```
llName       : \\DC01.
ner          : BUILTIN\Ad
stAccessTime : 6/22/2021 6:
stWriteTime  : 6/21/2021 7:07
eationTime   : 6/22/2021 6:34:3
ngth         : 1125
```

Powershell for Pentesters

Lab Installation Guide

(Not a Finished Product)

Version 1.0

9/1/2021

Table of Contents

Addendums and Updates

Section 1 - Introduction

Greetings, and welcome to my course “PowerShell for Pentesters.” This course is meant for beginner to intermediate pentest students who have some precursory knowledge about penetration testing. This knowledge could be derived from a course such as the Penetration Testing Student course from INE, the Practical Ethical Hacking course from TheCyberMentor, or other training. No matter where you’ve learned what you know so far, this course will hopefully help you along your way to becoming an offensive security practitioner.

I wish you my very best!

Joe

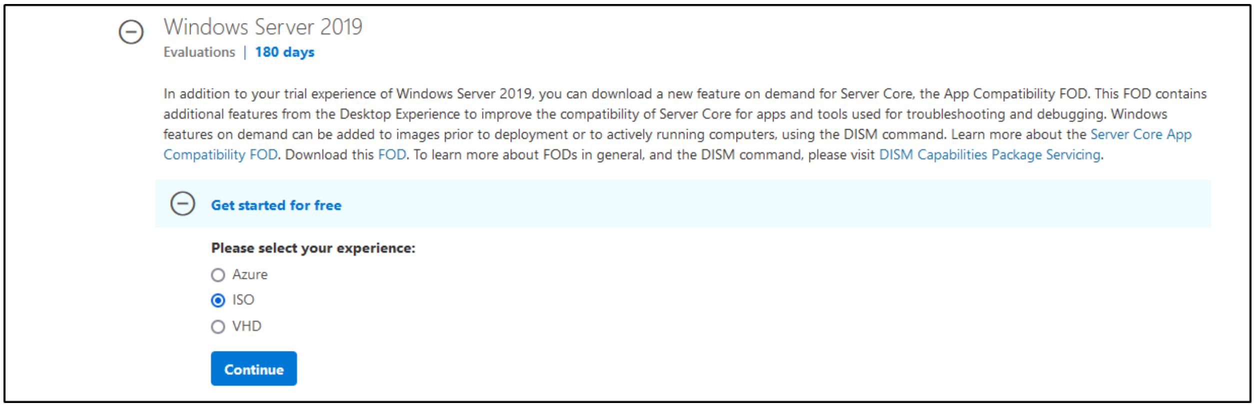
Section 2 - Lab and Network Generation

2-1 Introduction

For this course it is expected that the student already understands how to provision virtual machines in the local lab environment utilizing VirtualBox (VMWare will not be used for the course as we need multiple NAT networks for configuration). The course will cover generating the appropriate virtual networks for the lab environment and configuring each host to correctly interact with one another. Additionally, this section will cover the installation of Active Directory, populating the users, GPOs, ACLs, and other items necessary for the course, and connecting the user workstations to the domain.

2-2 Virtual Machine Downloads

Windows Server 2019 Evaluation ISO (https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019). Follow the instructions to download the trial version of Server 2019.



Windows Server 2019

Evaluations | **180 days**

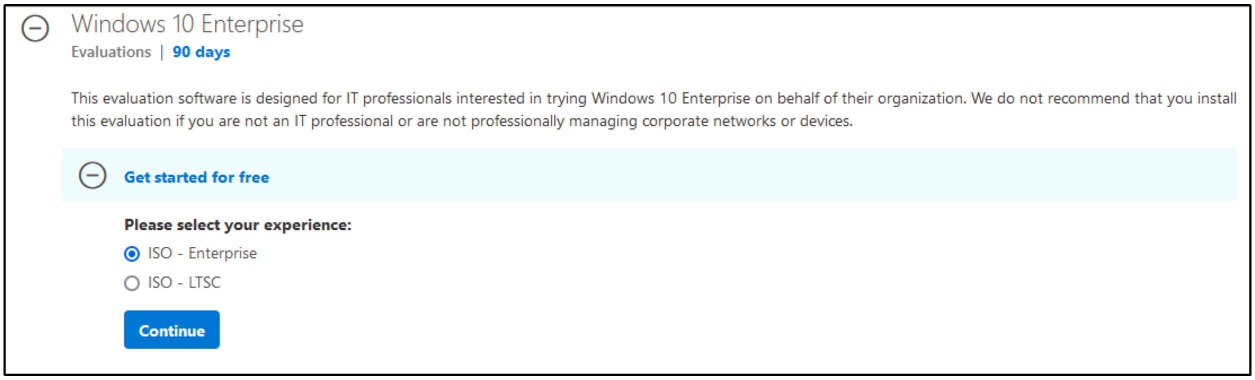
In addition to your trial experience of Windows Server 2019, you can download a new feature on demand for Server Core, the App Compatibility FOD. This FOD contains additional features from the Desktop Experience to improve the compatibility of Server Core for apps and tools used for troubleshooting and debugging. Windows features on demand can be added to images prior to deployment or to actively running computers, using the DISM command. Learn more about the Server Core App Compatibility FOD. Download this FOD. To learn more about FODs in general, and the DISM command, please visit DISM Capabilities Package Servicing.

Get started for free

Please select your experience:

○ Azure
● ISO
○ VHD

Windows 10 Pro Evaluation ISO (Will generate two VMs from this) (https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise). Follow the instructions to download the trial version of Windows 10 Enterprise.



Windows 10 Enterprise

Evaluations | **90 days**

This evaluation software is designed for IT professionals interested in trying Windows 10 Enterprise on behalf of their organization. We do not recommend that you install this evaluation if you are not an IT professional or are not professionally managing corporate networks or devices.

Get started for free

Please select your experience:

● ISO - Enterprise
○ ISO - LTSC

2-3 AD Generator Script

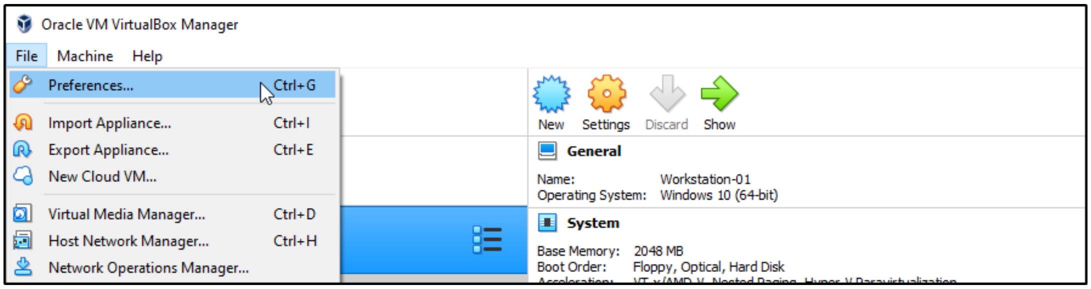
Students will need to download the individual Active Directory generation scripts to build the domain environment.

The PowerShell scripts are located at https://github.com/dievus/PowerShellForPentesters .

2-4 Network Configuration

A virtual network needs to be configured for the course. Configuring the network in VirtualBox is done with the following:

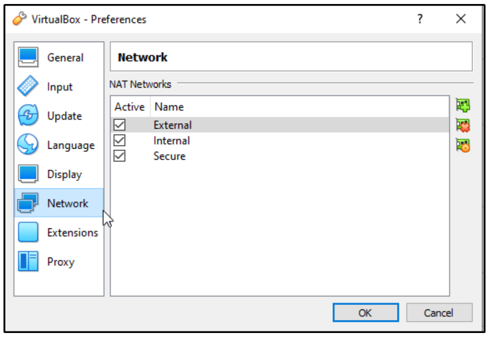
File > Preferences


Oracle VM VirtualBox Manager
File
Machine
Help
Preferences... Ctrl+G
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
New Cloud VM...
Virtual Media Manager... Ctrl+D
Host Network Manager... Ctrl+H
Network Operations Manager...
New
Settings
Discard
Show
General
System

Name: Workstation-01
Operating System: Windows 10 (64-bit)

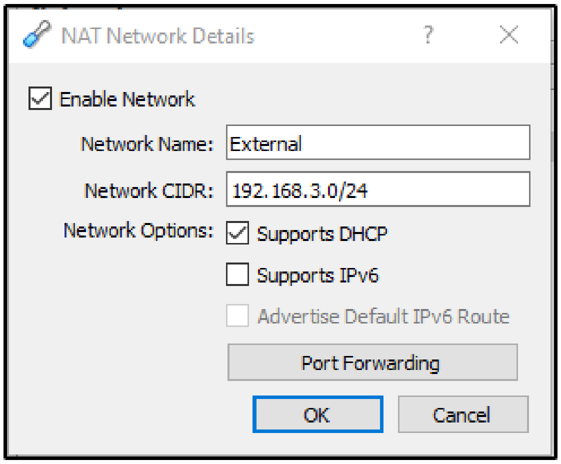
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Click on Network



Active	Name
☑	External
☑	Internal
☑	Secure

Click the Add (+ button) to create a new network. Double click the new network and enter the following information:



☑ Enable Network

Network Name: External

Network CIDR: 192.168.3.0/24

Network Options: ☑ Supports DHCP

□ Supports IPv6

□ Advertise Default IPv6 Route

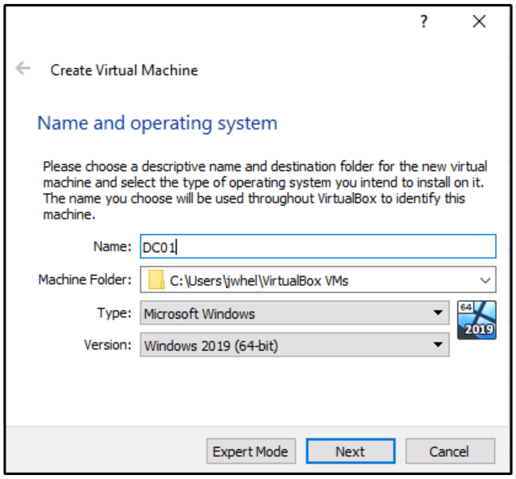
This will be the only virtual NAT network that will be used throughout the course. Make note of the IP subnets for later use.

2-5 VM Provisioning

Windows Server 2019 Setup and Installation

Once the student has downloaded the evaluation version of Windows 2019 from Microsoft, create a new virtual machine in VirtualBox. The following images are step by step settings to be followed. Note that images refer to RAM and hard disk space that should be used as a minimum baseline. It is acceptable, should the student's computer have the resources, to assign more resources that suggested.

Select New at the top of VirtualBox, which opens the Create Virtual Machine window. Name the workstation appropriately – DC01. Set the type to Windows, and Version to Windows 2019. Click Next.



Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

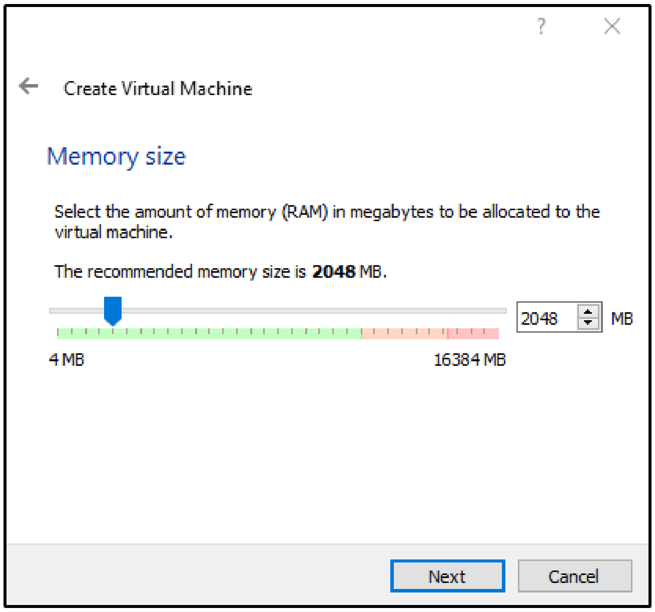
Name: DC01

Machine Folder: C:\Users\jwhel\VirtualBox VMs

Type: Microsoft Windows

Version: Windows 2019 (64-bit)

Set RAM to 2048 MB and click Next.



Create Virtual Machine

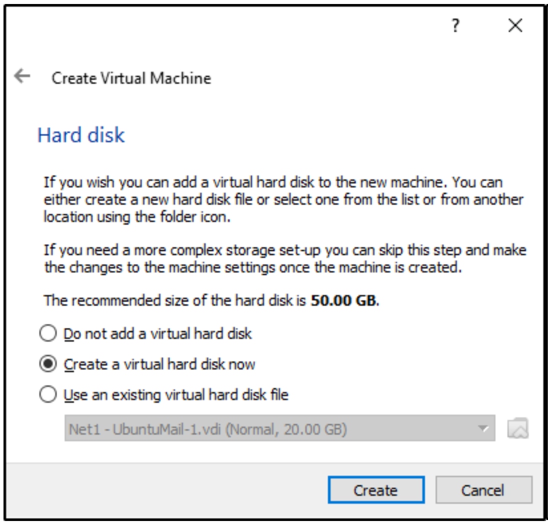
Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **2048** MB.

2048 MB

Make sure “Create a virtual hard disk now” is selected, click create, and ensure VDI is selected. Click Next.



Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

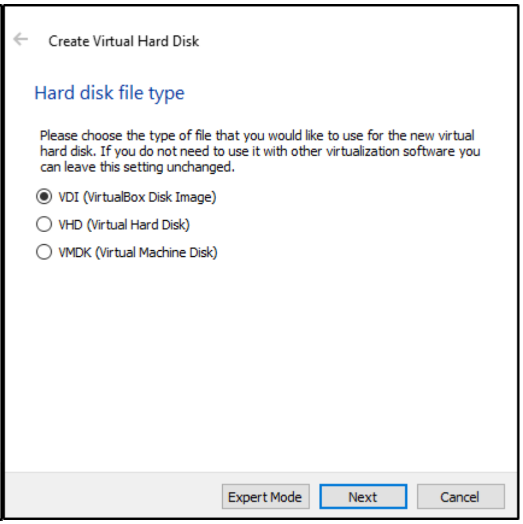
The recommended size of the hard disk is **50.00 GB**.

○ Do not add a virtual hard disk

● Create a virtual hard disk now

○ Use an existing virtual hard disk file

Net1 - UbuntuMail-1.vdi (Normal, 20.00 GB)



Create Virtual Hard Disk

Hard disk file type

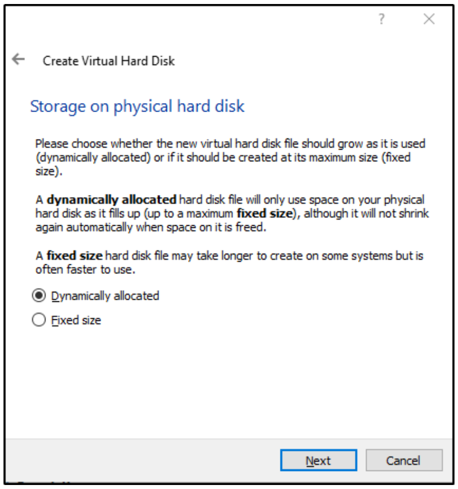
Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

● VDI (VirtualBox Disk Image)

○ VHD (Virtual Hard Disk)

○ VMDK (Virtual Machine Disk)

Ensure Dynamically allocated is selected and click next. Set the file size slider to 20 GB and click Create.



Create Virtual Hard Disk

Storage on physical hard disk

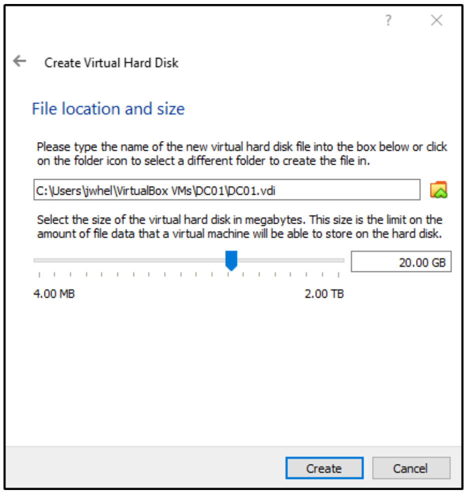
Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

● Dynamically allocated

○ Fixed size



Create Virtual Hard Disk

File location and size

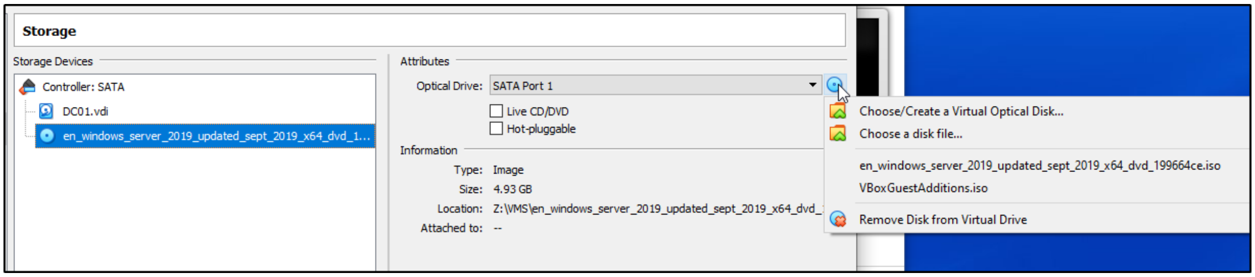
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

C:\Users\jwhel\VirtualBox VMs\DC01\DC01.vdi

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

20.00 GB

Click on the workstation, click Settings at the top, select Storage on the left. Click the empty disk under Storage devices, and on the right side of the screen click the blue disk. It is likely you will need to navigate to the download directory where the ISO is located. Select that ISO.



Storage

Storage Devices

Controller: SATA

DC01.vdi

en_windows_server_2019_updated_sept_2019_x64_dvd_1...

Attributes

Optical Drive: SATA Port 1

□ Live CD/DVD

□ Hot-pluggable

Information

Type: Image

Size: 4.93 GB

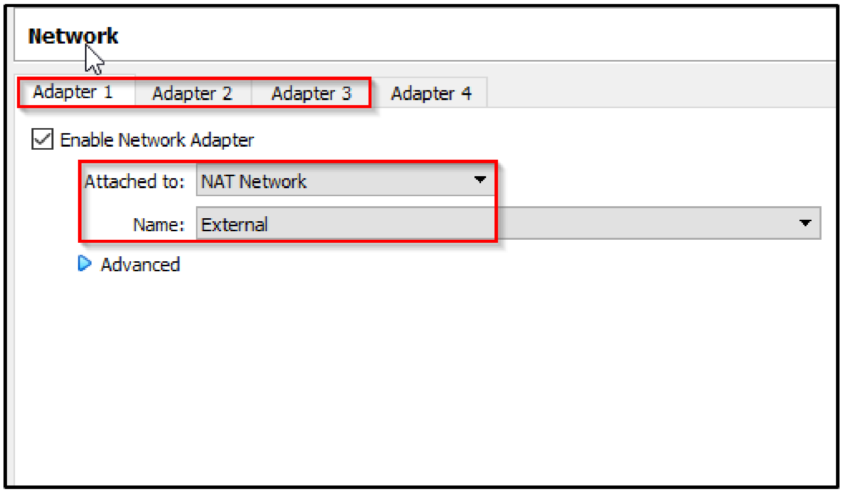
Location: Z:\VMS\en_windows_server_2019_updated_sept_2019_x64_dvd_

Attached to: --

Choose/Create a Virtual Optical Disk...
Choose a disk file...
en_windows_server_2019_updated_sept_2019_x64_dvd_199664ce.iso
VBoxGuestAdditions.iso
Remove Disk from Virtual Drive

Click on Network next. The following settings are required for the server:

- Set the network to the External network created before



Network

☑ Enable Network Adapter

Attached to: NAT Network

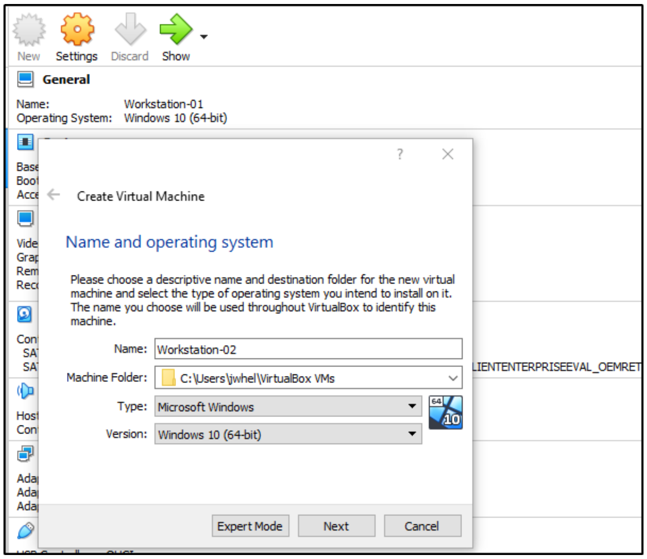
Name: External

Once configured click Ok. Boot the Windows server.

Workstation-01 Setup and Installation

Installation of the Windows workstation is straight forward. Once the student has downloaded the Windows 10 Enterprise Evaluation iso from Microsoft, create two new virtual machines in VirtualBox. The following images are step by step settings to be followed for creating Workstation-01.

Select New at the top of VirtualBox, which opens the Create Virtual Machine window. Set the type to Windows, and Version to Windows 10 x64. Click Next.



General

Name: Workstation-01
Operating System: Windows 10 (64-bit)

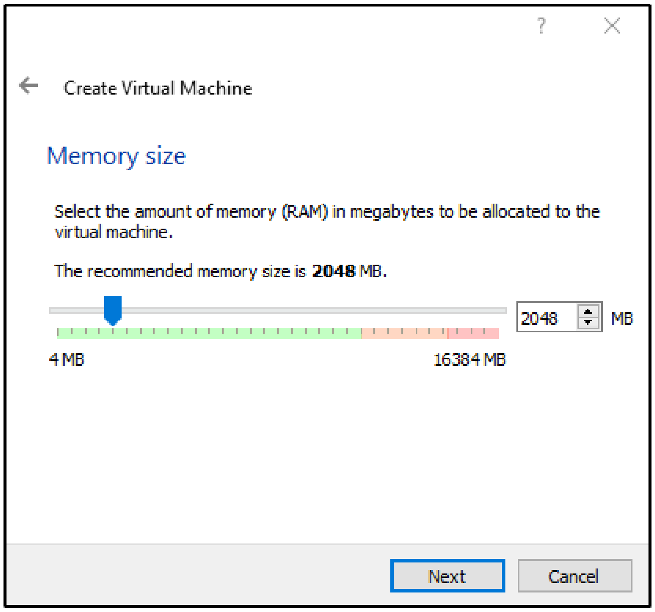
Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: Workstation-02
Machine Folder: C:\Users\jwhel\VirtualBox VMs
Type: Microsoft Windows
Version: Windows 10 (64-bit)

Set RAM to 2048 MB and click Next.



Create Virtual Machine

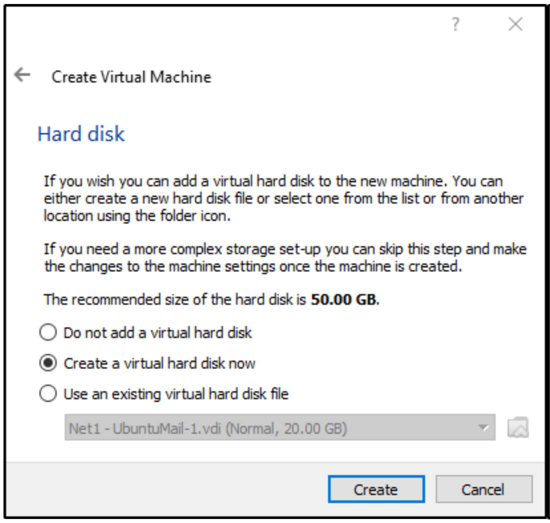
Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **2048** MB.

2048 MB

Make sure “Create a virtual hard disk now” is selected, click create, and ensure VDI is selected. Click Next.



Create Virtual Machine

Hard disk

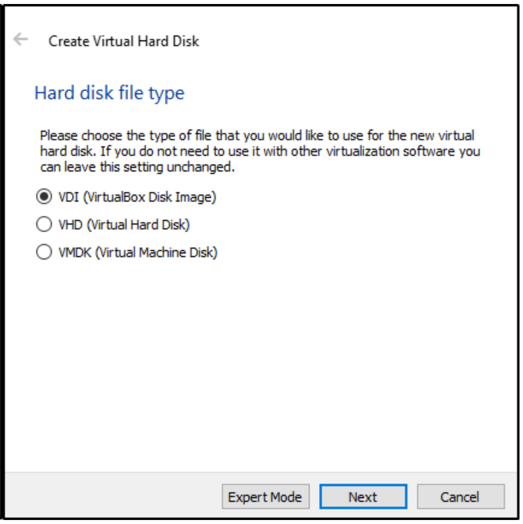
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **50.00 GB**.

○ Do not add a virtual hard disk
● Create a virtual hard disk now
○ Use an existing virtual hard disk file

Net1 - UbuntuMail-1.vdi (Normal, 20.00 GB)



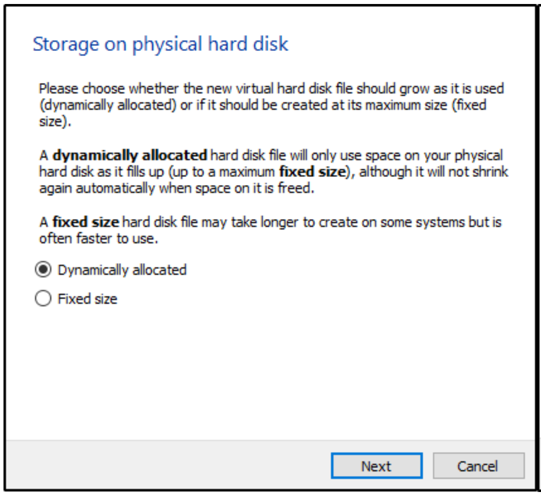
Create Virtual Hard Disk

Hard disk file type

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

● VDI (VirtualBox Disk Image)
○ VHD (Virtual Hard Disk)
○ VMDK (Virtual Machine Disk)

Ensure Dynamically allocated is selected and click next. Set the file size slider to 20 GB and click Create.



Storage on physical hard disk

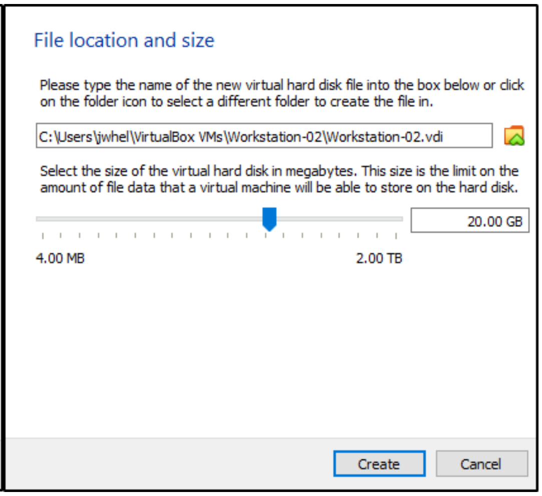
Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

● Dynamically allocated

○ Fixed size



File location and size

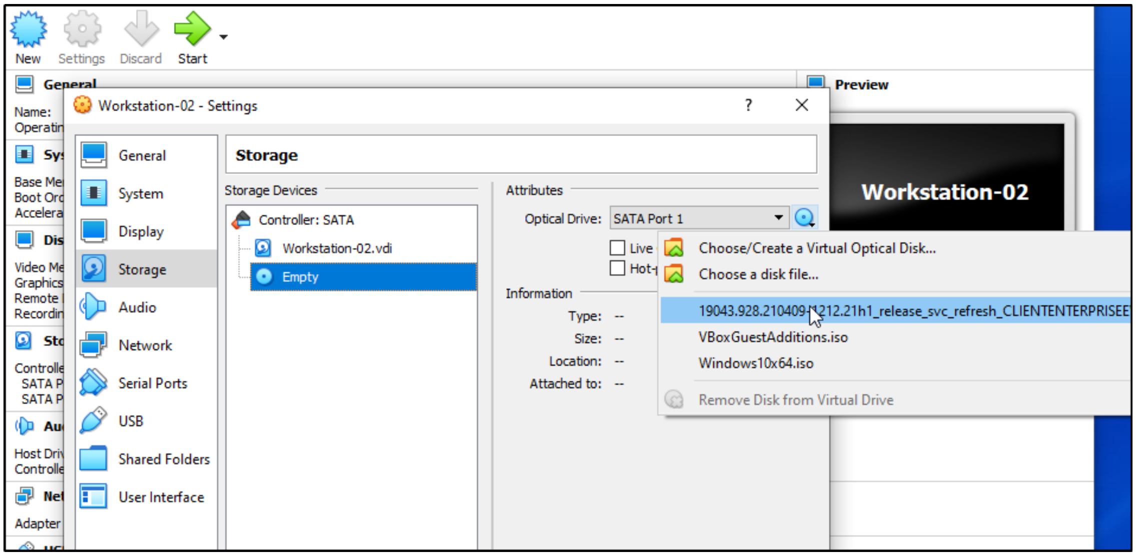
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

C:\Users\jwhel\VirtualBox VMs\Workstation-02\Workstation-02.vdi

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

20.00 GB

Click on the workstation, click Settings at the top, select Storage on the left. Click the empty disk under Storage devices, and on the right side of the screen click the blue disk. It is likely you will need to navigate to the download directory where the ISO is located. Select that ISO.



Workstation-02 - Settings

Storage

Storage Devices

Controller: SATA
Workstation-02.vdi
Empty

Attributes

Optical Drive: SATA Port 1

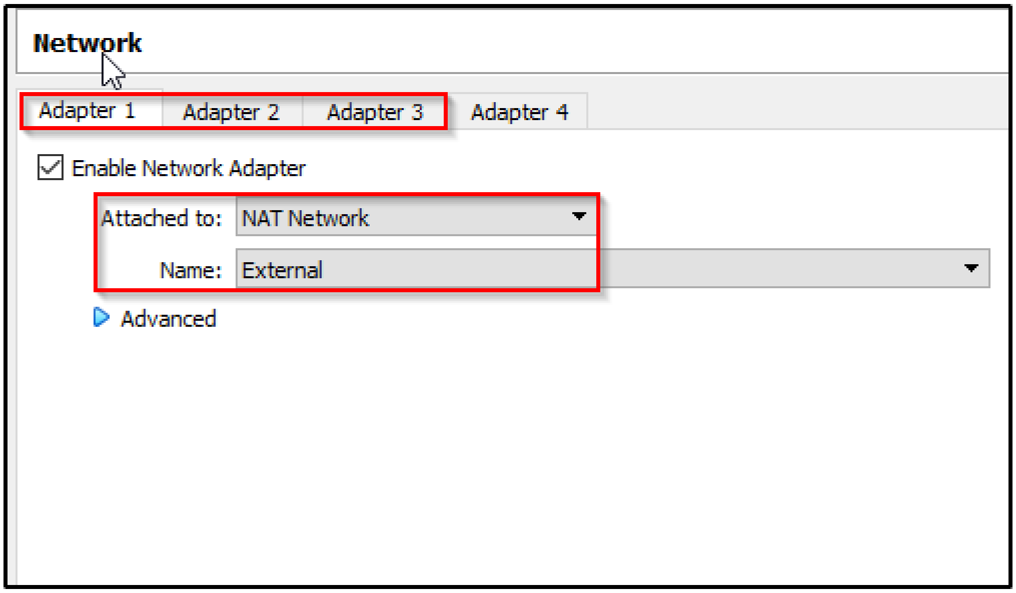
□ Live
□ Hot-

Information

Type: --
Size: --
Location: --
Attached to: --

Click on Network next. The following settings are required for Workstation-01

- Workstation 01 needs to be configured to utilize the External network generated before



☑ Enable Network Adapter

Attached to: NAT Network

Name: External

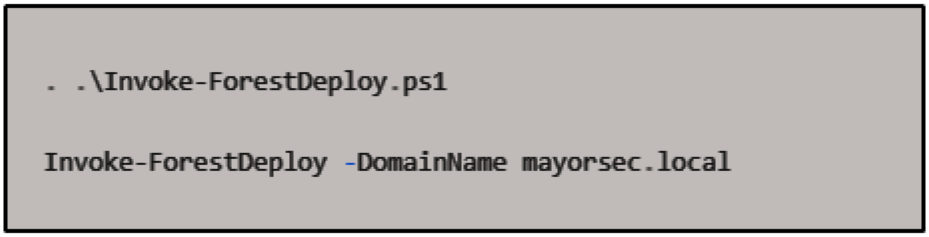
Once configured on both devices, click Ok. Boot the workstation.

2-6 Active Directory Domain Services and Forest Generation

After the student has provisioned appropriately configured virtual networks and machines, they should start the Server 2019 machine first. Follow the installation instructions and generate a username that will be used for various administrative tasks throughout the course. Upon startup, download the ADGenerator.ps1 and ForestDeploy.ps1 PowerShell scripts to the machine.

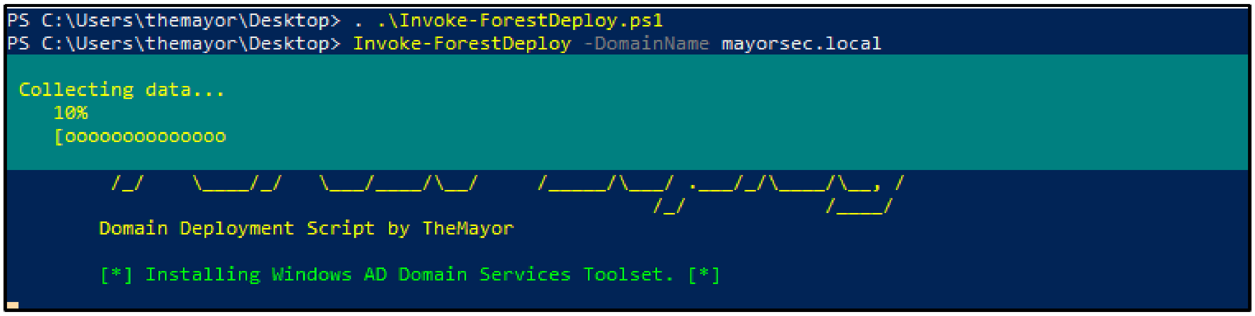
At this point I also created a new user, themayor and make them a domain administrator.

Open PowerShell as an administrator, navigate to the directory where the scripts are located, and run the following:



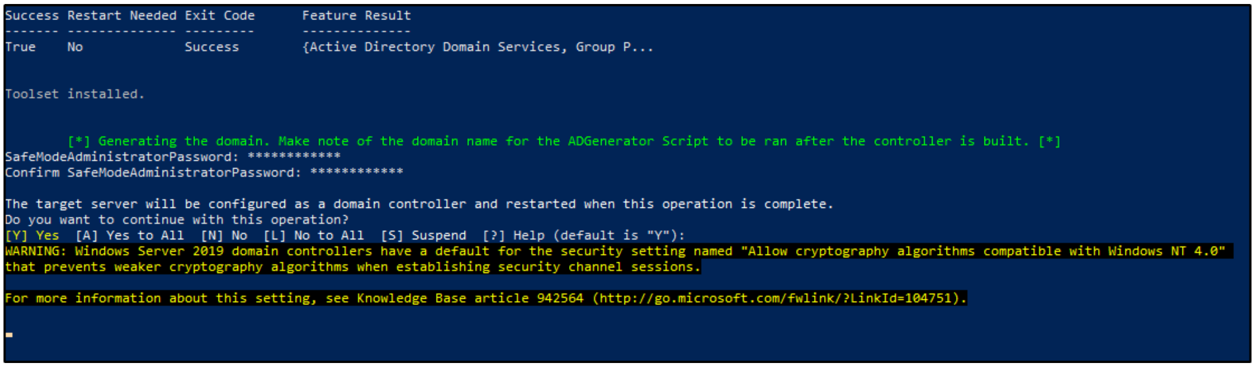
```
. .\Invoke-ForestDeploy.ps1

Invoke-ForestDeploy -DomainName mayorsec.local
```

This script will install Active Directory Domain Services on the server first, followed by generating the Active Directory and Domain Controller environment. Note that the Invoke-ADGenerator.ps1 script is configured to use the mayorsec.local domain. If the student wishes to use a different domain name it’s vital that the student change the domain name in all scripts.



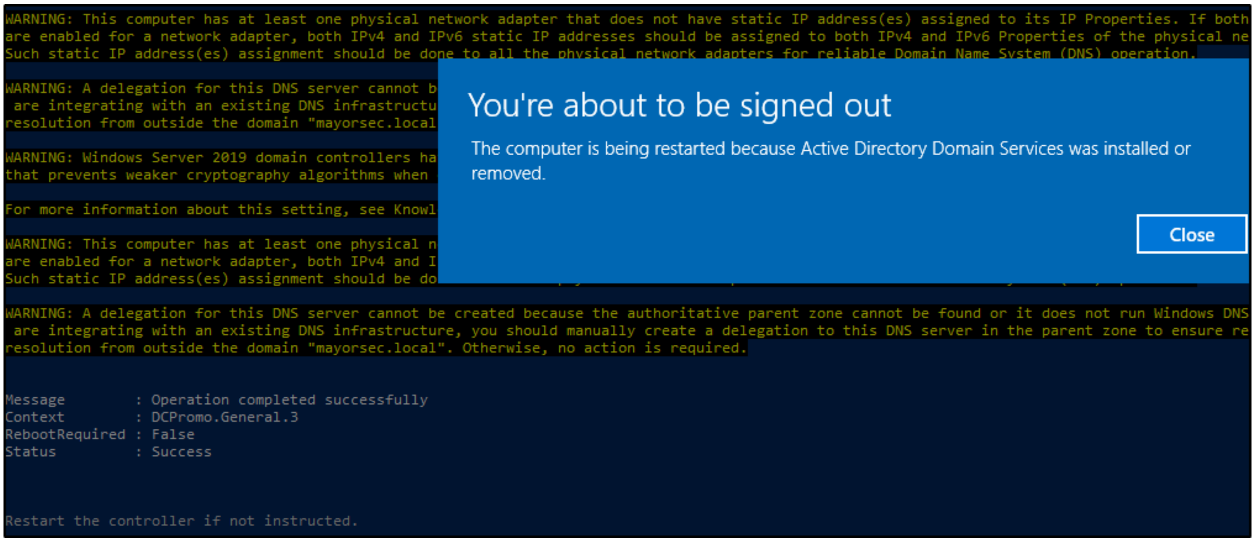
```
PS C:\Users\themayor\Desktop> . .\Invoke-ForestDeploy.ps1
PS C:\Users\themayor\Desktop> Invoke-ForestDeploy -DomainName mayorsec.local

 Collecting data...
    10%
    [oooooooooooooo
          /_/    \____/_/   \___/____/\__/     /_____/\___/ .___/_/\____/\__, /
                                                         /_/             /____/
         Domain Deployment Script by TheMayor

         [*] Installing Windows AD Domain Services Toolset. [*]
```

When prompted to enter the SafeModeAdministratorPassword, enter a secure password, press enter, and then press enter when prompted to configure as a domain controller. Warnings can be ignored.



```
Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services, Group P...


Toolset installed.


        [*] Generating the domain. Make note of the domain name for the ADGenerator Script to be ran after the controller is built. [*]
SafeModeAdministratorPassword: ************
Confirm SafeModeAdministratorPassword: ************

The target server will be configured as a domain controller and restarted when this operation is complete.
Do you want to continue with this operation?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
WARNING: Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0"
that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
```

Upon completion the student will be prompted to restart the controller for changes to take effect.



```
WARNING: This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both
are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical ne
Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

WARNING: A delegation for this DNS server cannot b
 are integrating with an existing DNS infrastructu
resolution from outside the domain "mayorsec.local

WARNING: Windows Server 2019 domain controllers ha
that prevents weaker cryptography algorithms when

For more information about this setting, see Knowl

WARNING: This computer has at least one physical n
are enabled for a network adapter, both IPv4 and I
Such static IP address(es) assignment should be do

WARNING: A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS
 are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure re
resolution from outside the domain "mayorsec.local". Otherwise, no action is required.


Message        : Operation completed successfully
Context        : DCPromo.General.3
RebootRequired : False
Status         : Success


Restart the controller if not instructed.
```

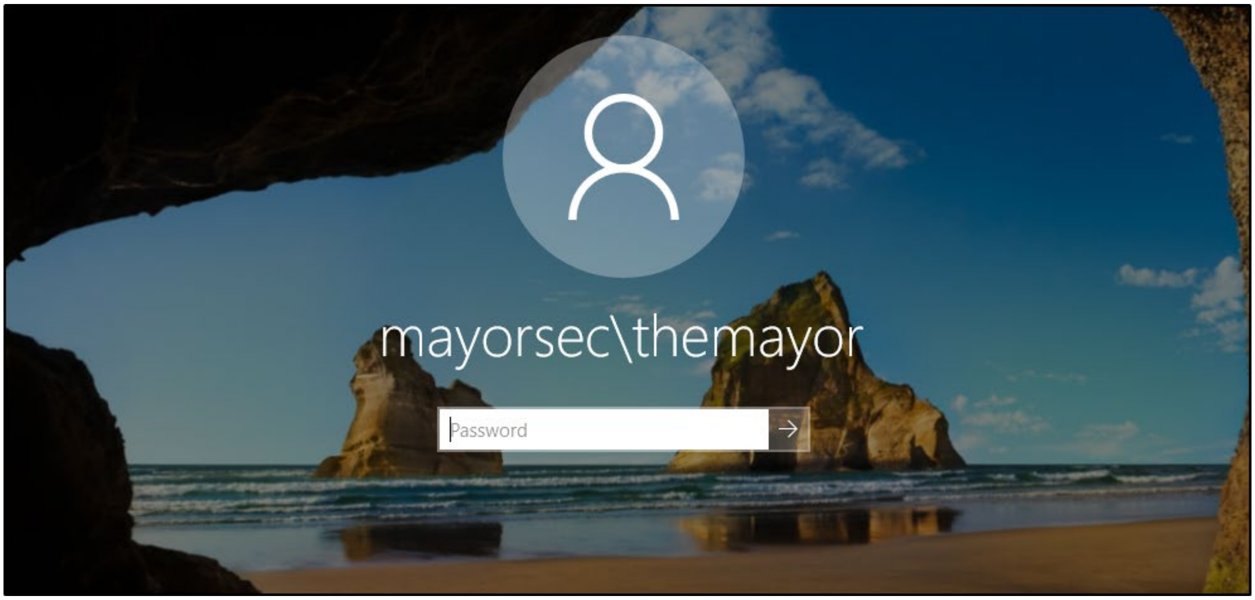
You're about to be signed out

The computer is being restarted because Active Directory Domain Services was installed or removed.

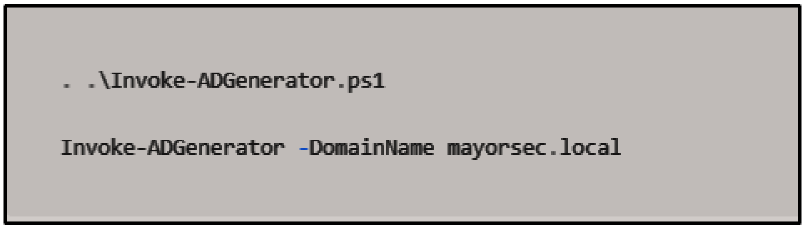
<u>GENERATE A SNAPSHOT OF THE VIRTUAL MACHINE ONCE IT FINISHES REBOOTING.</u>

2-7 – Domain Population

Upon completion of setting up Windows Server 2019, log in to the new domain controller with your previously created account credentials.



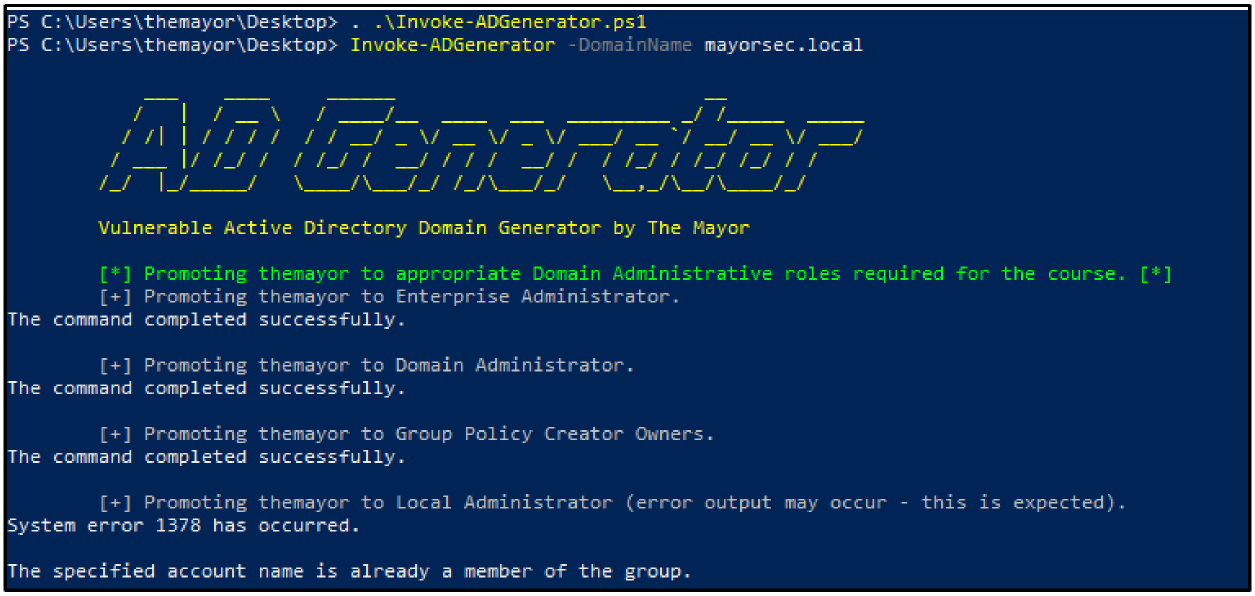
Open PowerShell in an elevated prompt and navigate to the directory where the Invoke-ADGenerator.ps1 script is located. Run the script using the following:



```
. .\Invoke-ADGenerator.ps1

Invoke-ADGenerator -DomainName mayorsec.local
```

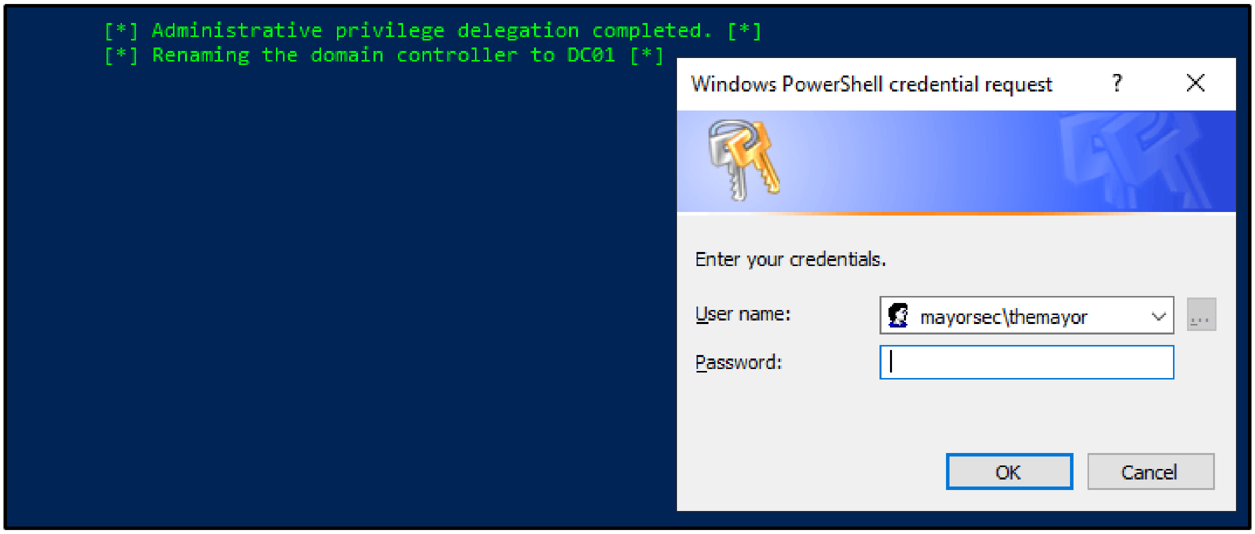
Note that the Invoke-ADGenerator.ps1 script has some hard-coding with the mayorsec.local domain name. If the student wishes to use a different name, scripts will have to be modified locally.

After running the command, the student’s account on the domain is elevated to Enterprise, Domain, and local administrator groups.



```
PS C:\Users\themayor\Desktop> . .\Invoke-ADGenerator.ps1
PS C:\Users\themayor\Desktop> Invoke-ADGenerator -DomainName mayorsec.local


            ___    ____     ______                           __
           /   |  / __ \   / ____/__  ____  ___  _________ _/ /_____  _____
          / /| | / / / /  / / __/ _ \/ __ \/ _ \/ ___/ __ `/ __/ __ \/ ___/
         / ___ |/ /_/ /  / /_/ /  __/ / / /  __/ /  / /_/ / /_/ /_/ / /
        /_/  |_/_____/   \____/\___/_/ /_/\___/_/   \__,_/\__/\____/_/

        Vulnerable Active Directory Domain Generator by The Mayor

        [*] Promoting themayor to appropriate Domain Administrative roles required for the course. [*]
        [+] Promoting themayor to Enterprise Administrator.
The command completed successfully.

        [+] Promoting themayor to Domain Administrator.
The command completed successfully.

        [+] Promoting themayor to Group Policy Creator Owners.
The command completed successfully.

        [+] Promoting themayor to Local Administrator (error output may occur - this is expected).
System error 1378 has occurred.

The specified account name is already a member of the group.
```

Students will then be prompted for domain credentials to authorize changing the name of the domain controller to DC01.



```
        [*] Administrative privilege delegation completed. [*]
        [*] Renaming the domain controller to DC01 [*]
```

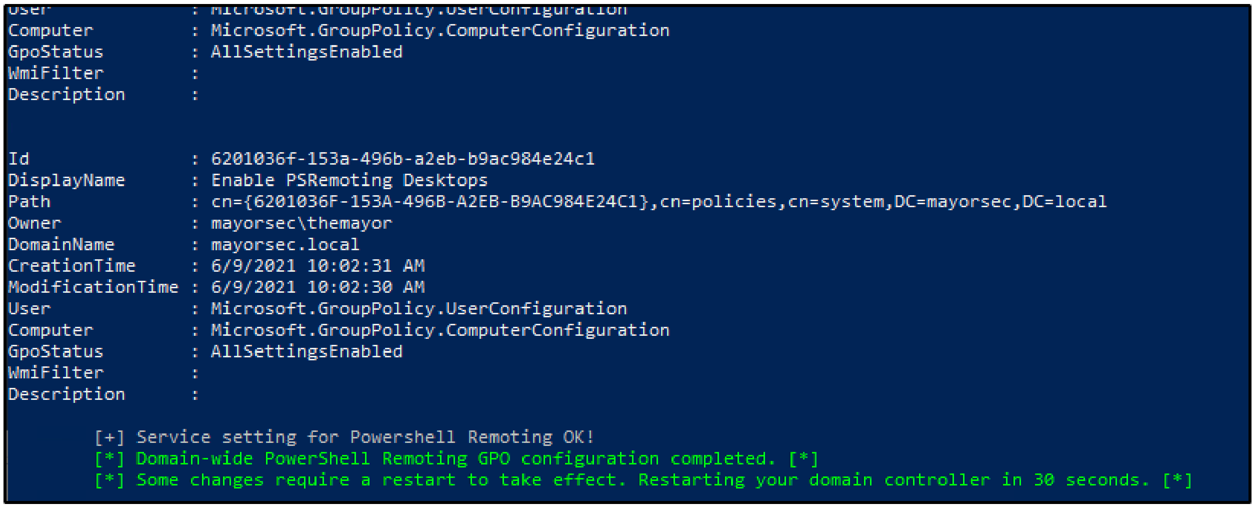
Windows PowerShell credential request

Enter your credentials.

User name: mayorsec\themayor

Password:

Once all changes have been populated the script will prompt that the domain controller will restart in 30 seconds. Note that if any error messages occurred during installation that it is best to revert to the snapshot previously generated.

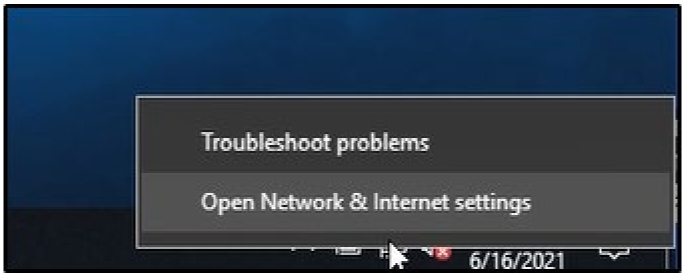


```
User             : Microsoft.GroupPolicy.UserConfiguration
Computer         : Microsoft.GroupPolicy.ComputerConfiguration
GpoStatus        : AllSettingsEnabled
WmiFilter        :
Description      :


Id               : 6201036f-153a-496b-a2eb-b9ac984e24c1
DisplayName      : Enable PSRemoting Desktops
Path             : cn={6201036F-153A-496B-A2EB-B9AC984E24C1},cn=policies,cn=system,DC=mayorsec,DC=local
Owner            : mayorsec\themayor
DomainName       : mayorsec.local
CreationTime     : 6/9/2021 10:02:31 AM
ModificationTime : 6/9/2021 10:02:30 AM
User             : Microsoft.GroupPolicy.UserConfiguration
Computer         : Microsoft.GroupPolicy.ComputerConfiguration
GpoStatus        : AllSettingsEnabled
WmiFilter        :
Description      :

        [+] Service setting for Powershell Remoting OK!
        [*] Domain-wide PowerShell Remoting GPO configuration completed. [*]
        [*] Some changes require a restart to take effect. Restarting your domain controller in 30 seconds. [*]
```

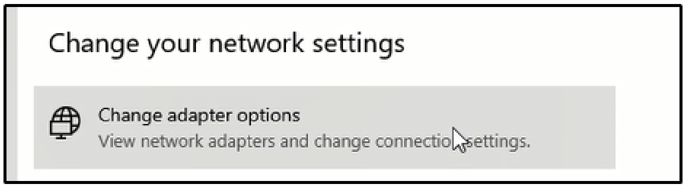
2-8 Join Workstations to the Domain Controller

Joining our Workstation-01 to the newly created domain controller takes multiple steps and attention to detail. First, start DC01 and Workstation-01.

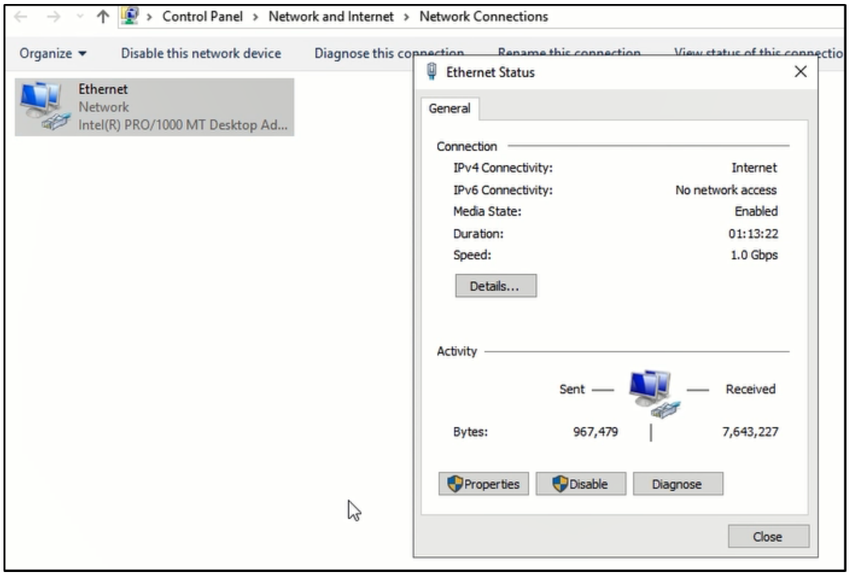
Once logged in to DC01, right click the network icon and select Open Network and Internet settings.



Select Change adapter options.


Change your network settings
Change adapter options
View network adapters and change connection settings.

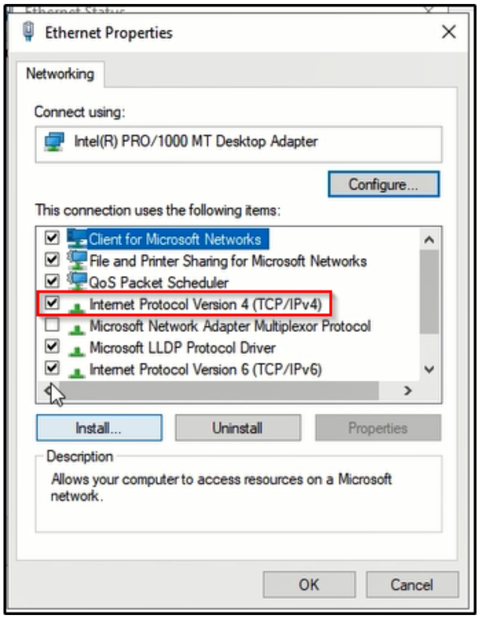
Double click the Ethernet adapter for the Secure network.



Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	01:13:22
Speed:	1.0 Gbps
Bytes:	967,479 | 7,643,227

Click Properties. Double click Internet Protocol Version 4.



Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

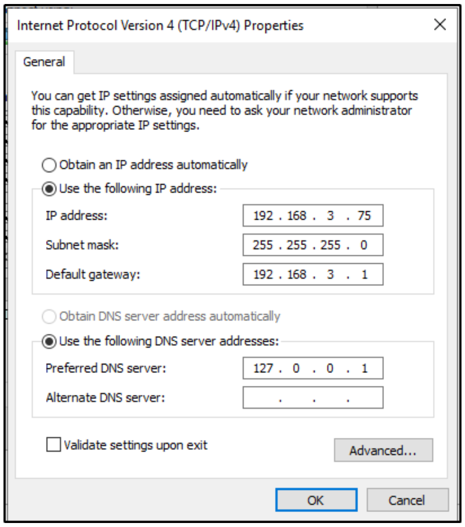
This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
□ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Allows your computer to access resources on a Microsoft network.

Configure the network settings as follows. We use 127.0.0.1 since the domain controller also acts as domain DNS, so localhost is required to resolve domain host names.



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 . 3 . 75

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 3 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

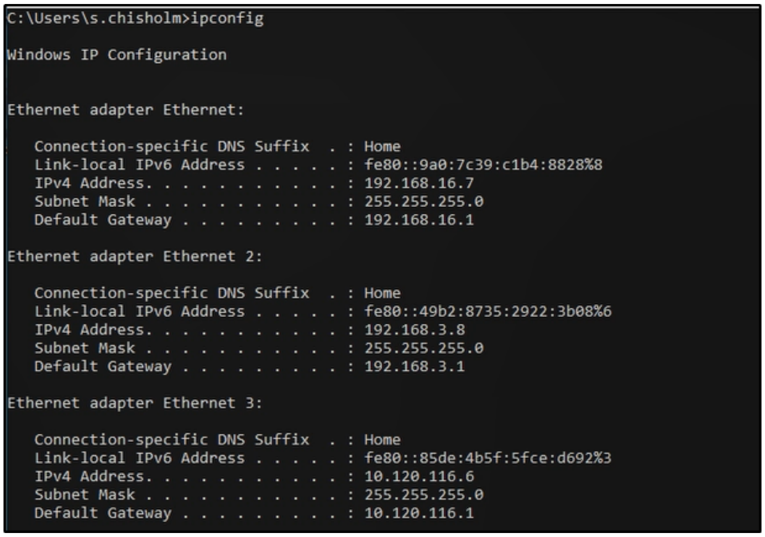
Preferred DNS server: 127 . 0 . 0 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

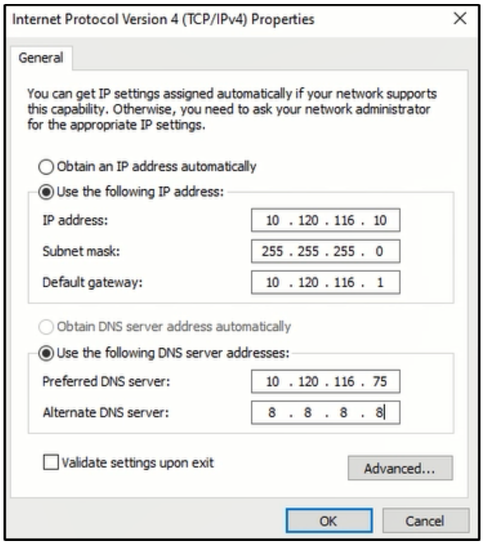
Click Ok. Click Ok again and close open windows.

Access Workstation-01, open a command prompt, and type ipconfig.



```
C:\Users\s.chisholm>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : Home
   Link-local IPv6 Address . . . . . : fe80::9a0:7c39:c1b4:8828%8
   IPv4 Address. . . . . . . . . . . : 192.168.16.7
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.16.1

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : Home
   Link-local IPv6 Address . . . . . : fe80::49b2:8735:2922:3b08%6
   IPv4 Address. . . . . . . . . . . : 192.168.3.8
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.3.1

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . : Home
   Link-local IPv6 Address . . . . . : fe80::85de:4b5f:5fce:d692%3
   IPv4 Address. . . . . . . . . . . : 10.120.116.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.120.116.1
```

Identify the 10.120.116.0/24 IP address and note the Ethernet adapter name (your adapter will be different than this possibly). From here, follow the same instructions as above until you get to the Internet Protocol Version 4 Properties window. Note that the preferred DNS is the domain controller so that the host is able to resolve domain names to IP addresses. Enter the following information into the fields:



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:	10 . 120 . 116 . 10
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10 . 120 . 116 . 1

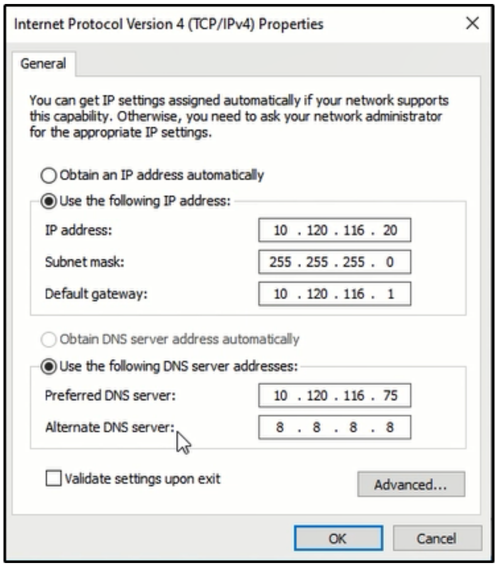
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	10 . 120 . 116 . 75
Alternate DNS server:	8 . 8 . 8 . 8

□ Validate settings upon exit

Follow the same instructions as above for Workstation-02, using the following settings:



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:	10 . 120 . 116 . 20
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10 . 120 . 116 . 1

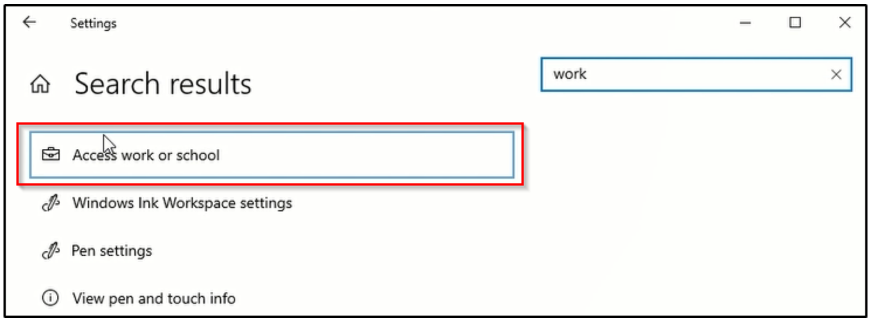
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

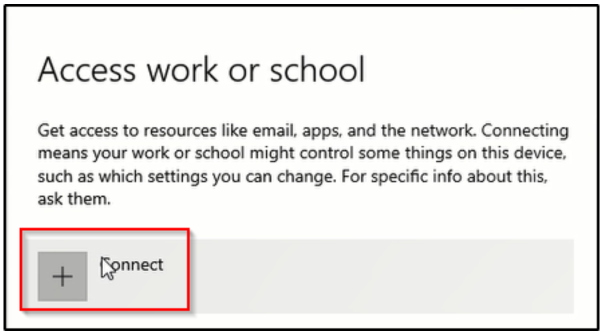
Preferred DNS server:	10 . 120 . 116 . 75
Alternate DNS server:	8 . 8 . 8 . 8

□ Validate settings upon exit

Now that ethernet settings are configured, search for the word “work,” and select Access Work or School. (These instructions will be exactly the same for both Workstation-01 and 02 with the exception of log in names).



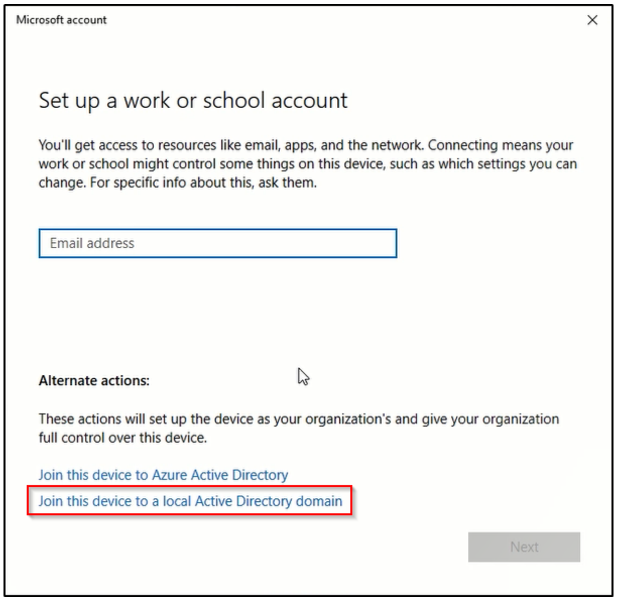
Select Connect.



Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Select Join this device to a local Active Directory domain.



Set up a work or school account

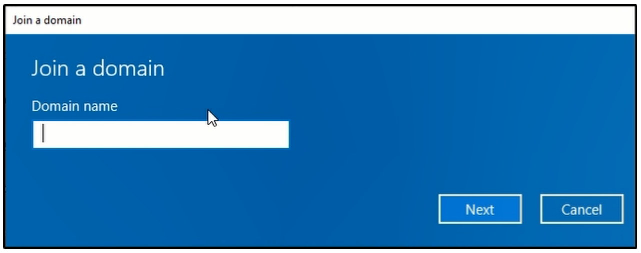
You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Alternate actions:

These actions will set up the device as your organization's and give your organization full control over this device.

Join this device to Azure Active Directory
Join this device to a local Active Directory domain
Next

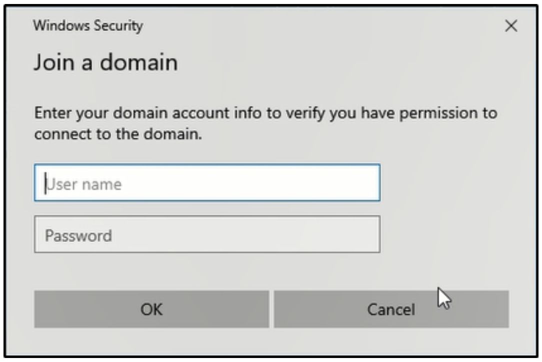
Enter mayorsec.local as the Domain name.



Join a domain

Enter the appropriate domain credentials for each workstation and press Ok:

- Workstation-01 – s.chisholm:FallOutBoy1!
- Workstation-02 – m.seitz:Phi11i35@44

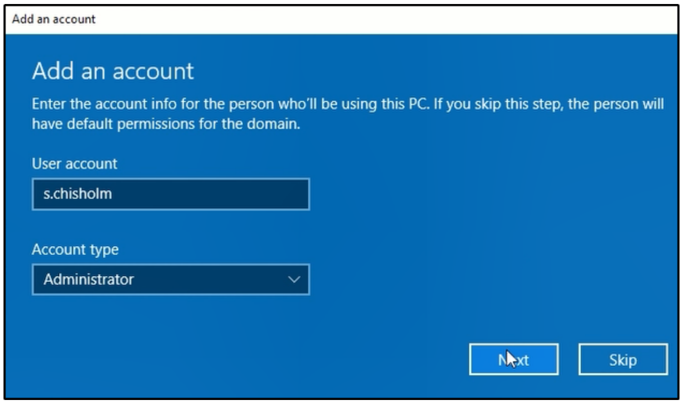


Windows Security

Join a domain

Enter your domain account info to verify you have permission to connect to the domain.

Select Account type – administrator and press next.



Add an account

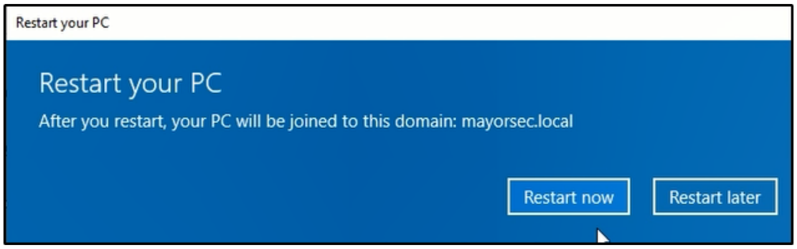
Add an account

Enter the account info for the person who'll be using this PC. If you skip this step, the person will have default permissions for the domain.

User account: s.chisholm

Account type: Administrator

Select Restart now to join the workstations to the domain.

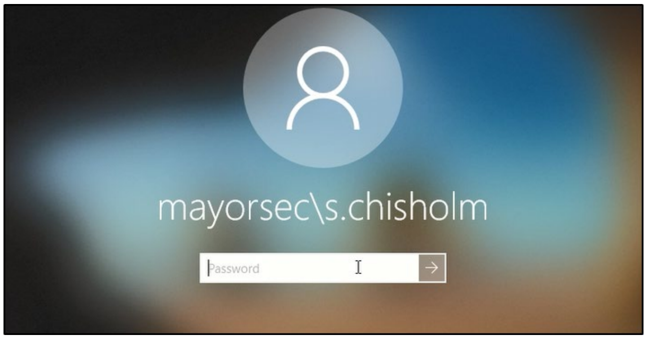


Restart your PC

Restart your PC

After you restart, your PC will be joined to this domain: mayorsec.local

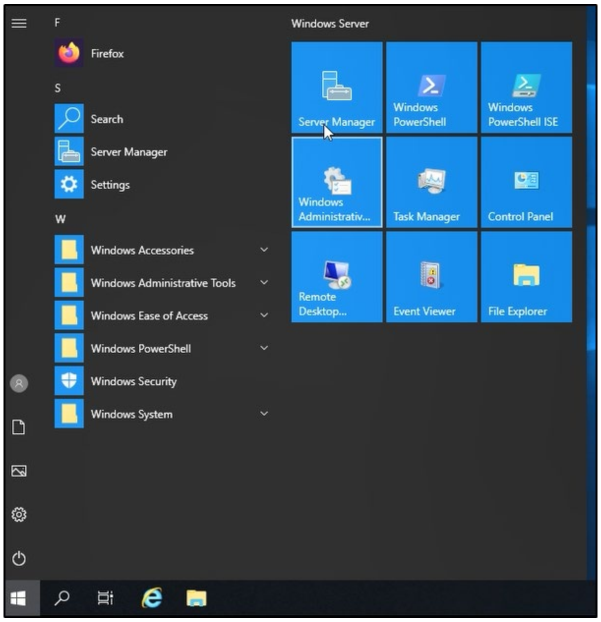
Upon restart you should be presented with a domain logon screen like the following:



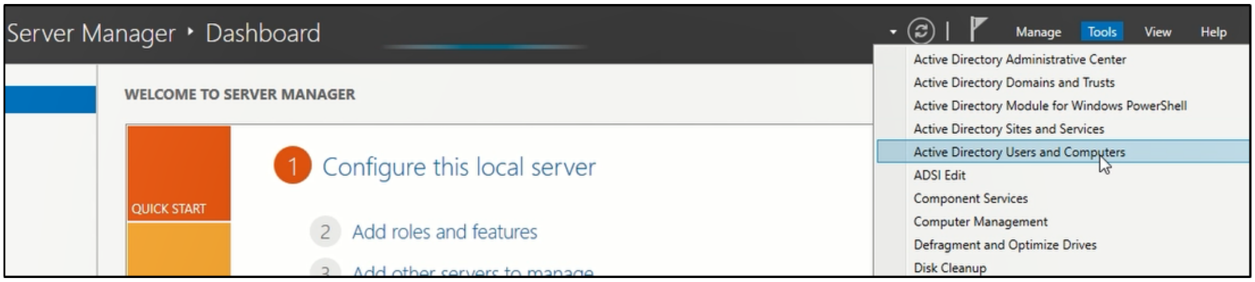
mayorsec\s.chisholm

Login with the appropriate credentials on both workstations.

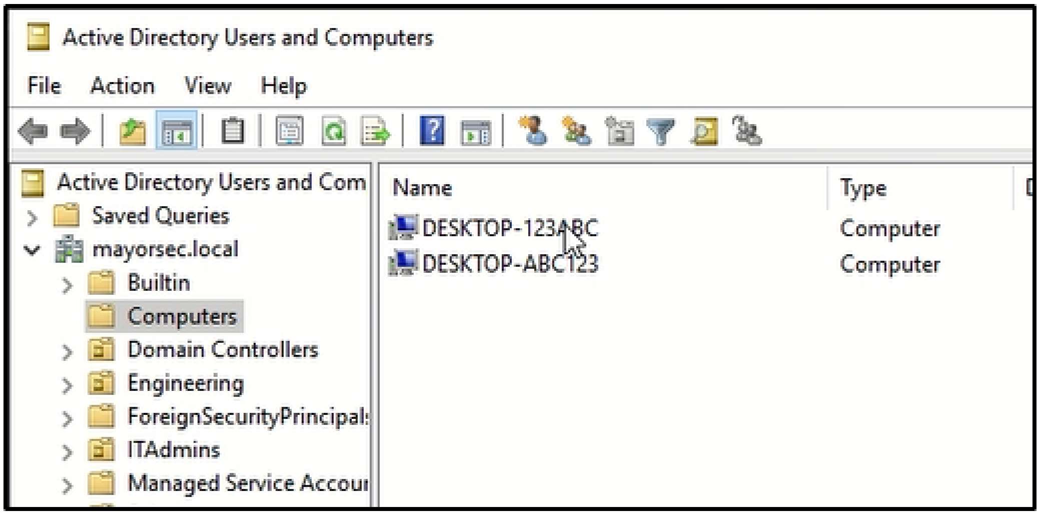
On the domain controller, DC01, open Server Manager.



Open Active Directory Users and Computers.

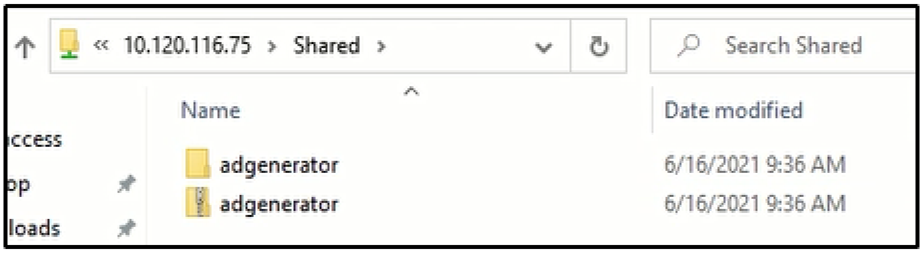

Server Manager ▸ Dashboard
Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
WELCOME TO SERVER MANAGER
QUICK START
1 Configure this local server
2 Add roles and features
3 Add other servers to manage

Confirm that the workstations are connected. Note the names are not set yet as they haven't been renamed.



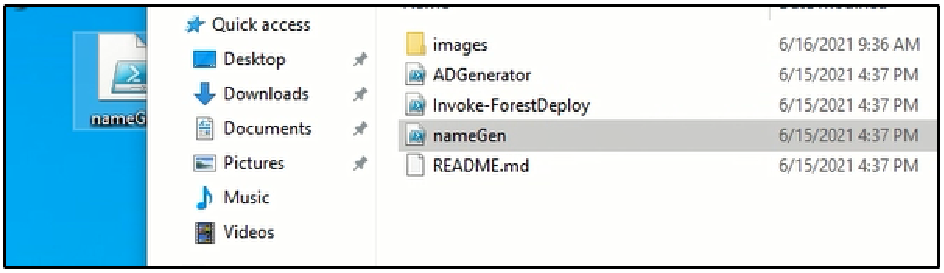
Name	Type
DESKTOP-123ABC	Computer
DESKTOP-ABC123	Computer

The ADGenerator script creates a read only file share on the domain controller. The installation scripts are stored there. Open File Explorer on both workstations and enter the address \\10.120.116.75\. Press enter to access the share.



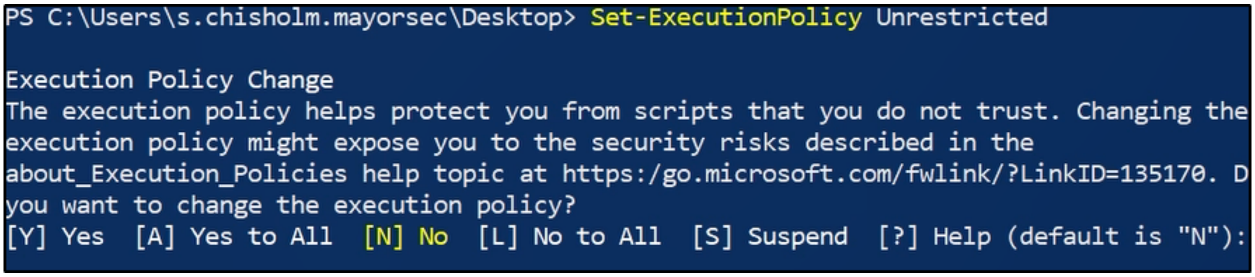
Name	Date modified
adgenerator	6/16/2021 9:36 AM
adgenerator	6/16/2021 9:36 AM

Open adgenerator and the subfolder to see the PowerShell scripts. Drag and drop nameGen.ps1 to both desktops.



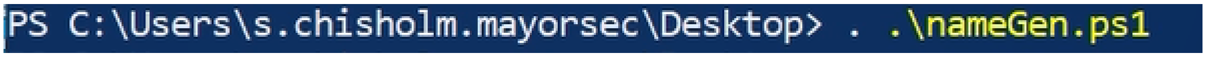
images	6/16/2021 9:36 AM
ADGenerator	6/15/2021 4:37 PM
Invoke-ForestDeploy	6/15/2021 4:37 PM
nameGen	6/15/2021 4:37 PM
README.md	6/15/2021 4:37 PM

Open PowerShell as administrator. Change directories to the user’s desktop and run Set-ExecutionPolicy Unrestricted and say yes to all.

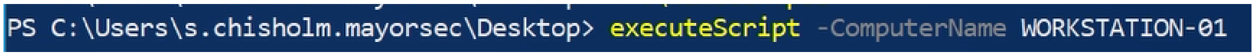


```
PS C:\Users\s.chisholm.mayorsec\Desktop> Set-ExecutionPolicy Unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the
execution policy might expose you to the security risks described in the
about_Execution_Policies help topic at https:/go.microsoft.com/fwlink/?LinkID=135170. D
you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"):
```

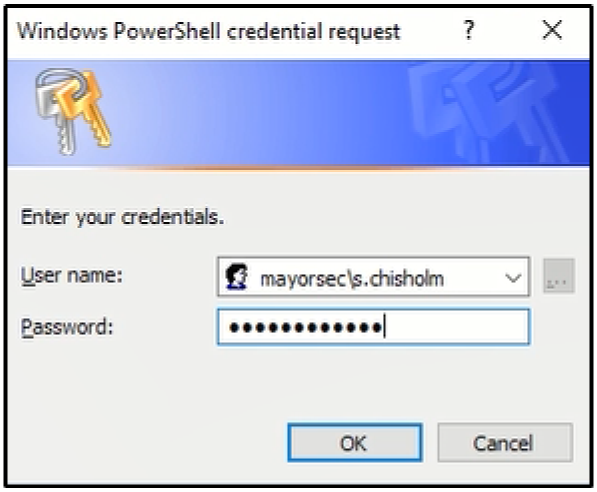
Import nameGen.ps1 and execute the script as follows. You will be asked for credentials for domain users in order to rename the computer at the domain controller.



```
PS C:\Users\s.chisholm.mayorsec\Desktop> . .\nameGen.ps1
```



```
PS C:\Users\s.chisholm.mayorsec\Desktop> executeScript -ComputerName WORKSTATION-01
```



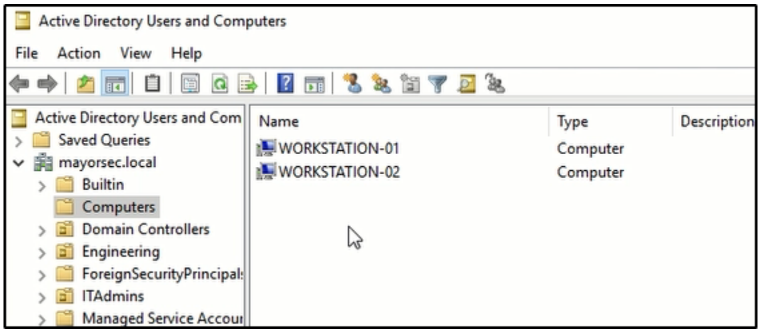
Windows PowerShell credential request

Enter your credentials.

User name: mayorsec\s.chisholm

Password: ●●●●●●●●●●●●●

Restart both computers to commit the changes. Confirm the changes on the domain controller.



Active Directory Users and Computers

- Active Directory Users and Com
  - Saved Queries
  - mayorsec.local
    - Builtin
    - Computers
    - Domain Controllers
    - Engineering
    - ForeignSecurityPrincipal:
    - ITAdmins
    - Managed Service Accour

Name	Type	Description
WORKSTATION-01	Computer	
WORKSTATION-02	Computer	