Active Directory Project

By Benjamin Enkaoua, Network & System Administrator

Index:

Virtualization

1) Vmware Network Setup

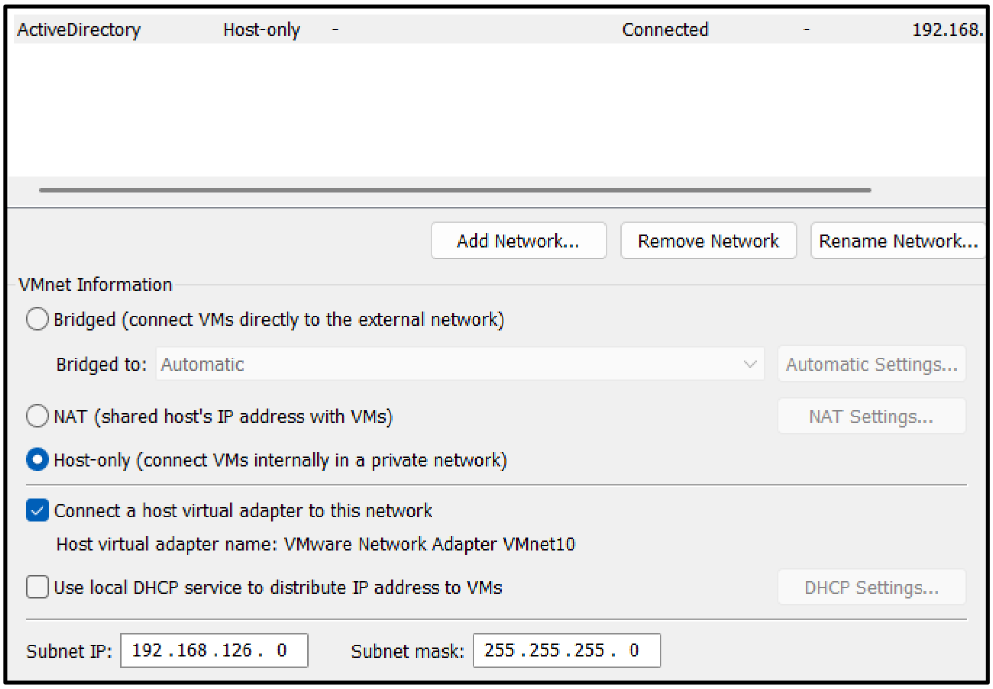
In order to set up our virtual machines, we must install Vmware and create a Virtual Network for our environment.

We can reach it in:

Edit → Virtual Network Editor

Let's choose VMnet10 and configure a Virtual Network:

- Change Virtual Network name from VMnet10 to ActiveDirectory
- Select "Host-Only"
- Change the Subnet IP to:
  - Range: 192.168.126.0
  - Netmask: 255.255.255.0 (/24)
- Uncheck the DHCP option



ActiveDirectory Host-only - Connected - 192.168.

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

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

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

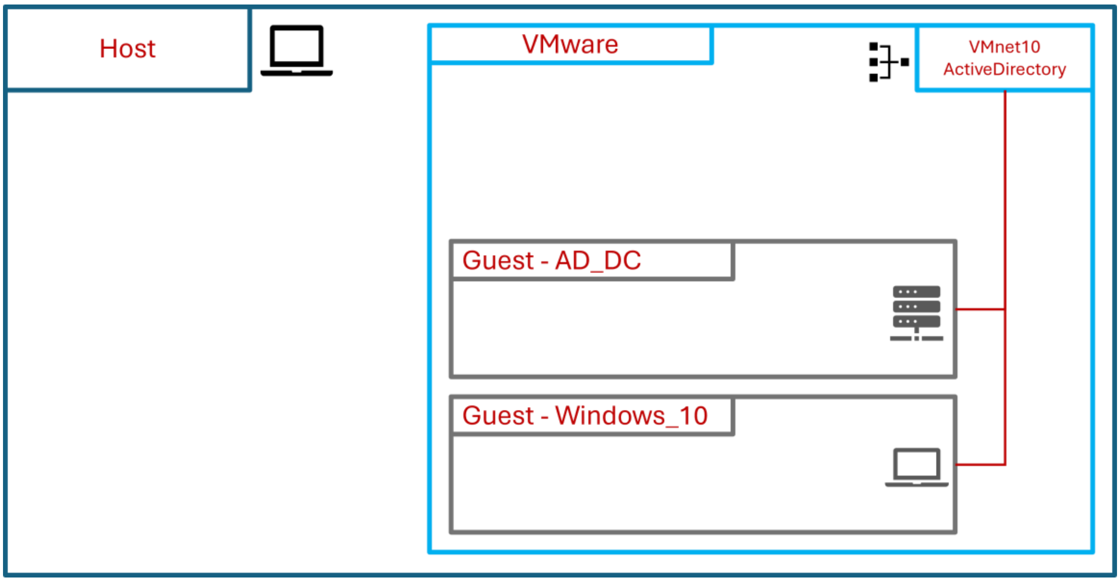
☑ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet10

□ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 .168 .126 . 0   Subnet mask: 255 .255 .255 . 0

We can schematize the network to make it clear:



2) Windows Server 2022 Installation

In order to install Windows Server 2022, we must have an ISO image.

Select:

File → New Virtual Machine → [Wizard] → Typical

From there, in "Guest Operating System Installation" select:

Installer disc image file (iso) → [Browse to the path of the ISO image]

Since we install it for educational and training purpose, we won't use a product key.

Create a username and a password.

The Operating System and its version are automatically detected.

Skip the error message related to the product key.

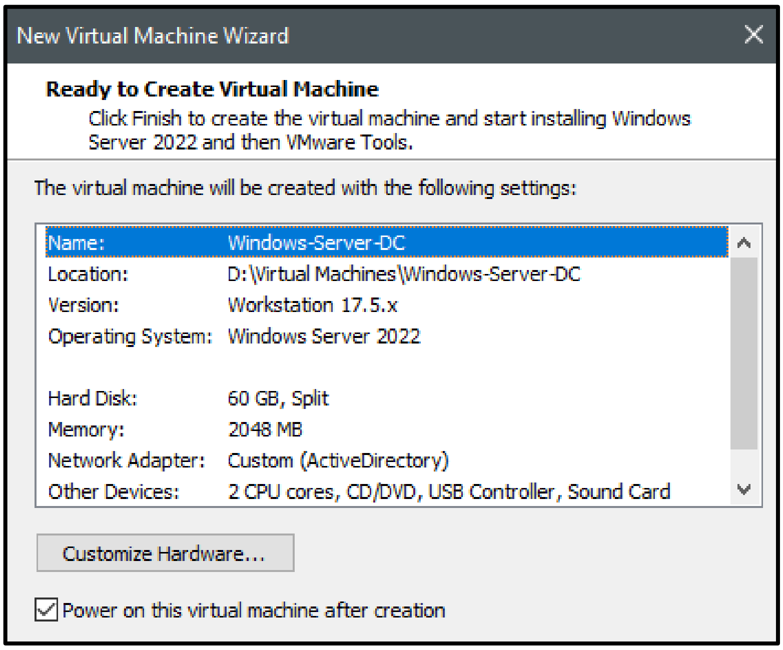
Name the machine Windows-Server-DC and choose an emplacement for the machine. Hit Next.

Chose a size in the Disk for the machine (I use 60GB), and choose “Split VD into multiple files”. Hit Next.

On the Hardware Details, NAT is chosen by default, and we want VMnet10.

In order to change that select:

Network Adapter → Custom → ActiveDirectory



New Virtual Machine Wizard

Ready to Create Virtual Machine

Click Finish to create the virtual machine and start installing Windows Server 2022 and then VMware Tools.

The virtual machine will be created with the following settings:

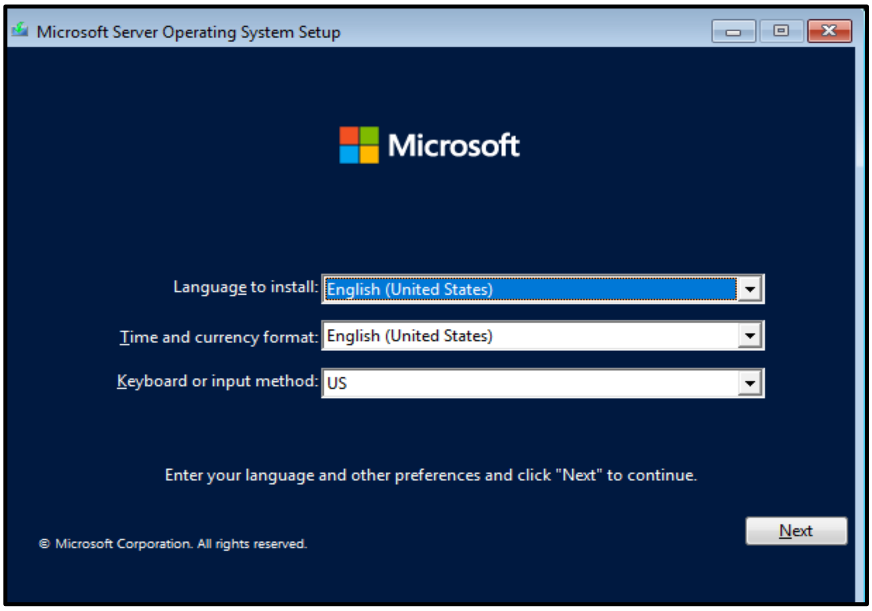
Name:	Windows-Server-DC
Location:	D:\Virtual Machines\Windows-Server-DC
Version:	Workstation 17.5.x
Operating System:	Windows Server 2022
Hard Disk:	60 GB, Split
Memory:	2048 MB
Network Adapter:	Custom (ActiveDirectory)
Other Devices:	2 CPU cores, CD/DVD, USB Controller, Sound Card

☑ Power on this virtual machine after creation

We’re going to click finish and shut down this virtual machine.

Let us power on the virtual machine for the first time.

Once the machine is turned on, press the install now button.



Microsoft Server Operating System Setup

Language to install: English (United States)

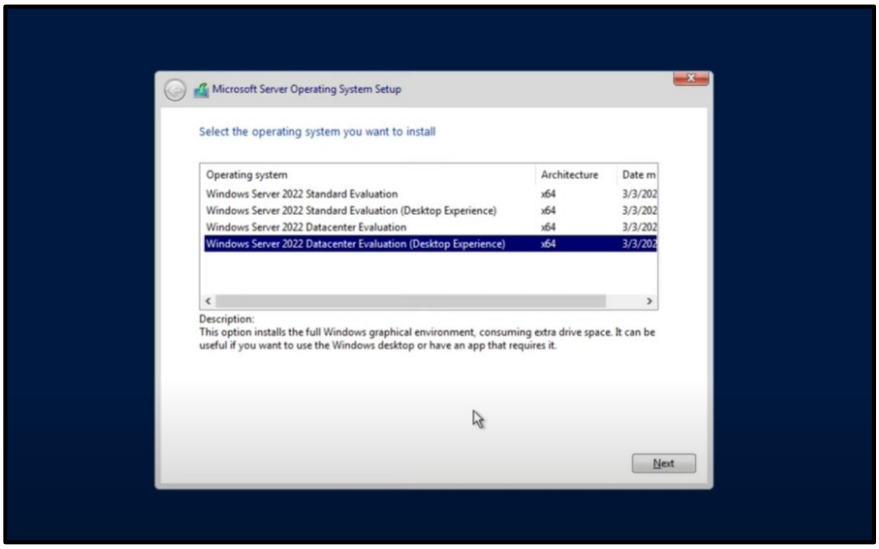
Time and currency format: English (United States)

Keyboard or input method: US

Enter your language and other preferences and click "Next" to continue.

© Microsoft Corporation. All rights reserved.

Choose the Language, Time and keyboard format and press Next.



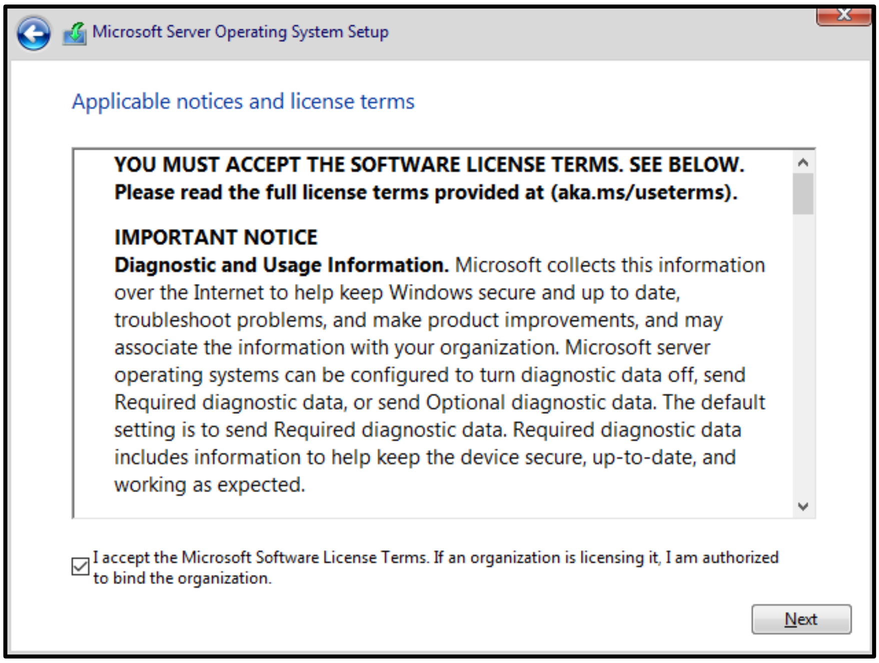
Microsoft Server Operating System Setup

Select the operating system you want to install

Operating system	Architecture	Date m
Windows Server 2022 Standard Evaluation	x64	3/3/202
Windows Server 2022 Standard Evaluation (Desktop Experience)	x64	3/3/202
Windows Server 2022 Datacenter Evaluation	x64	3/3/202
Windows Server 2022 Datacenter Evaluation (Desktop Experience)	x64	3/3/202

Description:
This option installs the full Windows graphical environment, consuming extra drive space. It can be useful if you want to use the Windows desktop or have an app that requires it.

We need to choose the Desktop experience because we want the actual desktop GUI, and not a Windows Server CLI. Press Next.



Applicable notices and license terms

YOU MUST ACCEPT THE SOFTWARE LICENSE TERMS. SEE BELOW. Please read the full license terms provided at (aka.ms/useterms).

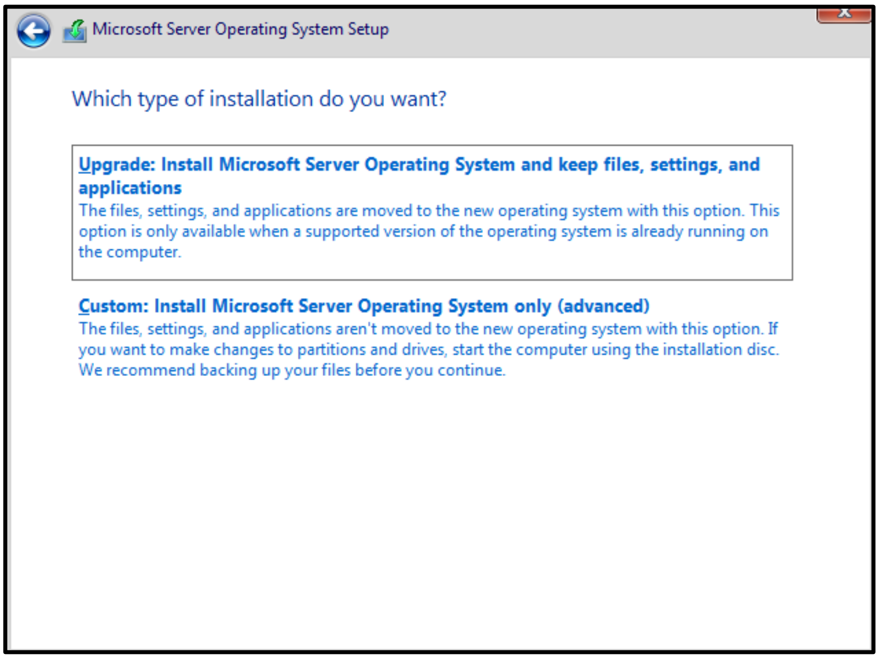
IMPORTANT NOTICE

Diagnostic and Usage Information. Microsoft collects this information over the Internet to help keep Windows secure and up to date, troubleshoot problems, and make product improvements, and may associate the information with your organization. Microsoft server operating systems can be configured to turn diagnostic data off, send Required diagnostic data, or send Optional diagnostic data. The default setting is to send Required diagnostic data. Required diagnostic data includes information to help keep the device secure, up-to-date, and working as expected.

☑ I accept the Microsoft Software License Terms. If an organization is licensing it, I am authorized to bind the organization.

Accept the license and press Next

The next step purpose is to indicate if we want to upgrade an actual existing server (Upgrade). Since we have an empty disk, we want to choose Install.

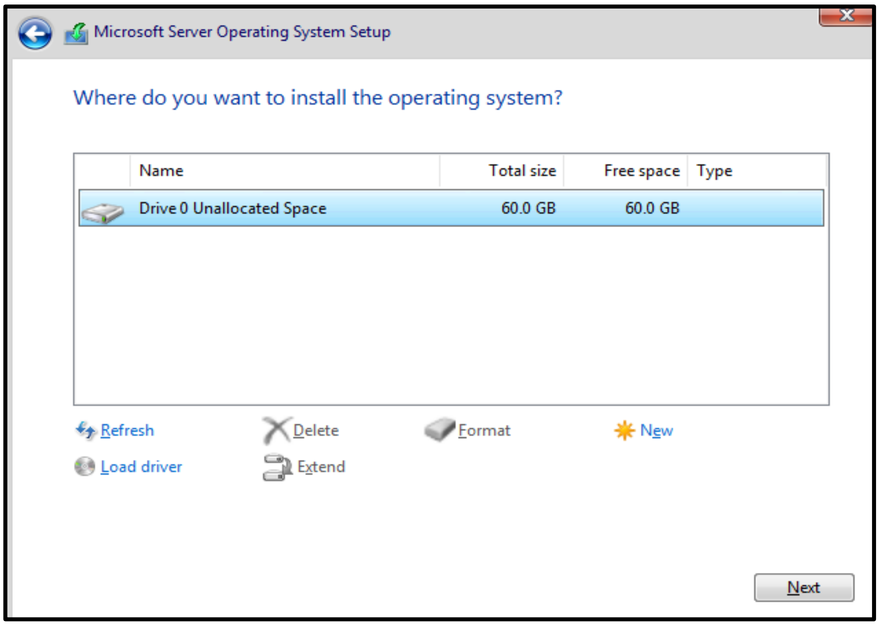


Which type of installation do you want?

Upgrade: Install Microsoft Server Operating System and keep files, settings, and applications
The files, settings, and applications are moved to the new operating system with this option. This option is only available when a supported version of the operating system is already running on the computer.

Custom: Install Microsoft Server Operating System only (advanced)
The files, settings, and applications aren't moved to the new operating system with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.

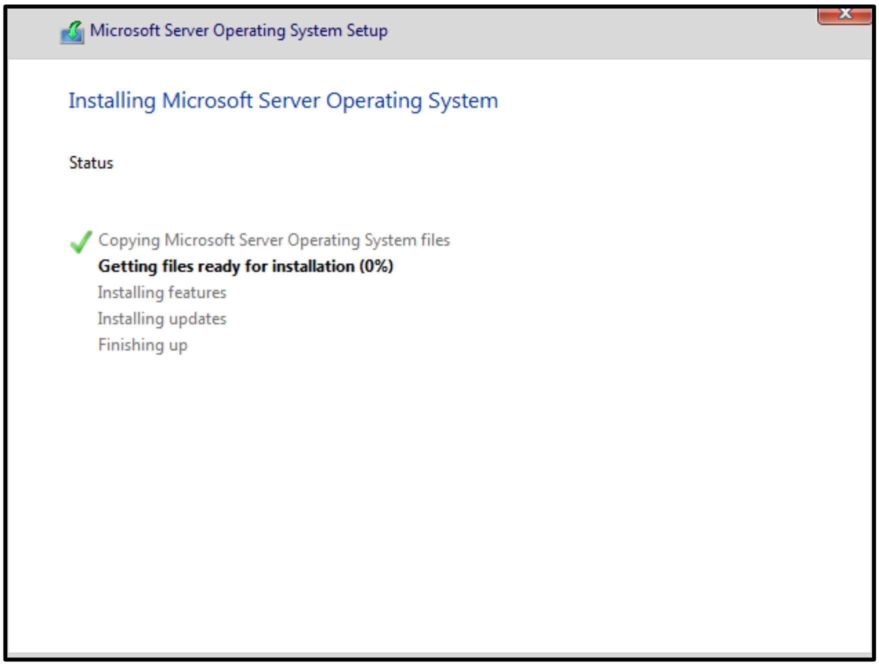
The free disk partition is detected (We allocated 60GB).



Where do you want to install the operating system?

Name	Total size	Free space	Type
Drive 0 Unallocated Space	60.0 GB	60.0 GB	

Click Next.



Installing Microsoft Server Operating System

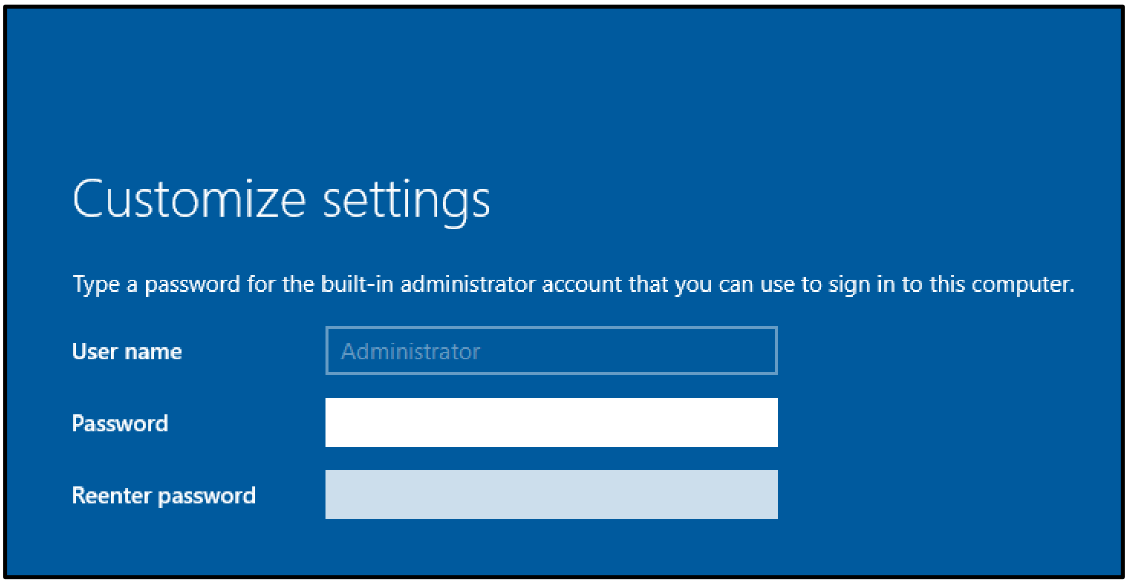
Status

✓ Copying Microsoft Server Operating System files
Getting files ready for installation (0%)
Installing features
Installing updates
Finishing up

We’ll let this run thought the installation process.

Now we have to choose a password for our Administrator user.

It is a very important step, since the password of the actual Administrator will be the password of our future Active Directory Domain Administrator.



Customize settings

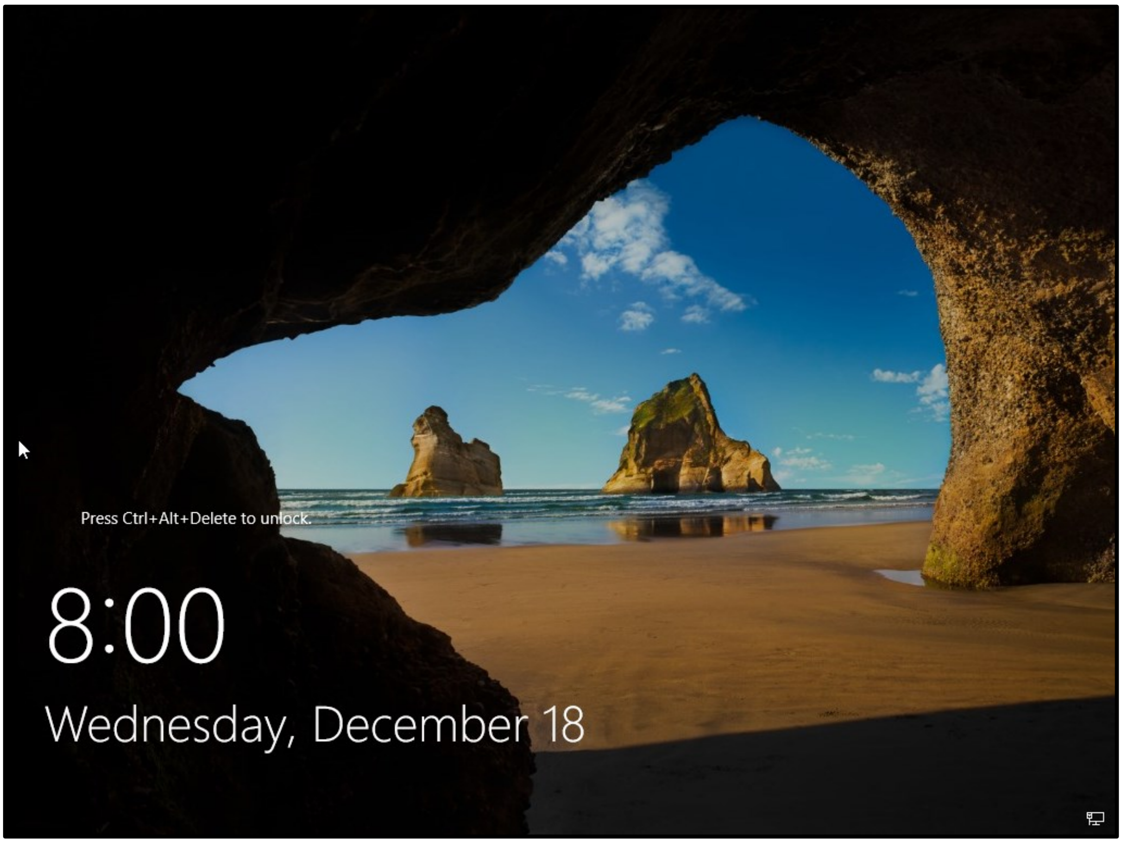
Type a password for the built-in administrator account that you can use to sign in to this computer.

User name: Administrator

Password:

Reenter password:

The next screen is the final one, and Congrats we installed our Windows Server.



Press Ctrl+Alt+Delete to unlock.

8:00

Wednesday, December 18

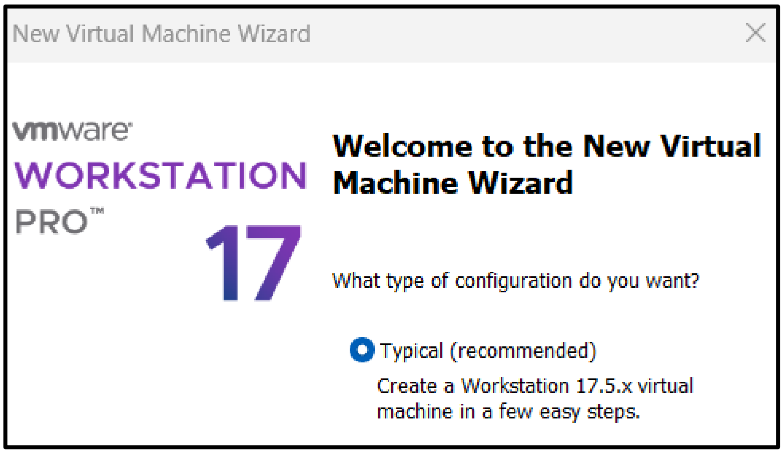
3) Windows 10 Installation

The first step is to install the ISO image from the following link

https://www.microsoft.com/en-us/software-download/windows10

Install the virtual machine in Vmware:

File → New Virtual machine → Next



New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

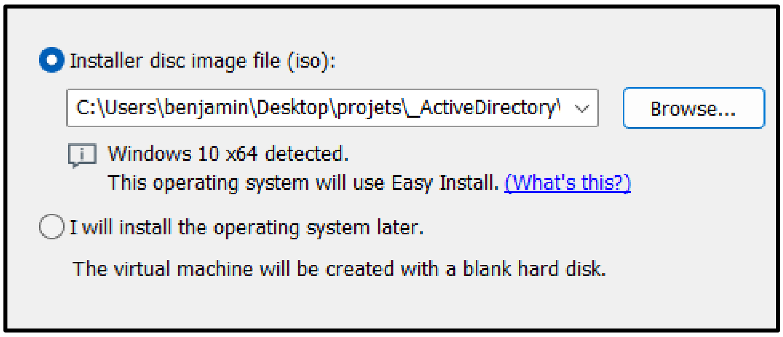
What type of configuration do you want?

● Typical (recommended)

Create a Workstation 17.5.x virtual machine in a few easy steps.

These steps look like the mentioned steps for the previous part.

We will install the ISO image downloaded earlier:



● Installer disc image file (iso):

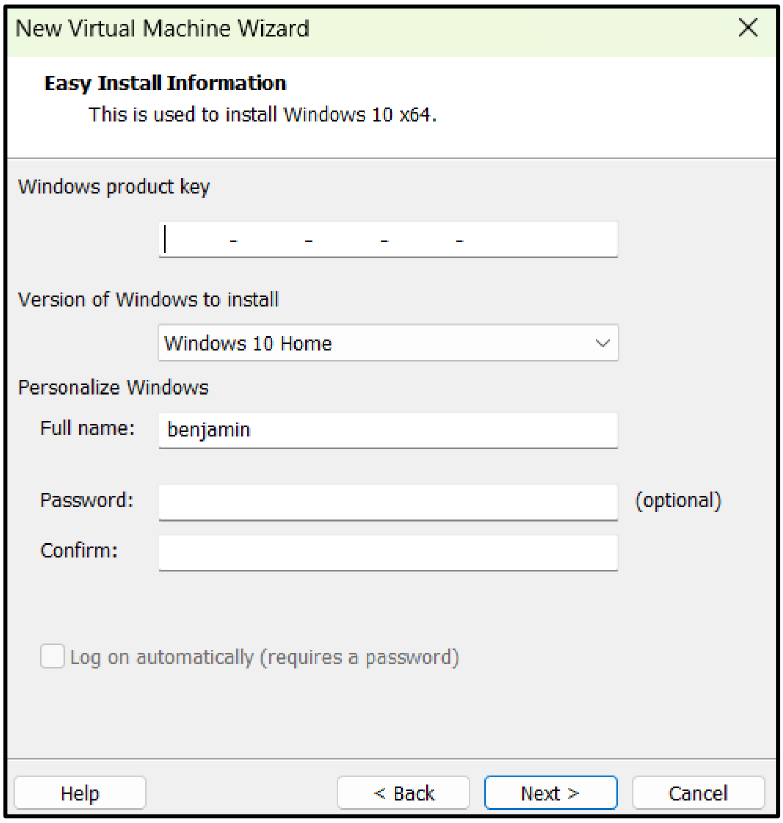
C:\Users\benjamin\Desktop\projets_ActiveDirectory\

Windows 10 x64 detected.
This operating system will use Easy Install. (What's this?)

○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Since we are using it for educational purposes, we won't use a key and use the free trial.



New Virtual Machine Wizard

Easy Install Information

This is used to install Windows 10 x64.

Windows product key: - - - -

Version of Windows to install: Windows 10 Home

Personalize Windows

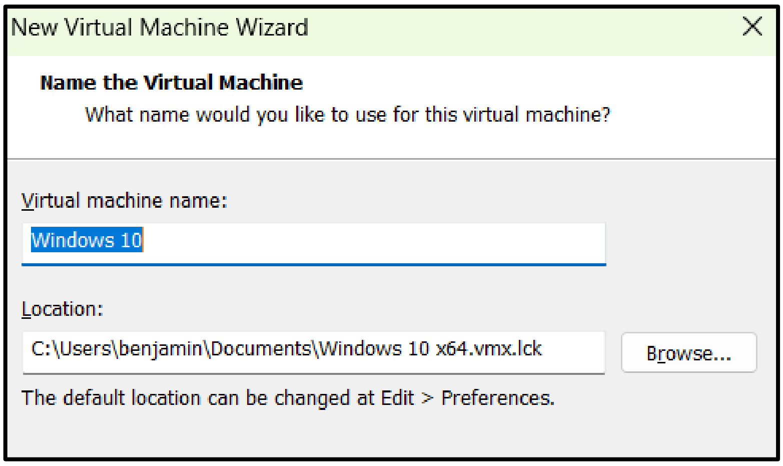
Full name: benjamin

Password: (optional)

Confirm:

□ Log on automatically (requires a password)

Choose a name for our Virtual Machine. I named it Windows10.



New Virtual Machine Wizard

Name the Virtual Machine

What name would you like to use for this virtual machine?

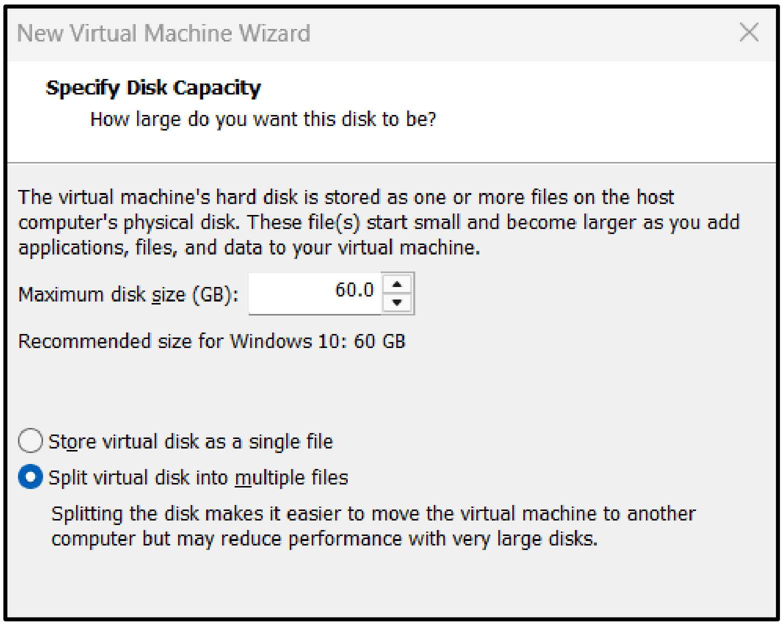
Virtual machine name: Windows 10

Location: C:\Users\benjamin\Documents\Windows 10 x64.vmx.lck

The default location can be changed at Edit > Preferences.

For this machine we will allocate 60GB as well.

Notice that it is better to split the disk into multiple files.



Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 60.0

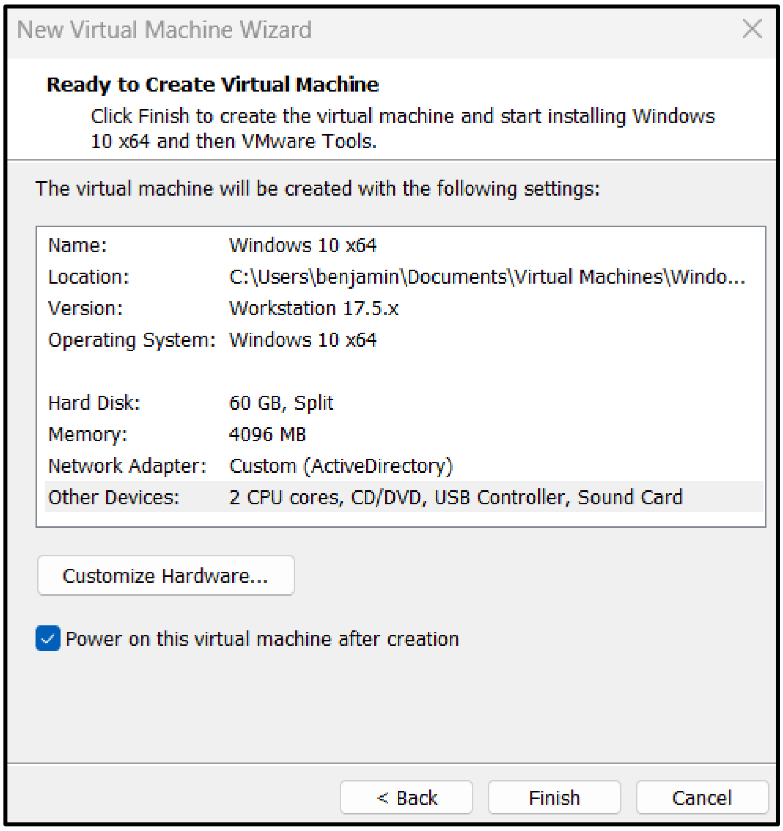
Recommended size for Windows 10: 60 GB

○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

We settled our machine to have 4GB of RAM and joined it to our VMnet10, ActiveDirectory.



Ready to Create Virtual Machine

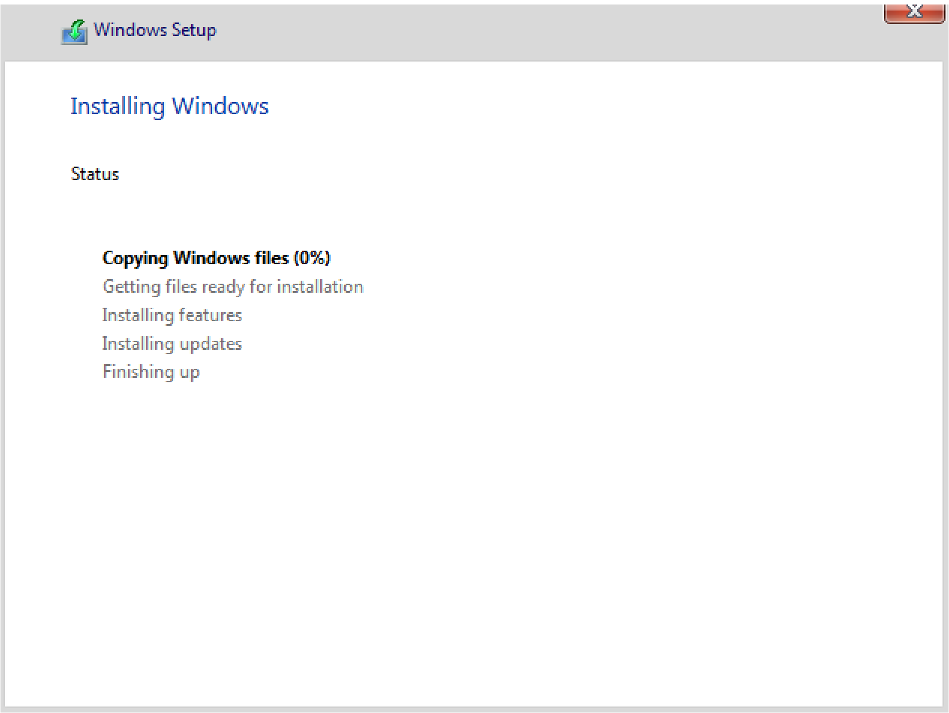
Click Finish to create the virtual machine and start installing Windows 10 x64 and then VMware Tools.

The virtual machine will be created with the following settings:

Name:	Windows 10 x64
Location:	C:\Users\benjamin\Documents\Virtual Machines\Windo...
Version:	Workstation 17.5.x
Operating System:	Windows 10 x64
Hard Disk:	60 GB, Split
Memory:	4096 MB
Network Adapter:	Custom (ActiveDirectory)
Other Devices:	2 CPU cores, CD/DVD, USB Controller, Sound Card

☑ Power on this virtual machine after creation

And let’s begin the installation.



Windows Setup

Installing Windows

Status

Copying Windows files (0%)
Getting files ready for installation
Installing features
Installing updates
Finishing up

The new VM is installed and now we can start configuring the network setting.

Windows Server Setup

1) Network Configuration

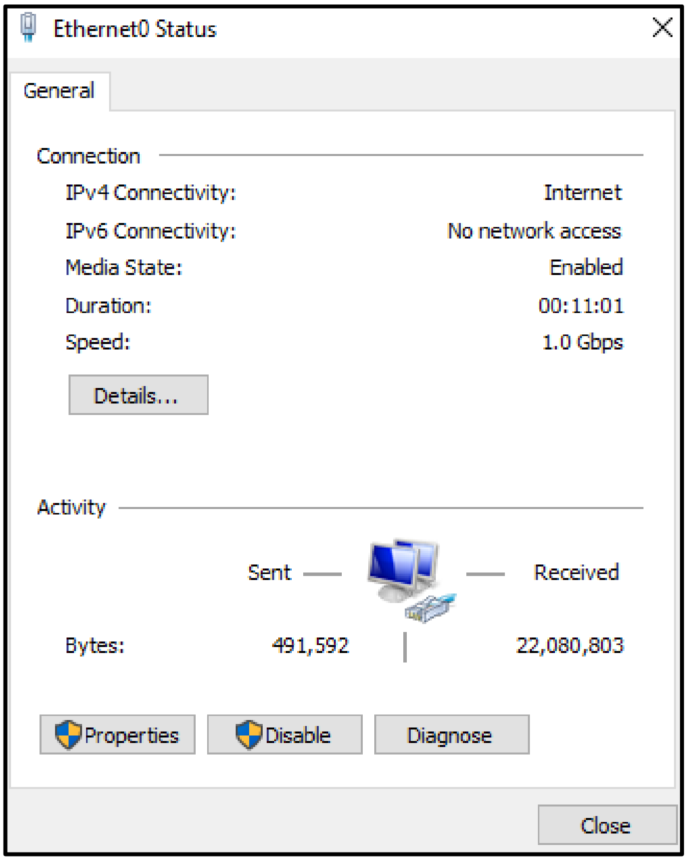
Our Windows Server machine is going to be an Active Directory Domain Controller later.

But a domain controller is also a DNS server.

When a machine is promoted to a DNS server, it’s IP is a reference for domain resolutions. For this reason, we must make sure that our IP is manually configured and not generated by a DHCP server.

Indeed, if the IP of a Domain Controller is distributed by a DHCP server, a bad configuration could lead to an IP regeneration and the joined machine will struggle to find the Logon Server and the DNS server.

WinKey + R → ncpa.cpl → Ethernet0 → Properties



Ethernet0 Status

General

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No network access

Media State: Enabled

Duration: 00:11:01

Speed: 1.0 Gbps

Activity

Sent — Received

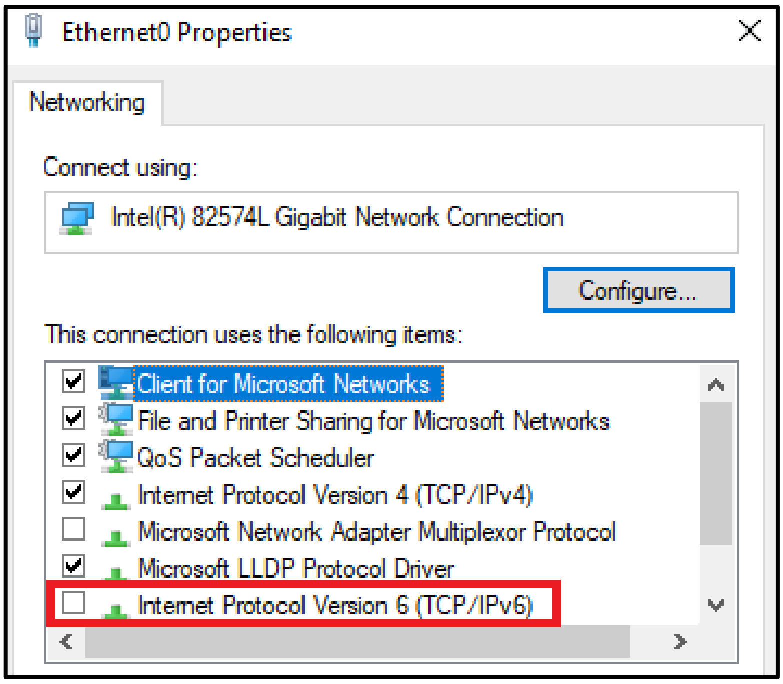
Bytes: 491,592 | 22,080,803

This interface is very important as it can help us to configure the network settings for our Windows Server machine.

Notice that many vulnerabilities related to IPv6 exist, especially MITM6 or CVE-2024-38063.

For that reason, we will uncheck it since we won't use IPv6 in our domain.

Notice also that for security purposes, limiting unnecessary features and restricting authorizations can help avoid many exploitations.



Ethernet0 Properties

Networking

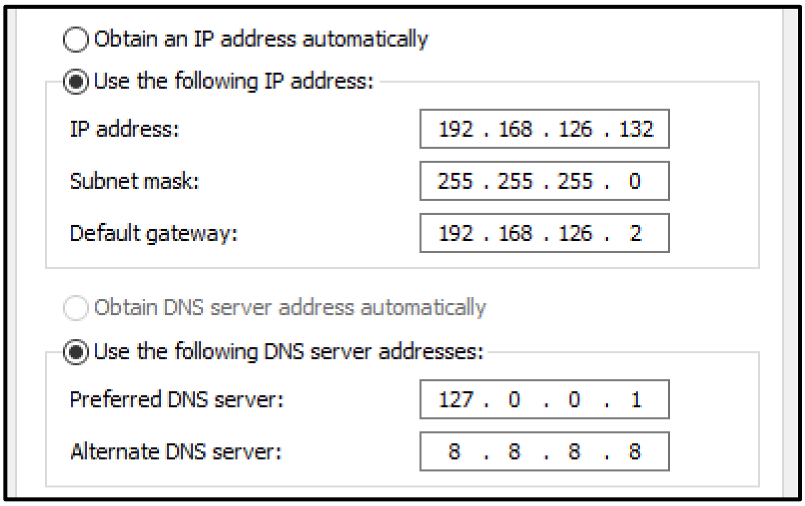
Connect using:

Intel(R) 82574L Gigabit Network Connection

This connection uses the following items:

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

Next, let us set a static IP for our Windows Server machine.



○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 126 . 132
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 126 . 2

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	127 . 0 . 0 . 1
Alternate DNS server:	8 . 8 . 8 . 8

Additionally, we added the preferred DNS server address to 127.0.0.1, since the server itself is running the service.

The alternate DNS server 8.8.8.8 is the google DNS address.

Active Directory Setup

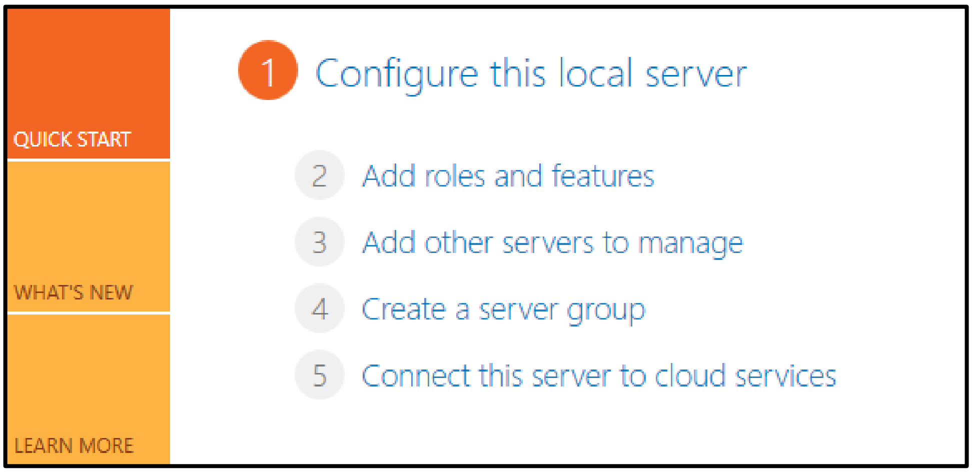
1) Basic Checks

We mentioned it before, but please check again the following:

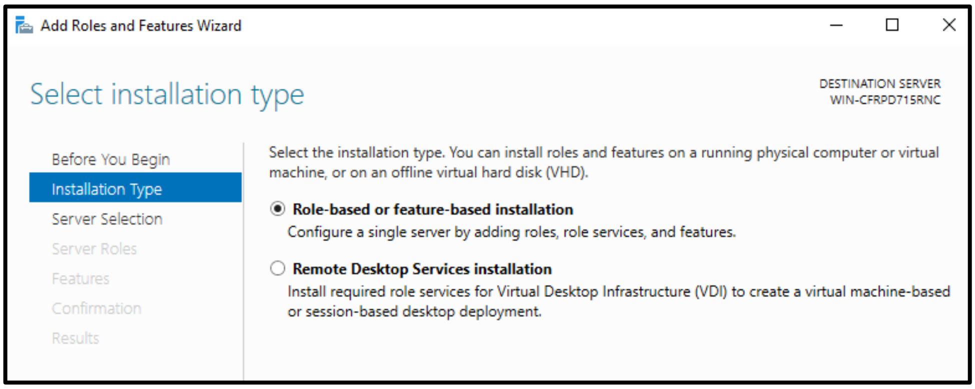
- Check the DC IPv4 address to be manually configured
- Check the Preferred DNS server to be 127.0.0.1 and the second is 8.8.8.8
- In virtualized environment, make sure that the VMs are in the same network

2) Domain Roles & Feature Installation

Select Add roles and Features


QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services

Now, the wizard will propose an installation type. Install a local server.



Select installation type

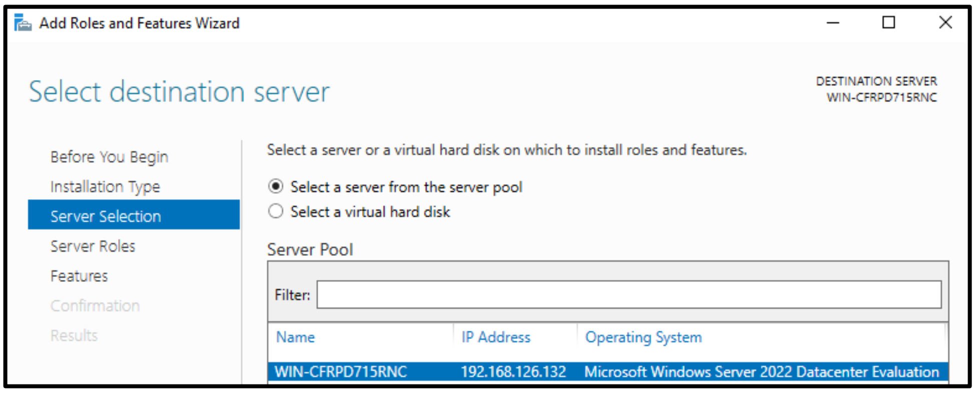
DESTINATION SERVER
WIN-CFRPD715RNC

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

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

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

We want to install it on the current server.



Select destination server

DESTINATION SERVER
WIN-CFRPD715RNC

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

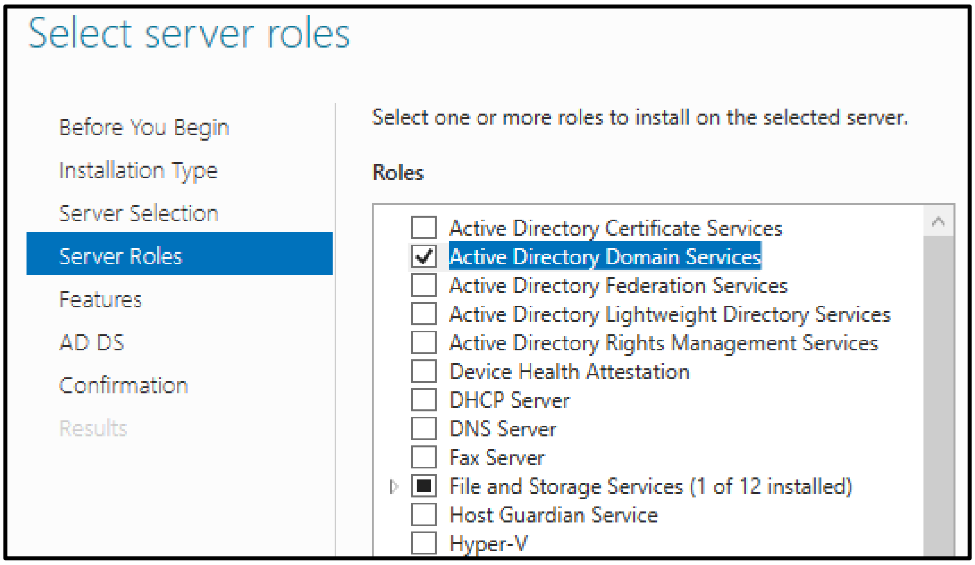
● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
WIN-CFRPD715RNC	192.168.126.132	Microsoft Windows Server 2022 Datacenter Evaluation

Now come the interesting part. Select Active Directory Domain Services.



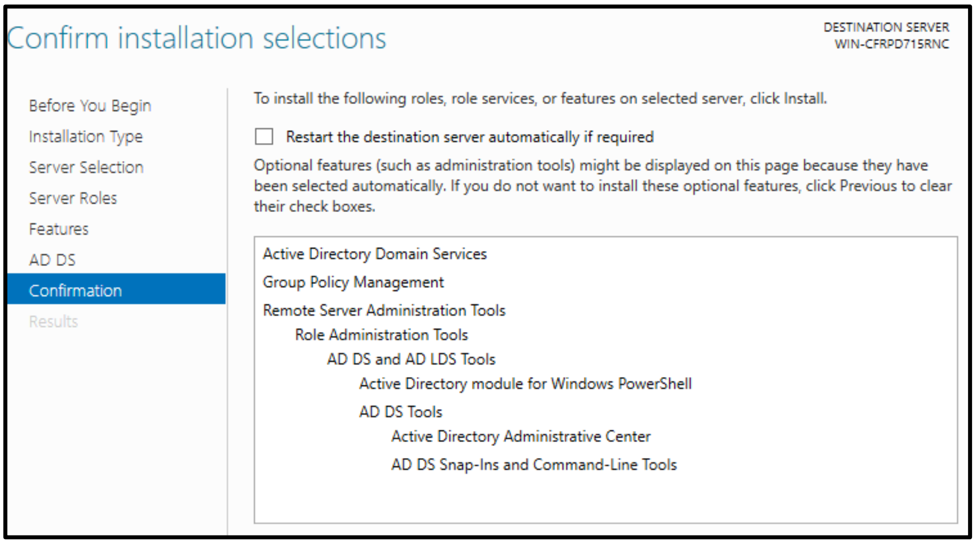
Select server roles

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

Roles

□ Active Directory Certificate Services
☑ Active Directory Domain Services
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Device Health Attestation
□ DHCP Server
□ DNS Server
□ Fax Server
■ File and Storage Services (1 of 12 installed)
□ Host Guardian Service
□ Hyper-V

We can confirm it.



Confirm installation selections

DESTINATION SERVER
WIN-CFRPD715RNC

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

□ Restart the destination server automatically if required

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

Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
    Role Administration Tools
        AD DS and AD LDS Tools
            Active Directory module for Windows PowerShell
            AD DS Tools
                Active Directory Administrative Center
                AD DS Snap-Ins and Command-Line Tools

Onto the next section, let’s install our domain controller and our AD Server.

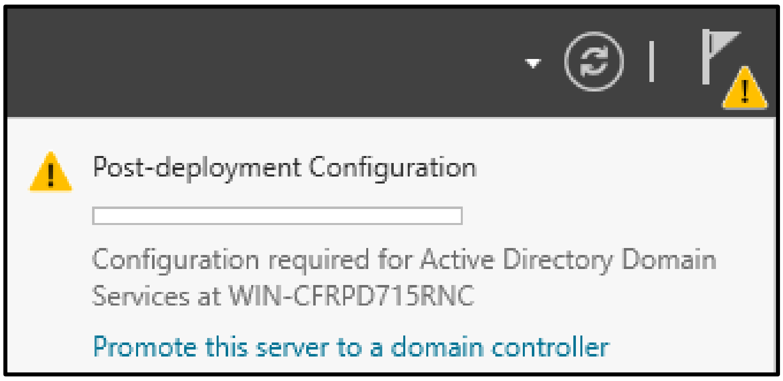
3) Domain Controller Setup

The domain controller is the main server in an Active Directory environment.

As the Domain Administrator is the user authority, the Domain Controller is the computer authority.

From our notifications, we can observe that we must configure the installed Active Directory Server.

Select Promote this server to a domain controller in the notification.

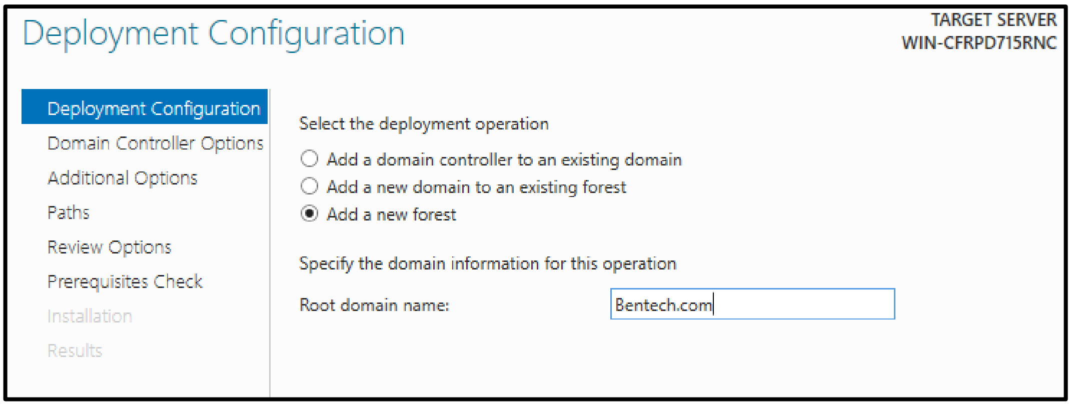


Post-deployment Configuration

Configuration required for Active Directory Domain Services at WIN-CFRPD715RNC

Promote this server to a domain controller

Select Add a new forest and choose your domain name (bentech.com)



Select the deployment operation

○ Add a domain controller to an existing domain

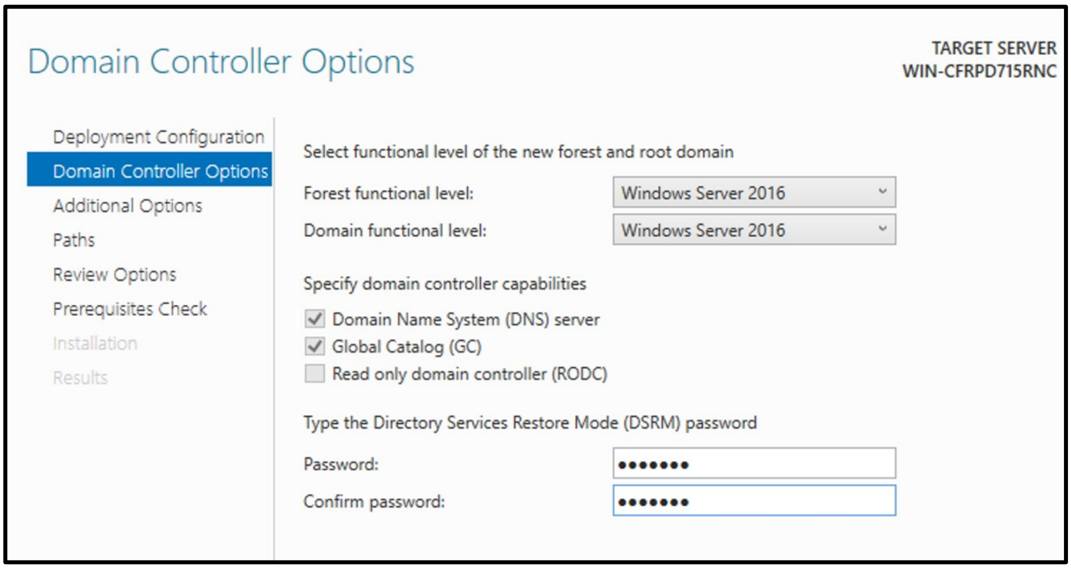
○ Add a new domain to an existing forest

● Add a new forest

Specify the domain information for this operation

Root domain name: Bentech.com

Don’t forget to add the DNS features at the following step



Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

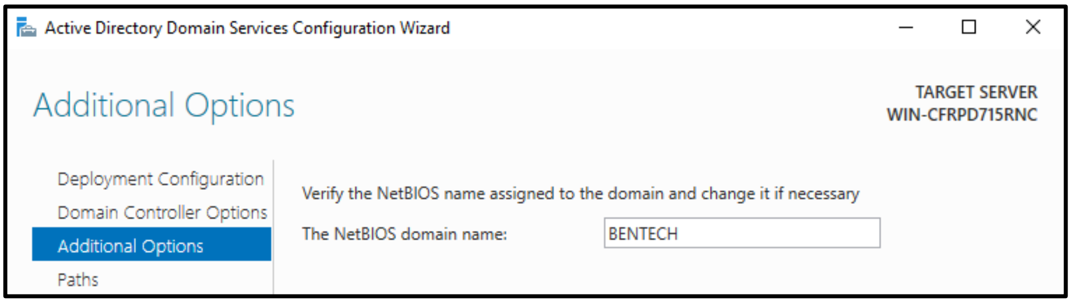
□ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: •••••••

Confirm password: •••••••

Let the NETBIOS name as generated



Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name: BENTECH

For the PATHS part, don't touch anything except if you want your most important files to be stored in another location (not recommended).

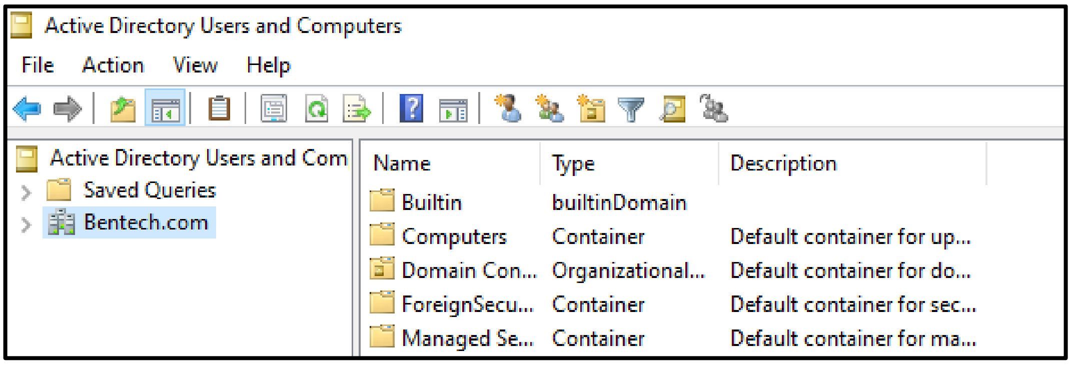
If everything is okay the prerequisite checks should indicate positive statements, press installation and the server should restart automatically.

4) OU & Users

Go to

Tools → Users and Computers

And check that your arborescence has been created


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
Bentech.com

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...

Our domain is composed of objects:

- Organizational Units (OU's)
- Users
- Groups
- Computers
- Policies
- Etc...

In order to organize them, we can assign objects to OU's (Documentation).

To create an OU, right click the Forest name and select the following

New → Organizational Unit → Choose a name

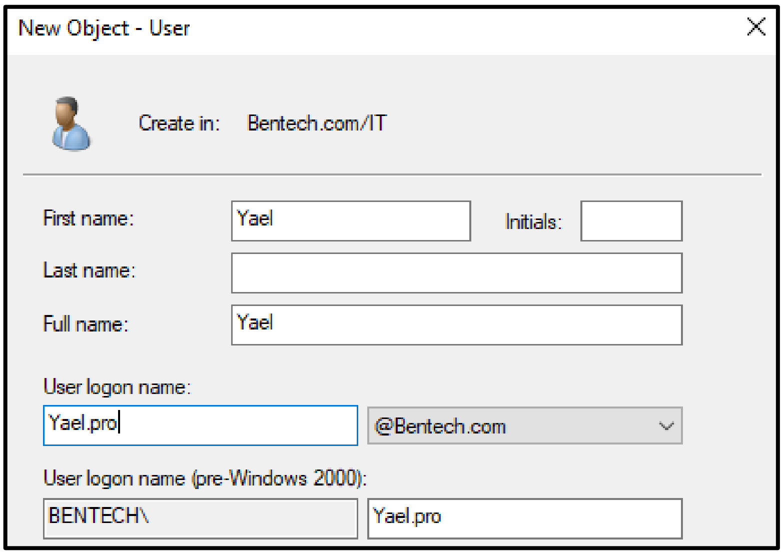
Under these OU’s, we can add objects as Users.

For management purposes, a System Administrator can locate easily a user or a computer for management using good OU indexing.

In order to create a user, right click the created OU and execute:

New → User

Configure the name and the logon name, which is the username for authentication.


New Object - User

Create in: Bentech.com/IT

First name: Yael

Initials:

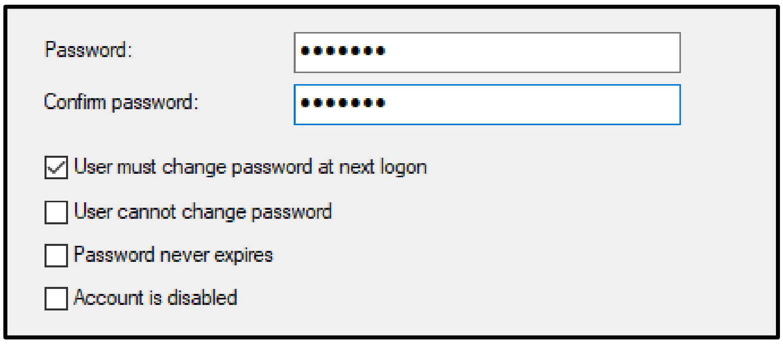
Last name:

Full name: Yael

User logon name: Yael.pro @Bentech.com

User logon name (pre-Windows 2000): BENTECH\ Yael.pro

Next, select a password and make sure the user has to change it once logged in for the first time, by selecting User must change password at next logon.


Password: •••••••

Confirm password: •••••••

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

This is a security measure.

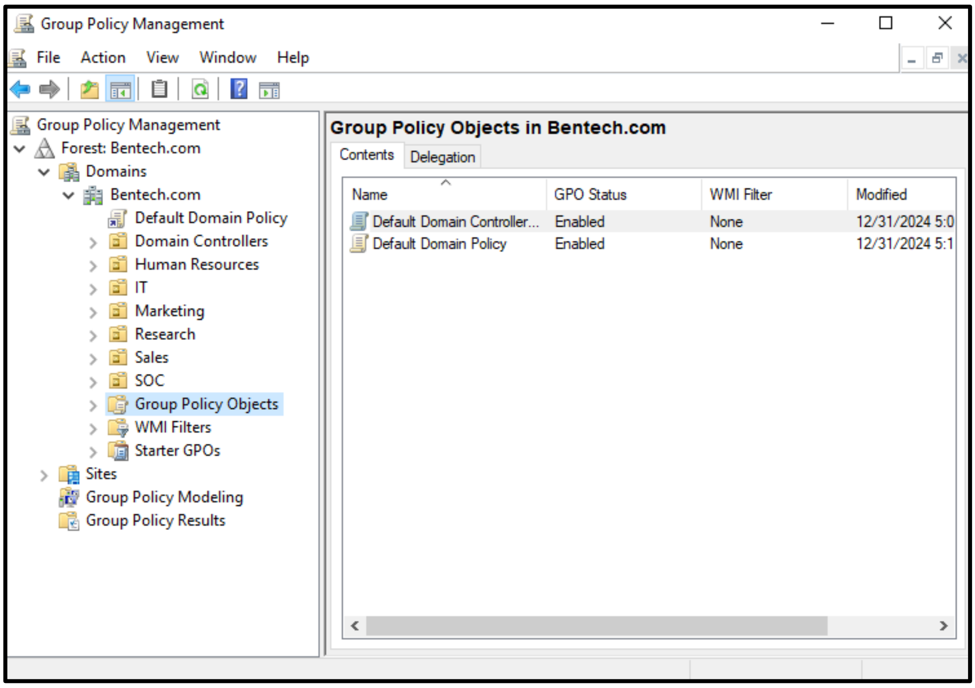
5) Users Restrictions

We will create 2 limitations for our users

- Users in the Human Resources OU have restricted access to cmd.exe
- A user in Human Resources will be restricted on working hours

For the first limitation we will be using a GPO. Select:

Tools → group Policy Management



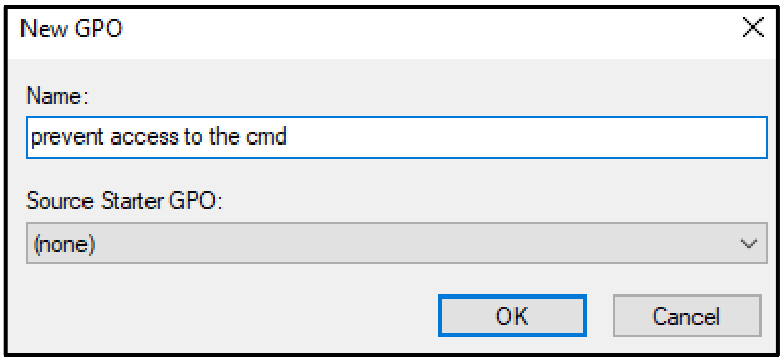
Group Policy Objects in Bentech.com

Name	GPO Status	WMI Filter	Modified
Default Domain Controller...	Enabled	None	12/31/2024 5:0
Default Domain Policy	Enabled	None	12/31/2024 5:1

Right click on the targeted OU (Human Resources) and select:

Create a GPO in this domain and link it here

We have got to create a new GPO named prevent access to the cmd.



New GPO

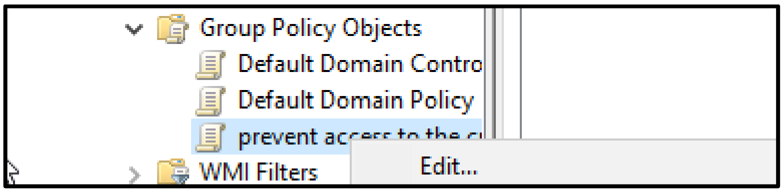
Name: prevent access to the cmd

Source Starter GPO: (none)

The GPO is now created. Now we have to edit what it will be doing.

In the same interface go now to Group Policy Objects and expand it.

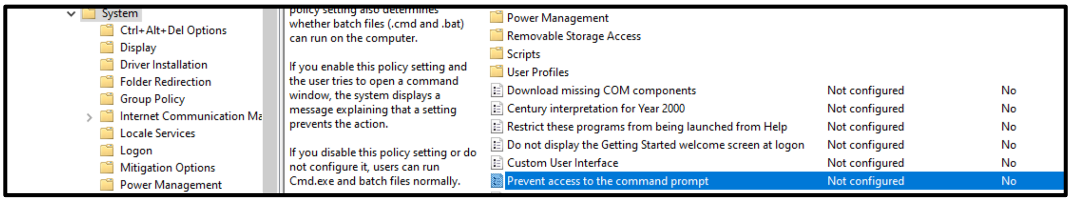
Right Click [prevent access to the cmd] → Edit...



Expand to:

User Configuration → Policies → Administrative Templates → System

From there we have to enable the installed GPO Prevent Access to the command prompt.



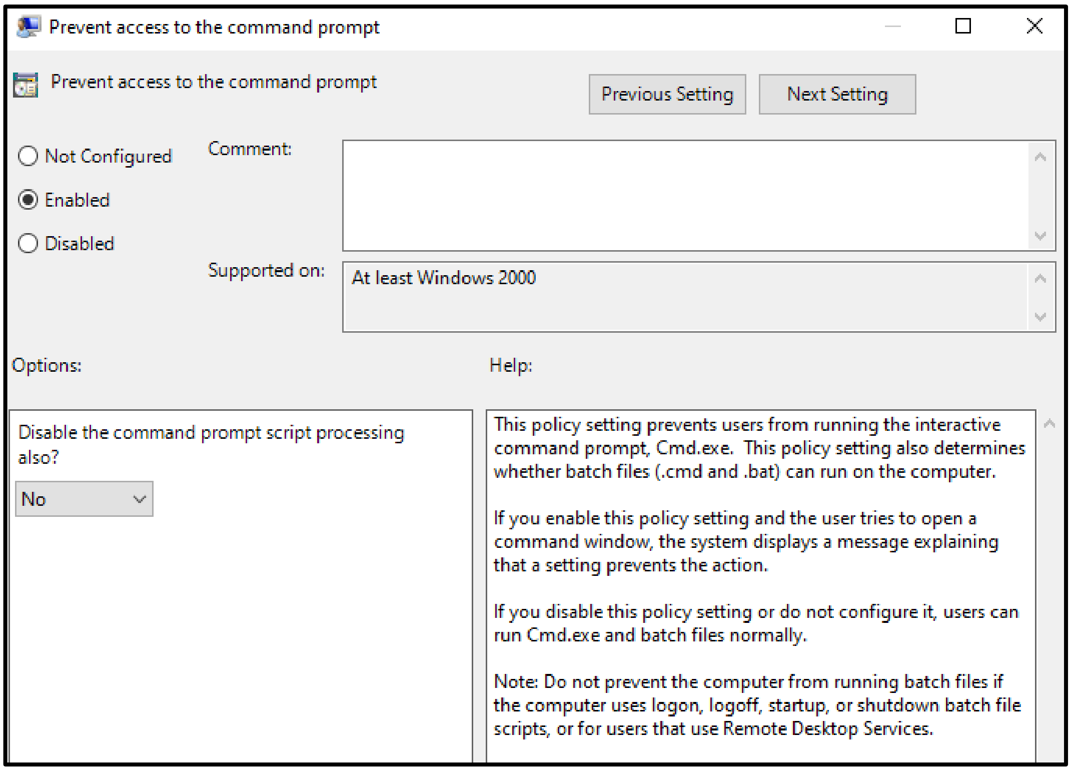
policy setting also determines whether batch files (.cmd and .bat) can run on the computer.

If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.

If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.

Power Management		
Removable Storage Access		
Scripts		
User Profiles		
Download missing COM components	Not configured	No
Century interpretation for Year 2000	Not configured	No
Restrict these programs from being launched from Help	Not configured	No
Do not display the Getting Started welcome screen at logon	Not configured	No
Custom User Interface	Not configured	No
Prevent access to the command prompt	Not configured	No

Select the GPO and enable it



Prevent access to the command prompt

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

Disable the command prompt script processing also?

No

Help:

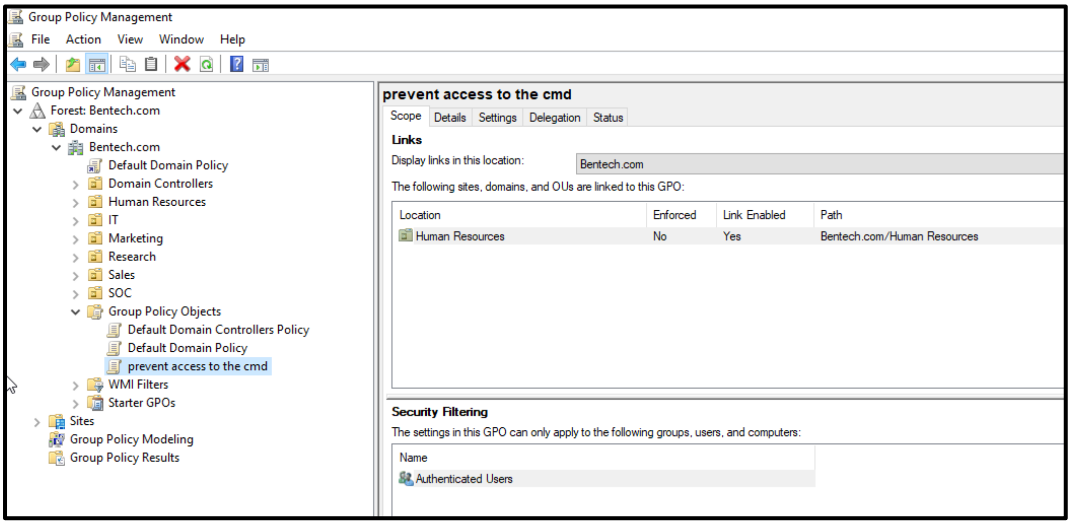
This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer.

If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.

If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.

Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.

We can check that the GPO is linked and enabled to our Human Resources OU by checking our GPO name.



prevent access to the cmd

Links

Display links in this location: Bentech.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
Human Resources	No	Yes	Bentech.com/Human Resources

Security Filtering

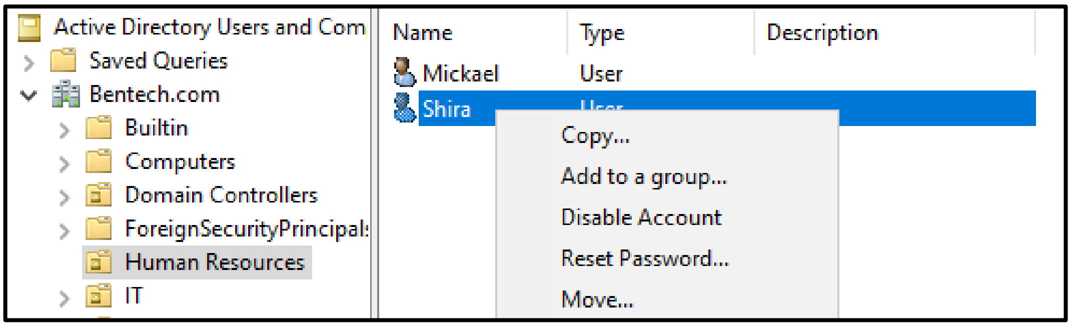
The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

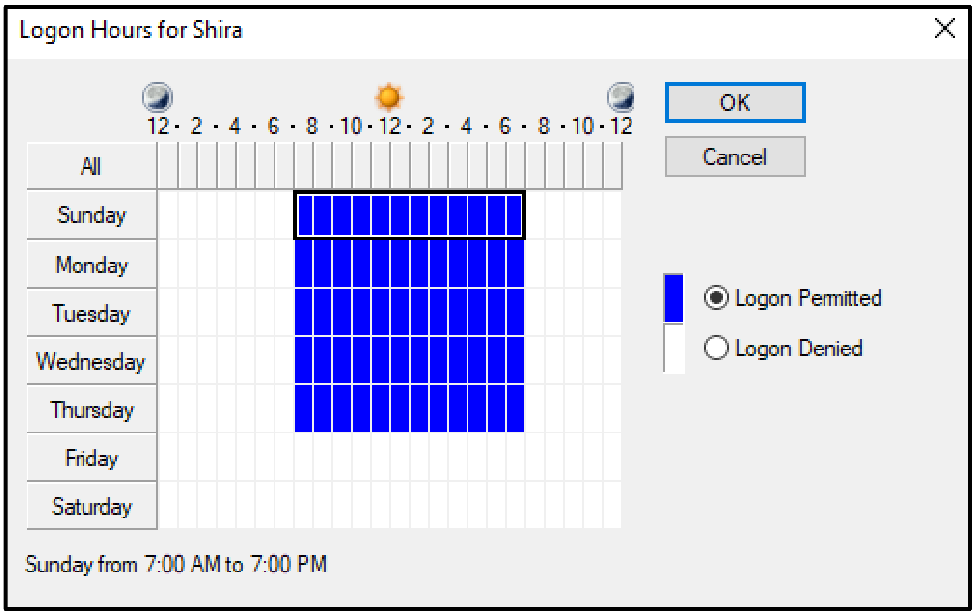
Since regular users are restricted from logging in the DC, we will check later in our Windows 10 machine joined to the domain that HR users can’t access cmd.

The second limitation is to restrict a user's logon hours.

Select the user in Users and Computers. Select the user's properties.



Go to Account → Logon Hours

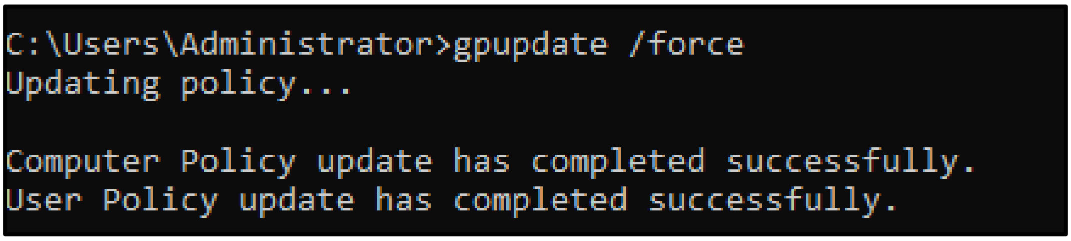


● Logon Permitted
○ Logon Denied

Sunday from 7:00 AM to 7:00 PM

We selected here a range of hours.

Now it's time to update our GPO. We will use the following command line:



```
C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

6) Computer Objects

Since computers are also parts of Active Directory, we will join a machine to our domain as an object.

Notice that it can also be part of an OU, helping the mapping of resources to different sections in an organization.

In the next chapter we will install a Windows 10 VM machine that will be joined to our domain.

Windows 10 Setup

1) Network Settings

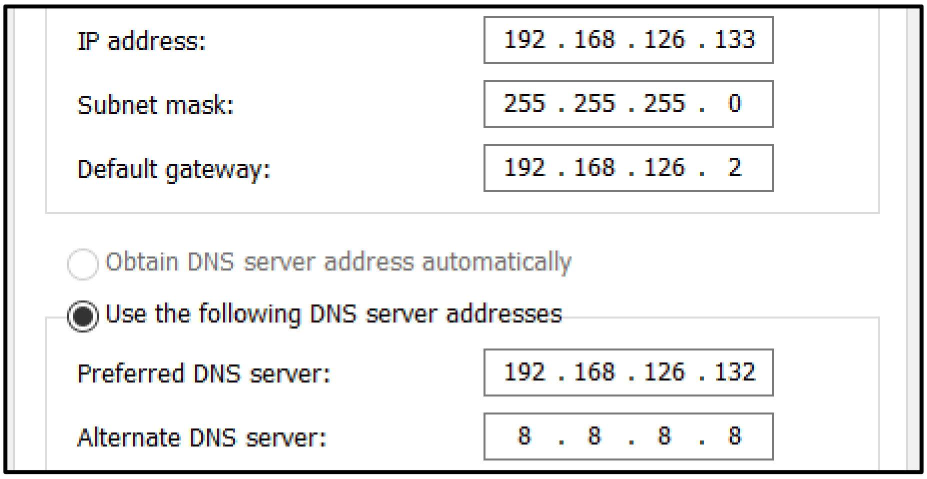
The machine is already installed.

We can get an IP from the DHCP server, or manually, it won't change anything as long as our machine is not a server.

Also, we must add the DNS of our domain controller, which is it's IP, in order to detect the DC at the domain joining part (next sub chapter).

To do so, select:

WinKey+R → ncpa.cpl → Ethernet0 → Properties → IPv4



IP address:	192 . 168 . 126 . 133
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 126 . 2

○ Obtain DNS server address automatically

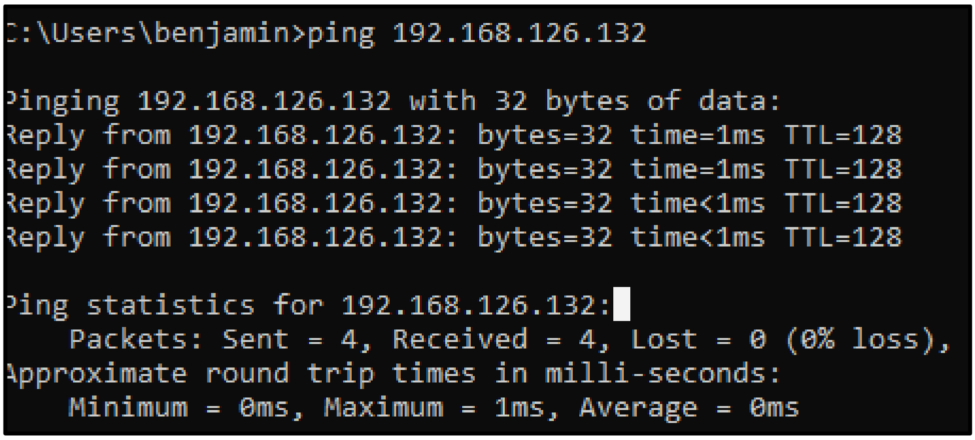
● Use the following DNS server addresses

Preferred DNS server:	192 . 168 . 126 . 132
Alternate DNS server:	8 . 8 . 8 . 8

The preferred DNS server will be the IP of the DC, and the second one will be the DNS of Google 8.8.8.8, we could choose also Cloudflare with 1.1.1.1 or 1.1.0.0 depending on your preferences.

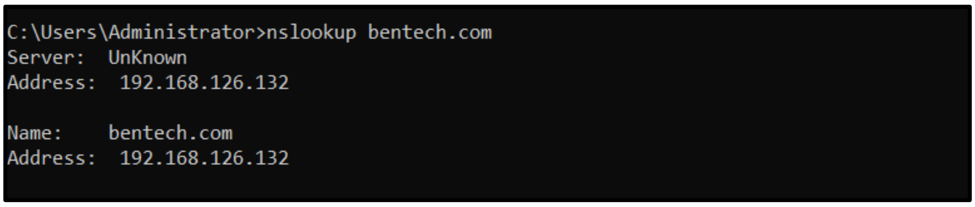
2) Connectivity Check

Let's ping the DC to make sure that both machine can communicate



```
:\Users\benjamin>ping 192.168.126.132

inging 192.168.126.132 with 32 bytes of data:
eply from 192.168.126.132: bytes=32 time=1ms TTL=128
eply from 192.168.126.132: bytes=32 time=1ms TTL=128
eply from 192.168.126.132: bytes=32 time<1ms TTL=128
eply from 192.168.126.132: bytes=32 time<1ms TTL=128

ing statistics for 192.168.126.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
pproximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Next, we must execute a nslookup command to make sure our DNS is ready to resolve bentech.com

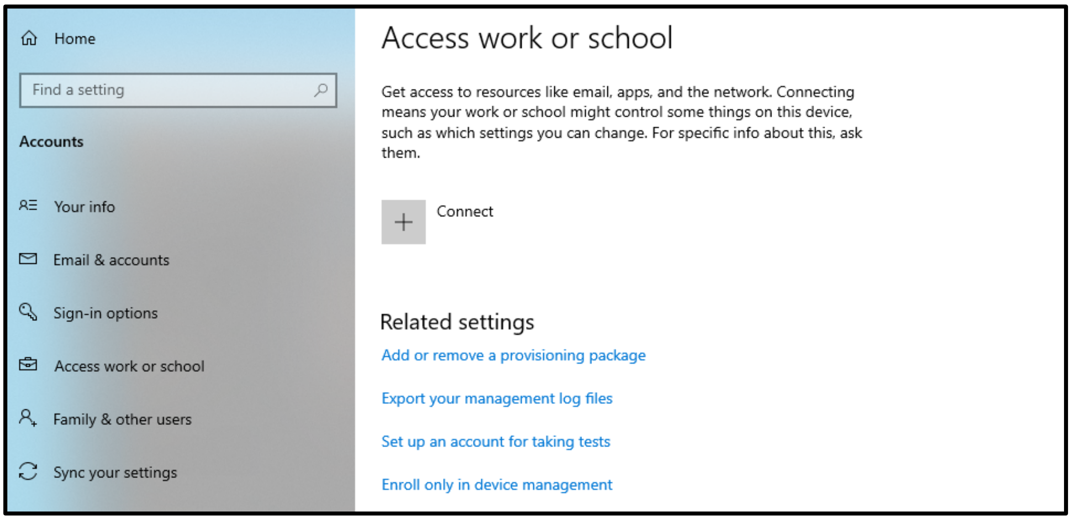


```
C:\Users\Administrator>nslookup bentech.com
Server:  UnKnown
Address:  192.168.126.132

Name:    bentech.com
Address:  192.168.126.132
```

Our machine is ready to be joined to the DC since the bentech.com domain can be resolved on a DNS request.

3) Domain Joining

In order to join our machine to the domain we must reach Access work or school.



Home
Find a setting
Accounts
Your info
Email & accounts
Sign-in options
Access work or school
Family & other users
Sync your settings

Access work or school

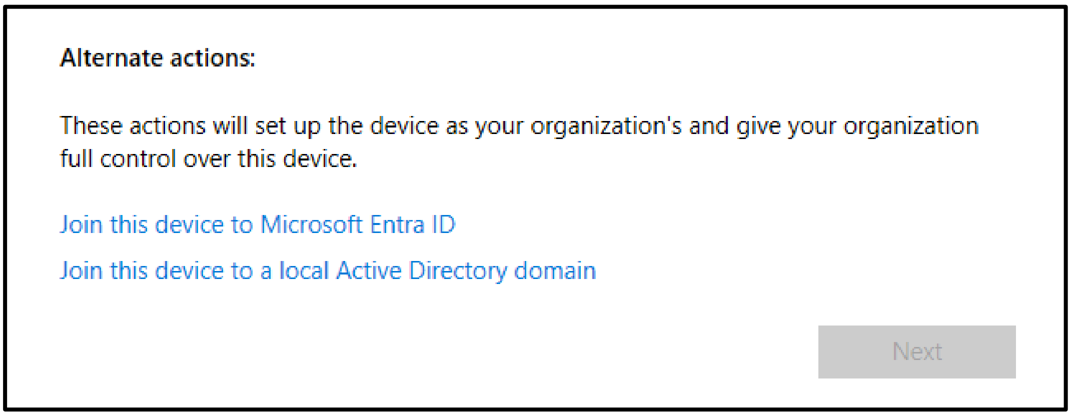
Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Related settings

Add or remove a provisioning package
Export your management log files
Set up an account for taking tests
Enroll only in device management

Select Connect

Now we want to join a local Active Directory domain (Below, in Alternate Actions).



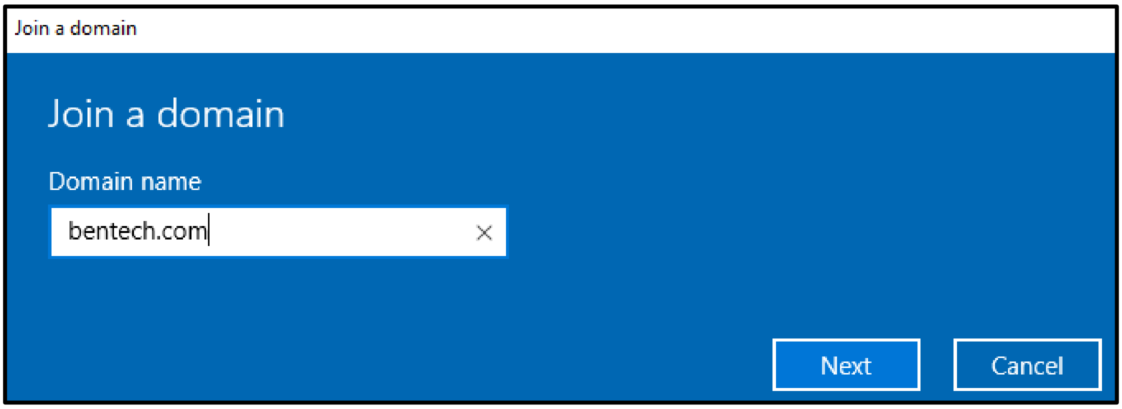
Alternate actions:

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

Join this device to Microsoft Entra ID

Join this device to a local Active Directory domain

Type the domain name (bentech.com)



Join a domain

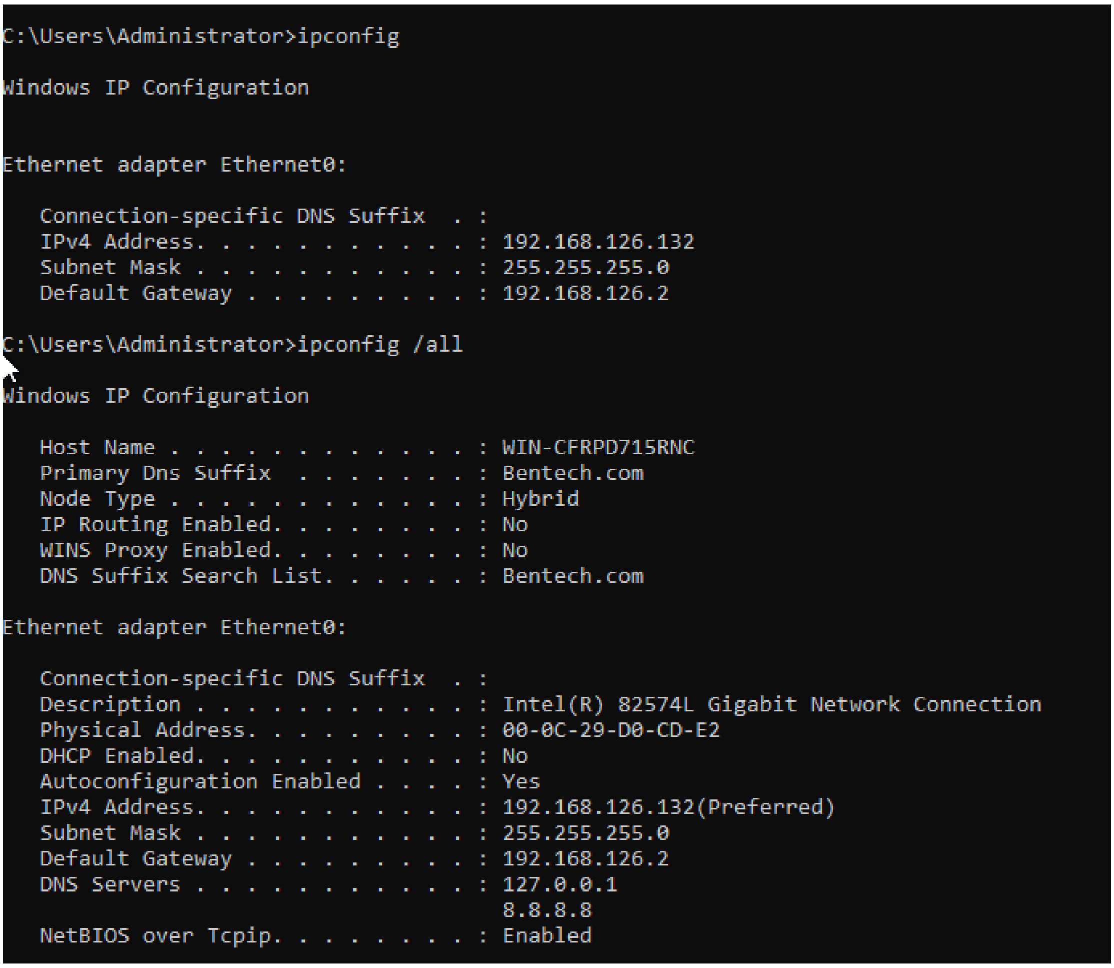
Join a domain

Domain name

bentech.com

Administrators username and password is required. Login and wait.

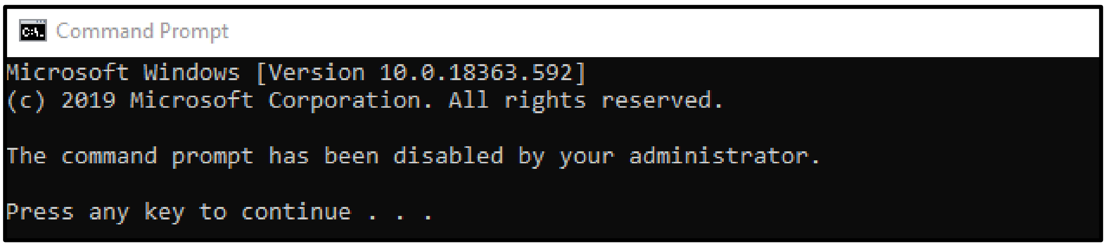
Now we can run ipconfig and make sure our machine is part of the domain.



```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.126.132
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.126.2

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : WIN-CFRPD715RNC
   Primary Dns Suffix  . . . . . . . : Bentech.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : Bentech.com

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-D0-CD-E2
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.126.132(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.126.2
   DNS Servers . . . . . . . . . . . : 127.0.0.1
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

4) Security Measures

We want to make sure our GPO is enabled and our user can connect at allowed hours. Let us open a cmd as the HR user and see what happens



```
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

The command prompt has been disabled by your administrator.

Press any key to continue . . .
```

Great. Our cmd has been disabled.

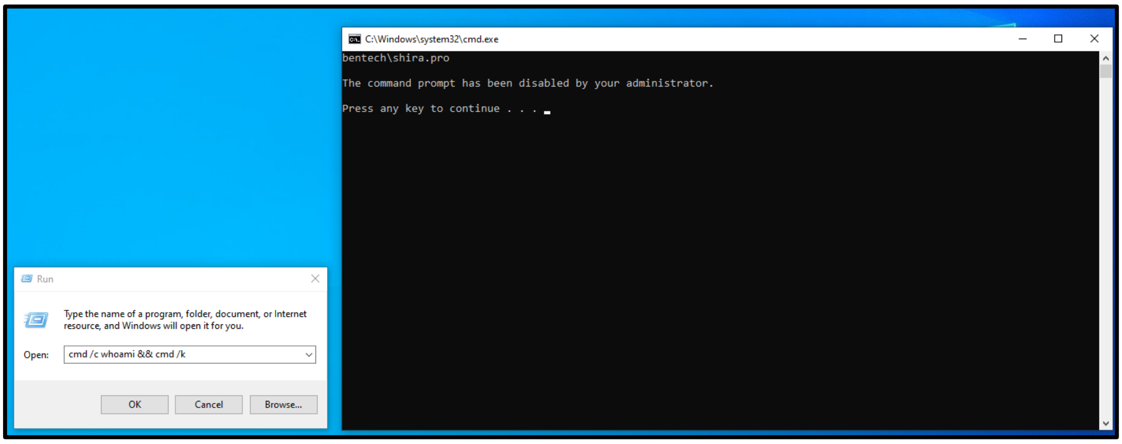
But especially in this case we should be careful with the GPO effectiveness.

Some bypasses exist to get the command to run.

Here are some examples.

The first one involve running from the following command:

WinKey+R → cmd /c whoami && cmd /k



C:\Windows\system32\cmd.exe

```
bentech\shira.pro

The command prompt has been disabled by your administrator.

Press any key to continue . . .
```

Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

Open: cmd /c whoami && cmd /k

As we can see, the command prompt is disabled but the command is still running.

The GPO cannot stop our command to run.

A recent phishing attack has been observed with a fake captcha leading users to run commands under the WinKey+R utility. Read more about it.

We can understand from there that GPO restrictions aren't enough sometimes against advanced techniques.

Conclusions

As a Network & System Administrator, I wanted to make sure that every step could be reproduced, for myself and anyone willing to setup from 0 an infrastructure, for testing or training purposes.

It was a great experience as it is my first project and footprint for my next goal, jumping into the world of Cyber Security.

Thanks to anyone who has been supporting me, especially for my mentor and brother, Ruben.