Adversaries Have it Easy: Having a Peek Behind the Curtain.

Build Your Own Lab At Home

Andy Gill & Neil Lines

Lares Labs

https://labs.lares.com

Contents

Overview

This document will walk you through how to setup a lab environment, step by step regardless of your skill level. It doesn't have all the different vulnerabilities but for a quick win on setup VulnerableAD(https://github.com/WazeHell/vulnerable-AD) will give and pre-configure some known attacks for easy attack paths.

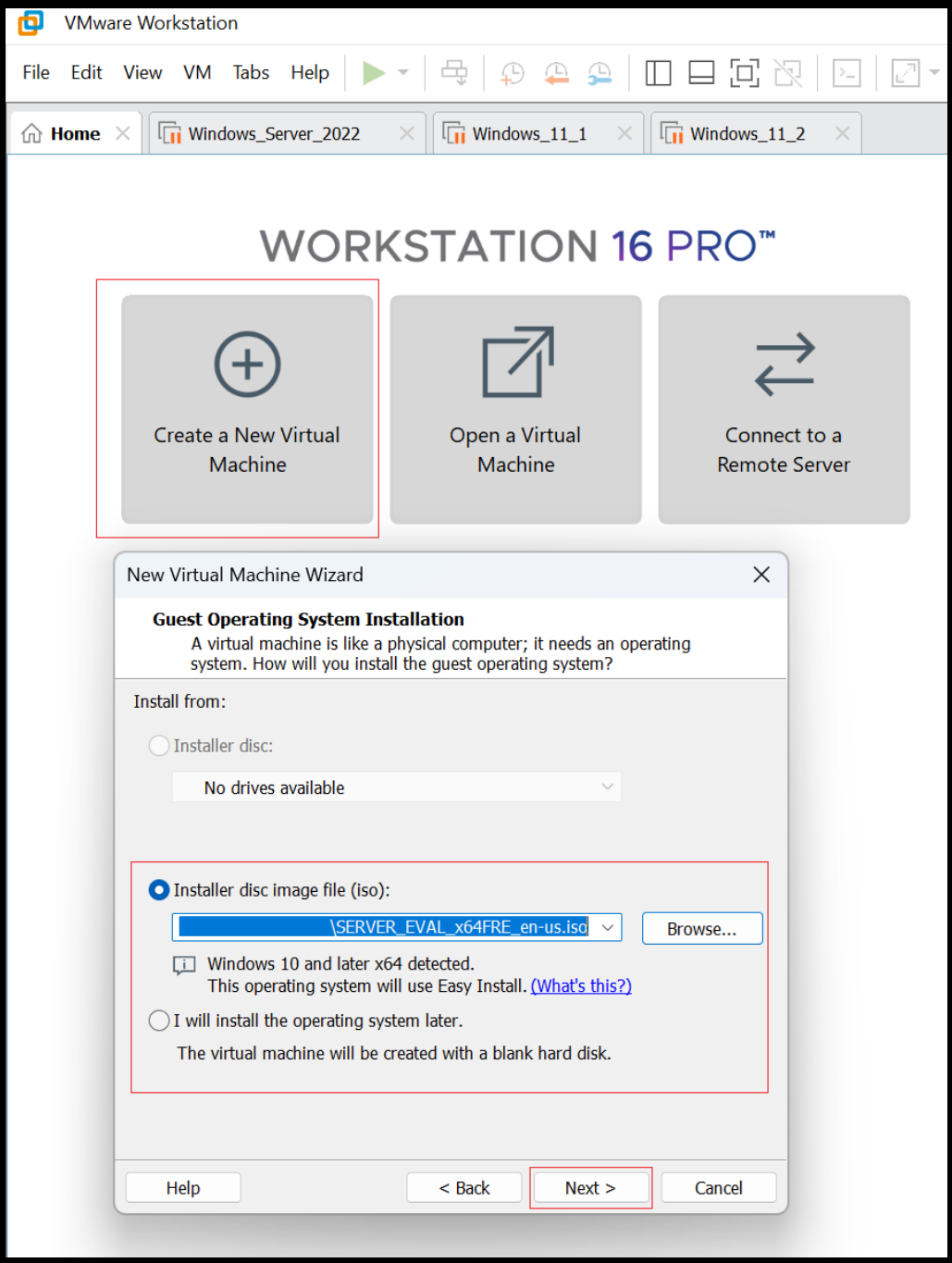
Lab Resources

- Server 2022 ISO: https://info.microsoft.com/ww-landing-windows-server-2022.html
- Windows 11 ISO: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-11-enterprise
- Virtual Box (Needed if you don't have VM): https://www.virtualbox.org/
- Hack Lab Domain Controller https://github.com/myexploit/LAB/blob/master/Hack_Lab_Domain

Server 2022 setup guide

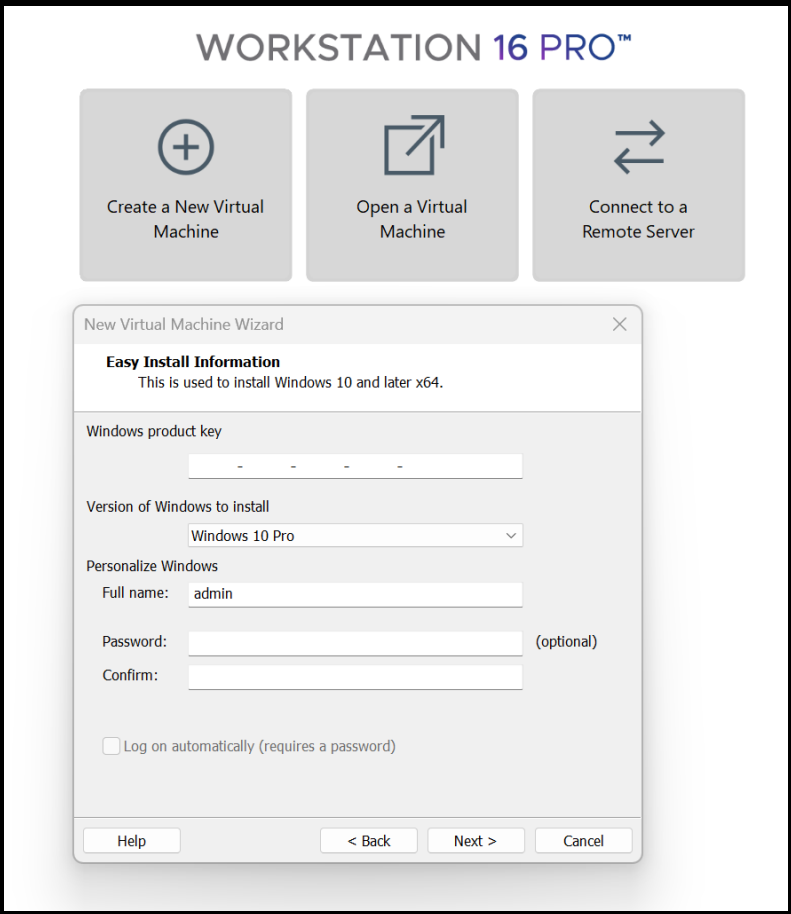
Using VM Workstation

1. Click on create a New Virtual Machine.
2. Select the server 2022 ISO.
3. Click Next.

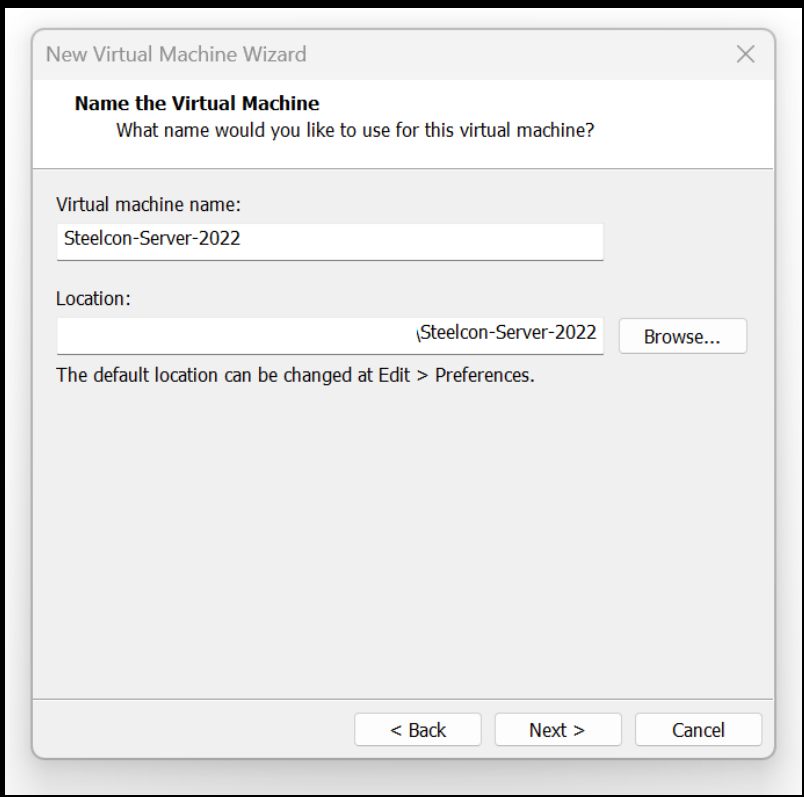


VM 16 didn't have a server 2022 predefined setup so opted for Windows 10 Pro.

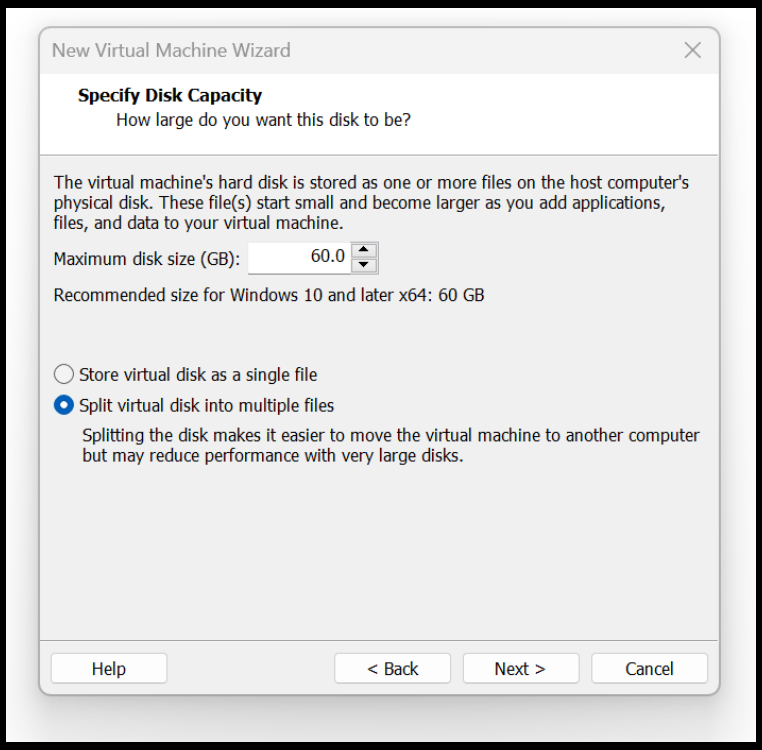
4. Add an account name.
5. Add a password.



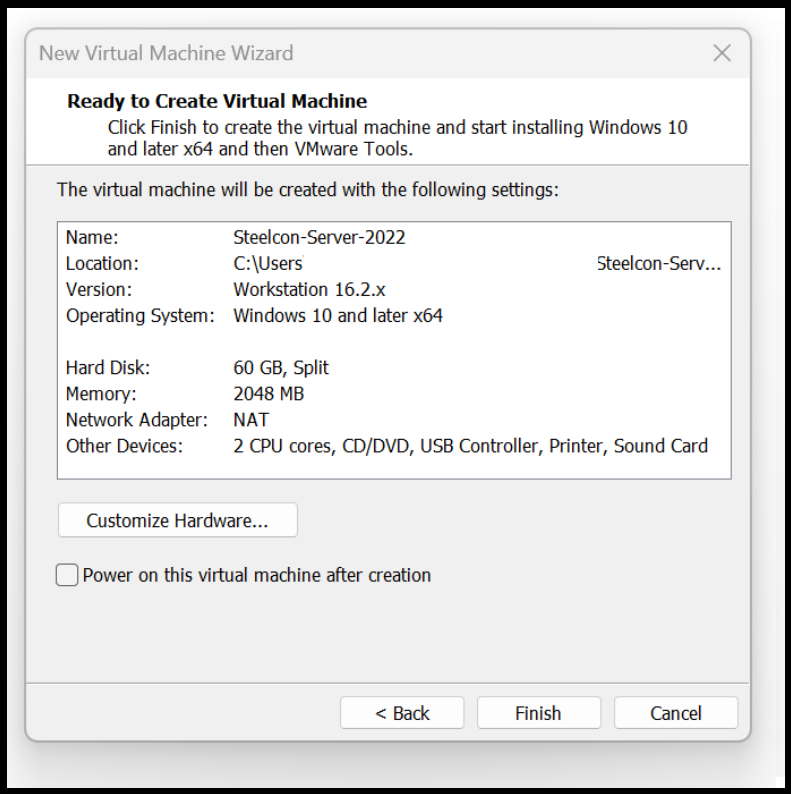
6. Rename the virtual machine.
7. Rename the location name to match (not required but for logical reason it makes sense.)
8. Click Next.



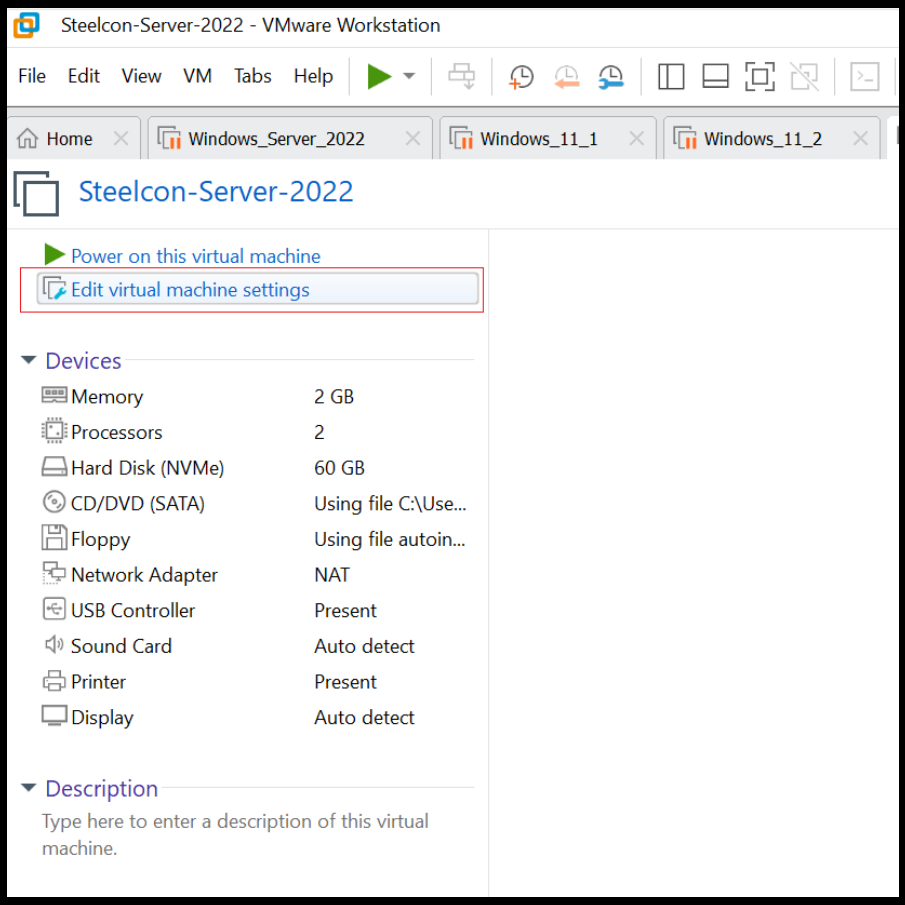
9. VM defaults to 60 GB of storage, but you should be able to get by with 30-40 GB if you're short on space?
10. Click Next.



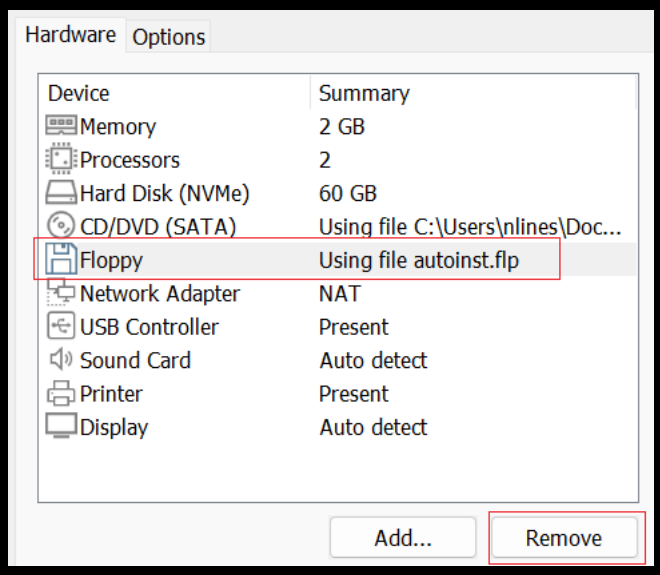
11. Untick' Power on this virtual machine after creation'.
12. Click Finish.



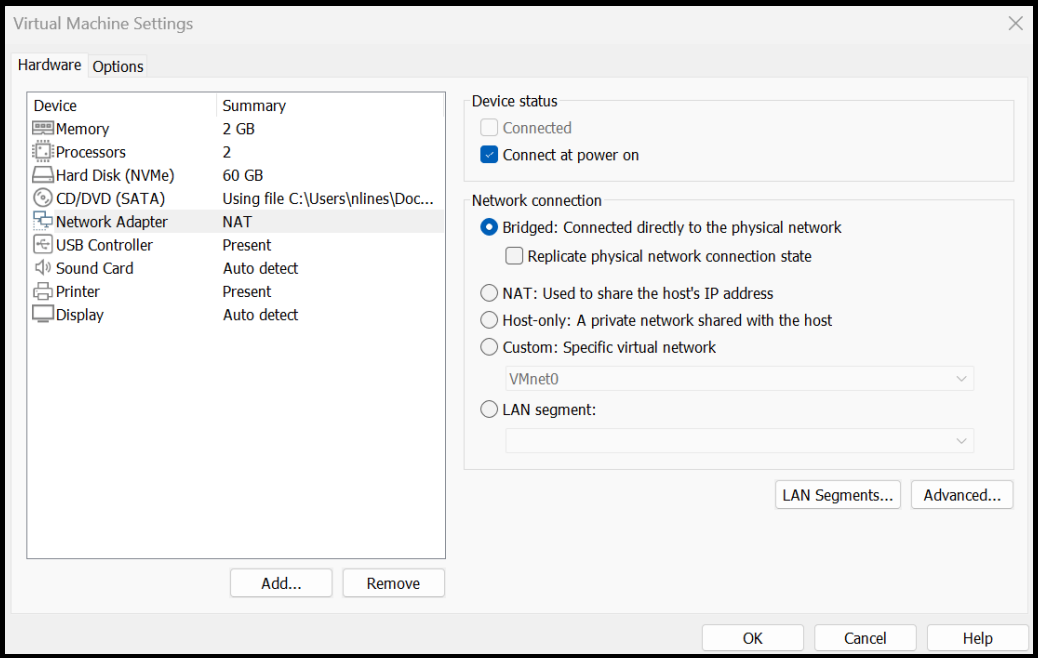
13. Click on 'Edit virtual machine settings.'



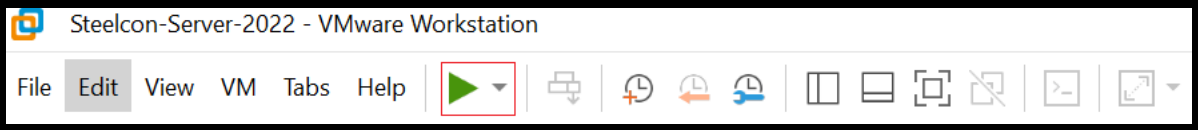
14. Click on Floppy and Remove.



15. Click on Network Adapter and change from NAT to Bridged: Connected directly to the physical network' (This is dependent of location and if there is a DHCP server, if not pick Custom: Specific virtual network and select whichever one you have configured VM to offer a DHCP IP address on, then make sure all your other LAB VM's are on the same network so they can communicate with each other.



16. Click on Start up the guest machine.

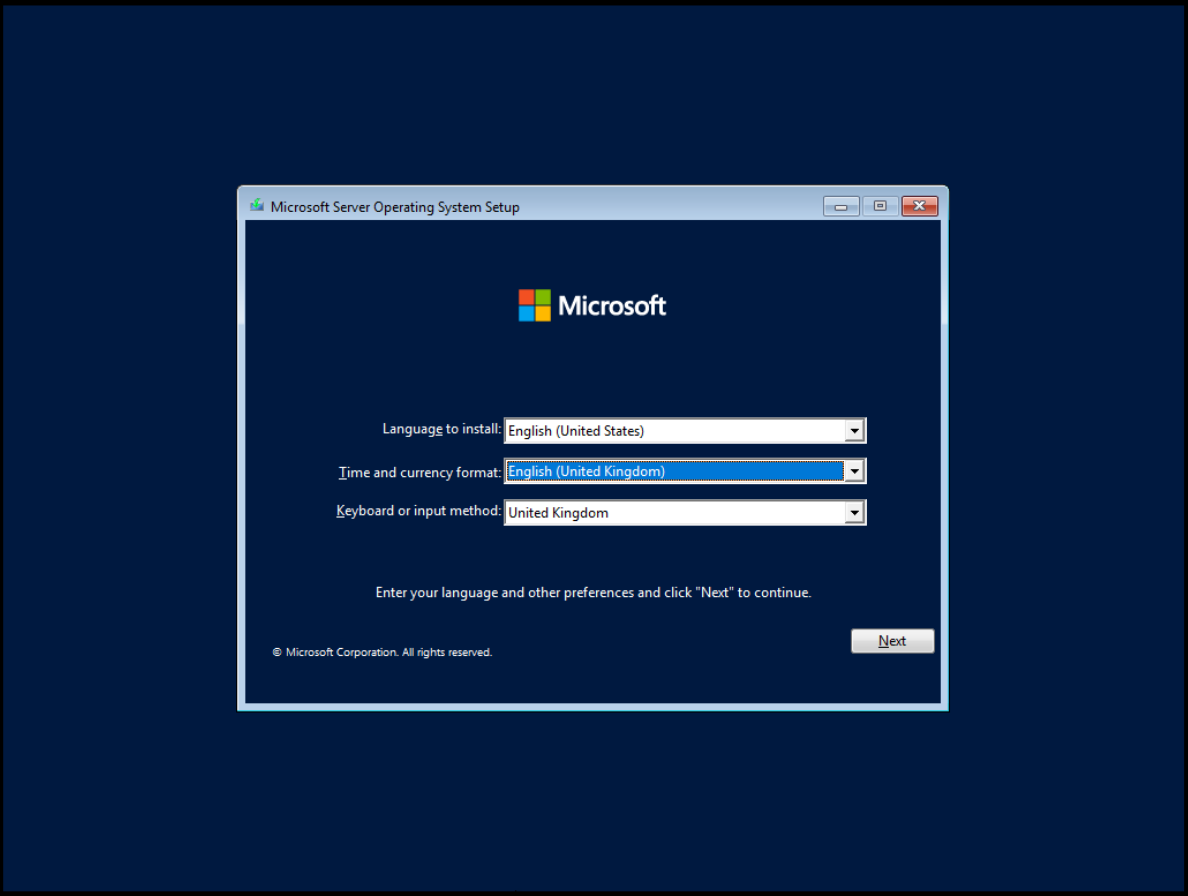


17. First boot you see the VM BIOS splash followed by Press any key to boot from CD or DVD, you must click in the screen and press enter fast!!

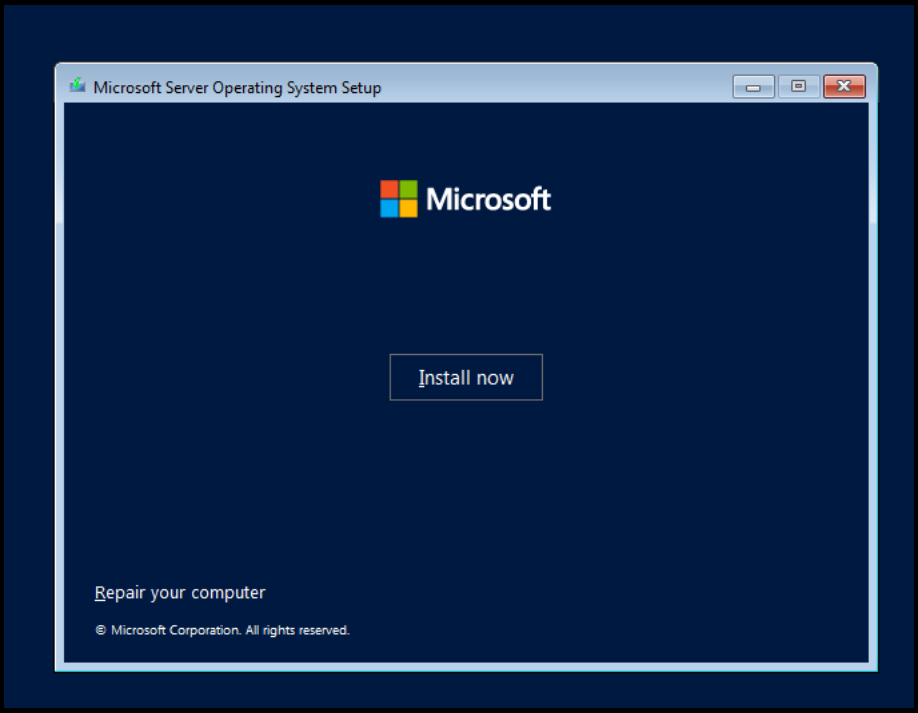
If you miss it don't worry just restart the VM and repeat until you get it!


```
Press any key to boot from CD or DVD.
```

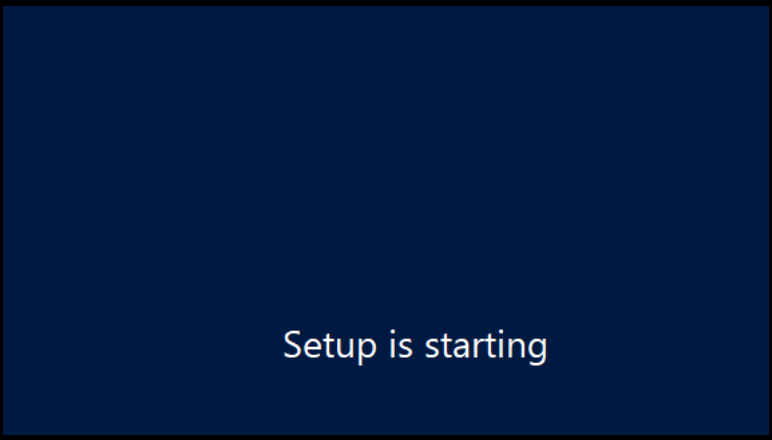
18. You should see a Windows splash screen press enter.
19. Change options to English.
20. Click Next.



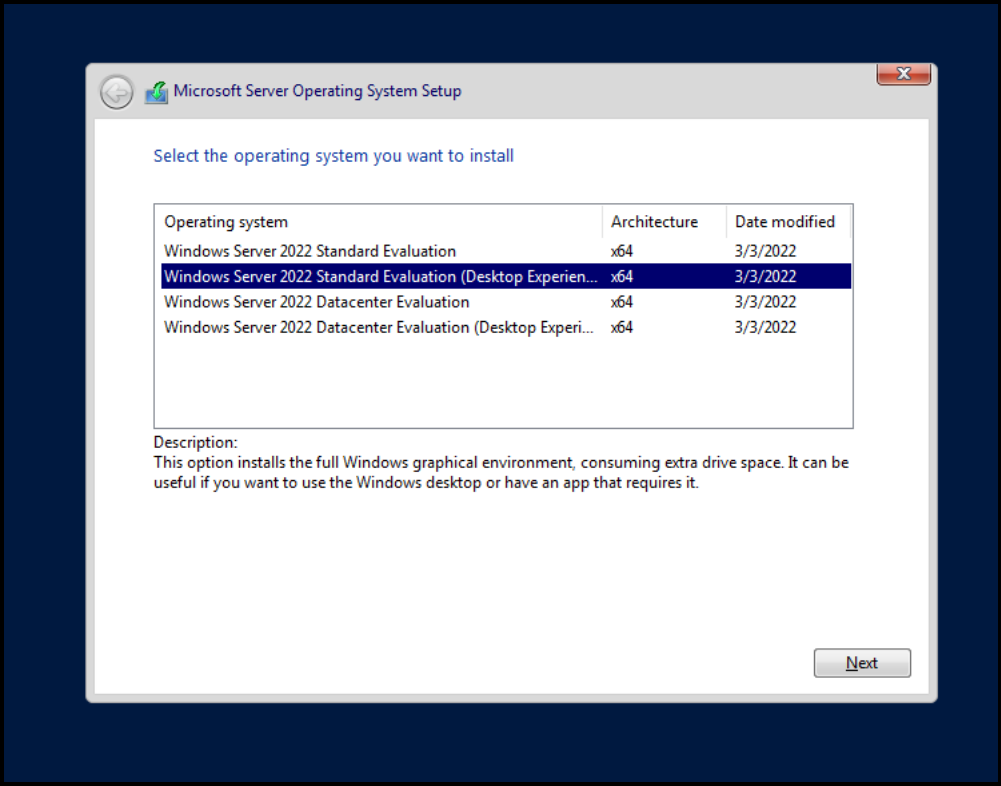
21. Click Install now.

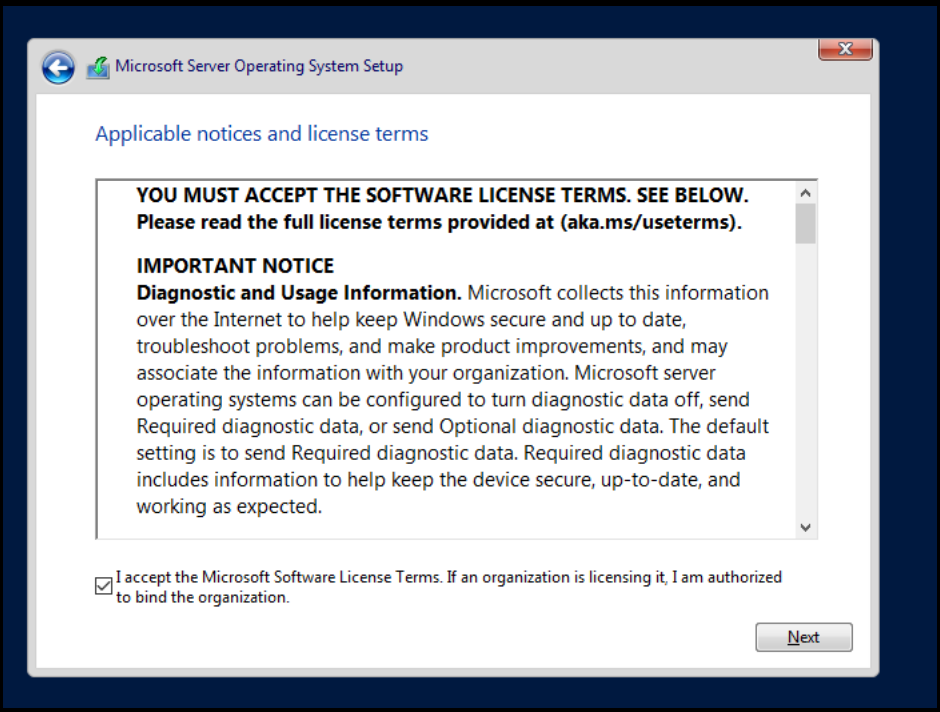


You should see Setup is starting.

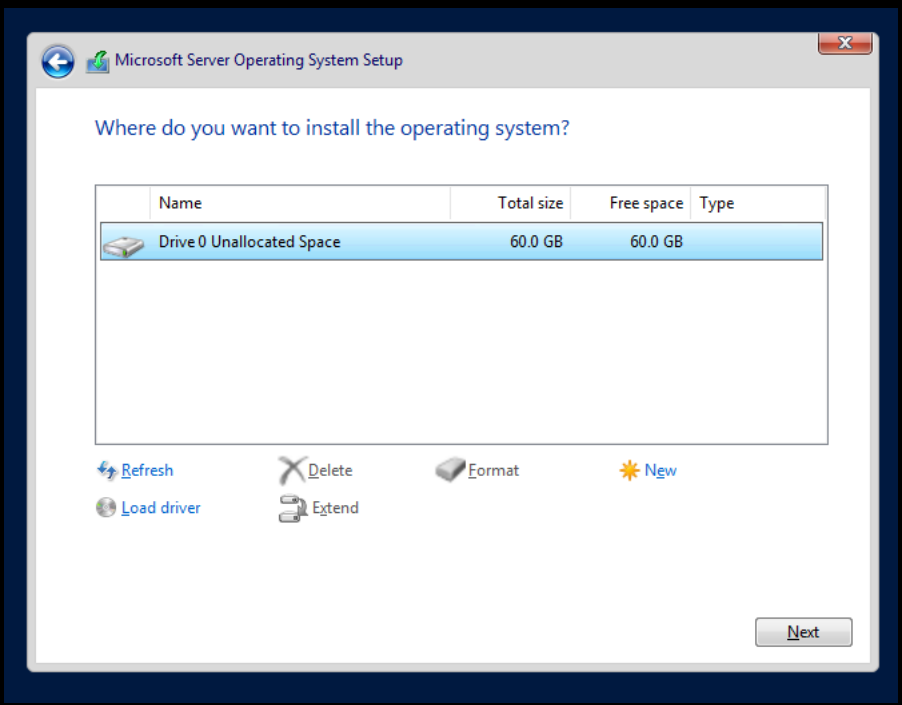


22. Make sure you pick an option with Desktop Experience, or you will install server core. (Pick the second option in the list).
23. Click Next

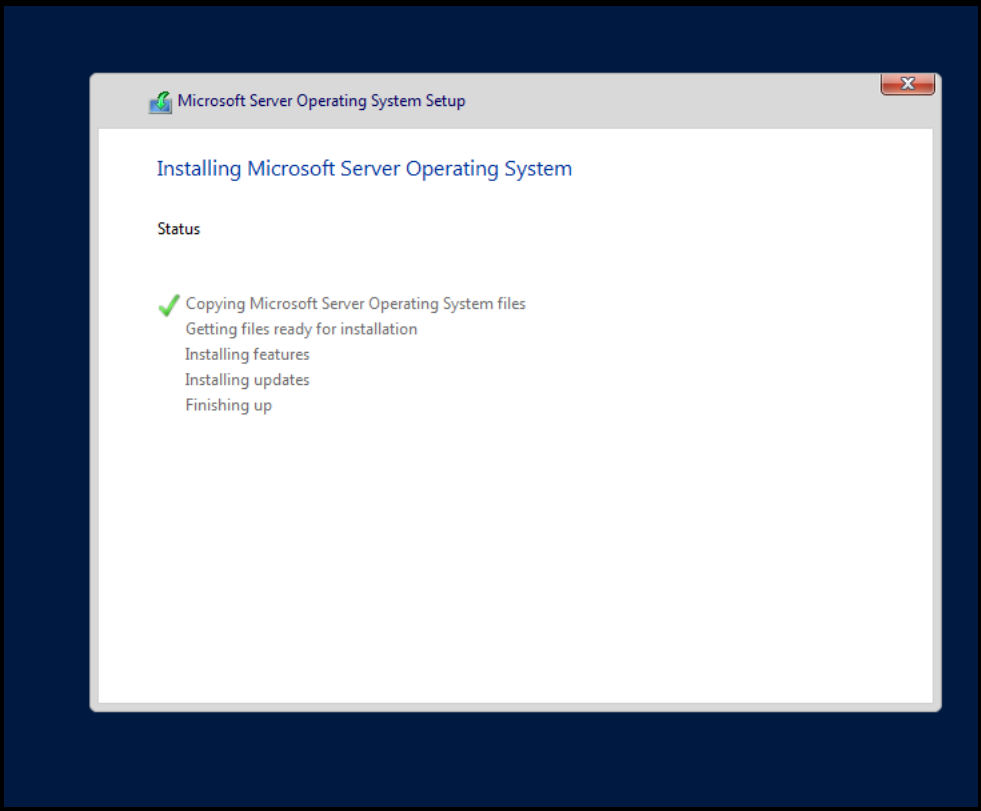




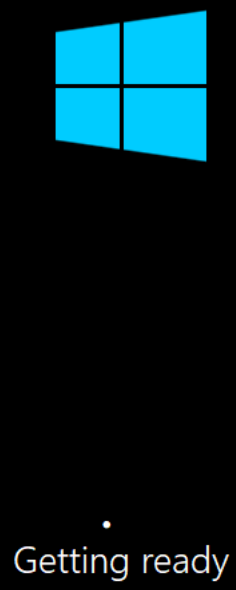
24. Tick the Terms.
25. Click Next.
26. The next option offers you Upgrade or Custom Installation, Select Custom Installation.
27. Click Next.



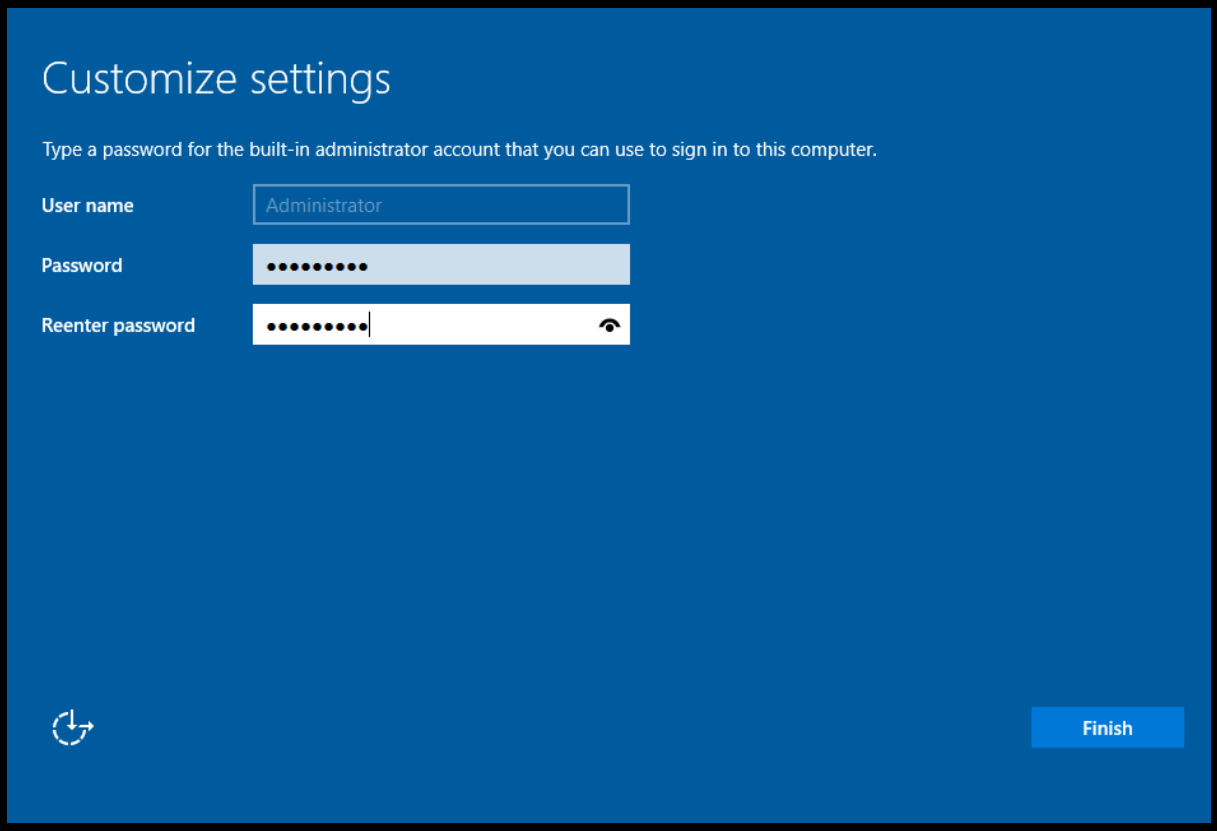
It should redirect to the installing page.



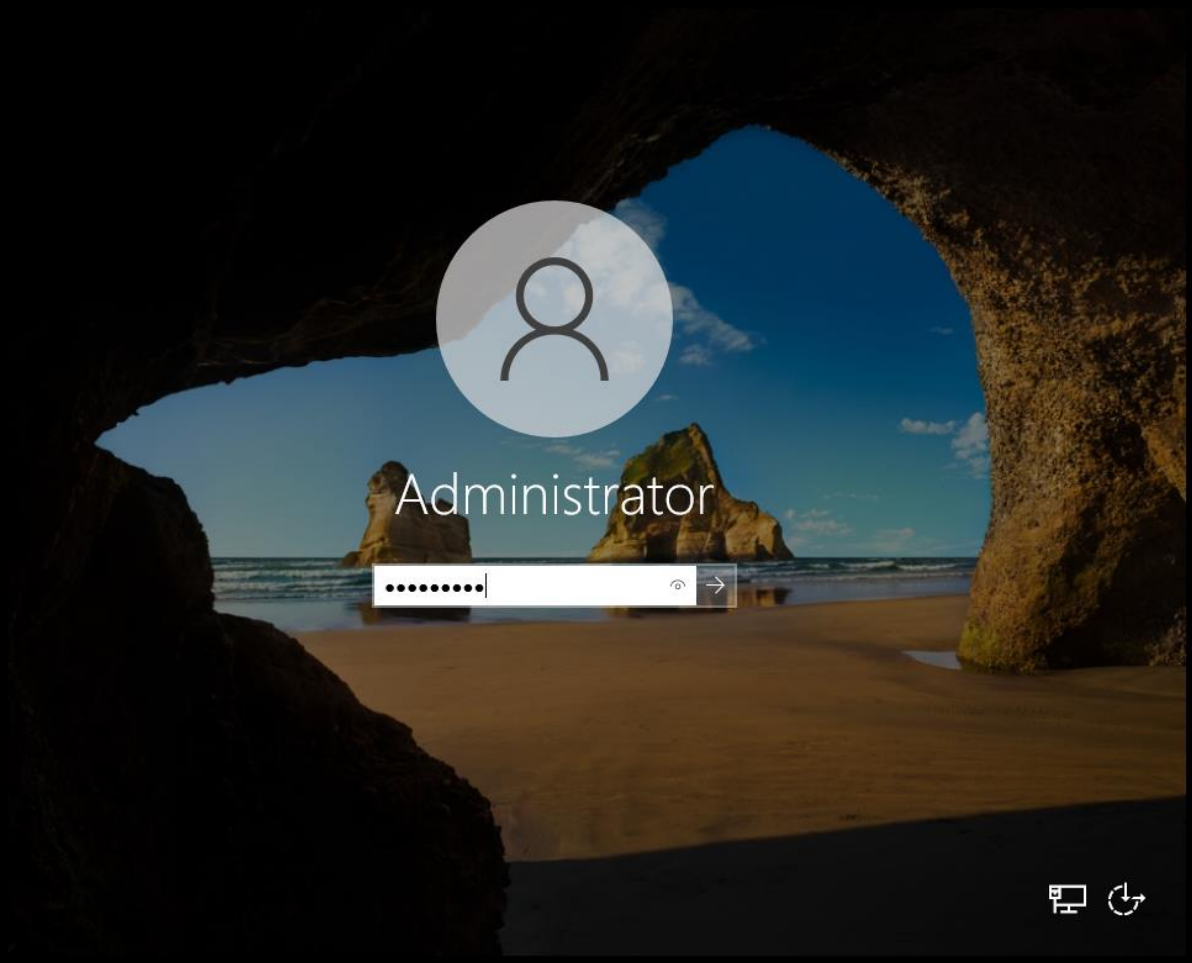
During the install it should auto reboot.



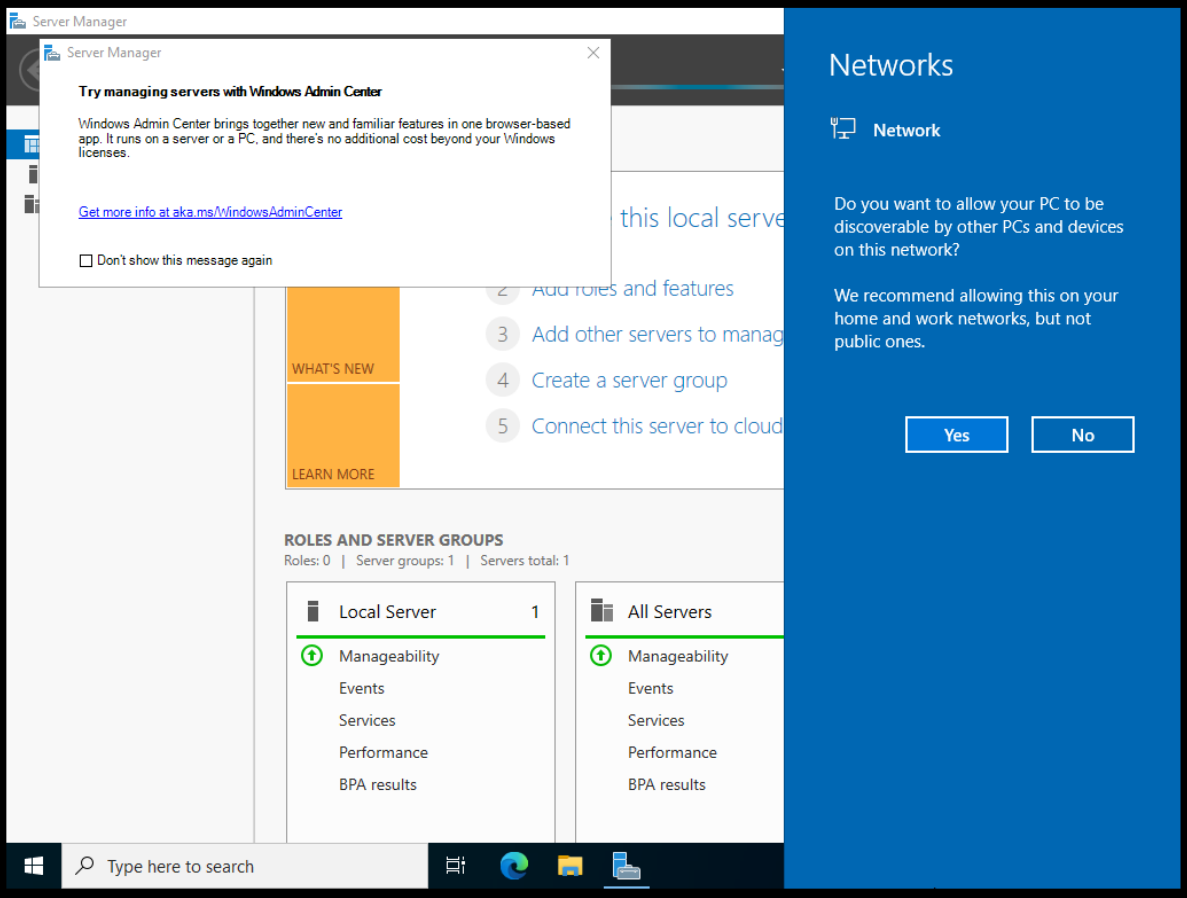
28. Add a password for the Administrator account (Select a password you can 100% remember).
29. Click Finish.



30. Login using the password you just set.

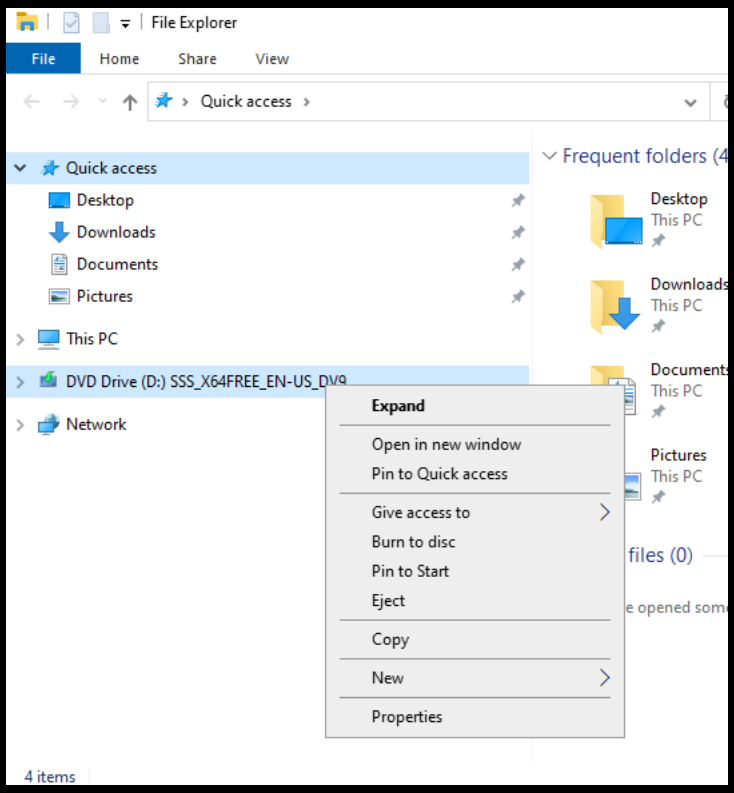


31. Click Yes on the Networks option.

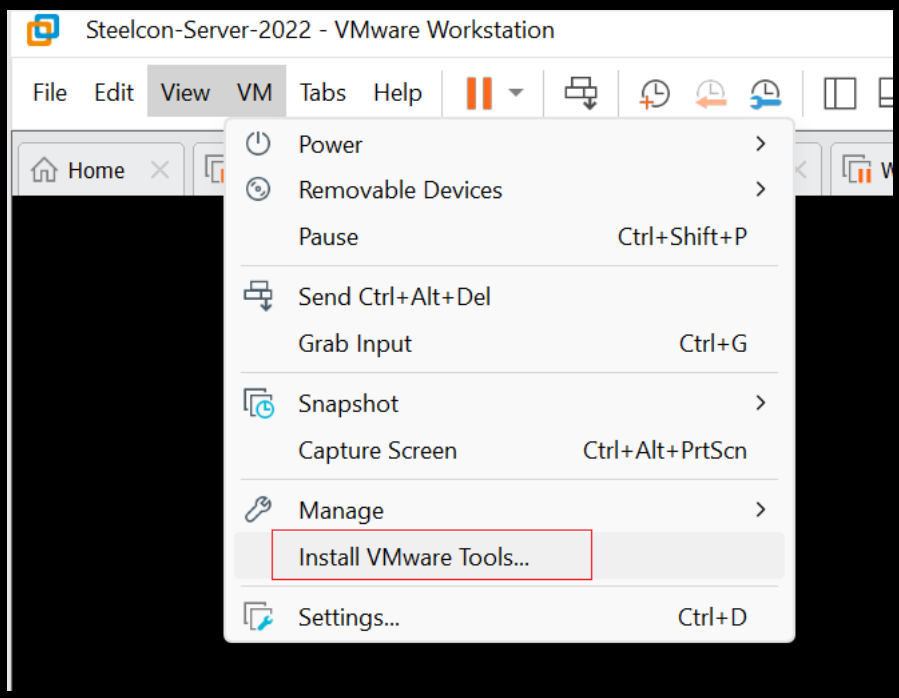


32. Click file explorer which is on the bottom toolbar.

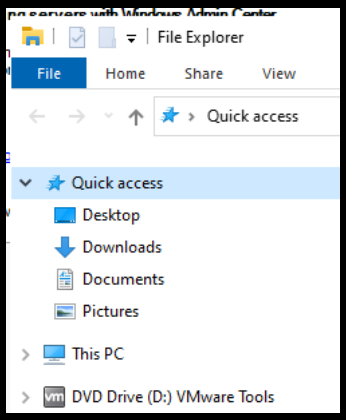
33. Right click on the DVD Drive and select Eject (so you can mount and install VM tools).



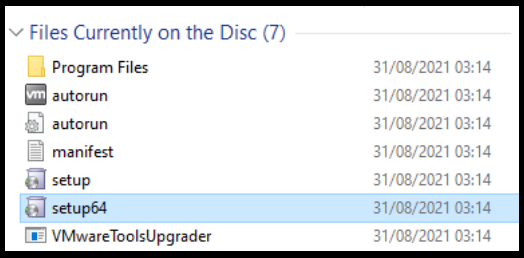
34. Click on VM tool bar, select VM then click Install VMware Tools…



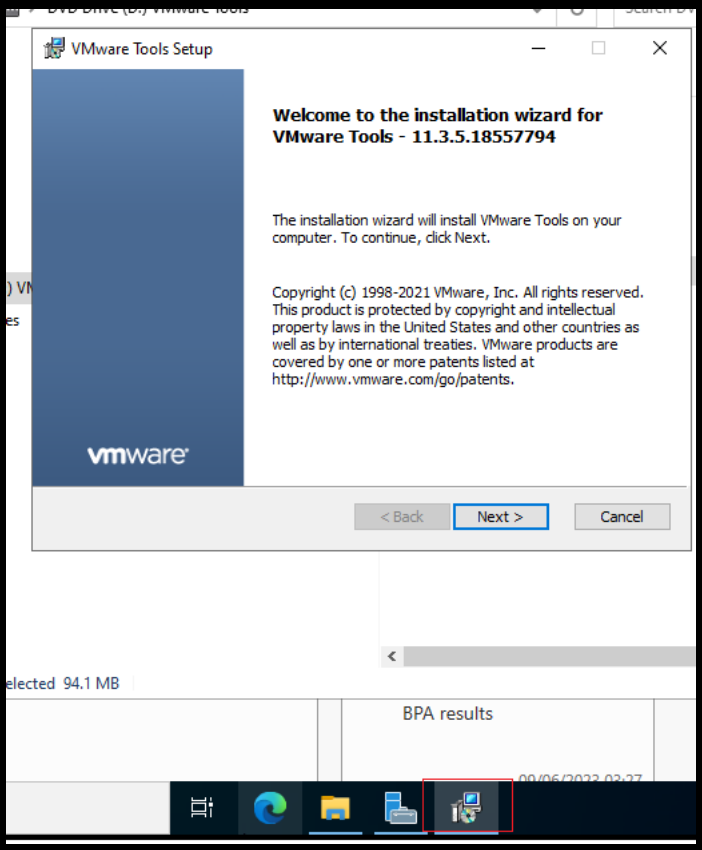
35. The VM tools Disk should mount the DVD Drive.
36. Double click to open.



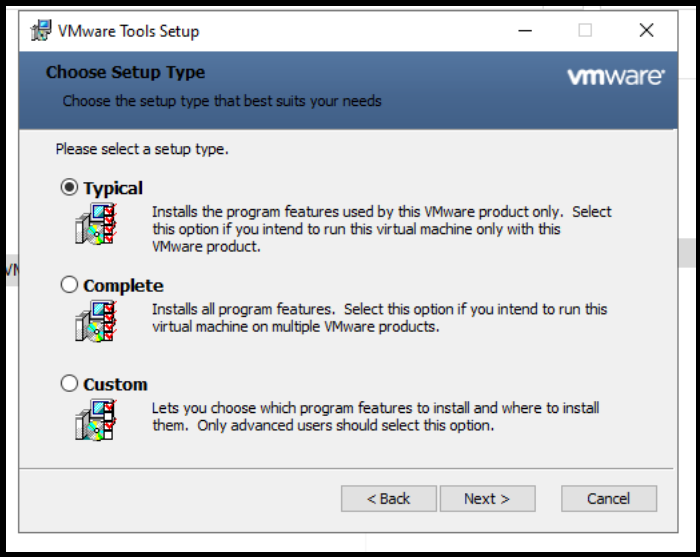
37. Double click 'setup64' to start installing VM Tools.



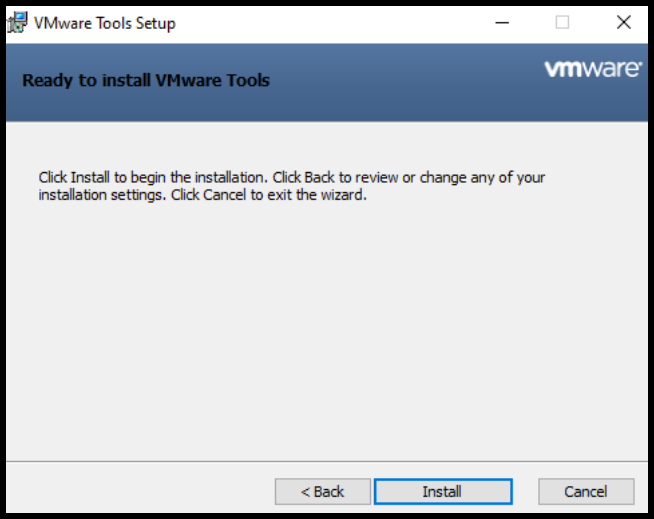
38. The VM tools installer will flash on the bottom taskbar, click it.
39. Click Next.



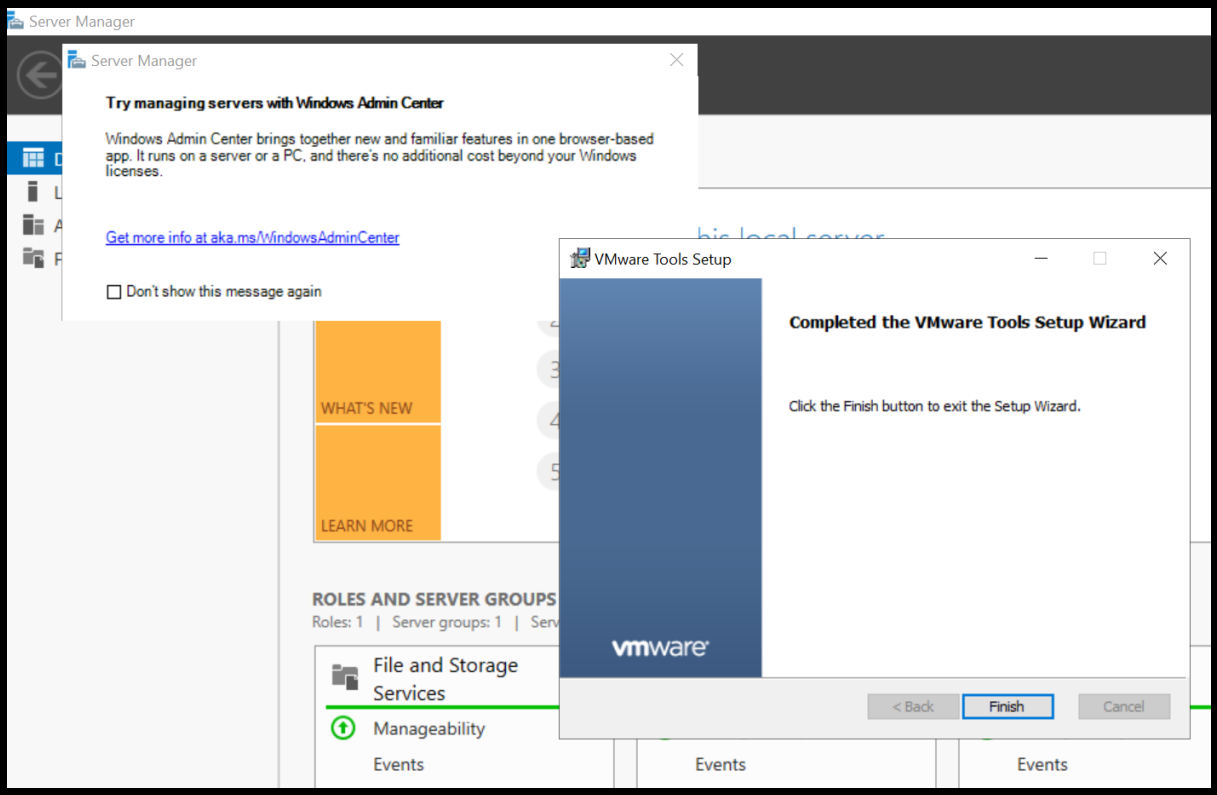
40. Select Typical
41. Click Next.



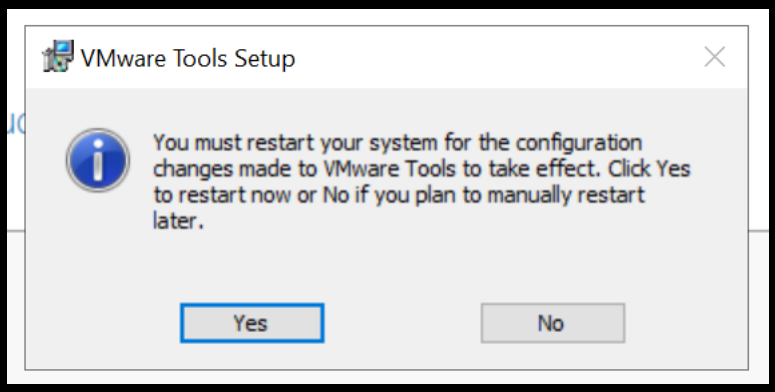
42. Click Install.



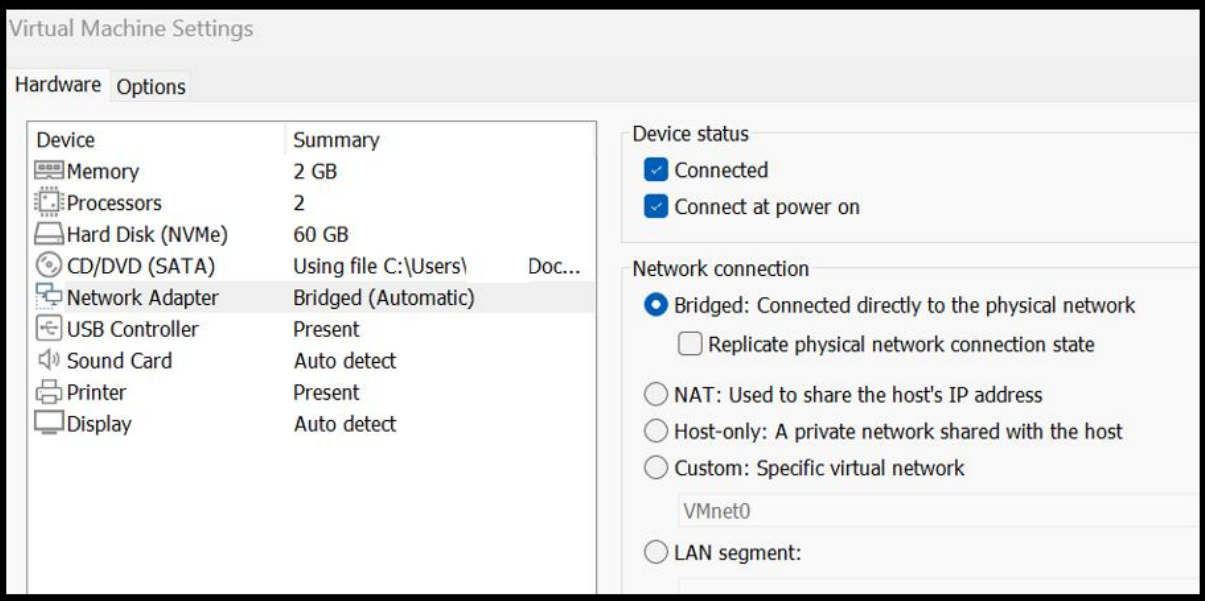
Once it finishes installing you will see the screen resolution improve, and the VM should the fill your monitor, if not reboot it.



43. VM Tools Setup Asks you to restart.



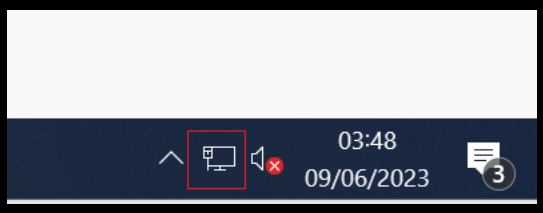
It is strongly recommended that you assign a static IP address to any server, this demo includes a walkthrough on how to assign an IP address using the network configuration we set for this demo.



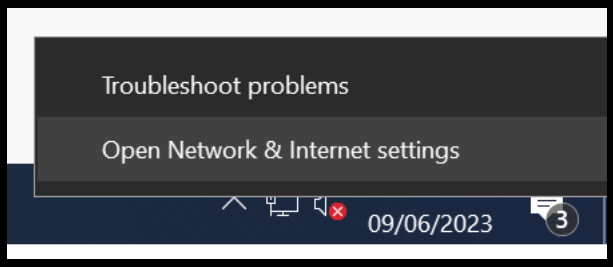
If you don't set a static IP address, there is a high chance that DNS will fail to resolve the domain name for any joining host machines.

This demo should also work for those who during the initial network settings opted for Custom, just make sure the VM custom network provides DHCP, you can do this by looking under VM tool bar \ Edit \ Virtual Network Editor.

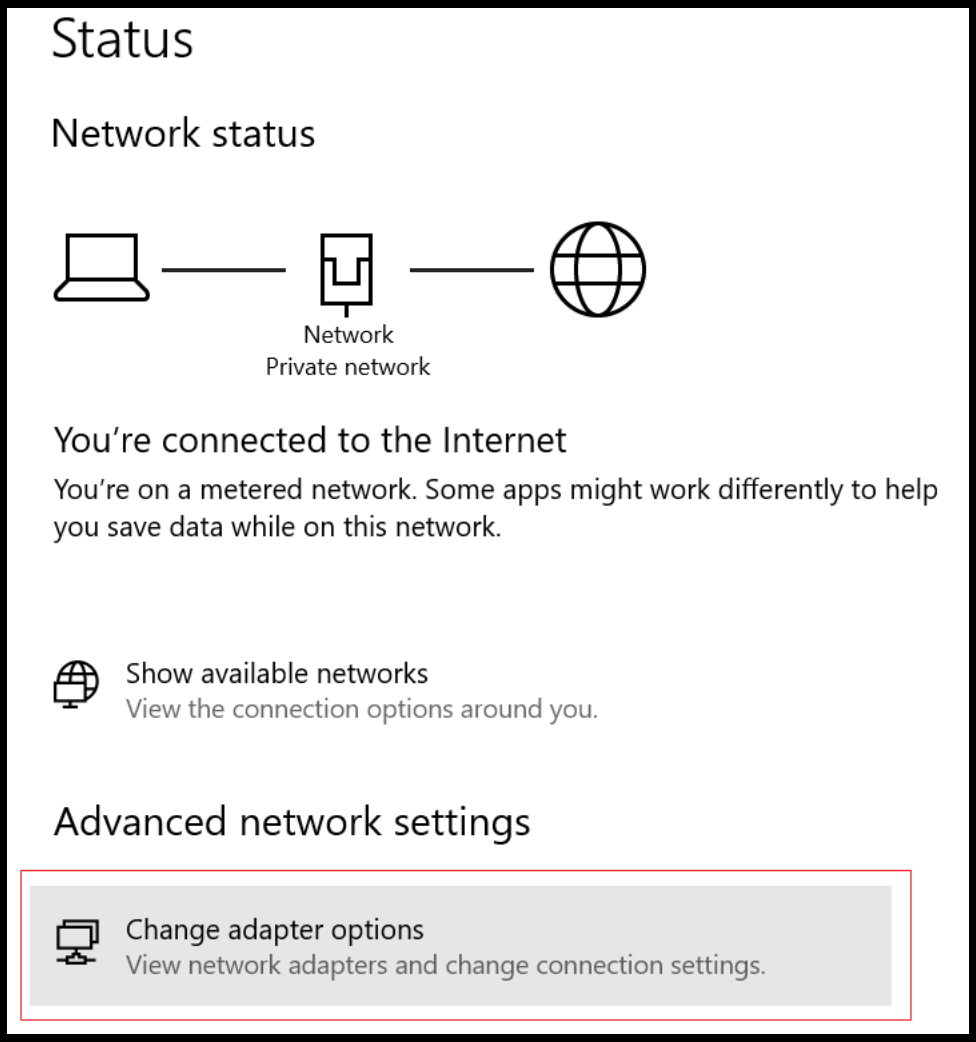
44. Login to the Server 2022 VM and on the Windows bottom tool bar towards the clock right click on Network Internet Access option.



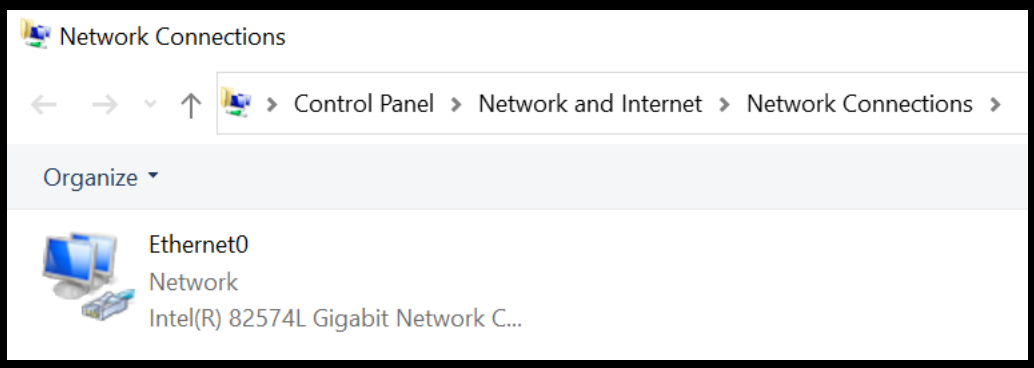
45. Select Open Network & Internet settings.



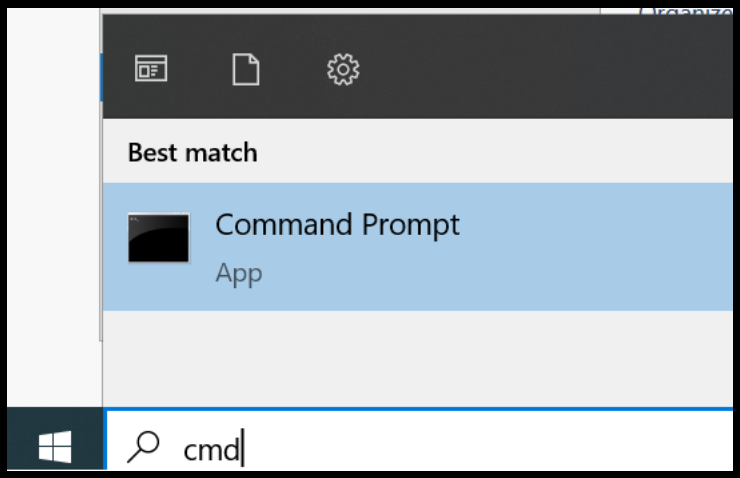
46. Click on Change adaptor options.



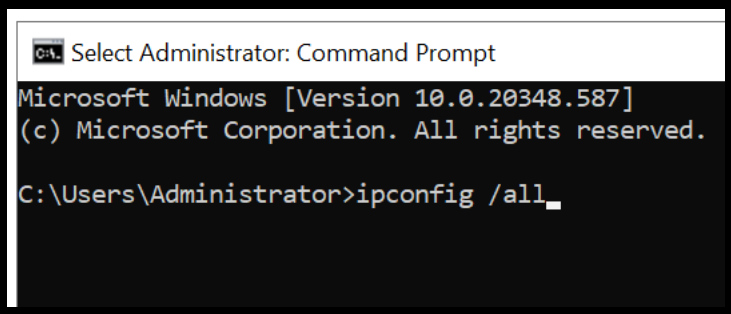
Which should allow you access to your network card.



47. Before we change that, open CMD (type cmd into search bar, which is next to the windows button, bottom tool bar, to the left).



48. Type in ipconfig /all
49. Press enter and make a note of your original IP address.

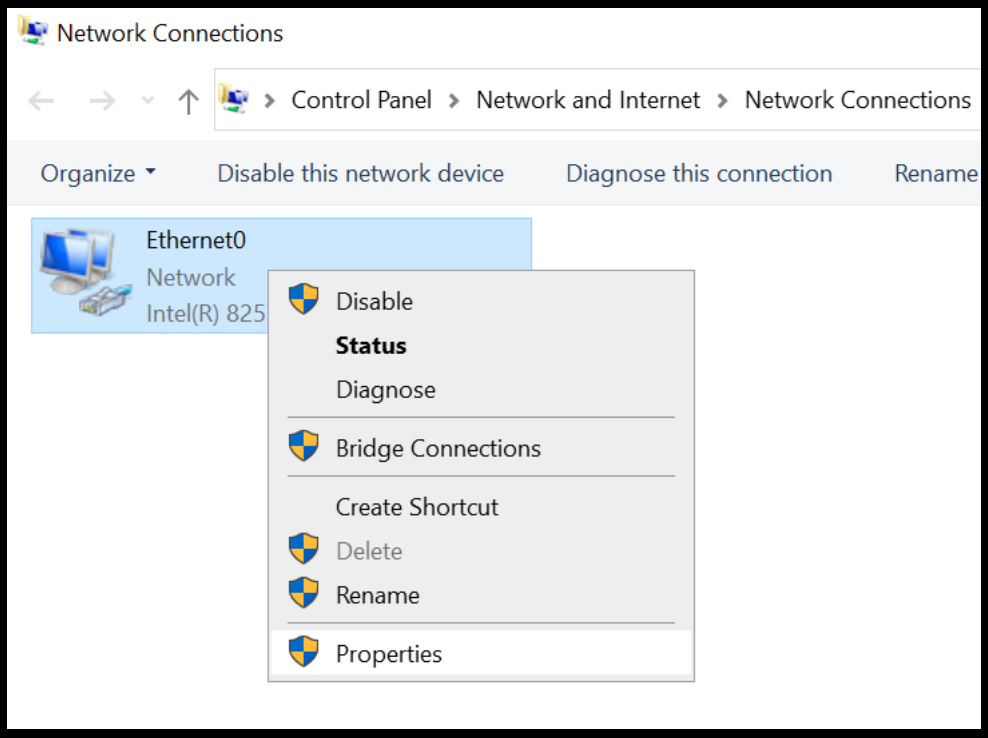


In this demo our IP address is 192.168.68.125 our subnet is 255.255.255.0 (/24), default gateway and DNS IP addresses are 192.168.68.1 make a note of your addresses.

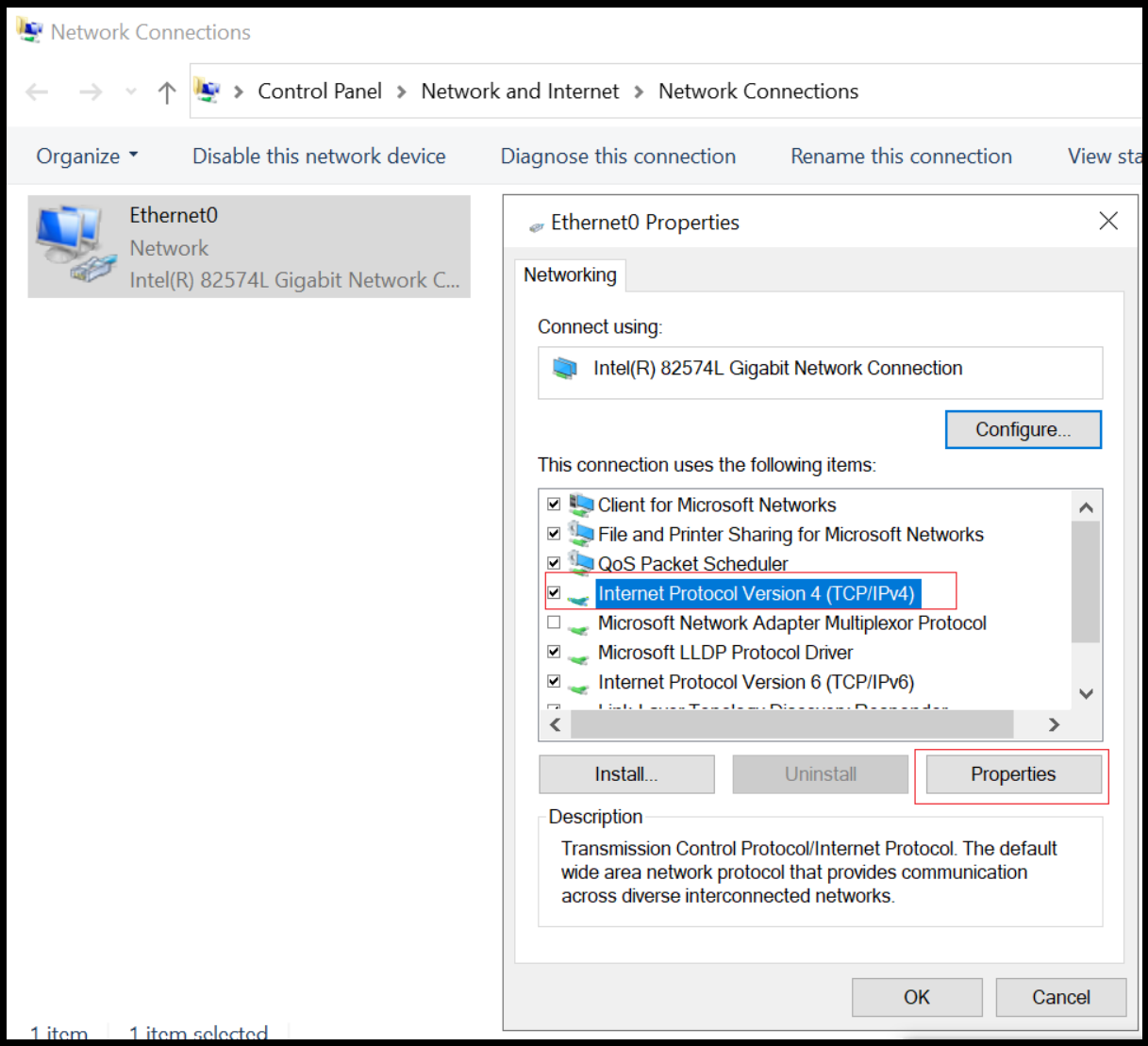
Administrator: Command Prompt

```
   Host Name . . . . . . . . . . . . : [redacted]
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : [redacted]
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : 192.168.68.125(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 09 June 2023 03:41:53
   Lease Expires . . . . . . . . . . : 09 June 2023 05:41:52
   Default Gateway . . . . . . . . . : [redacted]
                                       192.168.68.1
   DHCP Server . . . . . . . . . . . : 192.168.68.1
   DHCPv6 IAID . . . . . . . . . . . : [redacted]
   DHCPv6 Client DUID. . . . . . . . : [redacted]
   DNS Servers . . . . . . . . . . . : 192.168.68.1
```

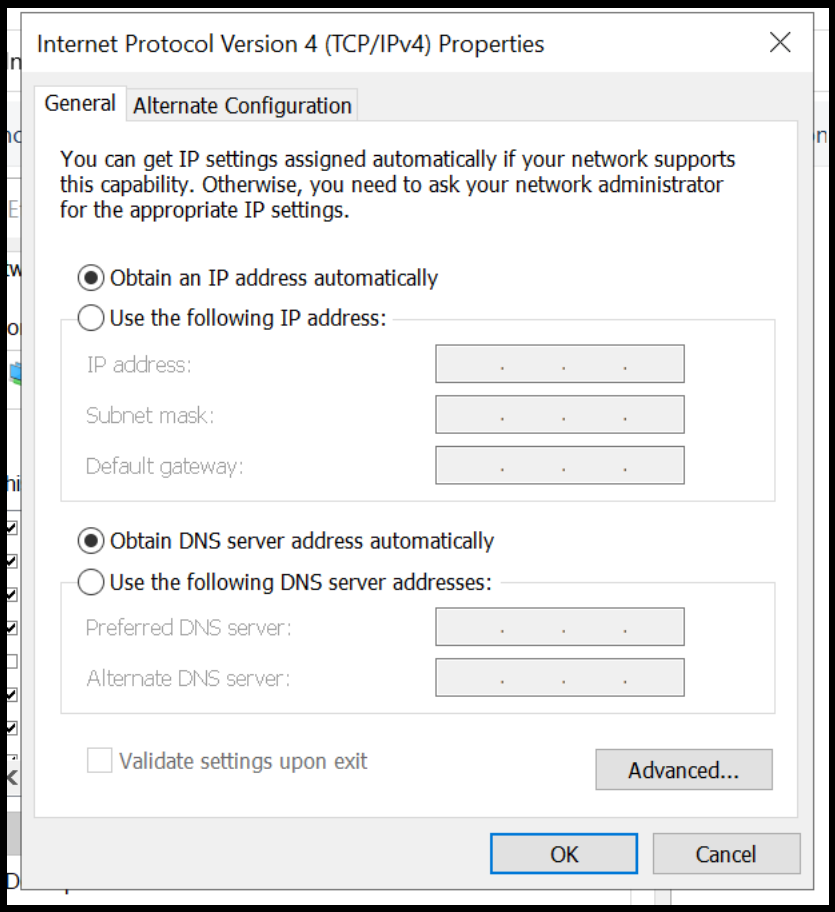
50. Go back to the Network card and right click and select Properties.



51. Click on Internet Protocol Version 4 (TCP/IPv4) so it is selected.
52. Then click on Properties.



This will open the Network card IP4 configuration options which by default, are as such.



53. Select Use the following IP address.

Now look back at your CMD open session as you need to set an IP address from within that IP range.

Below is the IP address that we were allocated during this demo.

IPv4 Address. . . . . : 192.168.68.125(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway 192.168.68.1
DNS Servers . . . . . : 192.168.68.1

As an example, under our circumstances we would set the servers static IP address configuration as such.

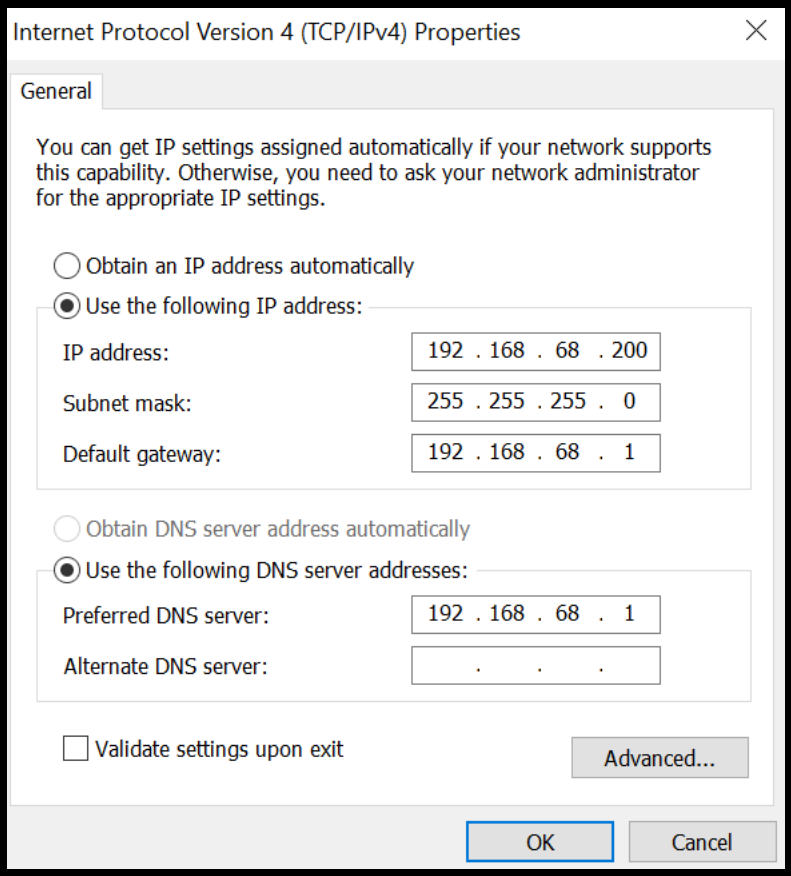
IP address: 192.168.68.200

Subnet mask: 255.255.255.0

Default gateway: 192.168.68.1

Preferred DNS Server: 192.168.68.1

54. Add your configuration, then click OK.



55. Close network settings, and go back to CMD.
56. Verify the settings changed by typing in ipconfig /all.
57. Check you can access the default gateway via pinging it's IP address.

```
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . :
   IPv4 Address. . . . . . . . . . . : 192.168.68.200(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
                                       192.168.68.1
   DHCPv6 IAID . . . . . . . . . . . :
   DHCPv6 Client DUID. . . . . . . . :
   DNS Servers . . . . . . . . . . . : 192.168.68.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Administrator>ping 192.168.68.1

Pinging 192.168.68.1 with 32 bytes of data:
Reply from 192.168.68.1: bytes=32 time=5ms TTL=64
Reply from 192.168.68.1: bytes=32 time=3ms TTL=64
Reply from 192.168.68.1: bytes=32 time=5ms TTL=64
Reply from 192.168.68.1: bytes=32 time=7ms TTL=64

Ping statistics for 192.168.68.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 7ms, Average = 5ms
```

Depending on how you configured your VM network setting, you may also wish to test access to the internet from the VM server. Internet access is not required for lab testing but is always nice to have.

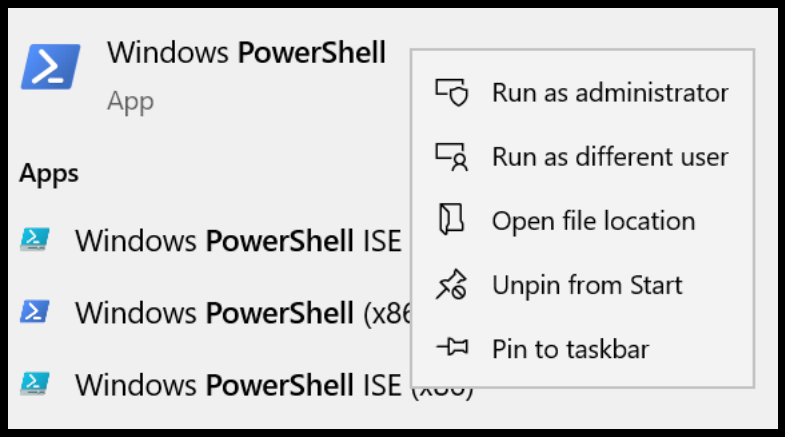
```
Pinging new-fp-shed.wg1.b.yahoo.com [87.248.100.215] with 32 bytes of data:
Reply from 87.248.100.215: bytes=32 time=40ms TTL=52
Reply from 87.248.100.215: bytes=32 time=31ms TTL=52

Ping statistics for 87.248.100.215:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 40ms, Average = 35ms
Control-C
^C
C:\Users\Administrator>
```

And with that your Server 2022 should be built and be ready to convert into a domain controller.

How to convert your server into a domain controller

Easy use a PowerShell script that does it all for you.

1. Search for PowerShell, right click on it and select Run as administrator.



Presented by Andy Gill & Neil Lines at Steelcon 2023

2. Copy and paste the following into the PowerShell session:

```
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force ;
Install-WindowsFeature AD-Domain-Services  ; Import-Module ADDSDeployment ;
Install-ADDSForest  -DatabasePath "C:\Windows\NTDS"  -DomainMode
"Win2008R2"  -DomainName "hacklab.local"  -DomainNetbiosName "HACKLAB"  -
ForestMode "Win2008R2"  -InstallDns:$true  -LogPath "C:\Windows\NTDS"  -
NoRebootOnCompletion:$true  -SysvolPath "C:\Windows\SYSVOL"  -Force:$true ;
Add-WindowsFeature RSAT-AD-Tools ; Restart-Computer
```

The above script was taken from https://github.com/myexploit/LAB/blob/master/Hack_Lab_Domain

For those who like to know what the one-liner is doing read below.

Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force: This command installs the NuGet package provider on your system. NuGet is a package manager for .NET, allowing you to install and manage software libraries and packages easily.

Install-WindowsFeature AD-Domain-Services: This command installs the Active Directory Domain Services role on your Windows server. Active Directory is a directory service provided by Microsoft that enables centralized management of users, groups, and computers in a network environment.

Import-Module ADDSDeployment: This command imports the ADDSDeployment module, which provides additional cmdlets for deploying Active Directory.

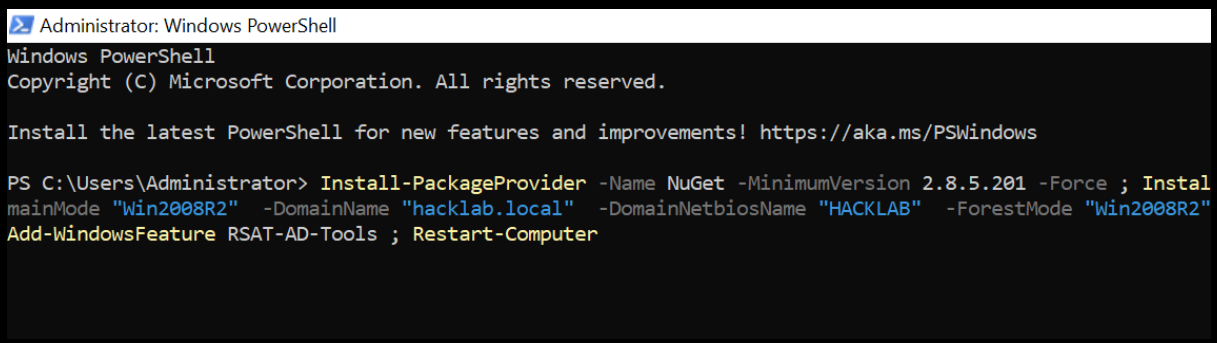
Install-ADDSForest: This command installs and configures a new Active Directory forest with the specified settings on your server. The provided parameters define various configuration options, such as the database and log file paths, Domain and forest modes, DNS installation, and more.

Add-WindowsFeature RSAT-AD-Tools: This command installs the Remote Server Administration Tools for Active Directory (RSAT-AD-Tools). These tools allow you to manage Active Directory from a different computer remotely.

Restart-Computer: This command restarts the computer to apply any changes made during installation.

These commands are used to automate the installation and configuration of Active Directory Domain Services on a Windows server, creating a new domain with the specified settings.

After pasting the one-liner in you will see each stage been configured.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

 Start Installation...
    46%
    [oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

Add-WindowsFeature RSAT-AD-Tools ; Restart-Computer

Name                        Version         Source          Summary
----                        -------         ------          -------
nuget                       2.8.5.208       https://onege... NuGet provider for the OneGet meta-package manager
```

3. During which you will be asked to add a password, it is important you remember this password.

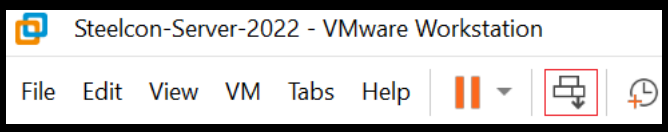
```
PS C:\Users\Administrator> Install-PackageProvider -Name NuGet -
mainMode "Win2008R2"  -DomainName "hacklab.local"  -DomainNetbio
Add-WindowsFeature RSAT-AD-Tools ; Restart-Computer

Name                        Version         Source
----                        -------         ------
nuget                       2.8.5.208       https://onege...

Success        : True
RestartNeeded  : No
FeatureResult  : {Active Directory Domain Services, Remote Server
ExitCode       : Success

SafeModeAdministratorPassword: *********
```

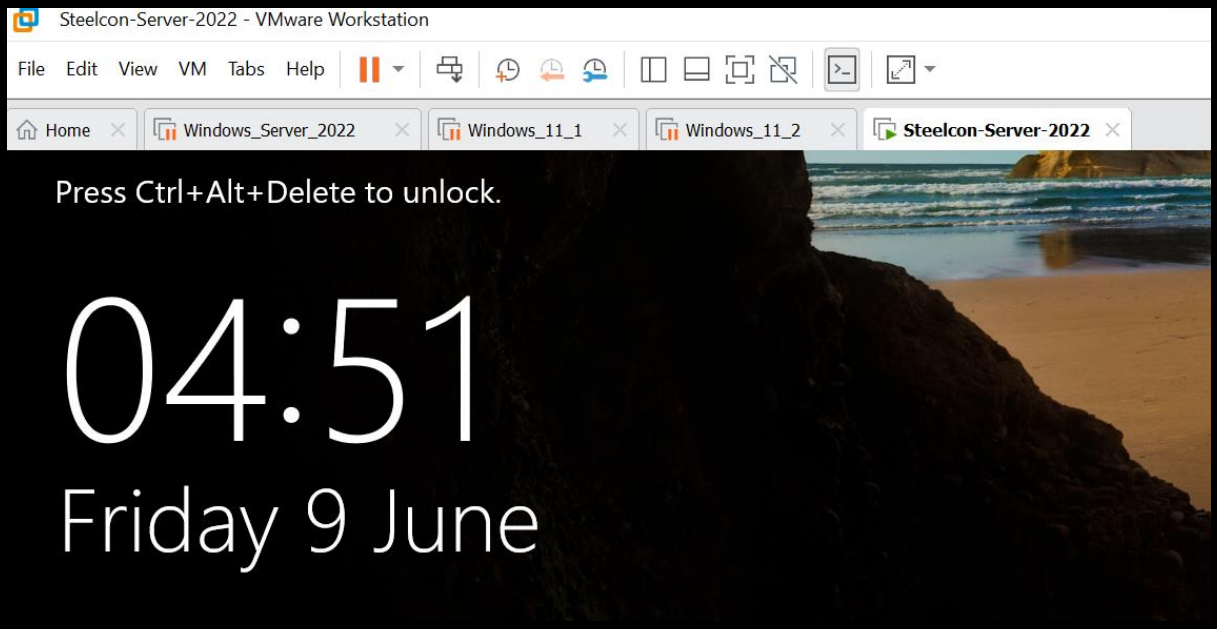
```
Message        : You must restart this computer to complete the operation.

Context        : DCPromo.General.4
RebootRequired : True
Status         : Success
```

If you see the above message, just ignore it do not reboot, once all is complete it will reboot itself.

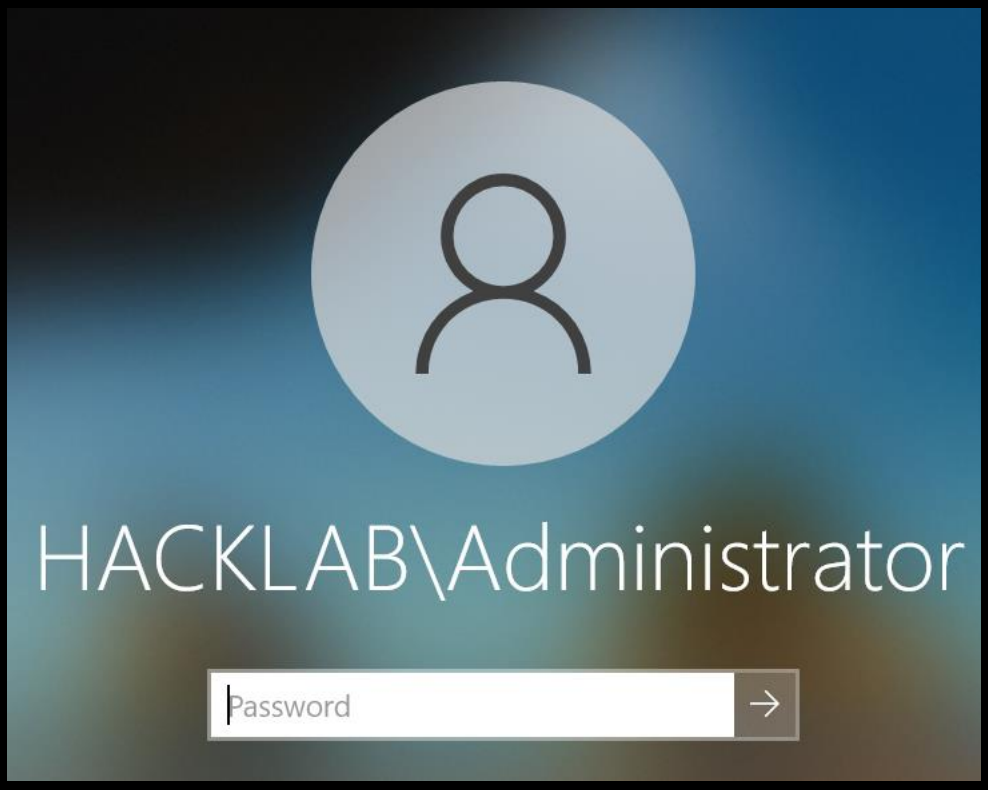
After the reboot you should be able to login as a domain member for the first time.

You can click the Ctrl+Alt+Delete key on the top VM tool bar in a VM.

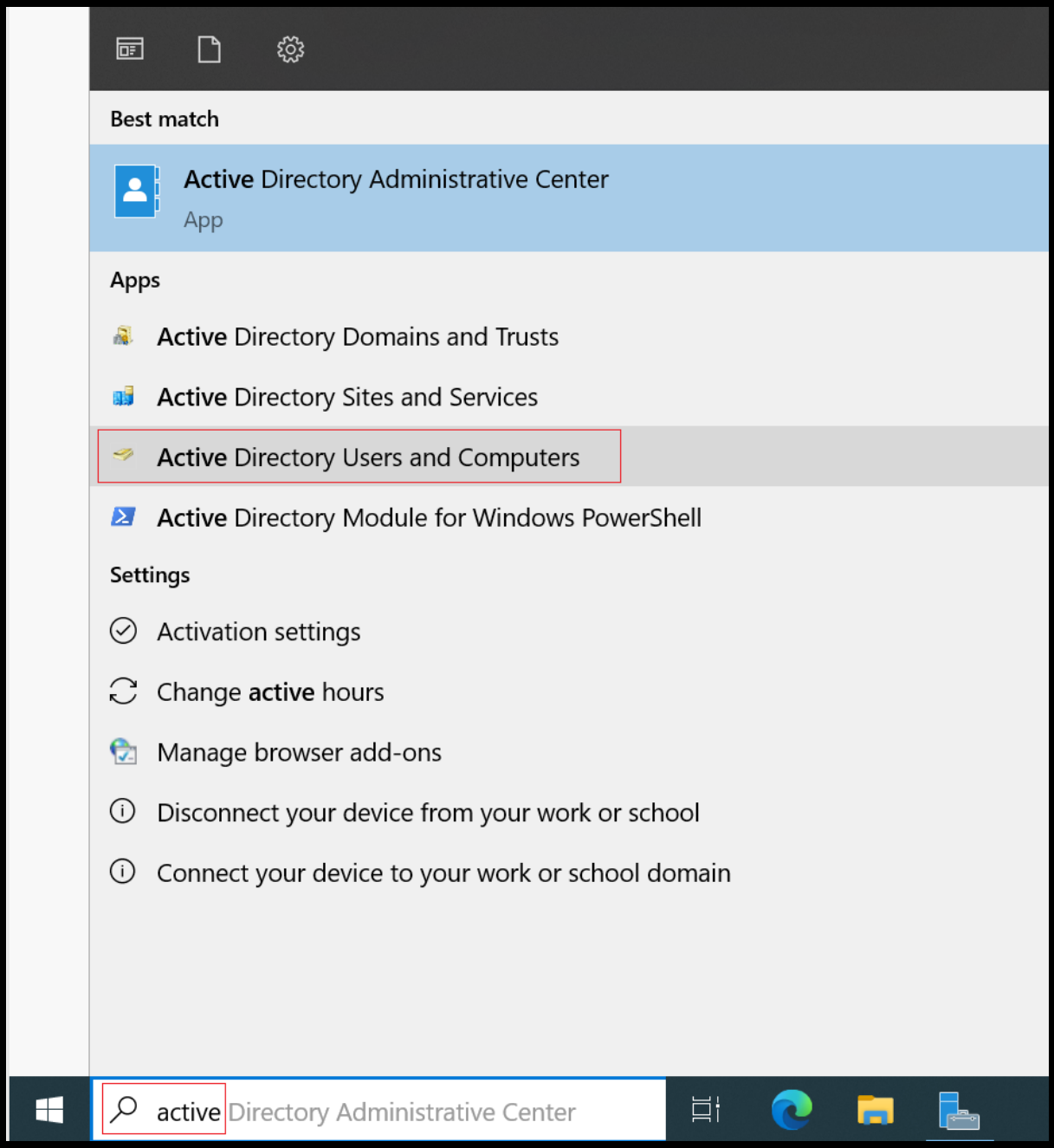




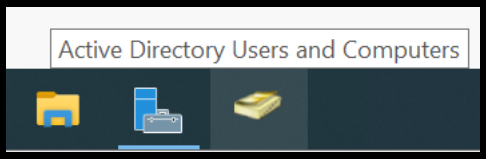
You should see the domain hacklab\ with the Administrator account set up during the conversion to a domain controller.



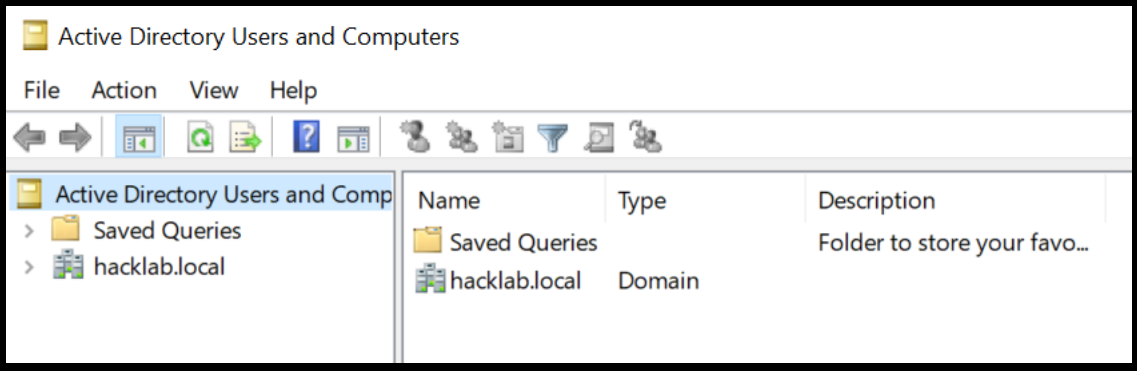
4. Type in Active into the search bar and this should bring up Active Directory Users and Computers, right click it and select pin to toolbar as you will be using it quite often.



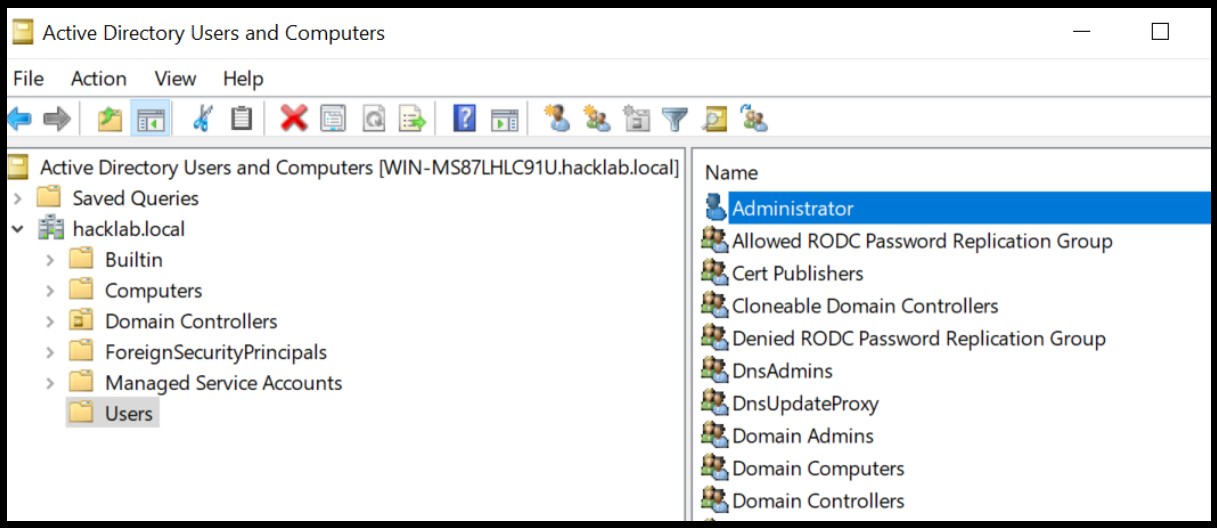
5. Open Active Directory Users and Computers by clicking on it.



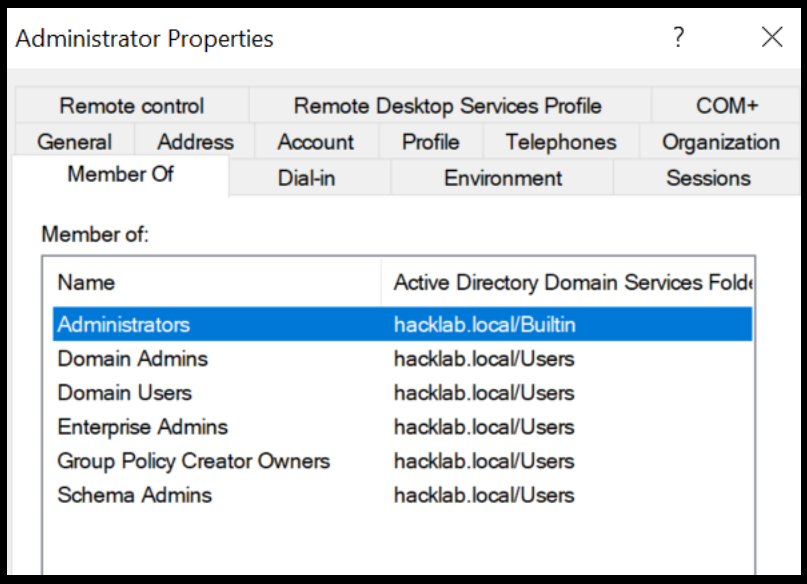
Welcome to Active Directory.



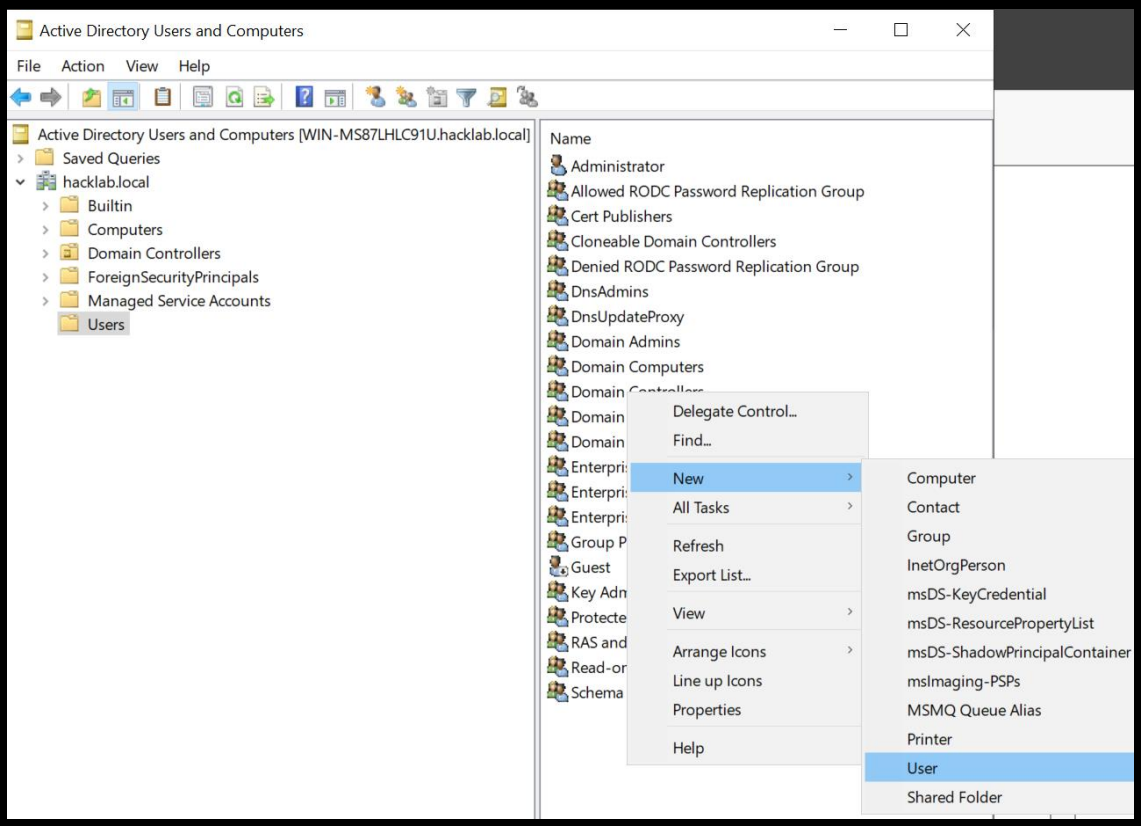
6. Click on the domain hacklab.local / Users and double click on your Administrator account.



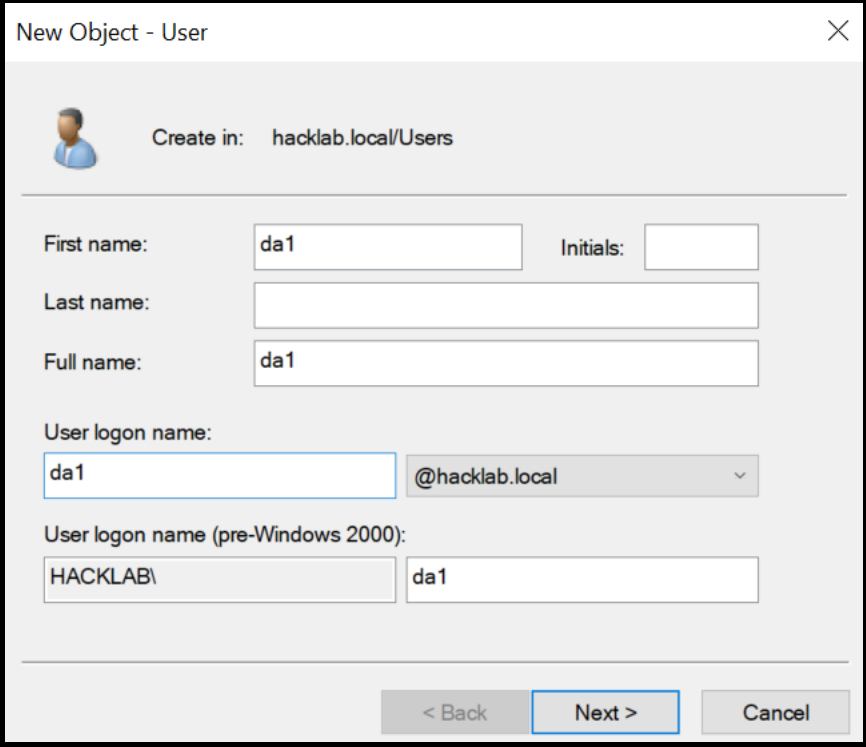
7. Click on Member Of to see the domain groups the account belongs to, in a real domain any account with these privileges should be considered as a break glass emergency account and should only be used in the initial creation of the Domain.



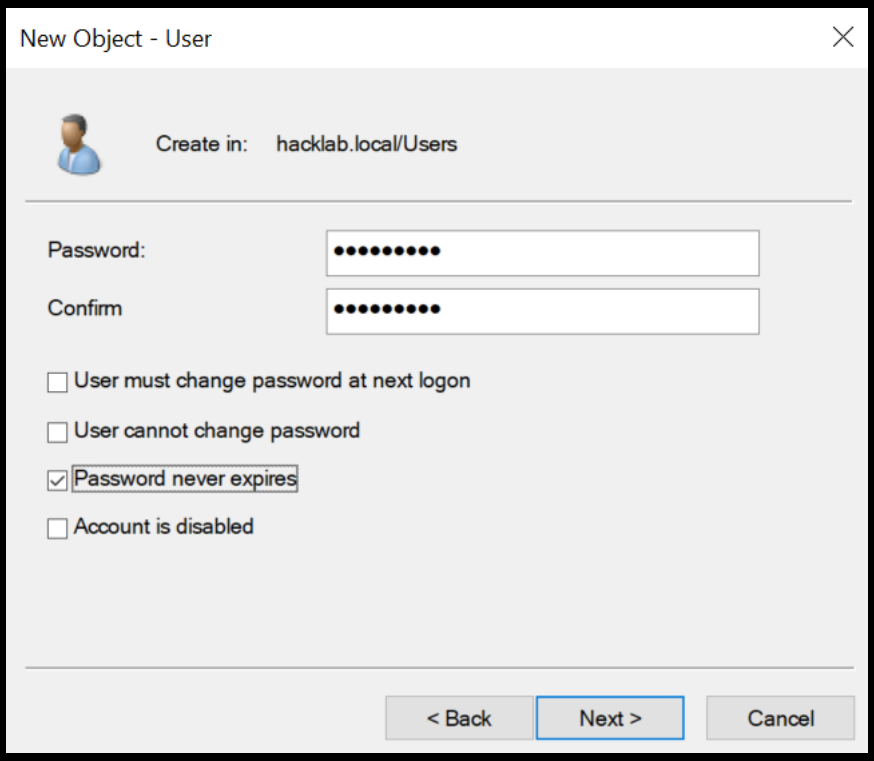
8. Create a new account for routine admin lab work (This is a lab for testing hacking tools and process in, it will never be secure and any recommendations here are for those proposes only.)



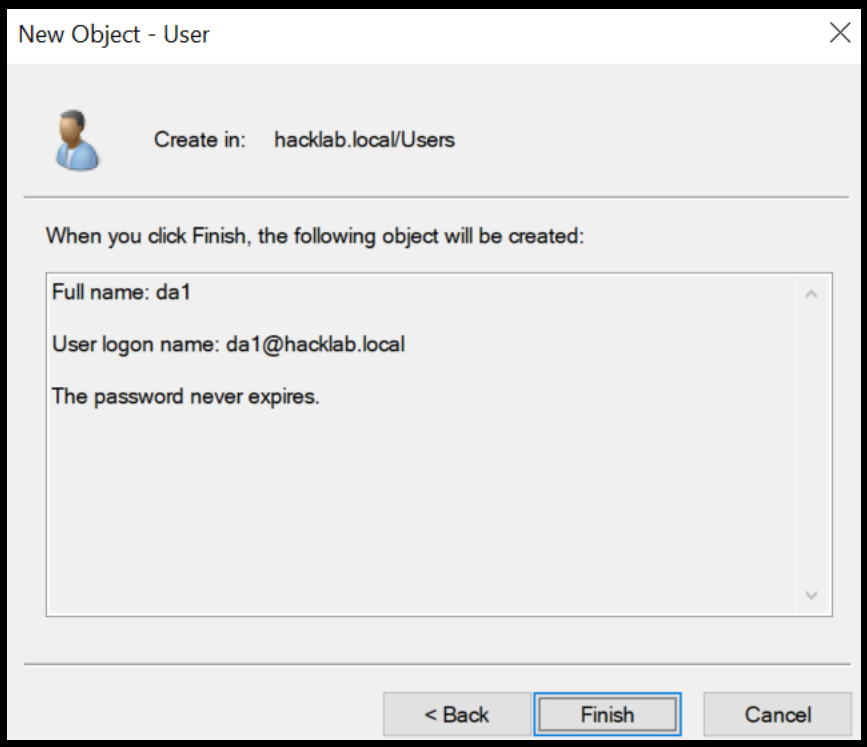
9. Add first name, last name, and user login name, then click Next.



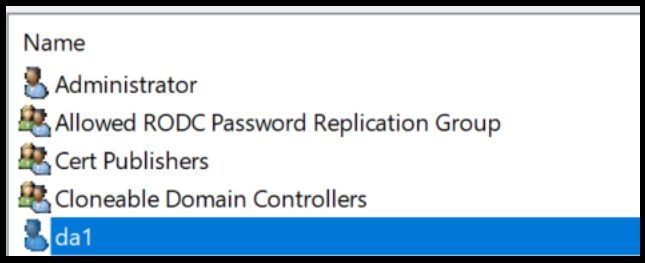
10. Add a password, and for lab use only you can tick Password never expiries if you wish. (In a production environment you would not typically tick Password never expiries because it is bad practice to do so.)



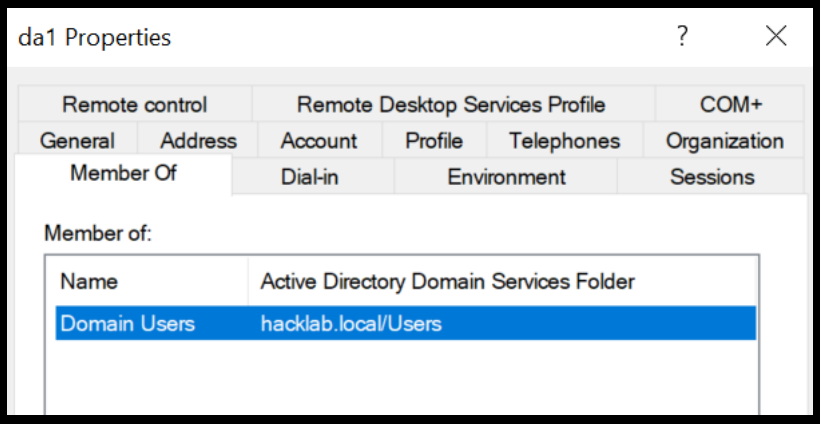
11. Click Finish.



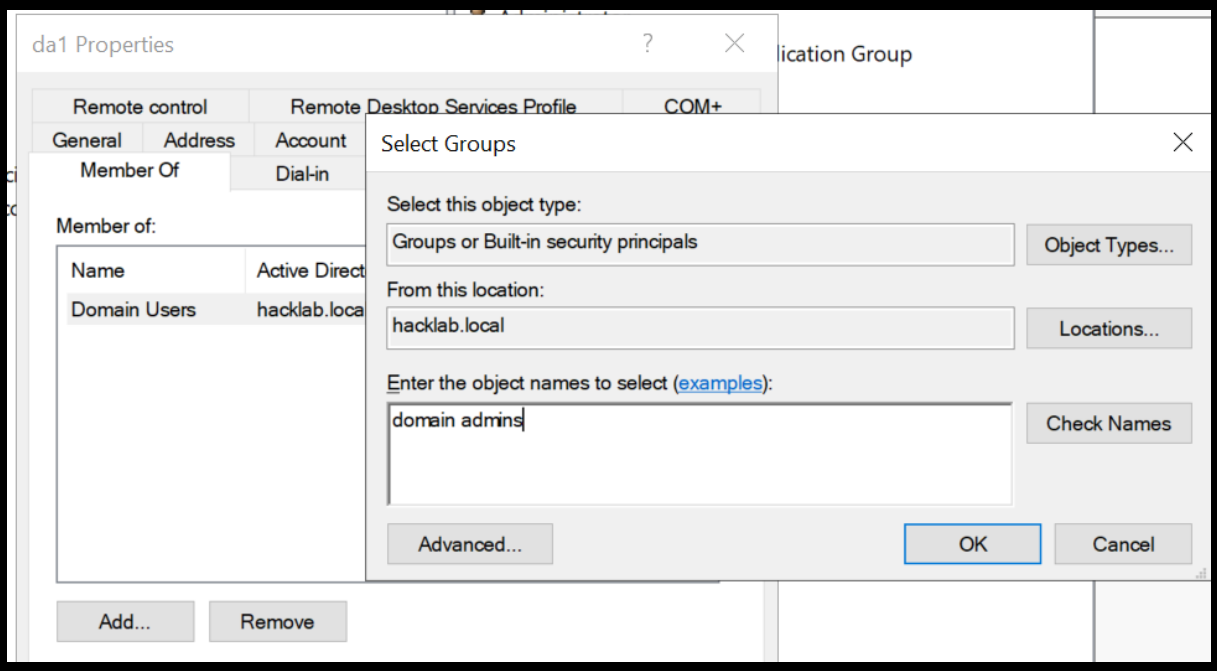
12. You should then see your created account, double click it.



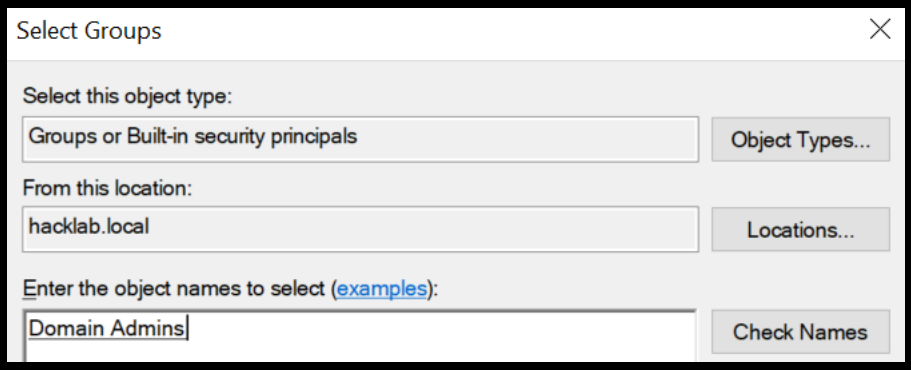
13. Click on the Member Of tab.



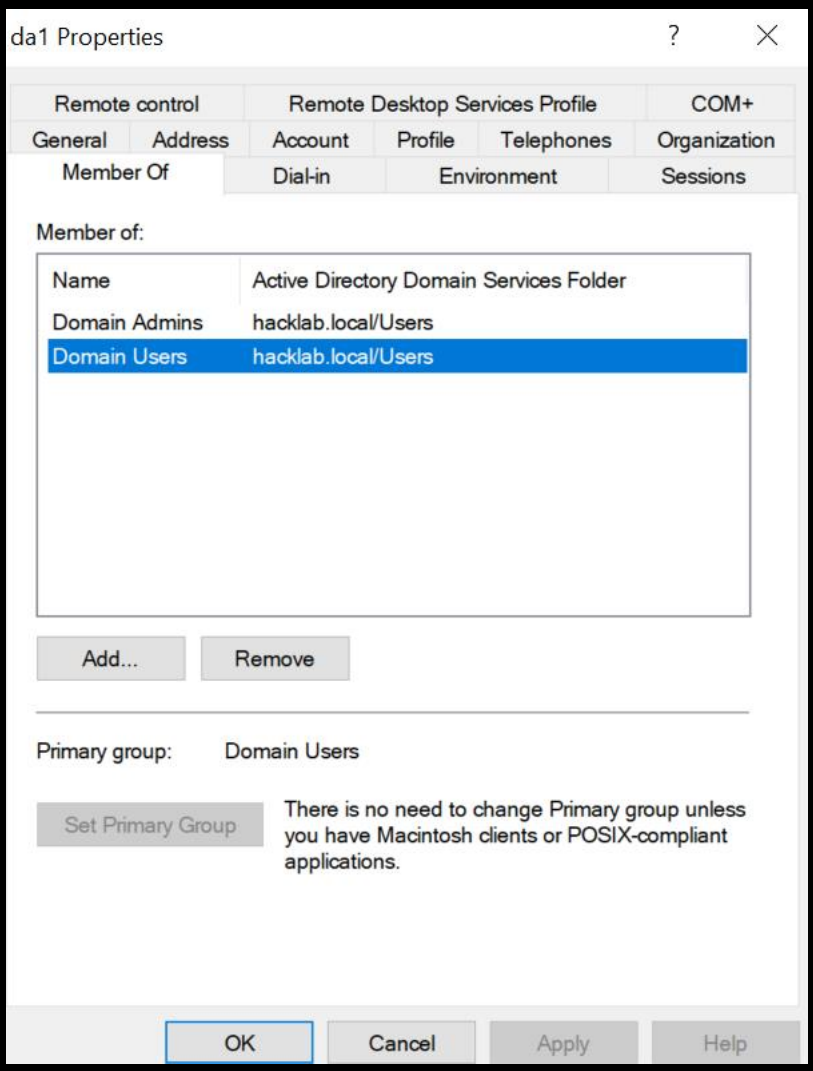
14. To add the account as a member to the Domain Admins group, click on Add then type in domain admins and click Check Names.



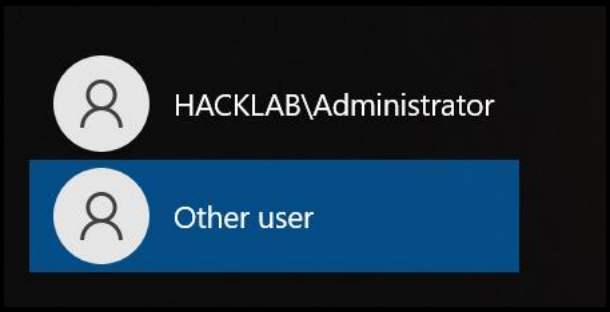
If located, you should see the name domain admins change.

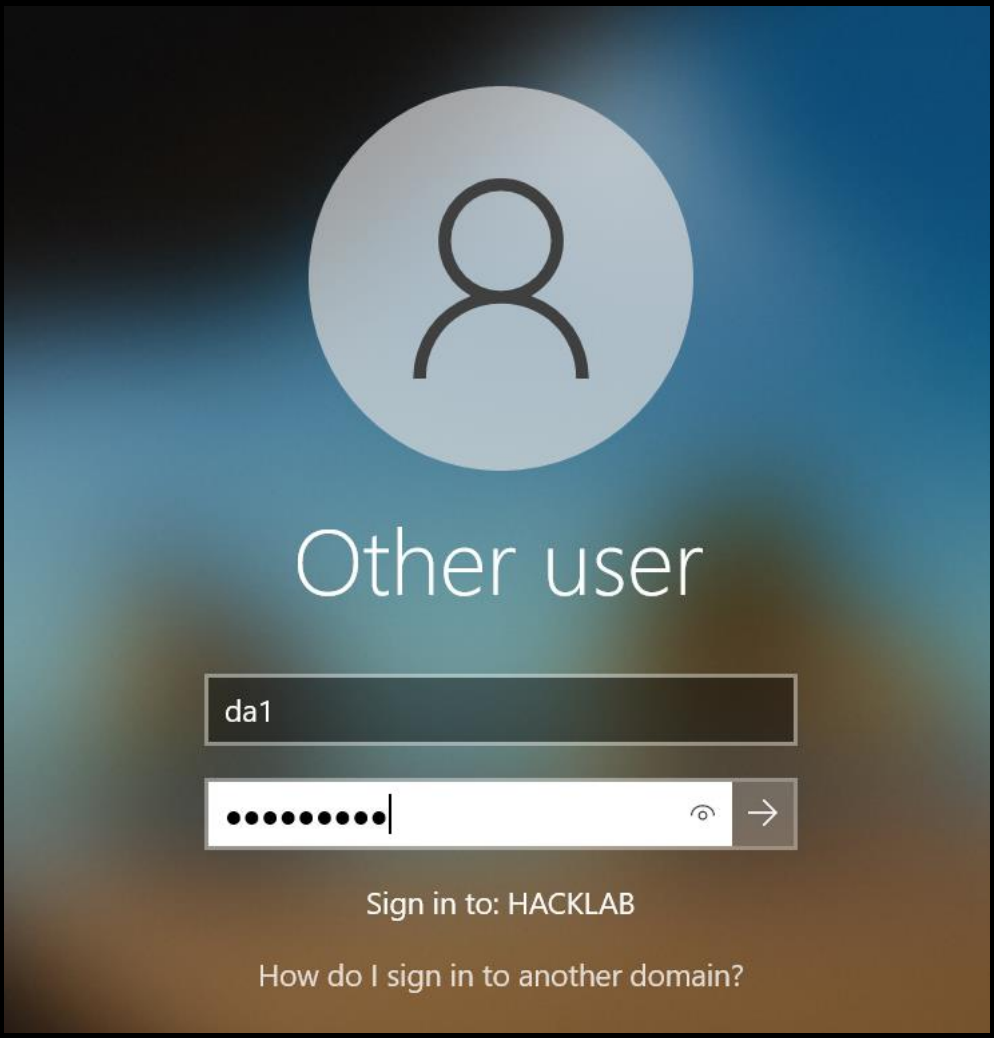


15. Then click OK.



16. Logout and then on the login page select Other user and login using the account you just created.


HACKLAB\Administrator
Other user


Other user
da1
Sign in to: HACKLAB
How do I sign in to another domain?

Creating a vulnerable Windows domain

Feel free to explore and build your simulation of a vulnerable Windows domain, over the years we have seen many misconfigurations and some of these we have built into a configuration script that you can just copy and paste into your lab domain controller to help speed up the process.

Word of caution this will add purposely created vulnerable accounts and settings for the ease of testing hacking tools and processes.

https://raw.githubusercontent.com/myexploit/LAB/master/Hack_Lab_Domain

1. The section you need to copy and paste initiates from the # Add Departments comment and concludes right down to the last word on the web page, exit.

But for ease of use below is the complete section you require.

```
# Add Departments organizational unit (OU) Add Head_Office OU with nested
department OU and IT OU.

dsadd ou ou=Departments,dc=hacklab,dc=local
dsadd ou "ou=IT,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Admins,ou=IT,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Service_Accounts,ou=IT,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Help_Desk,ou=IT,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=HR,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Sales,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Accounts,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Research,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Reception,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd ou
"ou=Administration,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd ou
"ou=Senior_Management,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"

# Create a user groups OU

dsadd ou ou=Groups,ou=Departments,dc=hacklab,dc=local

# Create the following user groups to the group OU

dsadd group cn=sales,ou=Groups,ou=Departments,dc=hacklab,dc=local
dsadd group cn=administration,ou=Groups,ou=Departments,dc=hacklab,dc=local
dsadd group cn=accounts,ou=Groups,ou=Departments,dc=hacklab,dc=local
dsadd group cn=help_desk,ou=Groups,ou=Departments,dc=hacklab,dc=local
dsadd group cn=support,ou=Groups,ou=Departments,dc=hacklab,dc=local
dsadd group cn=RDP,ou=Groups,ou=Departments,dc=hacklab,dc=local

# Create Lab Test accounts

# Head_Office / Accounts

dsadd user "cn=n.collins, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=o.davidson, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=p.davies, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
```

```
dsadd user "cn=q.dawson, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=u.dixon, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=r.edwards, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=s.elliot, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=t.evans, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=u.fisher, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=v.fletcher, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=w.ford, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=x.foster, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=y.fox, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=z.gibson, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=a.graham, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=b.grant, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=c.gray, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=d.green, ou=Accounts, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no

# Head_Office / Administration

dsadd user "cn=m.jenkins, ou=Administration, ou=Head_Office,
ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -
mustchpwd no
dsadd user "cn=n.johnson, ou=Administration, ou=Head_Office,
ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -
mustchpwd no
dsadd user "cn=o.jones, ou=Administration, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=g.white, ou=Administration, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=h.yalden, ou=Administration, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=i.yarbury, ou=Administration, ou=Head_Office,
ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -
mustchpwd no
dsadd user "cn=j.yardley, ou=Administration, ou=Head_Office,
ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -
mustchpwd no

# Head_Office / HR

dsadd user "cn=z.mcdonald, ou=HR, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=a.murphy, ou=HR, ou=Head_Office, ou=Departments, dc=hacklab,
dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=b.natt, ou=HR, ou=Head_Office, ou=Departments, dc=hacklab,
dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
```

```
dsadd user "cn=c.nelson, ou=HR, ou=Head_Office, ou=Departments, dc=hacklab,
dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=d.nightingale, ou=HR, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=e.nixon, ou=HR, ou=Head_Office, ou=Departments, dc=hacklab,
dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=f.nutter, ou=HR, ou=Head_Office, ou=Departments, dc=hacklab,
dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no

# Head_Office / Reception

dsadd user "cn=p.kelly, ou=Reception, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=q.kennedy, ou=Reception, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=u.king, ou=Reception, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=r.knight, ou=Reception, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=s.lawrence, ou=Reception, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=t.lee, ou=Reception, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no

# Head_Office / Research

dsadd user "cn=u.lewis, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=v.lloyd, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=w.marshall, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=x.martin, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=y.mason, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=g.dell, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=h.osborne, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=i.owen, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=j.oxley, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=k.page, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=l.painter, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=m.palmer, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=n.pastor, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=o.peterson, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=p.quill, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=q.quimby, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=u.quintrell, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
```

```
dsadd user "cn=r.ramsey, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=s.ratliff, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=t.richards, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=u.roberts, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=v.robinson, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=w.scott, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=x.simpson, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=y.smith, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=z.stewart, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=a.taylor, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=b.turner, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=c.walsh, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=d.ward, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=e.webb, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=f.west, ou=Research, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no

# Head_Office / Sales

dsadd user "cn=d.atkinson, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Summer123 -mustchpwd no
dsadd user "cn=e.bailey, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=f.baker, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=g.ball, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=h.bell, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=i.brown, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=j.burton, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=k.carter, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=l.clarke, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=m.cole, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=e.griffiths, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=f.hall, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=g.hamilton, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=h.harris, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
```

```
dsadd user "cn=i.harvey, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=j.hill, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=k.jackson, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=l.james, ou=Sales, ou=Head_Office, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no

# Head_Office / Senior_Management

dsadd user "cn=k.yarrow, ou=Senior_Management, ou=Head_Office,
ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -
mustchpwd no
dsadd user "cn=l.yates, ou=Senior_Management, ou=Head_Office,
ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -
mustchpwd no
dsadd user "cn=m.young, ou=Senior_Management, ou=Head_Office,
ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -
mustchpwd no
dsadd user "cn=n.zachary, ou=Senior_Management, ou=Head_Office,
ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -
mustchpwd no
dsadd user "cn=o.zelly, ou=Senior_Management, ou=Head_Office,
ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -
mustchpwd no
dsadd user "cn=p.zinc, ou=Senior_Management, ou=Head_Office,
ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -
mustchpwd no
dsadd user "cn=q.zouch, ou=Senior_Management, ou=Head_Office,
ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -
mustchpwd no

# Head_Office / Help_Desk

dsadd user "cn=a.adams, ou=Help_Desk, ou=IT, ou=Departments, dc=hacklab,
dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=b.allen, ou=Help_Desk, ou=IT, ou=Departments, dc=hacklab,
dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no
dsadd user "cn=c.armstrong, ou=Help_Desk, ou=IT, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no

# Admins / IT / DA

dsadd user "cn=adm.adams, ou=Admins, ou=IT, ou=Departments, dc=hacklab,
dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -memberof
"CN=Domain Admins,CN=Users,dc=hacklab, dc=local"
dsadd user "cn=adm.smith, ou=Admins, ou=IT, ou=Departments, dc=hacklab,
dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -memberof
"CN=Domain Admins,CN=Users,dc=hacklab, dc=local"
dsadd user "cn=adm.stewart, ou=Admins, ou=IT, ou=Departments, dc=hacklab,
dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -memberof
"CN=Domain Admins,CN=Users,dc=hacklab, dc=local"
dsadd user "cn=adm.natt, ou=Admins, ou=IT, ou=Departments, dc=hacklab,
dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -memberof
"CN=Domain Admins,CN=Users,dc=hacklab, dc=local"
dsadd user "cn=adm.nelson, ou=Admins, ou=IT, ou=Departments, dc=hacklab,
dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -memberof
"CN=Domain Admins,CN=Users,dc=hacklab, dc=local"

# Service Accounts / IT
```

```
dsadd user "cn=svc_afds, ou=Service_Accounts, ou=IT, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -
memberof "CN=Domain Admins,CN=Users,dc=hacklab, dc=local"
dsadd user "cn=svc_test, ou=Service_Accounts, ou=IT, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -
memberof "CN=Domain Admins,CN=Users,dc=hacklab, dc=local"
dsadd user "cn=svc_mssql1, ou=Service_Accounts, ou=IT, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -
memberof "CN=Domain Admins,CN=Users,dc=hacklab, dc=local"
dsadd user "cn=svc_mssql2, ou=Service_Accounts, ou=IT, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -
memberof "CN=Domain Admins,CN=Users,dc=hacklab, dc=local"
dsadd user "cn=svc_lab, ou=Service_Accounts, ou=IT, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -
memberof "CN=Domain Admins,CN=Users,dc=hacklab, dc=local"
dsadd user "cn=svc_admin, ou=Service_Accounts, ou=IT, ou=Departments,
dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -
memberof "CN=Domain Admins,CN=Users,dc=hacklab, dc=local"

# Set up Service Principal Name (SPN) for the following accounts so you can
kerberoast them.

setspn -s http/server1.hacklab.local:8082 svc_afds
setspn -s http/server1.hacklab.local:8083 svc_test
setspn -s http/server1.hacklab.local:8084 svc_mssql1
setspn -s http/server1.hacklab.local:8085 svc_mssql2
setspn -s http/server1.hacklab.local:8086 svc_lab
setspn -s http/server1.hacklab.local:8087 svc_admin

# Make the following accounts vulnerable to asreproast.

Set-ADAccountControl -Identity m.jenkins -DoesNotRequirePreAuth 1
Set-ADAccountControl -Identity z.mcdonald -DoesNotRequirePreAuth 1
Set-ADAccountControl -Identity u.lewis -DoesNotRequirePreAuth 1

# Create a description filed with a password in it.

Set-ADUser d.atkinson -Description "User Password Summer123"

# Disable SMB Signing on the DC.

Set-SmbClientConfiguration -RequireSecuritySignature 0 -
EnableSecuritySignature 0 -Confirm -Force

# Add Domain Machines

New-ADComputer -Name "SR2000-1" -SamAccountName "SR2000-1" -Enabled $True -
OperatingSystem "Windows Server 2000 Service Pack 4"
New-ADComputer -Name "SR2000-2" -SamAccountName "SR2000-2" -Enabled $True -
OperatingSystem "Windows Server 2000 Service Pack 4"
New-ADComputer -Name "SR2000-3" -SamAccountName "SR2000-3" -Enabled $True -
OperatingSystem "Windows Server 2000 Service Pack 4"
New-ADComputer -Name "SR2000-4" -SamAccountName "SR2000-4" -Enabled $True -
OperatingSystem "Windows Server 2000 Service Pack 4"
New-ADComputer -Name "SR2000-5" -SamAccountName "SR2000-5" -Enabled $True -
OperatingSystem "Windows Server 2000 Service Pack 4"
New-ADComputer -Name "SR2000-6" -SamAccountName "SR2000-6" -Enabled $True -
OperatingSystem "Windows Server 2000 Service Pack 4"
New-ADComputer -Name "SR2003-1" -SamAccountName "SR2003-1" -Enabled $True -
OperatingSystem "Windows Server 2003 Datacenter Service Pack 2"
```

```
New-ADComputer -Name "SR2003-2" -SamAccountName "SR2003-2" -Enabled $True -
OperatingSystem "Windows Server 2003 Datacenter Service Pack 2"
New-ADComputer -Name "SR2003-3" -SamAccountName "SR2003-3" -Enabled $True -
OperatingSystem "Windows Server 2003 Datacenter Service Pack 2"
New-ADComputer -Name "SR2003-4" -SamAccountName "SR2003-4" -Enabled $True -
OperatingSystem "Windows Server 2003 Datacenter Service Pack 2"
New-ADComputer -Name "SR2003-5" -SamAccountName "SR2003-5" -Enabled $True -
OperatingSystem "Windows Server 2003 Datacenter Service Pack 2"
New-ADComputer -Name "SR2003-6" -SamAccountName "SR2003-6" -Enabled $True -
OperatingSystem "Windows Server 2003 Datacenter Service Pack 2"
New-ADComputer -Name "SR2008-1" -SamAccountName "SR208-1" -Enabled $True -
OperatingSystem "Windows Server 2008 R2 Standard Service Pack 1"
New-ADComputer -Name "SR2008-2" -SamAccountName "SR208-2" -Enabled $True -
OperatingSystem "Windows Server 2008 R2 Standard Service Pack 1"
New-ADComputer -Name "SR2008-3" -SamAccountName "SR208-3" -Enabled $True -
OperatingSystem "Windows Server 2008 R2 Standard Service Pack 1"
New-ADComputer -Name "SR2008-4" -SamAccountName "SR208-4" -Enabled $True -
OperatingSystem "Windows Server 2008 R2 Standard Service Pack 1"
New-ADComputer -Name "SR2008-5" -SamAccountName "SR208-5" -Enabled $True -
OperatingSystem "Windows Server 2008 R2 Standard Service Pack 1"
New-ADComputer -Name "SR2008-6" -SamAccountName "SR208-6" -Enabled $True -
OperatingSystem "Windows Server 2008 R2 Standard Service Pack 1"
New-ADComputer -Name "SR2012-1" -SamAccountName "SR2012-1" -Enabled $True -
OperatingSystem "Windows Server 2012 Standard"
New-ADComputer -Name "SR2012-2" -SamAccountName "SR2012-2" -Enabled $True -
OperatingSystem "Windows Server 2012 Standard"
New-ADComputer -Name "SR2012-3" -SamAccountName "SR2012-3" -Enabled $True -
OperatingSystem "Windows Server 2012 Standard"
New-ADComputer -Name "SR2012-4" -SamAccountName "SR2012-4" -Enabled $True -
OperatingSystem "Windows Server 2012 Standard"
New-ADComputer -Name "SR2019-1" -SamAccountName "SR2019-1" -Enabled $True -
OperatingSystem "Windows Server 2019 Standard"
New-ADComputer -Name "SR2019-2" -SamAccountName "SR2019-2" -Enabled $True -
OperatingSystem "Windows Server 2019 Standard"
New-ADComputer -Name "SR2019-3" -SamAccountName "SR2019-3" -Enabled $True -
OperatingSystem "Windows Server 2019 Standard"
New-ADComputer -Name "SR2019-4" -SamAccountName "SR2019-4" -Enabled $True -
OperatingSystem "Windows Server 2019 Standard"
New-ADComputer -Name "W7-1" -SamAccountName "W7-1" -Enabled $True -
OperatingSystem "Windows 7 Professional Service Pack 1"
New-ADComputer -Name "W7-2" -SamAccountName "W7-2" -Enabled $True -
OperatingSystem "Windows 7 Professional Service Pack 1"
New-ADComputer -Name "W7-3" -SamAccountName "W7-3" -Enabled $True -
OperatingSystem "Windows 7 Professional Service Pack 1"
New-ADComputer -Name "W7-4" -SamAccountName "W7-4" -Enabled $True -
OperatingSystem "Windows 7 Professional Service Pack 1"
New-ADComputer -Name "W7-5" -SamAccountName "W7-5" -Enabled $True -
OperatingSystem "Windows 7 Professional Service Pack 1"
New-ADComputer -Name "W7-6" -SamAccountName "W7-6" -Enabled $True -
OperatingSystem "Windows 7 Professional Service Pack 1"
New-ADComputer -Name "XP-1" -SamAccountName "XP-1" -Enabled $True -
OperatingSystem "Windows XP Service Pack 1"

# Set UP ACL's

Import-Module ActiveDirectory
Set-Location AD:

Function SetAcl($for, $to, $right, $inheritance)
{
```

```
    $forSID = New-Object System.Security.Principal.SecurityIdentifier (Get-
ADUser $for).SID
    $objOU = ($to).DistinguishedName
    $objAcl = get-acl $objOU
    # https://docs.microsoft.com/fr-
fr/dotnet/api/system.directoryservices.activedirectoryrights?view=dotnet-
plat-ext-5.0
    $adRight =  [System.DirectoryServices.ActiveDirectoryRights] $right #
https://docs.microsoft.com/fr-
fr/dotnet/api/system.directoryservices.activedirectoryrights?view=dotnet-
plat-ext-5.0
    $type =  [System.Security.AccessControl.AccessControlType] "Allow" #
https://docs.microsoft.com/fr-
fr/dotnet/api/system.security.accesscontrol.accesscontroltype?view=dotnet-
plat-ext-5.0
    $inheritanceType =
[System.DirectoryServices.ActiveDirectorySecurityInheritance] $inheritance
# https://docs.microsoft.com/fr-
fr/dotnet/api/system.directoryservices.activedirectorysecurityinheritance?v
iew=dotnet-plat-ext-5.0
    $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule
$forSID,$adRight,$type,$inheritanceType
    $objAcl.AddAccessRule($ace)
    Set-Acl -AclObject $objAcl -path $objOU
}


Function SetAclExtended($for, $to, $right, $extendedRightGUID,
$inheritance)
{
    $forSID = New-Object System.Security.Principal.SecurityIdentifier (Get-
ADUser $for).SID
    $objOU = ($to).DistinguishedName
    $objAcl = get-acl $objOU
    # https://docs.microsoft.com/fr-
fr/dotnet/api/system.directoryservices.activedirectoryrights?view=dotnet-
plat-ext-5.0
    $adRight =  [System.DirectoryServices.ActiveDirectoryRights] $right #
https://docs.microsoft.com/fr-
fr/dotnet/api/system.directoryservices.activedirectoryrights?view=dotnet-
plat-ext-5.0
    $type =  [System.Security.AccessControl.AccessControlType] "Allow" #
https://docs.microsoft.com/fr-
fr/dotnet/api/system.security.accesscontrol.accesscontroltype?view=dotnet-
plat-ext-5.0
    $inheritanceType =
[System.DirectoryServices.ActiveDirectorySecurityInheritance] $inheritance
# https://docs.microsoft.com/fr-
fr/dotnet/api/system.directoryservices.activedirectorysecurityinheritance?v
iew=dotnet-plat-ext-5.0

    $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule
$forSID,$adRight,$type,$extendedRightGUID,$inheritanceType
    $objAcl.AddAccessRule($ace)
    Set-Acl -AclObject $objAcl -path $objOU
}

## acl values :
# AccessSystemSecurity
# CreateChild
# Delete
```

```
# DeleteChild
# DeleteTree
# ExtendedRight
# GenericAll
# GenericExecute
# GenericRead
# GenericWrite
# ListChildren
# ListObject
# ReadControl
# ReadProperty
# Self
# Synchronize
# WriteDacl
# WriteOwner
# WriteProperty

## extend rights
# "00299570-246d-11d0-a768-00aa006e0529" {$right = "User-Force-Change-
Password"}
# "45ec5156-db7e-47bb-b53f-dbeb2d03c40"  {$right = "Reanimate-Tombstones"}
# "bf9679c0-0de6-11d0-a285-00aa003049e2" {$right = "Self-Membership"}
# "ba33815a-4f93-4c76-87f3-57574bff8109" {$right = "Manage-SID-History"}
# "1131f6ad-9c07-11d1-f79f-00c04fc2dcd2" {$right = "DS-Replication-Get-
Changes-All"}

# ACL abuse scenarios
# https://sensepost.com/blog/2020/ace-to-rce/
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces
# https://adsecurity.org/?p=3658


# genericall-on-user1
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces#genericall-on-user

SetAcl (Get-ADUser "n.collins") (Get-ADUser "a.adams") "GenericAll" "None"

# genericall-on-group
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces#genericall-on-group

SetAcl (Get-ADUser "o.davidson") (Get-ADGroup "Domain Admins") "GenericAll"
"None"

# genericall-genericwrite-write-on-computer
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces#genericall-genericwrite-
write-on-computer

SetAcl (Get-ADUser "g.white") (Get-ADComputer "W7-4$")  "WriteProperty"
"All"

# writeproperty-on-group
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces#writeproperty-on-group

SetAcl (Get-ADUser "q.kennedy") (Get-ADGroup "Domain Admins")
"WriteProperty" "All"
```

```
# self-self-membership-on-group
# https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-acls-aces#self-self-membership-on-group

SetAclExtended (Get-ADUser "u.roberts") (Get-ADGroup "Domain Admins") "Self" "bf9679c0-0de6-11d0-a285-00aa003049e2" "None"

# writeproperty-self-membership
# https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-acls-aces#writeproperty-self-membership

SetAclExtended (Get-ADUser "f.west") (Get-ADGroup "Domain Admins") "WriteProperty" "bf9679c0-0de6-11d0-a285-00aa003049e2" "All"

# forcechangepassword
# https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-acls-aces#forcechangepassword
# https://docs.microsoft.com/fr-fr/windows/win32/adschema/r-user-change-password

SetAclExtended (Get-ADUser "l.james") (Get-ADUser "y.fox") "ExtendedRight" "00299570-246d-11d0-a768-00aa006e0529" "None"

# write owner on group
# https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-acls-aces#writeowner-on-group

SetAcl (Get-ADUser "a.graham") (Get-ADGroup "Domain Admins") "WriteOwner" "None"

# genericwrite-on-user
# https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-acls-aces#genericwrite-on-user

SetAcl (Get-ADUser "c.nelson") (Get-ADUser "w.marshall") "GenericWrite" "None"

# writedacl-writeowner
# https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-acls-aces#writedacl-writeowner

SetAcl (Get-ADUser "p.kelly") (Get-ADGroup "RDP") "WriteDacl" "None"

exit
```

2. Open PowerShell with an administrative session (Search for PowerShell, right click and select run as administrator.)

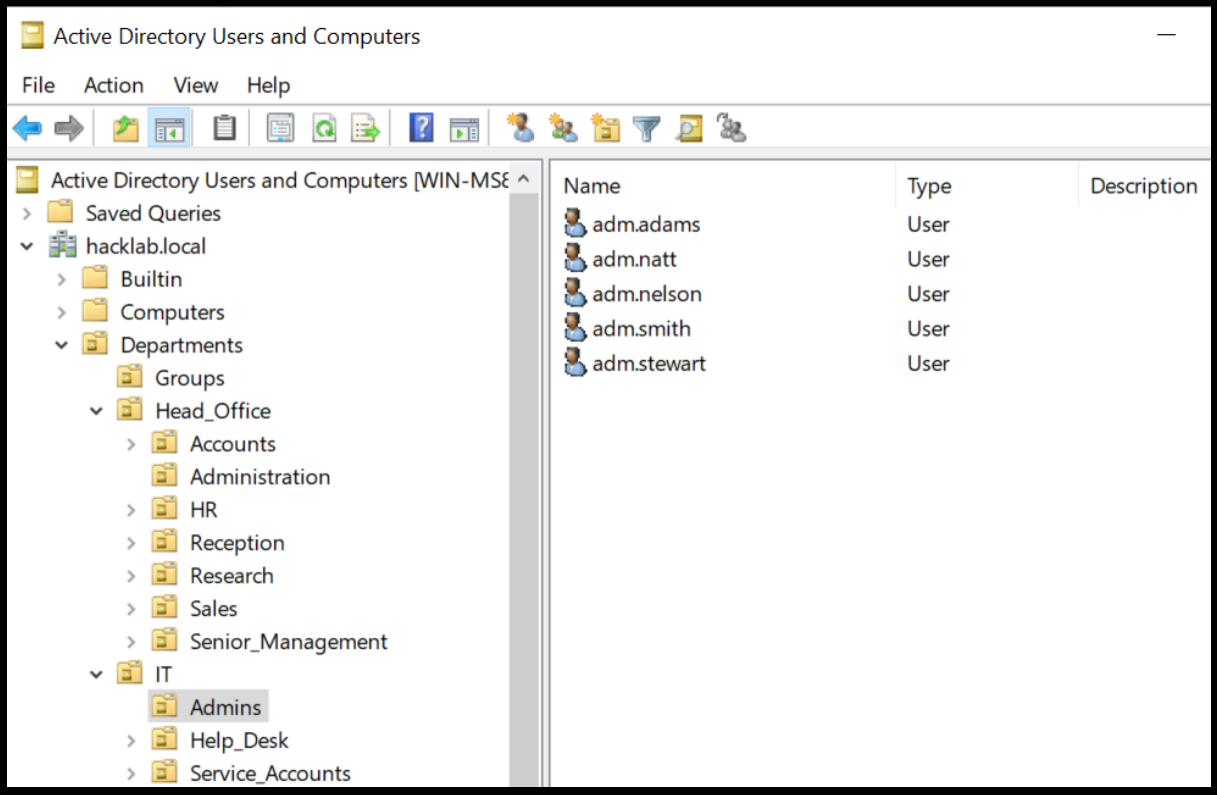
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32>
```

3. Highlight, copy and paste the complete PowerShell script into the Administrator session.

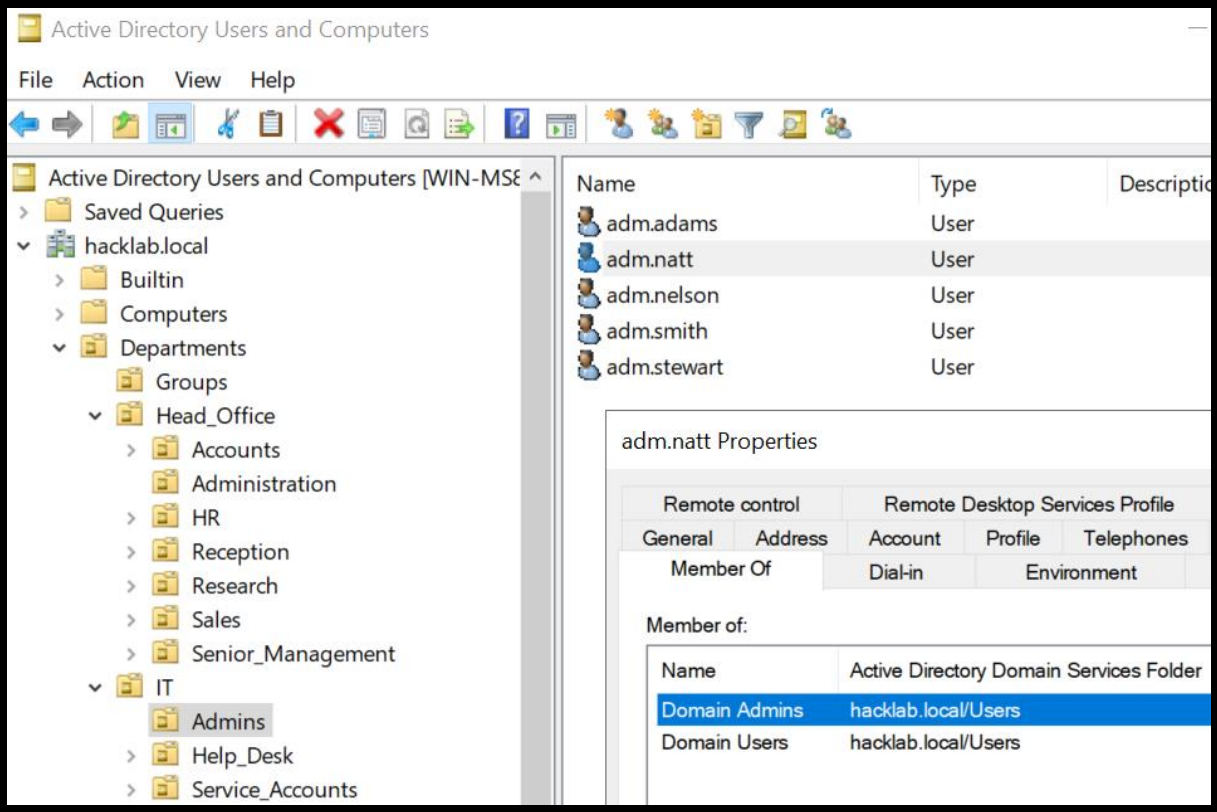
```
Administrator: Windows PowerShell
dsadd succeeded:ou=Service_Accounts,ou=IT,ou=Departments,dc=hacklab,dc=local
PS C:\Windows\system32> dsadd ou "ou=Help_Desk,ou=IT,ou=Departments,dc=hacklab,dc=local"
dsadd succeeded:ou=Help_Desk,ou=IT,ou=Departments,dc=hacklab,dc=local
PS C:\Windows\system32> dsadd ou "ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd succeeded:ou=Head_Office,ou=Departments,dc=hacklab,dc=local
PS C:\Windows\system32> dsadd ou "ou=HR,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd succeeded:ou=HR,ou=Head_Office,ou=Departments,dc=hacklab,dc=local
PS C:\Windows\system32> dsadd ou "ou=Sales,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd succeeded:ou=Sales,ou=Head_Office,ou=Departments,dc=hacklab,dc=local
PS C:\Windows\system32> dsadd ou "ou=Accounts,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd succeeded:ou=Accounts,ou=Head_Office,ou=Departments,dc=hacklab,dc=local
PS C:\Windows\system32> dsadd ou "ou=Research,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd succeeded:ou=Research,ou=Head_Office,ou=Departments,dc=hacklab,dc=local
PS C:\Windows\system32> dsadd ou "ou=Reception,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd succeeded:ou=Reception,ou=Head_Office,ou=Departments,dc=hacklab,dc=local
PS C:\Windows\system32> dsadd ou "ou=Administration,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd succeeded:ou=Administration,ou=Head_Office,ou=Departments,dc=hacklab,dc=local
PS C:\Windows\system32> dsadd ou "ou=Senior_Management,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd succeeded:ou=Senior_Management,ou=Head_Office,ou=Departments,dc=hacklab,dc=local
PS C:\Windows\system32>
PS C:\Windows\system32> # Create a user groups OU
PS C:\Windows\system32>
PS C:\Windows\system32> dsadd ou ou=Groups,ou=Departments,dc=hacklab,dc=local
dsadd succeeded:ou=Groups,ou=Departments,dc=hacklab,dc=local
PS C:\Windows\system32>
PS C:\Windows\system32> # Create the following user groups to the group OU
PS C:\Windows\system32>
PS C:\Windows\system32> dsadd group cn=sales,ou=Groups,ou=Departments,dc=hacklab,dc=local
dsadd succeeded:cn=sales,ou=Groups,ou=Departments,dc=hacklab,dc=local
```

This will add all the OU's, Groups, highly vulnerable User Accounts, Service Accounts, and general bad misconfigurations. All accounts have a password of Passw0rd! for ease of use, and yes this is dreadful and should never be used in production.

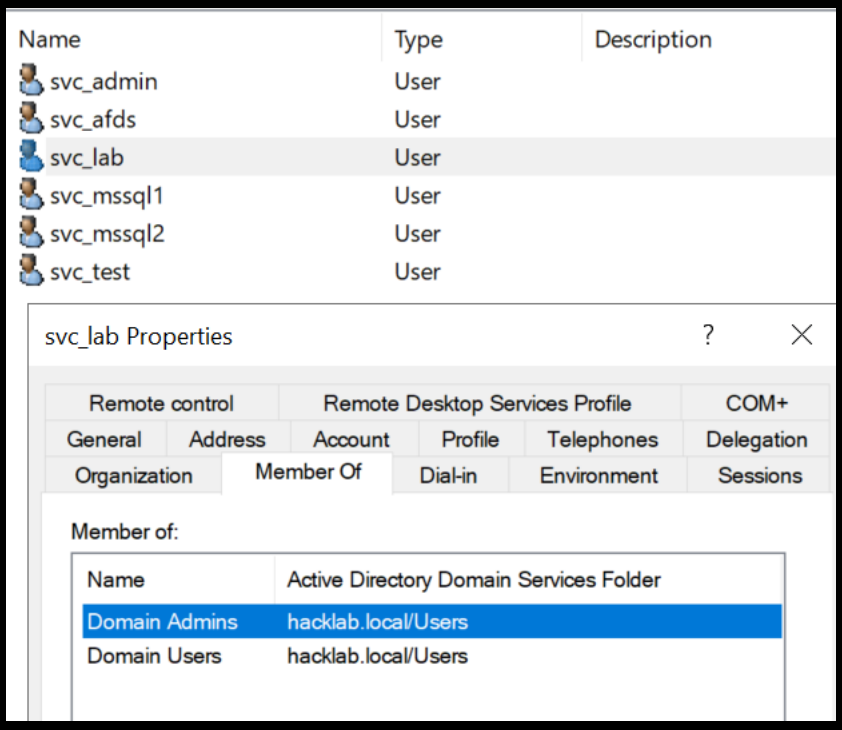
4. Once complete, reopen Active Directory Users and Computers. You should see the OU's and accounts, which gives the appearance of a more realistic environment.



Members of the Admins group found under the IT OU are all members of the domain admin group.



The service accounts are also members of the domain admin group and have been configured so they are ready for you to kerberoast.



Have fun!

In addition to spinning up users, often it is useful to have all the logging enabled too, so the following can be pasted into PowerShell or CMD.exe as administrator to enable on the various machines you have in your domain:

:: Audit Policy Settings

:: Hat tip to https://twitter.com/Antonlovesdnb for the tips on things to enable.

:: Audit Policy: Account Logon

Auditpol /set /category:"Account Logon" /success:enable /failure:enable

:: Audit Policy: Account Management

Auditpol /set /category:"Account Management" /subcategory:"Computer Account Management" /success:enable /failure:enable

Auditpol /set /category:"Account Management" /subcategory:"Other Account Management Events" /success:enable /failure:enable

Auditpol /set /category:"Account Management" /subcategory:"Security Group Management" /success:enable /failure:enable

Auditpol /set /category:"Account Management" /subcategory:"User Account Management" /success:enable /failure:enable

Presented by Andy Gill & Neil Lines at Steelcon 2023

:: Audit Policy: Detailed Tracking

Auditpol /set /category:"Detailed Tracking" /subcategory:"DPAPI Activity" /success:enable /failure:enable

Auditpol /set /category:"Detailed Tracking" /subcategory:"Process Creation" /success:enable /failure:enable

:: Audit Policy: DS Access

Auditpol /set /category:"DS Access" /success:enable /failure:enable

:: Audit Policy: Logon/Logoff

Auditpol /set /category:"Logon/Logoff" /subcategory:"Account Lockout" /success:enable /failure:enable

Auditpol /set /category:"Logon/Logoff" /subcategory:"Logon" /success:enable /failure:enable

Auditpol /set /category:"Logon/Logoff" /subcategory:"Other Logon/Logoff Events" /success:enable /failure:enable

Auditpol /set /category:"Logon/Logoff" /subcategory:"Special Logon" /success:enable /failure:enable

:: Audit Policy: Object Access

Auditpol /set /category:"Object Access" /subcategory:"Other Object Access Events" /success:enable /failure:enable

Auditpol /set /category:"Object Access" /subcategory:"Registry" /success:enable /failure:enable

:: Audit Policy: Policy Change

Auditpol /set /category:"Policy Change" /subcategory:"Audit Policy Change" /success:enable /failure:enable

:: Audit Policy: Privilege Use

Auditpol /set /category:"Privilege Use" /subcategory:"Sensitive Privilege Use" /success:enable /failure:disable

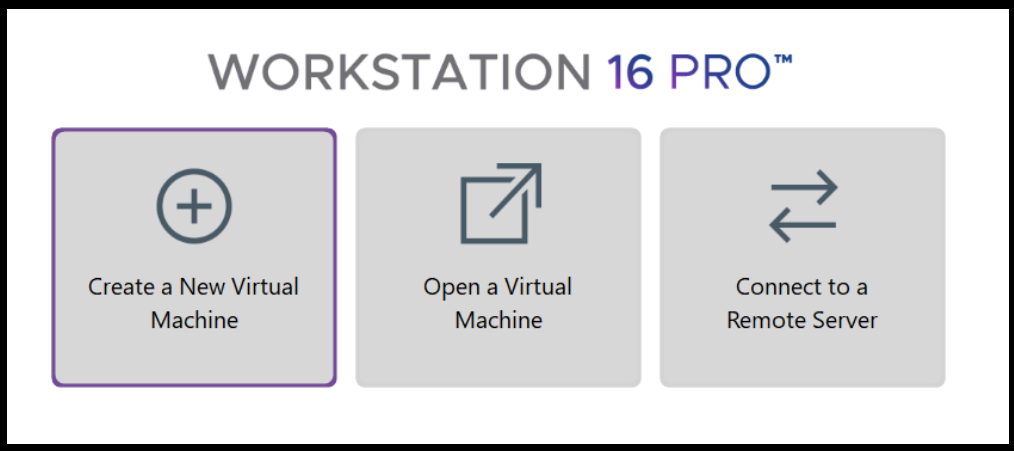
:: Audit Policy: System

```
Auditpol /set /category:"System" /subcategory:"Other System Events" /success:enable /failure:enable

Auditpol /set /category:"System" /subcategory:"System Integrity" /success:enable /failure:enable
```

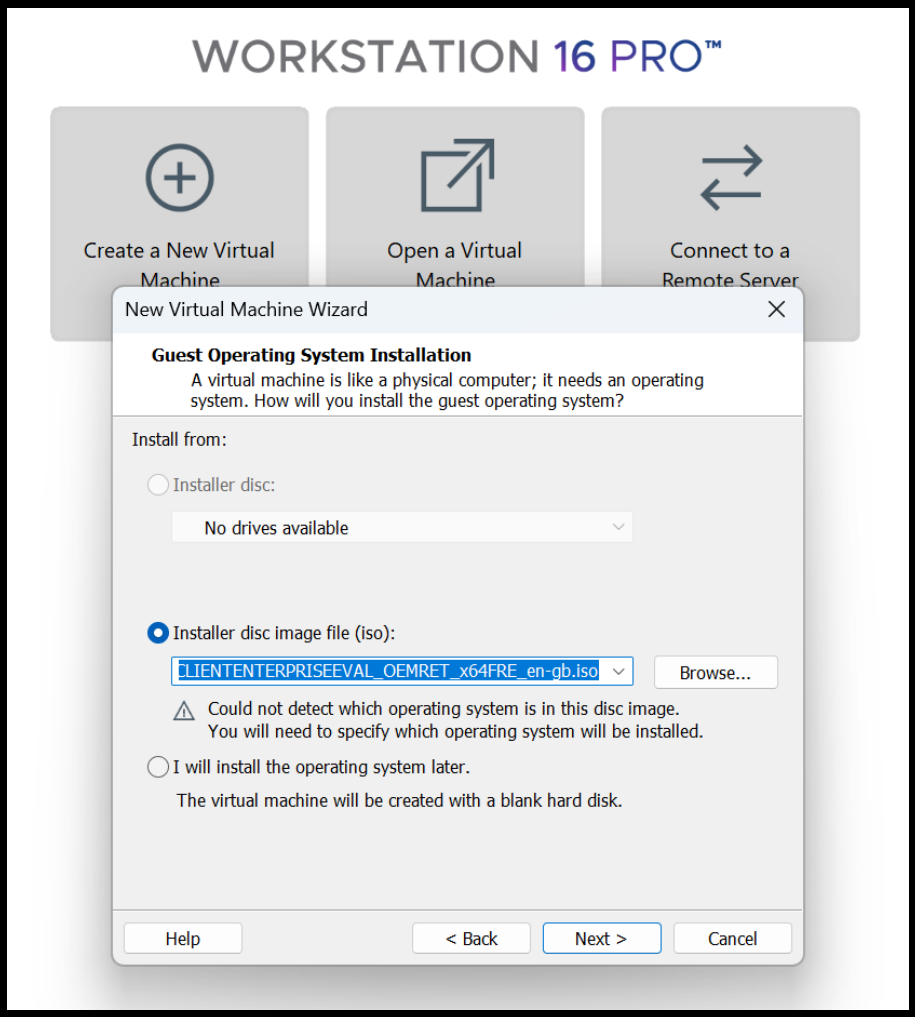
Windows 11 setup guide

The process to create a Windows 11 VM is slightly more complex than Server 2022 as it requires you to enable the encrypted Trusted Platform Module and set a boot encryption password, this guide will walk you through that process.

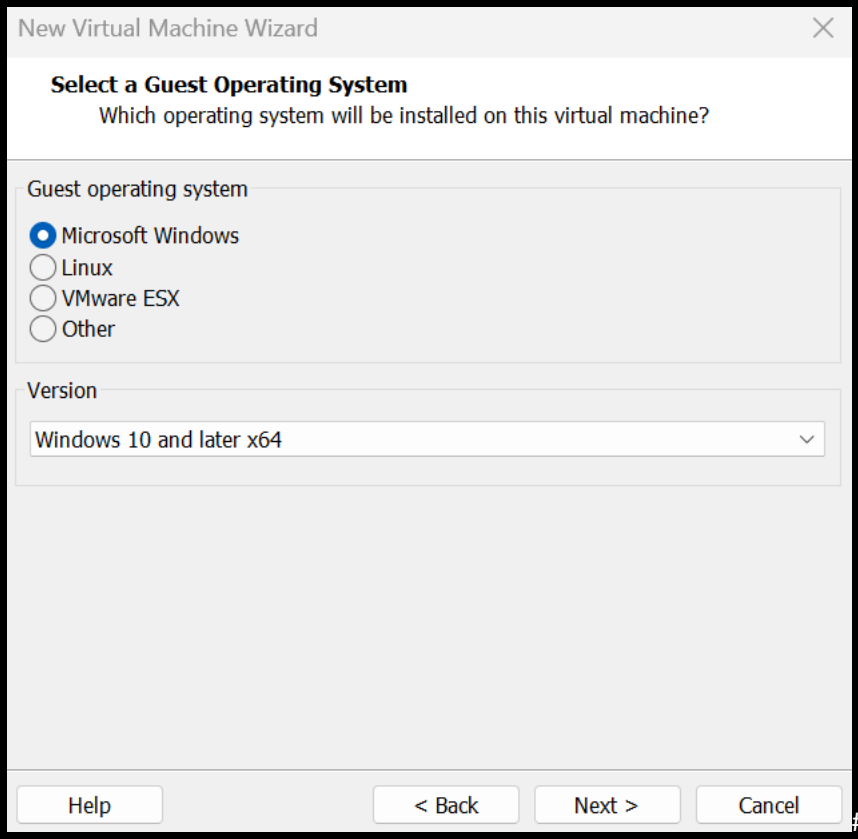
1. Home create a New Virtual Machine.



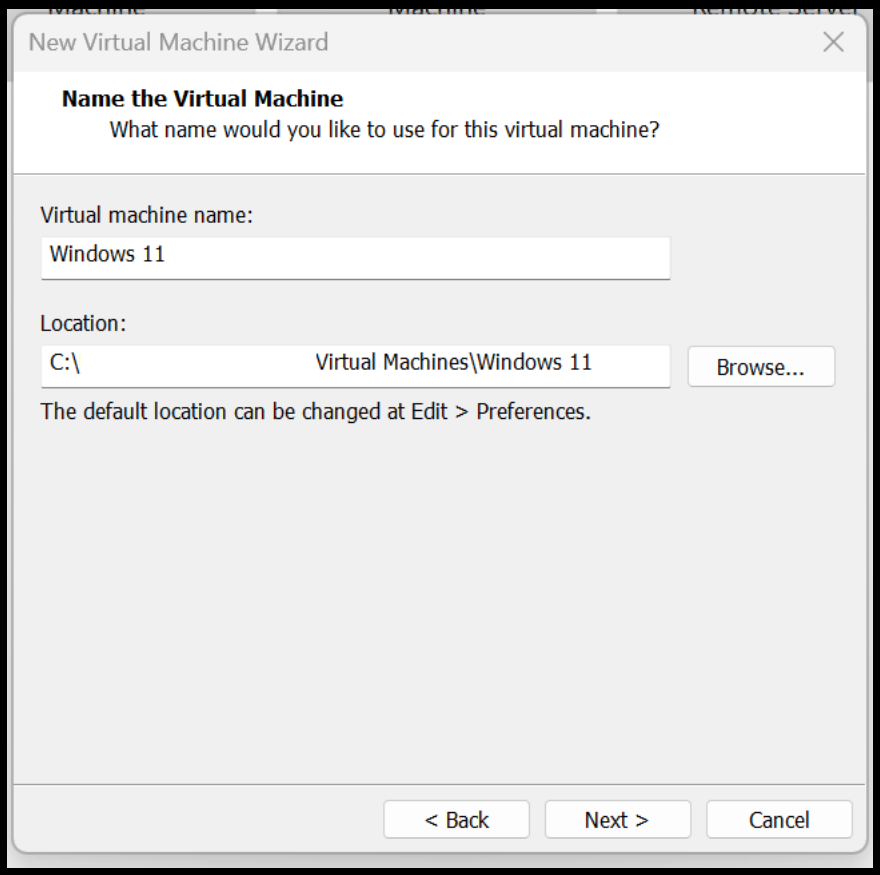
2. Select the Windows 11 ISO, then click Next.



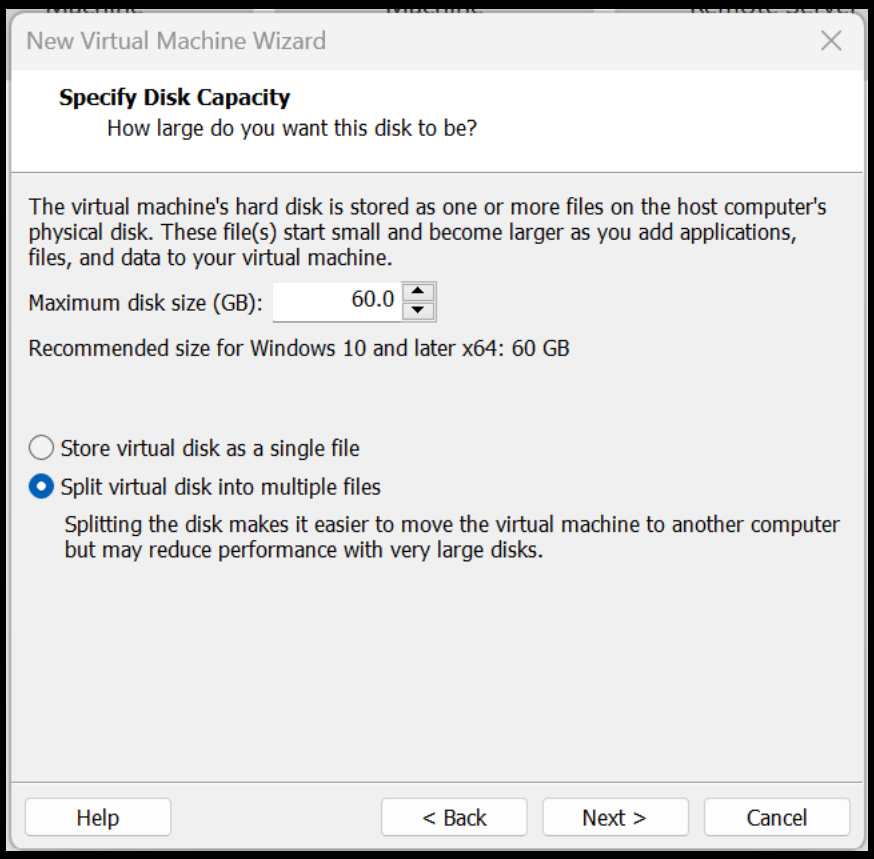
3. Select Microsoft Windows 10 and later x64, then click Next.



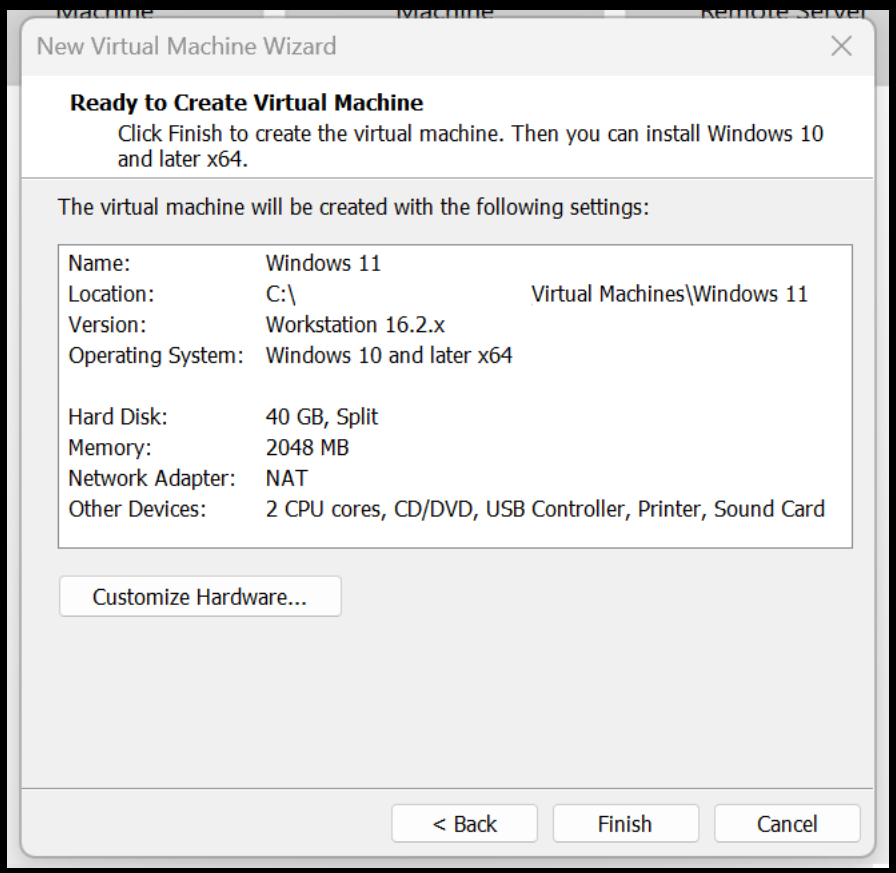
4. Name the machine, then click Next.



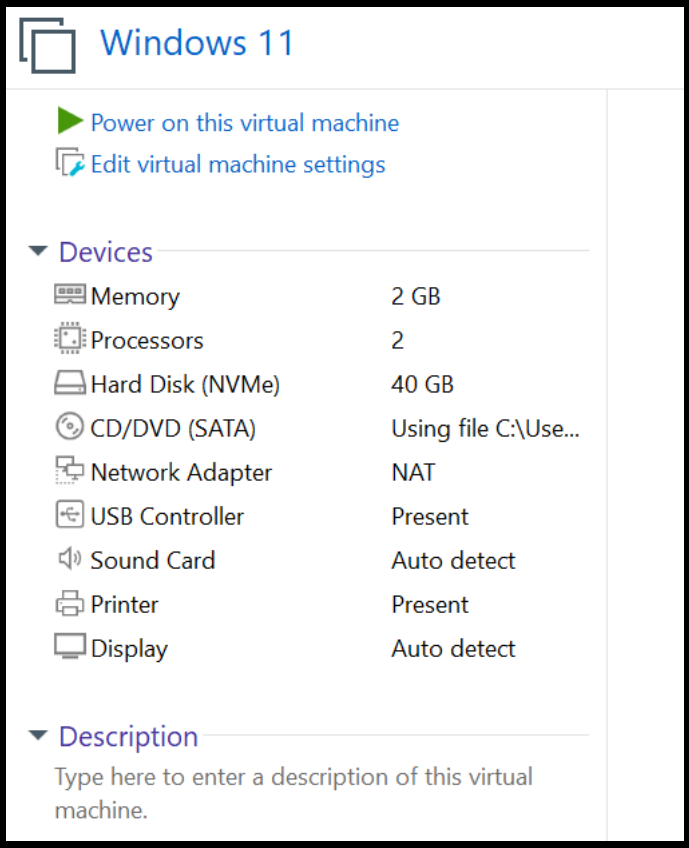
5. Allocate what storage you can, Windows 11 can run on 40GB.



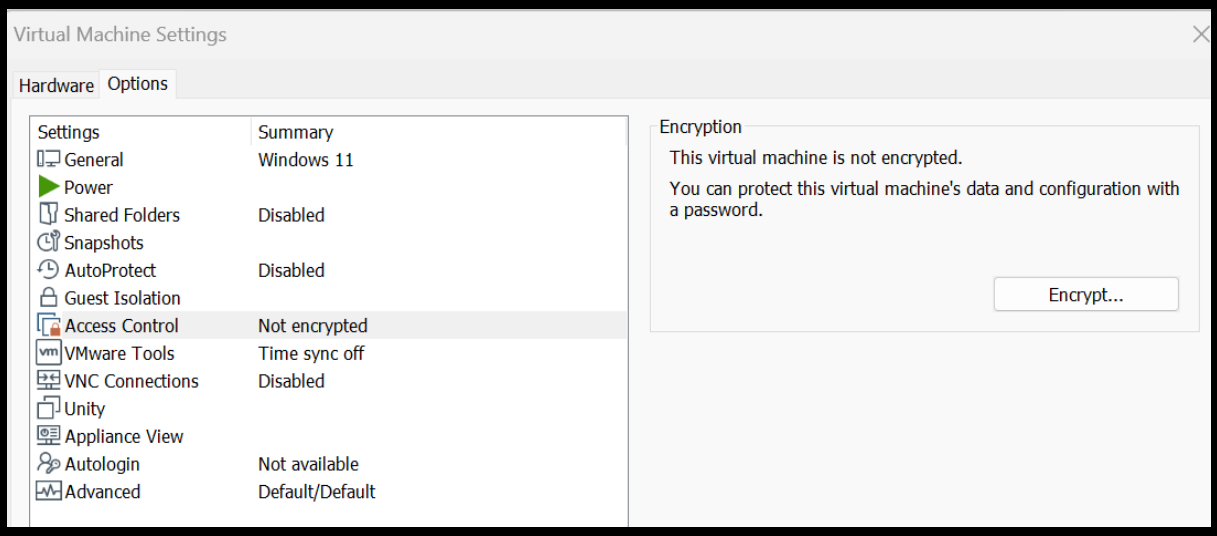
6. Click on Finish.



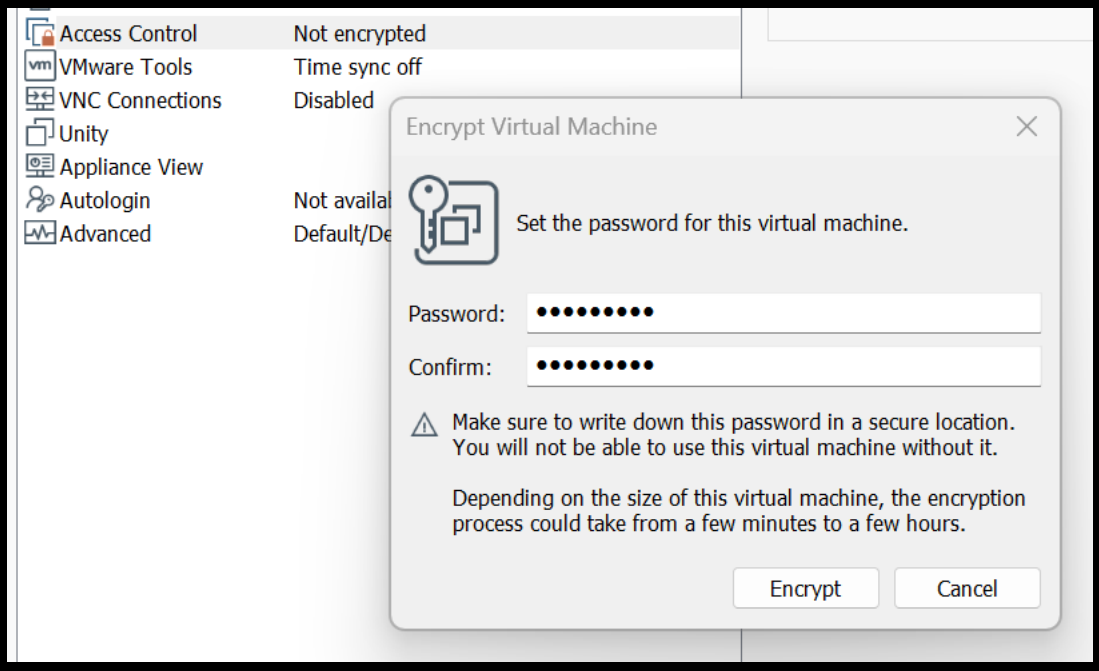
7. Click on Edit virtual machine settings.



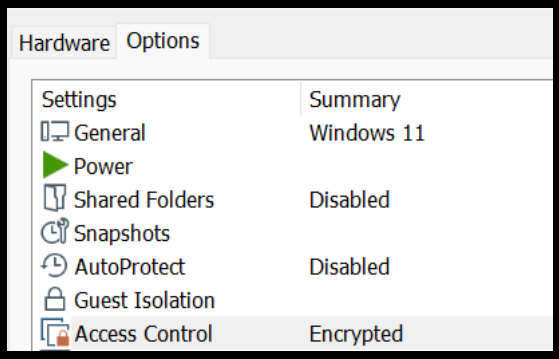
8. Click on Options then highlight Access Control and Select Encrypt.



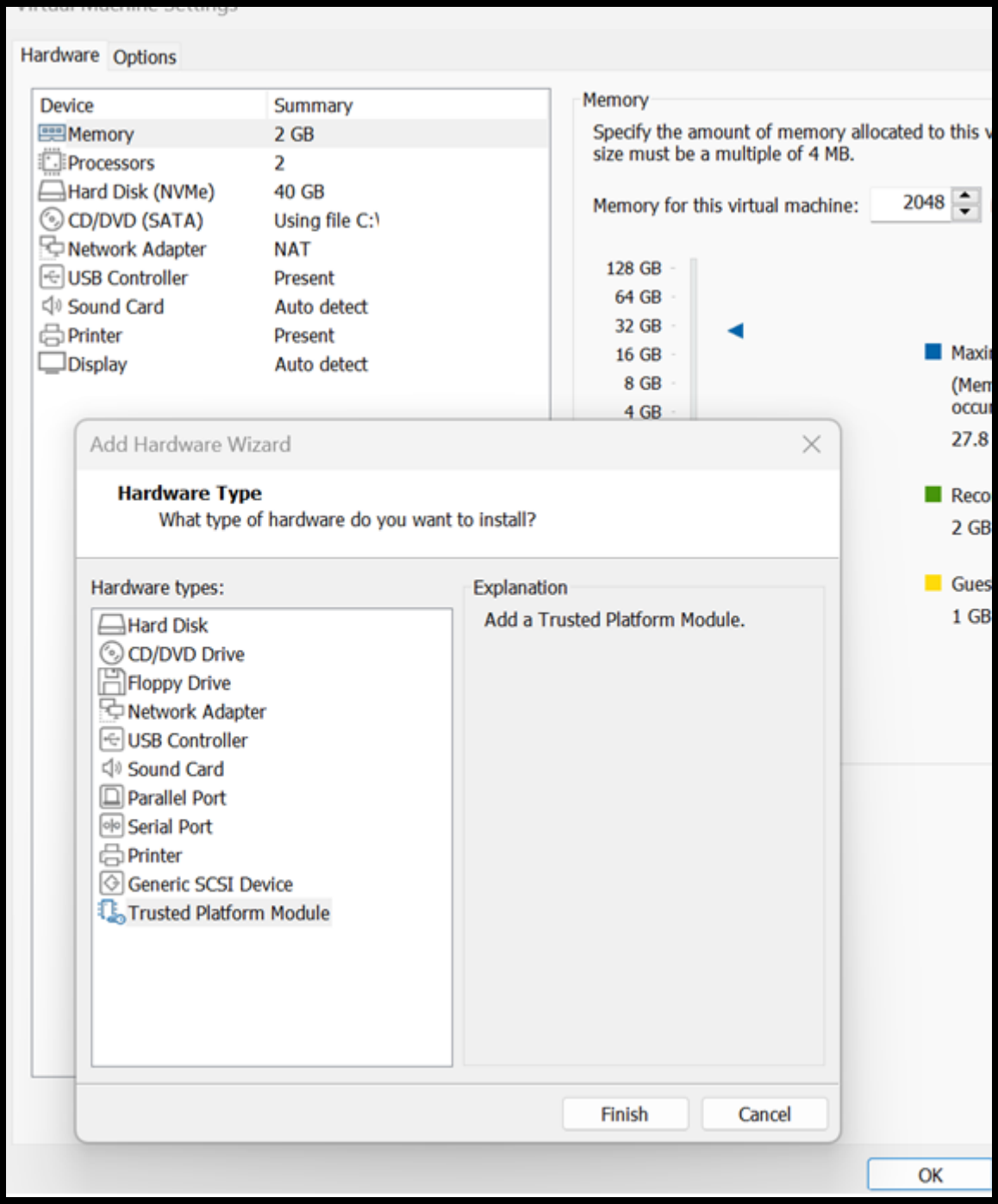
9. Add a Password then click Encrypt.



Access Control should now say Encrypted.



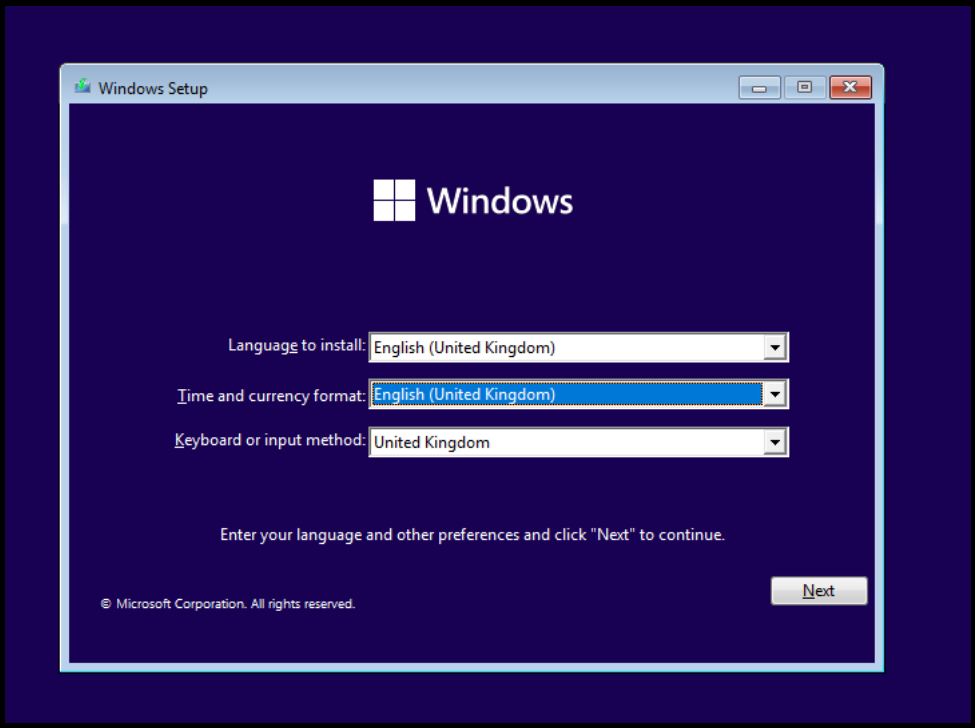
10. Click back on the Hardware tab, select Add then highlight Trusted Platform Module and click on Finish.



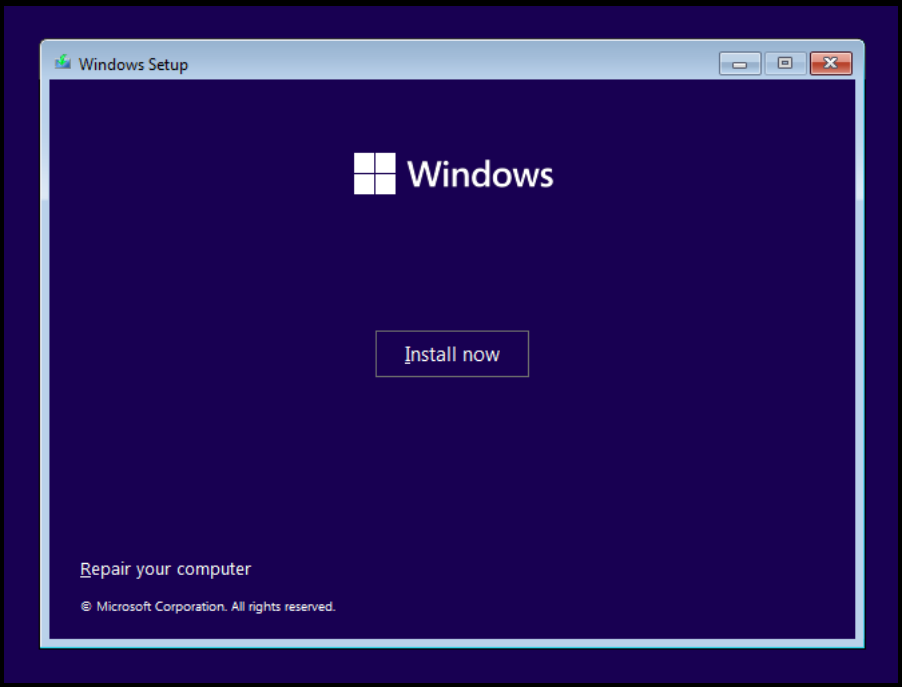
11. Give it slightly over 4GB of RAM, if you don't you will not be able to install Windows 11.
12. Finally check there is no Floppy Disk enabled as that will also stop the installation.
13. Click OK and then Start up the VM.
14. During the initial boot click in the screen and then press any key when prompted.

```
Press any key to boot from CD or DVD.
```

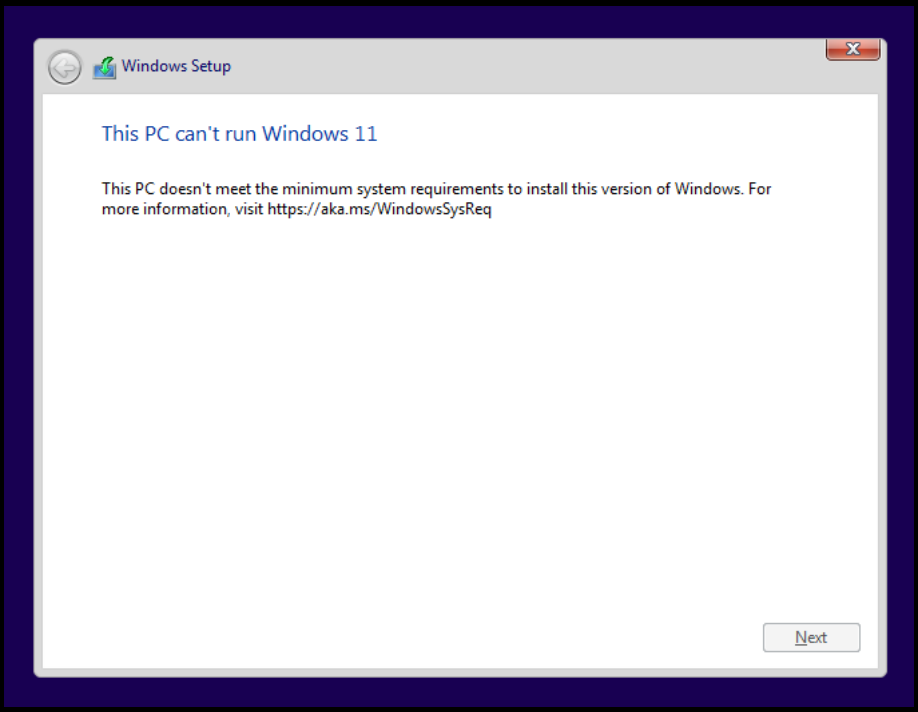
15. Select language then click Next.



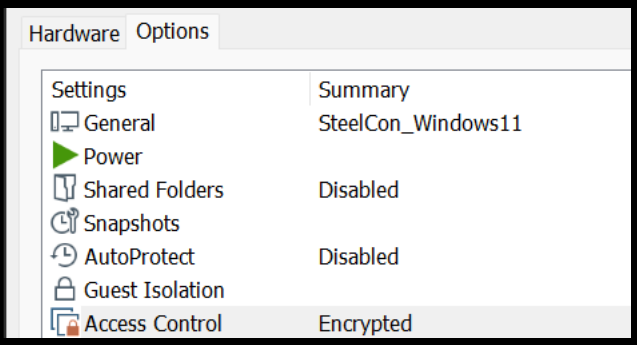
16. Click Install Now.



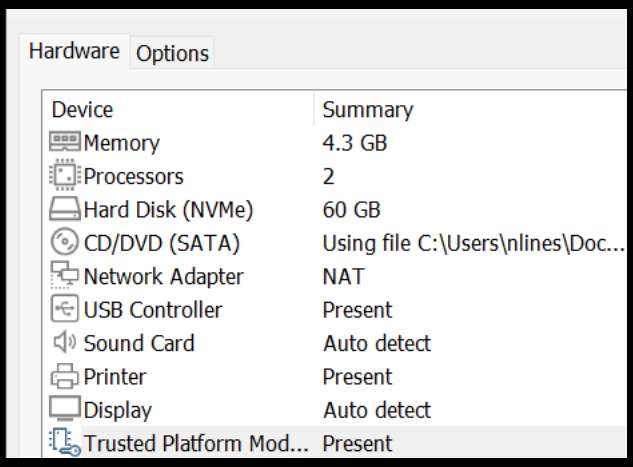
If you see this error during the initial install.



Check that you have set up Access Control by adding an encrypted password.

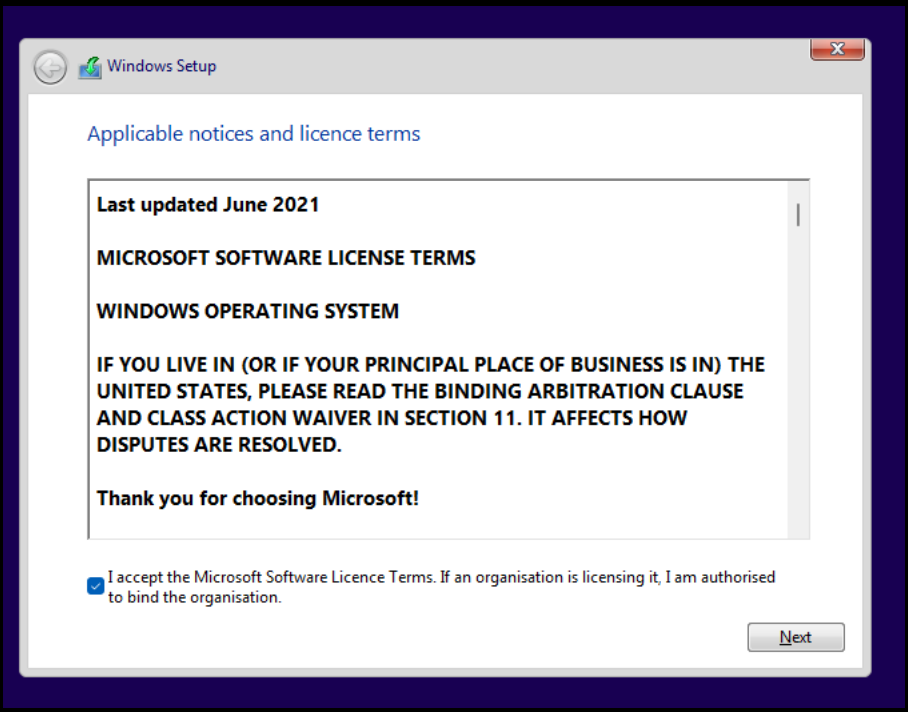


Check the Trusted Platform Module set to Present.

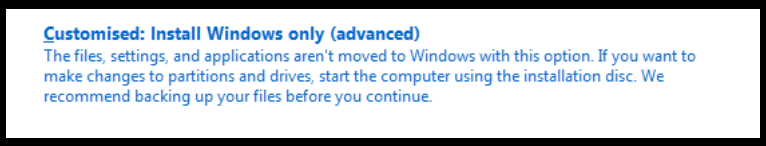


And make sure your VM has slightly over 4GB of RAM and does not have a Floppy Disk installed.

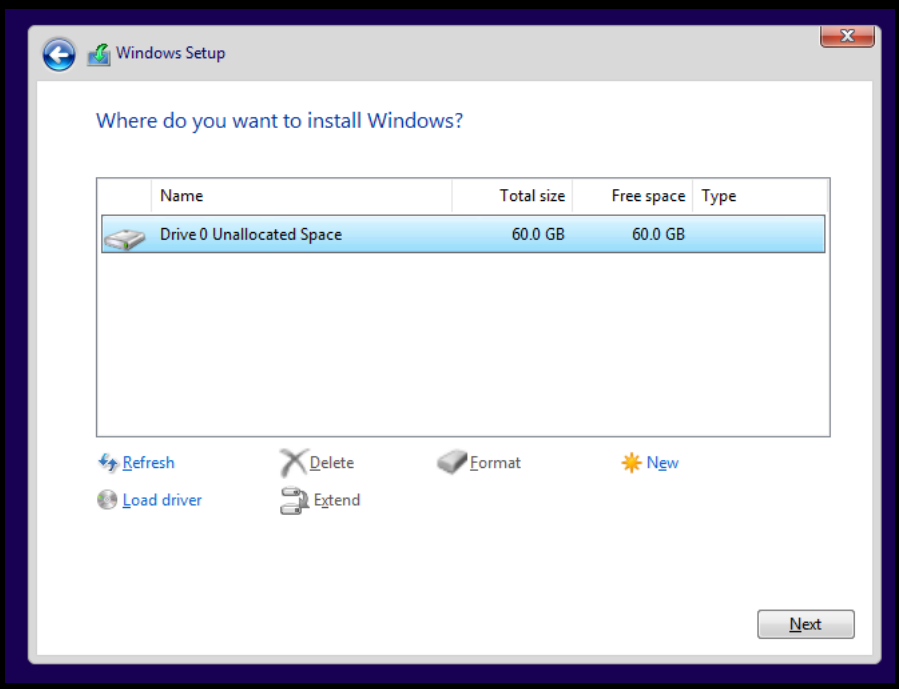
17. Accept the Licence and Click on Next.



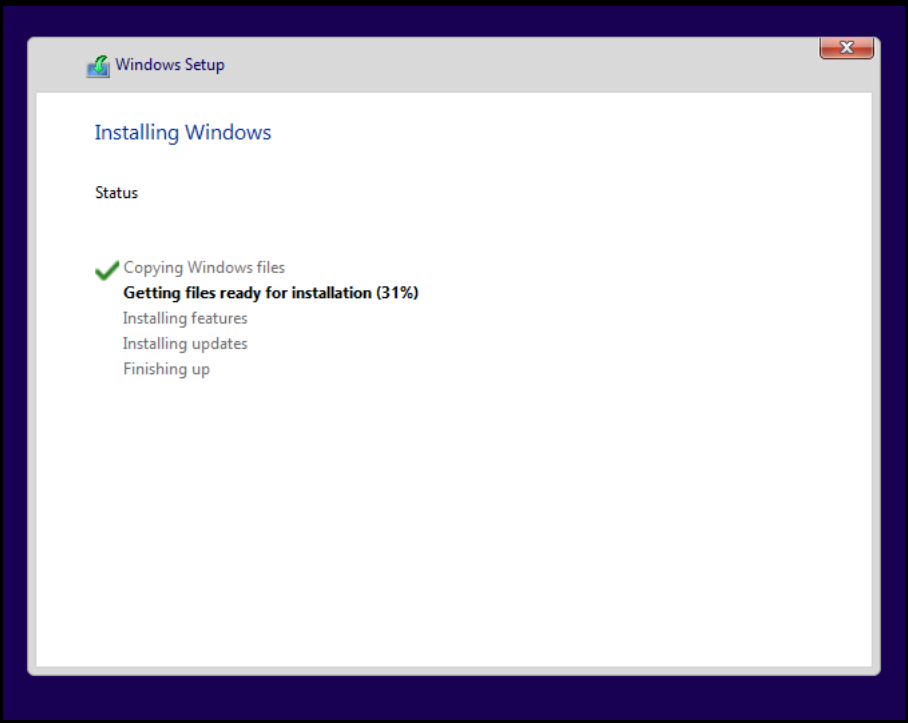
18. Select Customised: Install Windows only (advanced).

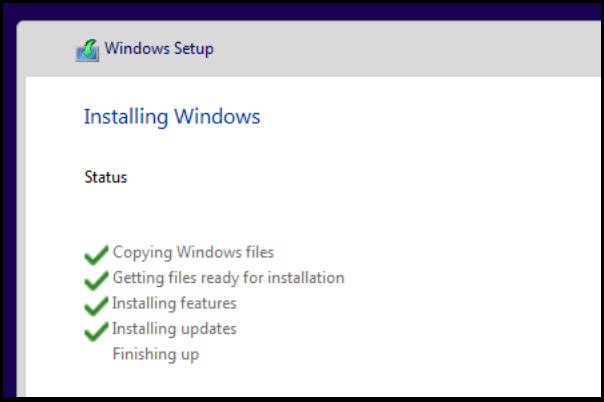


19. Click Next.

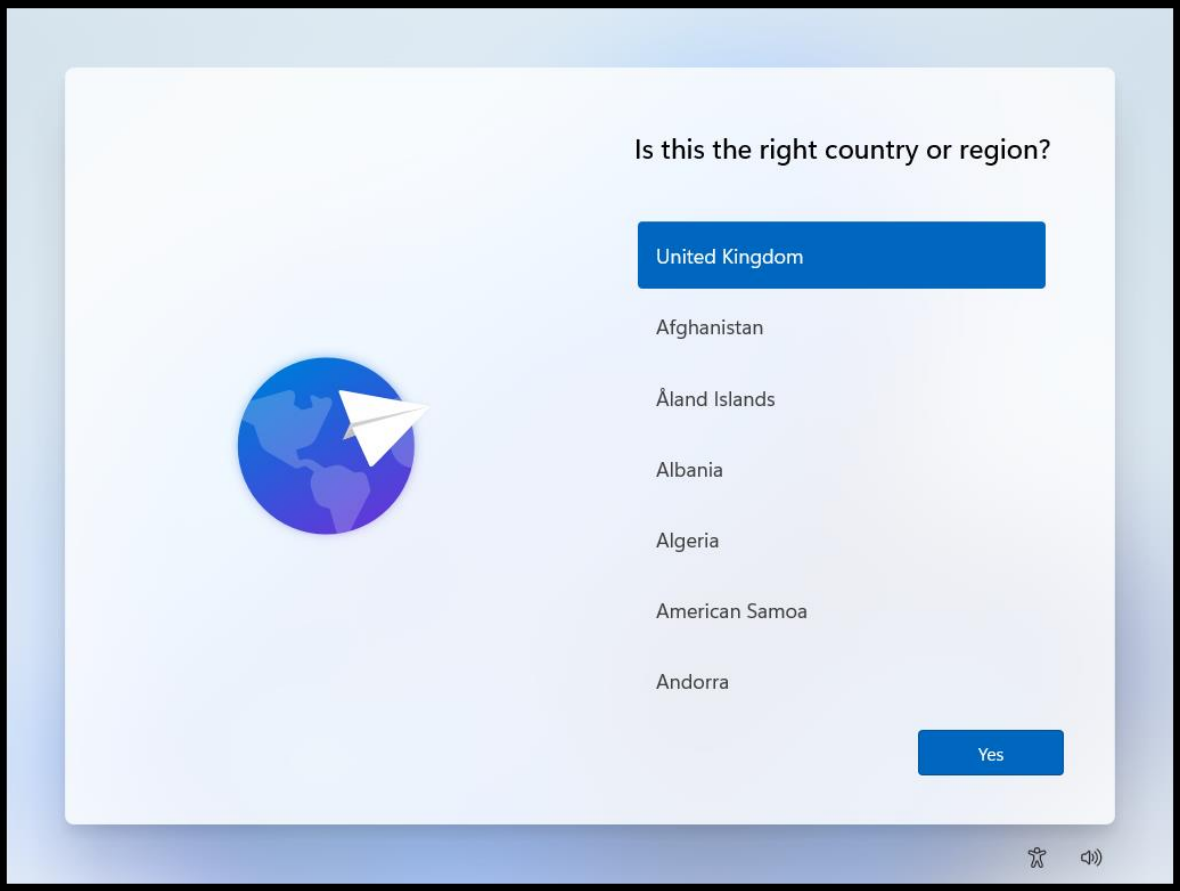


Windows 11 should then start to install and reboot when completed.

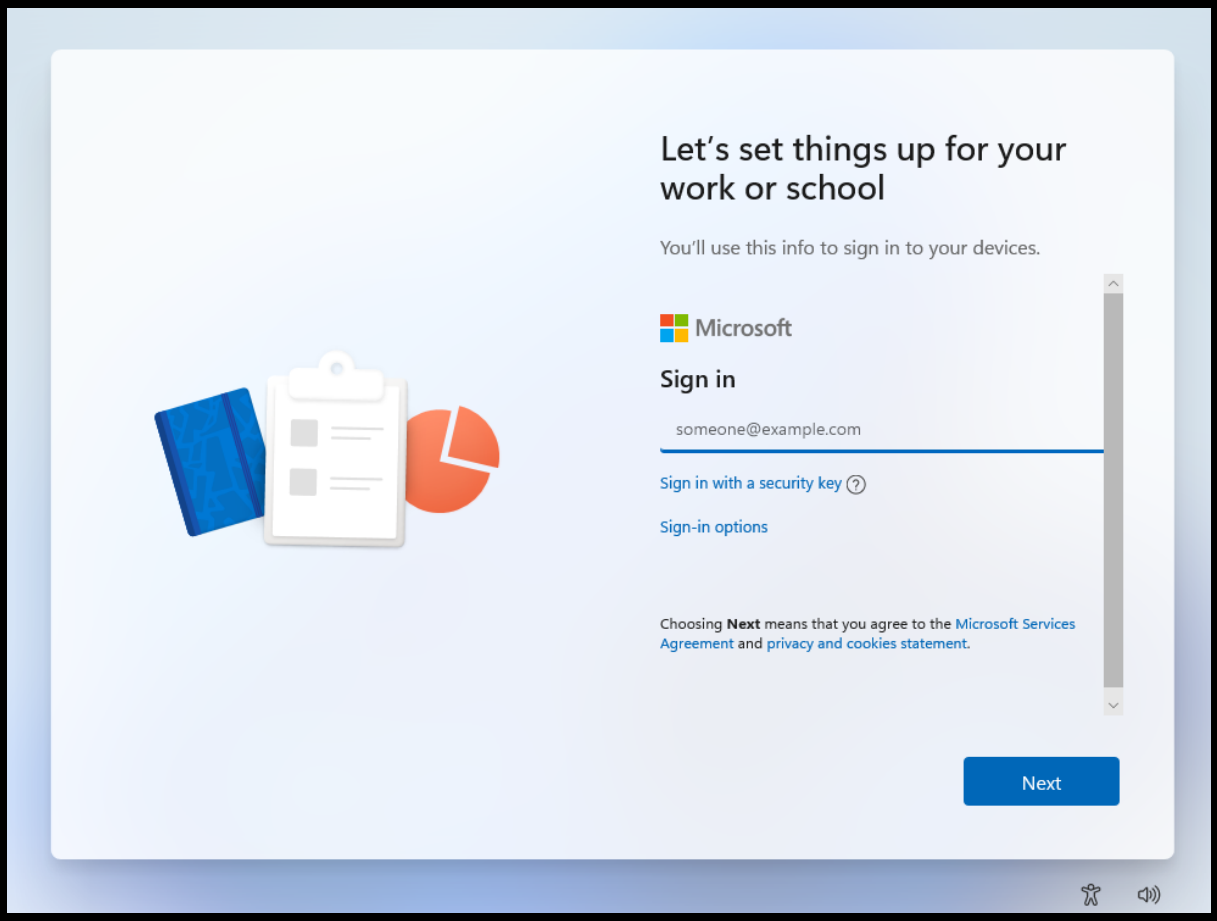




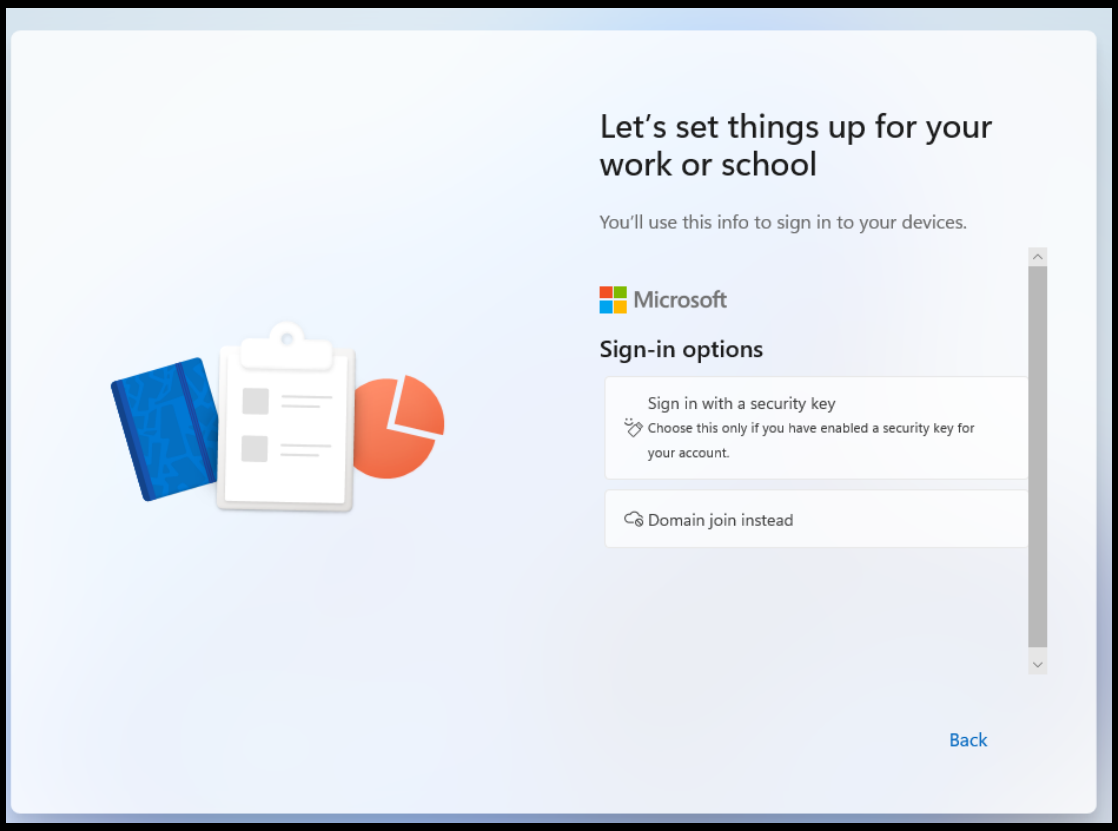
20. After the reboot select your country.



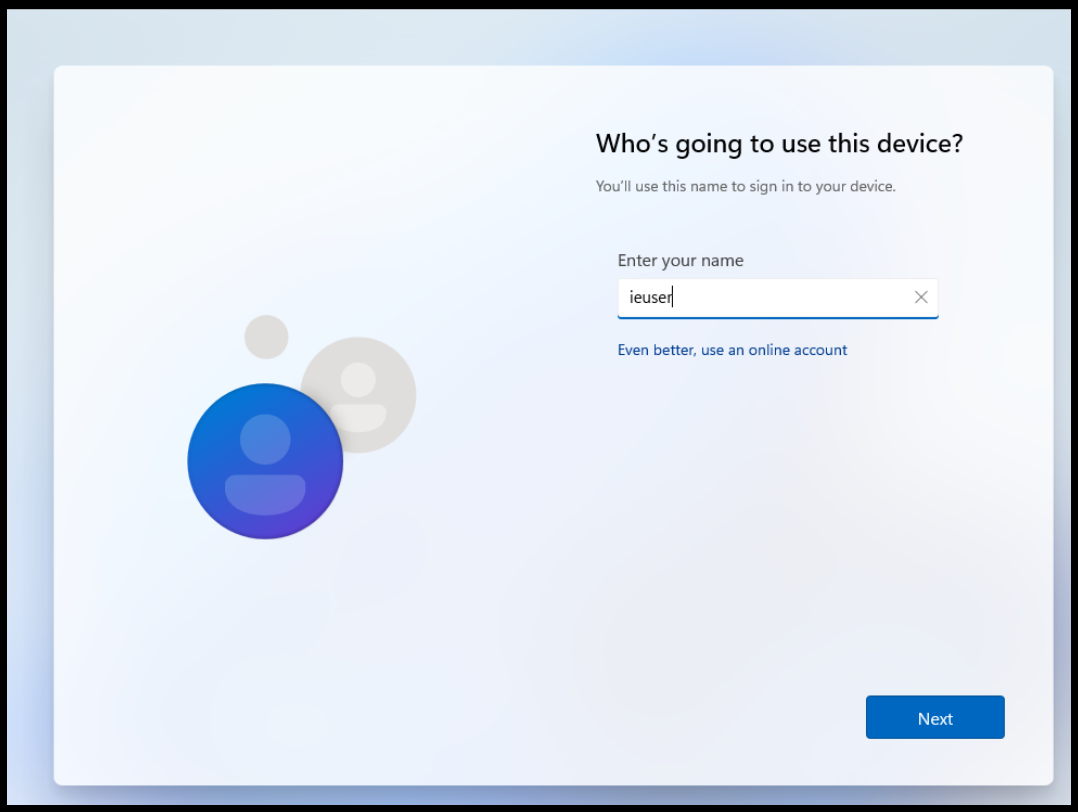
21. Select Sign-In options.



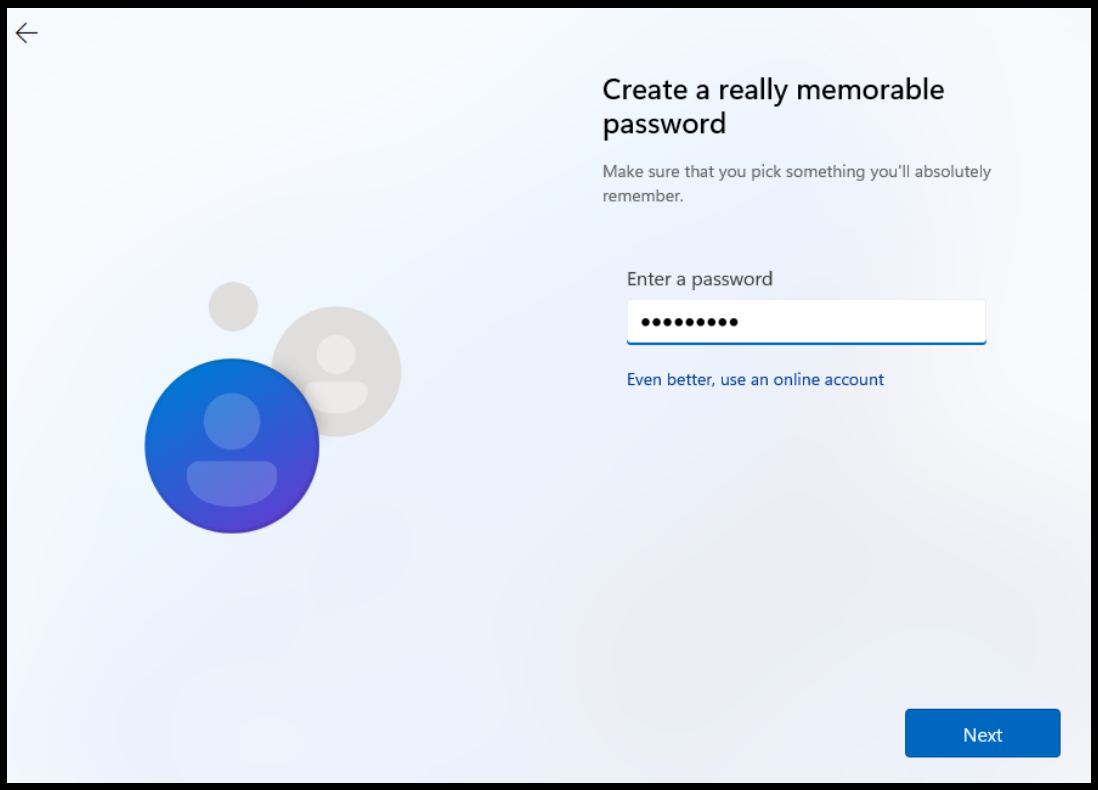
22. Select Domain join instead.



23. Add a username which will be used as the local admin account.

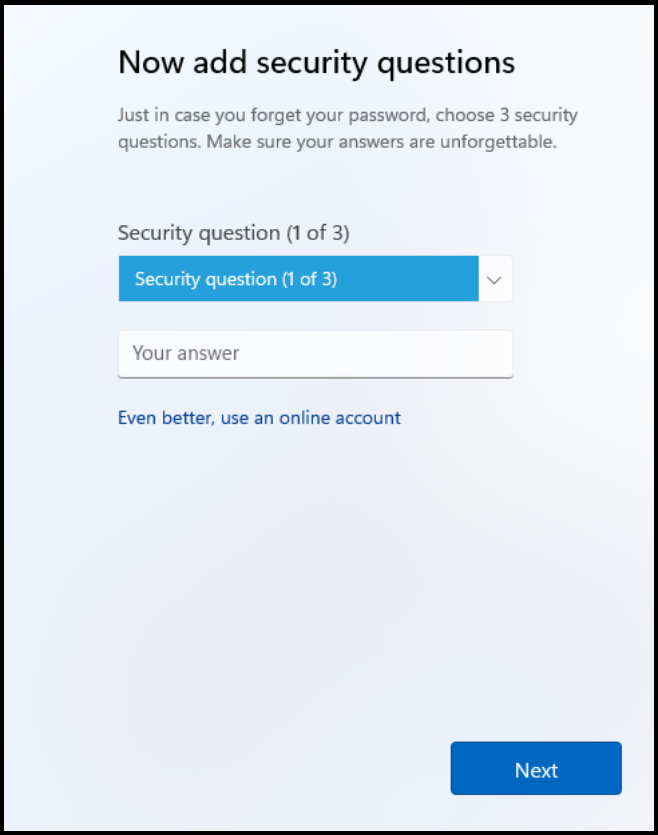


24. Add a password for the account then click on Next.

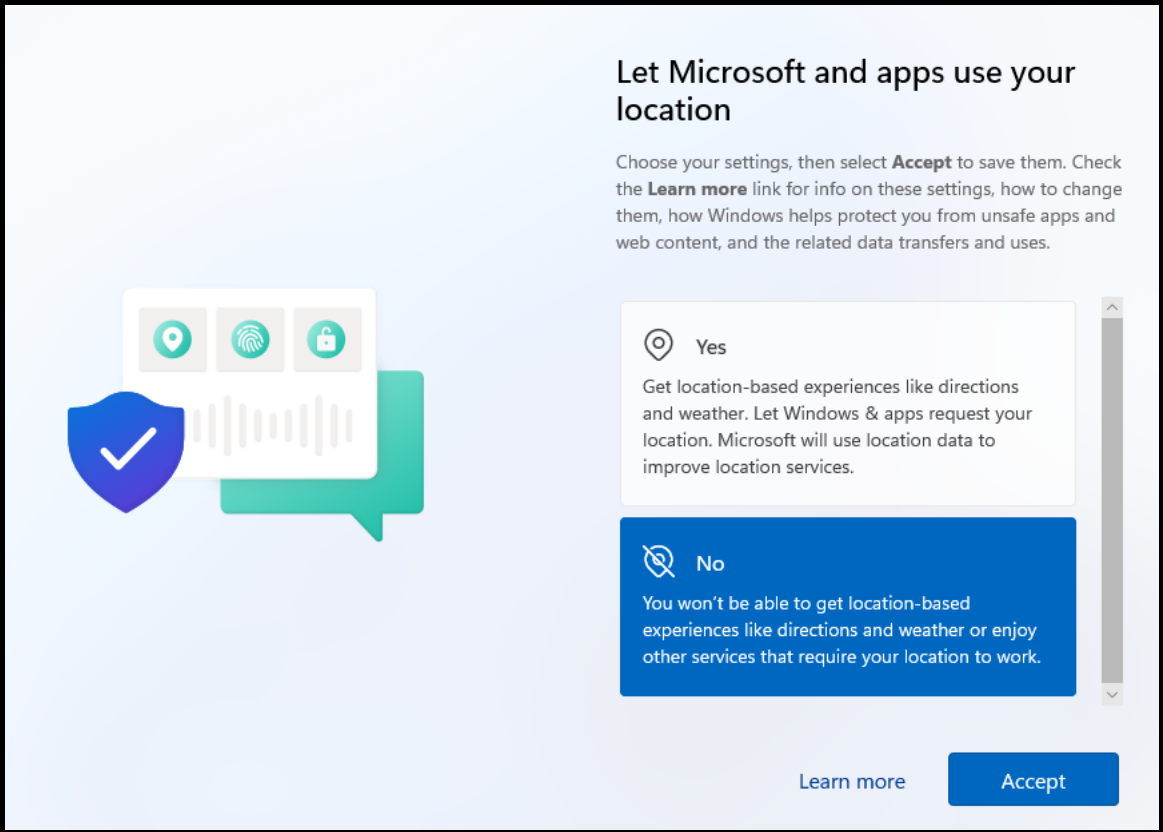


25. Confirm the Password then click on Next.

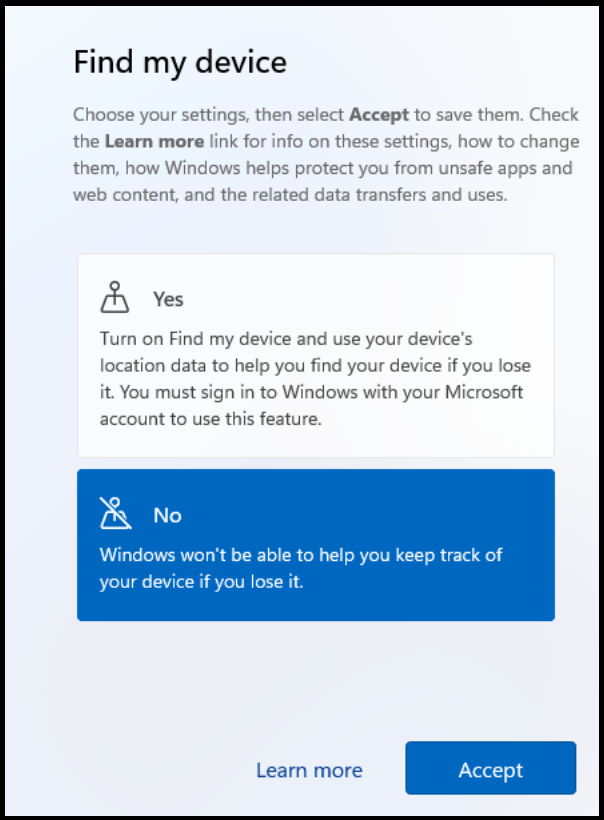
26. Set up your three security questions and answers.



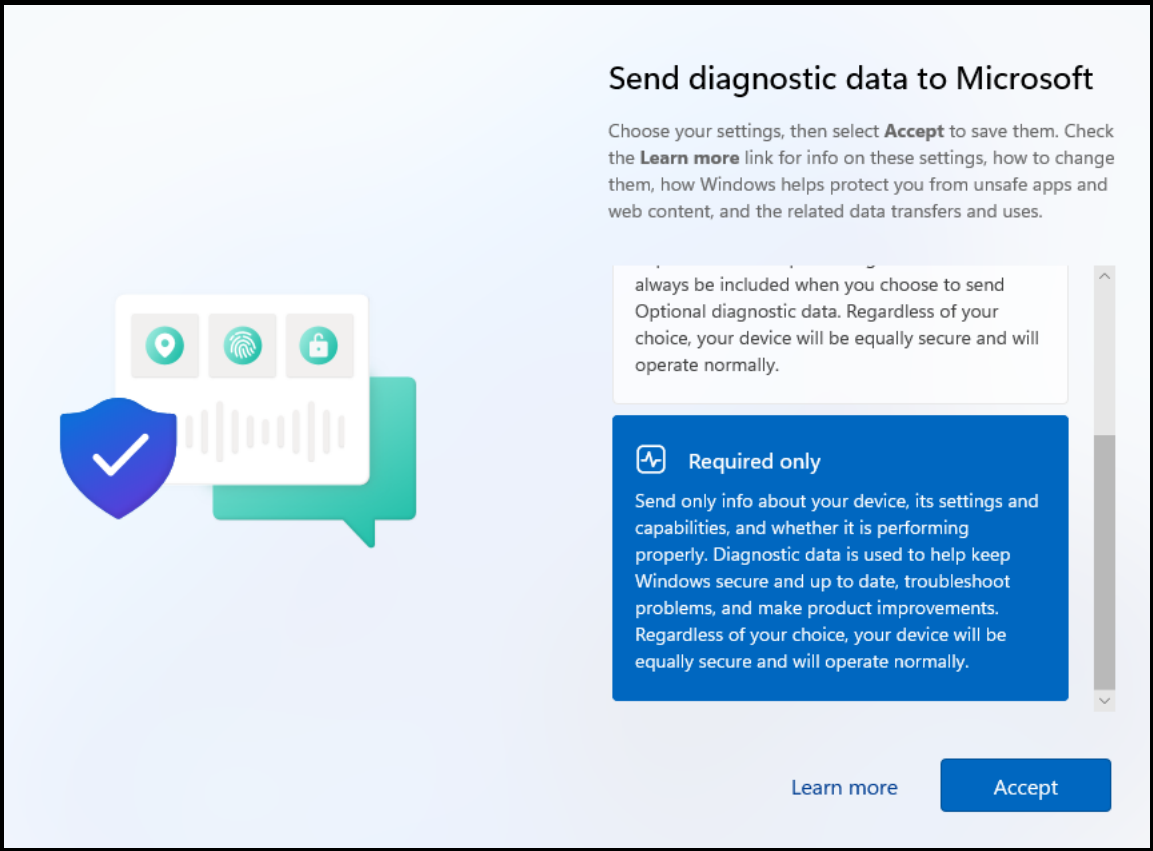
27. Configure location settings.



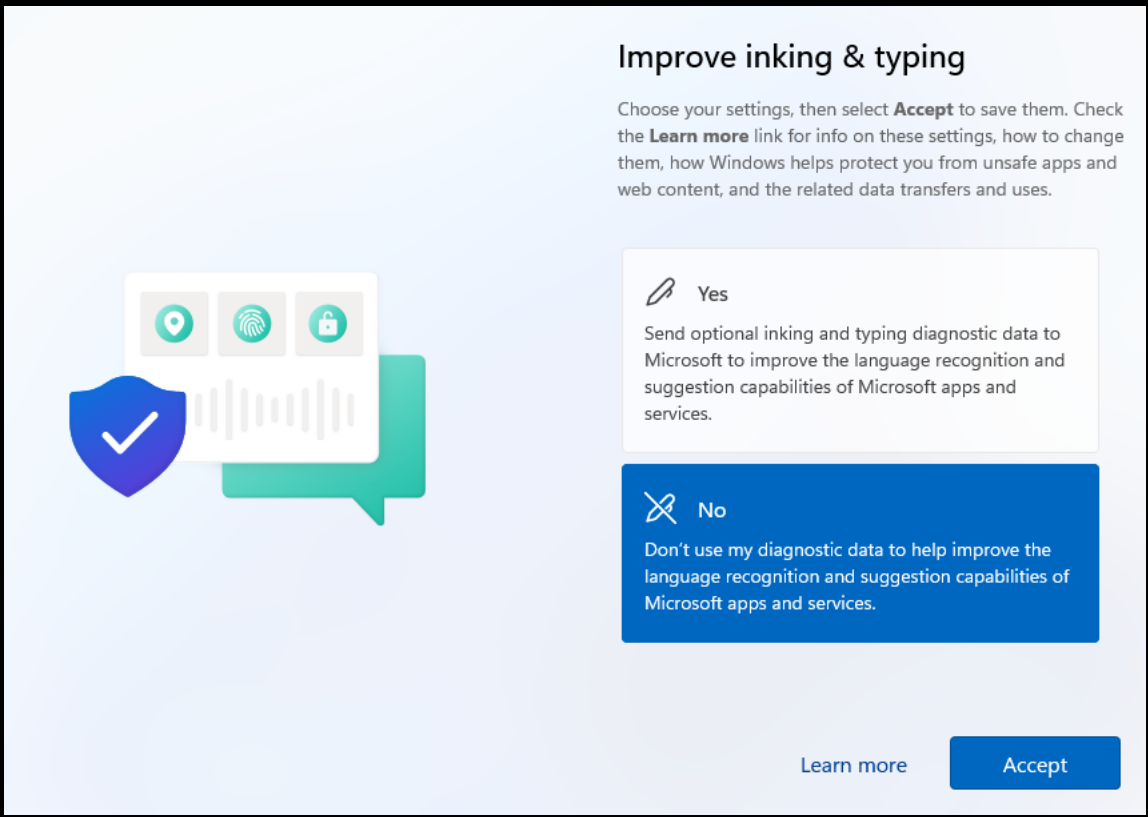
28. Configure Find my device settings.



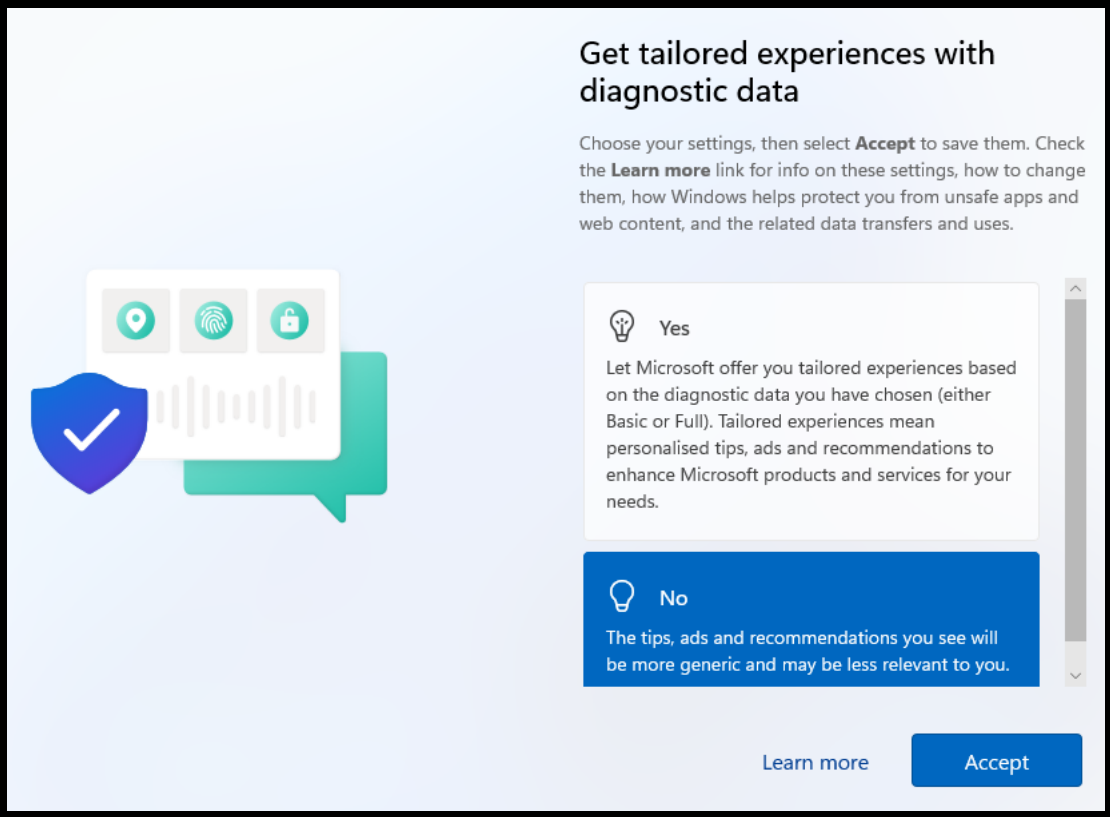
29. Configure Send diagnostic data settings.



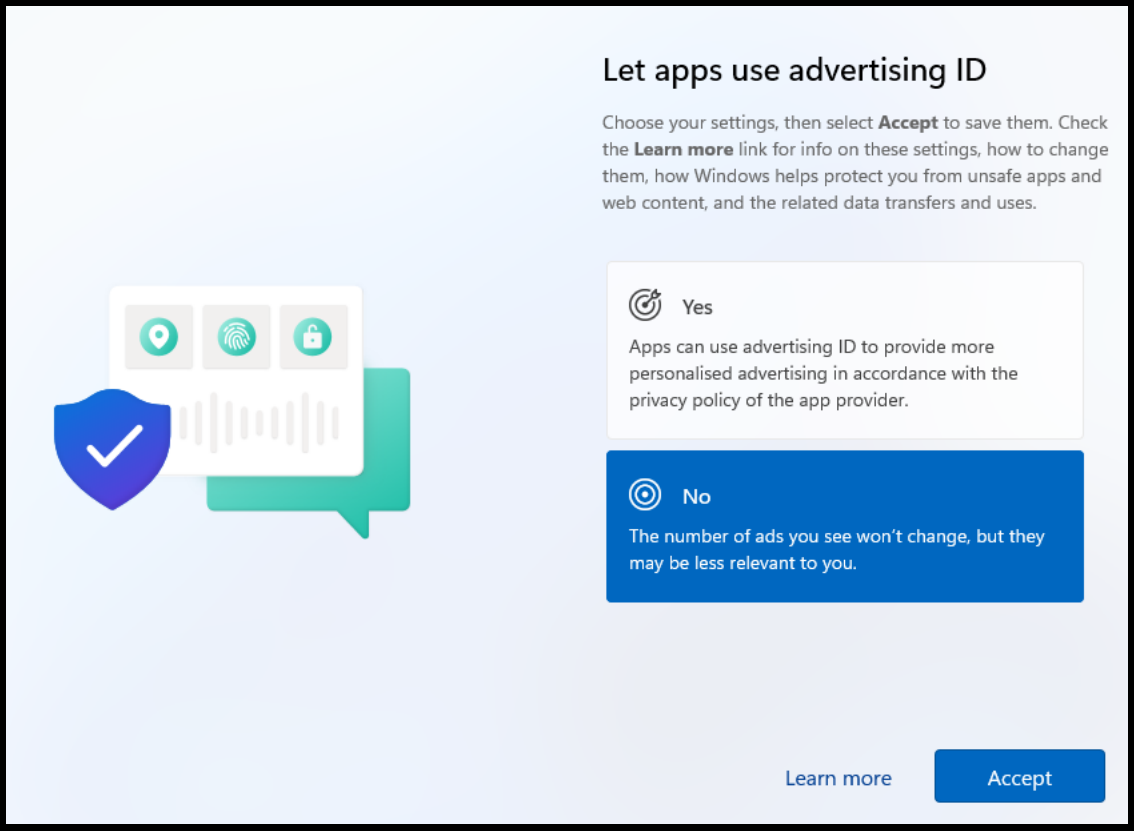
30. Configure the Improve inking settings.



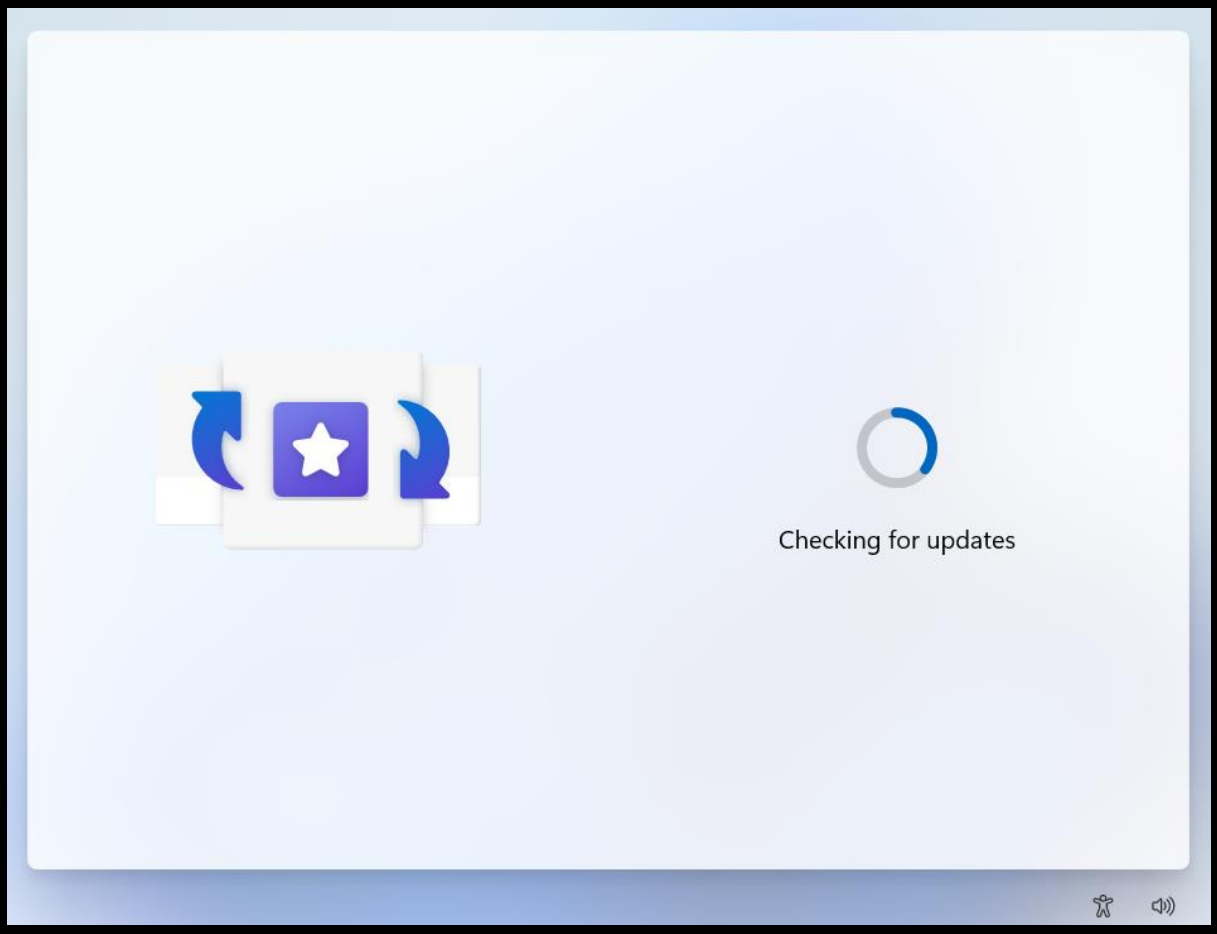
31. Configure the advertising settings.



32. Configure more advertising settings.



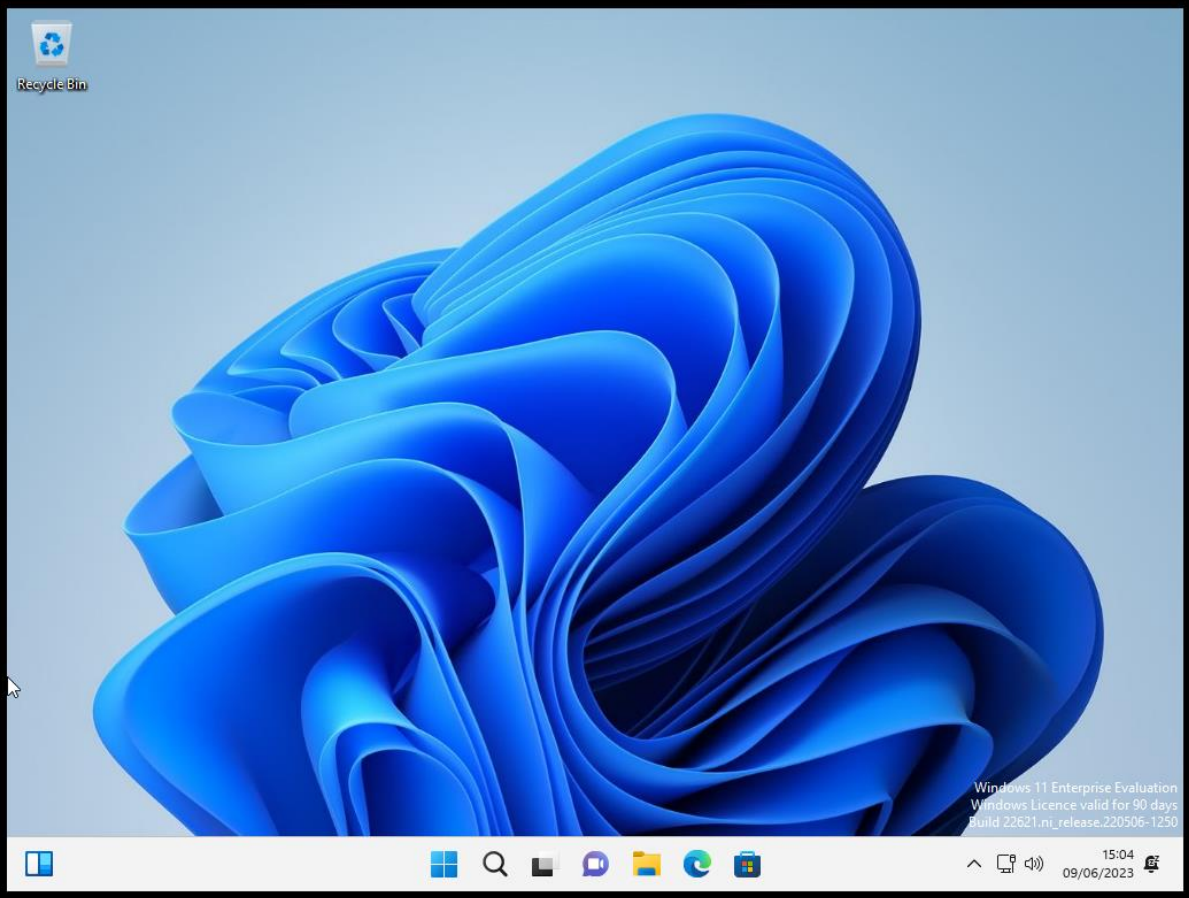
Then host should check for updates.



Presented by Andy Gill & Neil Lines at Steelcon 2023

And finally, you should be close to it completing.

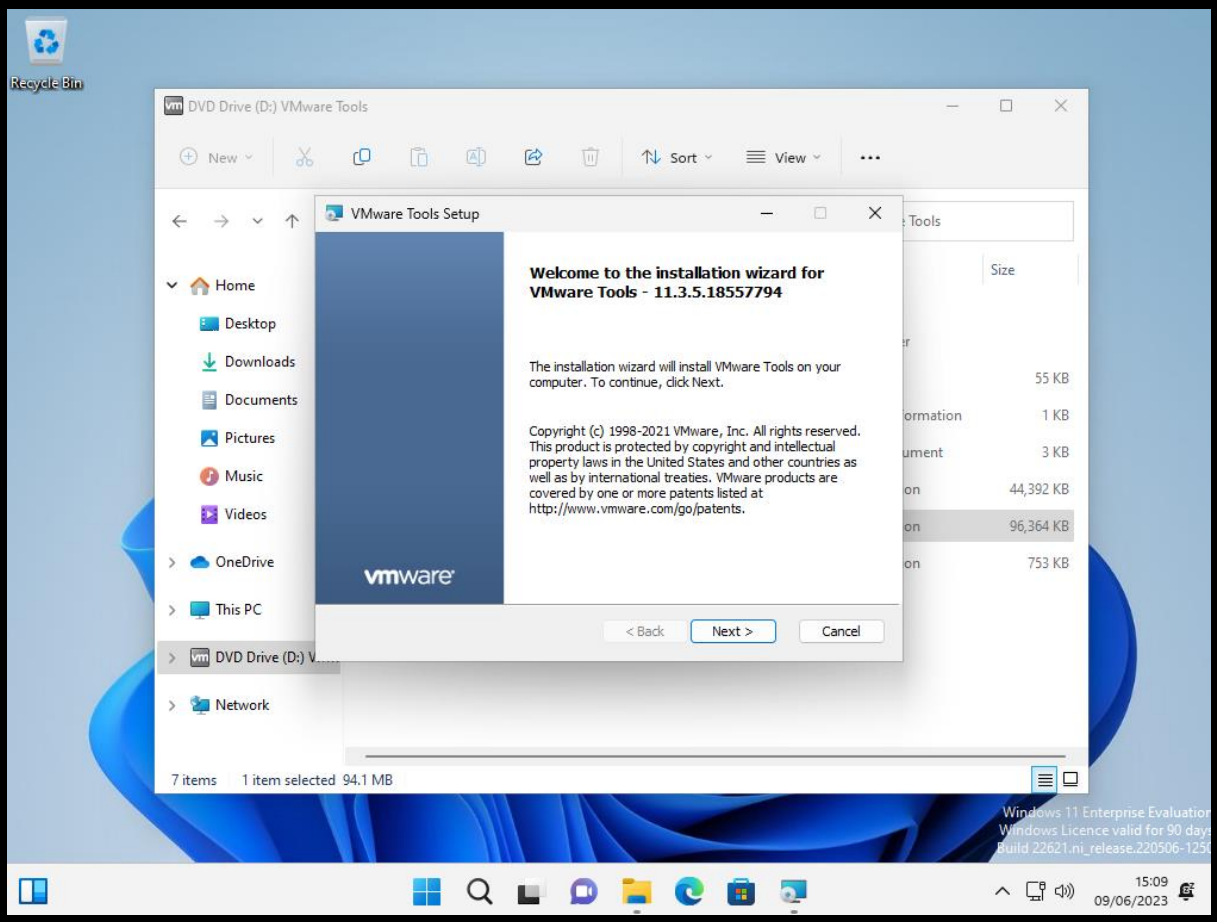
Don't waste time on customising your experience as you will not be using this initial account for long.



33. Firstly, you need to add VM Tools, which uses the same process as with Server 2022.

- Open File Explorer.
- Right Click on the DVD Drive and select Eject.
- Click on the VM tool bar which is outside of your Windows VM.
- Select Install VM Tools.
- Double click the mounted Disk in your VM.
- Double click on setup64.
- Select yes when prompted by UAC.

34. Select Next, Typical Installation followed by Next.



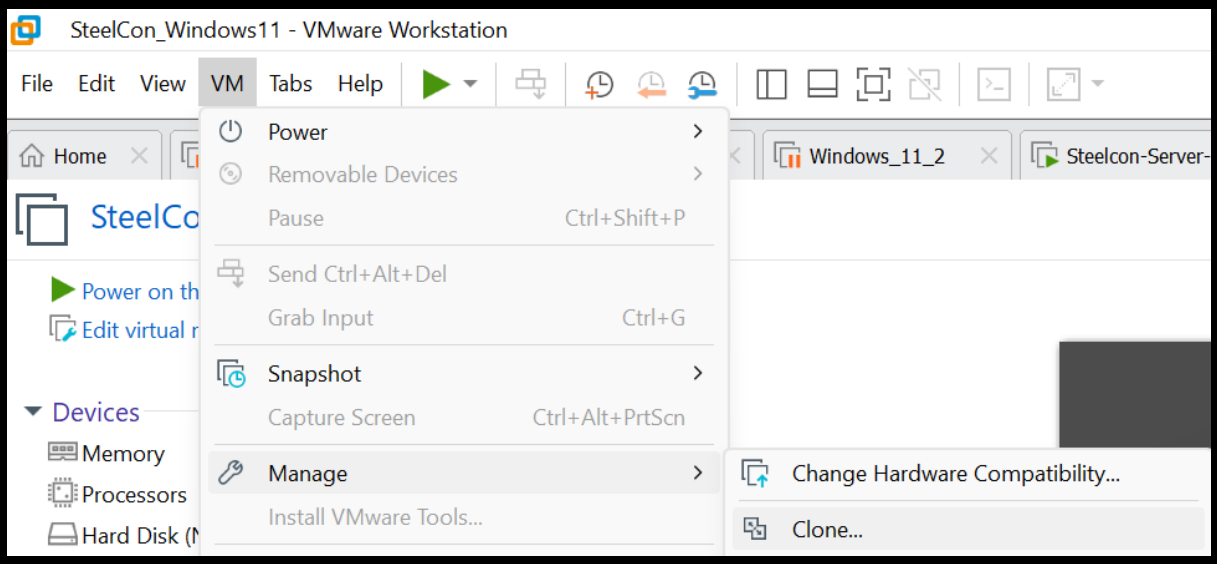
35. Restart the machine.

Windows 11 feels slower than Windows 10 VM's this could improve over time, but it could also be something we just have to get used to.

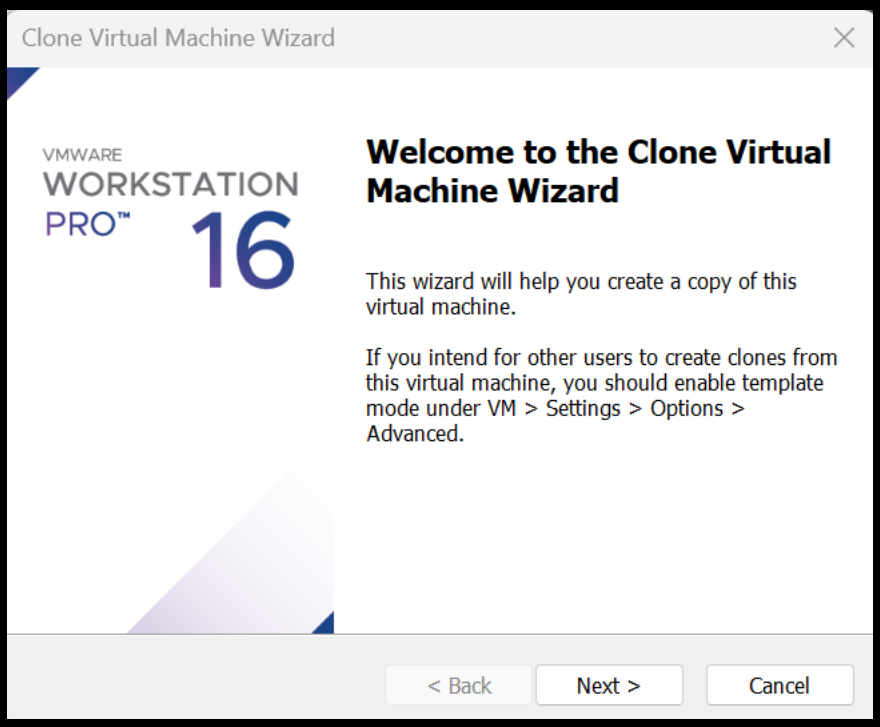
Cloning a Windows 11 VM

It is worth cloning the Windows 11 machine so you will have two domain machines to play around with.

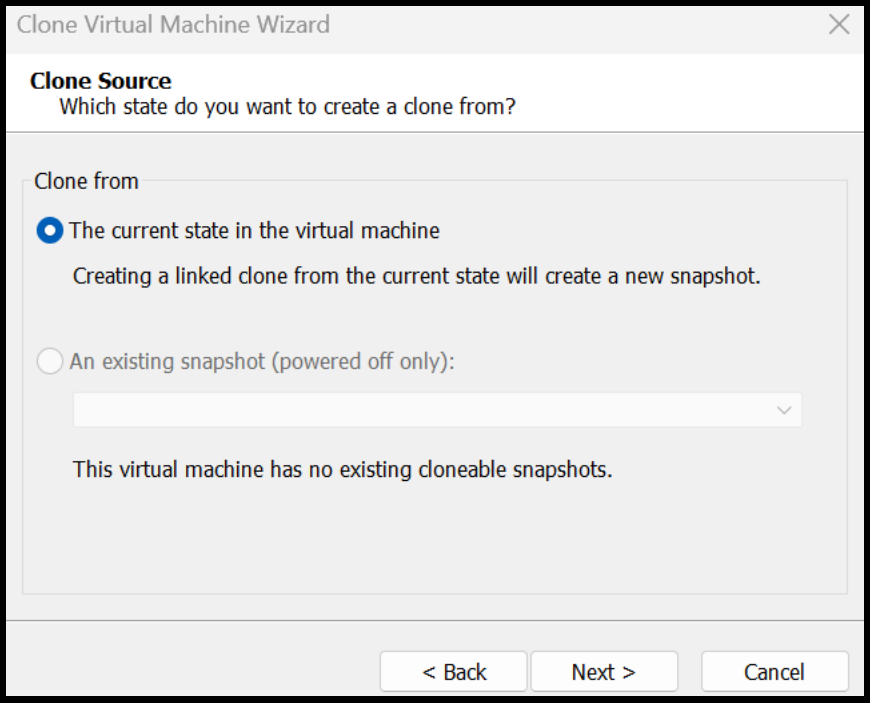
1. Make sure the VM you wish to clone is powered off.
2. Select VM from the tool bar / Manage / Clone.



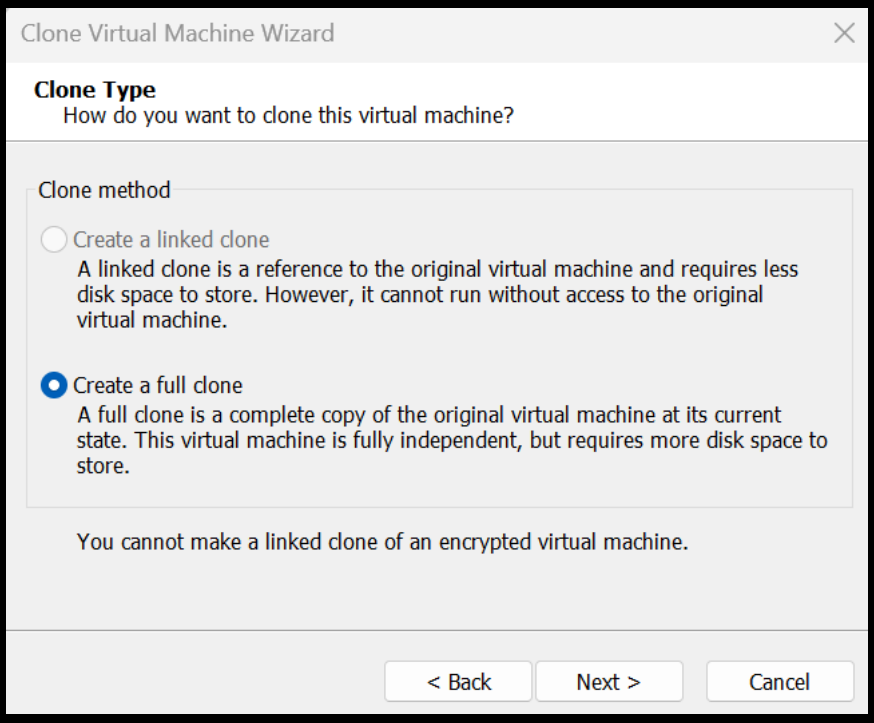
3. Click Next.



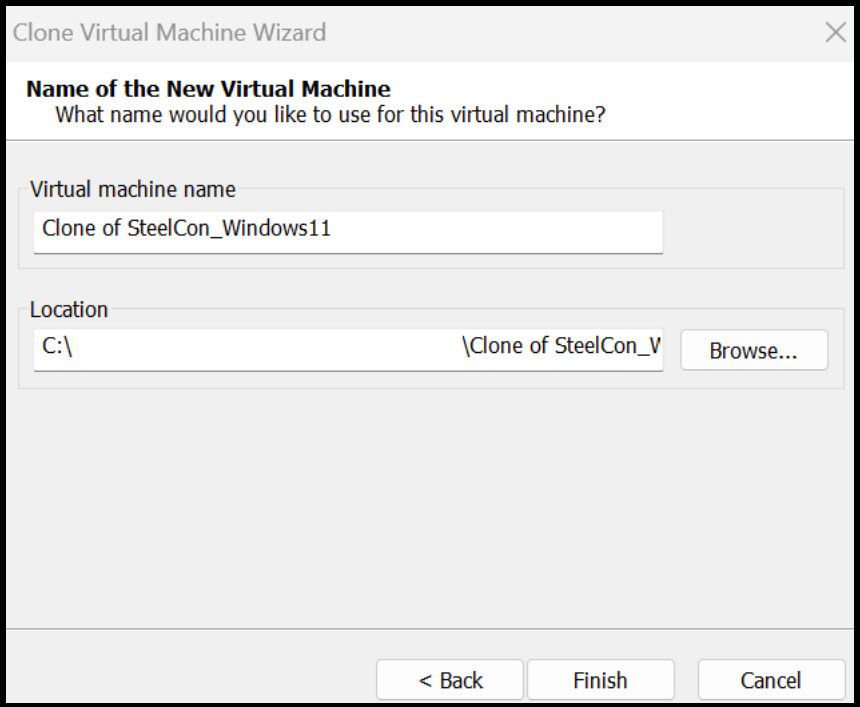
4. Select The current state in the virtual machine.



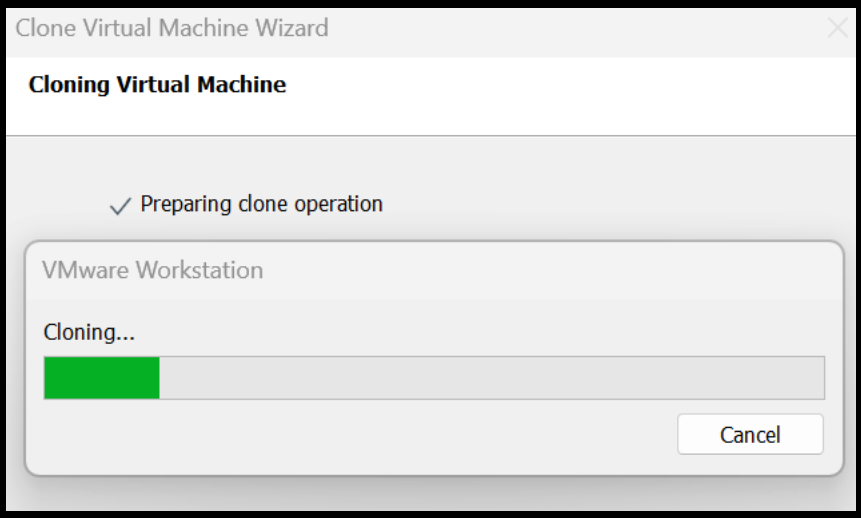
5. Click Next.



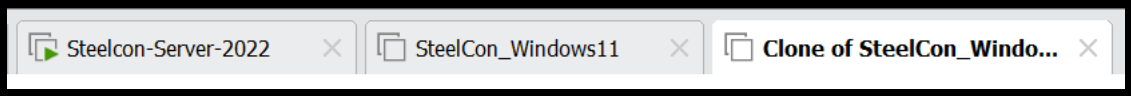
6. Rename it then select Finish.



The cloning process should initiate.

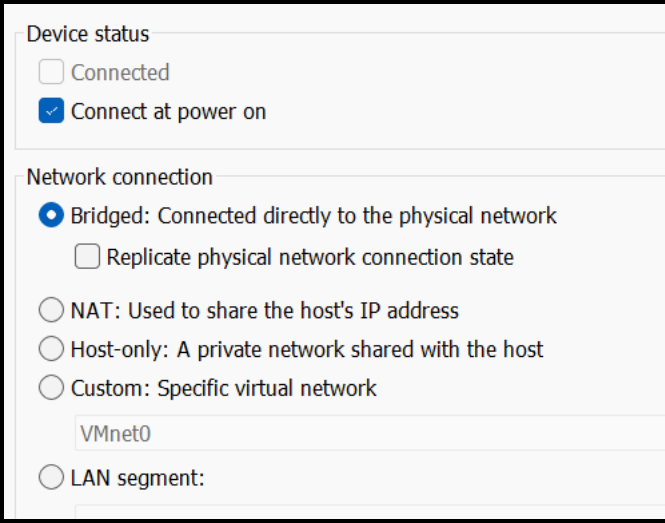


And once its completed you should see your three machines on the top VM tool bar.

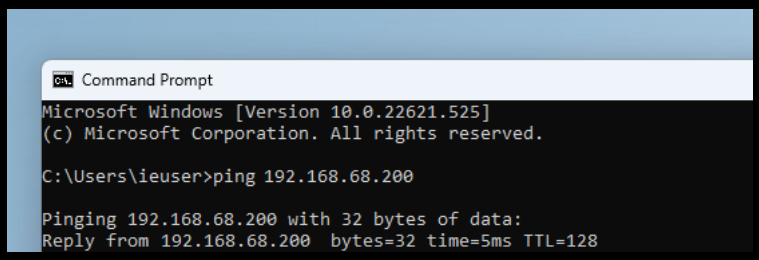


Adding a Windows 11 VM to the hacklab domain

1. Select the VM you want to add to the Domain, and under the setting make sure its Network connection is set to the same network as your domain controller.



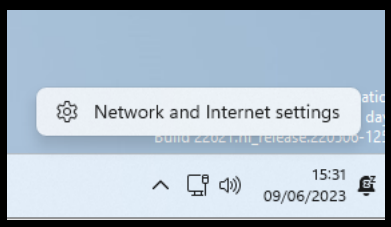
2. Open CMD and confirm you can ping the domain controllers IP address.



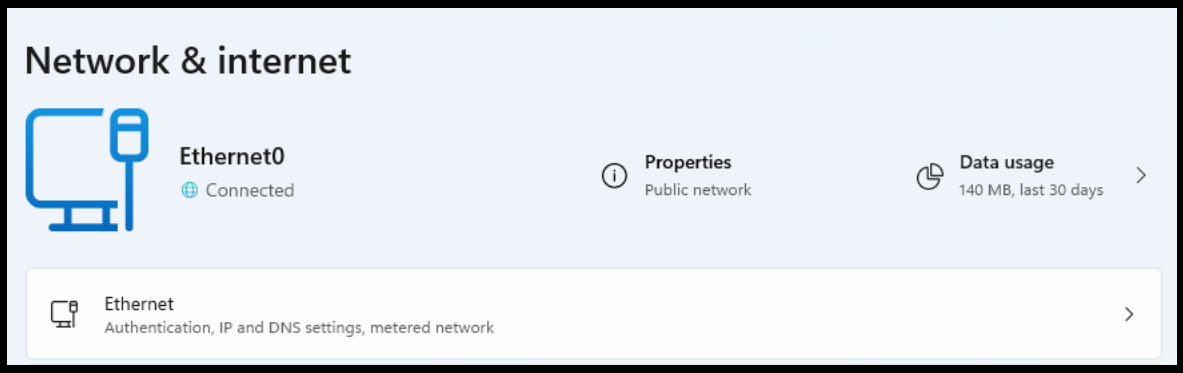
You can ping a DC even if it has its windows firewall enabled, If you don't get a reply from the DC's IP address you will not be able to add the machine to the Domain, check the DC's IP address is correct, then if that's ok double check the VM networking settings.

If you did get a reply from your DC continue onto step 3.

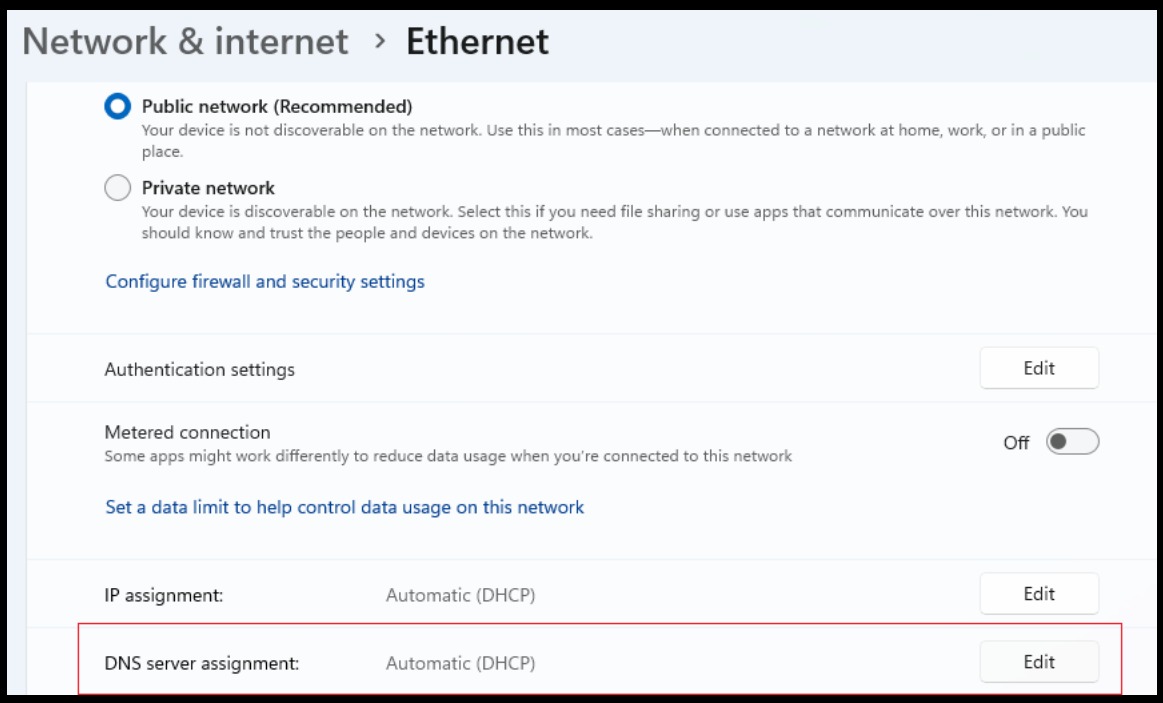
3. On your Windows 11 VM you need to open Network and Internet settings so you can add the domain controllers IP address for DNS services.



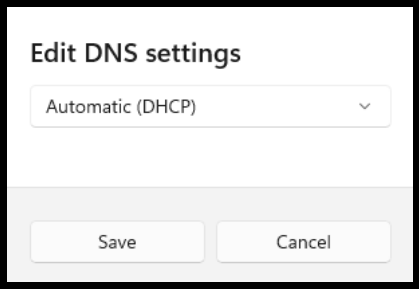
4. Click on Ethernet.



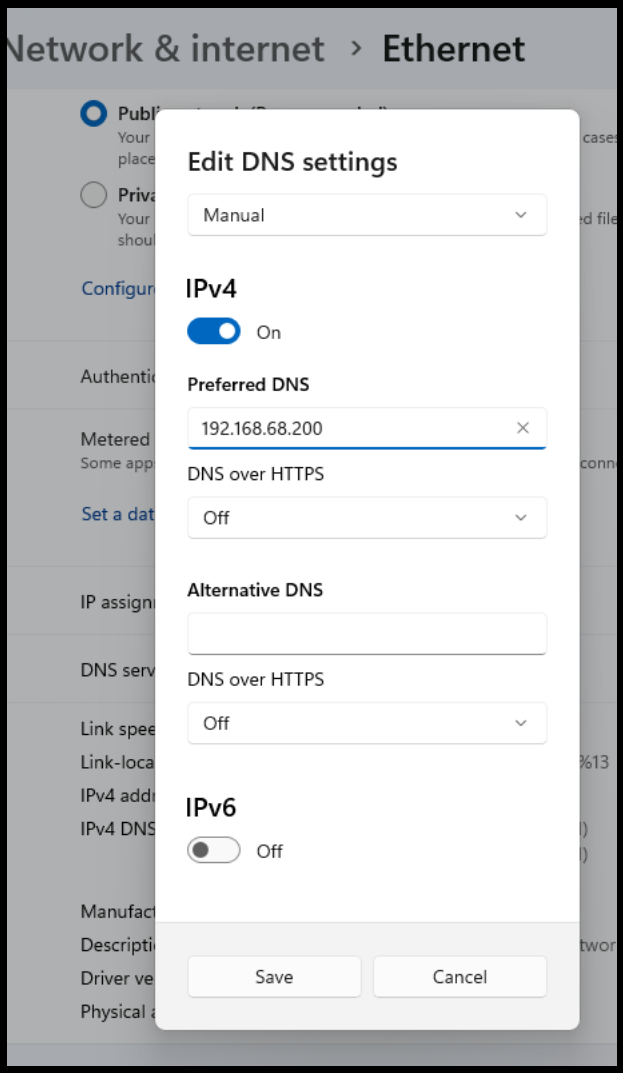
5. Under DNS server assignment, click Edit.



6. Change the default from Automatic (DHCP) to manual.



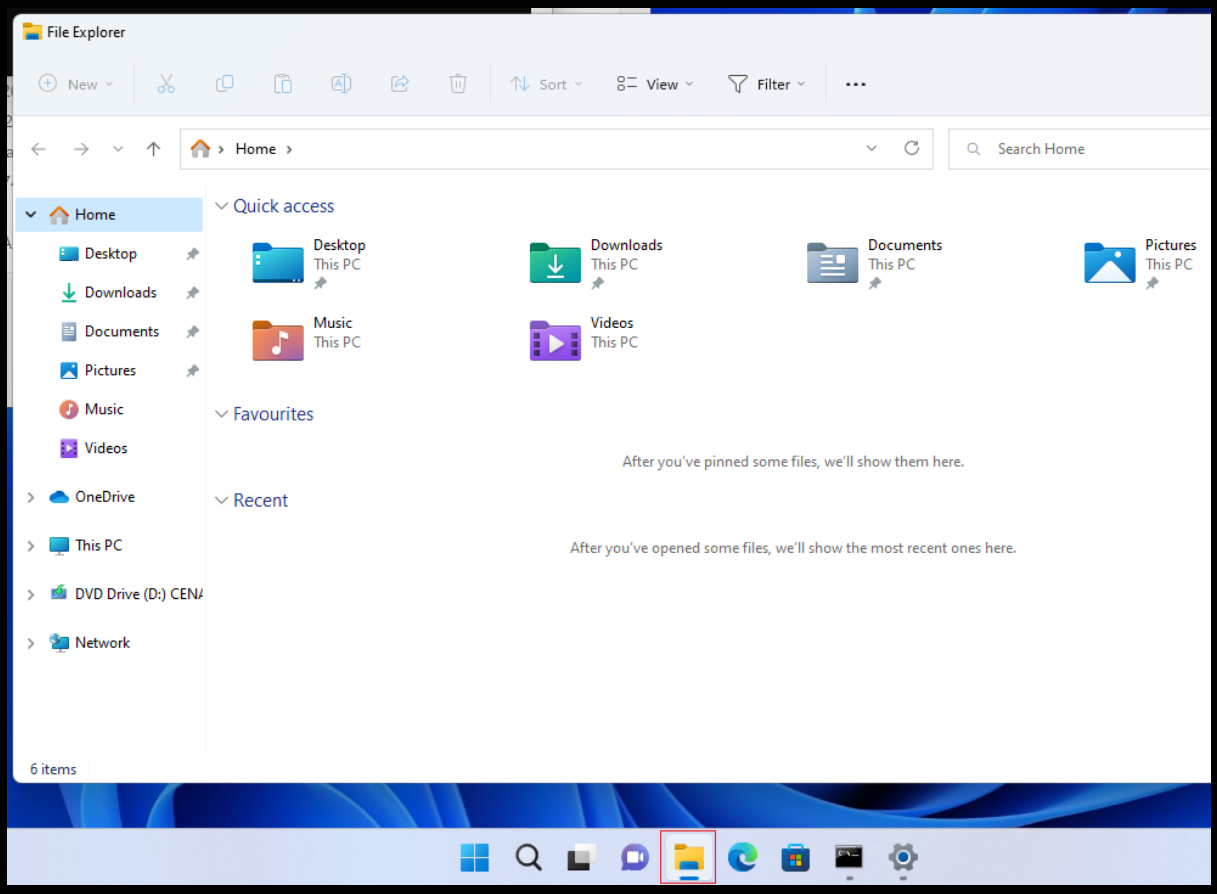
7. Tick on IPv4, then add the IP address of your domain controller followed by Save.



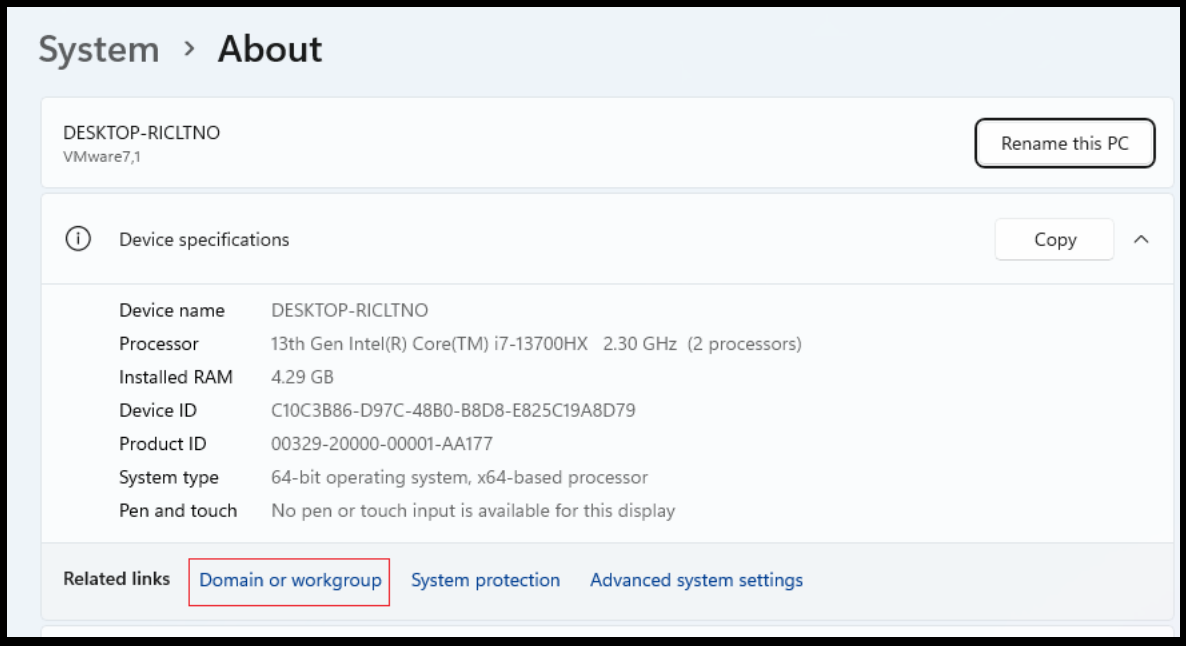
8. Try and ping hacklab.local from your windows 11 host, it should now resolve.

```
C:\Users\ieuser>ping hacklab.local

Pinging hacklab.local [192.168.68.200] with 32 bytes of data:
Reply from 192.168.68.200: bytes=32 time=1ms TTL=128
```

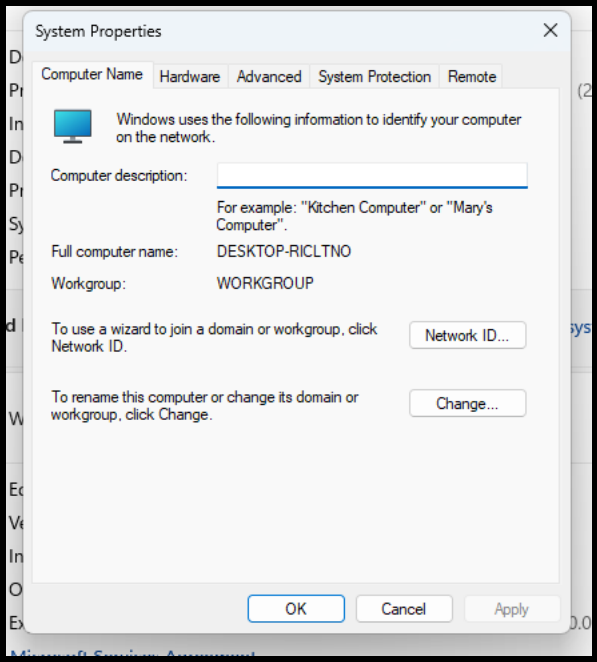
9. If you can ping the Domain, you are ready to add the machine to the Domain, Open File explorer.



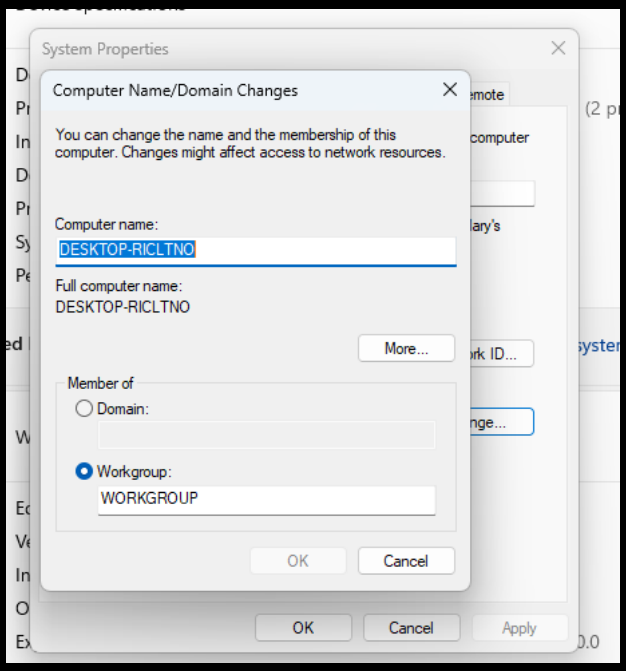
10. Right click on This PC and select Show More Options followed by Properties.
11. Select the Domain or workgroup settings.



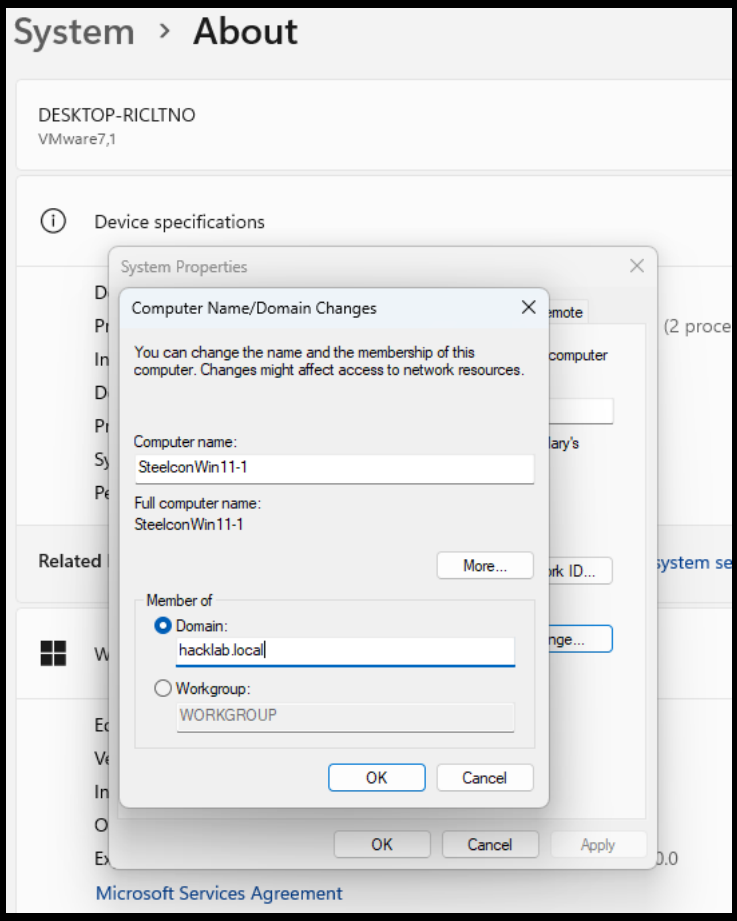
12. Click on Change.



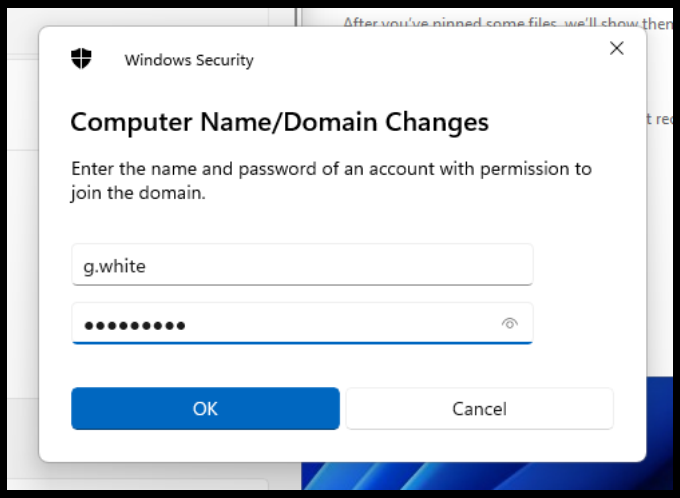
13. This is also your chance to rename the machine to something more logical.

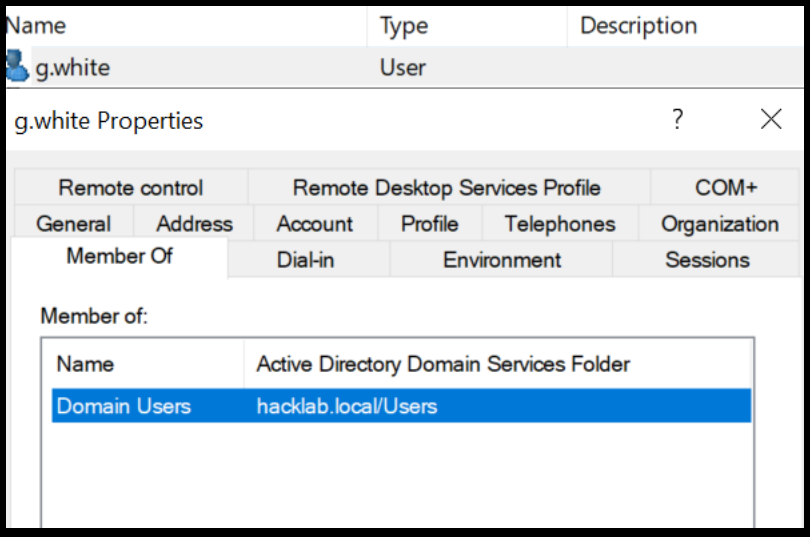


14. Select Domain then type in the full domain name hacklab.local followed by clicking on OK.

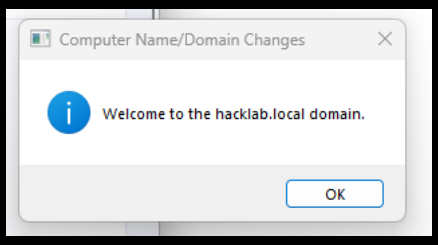


You should then be prompted to enter a domain account, by default any member of the domain users' group can add up to 10 machines to a domain. Yep any standard user!



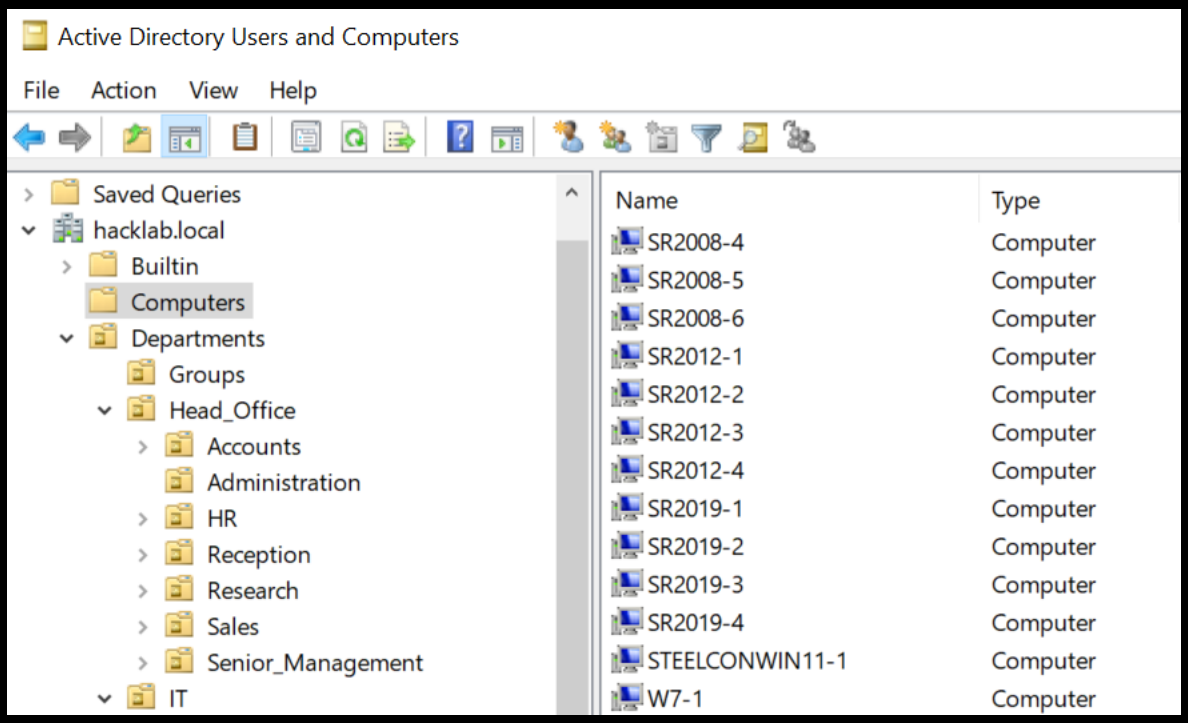


And if all is going to plan you should see Welcome to the Domain!

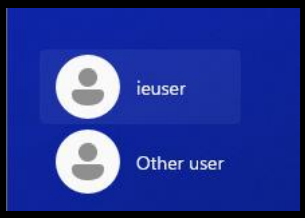


15. Reboot your Windows 11 machine.

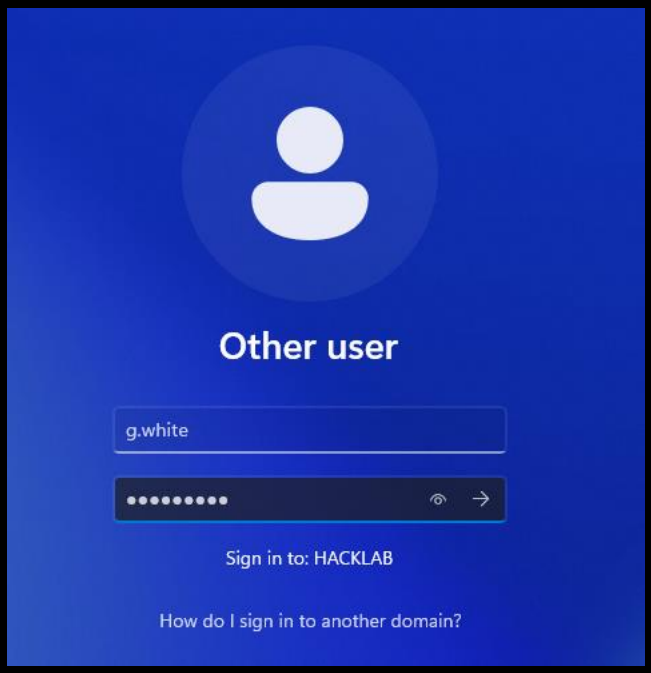
If you jump over to the domain controller and look under Computers you will see the machine that you have just added to the Domain.



16. After the restart click on Other user.



17. Then use any of the domain user accounts to login.



Repeat this process to add any other machines.

SlinkyCat

Download SlinkyCat: https://github.com/LaresLLC/SlinkyCat

Slinky Cat has been developed to automate some of the methods introduced in living off the land and to supplement ScrapingKit. To help security and IT teams reduce their AD exposures and uncover quick wins and fixes designed for pen-testers and defenders alike.

Slinky Cat attempts to give users an easy-to-navigate menu offering predefined Active Directory Service Interfaces (ADSI) and .NET System.DirectoryServices.AccountManagement namespace queries can be used to enumerate a Windows domain.

1. Download SlinkyCat.ps1 and attempt to import it, if you see the error below you need to bypass the default PowerShell execution policy.

```
Windows PowerShell    Windows PowerShell
PS C:\Users\g.white\Desktop\Steelcon\SlinkyCat> ipmo .\SlinkyCat.ps1
ipmo : File C:\Users\g.white\Desktop\Steelcon\SlinkyCat\SlinkyCat.ps1 cannot be loaded
because running scripts is disabled on this system. For more information, see
about_Execution_Policies at https:/go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ ipmo .\SlinkyCat.ps1
+ ~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [Import-Module], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess,Microsoft.PowerShell.Commands.ImportM
   oduleCommand
PS C:\Users\g.white\Desktop\Steelcon\SlinkyCat>
```

Method 1 to bypass PowerShell execution policy, copy and paste the line below and press enter.

powershell.exe -nop -exec bypass

```
Windows PowerShell    Windows PowerShell
PS C:\Users\g.white\Desktop\Steelcon\SlinkyCat> ipmo .\SlinkyCat.ps1
ipmo : File C:\Users\g.white\Desktop\Steelcon\SlinkyCat\SlinkyCat.ps1 cannot be loaded
because running scripts is disabled on this system. For more information, see
about_Execution_Policies at https:/go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ ipmo .\SlinkyCat.ps1
+ ~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [Import-Module], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess,Microsoft.PowerShell.Commands.ImportM
   oduleCommand
PS C:\Users\g.white\Desktop\Steelcon\SlinkyCat> powershell.exe -nop -exec bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindow
s

PS C:\Users\g.white\Desktop\Steelcon\SlinkyCat>
```

You should be able to import the script and then execute it.

```
PS C:\Users\g.white\Desktop\Steelcon\SlinkyCat> ipmo .\SlinkyCat.ps1
PS C:\Users\g.white\Desktop\Steelcon\SlinkyCat> Invoke-SlinkyCat
```

Method 2 which is a sneaky method, simply open the complete script in notepad, highlight it all, copy and paste it into a PowerShell session, it should load bypassing the restriction.

```
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\g.white> # SlinkyCat v1.0
PS C:\Users\g.white> # Lares Labs - https://labs.lares.com/
PS C:\Users\g.white> # Neil Lines & Andy Gill, 2023
PS C:\Users\g.white>
PS C:\Users\g.white> <#
>> .SYNOPSIS
>>     This script performs a series of AD enumeration tasks, giving output to the terminal
nal.
>>
>> .DESCRIPTION
>>     Slinky Cat has been developed to automate some of the methods introduced in living o
 ScrapingKit. To help security and IT teams reduce their AD exposures and uncover quick wir
testers and defenders alike.
>>
>> .PARAMETER domain
>>     The domain to be run against, it will default to whatever domain lives in USERDNSDOM
QDN.
>>
>> .EXAMPLE
>>     Invoke-SlinkyCat
```

2. The Menu allows you to select which method you want to use to enumerate the Domain.

```
Windows PowerShell
=== Menu ===
1. ADSI Enumeration
2. Dot NET System.DirectoryServices.AccountManagement Namespace Enumeration
3. List Available Individual Functions
Q. Quit
Enter your choice: :
```

All sub options from within the ADSI enumeration selection.

```
Windows PowerShell
=== Menu ===
1. ADSI Enumeration
2. Dot NET System.DirectoryServices.AccountManagement Namespace Enumeration
3. List Available Individual Functions
Q. Quit
Enter your choice: : 1
ADSI Optinos Menu Please select an option:
1. Enumerate all domain hosts
2. Enumerate all domain controllers
3. Enumerate all domain users
4. List all users in the domain admins group
5. List all accounts with an SPN
6. List all domain groups
7. List all password set to never expire
8. List all users which do not require a password
9. List all users with password must change at next logon
10. List all computers that are not Domain Controllers and are Windows 7
11. List all computers that are not Domain Controllers and are Windows 10
12. List all computers that are not Domain Controllers and are Windows 11
13. List all servers
14. List all Server 2008
15. List all Server 2012
16. List all Server 2016
17. List all Server 2019
18. List all Server 2022
19. List domain groups which are a member of the local admin group
20. List all trusts established with a domain
21. List all Exchange servers
22. List all accounts that have never logged in
23. List all domain user accounts which have a completed AD description field
24. List all accounts that reference 'pass' in their AD description field
25. List all users who have not changed their password in over 1 year
26. List all users' last password change date and time
27. List all systems with WinRM Open (Not OPSEC SAFE!)
28. List all systems with RDP Open (Not OPSEC SAFE!)
29. Find all machines where the current user has local admin acess (Not OPSEC Safe, will list all computers then attempt to mount C$)
A. Run all functions and export to an output folder full of txt files
Q. Quit
Enter your choice:
```

3. Selecting an option such as 22' List all accounts that have never logged in' reveals the response to the ADSI request.

```
Enter your choice: 22
Option: ADSI List all accounts that have never logged in
Guest
krbtgt
NULL
david
robert
chris
mike
dave
richard
thomas
steve
mark
daniel
george
paul
charlie
```

4. Option 29 'Find all machines where the current user has local admin access'.

```
Enter your choice: 29
************************ WARNING ************************
This operation will be noisy and could
potentially compromise operational security (OPSEC).

You are running as g.white

This will scan the whole network for where your current user has local admin access.

Are you sure you want to continue? (Y/N): Y

[*] User g.white has local Admin access(OR C$ is shared to everyone) to: STEELCONWIN11-1

[*] User g.white has local Admin access(OR C$ is shared to everyone) to: LABLAB-PC1
```

For more information on how SlinkyCat works check out the blog post
https://labs.lares.com/introducing-slinkycat/

Thank You For Reading; go forth and build, break, defend, and fix!

Presented by Andy Gill & Neil Lines at Steelcon 2023