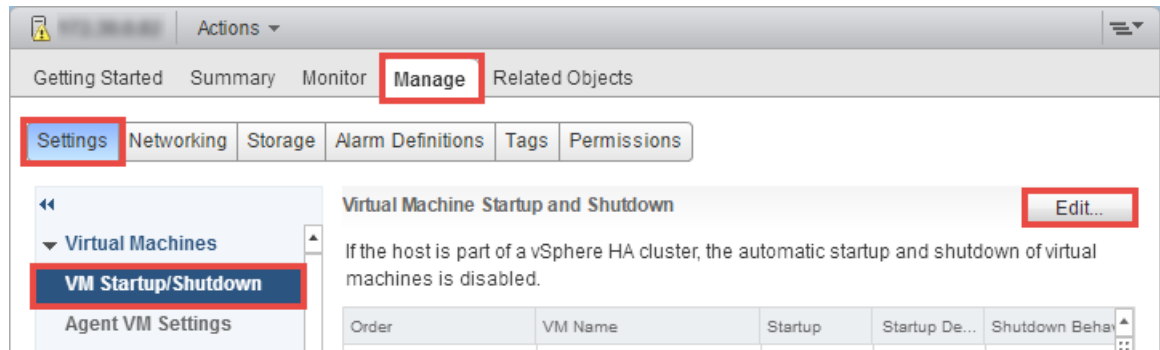
1. Use section 9 – Deploying the vCenter Server Appliance.
2. The subsections are Download the vCenter Server Appliance Installer, Install the Client Integration Plug-In, and Deploying a vCenter Server Appliance with an Embedded Platform Services Controller (pp. 233-238)
  - a. On step 9, choose to **Create a new Single Sign-On domain**.
  - b. On step 11, select the **Medium** appliance size.
  - c. On step 13, **Use an embedded database (vPostgres)**.
  - d. On step 14, select **Static** as the Network type (use the table you filled out in section 4 for the IP address of the appliance).

### 8.1 Configure Automatic Startup for vCenter

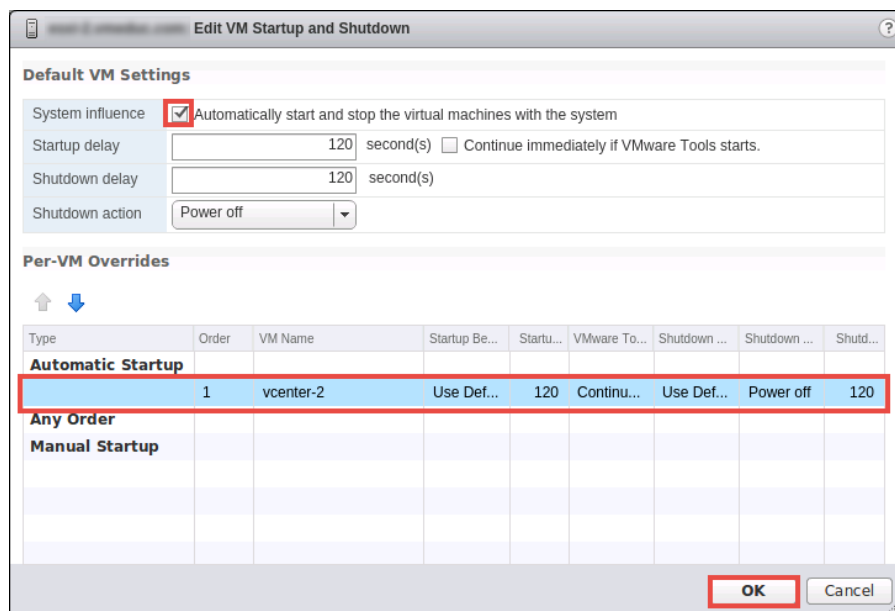
For this section, you will configure vCenter to start with the ESXi Management Server automatically. This is important because if it is not set up and the ESXi Management Server powers off or is rebooted, the vCenter Appliance will not start up causing NETLAB+ communication failure.

1. Using the *vSphere Web Client*, navigate to **Hosts and Clusters**.
2. Click on your ESXi host in the inventory pane where the vCSA reside.
3. With the host selected, select **Manage > Settings** from the top pane.

4. Under Virtual Machines, select **VM Startup/Shutdown** and click **Edit**.



5. On the *Edit VM Startup and Shutdown* window, click the checkbox to **Automatically start and stop the virtual machines with the system**.
6. Select your vCenter VM in the list and click the **Move Up** icon until it is directly under **Automatic Startup**.
7. Click **OK**.



8. Close **vSphere Web Client**.

## 9 vCenter Server Appliance Configuration

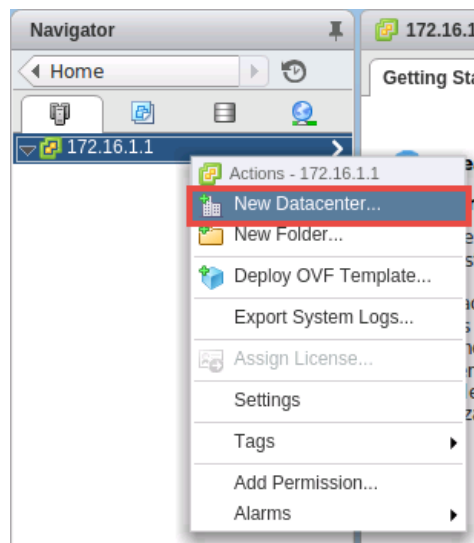
In this section, you will be:

- Setting up and configuring a NETLAB+ datacenter
- Adding your ESXi Host Servers to the datacenter
- Allowing Remote PC Viewer sessions in the ESXi firewall
- Modifying Password Policies

### 9.1 Create NETLAB+ datacenter in vCenter

In this section, we will be creating a NETLAB+ datacenter on the vCenter.

1. Using the vSphere Web Client, log into the vCSA using the IP address you set in section 8.
2. Click on **Hosts and Clusters**.
3. Right-click on your **vCSA** and select **New Datacenter**.



4. Set the datacenter name to **NETLAB** and click **OK**.

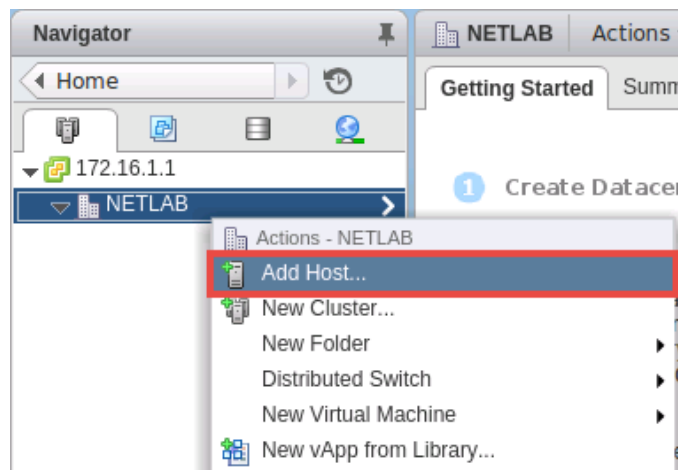
### 9.2 Adding ESXi hosts to the NETLAB+ datacenter

In this section, you will be adding ESXi Host Servers to the NETLAB+ datacenter so that they may be managed by vCenter.

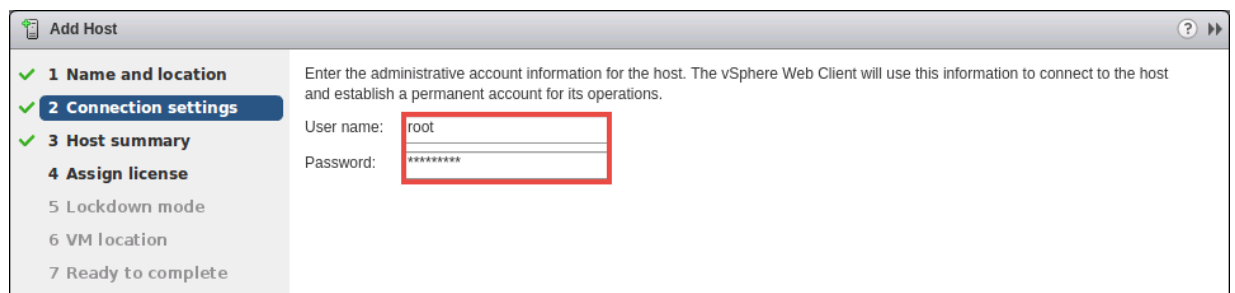


You will NOT add the Management Server to vCenter. You will only add your ESXi Host Servers that will house the virtual machines for the pods.

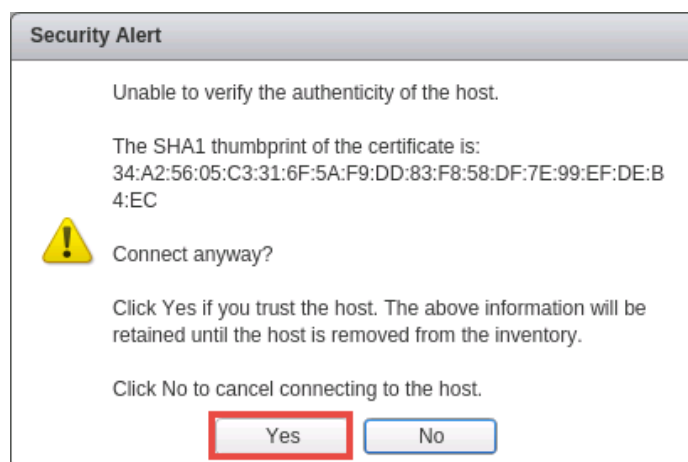
1. Right-click on the datacenter **NETLAB**, and select **Add Host**. The Add Host wizard appears.



2. First, you are going to add one of your ESXi host servers, enter the IP address you from your table in section 4. Click **Next**.
3. Enter the username and the password you set up in section 5.2 and click **Next**.

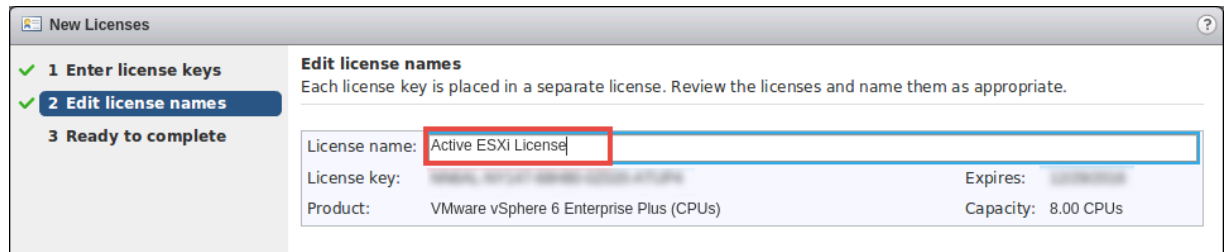


4. When prompted with a **Security Alert** window, click **Yes** to add the Host.



5. On the *Host summary* page, review the information and click **Next**.
6. On the *Assign license* page, click on the **Create New Licenses** icon (green plus).

7. In the *New Licenses* window, on the *Enter license keys* page, enter the key you received from VMware in section 2. Click **Next**.
8. On the *Edit license names* page, enter any desired name for your records and click **Next**.



9. On the *Ready to complete* page, review the information and click **Finish**. You will be redirected to the *Add Host* window.



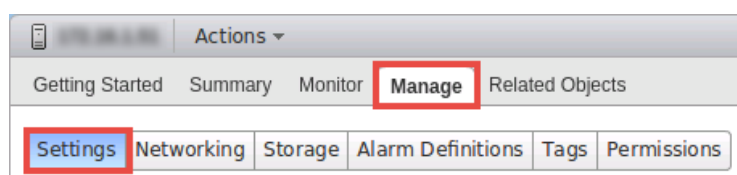
If brought back to the Connection settings page, enter the username and the password you set up in section 5.2 once more and click **Next**. Click **Yes** on the Security Alert dialog. Review the information on the *Host summary* page and click **Next**. On the *Assign license* page, select the radio button to the newly added license key and click **Next**.

10. On the *Lockdown mode* page, leave lockdown mode **disabled** and click **Next**.
11. On the *VM location* page, make sure **NETLAB** is selected and click **Next**.
12. On the *Ready to complete* page, review the information and click **Finish**.
13. Expand the **NETLAB** datacenter on the left pane and wait for the IP address of the host you entered to be added. Review the **Recent Tasks** pane on the right to make sure the status goes to **Completed**.
14. Repeat steps 1-13 to add any additional remaining host servers.

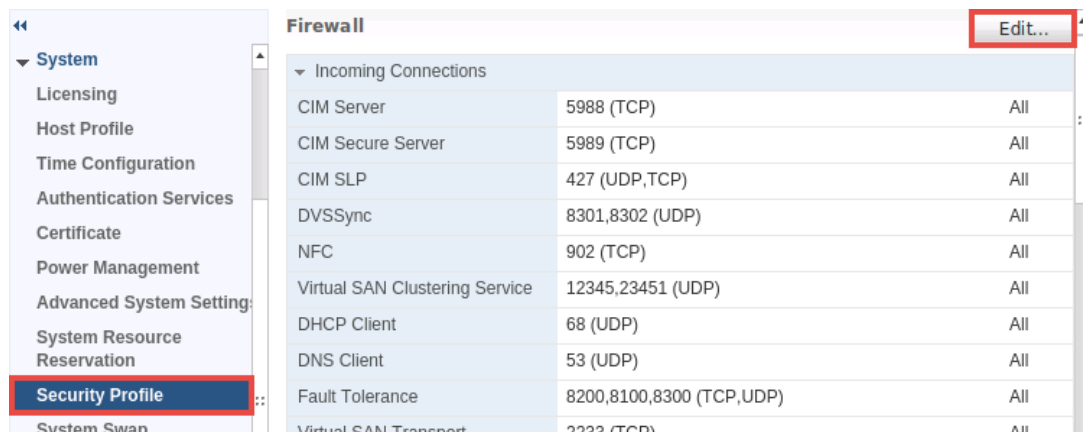
### 9.3 Allowing Remote PC Viewer sessions in ESXi firewall

In this section, you will be enabling a specific port range in the ESXi firewall to allow Remote PC Viewer sessions to have access to the virtual machine console.

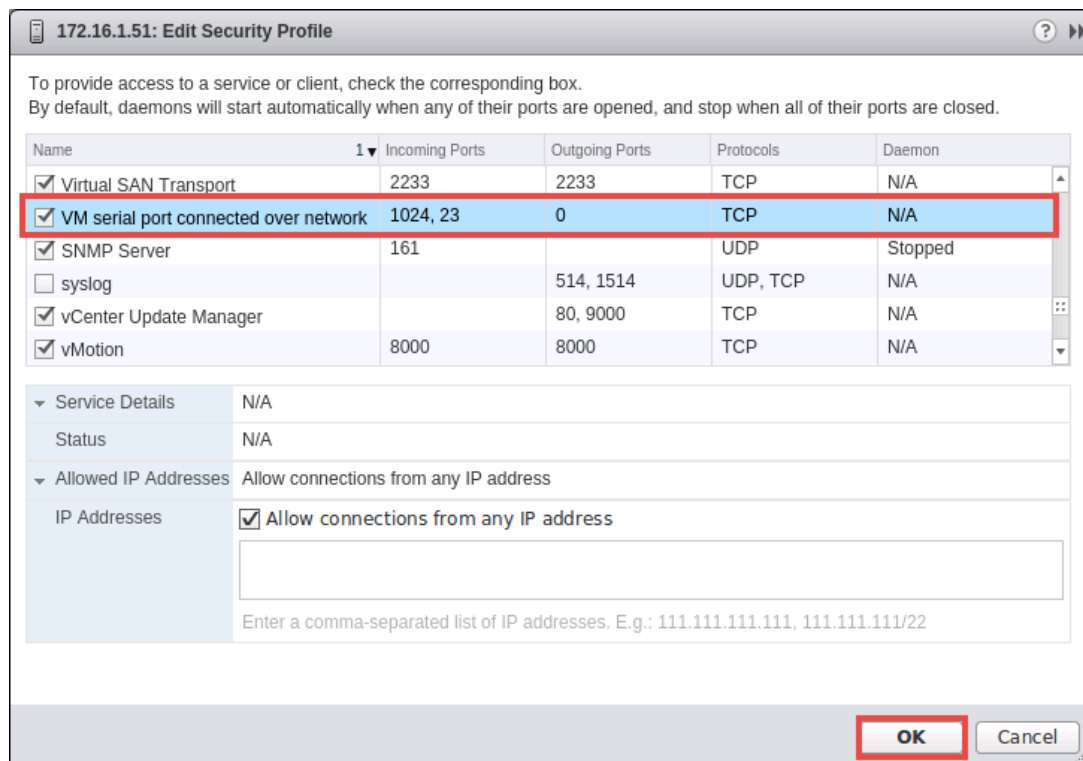
1. Select your first ESXi host in the **Inventory** pane on the left.
2. Navigate to **Manage > Settings**.



- Under **System** click on **Security Profile**. Then click on the **Edit** button to review the built-in ESXi firewall settings.



- In the *Edit Security Profile* window, scroll to the bottom of the list and click the checkbox for **VM serial port connected over network**. Click **OK** to save settings.



- Repeat steps 1-4 for each ESXi host.



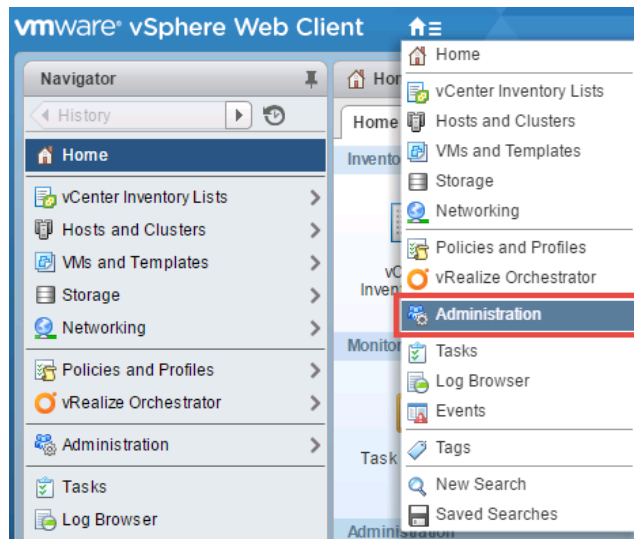
## 9.4 Modifying Password Policies

The subsections below provide details on modifying the password policies for SSO configuration and root configuration.

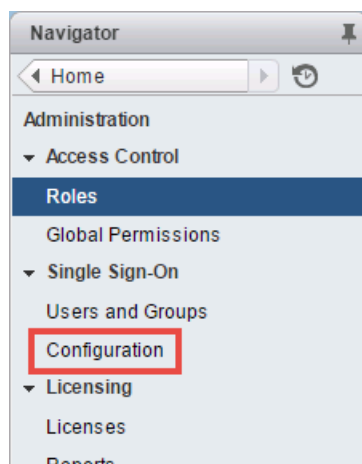
### 9.4.1 Modifying the SSO Configuration Password Policy

In this section, you will be modifying the password policy for SSO configuration.

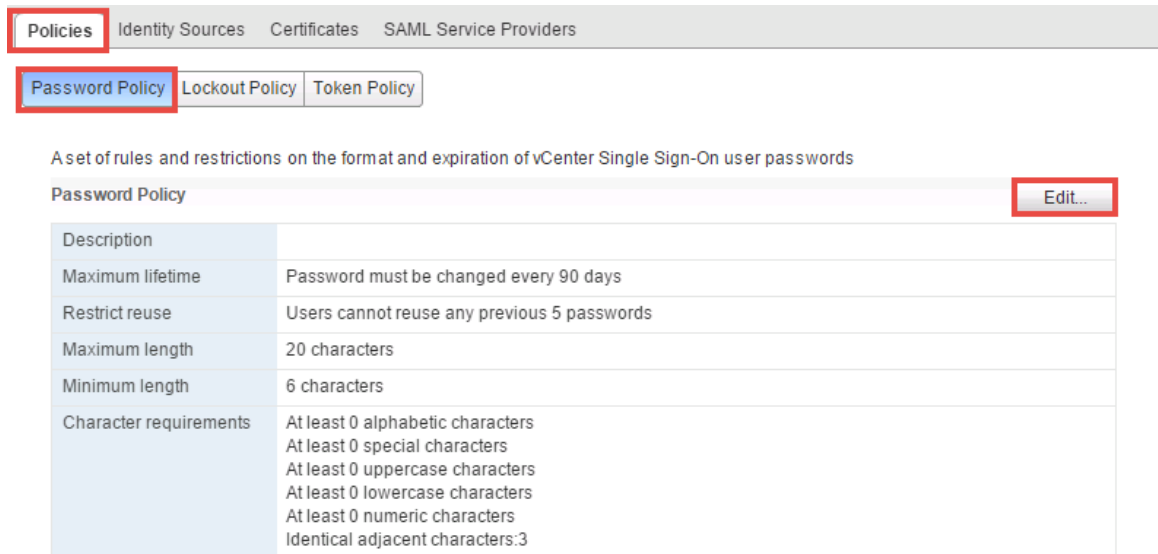
1. Using the *vSphere Client*, navigate to **Administration**.



2. In the *Navigator* pane located to the left, click on **Configuration** underneath the *Single Sign-On* header.

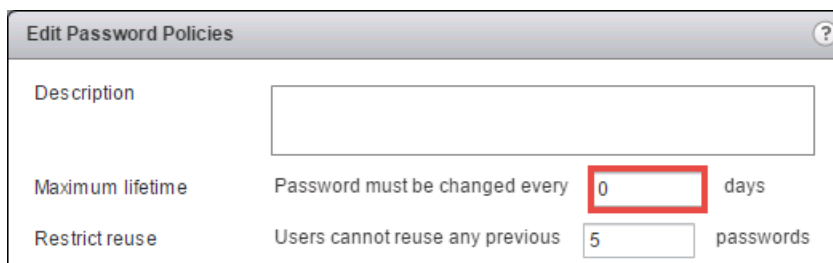


3. In the middle pane, ensure that the **Policies** tab is selected. Select the **Password Policy** button and click on the **Edit** button.



A set of rules and restrictions on the format and expiration of vCenter Single Sign-On user passwords	
Password Policy <span>Edit...</span>	
Description	
Maximum lifetime	Password must be changed every 90 days
Restrict reuse	Users cannot reuse any previous 5 passwords
Maximum length	20 characters
Minimum length	6 characters
Character requirements	At least 0 alphabetic characters At least 0 special characters At least 0 uppercase characters At least 0 lowercase characters At least 0 numeric characters Identical adjacent characters:3

4. In the *Edit Password Policies* window, change the value to reflect 0 days for *Maximum lifetime*.



Edit Password Policies	
Description	
Maximum lifetime	Password must be changed every 0 days
Restrict reuse	Users cannot reuse any previous 5 passwords

5. The remaining password policy options can be modified if desired.



For additional guidance on editing the single sign-on password policy, you may refer to the [VMware Knowledge Base article](#).

6. When finished, click **OK**.

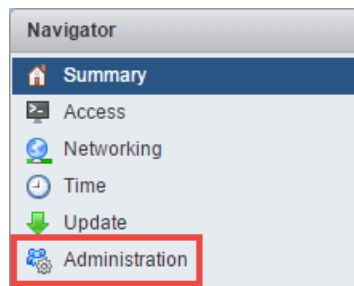
## 9.4.2 Modifying the root Password Policy

In this section, you will be modifying the password policy for root configuration.

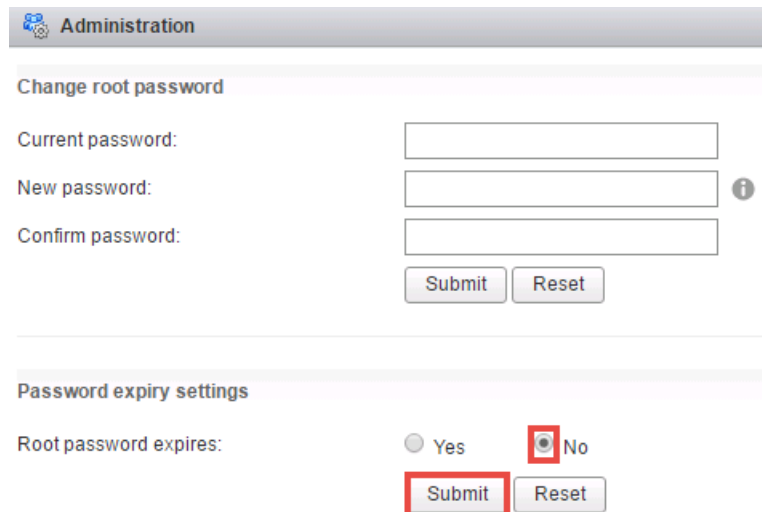


The following steps will not work on *VMware vCenter Server 6.0.0* running without the *U1* build. Refer to the [VMware Knowledge Base article](#).

1. Using the *vSphere Client*, navigate to `https://your_vcenter_ip:5480`.
2. Login with `root` as the *username* and its corresponding password, which was configured when *vCenter* was first deployed.
3. In the *Navigator* pane located to the left, click on **Administration**.



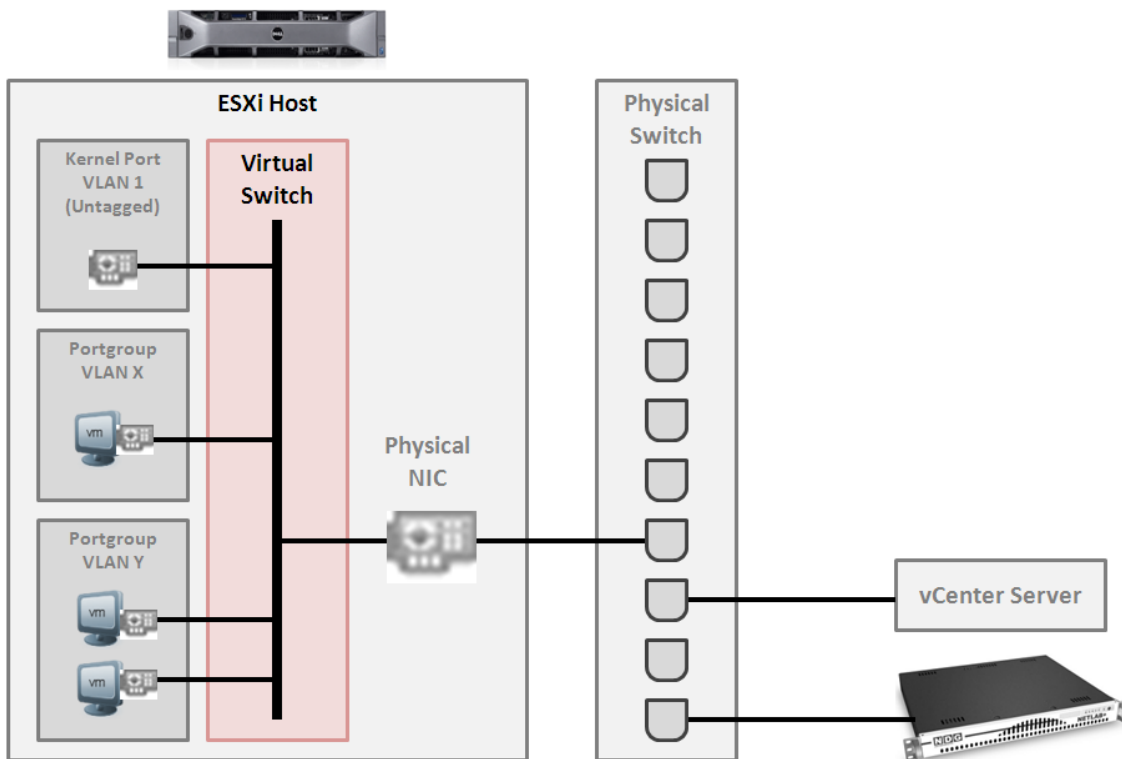
4. Notice by default, the root password is set to expire in 365 days. Select the radio button for **No** next to *Root password expires* and click **Submit**.



5. Logout of the *vSphere Client* as *root* and close the tab.

## 10 vSwitch Configuration

This section is designed to configure the vSwitches on the ESXi Host Servers. To review, a virtual switch (vSwitch) on the physical ESXi host bridges between physical networks, virtual machines, and the ESXi host kernel. Each vSwitch is an internal LAN, implemented entirely in software by the ESXi kernel.



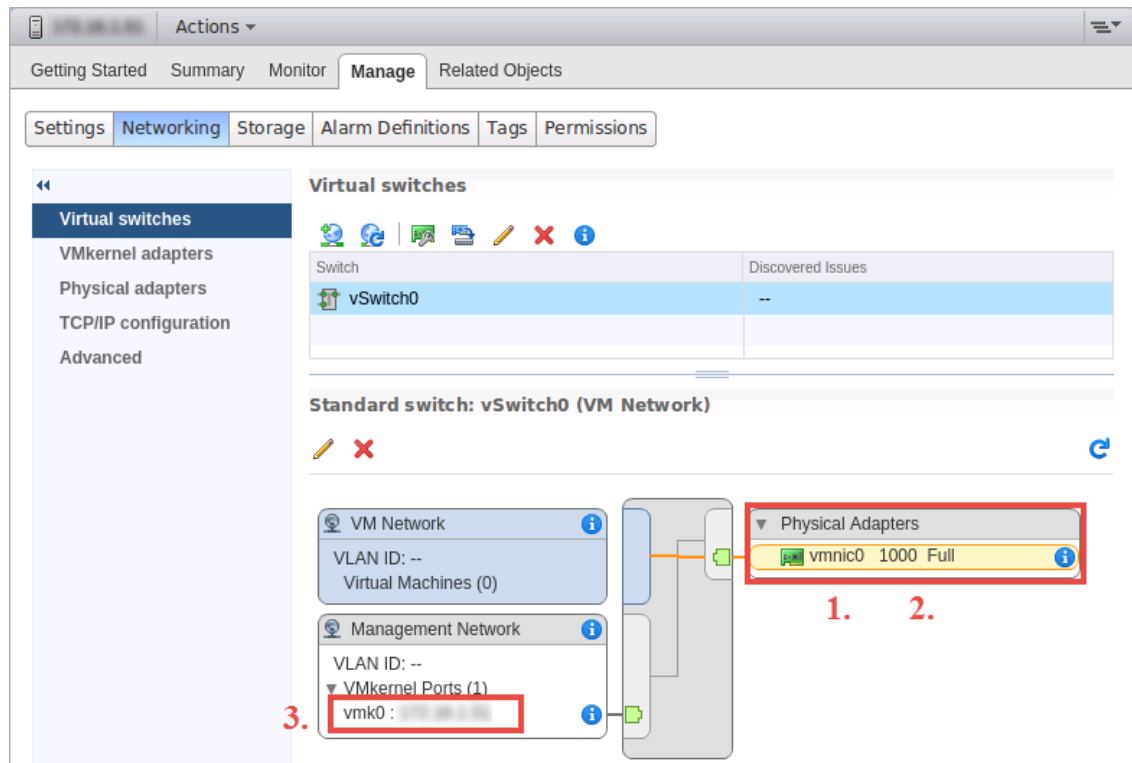
Your ESXi host(s) may connect to the outside network, inside network, or both depending on the network model you are using. The following table indicates which virtual switches are used for outside and inside connections.

Network Model	OUTSIDE vSwitch	INSIDE vSwitch
Single-Homed	vSwitch0	---
Dual-Homed	vSwitch0	vSwitch1

## 10.1 Verifying vSwitch0 Configuration

vSwitch0 is automatically created during the ESXi software installation (section 5.2). Using the *vSphere Client*, confirm that networking on vSwitch0 is properly configured (refer to the red numbered items in the screen below):

1. vSwitch0 is bound to the correct physical NIC (vmnic).
2. The physical NIC is connected and with correct speed/duplex.
3. The VMkernel port has the IP address you assigned when configuring your ESXi host. The IP address should be a campus LAN address.



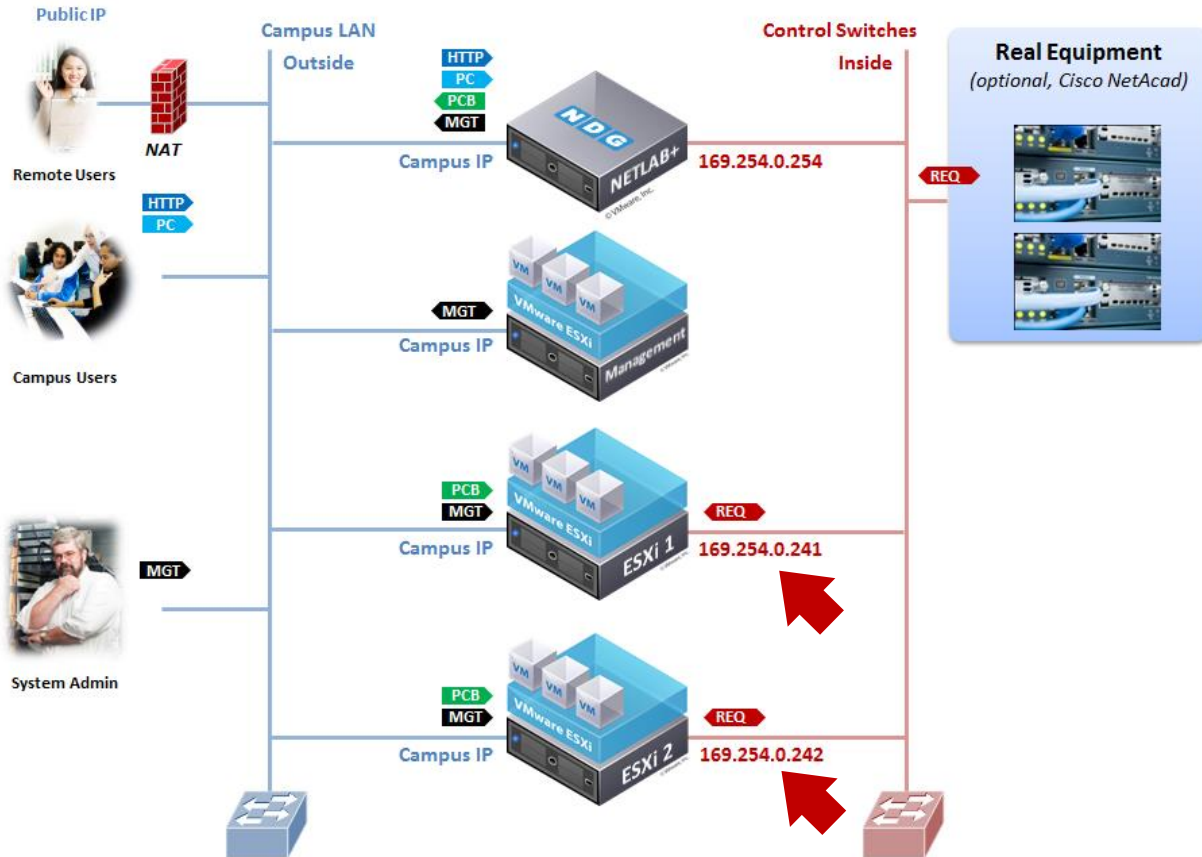
## 10.2 Inside Network Configuration

In this section, you will perform the final setup of the ESXi host inside networking. This section only applies to the dual-homed networking configuration that connects the ESXi host(s) to the inside network (see table below). This section describes various ESXi host networking components. We recommend reviewing this section even if inside networking is not used in your ESXi host configuration.

Networking Configuration	Inside Networking
Single-Homed Networking	No
Dual-Homed Networking	Yes

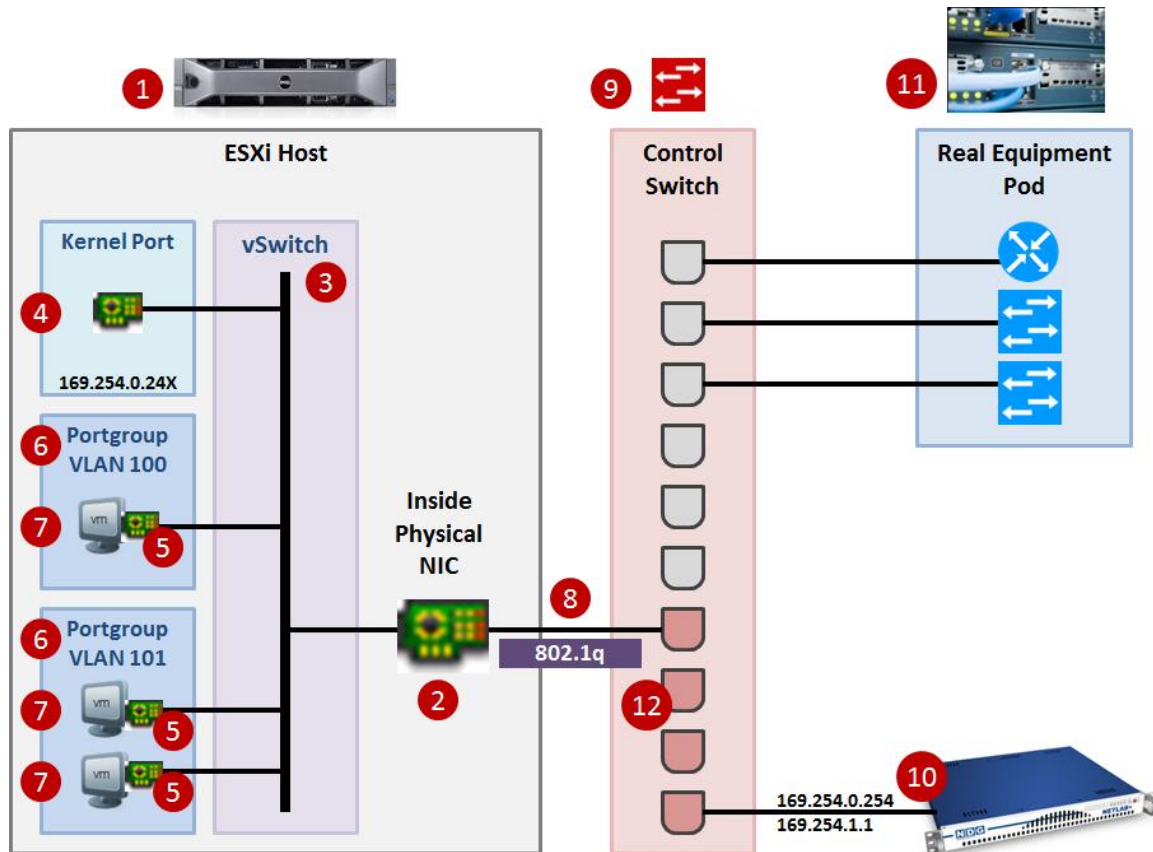


Repeat the setup tasks in this section for each ESXi host in your Virtual Machine Infrastructure.



There is only one type of network traffic can flow across the ESXi inside network connection, remote PC traffic between virtual machines and real equipment (VLANs 100 - 899).

The following diagram and table describe the various components of inside networking.



#	Component	Description
1	ESXi Host	The physical server where your virtual machines run.
2	Inside Physical NIC	The physical network interface on the ESXi Host (1) that connects virtual machines to the inside physical network.
3	vSwitch	A virtual switch on the physical ESXi host that bridges between physical networks (2,8,9), virtual machines (7), and the ESXi host kernel (4). Each vSwitch is an internal LAN, implemented entirely in software by the ESXi kernel.
4	Kernel Port	A virtual network interface on the ESXi host (1) that provides connectivity between the ESXi host kernel and other components such as NETLAB+.
5	Virtual Network Adapter (vNIC)	A virtualized networking adapter inside of a virtual machine that connects the virtual machine to a virtual switch.
6	Port Groups	A template for creating virtual network switch ports with a particular set of specifications. A port group allows a virtual network adapter (5) to be placed in a particular virtual LAN (VLAN). Port groups with specific VLAN IDs to connect virtual machines to real equipment.

7	Virtual Machines	In NETLAB+, a <i>virtual machine</i> is a remote PC or remote server that runs on virtualized hardware. Although the hardware is virtualized, real operating systems and real application software can still be used.
8	Uplink / Trunk	An uplink is a physical connection between ESXi Host (1,2) and a NETLAB+ control switch (9). If you are interfacing with real equipment pods (i.e., Cisco Networking Academy), your ESXi inside physical interface and the control switch port to which it is connected are configured in 802.1q trunk mode. Trunks allow multiple virtual LANs (VLANs) to exist on a single physical connection. VLAN assignments and the VLAN database on the control switch are managed by NETLAB+.
9	Control Switch	<p>A NETLAB+ control switch provides connectivity between the NETLAB+ server, ESXi host servers, asynchronous access servers, and switched outlet devices. Control switches are not accessed by lab users. There are three types of ports: reserved, assigned, and unassigned.</p> <p>An NDG supported control switch is required. See the NDG website for a list of supported control switches.</p>
10	NETLAB+ Inside Connection	<p>The NETLAB+ server inside interface connects to a designated reserved port on a control switch (9). The fixed addresses 169.254.0.254/24 and 169.254.1.1/24 are assigned to the inside interface (these cannot be changed).</p> <p>802.1q trunk mode should NOT be enabled on the control switch port for this connection.</p>
11	Real Equipment Pods	Real lab equipment (optional) is connected to one or more control switches (9).
12	Reserved Ports	Reserved ports are ports on a control switch (9) that are reserved to provide connectivity between the NETLAB+ server, ESXi host servers, asynchronous access servers, and switched outlet devices.

The following table summarizes the traffic types that will flow over the ESXi inside network.

Networking Configuration	Management Traffic (VLAN 1)	Remote Display (VLAN 1)	802.1q Trunk
Single-Homed Networking	n/a	n/a	n/a
Dual-Homed Networking	No	No	Real Gear*

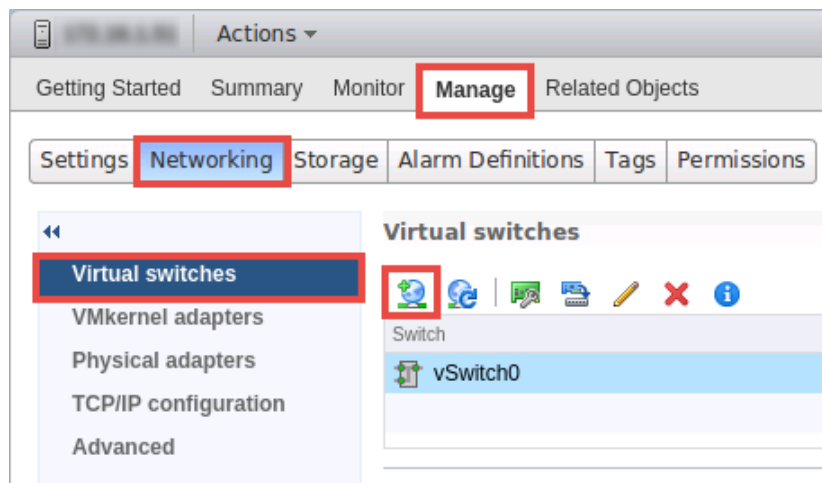
\* ESXi interface and corresponding control port is configured as 802.1q trunk when interfacing with real equipment.



## 10.3 Creating vSwitch1 and Binding to Physical NIC

If your ESXi host is dual-homed (connected to both outside and inside networks), you must create an inside virtual switch (vSwitch 1), bind a physical NIC to vSwitch1, and create a VMkernel port for management traffic. These tasks are performed through vCenter.

1. Log in to vCenter using the vSphere Web Client.
2. Navigate to **Home > Inventories > Hosts and Clusters**.
3. Click on the ESXi host to configure in the left sidebar.
4. Click on the **Manage**.
5. Click on **Networking**.
6. Click on the **Virtual Switches** menu item if not already selected.
7. Click on the **Add host networking** icon.



8. In the *Add Networking* window, on the *Select connection type* page, add a *VMkernel Network Adapter* to allow the ESXi host kernel to communicate with the inside network. Select the **VMkernel Network Adapter** radio button, and then click **Next**.

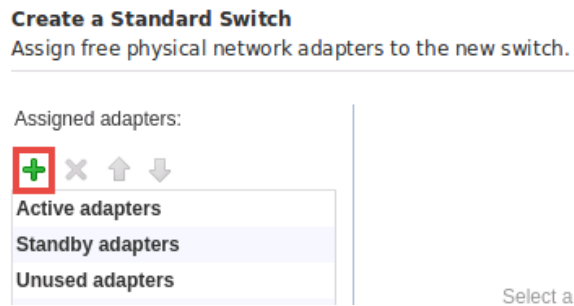
### Select connection type

Select a connection type to create.

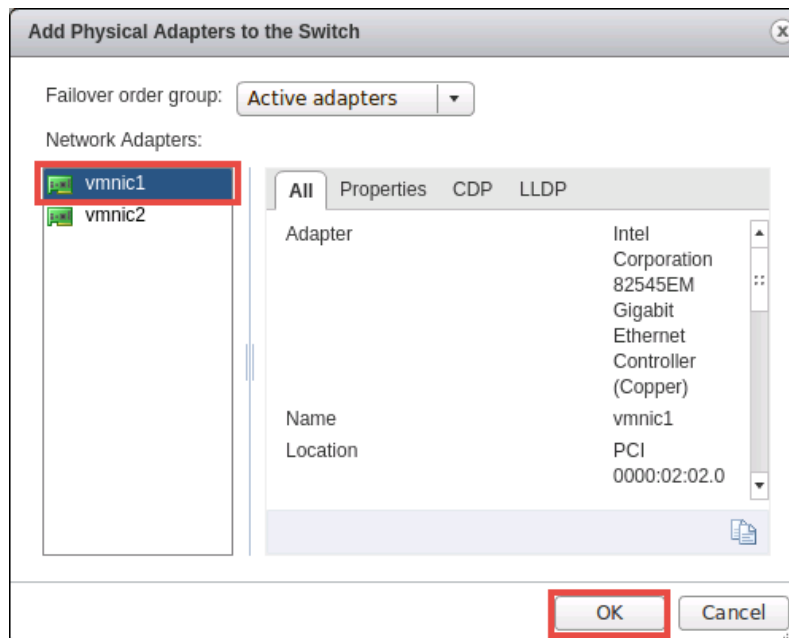
- ☒ **VMkernel Network Adapter**  
The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, Virtual SAN and host management.
- ☐ **Physical Network Adapter**  
A physical network adapter handles the network traffic to other hosts on the network.
- ☐ **Virtual Machine Port Group for a Standard Switch**  
A port group handles the virtual machine traffic on standard switch.

9. On the *Select target device* page, select the **New standard switch** radio button and click **Next**.

10. On the *Create a Standard Switch* page, click the **Add adapters** icon (green plus).



11. In the Add Physical Adapters to the Switch window, select the physical NIC that will connect vSwitch1 to the control switch. We recommend using vmnic1 for inside connections (vmnic0 should already be connected to the outside network). Click **OK**.



12. In the *Add Networking* window, on the *Create a Standard Switch*, review the configurations and click **Next**.
13. On the *Port Properties* page, enter the port group properties as shown above.
- Network label*: "**NETLAB Inside**"
  - VLAN ID*: **None(0)** (default)
  - Check option **Management traffic**
14. Click **Next**.

15. On the IPv4 settings page, enter a unique inside IP address and subnet mask from the following table.

Inside Interface	IP Address	Subnet Mask
ESXi Server 1 Inside	169.254.0.241	255.255.255.0
ESXi Server 2 Inside	169.254.0.242	255.255.255.0
ESXi Server 3 Inside	169.254.0.243	255.255.255.0
ESXi Server 4 Inside	169.254.0.244	255.255.255.0
ESXi Server 5 Inside	169.254.0.245	255.255.255.0
ESXi Server 6 Inside	169.254.0.246	255.255.255.0
ESXi Server 7 Inside	169.254.0.247	255.255.255.0
ESXi Server 8 Inside	169.254.0.248	255.255.255.0
ESXi Server 9 Inside	169.254.0.249	255.255.255.0

#### IPv4 settings

Specify VMkernel IPv4 settings.

- ☐ Obtain IPv4 settings automatically
- ☒ Use static IPv4 settings

IPv4 address: 169 . 254 . 0 . .241 to .249

Subnet mask: 255 . 255 . 255 . 0

Default gateway for IPv4: 172.16.1.1

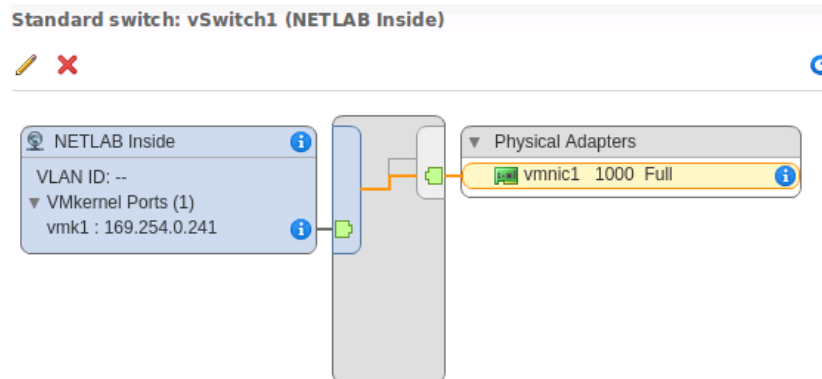
DNS server addresses: 172.16.1.1



No changes to the VMkernel Default Gateway setting should be necessary. This should already be set to the default gateway on your campus LAN.

16. Click **Next** to continue.
17. On the *Ready to complete* page, review the information and click **Finish**.

18. Confirm that vSwitch1 appears as follows (IP varies for each host).
  - a. VMkernel port (vmk1) has the correct IP address.
  - b. vSwitch1 is bound to the physical adapter (vmnic1)
  - c. The physical adapter is up (speed and duplex are detected)



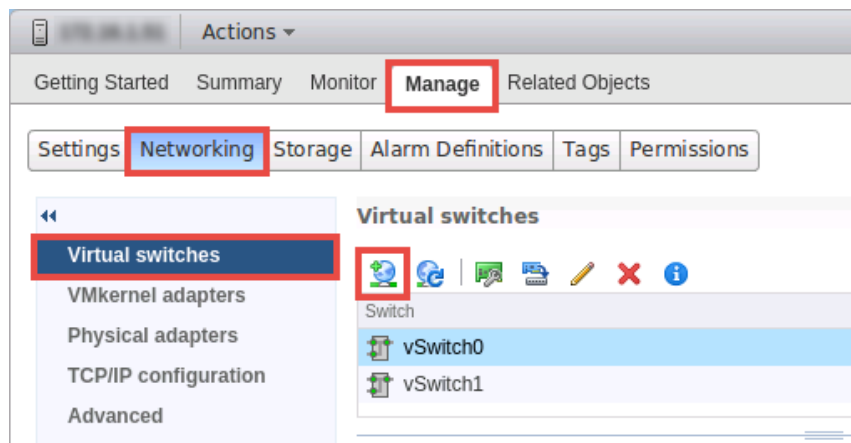
A **✗** mark displayed near the Physical Adapter indicates that the connection has not yet been physically cabled or the corresponding control switch port is shut down.

## 10.4 Create a Safe Staging Network

In this section, you will be creating a Safe Staging Network called “Safety Net,” to connect our VMs temporarily. The Safe Staging Network consists of a virtual switch and a port group that is not connected to any other networks (virtual or real). Should the virtual machine be powered on, its traffic will be confined to the safety net. This ensures that the virtual machine will not pose a security risk to your campus LAN or interfere with other pods until it is relocated to its final network via automatic or manual networking.

1. Using the vSphere Web Client, navigate to **Hosts and Clusters**.
2. Select your first ESXi host in the **Inventory** pane on the left.
3. Click on the **Manage** tab.
4. Click on **Networking**.

5. With **Virtual switches** selected, click on the **Add host networking** icon to create a new virtual switch.



6. In the *Add Networking* window, on the *Select connection type* page, select the radio button for **Virtual Machine Port Group for a Standard Switch** and click **Next**.

#### Select connection type

Select a connection type to create.

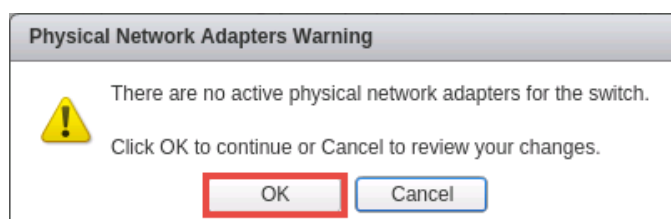
- ☐ **VMkernel Network Adapter**  
The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, Virtual SAN and host management.
- ☐ **Physical Network Adapter**  
A physical network adapter handles the network traffic to other hosts on the network.
- ☒ **Virtual Machine Port Group for a Standard Switch**  
A port group handles the virtual machine traffic on standard switch.

7. On the *Select target device* page, select **New standard switch** and click **Next**.
8. On the *Create a Standard Switch* page, make sure no adapters appear and click **Next**.



**UNCHECK** any vmnics under *Assigned adapters*; this virtual switch should not be bound to any real network adapters on the ESXi host.

9. When prompted that no active physical network adapters are present, click **OK** to continue.



10. On the *Connection settings* page, enter **SAFETY NET** in the Port Group's **Network label** property and then click **Next**.

#### Connection settings

Use network labels to identify migration-compatible connections common to two or more hosts.

Network label:	<input type="text" value="SAFETY NET"/>
VLAN ID (Optional):	<input type="text" value="None (0)"/>

11. On the *Ready to complete* page, review the information and click **Finish**.
12. Repeat Steps 1-11 for each ESXi host server.

SAFETY NET is now available for use as a safe temporary network location for new virtual machines.



The safety network is an ideal place to bind the network interface(s) of master virtual machines. Automatic networking will bind network interfaces of cloned VMs to their runtime networks when their respective pods are started.