UQ Cyber
19 November 2020

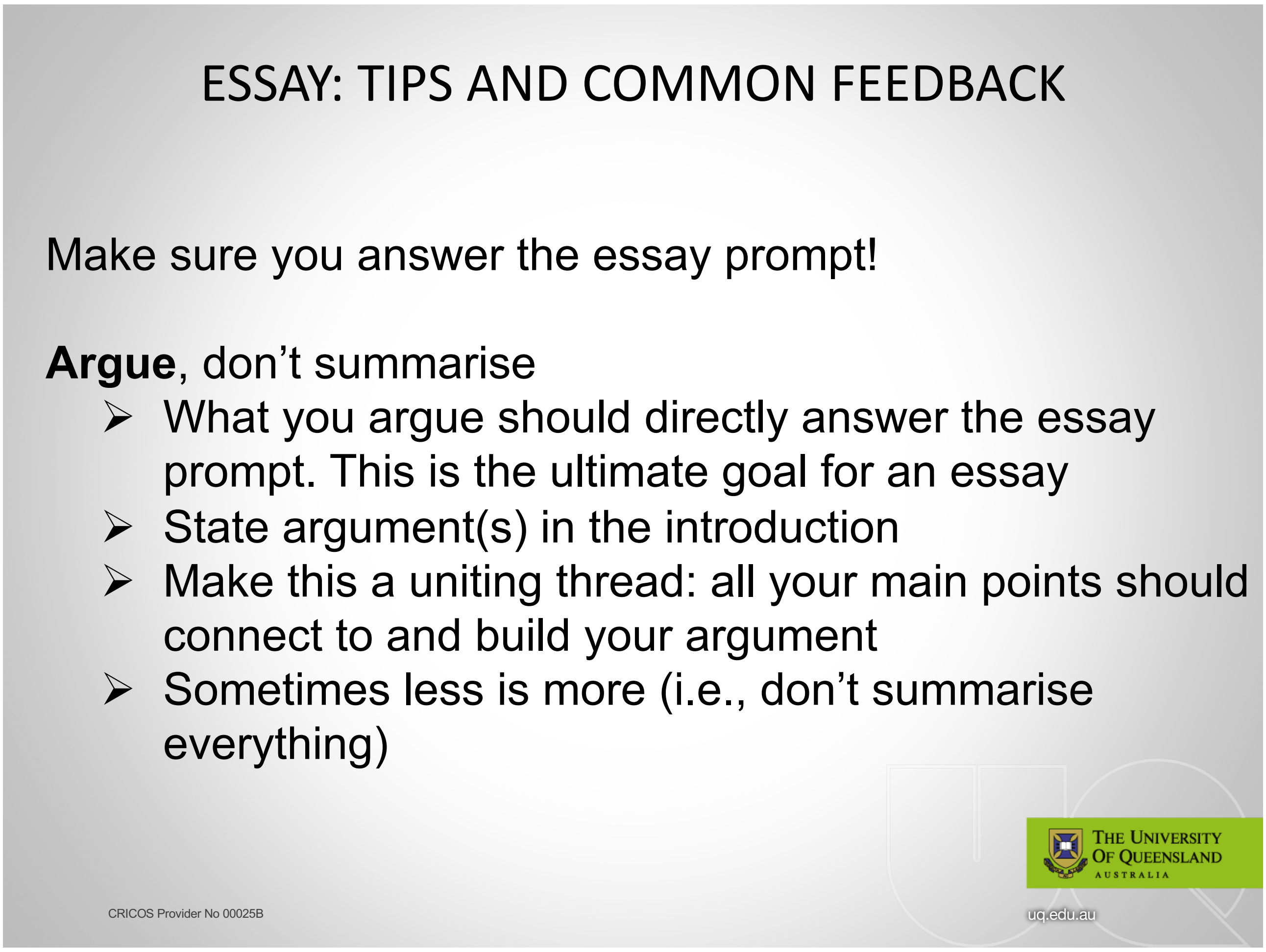
THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Master of Cyber Security Self-Study Resource List Appendix

Contents

Appendix 1

Writing Tips – Jonah Rimer



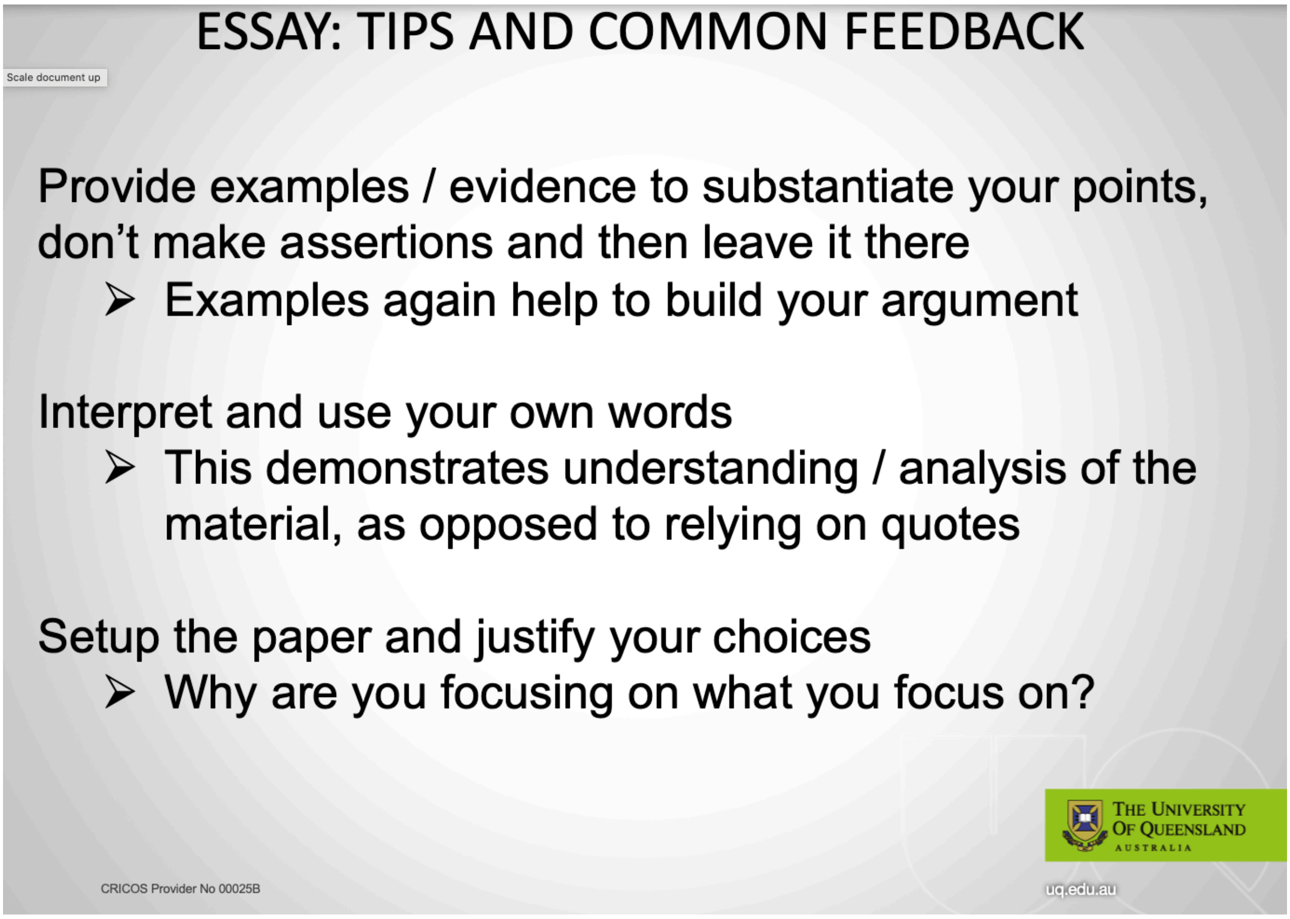
ESSAY: TIPS AND COMMON FEEDBACK

Make sure you answer the essay prompt!

Argue, don't summarise

- What you argue should directly answer the essay prompt. This is the ultimate goal for an essay
- State argument(s) in the introduction
- Make this a uniting thread: all your main points should connect to and build your argument
- Sometimes less is more (i.e., don't summarise everything)

CRICOS Provider No 00025B



ESSAY: TIPS AND COMMON FEEDBACK

Provide examples / evidence to substantiate your points, don't make assertions and then leave it there

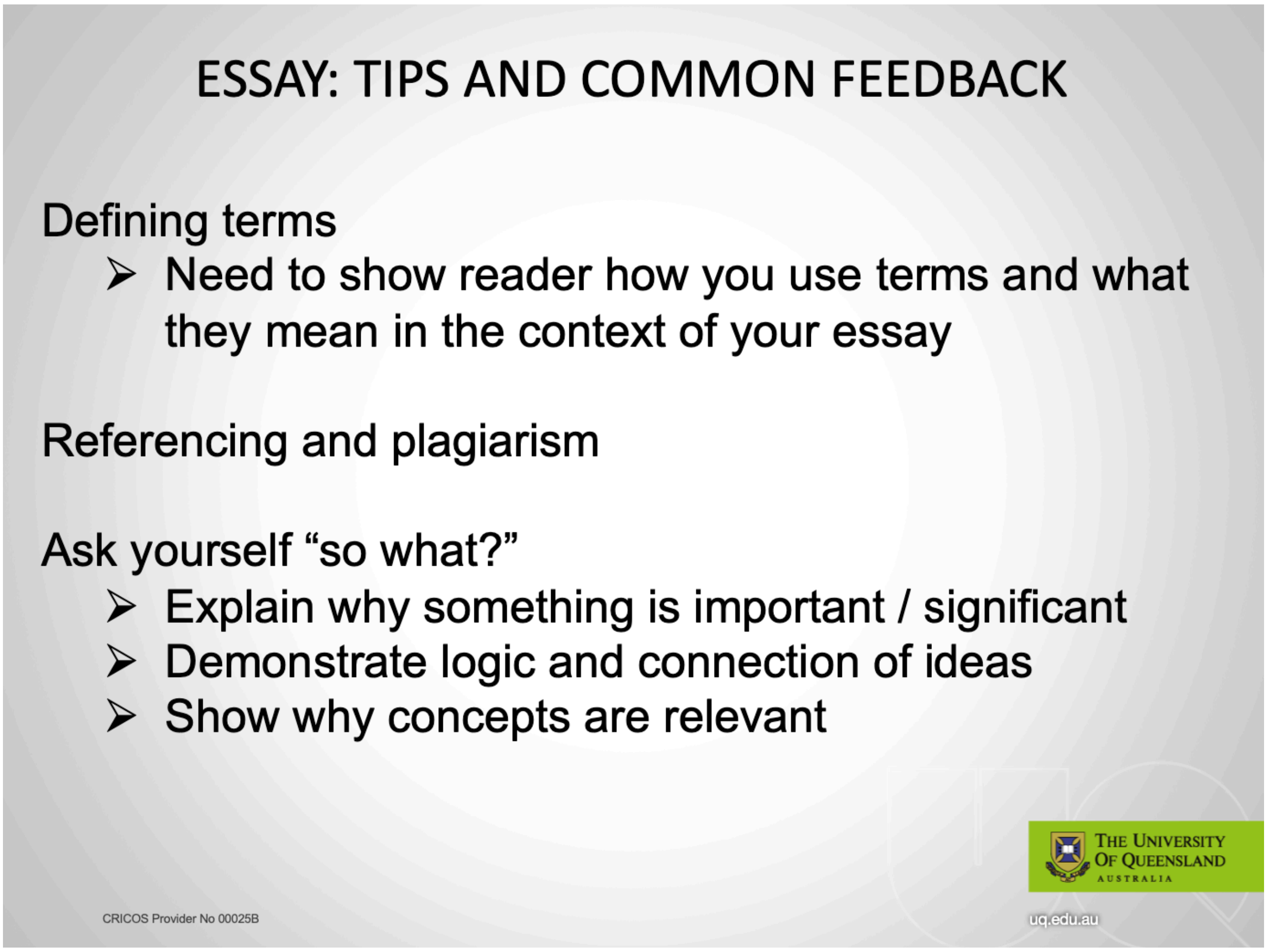
- Examples again help to build your argument

Interpret and use your own words

- This demonstrates understanding / analysis of the material, as opposed to relying on quotes

Setup the paper and justify your choices

- Why are you focusing on what you focus on?



ESSAY: TIPS AND COMMON FEEDBACK

Defining terms

- Need to show reader how you use terms and what they mean in the context of your essay

Referencing and plagiarism

Ask yourself “so what?”

- Explain why something is important / significant
- Demonstrate logic and connection of ideas
- Show why concepts are relevant

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CRICOS Provider No 00025B
uq.edu.au

Appendix 2

9.0.1_VMware_Workstation_Pod_Setup

Palo Alto Networks

VMware Workstation 9.0 Academy Labs

Document Version: 2019-07-04

Table of Contents:

Overview:

The purpose of this guide is to provide setup instructions to deploy the 9.0.1 virtual firewall appliance lab pod on VMware Workstation. The 9.0.1 VMware Workstation firewall appliance lab pod is almost identical to the 8.0 VMware Workstation firewall appliance lab pod.

The 9.0.1 lab pod consists of 4 virtual machines: Centos Linux virtual router, Windows Server 2016 client, Centos DMZ and a 9.0.1 VM-50 virtual firewall appliance. We are providing ova's for you to download for all the virtual machines except for the Windows Server 2016 client.

We are no longer providing the Windows/Server client ova for the 9.0.1 VMware Workstation lab pod as we did for the 8.0 VMware Workstation lab pod. Instead, academies will either have to configure a Windows Server 2016 Client using a Microsoft base image and the setup instructions in this guide or continue to use 8.0 Windows Server 2012 client in their new 9.0.1 VMware Workstation lab pod if they have already downloaded/used the Windows Server 2012 client.

In summary, academies have the following VMware Workstation use options for supporting all 8.0 and 9.0 CIC and CPC Moodle courses:

1. If an academy has already deployed and is using the 8.0 VMware workstation lab pod, they may continue to use this pod for the above courses.
2. If an academy is new to the program or has not previously downloaded and used the ovas in the 8.0 VMware Workstation lab pod then the academy will have to follow this guide and to deploy and configure a 9.0.1 VMware lab pod pod.
3. If an academy has been using the 8.0 VMware Workstation lab pod and wants to upgrade to the 9.0.1 lab, the academy may continue to use the Windows Server 2012 lab along with the new 9.0 virtual machines instead of following the instructions in this guide to configure and deploy a new Windows Server 2016 client.

It is important to follow the steps as is so that your students will not experience any issues during their learning experience.

All steps in this document were created and verified using:

Product: VMware Workstation 15 Pro

Version: 15.1.0 build-13591040

Note: Most VMware workstations are backward compatible. As in, newer versions will take older virtual machines, but older VMware workstations will not take the VMs created in newer versions of VMware.

Downloads, Licensing and Resources:

You will need to provide your own licensing for both VMware workstation and Server 2012 / 2016 operations systems.

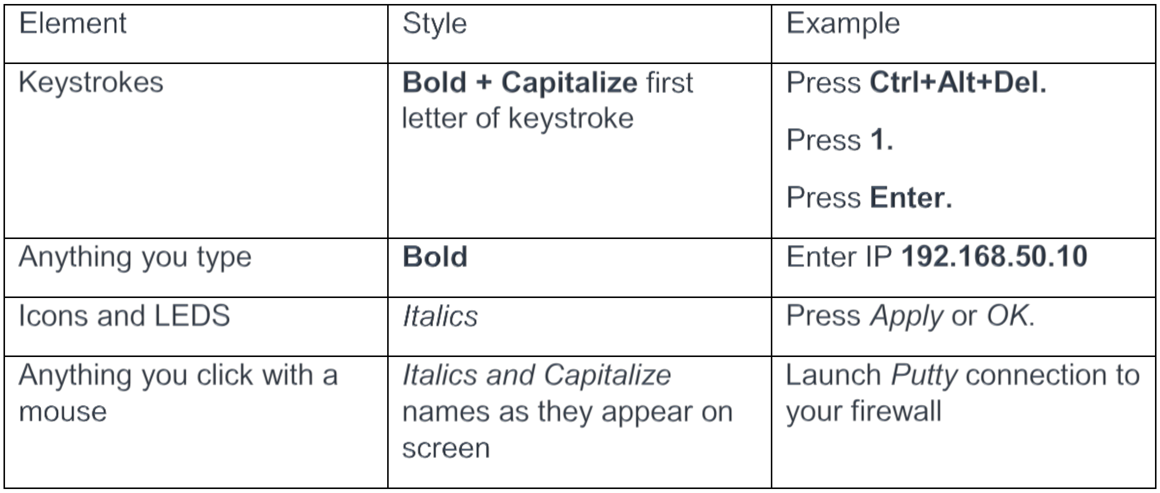
The following links will direct you to VMWare and Microsoft.

The first link directs you to VMWare's Academic Subscription Site.

The other links map to VMWare Standard License product downloads and resources. VMware workstation Pro is available as a free 30-day trial. You do not need to create a VMWare account to download the free trial.

- https://labs.vmware.com/academic/licensing-overview
- https://vmapss.onthehub.com/WebStore/Welcome.aspx
- https://docs.vmware.com/en/VMware-Workstation-Pro/index.html
- https://www.vmware.com/products/workstation-pro.html
- https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation_pro/15_0
- https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html
- https://docs.vmware.com/en/VMware-Workstation-Pro/15/rn/VMware-Workstation-151-Pro-Release-Notes.html
- https://www.microsoft.com/en-us/education/itdm/setup-management/default.aspx?&OCID=AID2000043_SEM_7OfoGTMi&utm_source=google&gclid=EAIaIQobChMI8Ovxzd_f4wIVIB6tBh3OrA01EAAYASAAEgJpfPD_BwE

Style Reference Table:



Element	Style	Example
Keystrokes	**Bold + Capitalize** first letter of keystroke	Press **Ctrl+Alt+Del.** Press **1.** Press **Enter.**
Anything you type	**Bold**	Enter IP **192.168.50.10**
Icons and LEDS	*Italics*	Press *Apply* or *OK.*
Anything you click with a mouse	*Italics and Capitalize* names as they appear on screen	Launch *Putty* connection to your firewall

Lab Scenario:

All the virtual machines for this VMware Workstation lab pod are preconfigured with IP addresses that match the subnets for the VMnets outlined in this document. If you want to change your Workstation VMnet subnets, then you will have to change the IP addresses of the virtual machines in this lab pod to correspond with your changed subnet network IDs.

Note: Once this lab is complete it will support the following Cybersecurity Academy Moodle Courses when doing the labs through VMware workstation: Cybersecurity Infrastructure Configuration course, Cybersecurity Prevention and Countermeasures course, Firewall Essentials Configuration and Management course and the Optimizing Firewall Threat Prevention course.

In this lab, you will:

1. Configure your host computer's VMware Workstation VMnets for your VM-50 lab pod.

2. Download and import the academy VM-50 workstation appliance Firewall ova that is pre-configured to operate on the Workstation VMnets.

3. Import the workstation-DMZ ova into your host computer's VMware Workstation application and assign the client's network adapter to the correct VMnet.

4. Import the workstation-VR ova into your host computer's VMware Workstation application and assign the client's network adapters to the correct VMnets.

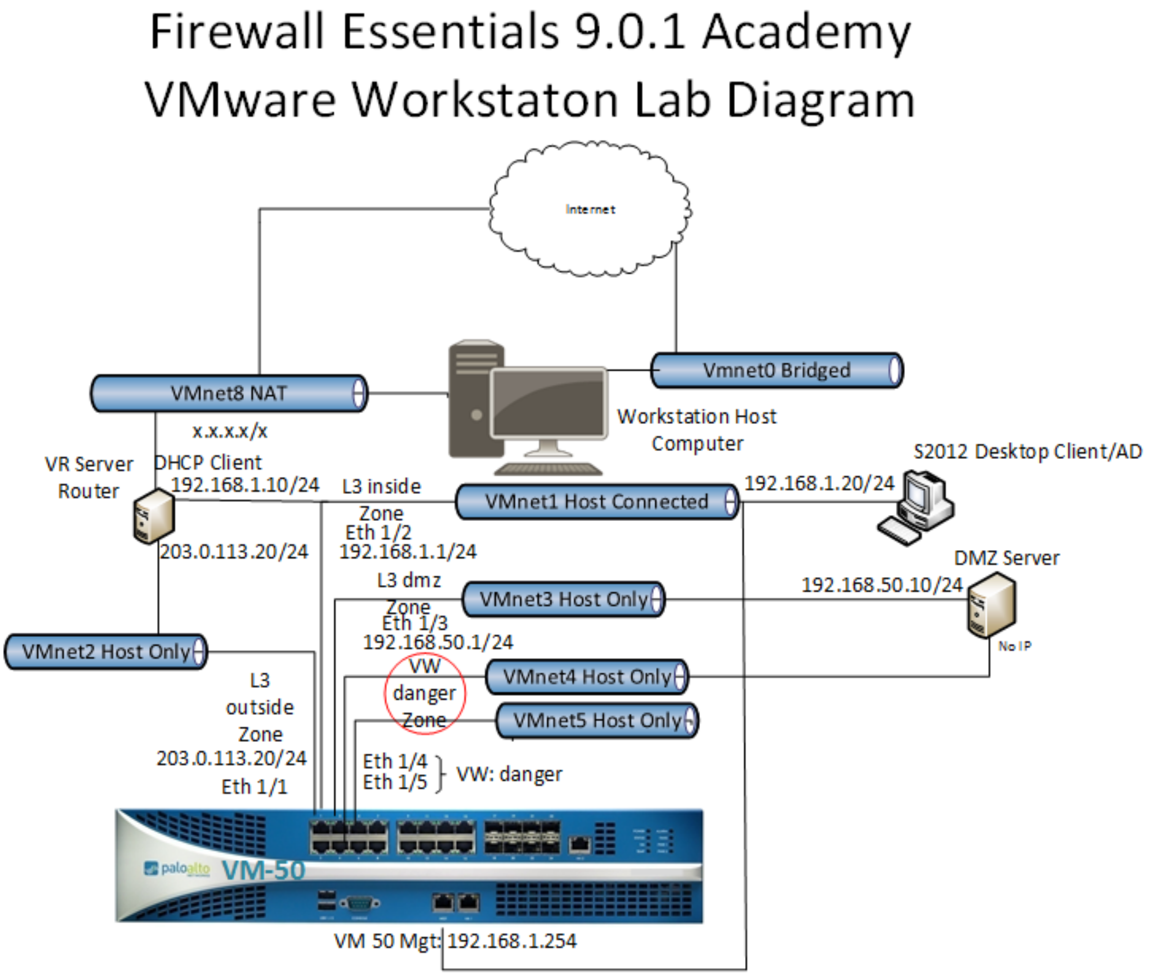
5. Configure your Windows Client/Server 2016 virtual machine.

6. License your VM-50 workstation appliance with provided AUTH code, check to insure your firewall correctly installs the licenses on your appliance and perform dynamic updates.

Note: When doing labs on VMware workstation lab pods it is important to load the correct named configuration snapshot. This will be outlined in each of the lab documents for the respective course that you will complete.

Configuration Diagram with Usernames and Passwords

The information in the diagram and table below contains information you will need to complete this lab.



Virtual Machine	Username	Password
VM-50 Academy Appliance	admin	admin
Server 2012	lab-user	Pal0Alt0
Centos AAC DMZ	root	Pal0Alt0
Centos Virtual Router	root	Pal0Alt0

Lab Solution:

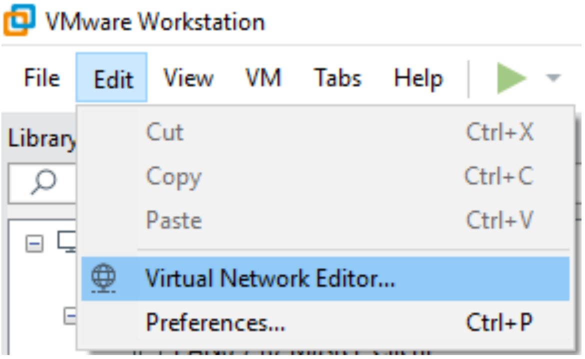
Windows VMware Workstation Setup Instructions for Palo Alto Networks 9.0 Pod

1 Configure your host computer's VMware Workstation VMnets for your VM-50 lab pod.

Before you begin installing your virtual machines you will need to create the necessary virtual network.

1.1 Open VMware Workstation and access the Virtual Network Editor by navigating to:

Edit > Virtual Network Editor.

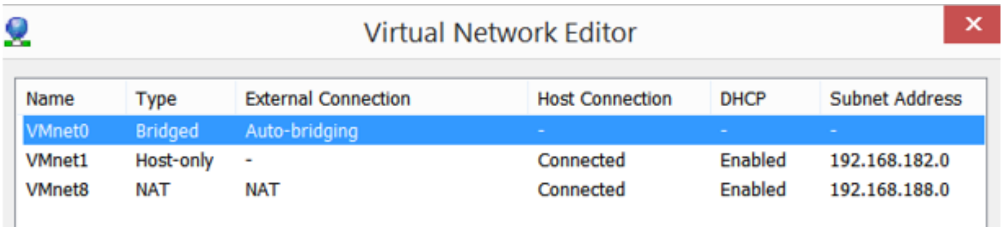


Note: You may need administrator privileges here to make a change. To do this please select the *Change Settings* button.

1.2 Your lab environment will need 7 Virtual Networks. Two of them, VMNet0 and VMNet8 will be built by default. You may also have a third adapter, VMNet1 that you will customize. If your network settings do not display VMNet1 its ok, you will create it when you create the other adapters.

VMNet0 – Type: Bridged. Used to connect to the local host

VMNet8 – Type: NAT. Used to assign DHCP addresses to the VMS



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.182.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.188.0

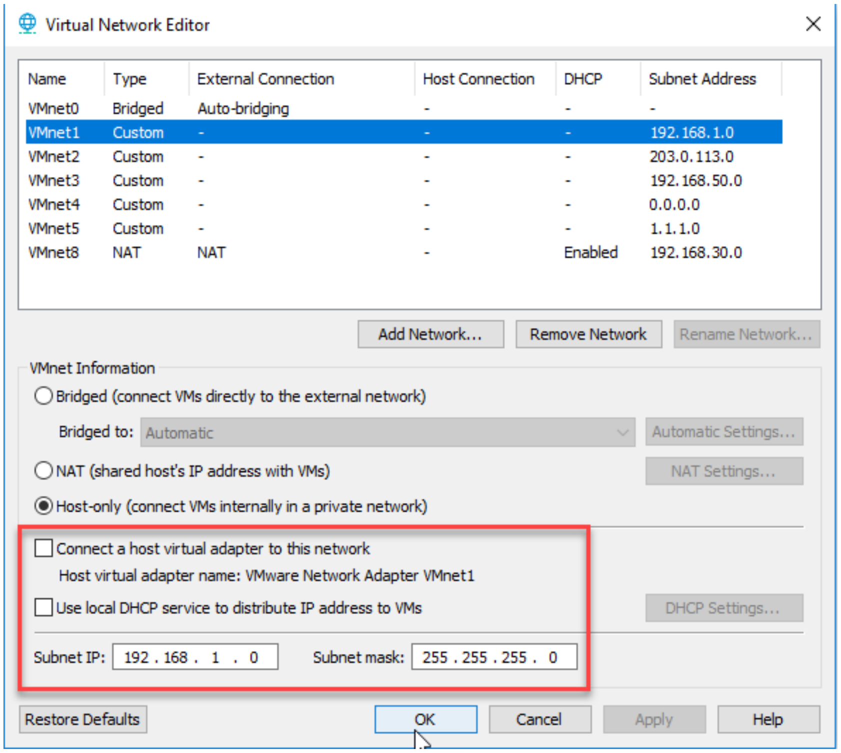
Possibly you may also see: VMNet1 – Type: Host-only.

** If it appears you will customize this adapter as directed in the following slides. If it doesn't appear you will create it in the following slides.

1.3 In the Virtual Network Editor dialog box, select to highlight "*VMnet1*" and under "VMnet Information" do the following:

1.3.1 Select the radial button, "*Host-only*" (connect VMs internally in a private network).

1.3.2 Set the "Subnet IP" to **192.168.1.0** and the "Subnet mask" to **255.255.255.0**



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Custom	-	-	-	192.168.1.0
VMnet2	Custom	-	-	-	203.0.113.0
VMnet3	Custom	-	-	-	192.168.50.0
VMnet4	Custom	-	-	-	0.0.0.0
VMnet5	Custom	-	-	-	1.1.1.0
VMnet8	NAT	NAT	-	Enabled	192.168.30.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

● Host-only (connect VMs internally in a private network)

□ Connect a host virtual adapter to this network

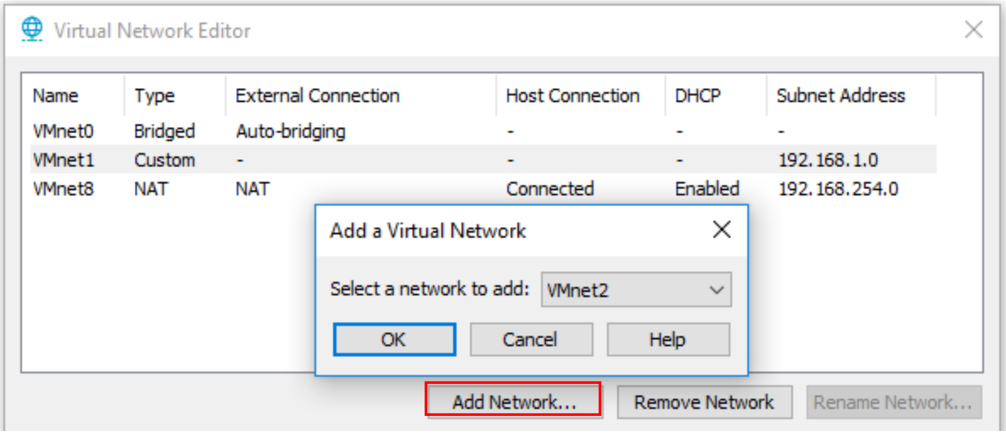
Host virtual adapter name: VMware Network Adapter VMnet1

□ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 . 168 . 1 . 0 Subnet mask: 255 . 255 . 255 . 0

1.3.3 Click *Apply*.

1.4 In the “Virtual Network Editor” dialog box, select “*Add Network*” and then select *OK*.



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Custom	-	-	-	192.168.1.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.254.0

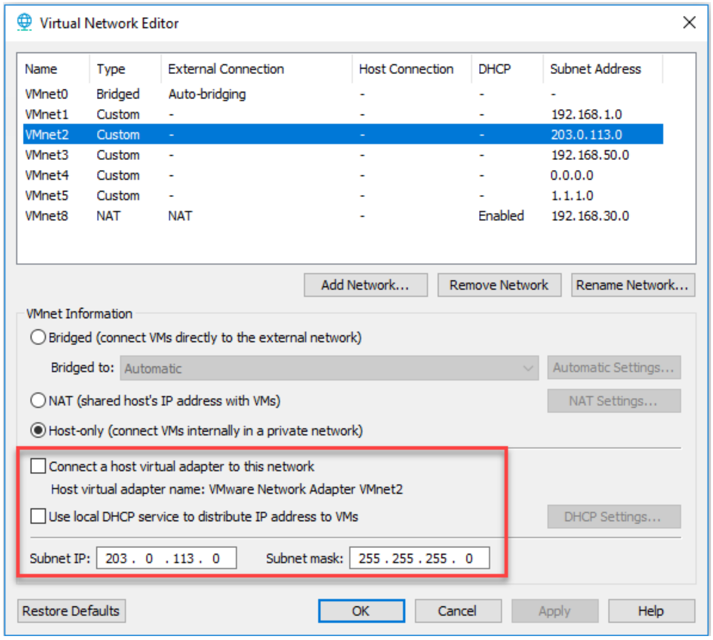
Add a Virtual Network

Select a network to add: VMnet2

1.4.1 In the “Virtual Network Editor” dialog box for VMnet2, *uncheck* the boxes next to “*Connect a host virtual adapter to this network*” and *uncheck* “*Use local DHCP service to distribute IP addresses to VMs”*.

For Subnet IP enter **203.0.113.0** and for Subnet Mask enter **255.255.255.0**

1.4.2 Click *Apply*.



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Custom	-	-	-	192.168.1.0
VMnet2	Custom	-	-	-	203.0.113.0
VMnet3	Custom	-	-	-	192.168.50.0
VMnet4	Custom	-	-	-	0.0.0.0
VMnet5	Custom	-	-	-	1.1.1.0
VMnet8	NAT	NAT	-	Enabled	192.168.30.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

● Host-only (connect VMs internally in a private network)

□ Connect a host virtual adapter to this network

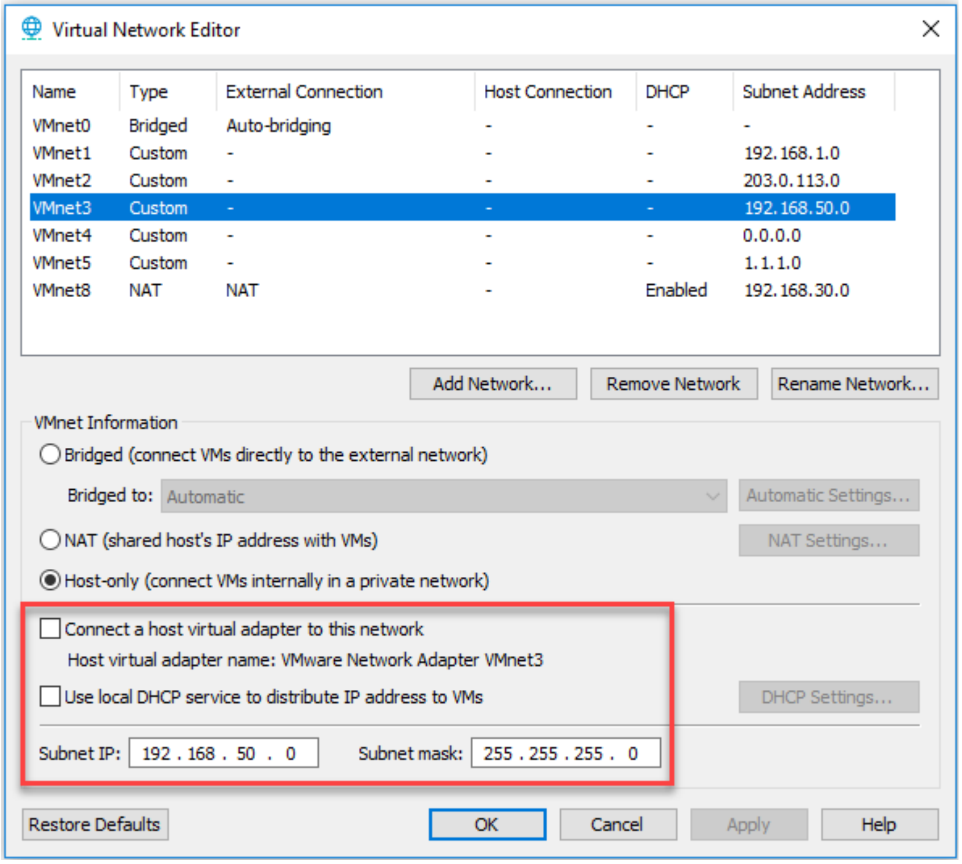
Host virtual adapter name: VMware Network Adapter VMnet2

□ Use local DHCP service to distribute IP address to VMs

Subnet IP: 203 . 0 . 113 . 0 Subnet mask: 255 . 255 . 255 . 0

1.5 In the "Virtual Network Editor" dialog box, select "*Add Network*".

1.5.1 In the "Virtual Network Editor" dialog box for VMnet3, *uncheck* the boxes next to "*Connect a host virtual adapter to this network*" and *uncheck* "*Use local DHCP service to distribute IP addresses to VMs"*.



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Custom	-	-	-	192.168.1.0
VMnet2	Custom	-	-	-	203.0.113.0
VMnet3	Custom	-	-	-	192.168.50.0
VMnet4	Custom	-	-	-	0.0.0.0
VMnet5	Custom	-	-	-	1.1.1.0
VMnet8	NAT	NAT	-	Enabled	192.168.30.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

● Host-only (connect VMs internally in a private network)

□ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet3

□ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 . 168 . 50 . 0 Subnet mask: 255 . 255 . 255 . 0

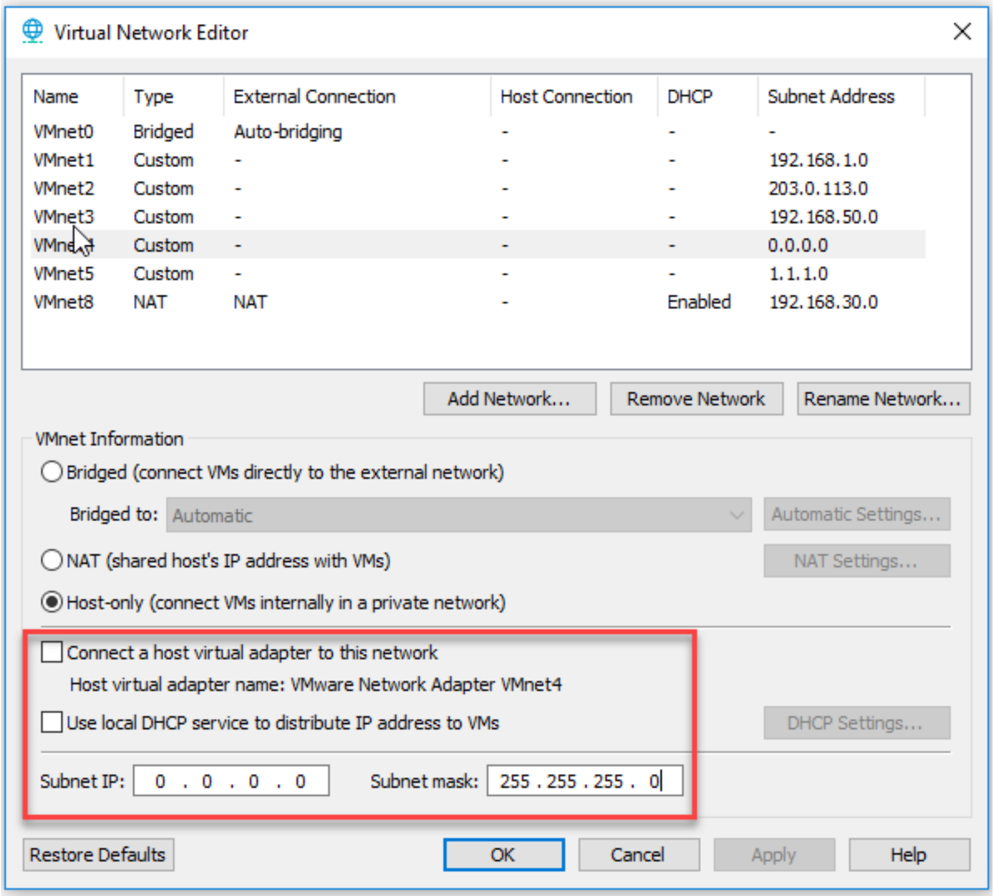
1.5.2 For Subnet IP enter **192.168.50.0** and for Subnet Mask enter ***255.255.255.0***

1.5.3 Click *Apply*.

1.6 In the "Virtual Network Editor" dialog box, select "*Add Network*"**.**

1.6.1 In the "Virtual Network Editor" dialog box for VMnet4, *uncheck* the boxes next to "*Connect a host virtual adapter to this network*" and *uncheck* "*Use local DHCP service to distribute IP addresses to VMs*".

For Subnet IP enter **0.0.0.0** and for Subnet Mask enter **255.255.255.0** and



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Custom	-	-	-	192.168.1.0
VMnet2	Custom	-	-	-	203.0.113.0
VMnet3	Custom	-	-	-	192.168.50.0
VMnet4	Custom	-	-	-	0.0.0.0
VMnet5	Custom	-	-	-	1.1.1.0
VMnet8	NAT	NAT	-	Enabled	192.168.30.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

● Host-only (connect VMs internally in a private network)

□ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet4

□ Use local DHCP service to distribute IP address to VMs

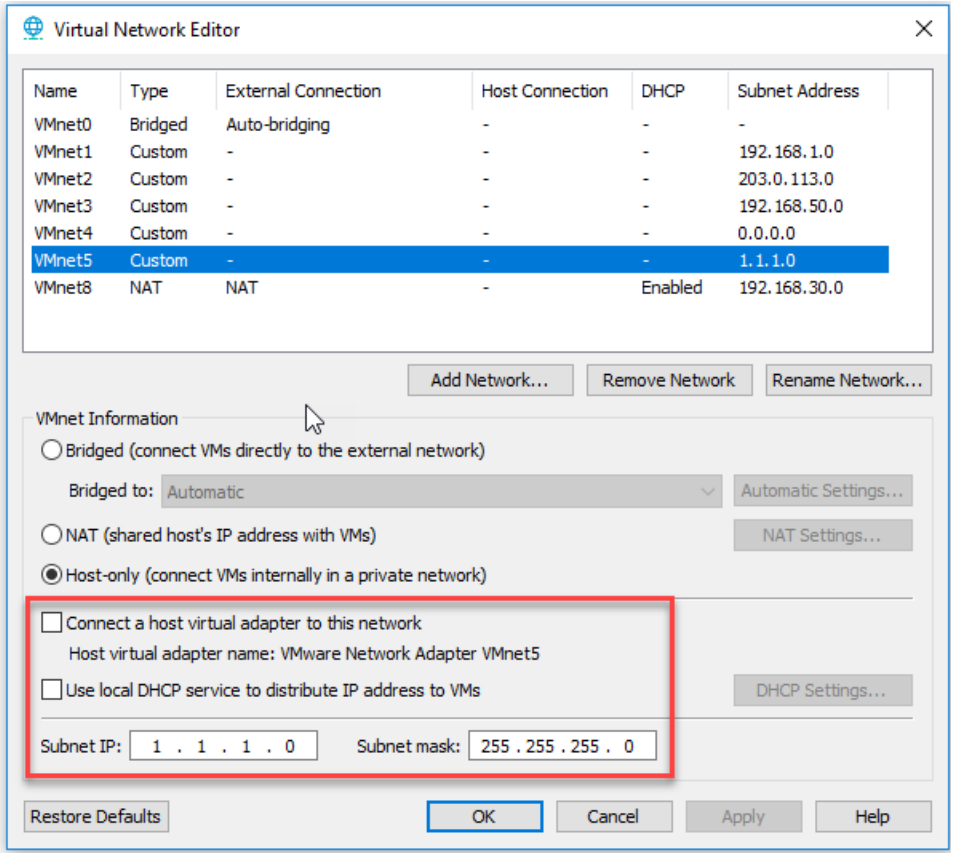
Subnet IP: 0 . 0 . 0 . 0   Subnet mask: 255 . 255 . 255 . 0

1.6.2 Click *Apply.*

1.7 In the "Virtual Network Editor" dialog box, select "*Add Network*".

1.7.1 In the "Virtual Network Editor" dialog box for VMnet5, *uncheck* the boxes next to "*Connect a host virtual adapter to this network*" and *uncheck* "*Use local DHCP service to distribute IP addresses to VMs*".

1.7.2 For Subnet IP enter **1.1.1.0** and for Subnet Mask enter **255.255.255.0**.



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Custom	-	-	-	192.168.1.0
VMnet2	Custom	-	-	-	203.0.113.0
VMnet3	Custom	-	-	-	192.168.50.0
VMnet4	Custom	-	-	-	0.0.0.0
VMnet5	Custom	-	-	-	1.1.1.0
VMnet8	NAT	NAT	-	Enabled	192.168.30.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

● Host-only (connect VMs internally in a private network)

□ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet5

□ Use local DHCP service to distribute IP address to VMs

Subnet IP: 1 . 1 . 1 . 0 Subnet mask: 255 . 255 . 255 . 0

1.7.3 Click *Apply*.

1.8 In the “Virtual Network Editor” dialog box, select *VMnet 8*.

1.8.1 Select the radial button *NAT (Share host’s IP address with VMs)*

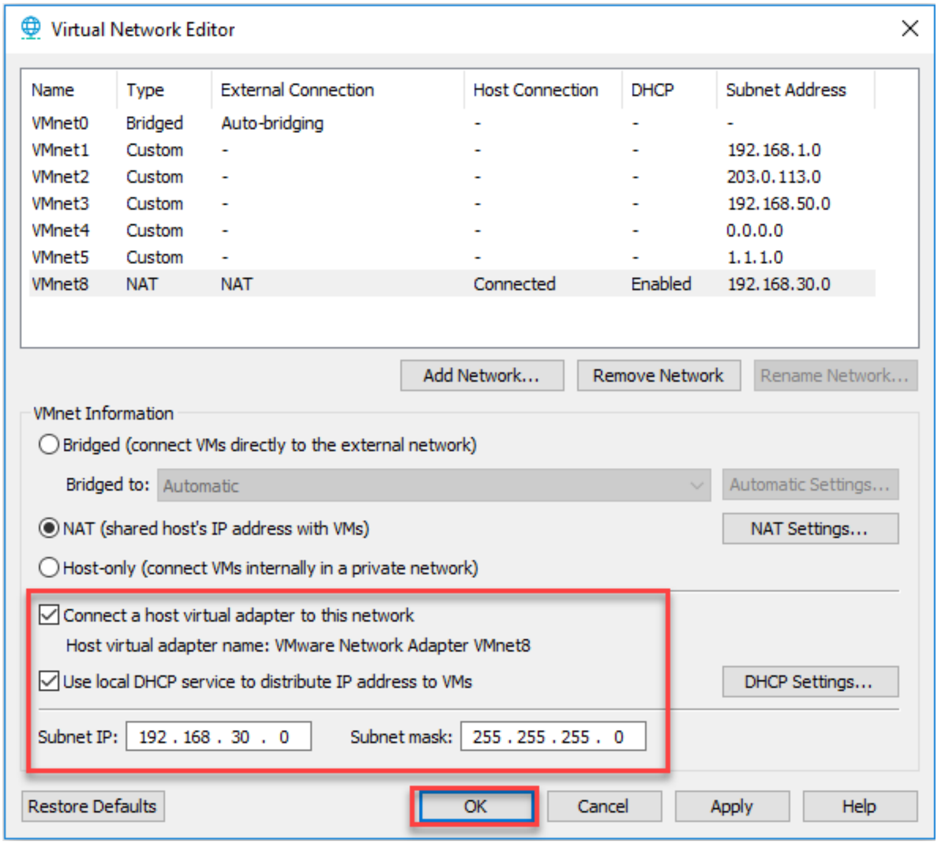
Note: Your VMnet8 NAT Subnet Address should be automatically assigned and will likely be different than the display below. **Please make sure vmnet8 does not use the same subnet as vmnet1, 192.168.1.0/24, in order to prevent address collision.** You can change your NAT subnet address to **192.168.30.0** and the “Subnet mask” to **255.255.255.0** if you want but it is not necessary.

If you have any questions, please consult with your instructor.

Also, if you change your NAT settings you may need to reboot your laptop for these settings to be applied.

1.8.2 Ensure the box next to "*Connect a host virtual adapter to this network*" is *checked*

1.8.3 Ensure the box next to **"***Use local DHCP service to distribute IP addresses to VMs*" is *checked*.



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Custom	-	-	-	192.168.1.0
VMnet2	Custom	-	-	-	203.0.113.0
VMnet3	Custom	-	-	-	192.168.50.0
VMnet4	Custom	-	-	-	0.0.0.0
VMnet5	Custom	-	-	-	1.1.1.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.30.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

● NAT (shared host's IP address with VMs)

○ Host-only (connect VMs internally in a private network)

☑ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet8

☑ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 . 168 . 30 . 0   Subnet mask: 255 . 255 . 255 . 0

1.8.4 Click *Apply*.

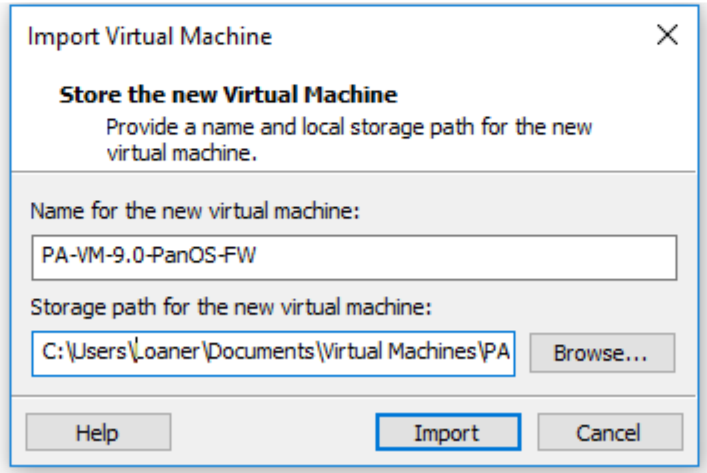
1.8.5 Click *OK*.

Import and Configure Firewall on VMware Workstation

2 Download and Import the academy VM-50 workstation firewall appliance ova into your host computers VMware Workstation application and check to insure appliance's network adapters are assigned to the correct VMnets. The VMware Workstation ova/lab config share drive URL is posted in the following Cybersecurity Academy Moodle Courses: Configuration Infrastructure course, Cybersecurity Prevention and Countermeasures course, Firewall Essentials Configuration and Management course and the Optimizing Firewall Threat Prevention course.

2.1.1 In the VMware Workstation application click *File* and select *Open*.

2.1.2 In the Open dialog box, browse to the location of the PA-VM-9.0-PanOS-FW-OVA and select. Click *Open*.



Import Virtual Machine

Store the new Virtual Machine

Provide a name and local storage path for the new virtual machine.

Name for the new virtual machine:

PA-VM-9.0-PanOS-FW

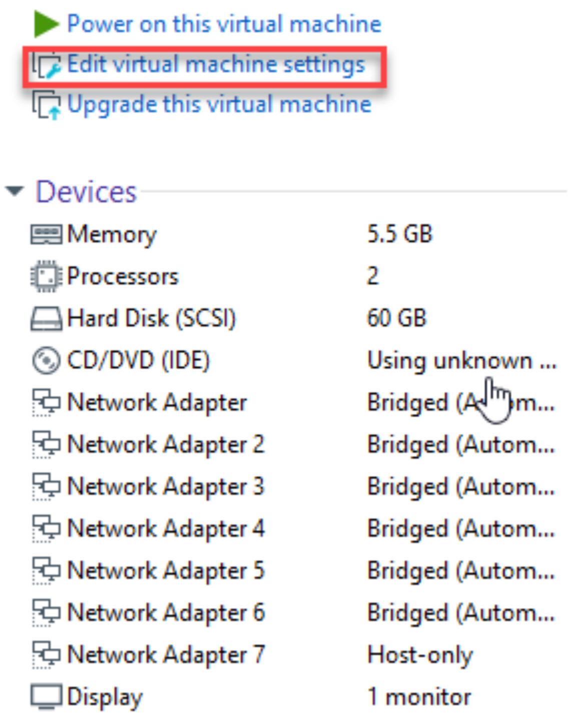
Storage path for the new virtual machine:

C:\Users\Loaner\Documents\Virtual Machines\PA

2.1.3 In the "Import Virtual Machine" dialog box, choose the location of your PA-VM-9.0-PanOS-FW virtual machine.

2.1.4 Click *Import*.

2.1.5 In VMware workstation PA-VM-9.0-PanOS-FW, select edit *Virtual Machine Settings*



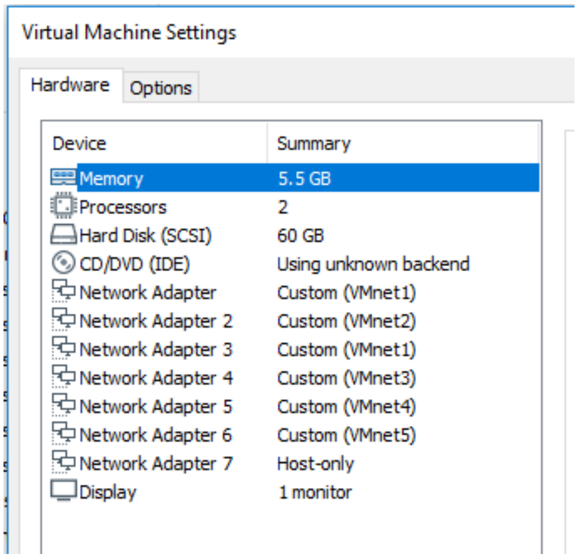
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine

Devices

Memory	5.5 GB
Processors	2
Hard Disk (SCSI)	60 GB
CD/DVD (IDE)	Using unknown ...
Network Adapter	Bridged (Autom...
Network Adapter 2	Bridged (Autom...
Network Adapter 3	Bridged (Autom...
Network Adapter 4	Bridged (Autom...
Network Adapter 5	Bridged (Autom...
Network Adapter 6	Bridged (Autom...
Network Adapter 7	Host-only
Display	1 monitor

and in the dialog box make sure that:

Network adapter 1 is assigned to Custom *"VMnet1".*
Network Adapter 2 is assigned to the Custom *"VMnet2".*
Network Adapter 3 is assigned to Custom *"VMnet1".*
Network Adapter 4 is assigned to Custom *"VMnet3".*
Network Adapter 5 is assigned to Custom *"VMnet4".*
***Network Adapter* 6** is assigned to *"VMnet5".*
Network Adapter 7 is assigned to *"Host-only".*



Virtual Machine Settings

Device	Summary
Memory	5.5 GB
Processors	2
Hard Disk (SCSI)	60 GB
CD/DVD (IDE)	Using unknown backend
Network Adapter	Custom (VMnet1)
Network Adapter 2	Custom (VMnet2)
Network Adapter 3	Custom (VMnet1)
Network Adapter 4	Custom (VMnet3)
Network Adapter 5	Custom (VMnet4)
Network Adapter 6	Custom (VMnet5)
Network Adapter 7	Host-only
Display	1 monitor

Note: Please make sure that the allocated memory for the VM50 appliance is at least **5.5 GB** of RAM. If you set this lower you lose some functionality in the VM-50

2.1.6 Click *OK* to close the dialog box.

2.1.7 Do not power on the firewall yet.

Import and Configure Virtual Router on VMware Workstation

3 Download and Import the PA-VM-9.0-PanOS-VR OVA into your host computer's VMware Workstation application and assign the client's network adapter to the correct VMnet2. The VMware Workstation ova/lab config share drive URL is posted in the following Cybersecurity Academy Moodle Courses: Configuration Infrastructure course, Cybersecurity Prevention and Countermeasures course, Firewall Essentials Configuration and Management course and the Optimizing Firewall Threat Prevention course.

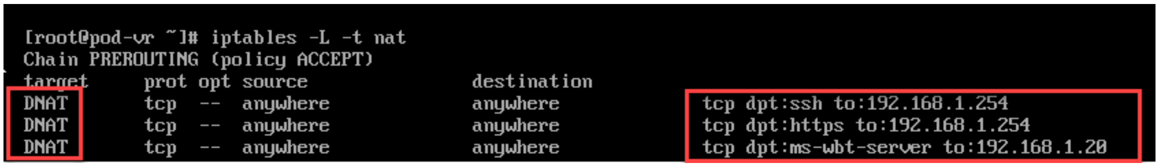
You will follow the same basic steps you did when importing your PA-VM-9.0-PanOS-FW.

The virtual router is configured with 3 destination NATs to connect from your host computer to your VMware Workstation pod as shown in the screen shot below. These destination NATs will allow you to do the following:

1. Connect to your PANOS 9.0.1 VM-50 firewall appliance's management interface WebUI using your host computer's Web browser and the destination https URL composed of the external address of your virtual router's *ens160* interface;

2. Connect to your PANOS 9.0.1 VM-50 firewall appliance's management interface via *ssh* from PuTTY on your host computer using the destination IP address assigned to your virtual router's *ens160* interface and

3. Connect to your pod's Server/Client 2016 via RDP using the destination IP address assigned to your virtual router's ens160 interface.

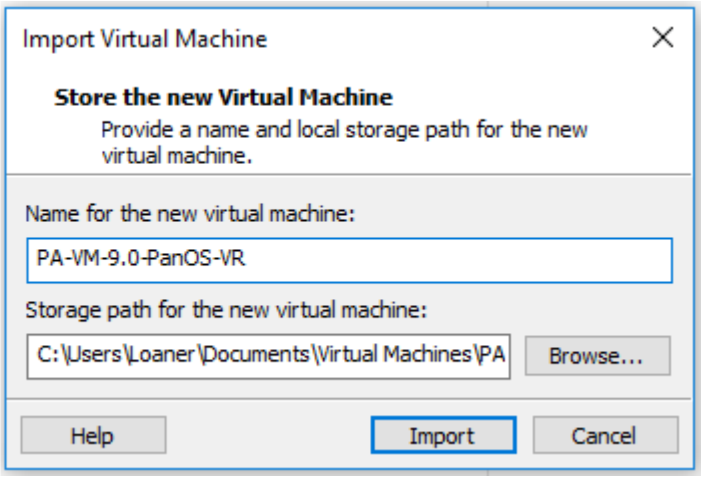


```
[root@pod-vr ~]# iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             anywhere             tcp dpt:ssh to:192.168.1.254
DNAT       tcp  --  anywhere             anywhere             tcp dpt:https to:192.168.1.254
DNAT       tcp  --  anywhere             anywhere             tcp dpt:ms-wbt-server to:192.168.1.20
```

3.1.1 In the VMware Workstation application click *File* and select *Open* in the drop-down menu.

3.1.2 In the Open dialog box, browse to the location of the PA-VM-9.0-PanOS-VR ova and select to open it.

3.1.3 In the "Import Virtual Machine" dialog box, chose the location of your virtual machine and click *Import*.



Import Virtual Machine

Store the new Virtual Machine

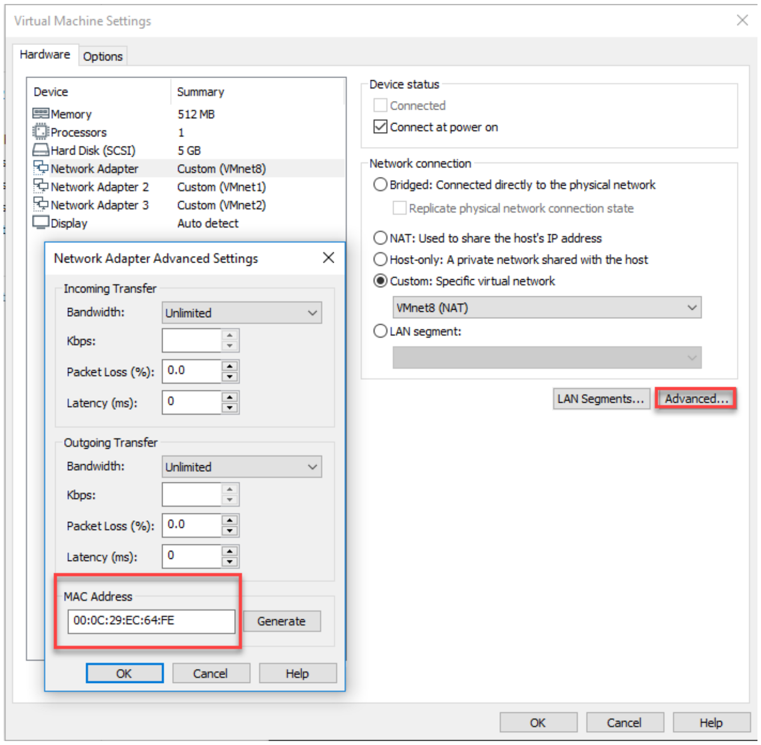
Provide a name and local storage path for the new virtual machine.

Name for the new virtual machine: PA-VM-9.0-PanOS-VR

Storage path for the new virtual machine: C:\Users\Loaner\Documents\Virtual Machines\PA

3.1.4 In Workstation on your PA-VM-9.0-PanOS-VR tab, select *edit virtual network machine settings* and assign the Network Adapter 1 to **NAT (“VMnet8)”**

3.1.5 Select the *Advanced* option. Once in the Advanced menu please manually enter the following MAC Address: “**00:0C:29:EC:64:FE**” and select *OK*.



Virtual Machine Settings

Device	Summary
Memory	512 MB
Processors	1
Hard Disk (SCSI)	5 GB
Network Adapter	Custom (VMnet8)
Network Adapter 2	Custom (VMnet1)
Network Adapter 3	Custom (VMnet2)
Display	Auto detect

Device status
□ Connected
☑ Connect at power on

Network connection
○ Bridged: Connected directly to the physical network
□ Replicate physical network connection state
○ NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
● Custom: Specific virtual network
VMnet8 (NAT)
○ LAN segment:

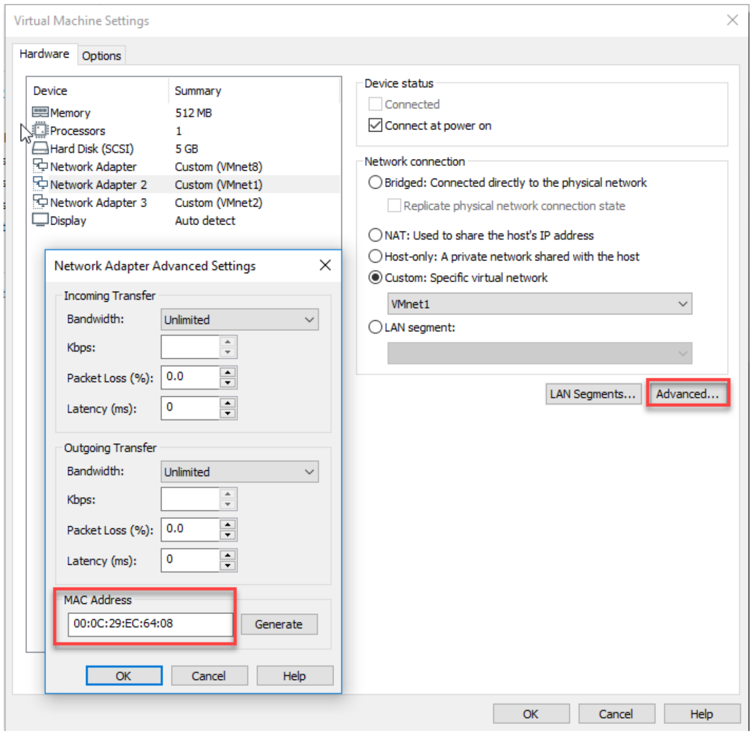
Network Adapter Advanced Settings

Incoming Transfer
Bandwidth: Unlimited
Kbps:
Packet Loss (%): 0.0
Latency (ms): 0

Outgoing Transfer
Bandwidth: Unlimited
Kbps:
Packet Loss (%): 0.0
Latency (ms): 0

MAC Address
00:0C:29:EC:64:FE

3.1.6 Set *Network Adapter* 2 to “**Custom(VMnet1)**” and then select the *Advanced* option. Once in the Advanced menu please manually enter the following MAC Address: “**00:0C:29:EC:64:08**” and select *OK*.



Virtual Machine Settings

Device	Summary
Memory	512 MB
Processors	1
Hard Disk (SCSI)	5 GB
Network Adapter	Custom (VMnet8)
Network Adapter 2	Custom (VMnet1)
Network Adapter 3	Custom (VMnet2)
Display	Auto detect

Device status
□ Connected
☑ Connect at power on

Network connection
○ Bridged: Connected directly to the physical network
□ Replicate physical network connection state
○ NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
● Custom: Specific virtual network
VMnet1
○ LAN segment:

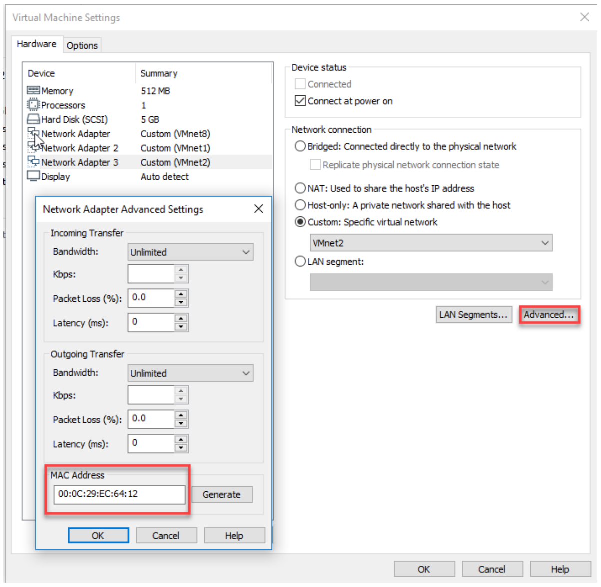
Network Adapter Advanced Settings

Incoming Transfer
Bandwidth: Unlimited
Kbps:
Packet Loss (%): 0.0
Latency (ms): 0

Outgoing Transfer
Bandwidth: Unlimited
Kbps:
Packet Loss (%): 0.0
Latency (ms): 0

MAC Address
00:0C:29:EC:64:08

3.1.7 Set **Network Adapter 3** to "**Custom(VMnet2)**" and then select the *Advanced* option. Once in the Advanced menu please manually enter the following MAC Address: "**00:0C:29:EC:64:12**" and select *OK* 2 times.



Virtual Machine Settings

Device	Summary
Memory	512 MB
Processors	1
Hard Disk (SCSI)	5 GB
Network Adapter	Custom (VMnet8)
Network Adapter 2	Custom (VMnet1)
Network Adapter 3	Custom (VMnet2)
Display	Auto detect

Device status
□ Connected
☑ Connect at power on

Network connection
○ Bridged: Connected directly to the physical network
□ Replicate physical network connection state
○ NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
● Custom: Specific virtual network
VMnet2
○ LAN segment:

Network Adapter Advanced Settings

Incoming Transfer
Bandwidth: Unlimited
Kbps:
Packet Loss (%): 0.0
Latency (ms): 0

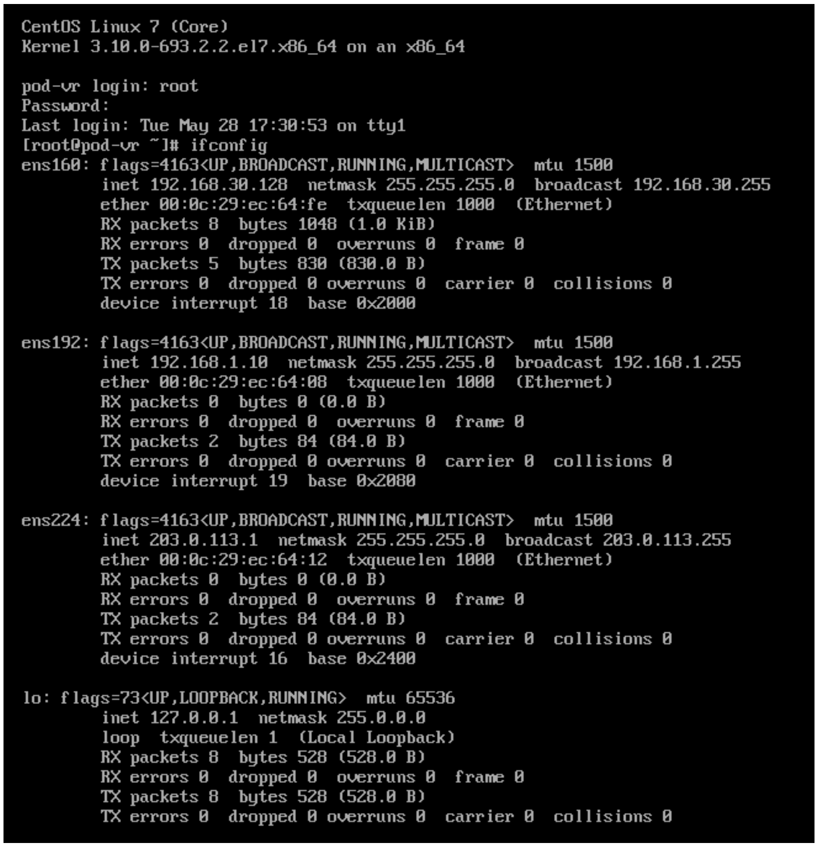
Outgoing Transfer
Bandwidth: Unlimited
Kbps:
Packet Loss (%): 0.0
Latency (ms): 0

MAC Address
00:0C:29:EC:64:12

3.1.8 *Power* on your PA-VM-9.0-PanOS-VR VM. You will need the VM's built in router to connect your VM-50 management interface to the Internet for licensing.

3.1.9 *Log on* to the VR using the username **root** and password **Pal0Alt0**. *Type* **ifconfig** and confirm that you can see the following:

Note: If you do not see the IP addresses associated with each interface repeat the previous steps for the VR machine**.**

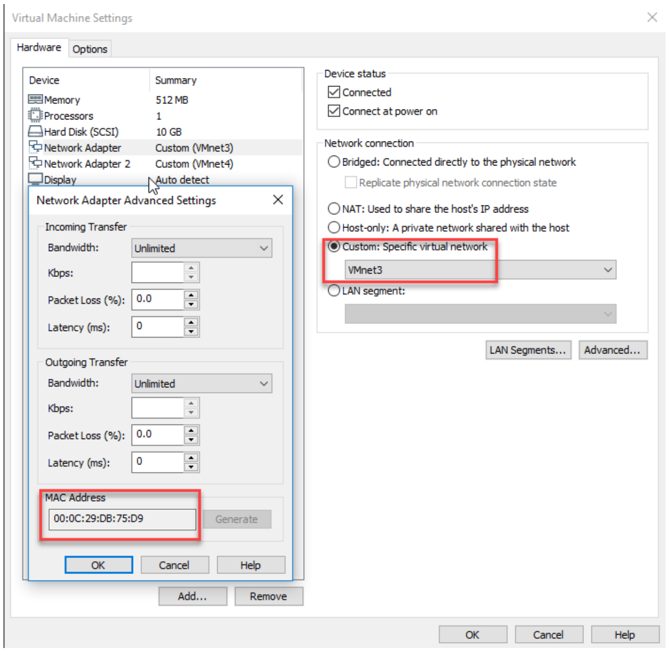


```
CentOS Linux 7 (Core)
Kernel 3.10.0-693.2.2.el7.x86_64 on an x86_64

pod-vr login: root
Password:
Last login: Tue May 28 17:30:53 on tty1
[root@pod-vr ~]# ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.30.128  netmask 255.255.255.0  broadcast 192.168.30.255
        ether 00:0c:29:ec:64:fe  txqueuelen 1000  (Ethernet)
        RX packets 8  bytes 1048 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5  bytes 830 (830.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 18  base 0x2000

ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        ether 00:0c:29:ec:64:08  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2  bytes 84 (84.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2080

ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 203.0.113.1  netmask 255.255.255.0  broadcast 203.0.113.255
        ether 00:0c:29:ec:64:12  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2  bytes 84 (84.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  base 0x2400

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1  (Local Loopback)
        RX packets 8  bytes 528 (528.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 528 (528.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Import and Configure DMZ Server on VMware Workstation

4 Download and import the PA-VM-9.0-PanOS-DMZ ova into your host computer's VMware Workstation application and assign the client's network adapter to the correct VMnet2. Follow the same steps as you have done for both the FW and the VR virtual machines previously. The VMware Workstation ova/lab config share drive URL is posted in the following Cybersecurity Academy Moodle Courses: Configuration Infrastructure course, Cybersecurity Prevention and Countermeasures course, Firewall Essentials Configuration and Management course and the Optimizing Firewall Threat Prevention course.

4.1.1 In Workstation on your PA-VM-9.0-PanOS-DMZ tab, select *edit virtual network settings* and assign the **Network Adapter 1** to "**Custom(VMnet3)**", and then select the *Advanced* option. Once in the Advanced menu please manually enter the following MAC Address: "**00:0C:29:DB:75:D9**" and select *OK*.



Virtual Machine Settings

Device	Summary
Memory	512 MB
Processors	1
Hard Disk (SCSI)	10 GB
Network Adapter	Custom (VMnet3)
Network Adapter 2	Custom (VMnet4)
Display	Auto detect

Device status
☑ Connected
☑ Connect at power on

Network connection
○ Bridged: Connected directly to the physical network
□ Replicate physical network connection state
○ NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
● Custom: Specific virtual network
VMnet3
○ LAN segment:

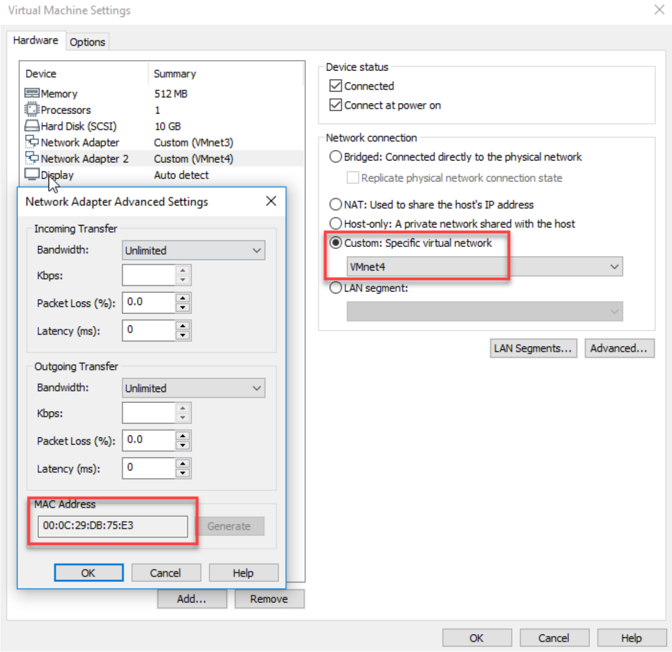
Network Adapter Advanced Settings

Incoming Transfer
Bandwidth: Unlimited
Kbps:
Packet Loss (%): 0.0
Latency (ms): 0

Outgoing Transfer
Bandwidth: Unlimited
Kbps:
Packet Loss (%): 0.0
Latency (ms): 0

MAC Address
00:0C:29:DB:75:D9

4.1.2 In Workstation on your PA-VM-9.0-PanOS-DMZ tab, select *edit virtual network settings* and assign the **Network Adapter 2** to "**Custom(VMnet4)**", and then select the *Advanced* option. Once in the Advanced menu please manually enter the following MAC Address: "**00:0C:29:DB:75:E3**" and select *OK* 2 times.



Virtual Machine Settings

Device	Summary
Memory	512 MB
Processors	1
Hard Disk (SCSI)	10 GB
Network Adapter	Custom (VMnet3)
Network Adapter 2	Custom (VMnet4)
Display	Auto detect

Network Adapter Advanced Settings

Incoming Transfer
Bandwidth: Unlimited
Kbps:
Packet Loss (%): 0.0
Latency (ms): 0

Outgoing Transfer
Bandwidth: Unlimited
Kbps:
Packet Loss (%): 0.0
Latency (ms): 0

MAC Address
00:0C:29:DB:75:E3

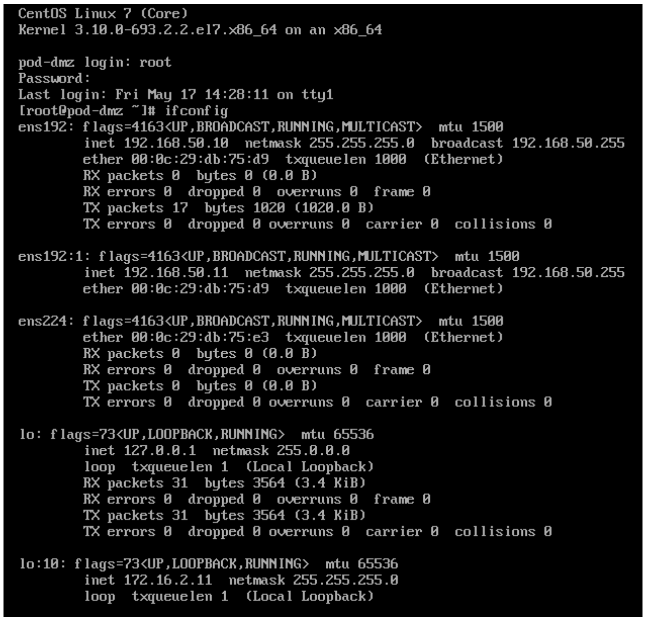
Device status
☑ Connected
☑ Connect at power on

Network connection
○ Bridged: Connected directly to the physical network
□ Replicate physical network connection state
○ NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
● Custom: Specific virtual network
VMnet4
○ LAN segment:

4.1.3 *Power* on your PA-VM-9.0-PanOS-DMZ VM.

4.1.4 *Log on* to the DMZ using the username **root** and password **Pal0Alt0**. Type **ifconfig** and confirm that you can see the following:

Note: If you do not see the IP addresses associated with each interface repeat the previous steps for the DMZ machine.



```
CentOS Linux 7 (Core)
Kernel 3.10.0-693.2.2.el7.x86_64 on an x86_64

pod-dmz login: root
Password:
Last login: Fri May 17 14:28:11 on tty1
[root@pod-dmz ~]# ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.10  netmask 255.255.255.0  broadcast 192.168.50.255
        ether 00:0c:29:db:75:d9  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17  bytes 1020 (1020.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens192:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.11  netmask 255.255.255.0  broadcast 192.168.50.255
        ether 00:0c:29:db:75:d9  txqueuelen 1000  (Ethernet)

ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 00:0c:29:db:75:e3  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1  (Local Loopback)
        RX packets 31  bytes 3564 (3.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 31  bytes 3564 (3.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo:10: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 172.16.2.11  netmask 255.255.255.0
        loop  txqueuelen 1  (Local Loopback)
```

Configure Windows 2016 Client to work on VMware Workstation

5 If you are an existing Academy and have used the PANOS 8.0 Windows Server/Client 2012R2 Virtual Machine: You may use this virtual machine, licensed via your institution, for the PANOS 9.0.1 VMware Workstation lab pod.

If you do not have this virtual machine from the PANOS 8.0 VMware Workstation lab pod, then please follow the directions in the steps below to configure a Server/Client 2016 virtual machine which you will need to license using your institution's Microsoft license.

There are 16 individual configuration settings that need to be performed on your Windows Server / Client in order to function properly, including external authentication, certificate services, installing WireShark, folder paths and more.

Note: The following steps need to be configured in order for the labs to function correctly.

5.1.1 *Create* a New Windows Server/Client 2016 Virtual Machine:

5.1.2 *Download* the Windows Sever 2016 ISO image from your Microsoft account and create a new VMware Workstation virtual machine using this ISO image.

For the default "administrator" account use "**Pal0Alt0**" as the password and install VMware tools after creating the Server 2016 virtual machine. Temporarily connect your Server 2016 network adapter to *vmnet8*, the VMware Workstation's NAT'd VMnet.

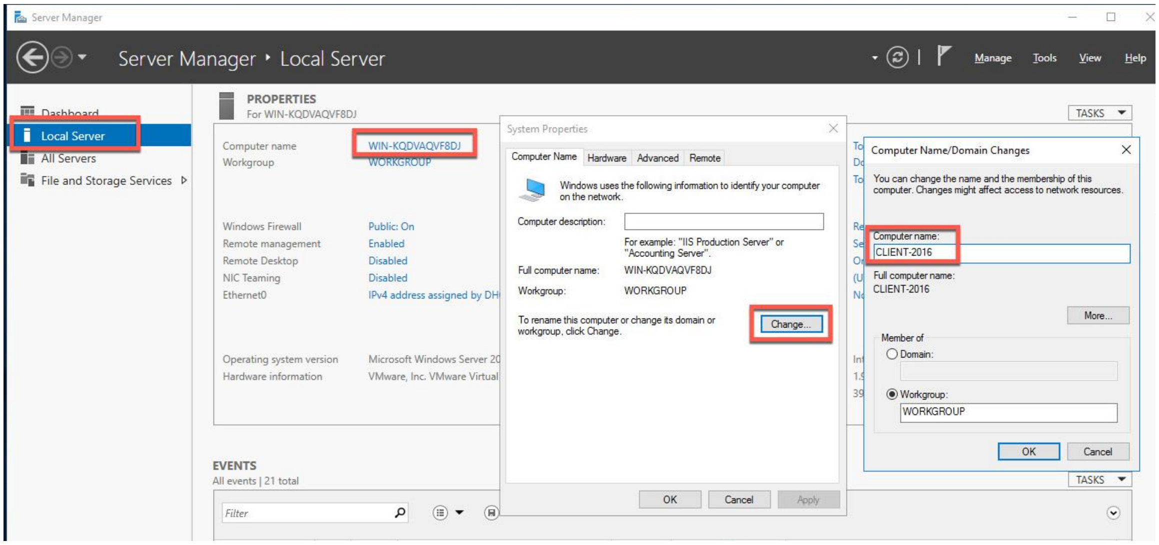
Set the RAM of your Server 2016 to **2024** MB.

5.1.3 Rename Your Server 2016:

Open "*Server Manager*" and on the left pane select "*Local Server*" then under the "*Properties*" window *click* the default name of your computer. This will open the System Properties dialog box.

In the "System Properties" dialog box click "*Change*". This will open the "Computer Name/Domain Changes" dialog box. In the "Computer name" text box, change the default name to "**CLIENT-2016**".

After changing the name, you will need to *restart* the computer.



PROPERTIES
For WIN-KQDVAQVF8DJ

Computer name: WIN-KQDVAQVF8DJ
Workgroup: WORKGROUP
Windows Firewall: Public: On
Remote management: Enabled
Remote Desktop: Disabled
NIC Teaming: Disabled
Ethernet0: IPv4 address assigned by DH
Operating system version: Microsoft Windows Server 20
Hardware information: VMware, Inc. VMware Virtual

EVENTS
All events | 21 total

Windows uses the following information to identify your computer on the network.

Computer description:
For example: "IIS Production Server" or "Accounting Server".
Full computer name: WIN-KQDVAQVF8DJ
Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

Computer Name/Domain Changes

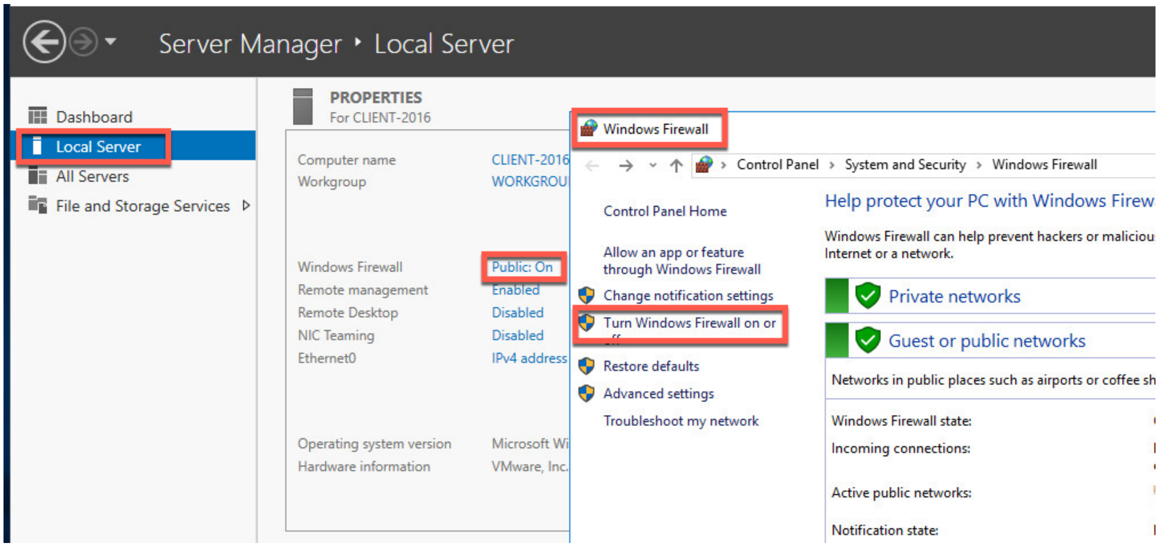
You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: CLIENT-2016
Full computer name: CLIENT-2016

Member of
○ Domain:
● Workgroup: WORKGROUP

5.1.4 Disable Windows Firewall:

On your Server 2016 desktop in *Server Manager* under “*Properties*” window click “*Public On*” after Windows Firewall and in the Windows Firewall dialog box, select “Turn Windows Firewall on or off”. This will bring up the “Customize Settings” dialog box, select to “*Turn Off Windows Firewall …*” in *Private network* settings and *Public network* settings.


Server Manager ‣ Local Server
Dashboard
Local Server
All Servers
File and Storage Services
Windows Firewall
Control Panel › System and Security › Windows Firewall
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Private networks
Guest or public networks

PROPERTIES
For CLIENT-2016

Computer name: CLIENT-2016
Workgroup: WORKGROU
Windows Firewall: Public: On
Remote management: Enabled
Remote Desktop: Disabled
NIC Teaming: Disabled
Ethernet0: IPv4 address
Operating system version: Microsoft Wi
Hardware information: VMware, Inc.

Help protect your PC with Windows Firew

Windows Firewall can help prevent hackers or maliciou Internet or a network.

Networks in public places such as airports or coffee sh

Windows Firewall state:
Incoming connections:
Active public networks:
Notification state:

5.1.5 Promote Server 2016 to a Domain Controller:

Follow the directions at this Web site to upgrade your server to a domain controller: https://blogs.technet.microsoft.com/canitpro/2017/02/22/step-by-step-setting-up-active-directory-in-windows-server-2016/.

Don’t change the temporary DHCP IP address of your Server 2016 but do change your Server’s preferred DNS to **127.0.0.1** as your Primary DNS server and use **1.1.1.1** or your NAT’d, VMnet8 default gateway as your Alternate DNS server.

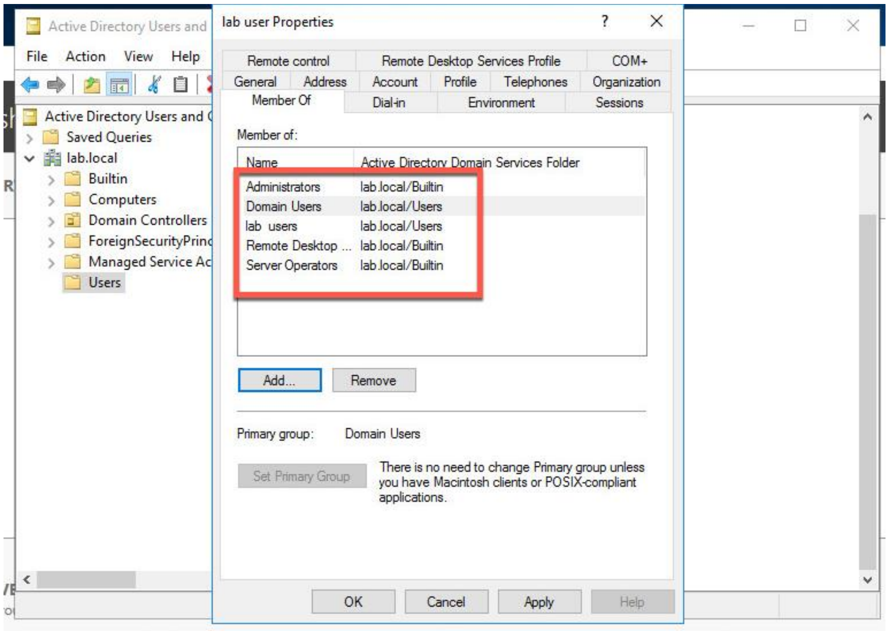
After installing most of the required lab applications on your Server 2016 domain controller, you will change the IP address from DHCP client to a static **192.16.1.20**. Name your domain forest: “**lab.local**”. Use the password “**Pal0Alt0**” as the DRSM password.

5.1.6 Create the following users in Active Directory

lab-user Account and Group:

Log on to your Server 2016 Domain Controller and create a new user account in Active Directory Users and Computers using the following data:
First name: **lab**
Last name: **user**
User logon name: **lab-user**.
For *password* use: “**Pal0Alt0**” and *uncheck* “User must change password at next logon” and “Password never expires”.

Add lab-user to the following groups:
Remote Desktop; Administrators and Server Operators.
Create a new global security group named: *lab users* and add *lab-user* as a member.



Member of:

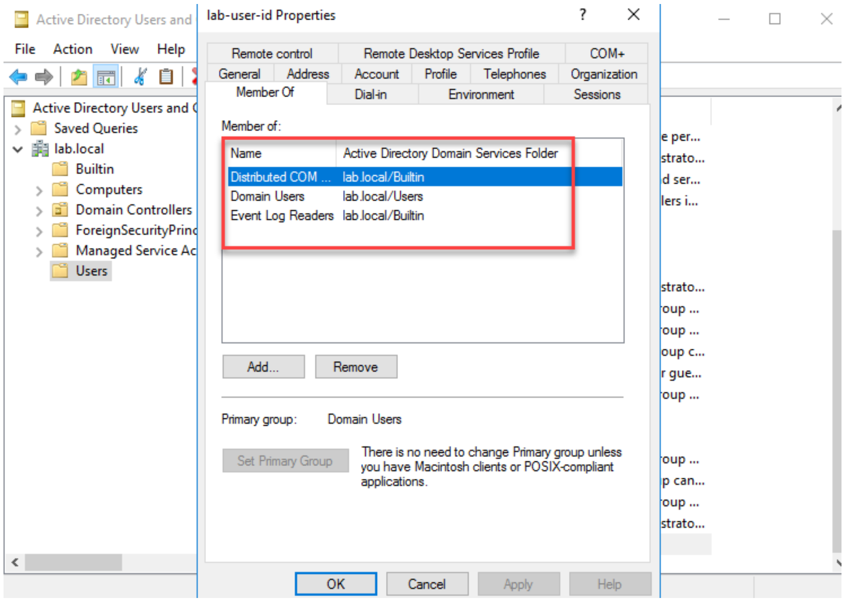
Name	Active Directory Domain Services Folder
Administrators	lab.local/Builtin
Domain Users	lab.local/Users
lab users	lab.local/Users
Remote Desktop ...	lab.local/Builtin
Server Operators	lab.local/Builtin

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

5.1.7 Active Directory Users and Computers using the following data:
First name: **lab-user-id**
User logon name: **lab-user-id**.
For *password* use: “**Pal0Alt0**” and *uncheck* “User must change password at next logon” and “Password never expires”

Add lab-user-id to the following groups:
Domain Users, Distributed COM Users, Event Log Readers.



Member of:

Name	Active Directory Domain Services Folder
Distributed COM ...	lab.local/Builtin
Domain Users	lab.local/Users
Event Log Readers	lab.local/Builtin

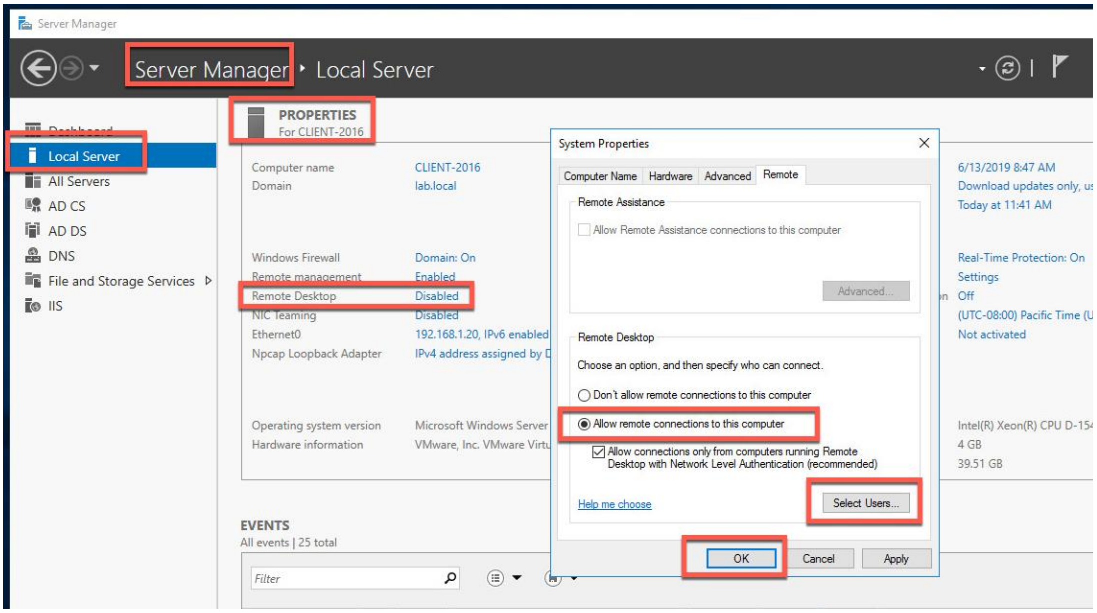
Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

5.1.8 Enable Remote Desktop on the Client/Server:

In *Server Manager* > *Properties* Windows enable *Remote Desktop*. In the System Properties dialog box click Select *Users*.

Add the *Administrator* and *lab-user* users.



Server Manager ▸ Local Server

PROPERTIES
For CLIENT-2016

Computer name	CLIENT-2016
Domain	lab.local
Windows Firewall	Domain: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet0	192.168.1.20, IPv6 enabled
Npcap Loopback Adapter	IPv4 address assigned by D
Operating system version	Microsoft Windows Server
Hardware information	VMware, Inc. VMware Virtu

System Properties

Computer Name | Hardware | Advanced | Remote

Remote Assistance

□ Allow Remote Assistance connections to this computer

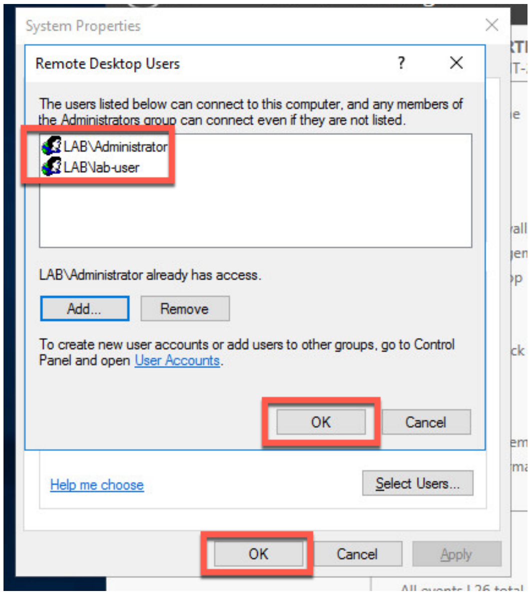
Remote Desktop

Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)



System Properties

Remote Desktop Users

The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

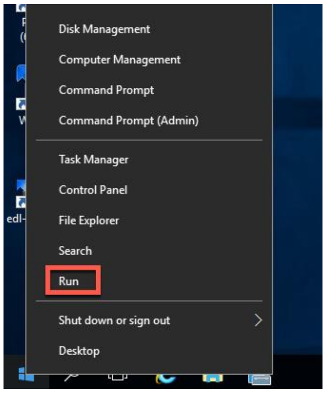
LAB\Administrator
LAB\lab-user

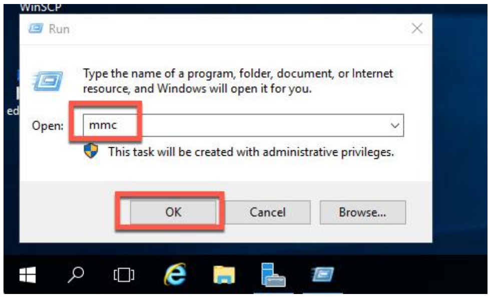
LAB\Administrator already has access.

To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

5.1.9 Configure default domain password policy with no restrictions and configure the default domain auditing policy.

xv. Right click the Microsoft Windows icon in the lower left of your desktop and select run. In the “Run” dialog box enter mmc and click “OK”.



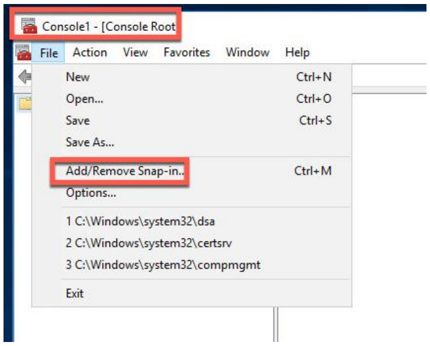


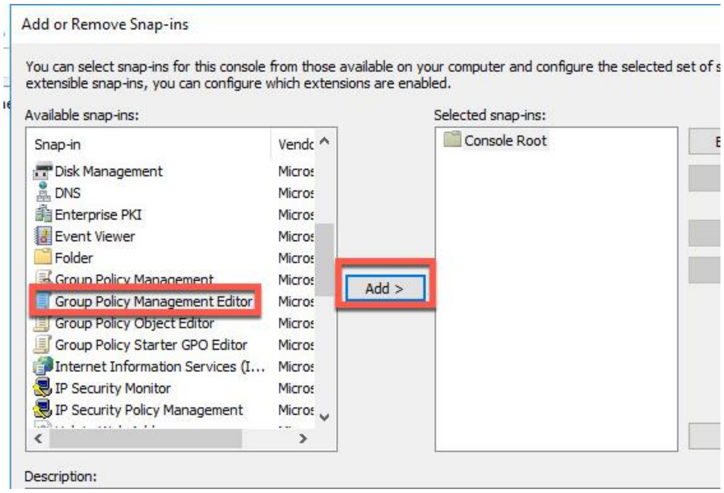
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

This task will be created with administrative privileges.

xvi. In the “Console1” dialog box under the “File” tab, click “Add/Remove Snap-in”. In the “Add or Remove Snap-ins” select “Group Policy Management Editor” and in the “Select Group Policy Object” dialog box browse and select “Default Domain Policy” to edit and click OK then Finish then OK to exit out of the “Add or Remove Snap-ins” dialog box.





Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of s extensible snap-ins, you can configure which extensions are enabled.

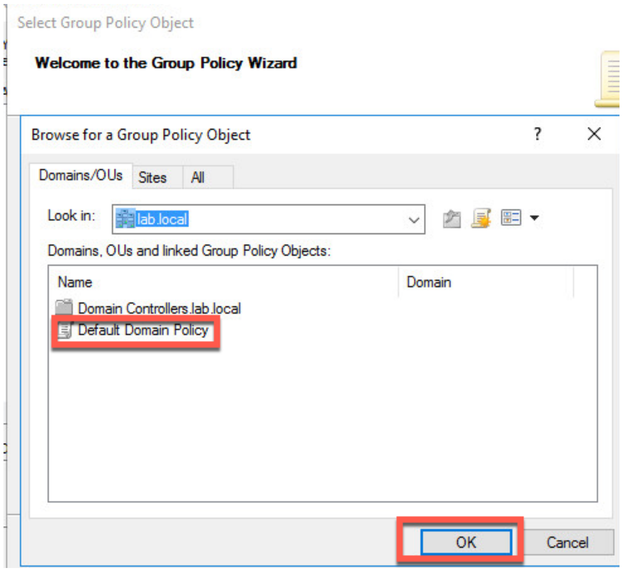
Available snap-ins:

Snap-in	Vendc
Disk Management	Micros
DNS	Micros
Enterprise PKI	Micros
Event Viewer	Micros
Folder	Micros
Group Policy Management	Micros
Group Policy Management Editor	Micros
Group Policy Object Editor	Micros
Group Policy Starter GPO Editor	Micros
Internet Information Services (I...	Micros
IP Security Monitor	Micros
IP Security Policy Management	Micros

Selected snap-ins:

Console Root

Description:



Select Group Policy Object

Welcome to the Group Policy Wizard

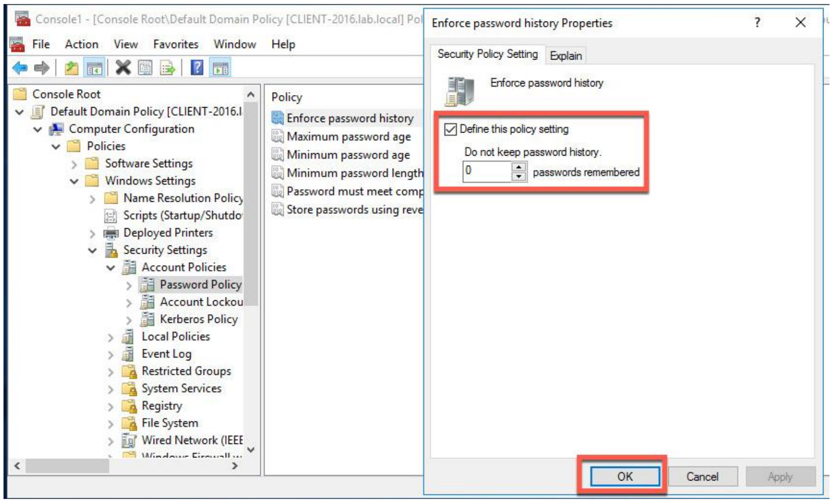
Browse for a Group Policy Object

Look in: lab.local

Domains, OUs and linked Group Policy Objects:

Name	Domain
Domain Controllers.lab.local	
Default Domain Policy	

xvii. In the “Console1” mmc dialog box browse to Default Domain Policy>Computer Configuration>Security Settings>Account Policies>Password Policy. Double click Enforce password history and in the “Enforce password history Properties” dialog box, select “0” passwords remembered and click “OK” to close the dialog box. Double click “Maximum password age” and in the dialog box uncheck the “Define this policy setting” box and click “OK” and click “OK” to allow change to “Minimum password age”. Double click “Password must meet complexity requirements” and click disabled in the dialog box.



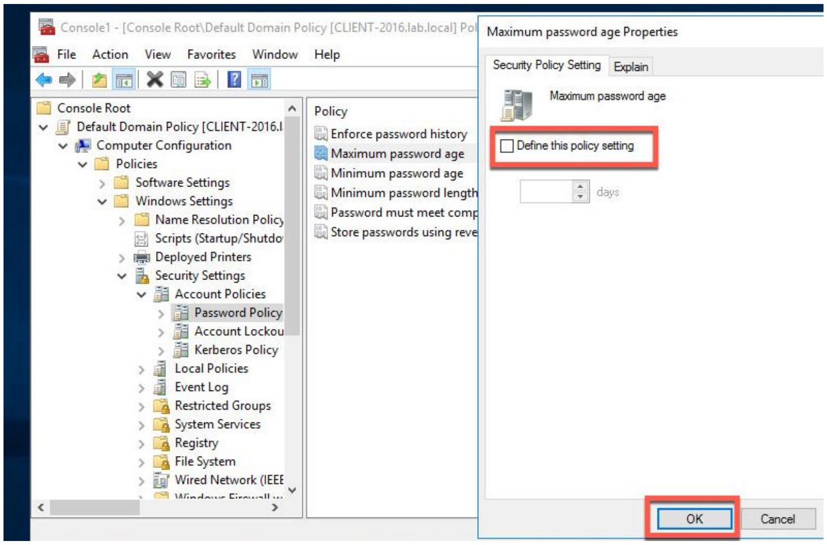
Enforce password history Properties

Enforce password history

☑ Define this policy setting

Do not keep password history.

0 passwords remembered

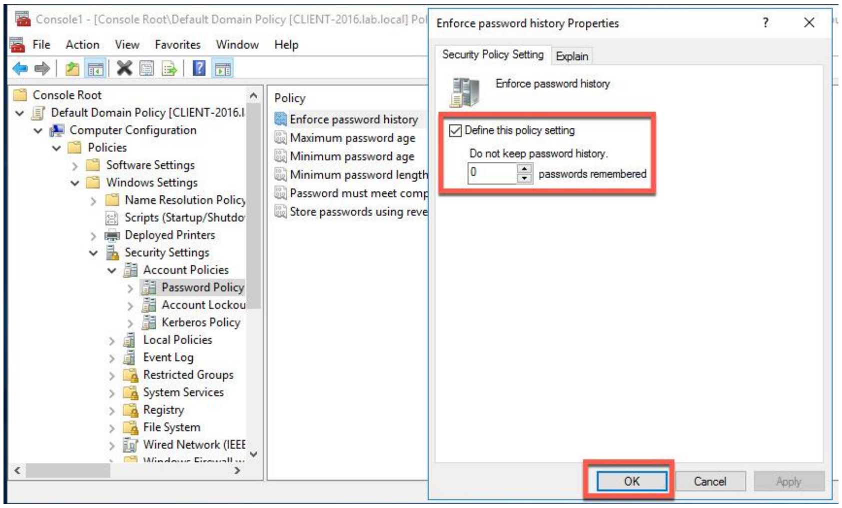


Maximum password age Properties

Maximum password age

☐ Define this policy setting

days



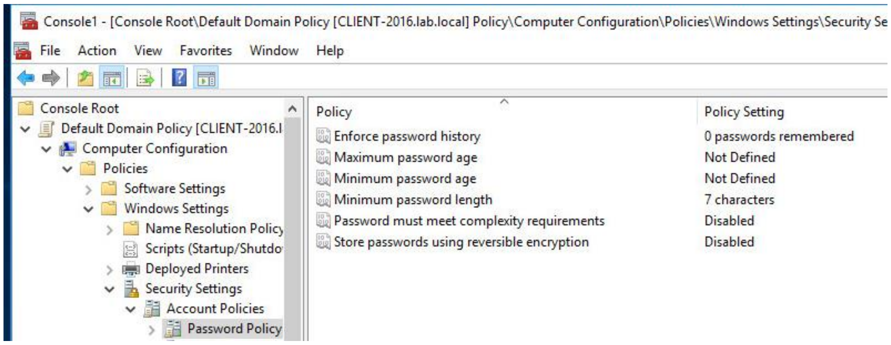
Enforce password history Properties

Enforce password history

☑ Define this policy setting

Do not keep password history.

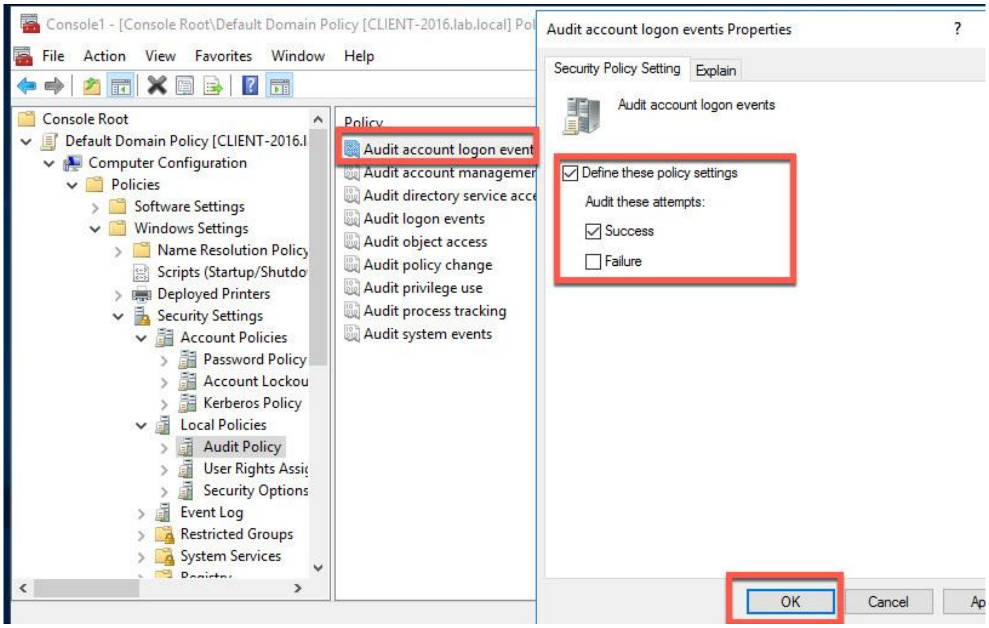
0 passwords remembered



Console1 - [Console Root\Default Domain Policy [CLIENT-2016.lab.local] Policy\Computer Configuration\Policies\Windows Settings\Security Se

Policy	Policy Setting
Enforce password history	0 passwords remembered
Maximum password age	Not Defined
Minimum password age	Not Defined
Minimum password length	7 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

xviii. In the Console1 GPO editor mmc, browse to Computer Configuration>Policies>Windows Settings>Security Settings>Local Policies>Audit Policy and double click "Audit account logon events". In the dialog box, select: "Define these policy settings", Success and click OK to exit the dialog box. Double click "Audit logon events", select "Define these policy settings", "Success" and click OK to exit the dialog box.



Console1 - [Console Root\Default Domain Policy [CLIENT-2016.lab.local] Pol

Audit account logon events Properties

Security Policy Setting | Explain

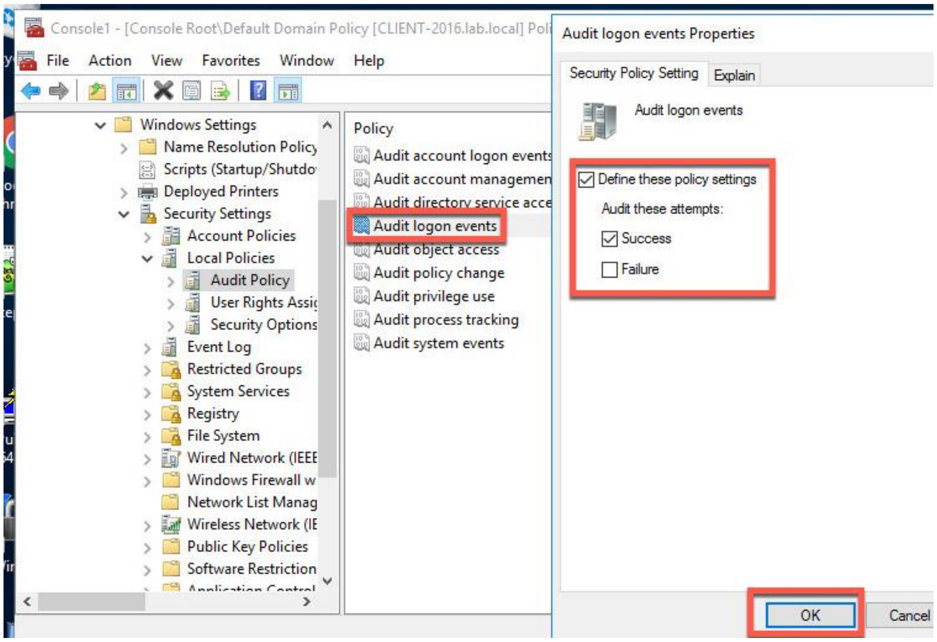
Audit account logon events

☑ Define these policy settings

Audit these attempts:

☑ Success

□ Failure



☑ Define these policy settings

Audit these attempts:

☑ Success

□ Failure

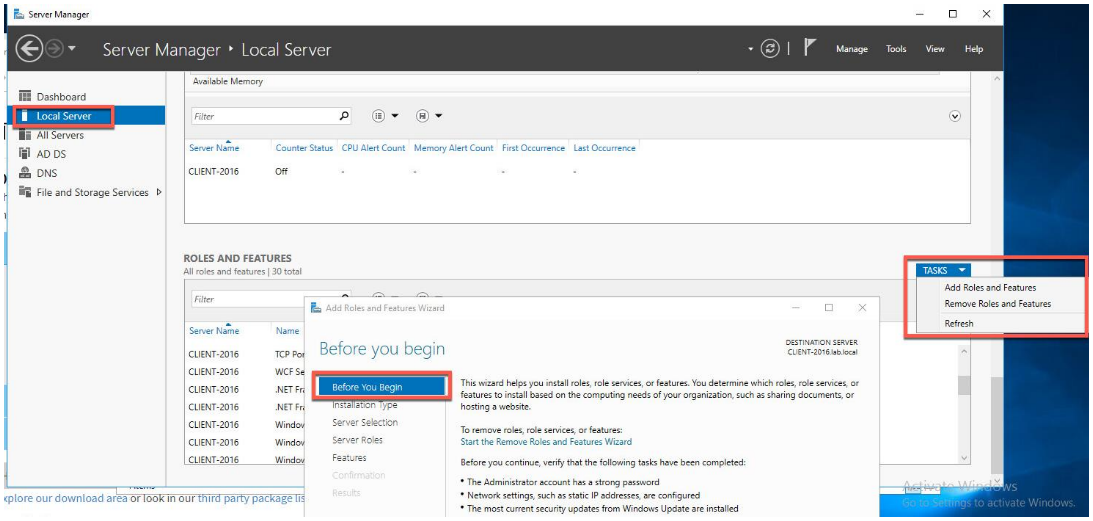
5.1.10 Install Active Directory Certificate Services:

The general directions are found here: https://technet.microsoft.com/en-us/library/jj717285(v=ws.11).aspx.

The steps used to configure the Windows Server 2016 host in your lab pod are listed below.

ii. Open the Server Manager.

iii. Select *Manage > Add Roles and Features*.



Server Name	Counter Status	CPU Alert Count	Memory Alert Count	First Occurrence	Last Occurrence
CLIENT-2016	Off	-	-	-	-

Server Name	Name
CLIENT-2016	TCP Por
CLIENT-2016	WCF Se
CLIENT-2016	.NET Fr
CLIENT-2016	.NET Fr
CLIENT-2016	Windov
CLIENT-2016	Windov
CLIENT-2016	Windov

Before you begin

DESTINATION SERVER
CLIENT-2016.lab.local

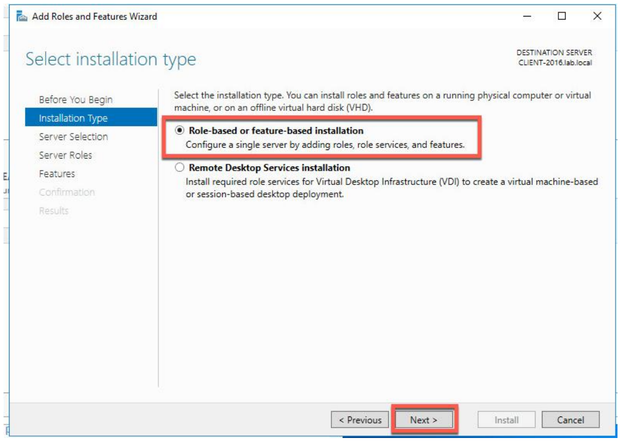
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

iv. Select *Role-based* or *feature-based installation* and click *Next*.



Select installation type

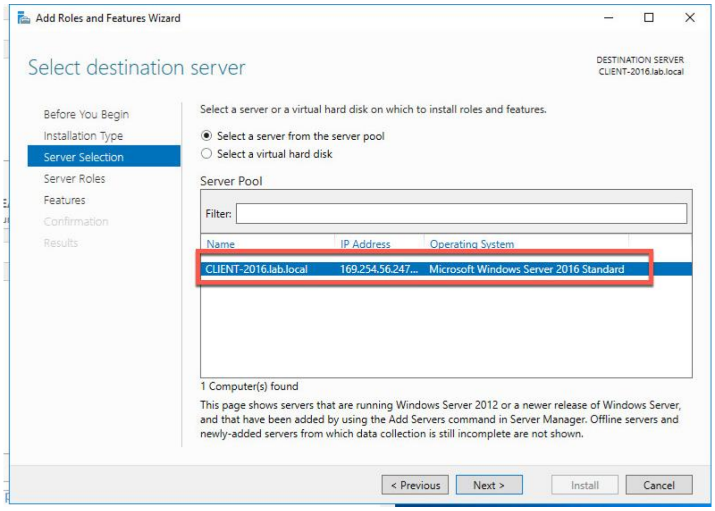
DESTINATION SERVER
CLIENT-2016.lab.local

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

v. *Accept* default server (the local machine) and click *Next*.



Select destination server

DESTINATION SERVER
CLIENT-2016.lab.local

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Filter:

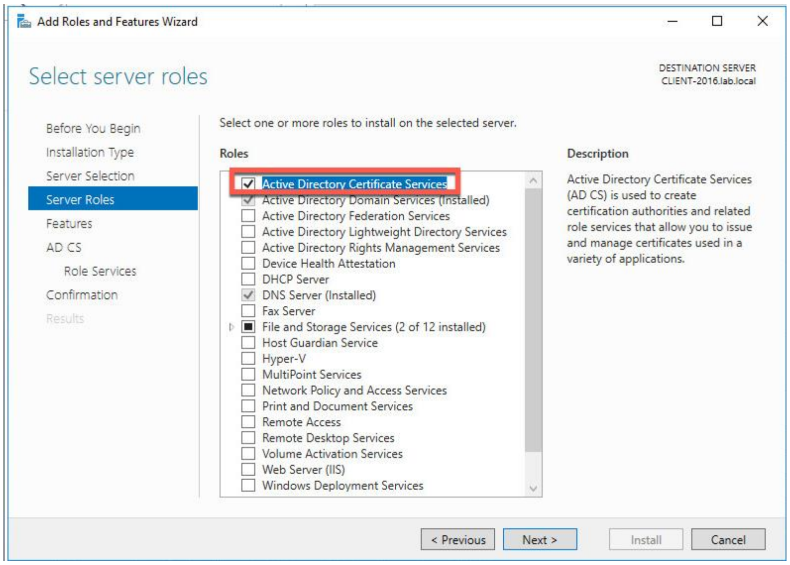
Name	IP Address	Operating System
CLIENT-2016.lab.local	169.254.56.247...	Microsoft Windows Server 2016 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

vi. Select *Active Directory Certificate Services.*

vii. Click *Next.*



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
CLIENT-2016.lab.local

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Confirmation
Results

Select one or more roles to install on the selected server.

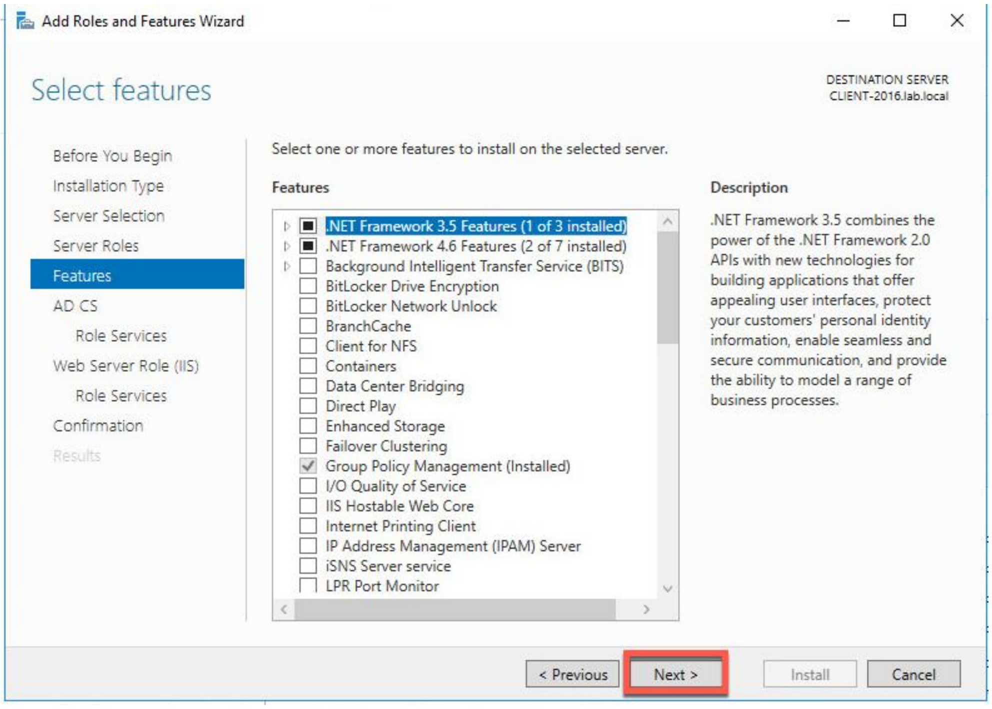
Roles

- ☑ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ MultiPoint Services
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

viii. In the features Window, click *Next*.



Add Roles and Features Wizard

Select features

DESTINATION SERVER
CLIENT-2016.lab.local

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results

Select one or more features to install on the selected server.

Features

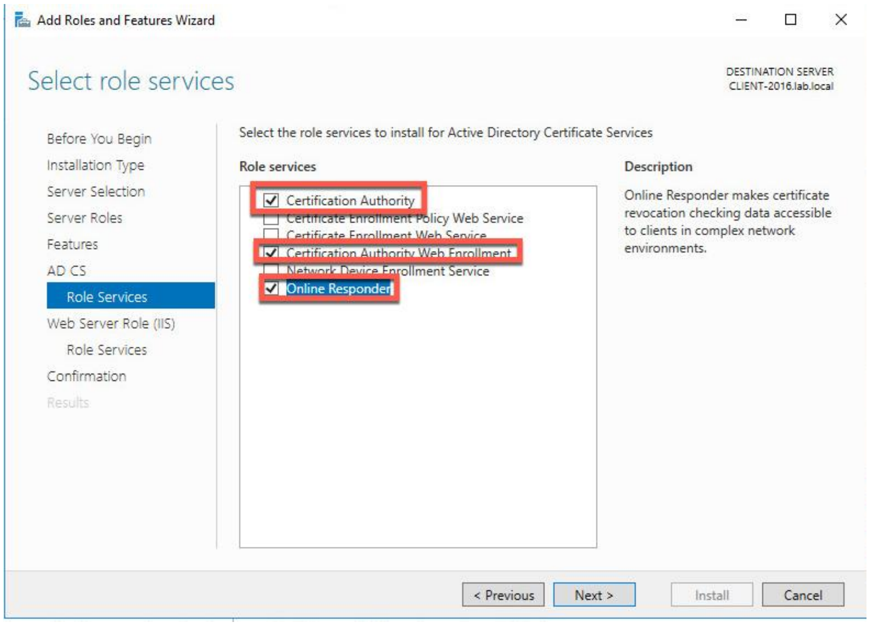
- ■ .NET Framework 3.5 Features (1 of 3 installed)
- ■ .NET Framework 4.6 Features (2 of 7 installed)
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache
- ☐ Client for NFS
- ☐ Containers
- ☐ Data Center Bridging
- ☐ Direct Play
- ☐ Enhanced Storage
- ☐ Failover Clustering
- ☑ Group Policy Management (Installed)
- ☐ I/O Quality of Service
- ☐ IIS Hostable Web Core
- ☐ Internet Printing Client
- ☐ IP Address Management (IPAM) Server
- ☐ iSNS Server service
- ☐ LPR Port Monitor

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

ix. In the Role Services window, select *Certification Authority, Certificate Authority Web Enrolment, Online Responder*.

x. Continue to click *Next* until Confirmation step



Select role services

DESTINATION SERVER
CLIENT-2016.lab.local

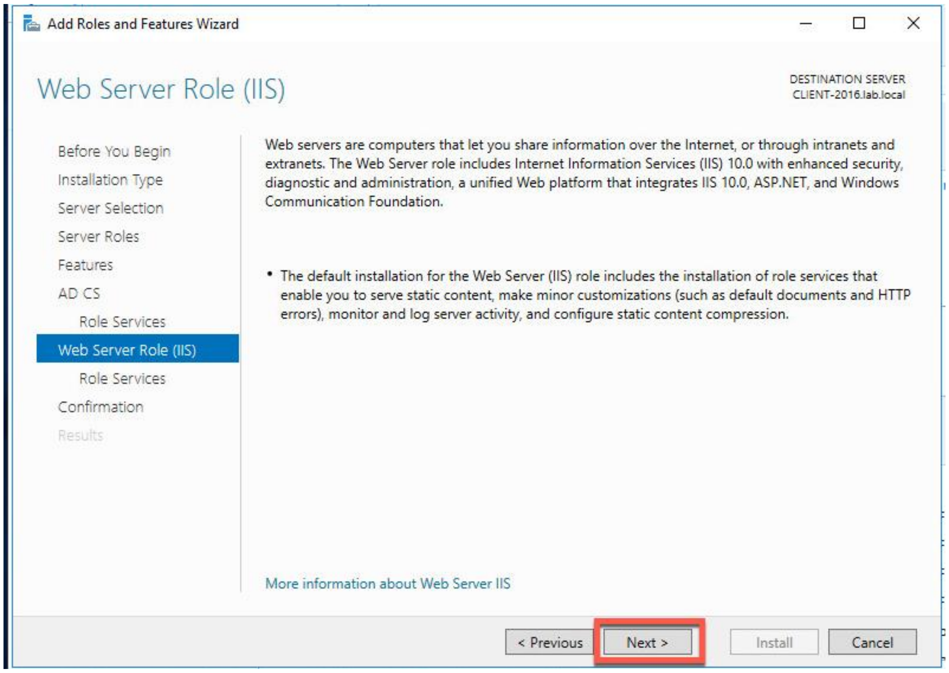
Select the role services to install for Active Directory Certificate Services

Role services

- ☑ Certification Authority
- ☐ Certificate Enrollment Policy Web Service
- ☐ Certificate Enrollment Web Service
- ☑ Certification Authority Web Enrollment
- ☐ Network Device Enrollment Service
- ☑ Online Responder

Description

Online Responder makes certificate revocation checking data accessible to clients in complex network environments.



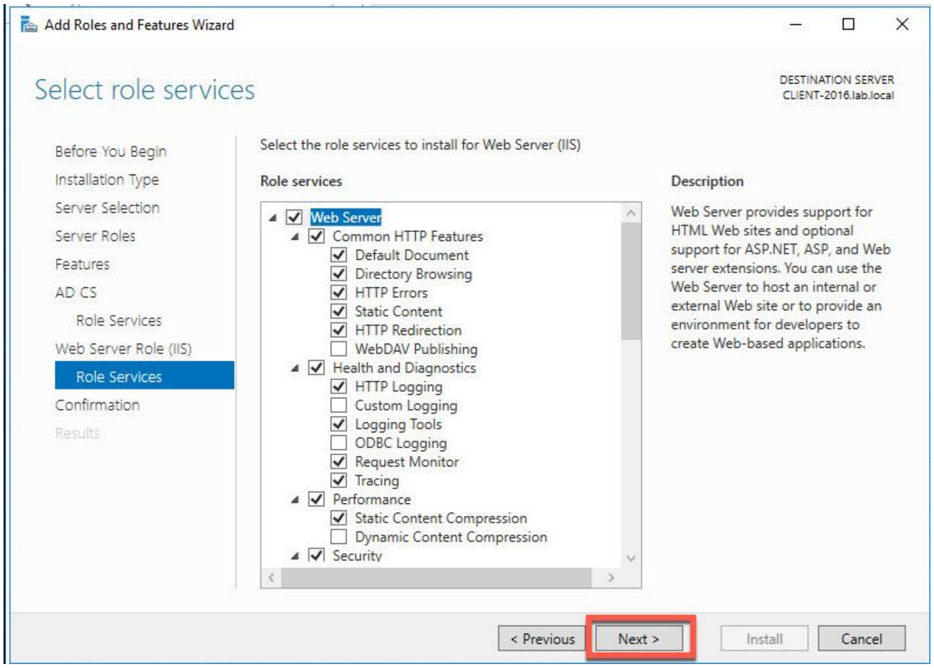
Web Server Role (IIS)

DESTINATION SERVER
CLIENT-2016.lab.local

Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.NET, and Windows Communication Foundation.

- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

More information about Web Server IIS



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
CLIENT-2016.lab.local

Select the role services to install for Web Server (IIS)

Role services

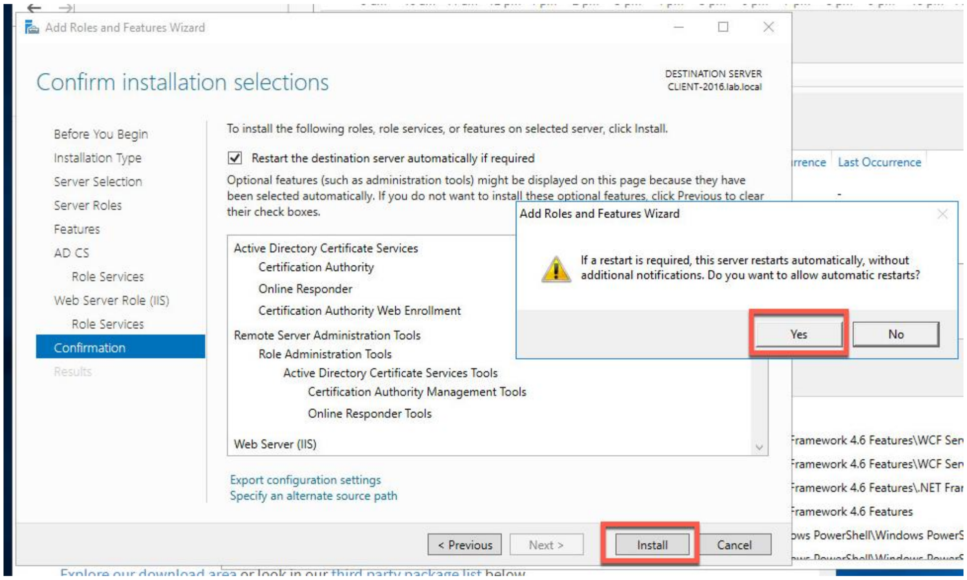
- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - ☑ HTTP Redirection
    - □ WebDAV Publishing
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - □ Custom Logging
    - ☑ Logging Tools
    - □ ODBC Logging
    - ☑ Request Monitor
    - ☑ Tracing
  - ☑ Performance
    - ☑ Static Content Compression
    - □ Dynamic Content Compression
  - ☑ Security

Description

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

xi. In the confirmation window, select "*Restart the destination server automatically if required*" and click *Install*.

Note: Installation begins but the server will reboot. Installation finishes after the reboot.



Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
CLIENT-2016.lab.local

To install the following roles, role services, or features on selected server, click Install.

☑ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Certificate Services
    Certification Authority
    Online Responder
    Certification Authority Web Enrollment
Remote Server Administration Tools
    Role Administration Tools
        Active Directory Certificate Services Tools
            Certification Authority Management Tools
            Online Responder Tools
Web Server (IIS)

Export configuration settings
Specify an alternate source path

Add Roles and Features Wizard

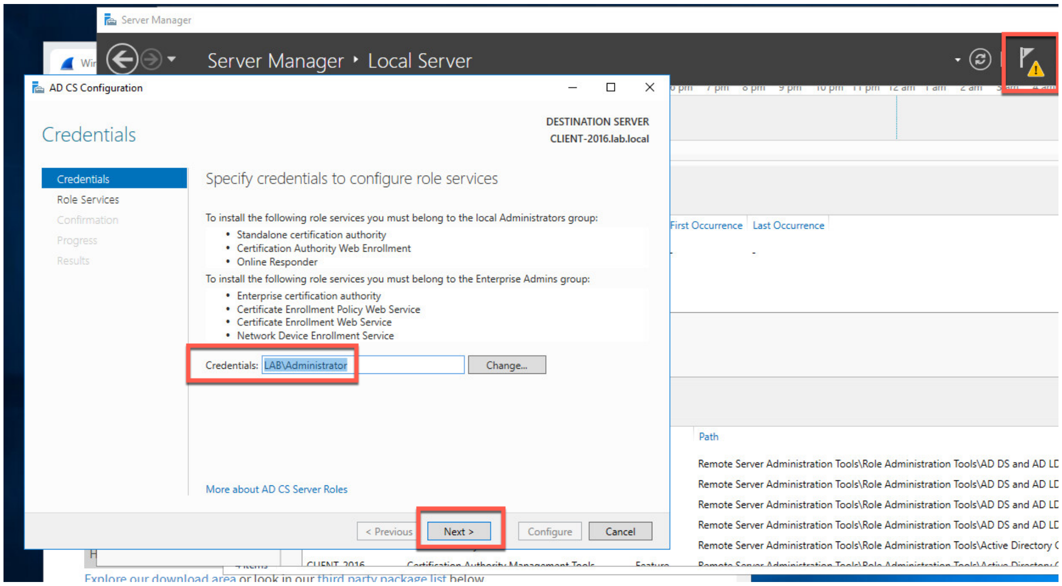
If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts?

xii. The Windows server (student desktop) will reboot and you will be disconnected for a time.

xiii. Click *Close* on the Add Roles and Features Wizard window.

xiv. Click the Warning notification in the Server Manager and click "*Configure Active Directory Certificate Services*" on the destination server.

xv. In the AD CS Configuration window, click *Next* to accept the default credential user.



Credentials

DESTINATION SERVER
CLIENT-2016.lab.local

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

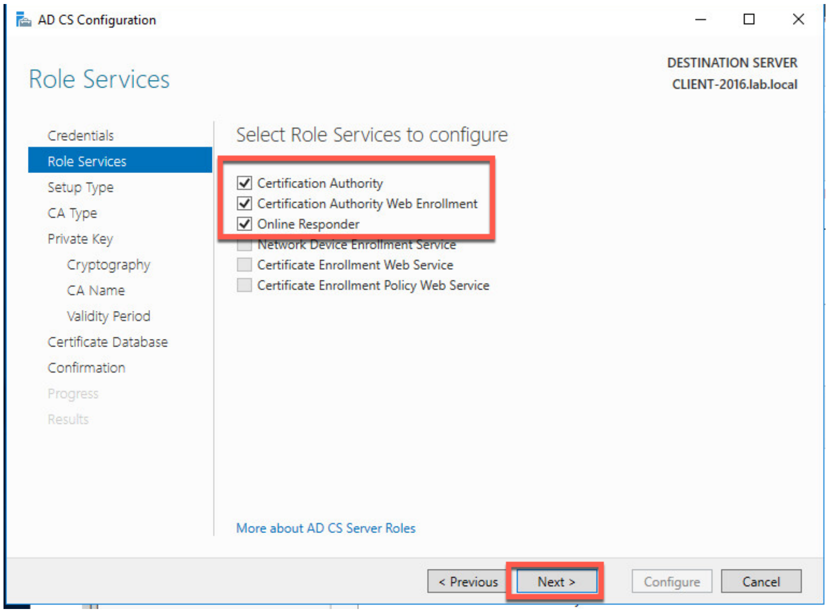
- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: LAB\Administrator

xvi. In the Role Services window, select Certification Authority, *Certification Authority Web Enrollment, Online Responder* and click *Next*.



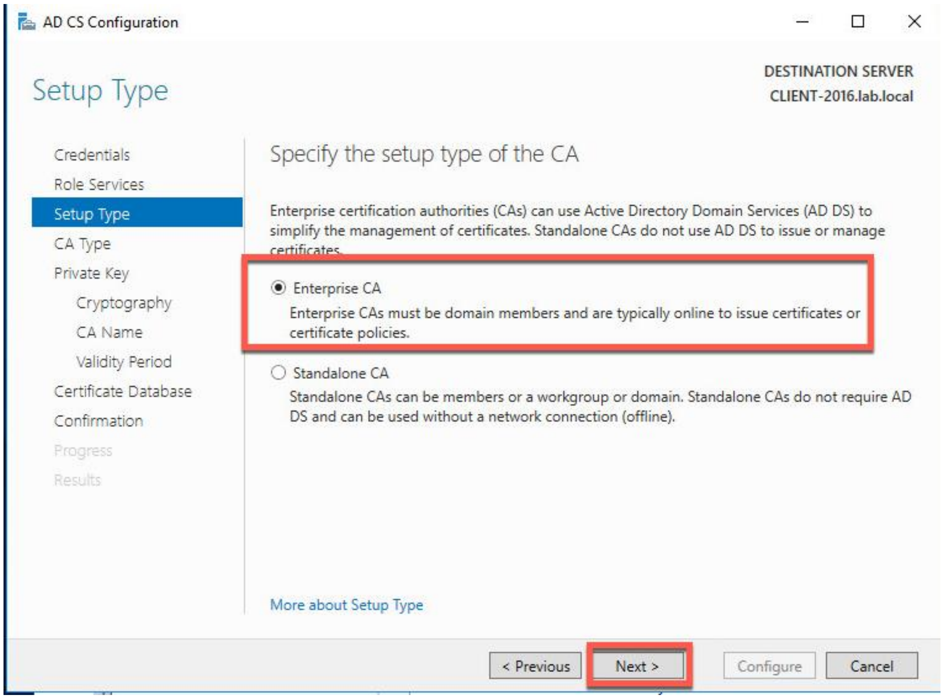
Role Services

DESTINATION SERVER
CLIENT-2016.lab.local

Select Role Services to configure

☑ Certification Authority
☑ Certification Authority Web Enrollment
☑ Online Responder
☐ Network Device Enrollment Service
☐ Certificate Enrollment Web Service
☐ Certificate Enrollment Policy Web Service

xvii. Select *Enterprise CA* (not Standalone CA) and click *Next*.



AD CS Configuration

DESTINATION SERVER
CLIENT-2016.lab.local

Setup Type

Specify the setup type of the CA

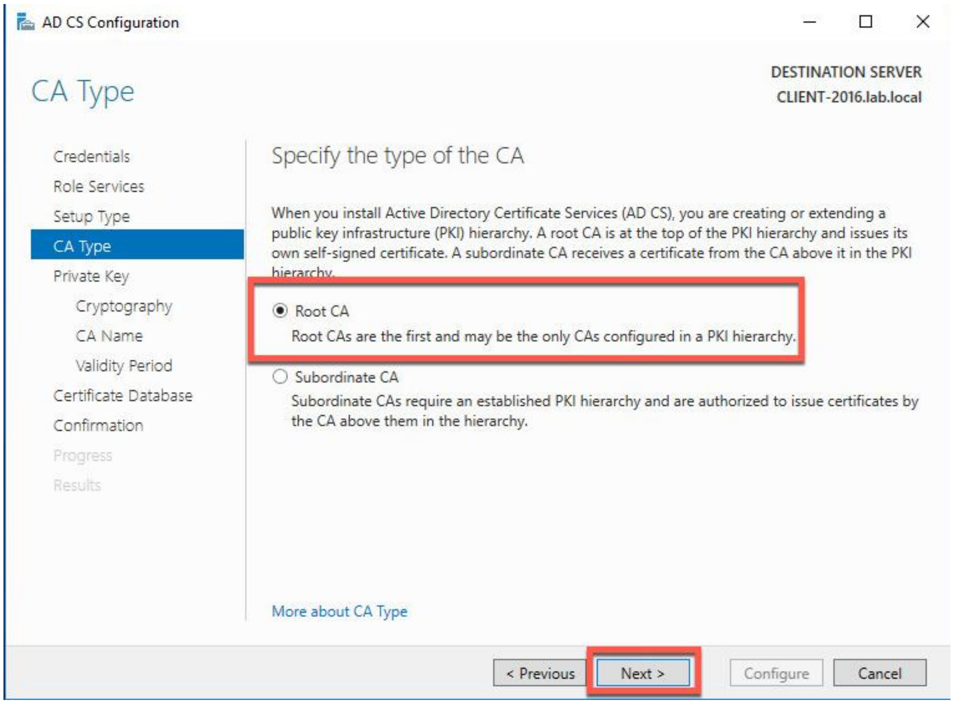
Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

● Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

○ Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

More about Setup Type

xviii. Select *Root CA* and click *Next*.



AD CS Configuration

DESTINATION SERVER
CLIENT-2016.lab.local

CA Type

Specify the type of the CA

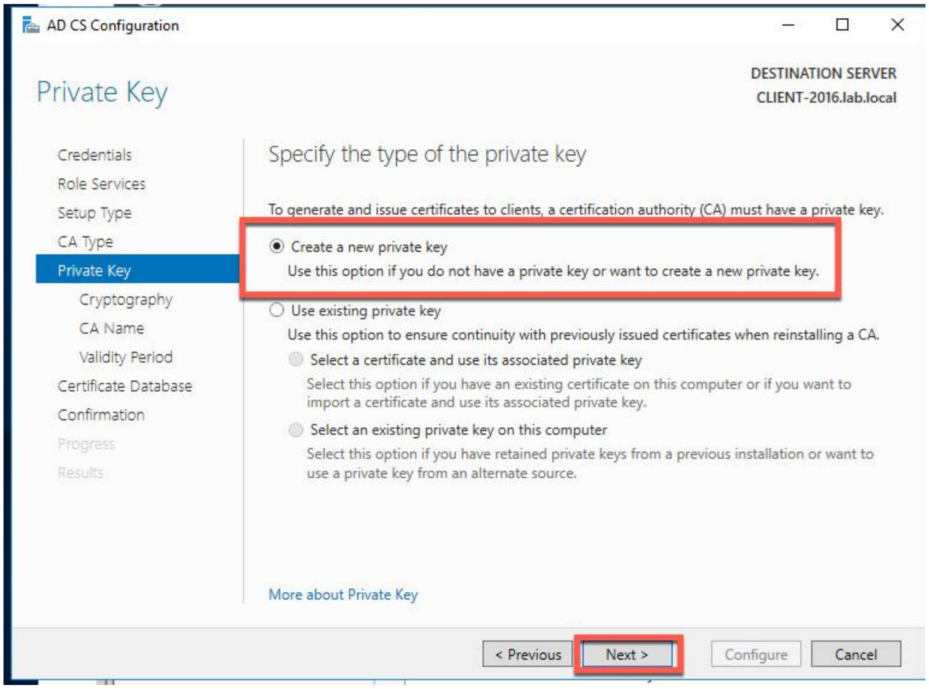
When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

● Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

○ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

More about CA Type

xix. Select *Create a new private key* and click *Next*.



AD CS Configuration

Private Key

DESTINATION SERVER
CLIENT-2016.lab.local

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

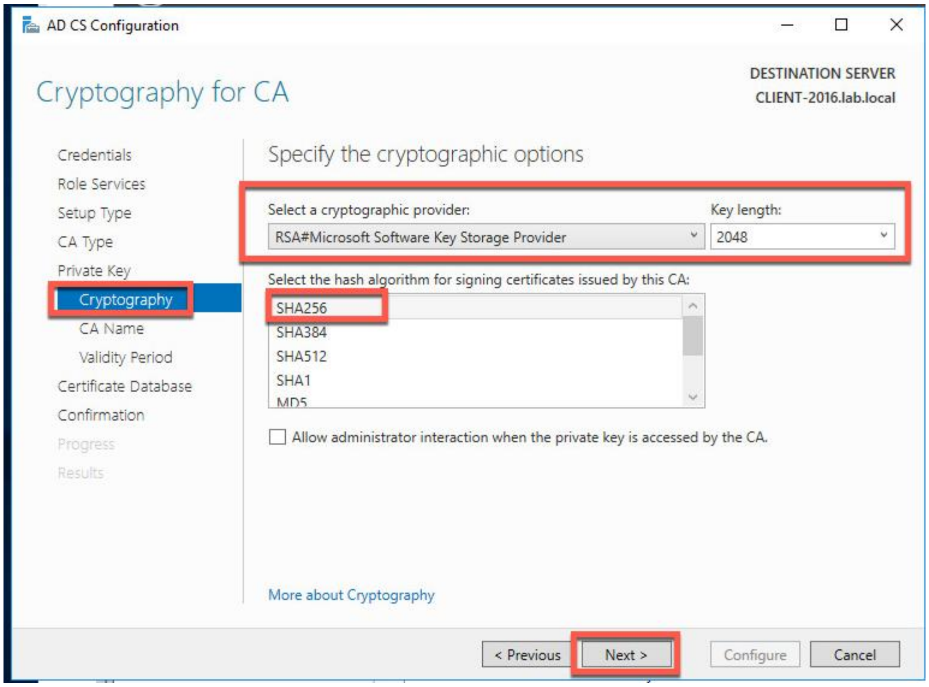
● Create a new private key
Use this option if you do not have a private key or want to create a new private key.

○ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

○ Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

xix. Leave the default RSA 2048 but select *SHA256* and click *Next*.



AD CS Configuration

Cryptography for CA

DESTINATION SERVER
CLIENT-2016.lab.local

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

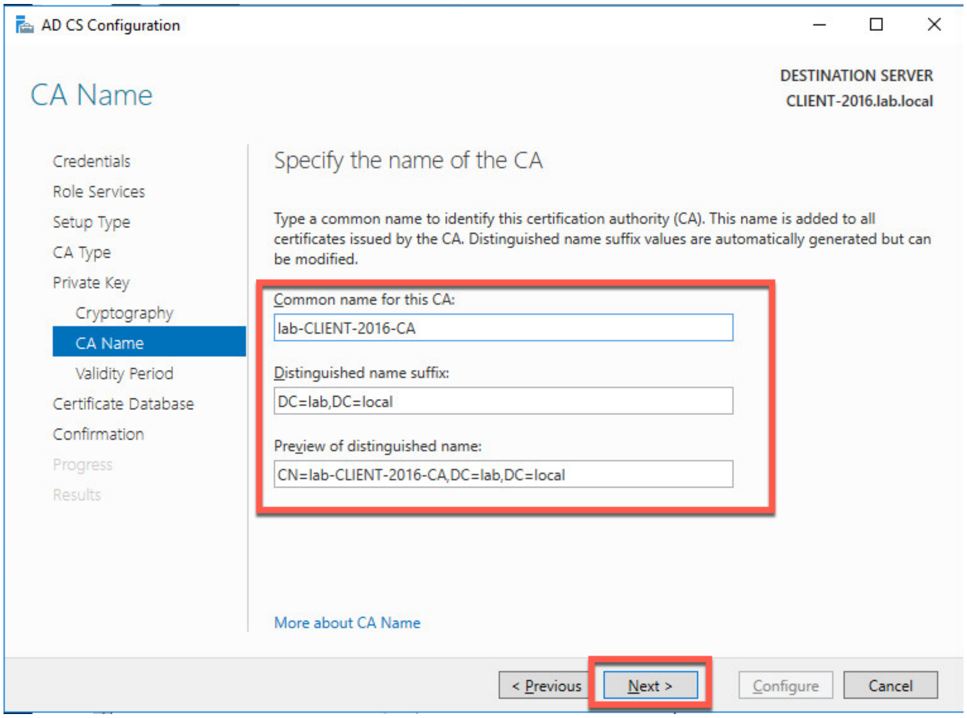
Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1
MD5

□ Allow administrator interaction when the private key is accessed by the CA.

xx. Leave the default CA Name and click *Next*.



AD CS Configuration

DESTINATION SERVER
CLIENT-2016.lab.local

CA Name

Specify the name of the CA

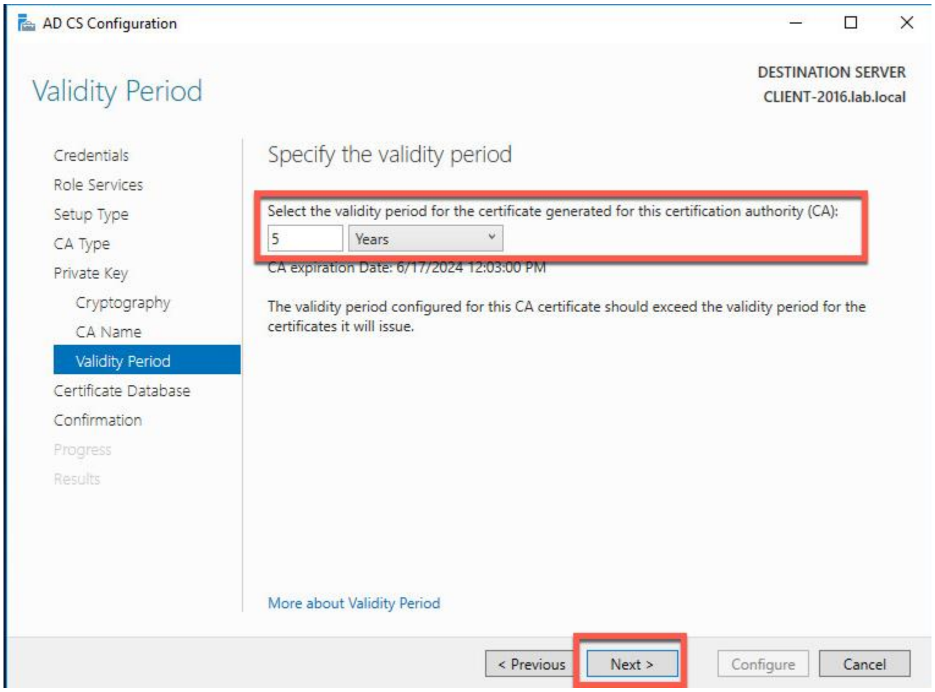
Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:
lab-CLIENT-2016-CA

Distinguished name suffix:
DC=lab,DC=local

Preview of distinguished name:
CN=lab-CLIENT-2016-CA,DC=lab,DC=local

xxi. Leave the default validity period and click *Next*.



AD CS Configuration

DESTINATION SERVER
CLIENT-2016.lab.local

Validity Period

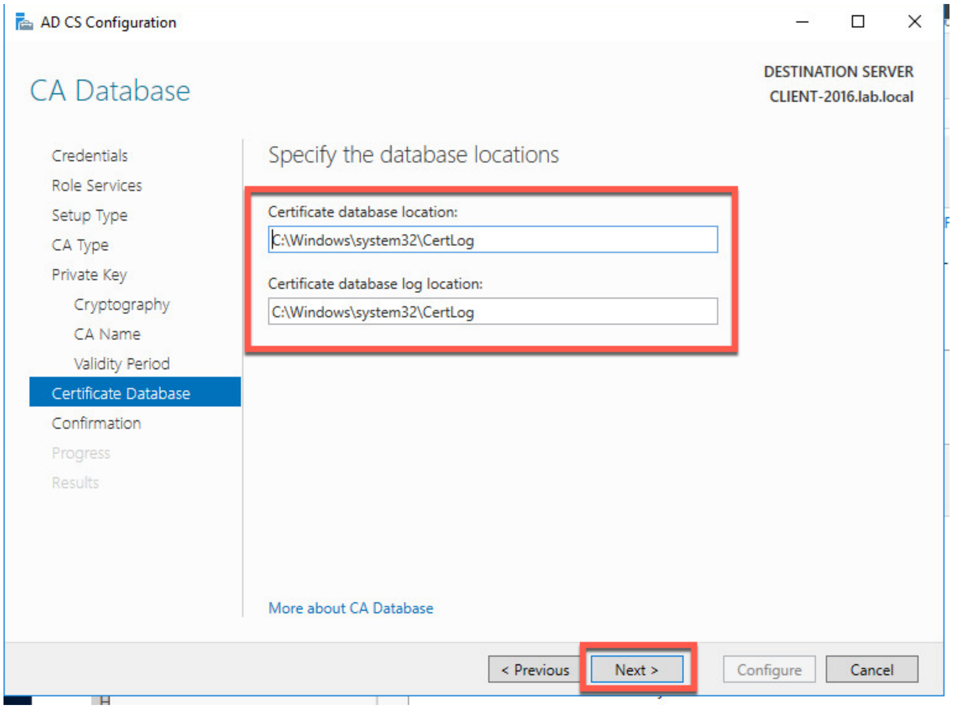
Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):
5 Years

CA expiration Date: 6/17/2024 12:03:00 PM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

xxii. Leave the default database locations and click *Next*.



AD CS Configuration

CA Database

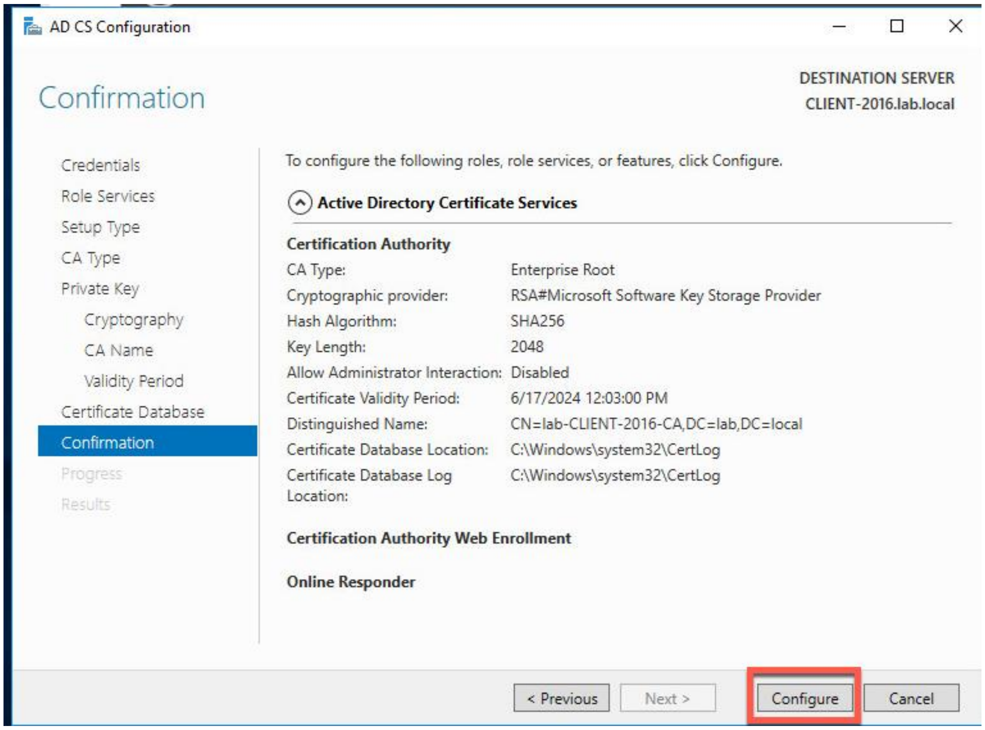
DESTINATION SERVER
CLIENT-2016.lab.local

Specify the database locations

Certificate database location: C:\Windows\system32\CertLog

Certificate database log location: C:\Windows\system32\CertLog

xxiii. Click *Configure*.



AD CS Configuration

Confirmation

DESTINATION SERVER
CLIENT-2016.lab.local

To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

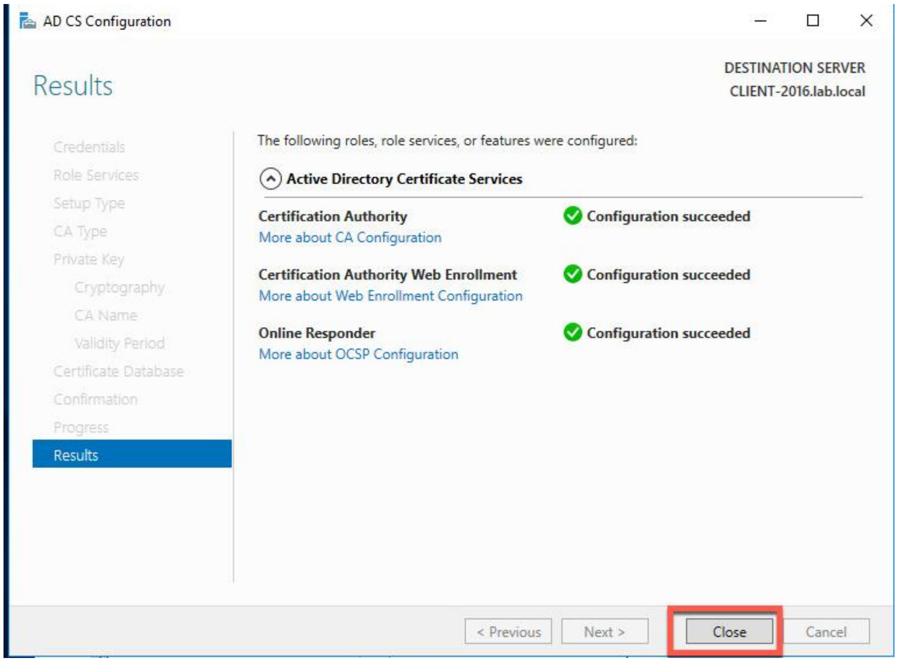
Certification Authority

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	6/17/2024 12:03:00 PM
Distinguished Name:	CN=lab-CLIENT-2016-CA,DC=lab,DC=local
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

Certification Authority Web Enrollment

Online Responder

xxiv. View the success status and click *Close*.



AD CS Configuration

DESTINATION SERVER
CLIENT-2016.lab.local

Results

The following roles, role services, or features were configured:

Active Directory Certificate Services

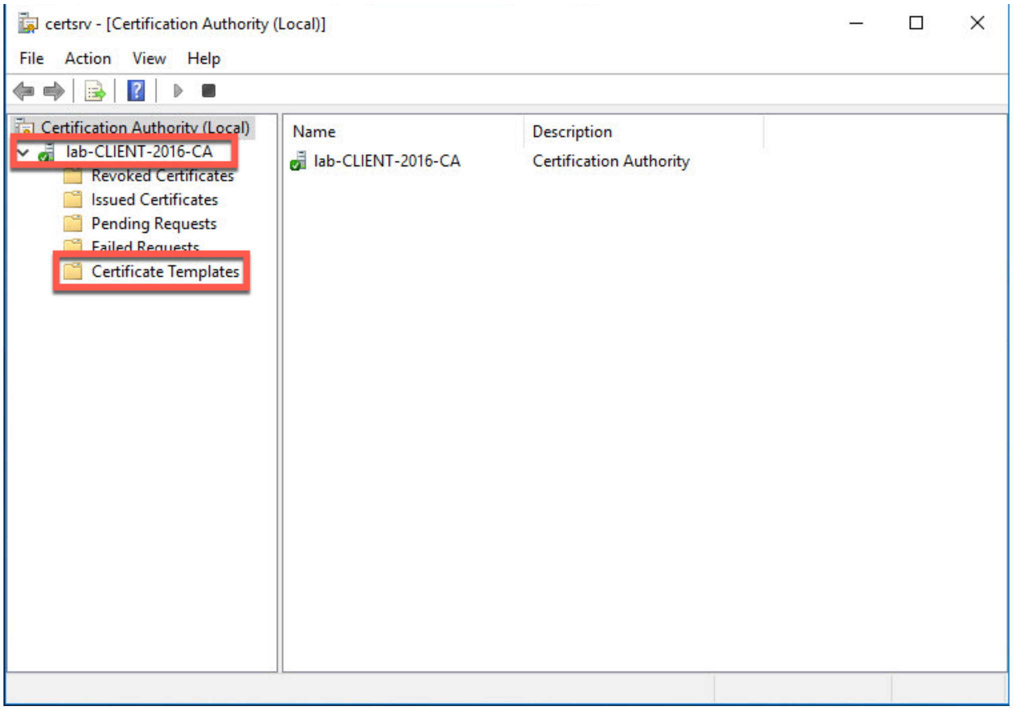
Certification Authority — Configuration succeeded
More about CA Configuration

Certification Authority Web Enrollment — Configuration succeeded
More about Web Enrollment Configuration

Online Responder — Configuration succeeded
More about OCSP Configuration

xxv. In Server Manager go to *Tools>Administrative Tools > Certification Authority.*

xxvi. Click *lab-CLIENT-2016-CA* (or what your host is).



certsrv - [Certification Authority (Local)]

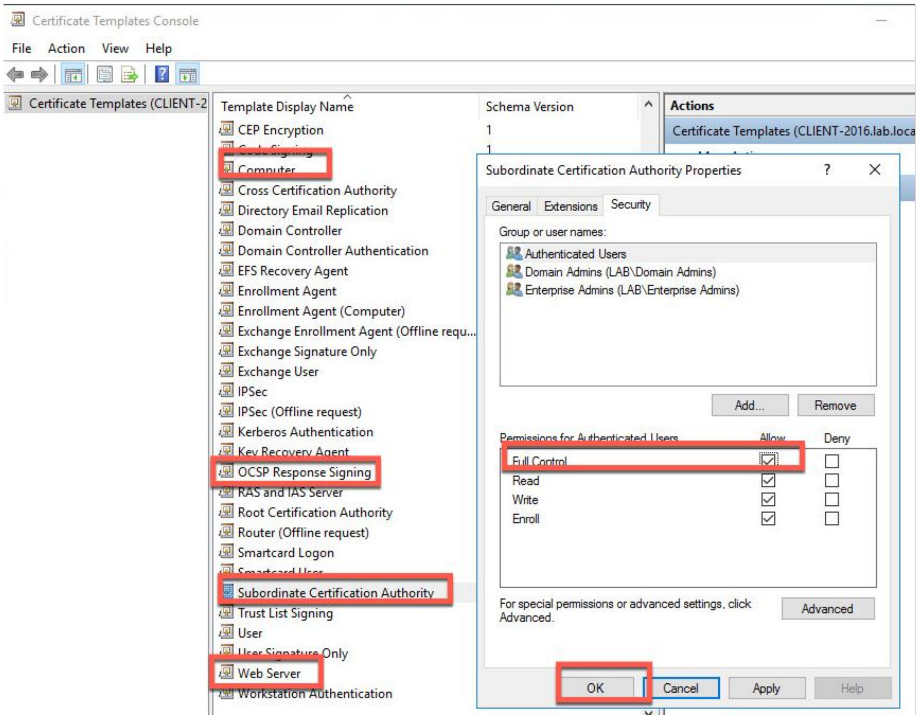
Name	Description
lab-CLIENT-2016-CA	Certification Authority

xxvii. Right-click *Certificate Templates* and select *Manage* to open the MMC.

xxviii. Right-click *Subordinate Certification Authority* and select *Properties*.

xxix. Click the *Security tab*.

xxx. Select *Full Control* and click *OK*.



Group or user names:

- Authenticated Users
- Domain Admins (LAB\Domain Admins)
- Enterprise Admins (LAB\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	☑	☐
Read	☑	☐
Write	☑	☐
Enroll	☑	☐

For special permissions or advanced settings, click Advanced.

xxxi. Repeat for the templates Computer, OCSP Response Signing, Web Server.

xxxii. *Close* the open windows.

xxxiii. You should be able to open Chrome and browse to **localhost/certsrv** and issue a certificate.

5.1.11 Log in as “**lab-user**”:

Log in as the lab-user using the password you set up for this user (**Pal0Alt0**) and start installing the applications listed below.

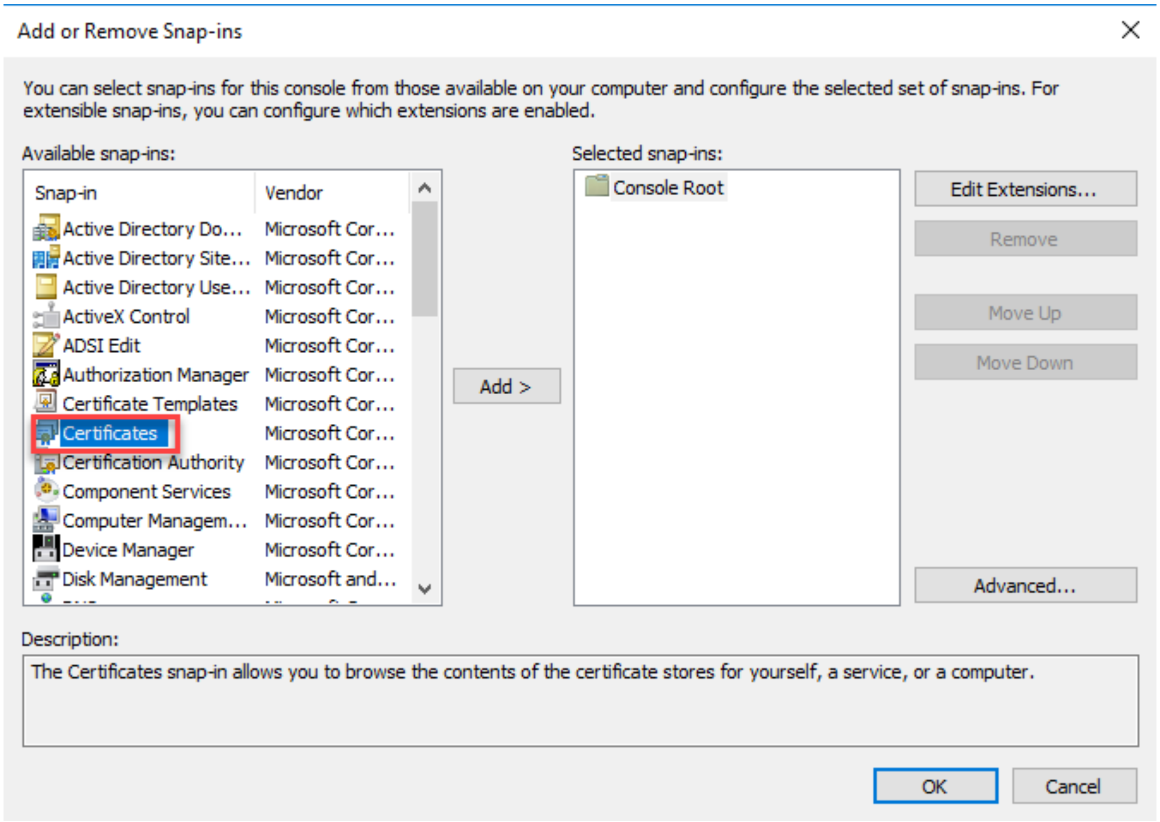
Create a certificate management shortcut on the desktop.

Right click the window pane (located on the bottom left of the screen) and type select Run.

Enter mmc into the Run text box and press Enter.

Click Yes

In Console1 dialog box select File / Add or Remove Snap-ins and select certificates



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...

Selected snap-ins:

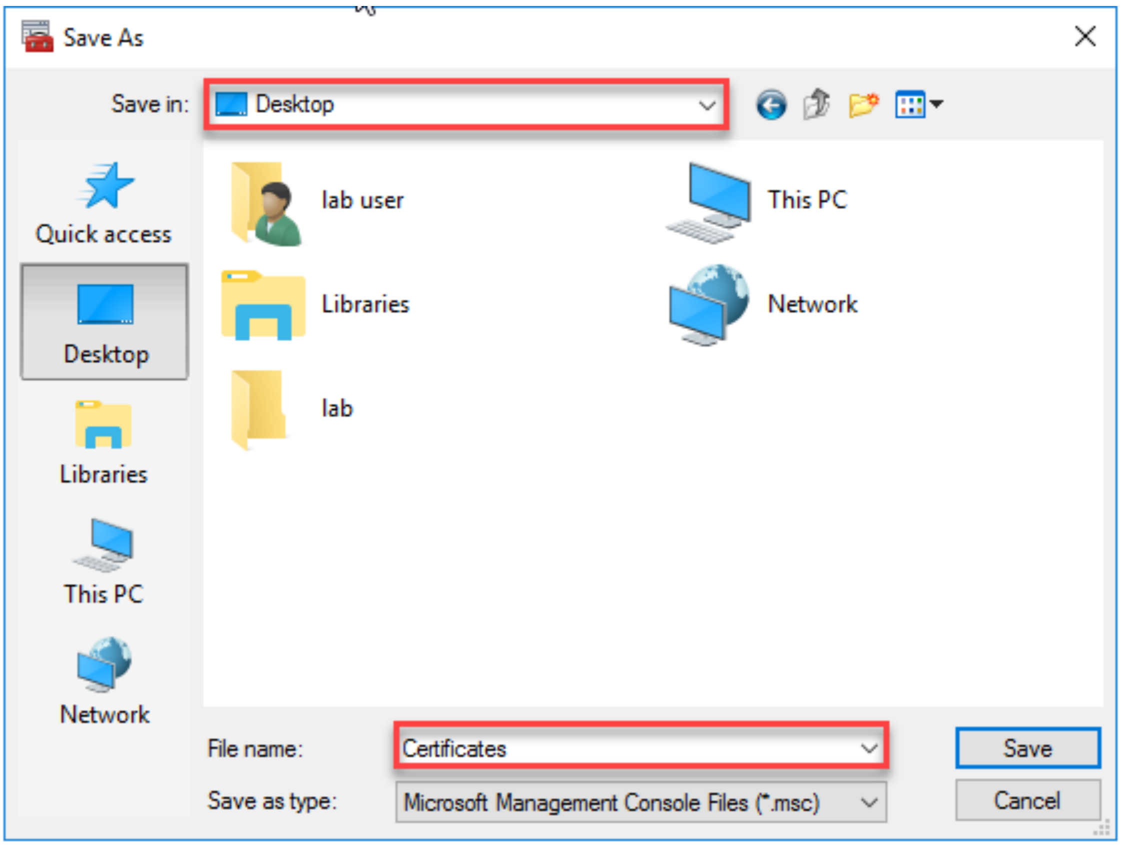
Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Accept the defaults and click finish.

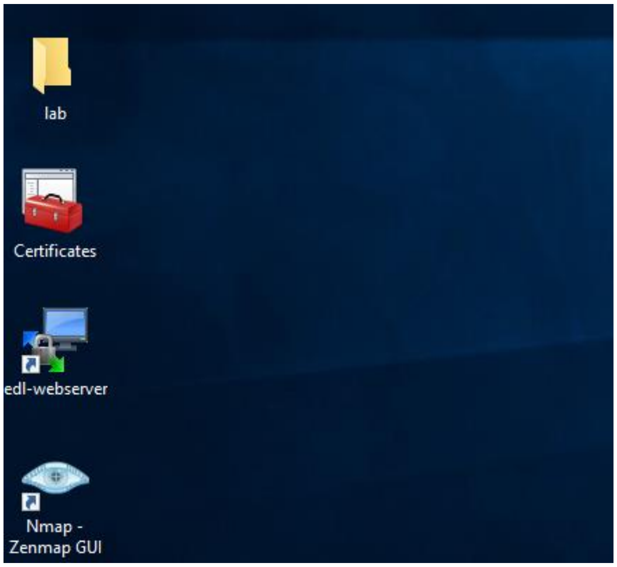
Go to File Save As and save this certificate mmc to the desktop with the name Certificates.



File name: Certificates

Save as type: Microsoft Management Console Files (*.msc)

Your desktop should now show the following certificate mmc

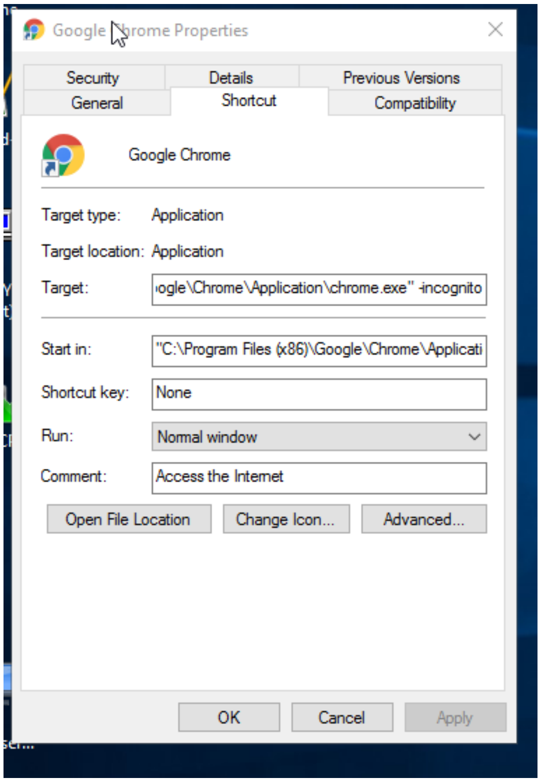


5.1.12 Install Google Chrome:

Due to the enhanced security default configuration of Microsoft Internet installer, it is easier to install the Google chrome browser via Windows PowerShell.

Here is a url ink to a site with PowerShell install script: https://www.ryadel.com/en/install-google-chrome-with-powershell-script/

After installing, Chrome, create a Desktop shortcut. Right click the Google Chrome shortcut and select properties. In the Google Chrome Properties dialog box, enter "-incognito" right after …\chrome.exe" and click OK to close the dialog box. Chrome will now open up in incognito mode by default.



Target type: Application

Target location: Application

Target: ›ogle\Chrome\Application\chrome.exe" -incognito

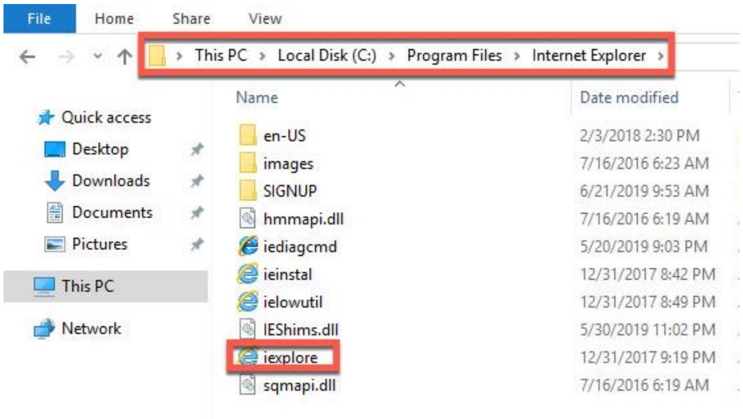
Start in: "C:\Program Files (x86)\Google\Chrome\Applicati

Shortcut key: None

Run: Normal window

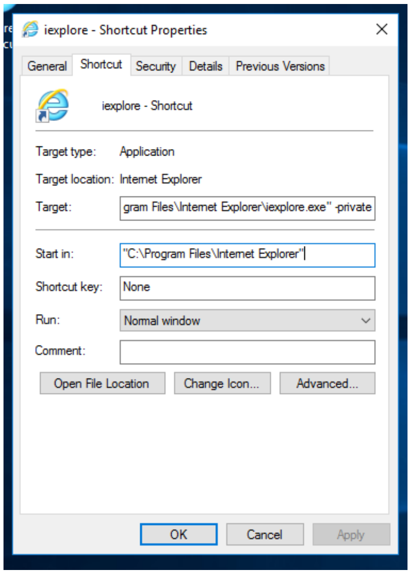
Comment: Access the Internet

Create a Desktop shortcut for Internet Explorer by dragging and dropping C:\Program Files\Internet Explorer\iexplore onto your Desktop. Right click the Internet Explorer shortcut and in the target text box enter "-private" after …\iexplore.exe". Internet Explorer will now open up in private window mode by default.



This PC > Local Disk (C:) > Program Files > Internet Explorer >

Name	Date modified
en-US	2/3/2018 2:30 PM
images	7/16/2016 6:23 AM
SIGNUP	6/21/2019 9:53 AM
hmmapi.dll	7/16/2016 6:19 AM
iediagcmd	5/20/2019 9:03 PM
ieinstal	12/31/2017 8:42 PM
ielowutil	12/31/2017 8:49 PM
IEShims.dll	5/30/2019 11:02 PM
iexplore	12/31/2017 9:19 PM
sqmapi.dll	7/16/2016 6:19 AM



iexplore - Shortcut

Target type: Application

Target location: Internet Explorer

Target: gram Files\Internet Explorer\iexplore.exe" -private

Start in: "C:\Program Files\Internet Explorer"

Shortcut key: None

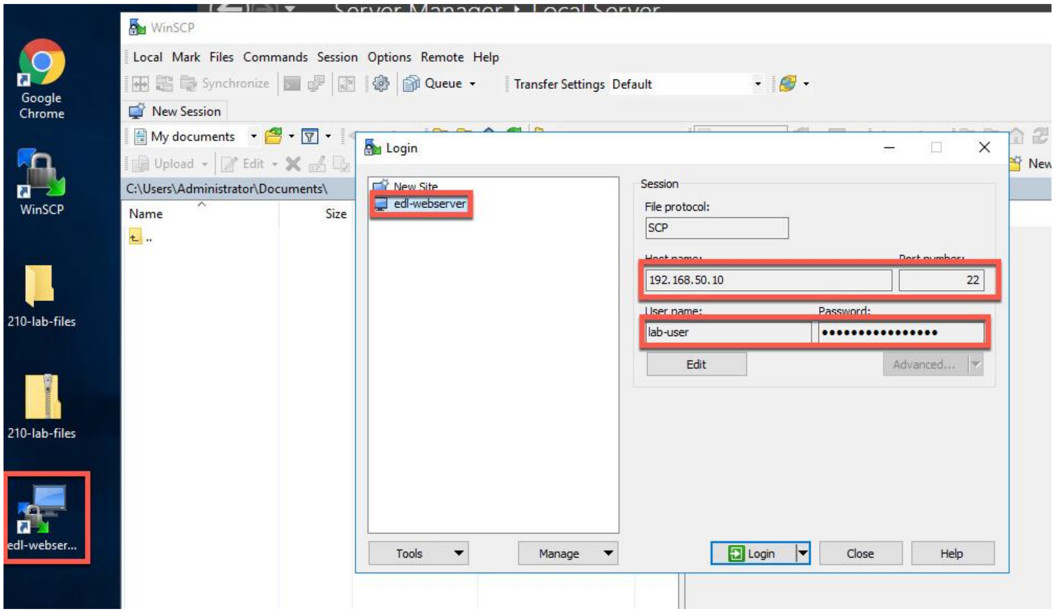
Run: Normal window

Comment:

5.1.13 Install WinSCP:

Download and install WinSCP from https://winscp.net .
Create a shortcut on the desktop with one preconfigured entry for edl-web server with the following attributes:

1. File protocol: *SCP*
2. Host name: **192.168.50.10**
3. Lab name: **lab-user**
4. Password: **paloalto**
5. Name: **edl-webserver**



File protocol: SCP

Host name: 192.168.50.10 Port number: 22

User name: lab-user Password: ••••••••••••••••

5.1.14 Install WireShark:

Install WireShark from https://www.wireshark.org and turn off Wireshark updates by following the directions below.

1. Go to Edit > Preferences... > Advanced. Search for “**gui**”.
2. Find the option *gui.update.enabled*.
3. Double-click the value “*TRUE*” to change it to “*FALSE*”
4. Click *OK* to close the Preferences dialog.
5. Close the Wireshark program.

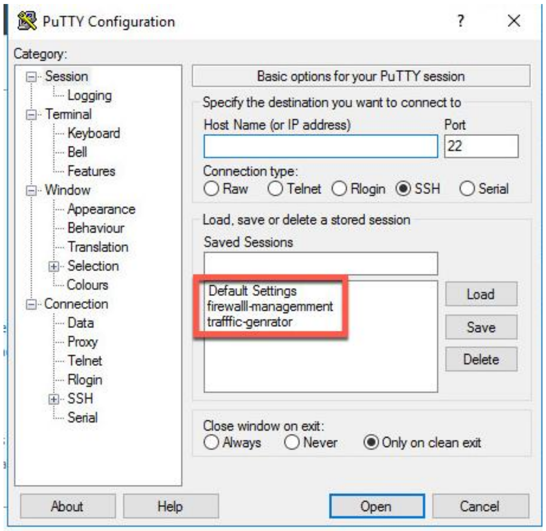
5.1.15 Install Zenmap/nmap:

Download and install nmap from https://nmap.org/download.html.

5.1.16 Install PuTTY:

Go to https://www.putty.org and download and install PuTTY.
Create a shortcut on your desktop.
Open PuTTY and create 2 preconfigured SSH entries:

i. “**firewall management**” with IP address: **192.168.1.254**
ii. “**traffic-generator**” with IP address: **192.168.50.10**



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

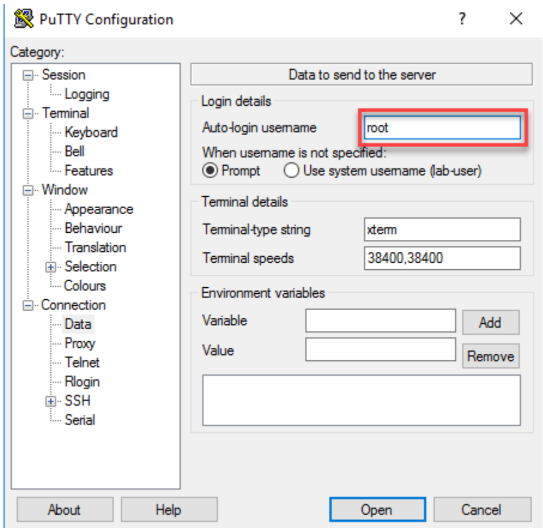
Load, save or delete a stored session

Saved Sessions

Default Settings
firewalll-management
trafffic-genrator

Close window on exit: ○ Always ○ Never ● Only on clean exit

iii. To add a predefined user to Putty for traffic-generator. Configure the following:
Go to *Connection* -> *Data* and specify the username with that you want to log in to your SSH server under Auto-login username. In this case use **root**: Then go to Session again.



PuTTY Configuration

Data to send to the server

Login details

Auto-login username: root

When username is not specified: ● Prompt ○ Use system username (lab-user)

Terminal details

Terminal-type string: xterm

Terminal speeds: 38400,38400

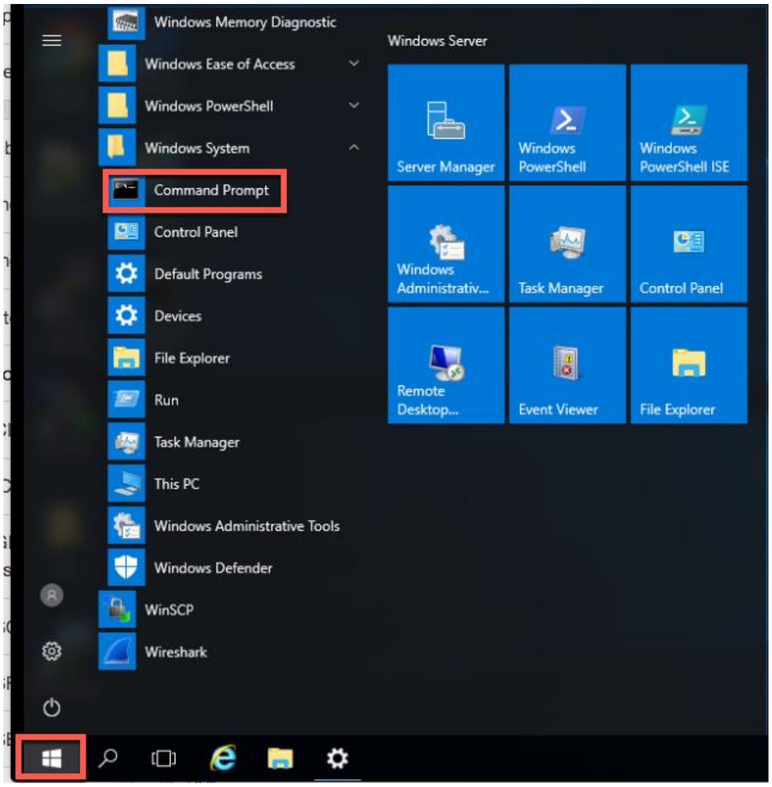
Environment variables

Variable:

Value:

5.1.17 Create Desktop shortcut for the command prompt.

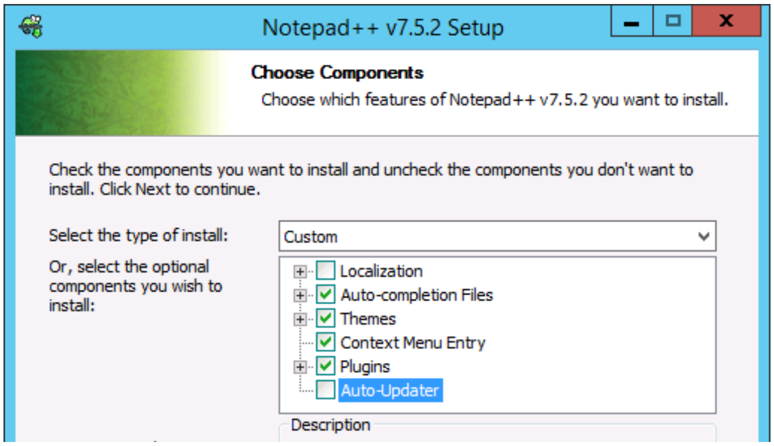
Click the windowpane in the bottom left corner of your Desktop and go to Windows System>Command Prompt. Drag the Command Prompt icon to your desktop.



5.1.18 Install Notepad++:

Go to https://notepad-plus-plus.org and download and install the latest version.

i. On the first *Choose Components* page, accept the defaults *except* deselect Auto- Updater**.**


Notepad++ v7.5.2 Setup

Choose Components

Choose which features of Notepad++ v7.5.2 you want to install.

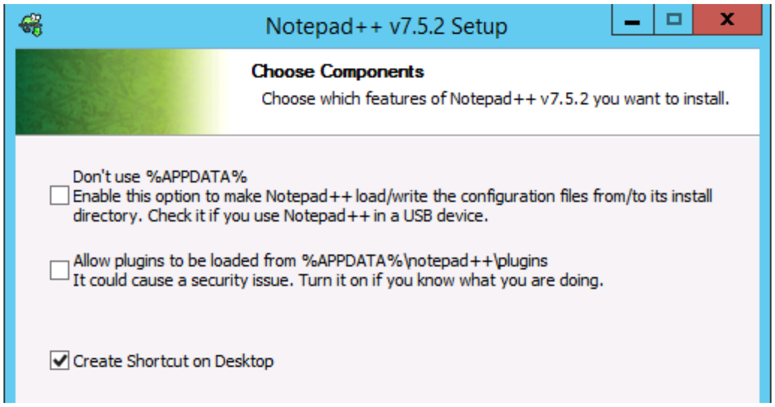
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Custom

Or, select the optional components you wish to install:

- □ Localization
- ☑ Auto-completion Files
- ☑ Themes
- ☑ Context Menu Entry
- ☑ Plugins
- □ Auto-Updater

ii. On the second *Choose Components* page, select to Create Shortcut on Desktop.



Choose Components

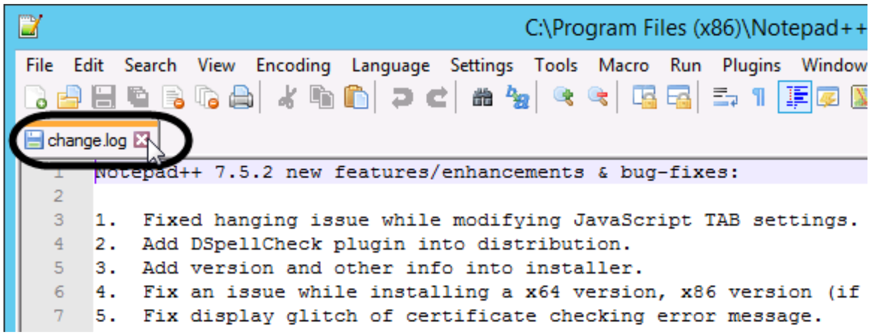
Choose which features of Notepad++ v7.5.2 you want to install.

☐ Don't use %APPDATA%
Enable this option to make Notepad++ load/write the configuration files from/to its install directory. Check it if you use Notepad++ in a USB device.

☐ Allow plugins to be loaded from %APPDATA%\notepad++\plugins
It could cause a security issue. Turn it on if you know what you are doing.

☑ Create Shortcut on Desktop

iii. After the installation is complete, launch the *Notepad*++ program and *close* the change.log tab. The default "new 1" tab will appear.



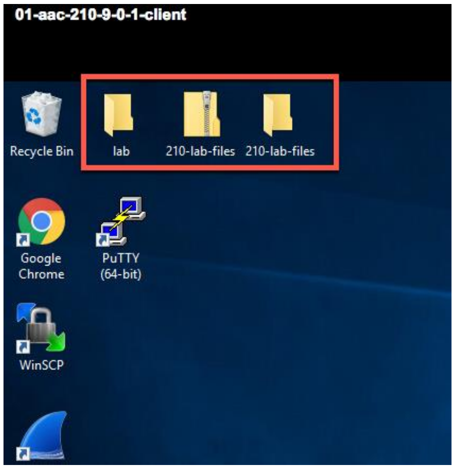
C:\Program Files (x86)\Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window
change.log

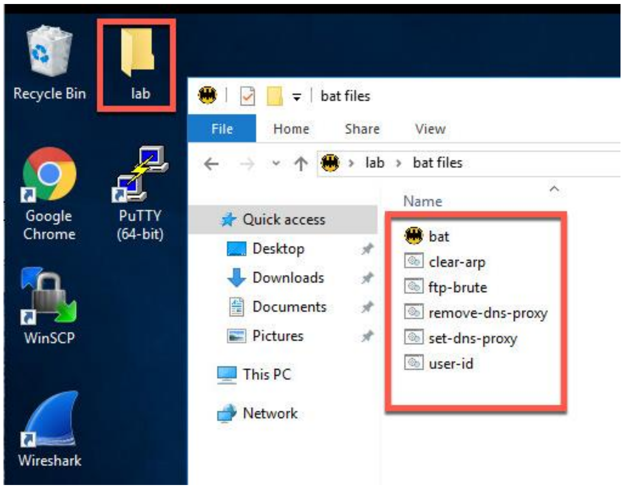
```
Notepad++ 7.5.2 new features/enhancements & bug-fixes:

1.  Fixed hanging issue while modifying JavaScript TAB settings.
2.  Add DSpellCheck plugin into distribution.
3.  Add version and other info into installer.
4.  Fix an issue while installing a x64 version, x86 version (if
5.  Fix display glitch of certificate checking error message.
```

5.1.19 Set up Lab Folder:

Download the 210-lab-files zip folder from the academy share to the server's desktop and extract the 210-lab-files folder on your desktop. In the 210-lab-files folder move the "lab" folder to the server's Desktop. The VMware Workstation ova/lab config share drive URL is posted in the following Cybersecurity Academy Moodle Courses: Configuration Infrastructure course, Cybersecurity Prevention and Countermeasures course, Firewall Essentials Configuration and Management course and the Optimizing Firewall Threat Prevention course.

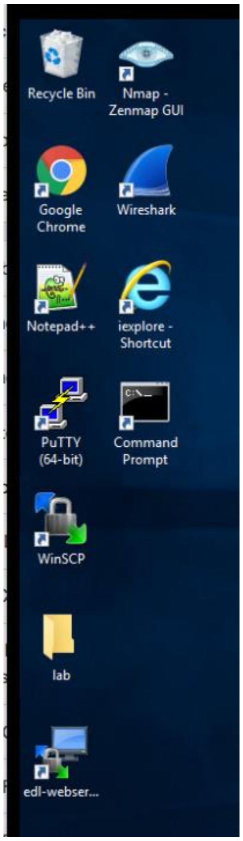
Delete the 210-lab-files zip folder and 210-lab-files folder so only the "lab" folder remains with the bat files remain on the Desktop.





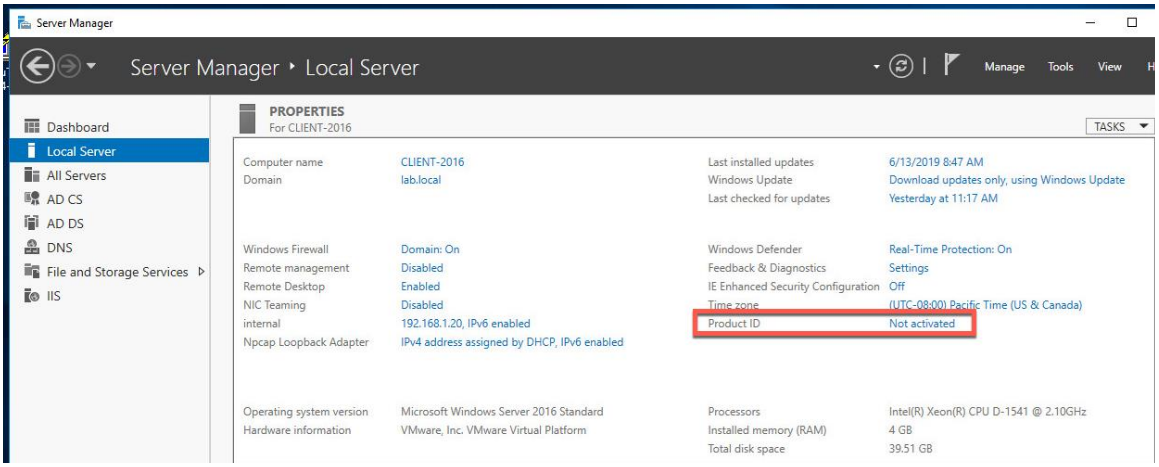
5.1.20 The “lab-user” Desktop and Licensing Your Server 2016:

After completing all your installations the lab-user’s desktop should have the have the following application shortcuts:



5.1.21 Google Chrome, PuTTY, WinSCP, Wireshark, Nmap-Zenmap GUI, WinSCP edl-webuser and Notepad++.

In Server Manager > Properties > Product ID click "*Not Activated*" and **enter** your institution's Microsoft account product ID to license your Server 2016.

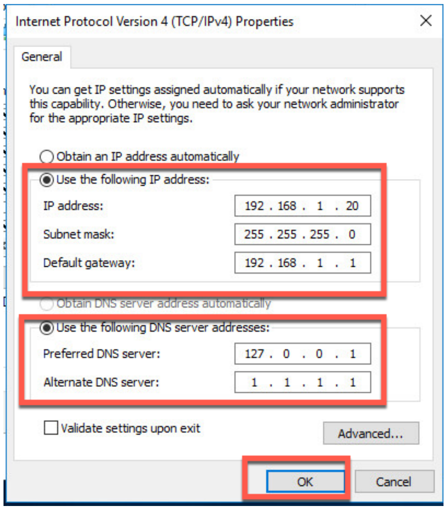


PROPERTIES
For CLIENT-2016

Computer name	CLIENT-2016	Last installed updates	6/13/2019 8:47 AM
Domain	lab.local	Windows Update	Download updates only, using Windows Update
		Last checked for updates	Yesterday at 11:17 AM
Windows Firewall	Domain: On	Windows Defender	Real-Time Protection: On
Remote management	Disabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	Off
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
internal	192.168.1.20, IPv6 enabled	Product ID	Not activated
Npcap Loopback Adapter	IPv4 address assigned by DHCP, IPv6 enabled		
Operating system version	Microsoft Windows Server 2016 Standard	Processors	Intel(R) Xeon(R) CPU D-1541 @ 2.10GHz
Hardware information	VMware, Inc. VMware Virtual Platform	Installed memory (RAM)	4 GB
		Total disk space	39.51 GB

5.1.22 Change the IP Address and Default Gateway the Server and Connect the Server to vmnet1:

Open the network adapter make the following changes:
IP Address: **192.168.1.20**
Subnet mask: **255.255.255.0**
Default gateway: **192.168.1.1**
Keep the *Primary DNS* server IP address as *127.0.0.1* and use either **1.1.1.1** or your *NAT'd VMnet8* default gateway address as the Alternate DNS Server.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 1 . 20
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1

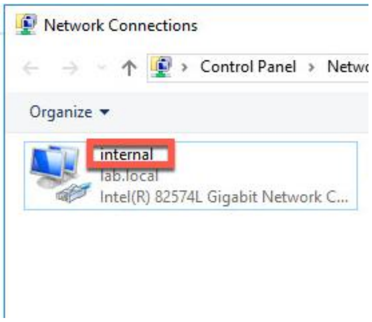
○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 127 . 0 . 0 . 1
Alternate DNS server: 1 . 1 . 1 . 1

□ Validate settings upon exit

5.1.23 Change the Name of the Network Adapter:

Rename your network adapter from the default name "Ethernet0" to the name "**internal**".



Network Connections

internal
lab.local
Intel(R) 82574L Gigabit Network C...

5.1.24 Baseline Snapshot Your Server 2016 VM:

Take a VMware Workstation snapshot of your virtual machine after completing all the above configurations and licensing it.

You can return to this snapshot if your virtual machine becomes corrupted and unusable.

License Firewall on VMware Workstation

6 License your VM-50 workstation appliance with provided AUTH code, check that your firewall correctly installs the licenses on your appliance and perform dynamic updates.

Note: If you have not already received a VM50 firewall license please ask your instructor.

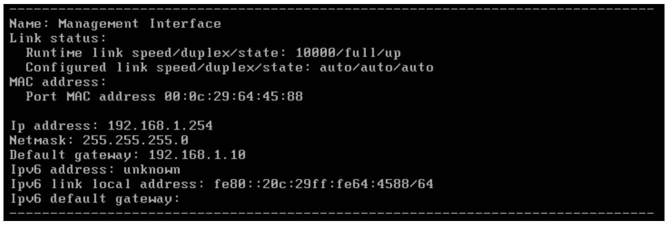
6.1.1 In VMware workstation PA-VM-9.0-PanOS-FW tab, select "*Power on this virtual machine*". Your VM-50 appliance will start the boot up process.

Note: This will take approximately 5 minutes. Make sure your VR virtual machine is powered on and connected to correct VMnets before attempting licensing.

The VR provides routing to the Internet for your VM-50 appliance which you will need to license your VM 50 appliance by connecting to the updates.paloaltonetworks.com server.

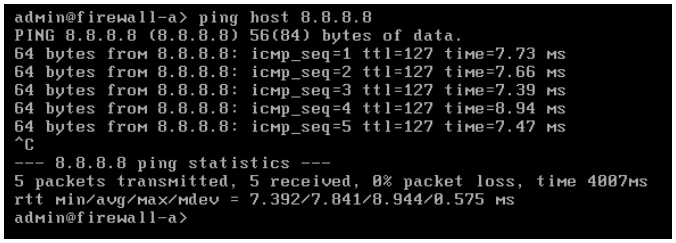
6.1.2 Log onto your firewall with username **admin** and password **admin**. Type the following command "**show interface management**" and click *enter*.

Note: Your IP address should match 192.168.1.254.



```
--------------------------------------------------------------------------------
Name: Management Interface
Link status:
  Runtime link speed/duplex/state: 10000/full/up
  Configured link speed/duplex/state: auto/auto/auto
MAC address:
  Port MAC address 00:0c:29:64:45:88

Ip address: 192.168.1.254
Netmask: 255.255.255.0
Default gateway: 192.168.1.10
Ipv6 address: unknown
Ipv6 link local address: fe80::20c:29ff:fe64:4588/64
Ipv6 default gateway:
--------------------------------------------------------------------------------
```

Also enter the following to verify connectivity: "**ping host 8.8.8.8**"



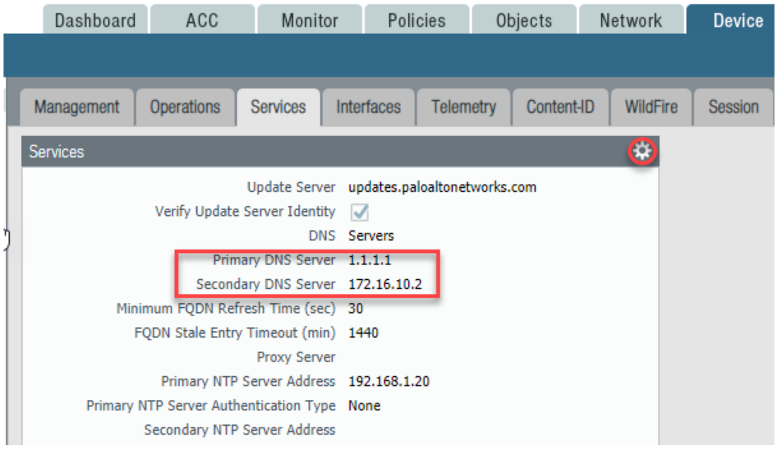
```
admin@firewall-a> ping host 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=7.73 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=7.66 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=7.39 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=8.94 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=7.47 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 7.392/7.841/8.944/0.575 ms
admin@firewall-a>
```

6.1.3 *Open* your host computer's Chrome browser and connect to your VM-50 Web-UI by entering **https://<vr_ext_ip_ens160_int>** in the host browser's URL. A privacy error will occur, click "*Advanced*" and then click "*Proceed to 192.168.1.254* (unsafe).

6.1.4 Log into your VM-50 appliance using username: “**admin**” and password: “**admin**”. Select the *Device* tab and on the left-hand side of Web-UI click *Setup*.

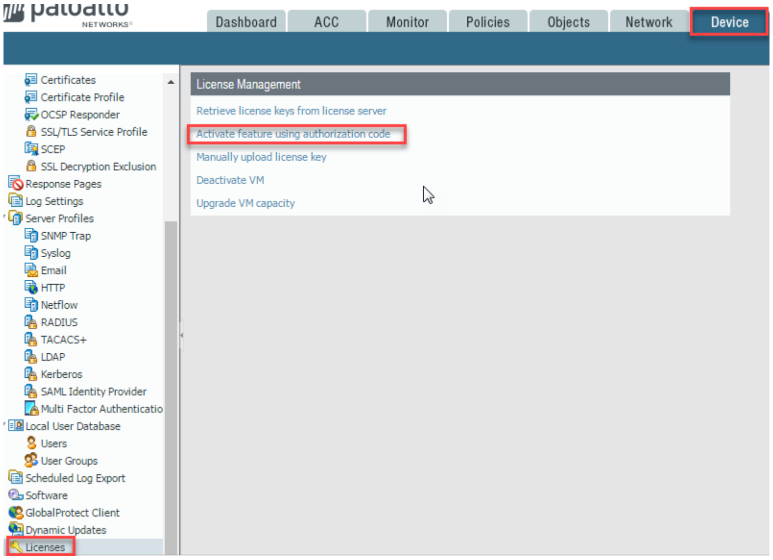
6.1.5 Now select the *Services* tab and then click the *settings* icon on right hand side.

6.1.6 In the Services dialog box set the Primary DNS Server to 1.1.1.1 or the gateway address for your vmnet8. If the network ID of your vmnet8 is 172.16.10.0/24 then the vmnet8 default gateway address would be 172.16.10.2 as shown in screenshot below.

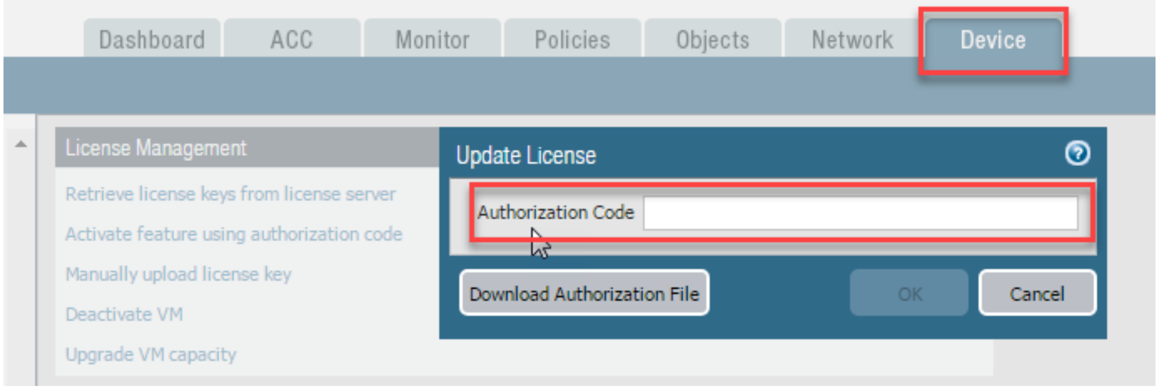


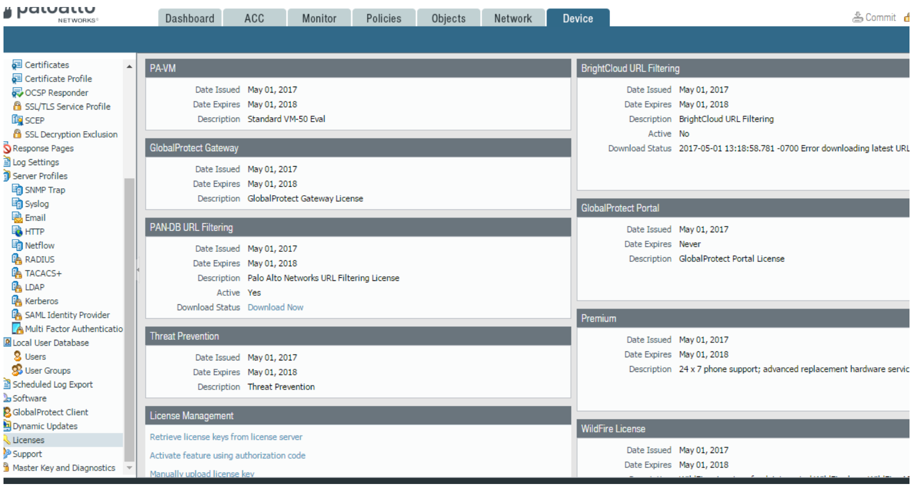
Update Server updates.paloaltonetworks.com
Verify Update Server Identity ☑
DNS Servers
Primary DNS Server 1.1.1.1
Secondary DNS Server 172.16.10.2
Minimum FQDN Refresh Time (sec) 30
FQDN Stale Entry Timeout (min) 1440
Proxy Server
Primary NTP Server Address 192.168.1.20
Primary NTP Server Authentication Type None
Secondary NTP Server Address

6.1.7 In *Device > Licenses* under “*License Management*”, click “*Activate features using authorization code*”.



6.1.8 **Enter** the authorization code provided to you by your academy representative, click OK and click OK after receiving warning. Your firewall will now reboot to load your licenses.





PA-VM
Date Issued May 01, 2017
Date Expires May 01, 2018
Description Standard VM-50 Eval

GlobalProtect Gateway
Date Issued May 01, 2017
Date Expires May 01, 2018
Description GlobalProtect Gateway License

PAN-DB URL Filtering
Date Issued May 01, 2017
Date Expires May 01, 2018
Description Palo Alto Networks URL Filtering License
Active Yes
Download Status Download Now

Threat Prevention
Date Issued May 01, 2017
Date Expires May 01, 2018
Description Threat Prevention

BrightCloud URL Filtering
Date Issued May 01, 2017
Date Expires May 01, 2018
Description BrightCloud URL Filtering
Active No
Download Status 2017-05-01 13:18:58.781 -0700 Error downloading latest URL

GlobalProtect Portal
Date Issued May 01, 2017
Date Expires Never
Description GlobalProtect Portal License

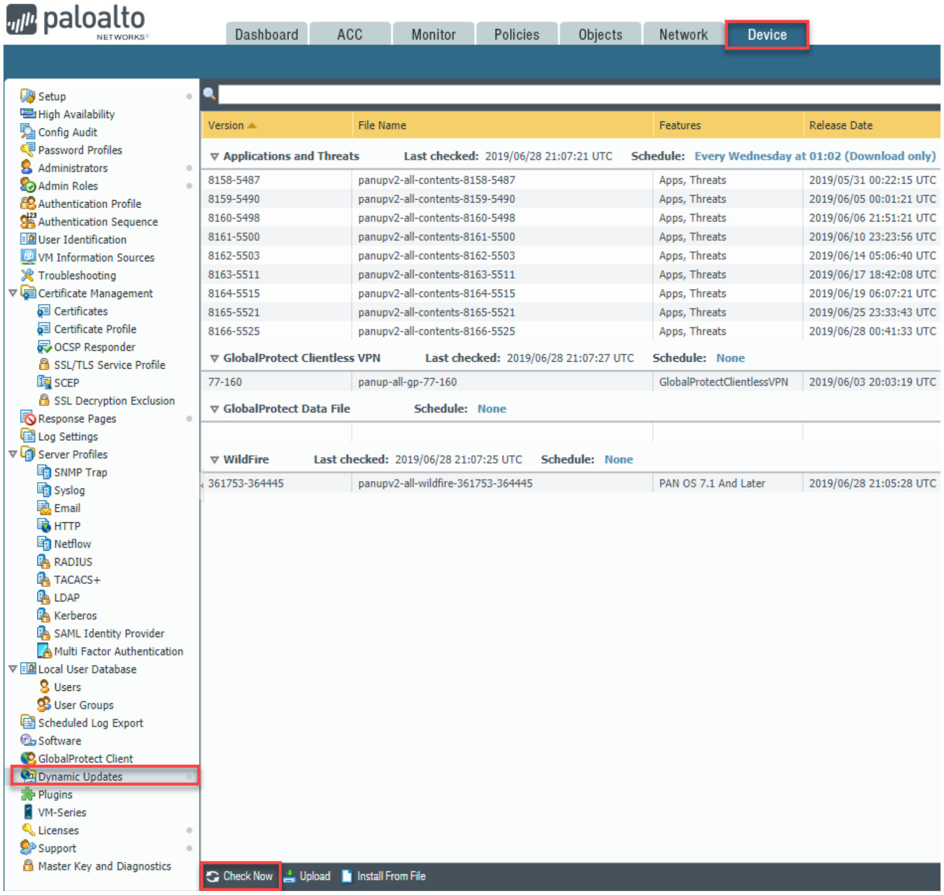
Premium
Date Issued May 01, 2017
Date Expires May 01, 2018
Description 24 x 7 phone support; advanced replacement hardware servic

WildFire License
Date Issued May 01, 2017
Date Expires May 01, 2018

6.1.9 Log back into your firewall. *Close* the welcome page and go to *Device Tab > Dynamic Updates* and click *Check Now* on the lower left-hand side.

6.1.10 *Download and install all the updates*.

Continue to Check Now and install the most recent updates until there are no longer any updates to be downloaded.



Version	File Name	Features	Release Date
Applications and Threats	**Last checked:** 2019/06/28 21:07:21 UTC	**Schedule:** Every Wednesday at 01:02 (Download only)	
8158-5487	panupv2-all-contents-8158-5487	Apps, Threats	2019/05/31 00:22:15 UTC
8159-5490	panupv2-all-contents-8159-5490	Apps, Threats	2019/06/05 00:01:21 UTC
8160-5498	panupv2-all-contents-8160-5498	Apps, Threats	2019/06/06 21:51:21 UTC
8161-5500	panupv2-all-contents-8161-5500	Apps, Threats	2019/06/10 23:23:56 UTC
8162-5503	panupv2-all-contents-8162-5503	Apps, Threats	2019/06/14 05:06:40 UTC
8163-5511	panupv2-all-contents-8163-5511	Apps, Threats	2019/06/17 18:42:08 UTC
8164-5515	panupv2-all-contents-8164-5515	Apps, Threats	2019/06/19 06:07:21 UTC
8165-5521	panupv2-all-contents-8165-5521	Apps, Threats	2019/06/25 23:33:43 UTC
8166-5525	panupv2-all-contents-8166-5525	Apps, Threats	2019/06/28 00:41:33 UTC
GlobalProtect Clientless VPN	**Last checked:** 2019/06/28 21:07:27 UTC	**Schedule:** None	
77-160	panup-all-gp-77-160	GlobalProtectClientlessVPN	2019/06/03 20:03:19 UTC
GlobalProtect Data File	**Schedule:** None		
WildFire	**Last checked:** 2019/06/28 21:07:25 UTC	**Schedule:** None	
361753-364445	panupv2-all-wildfire-361753-364445	PAN OS 7.1 And Later	2019/06/28 21:05:28 UTC

Note: Antivirus updates will not show until you install your Applications and Threats updates. Once installed please click the Check Now button again so that Antivirus shows up and then install them.

Contact details

Associate Professor John Williams

E j.williams1@uq.edu.au

CRICOS Provider Number 00025B