Active Directory (AD) is a core component of Microsoft's Windows Server environment that provides centralized management of users, computers, and network resources. It enables administrators to organize and control access to information, enforce security policies, and streamline network administration across an organization.

Setting up Active Directory is a crucial step in building a secure and efficient IT infrastructure. It allows organizations to manage authentication, authorization, and directory-based services through a single, unified system. Whether you're deploying it in a small business or a large enterprise, understanding the setup process ensures a stable and scalable environment.

This guide provides a **step-by-step walkthrough** for installing, configuring, and verifying Active Directory Domain Services (AD DS) on a Windows Server. By following these steps, you will learn how to:

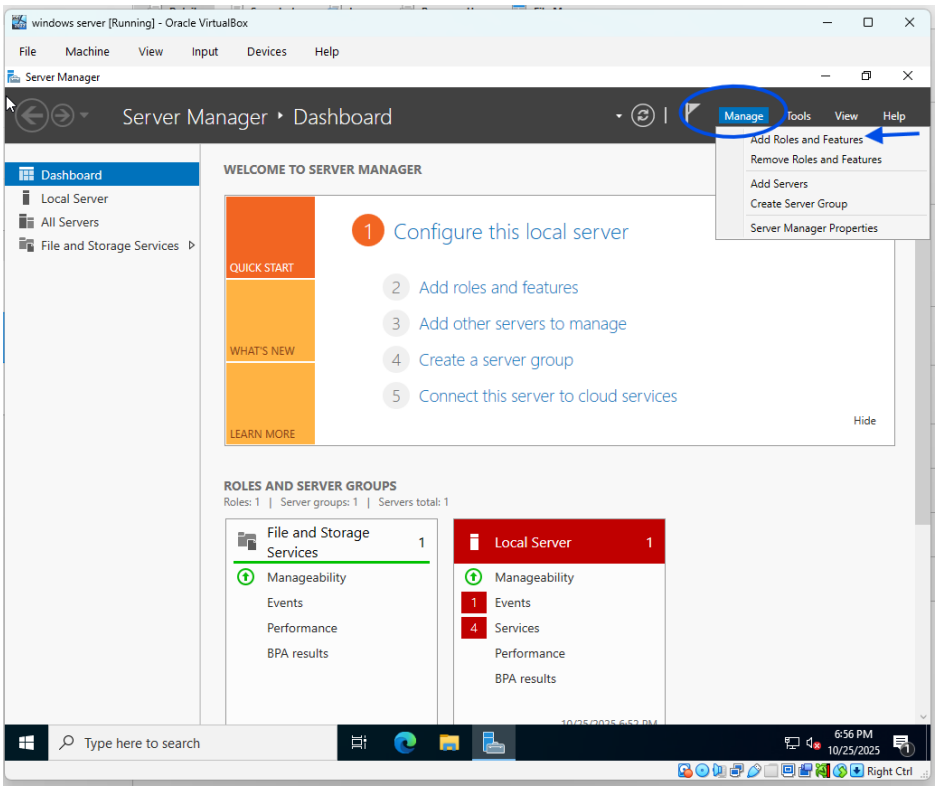
- Prepare your server environment for AD installation
- Install the Active Directory Domain Services role
- Promote the server to a domain controller
- Configure DNS and domain settings
- Verify and manage your new domain

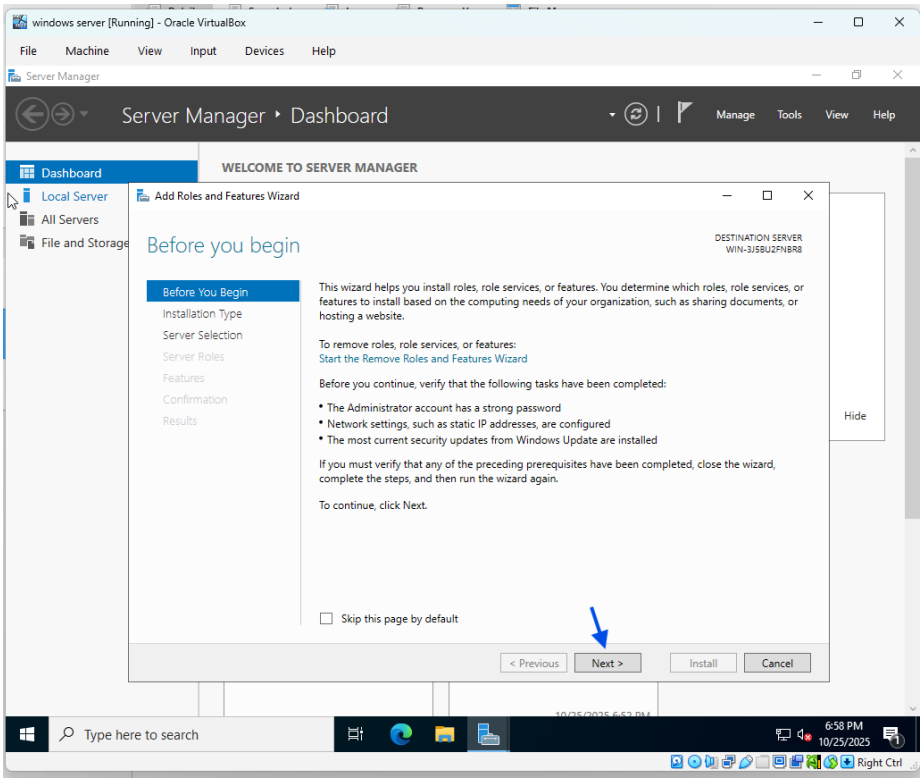
By the end of this guide, you will have a fully functional Active Directory domain ready to manage users, groups, and network resources within your organization.

On the server, we first need to install the AD, this can be done on the server manager dashboard

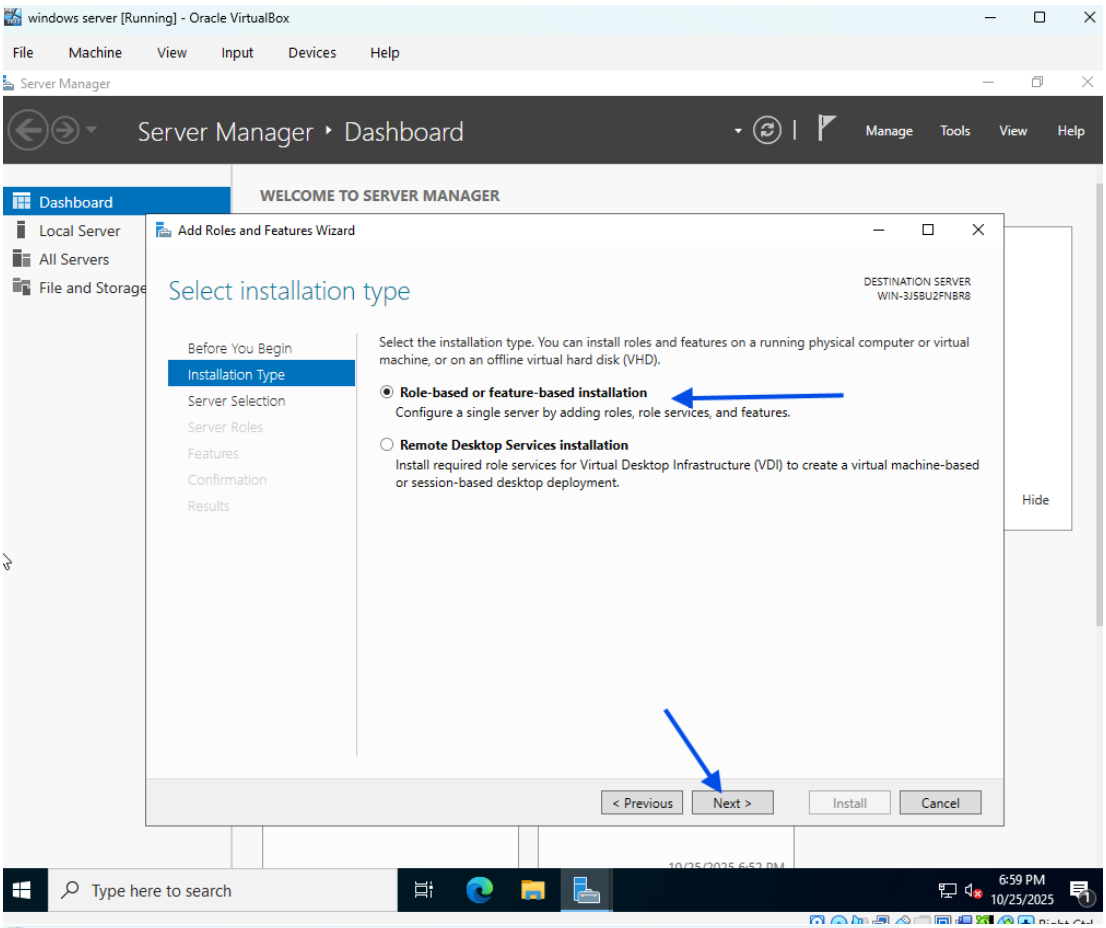
Click Manage>> add roles and features

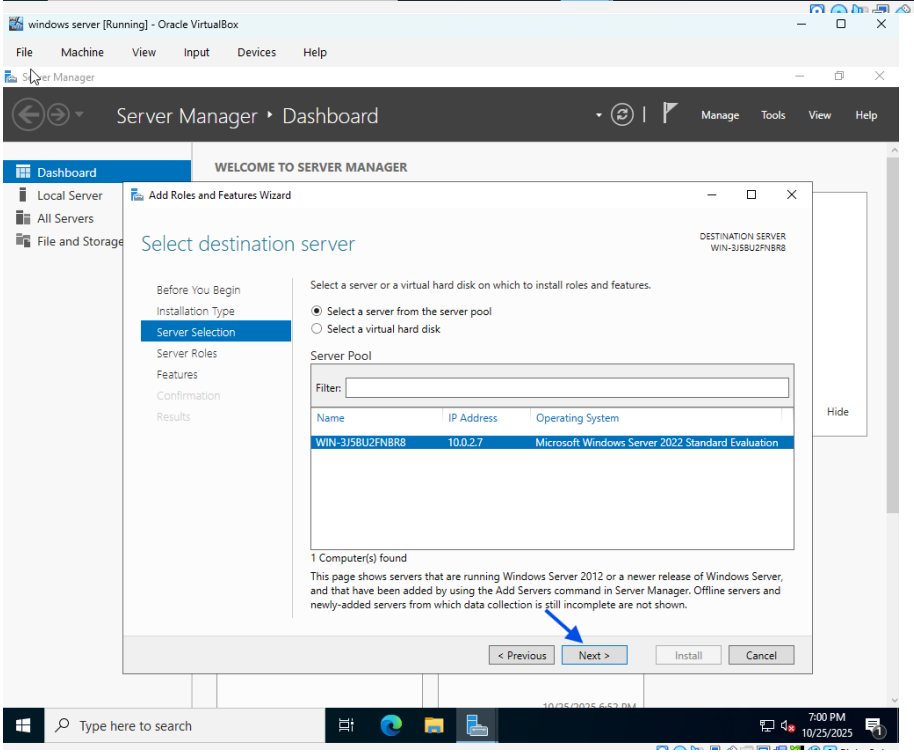
follow the prompts by clicking next


windows server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Add Roles and Features
Remove Roles and Features
Add Servers
Create Server Group
Server Manager Properties
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
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
Hide
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
BPA results
Local Server 1
Manageability
1 Events
4 Services
Performance
BPA results
Type here to search
6:56 PM
10/25/2025
Right Ctrl

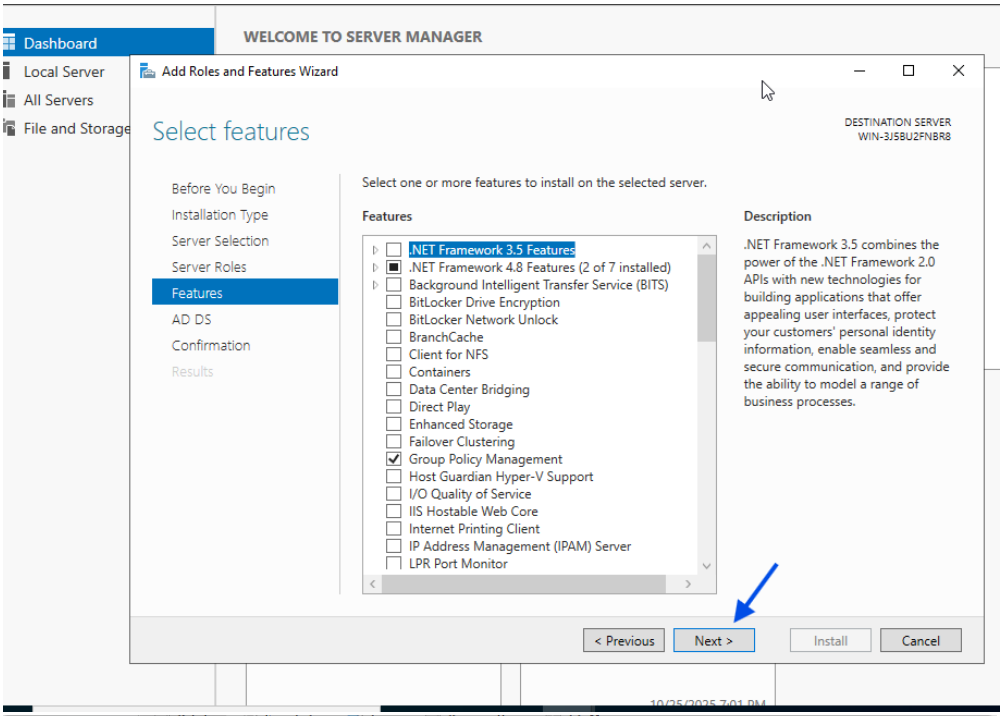

windows server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
File and Storage
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
WIN-3J5BU2FNBR8
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel
Hide
Type here to search
6:58 PM
10/25/2025
Right Ctrl

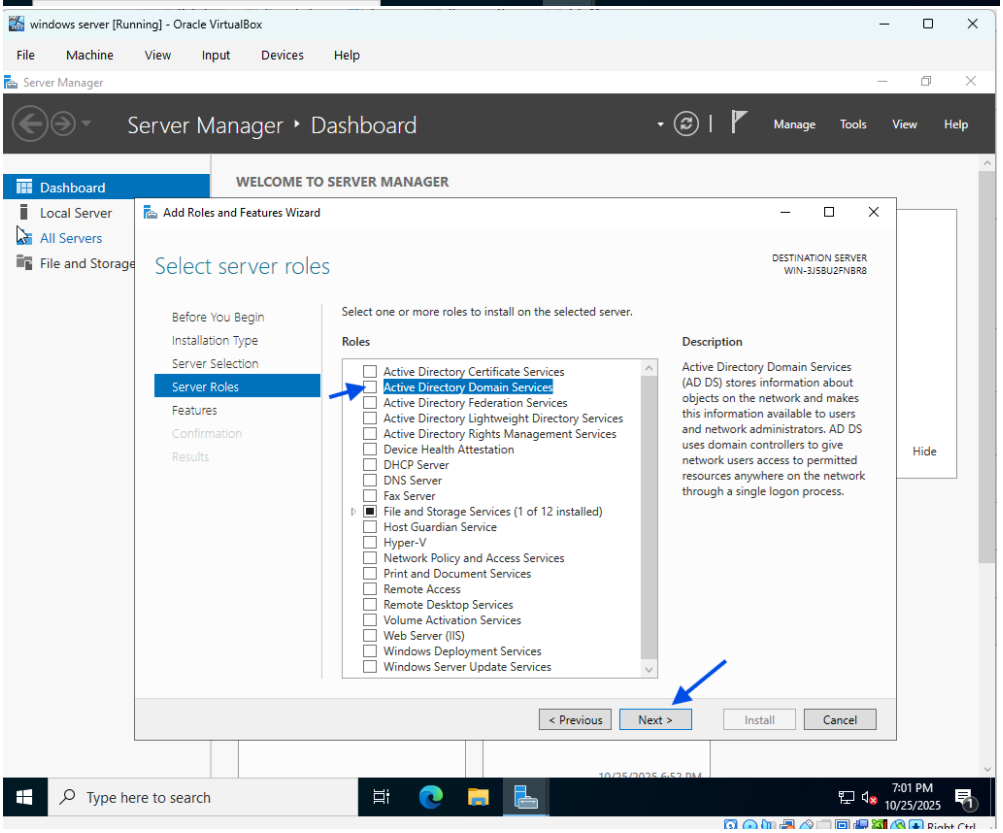
Select “role based or feature based installation” and click next



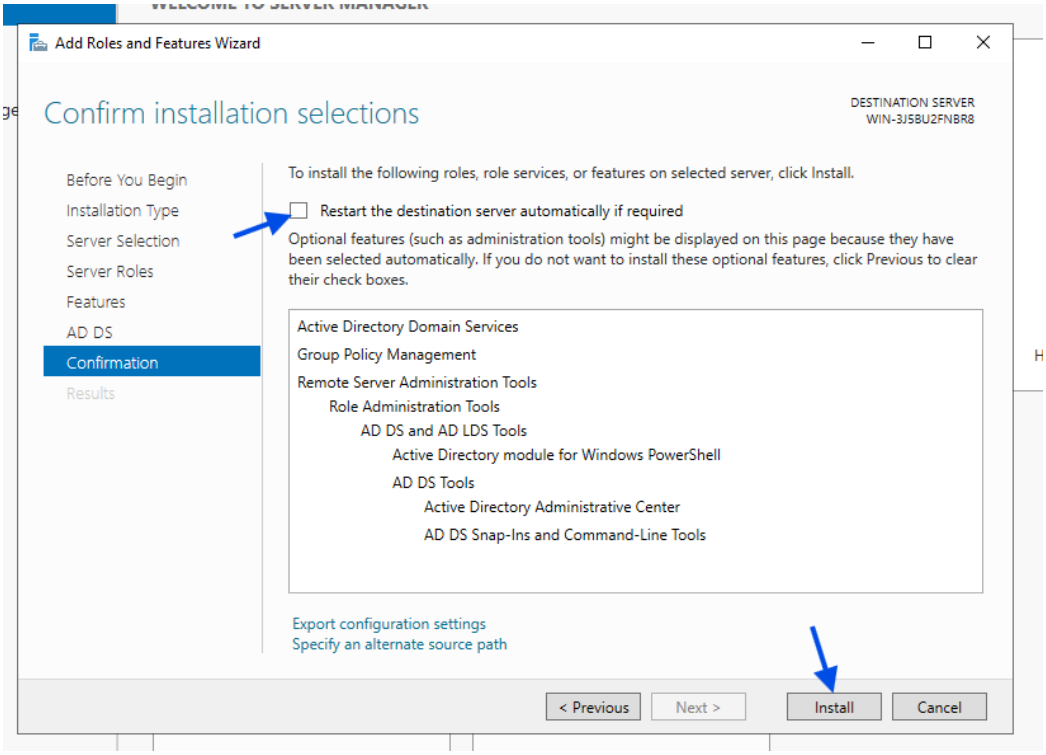


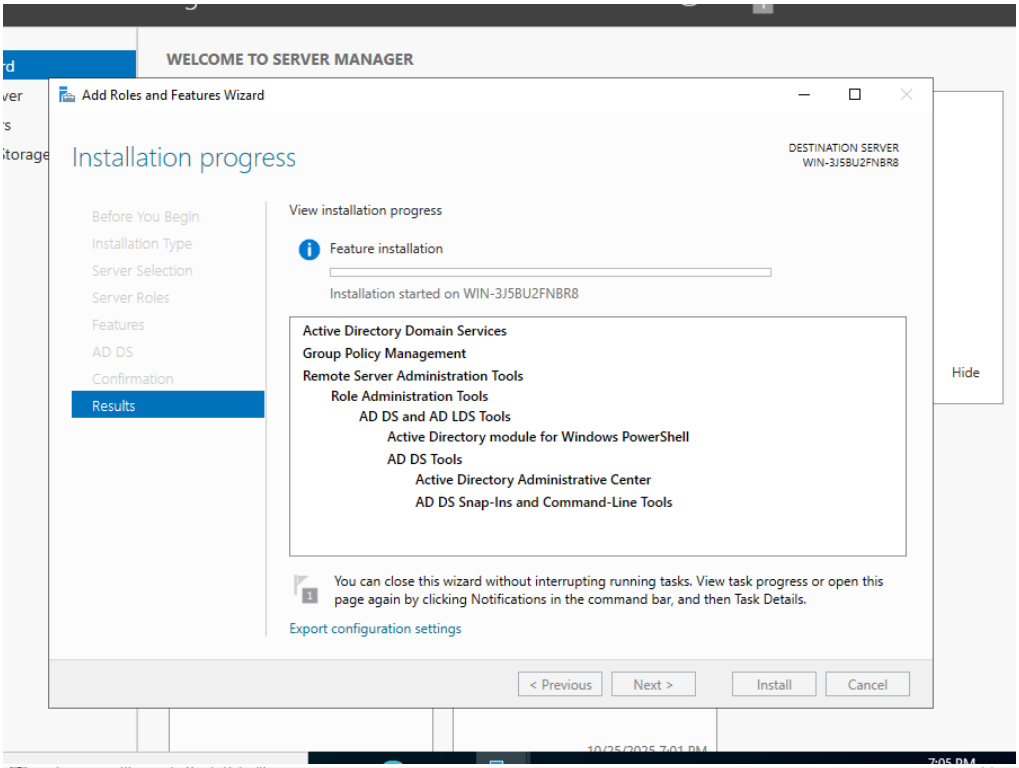
Check box “Active directory domain services”

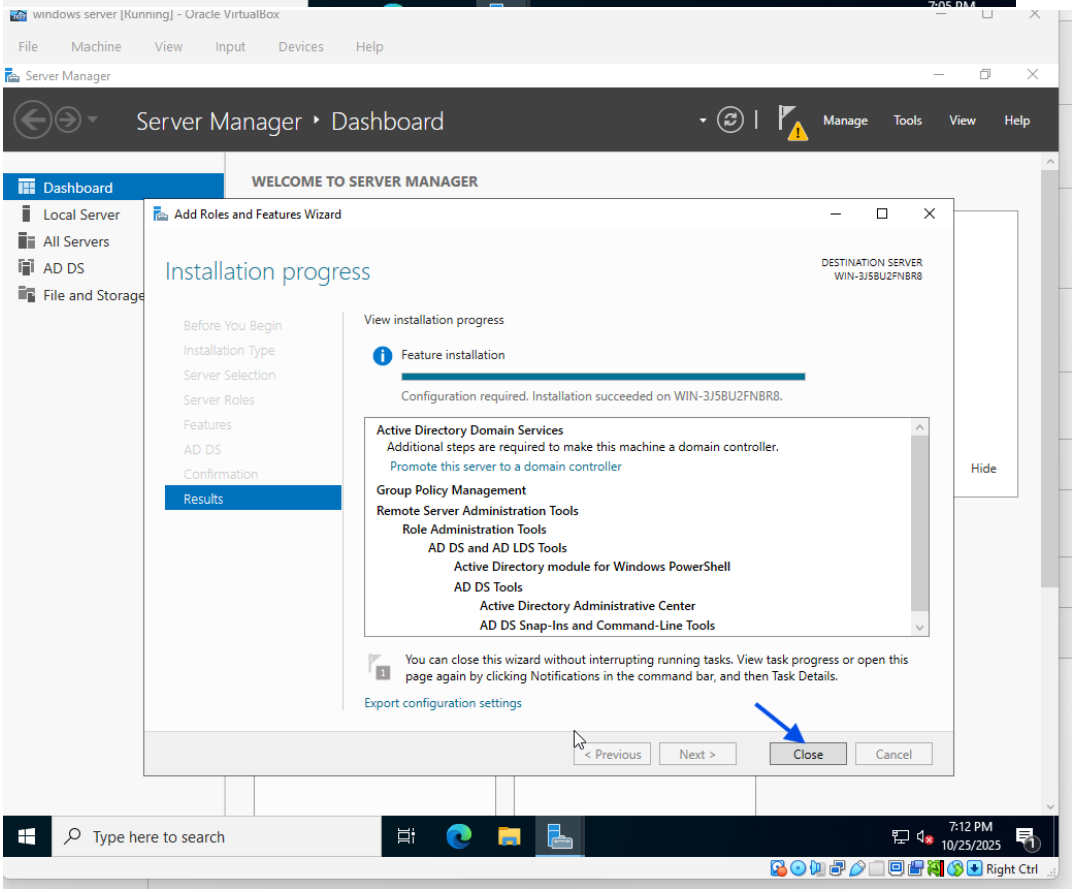




Check retart box and click install

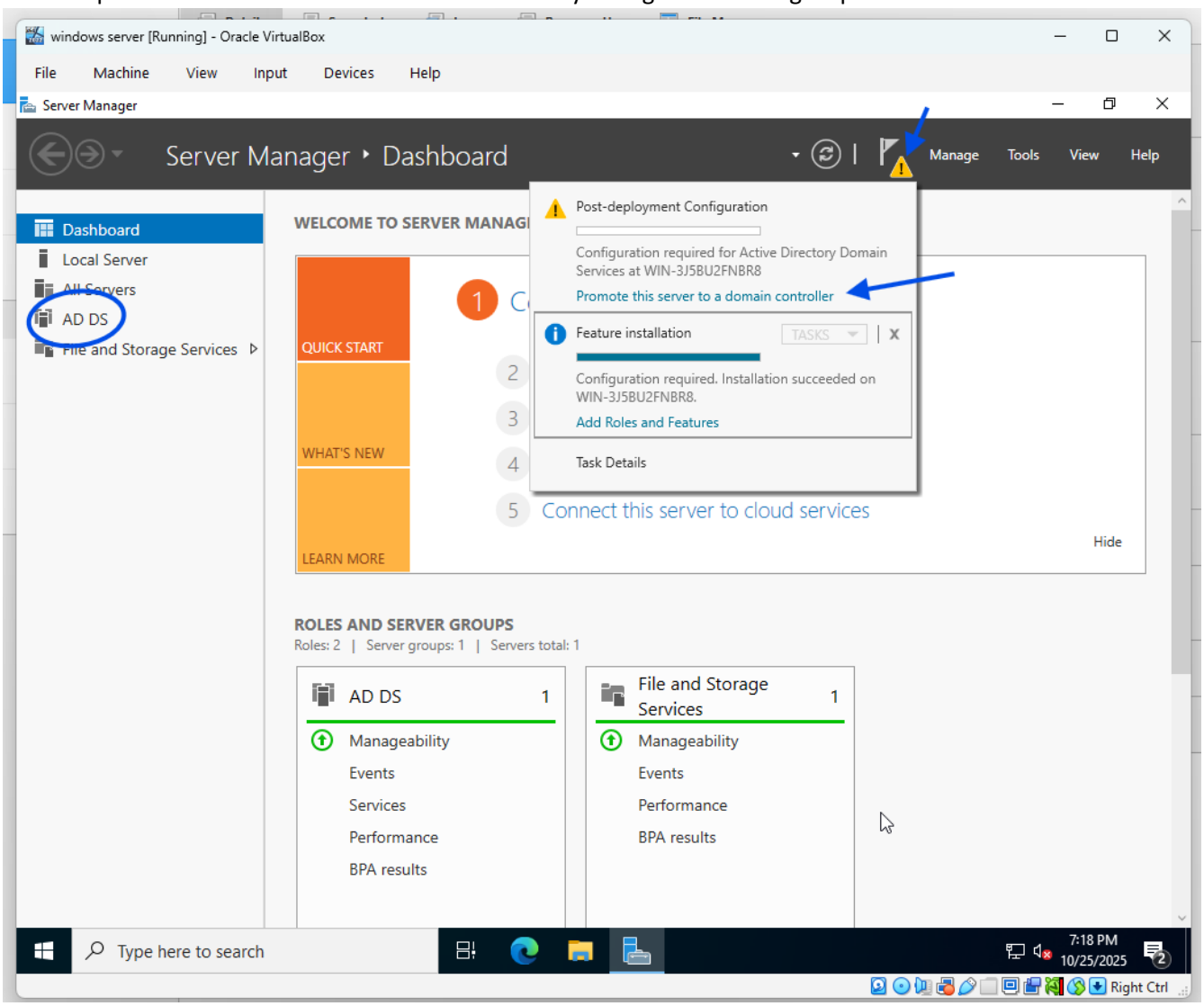




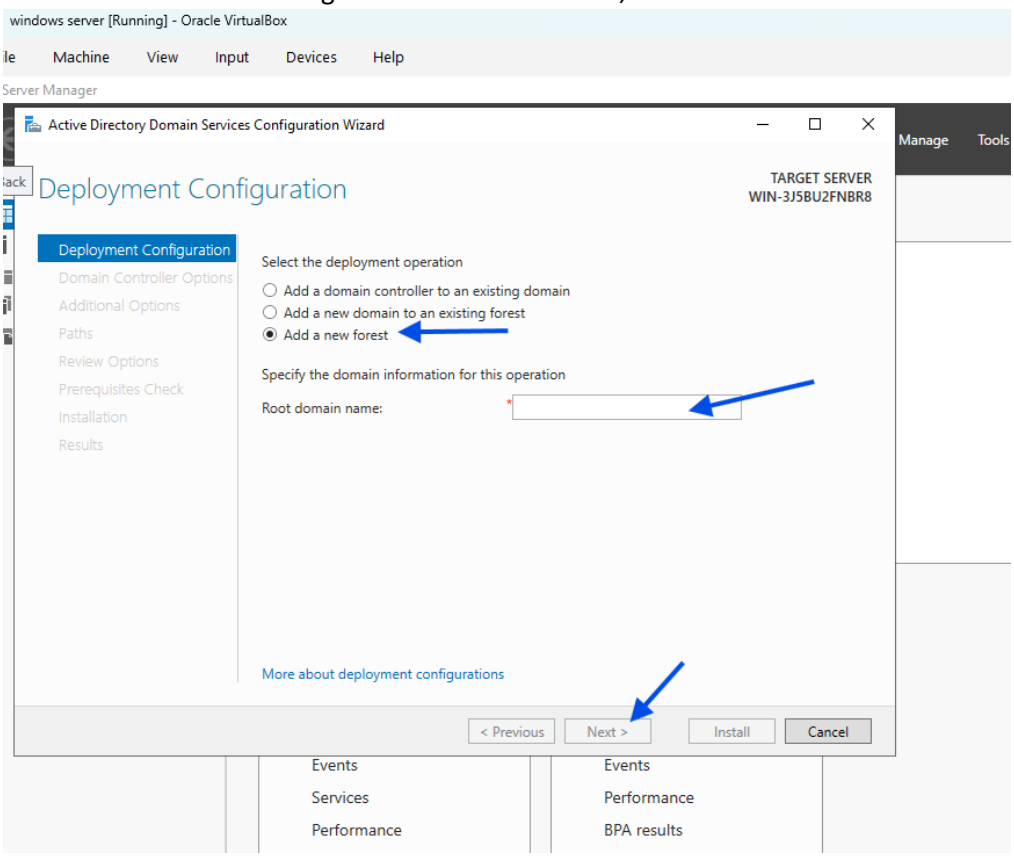


Installation is complete.

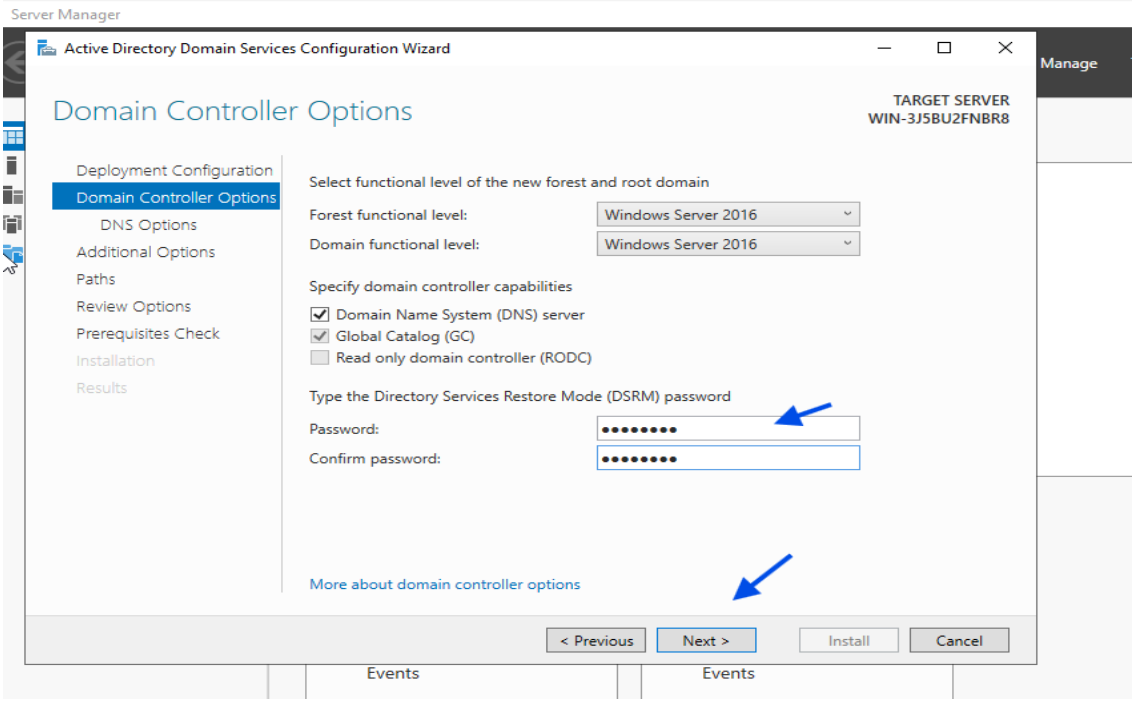
Now we promote the server to a domain controller by taking the following steps

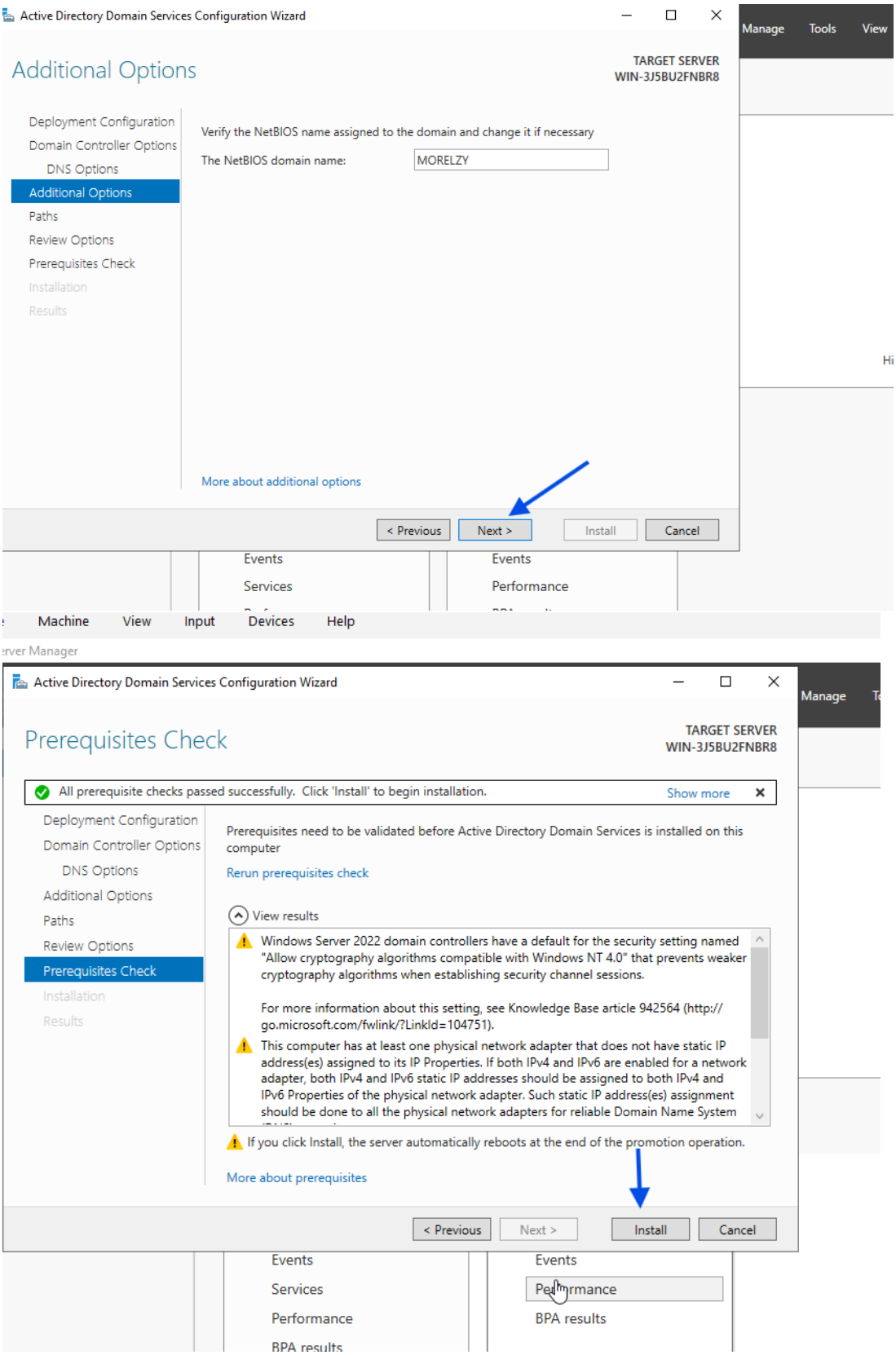


Select “add a foreste” and give a root domain name, then click next

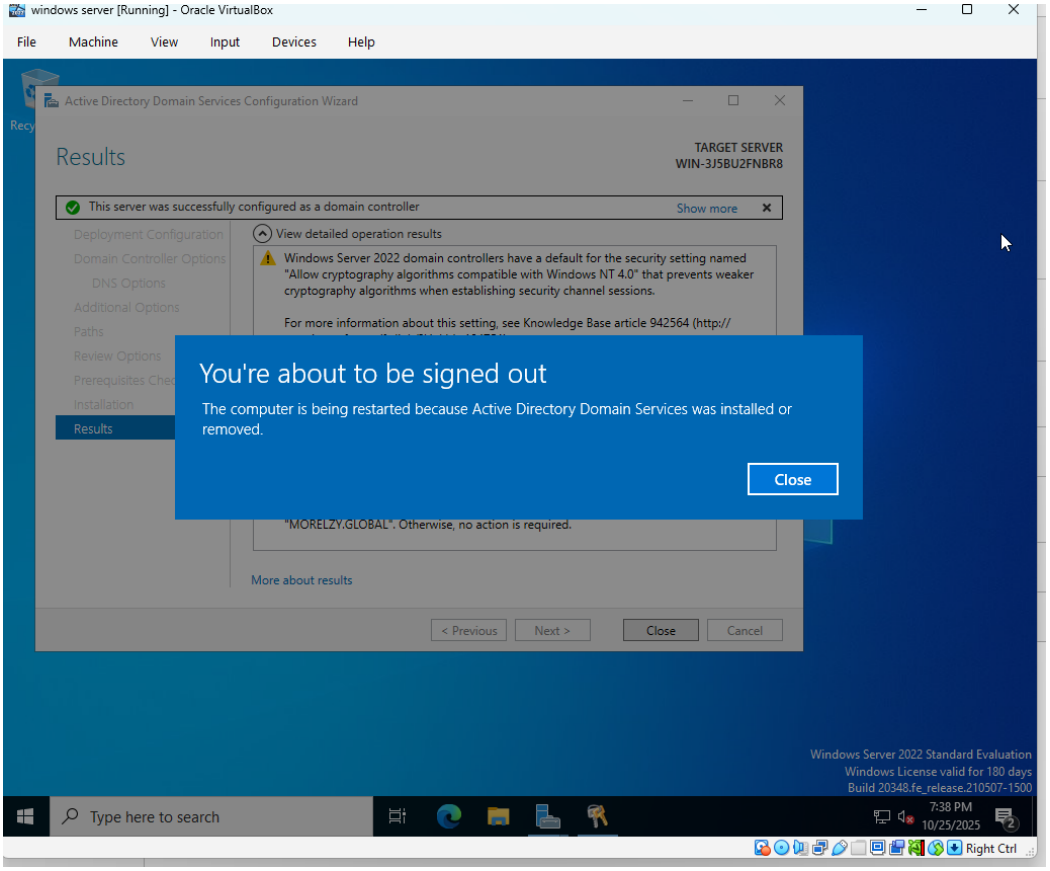


Provide password and click next





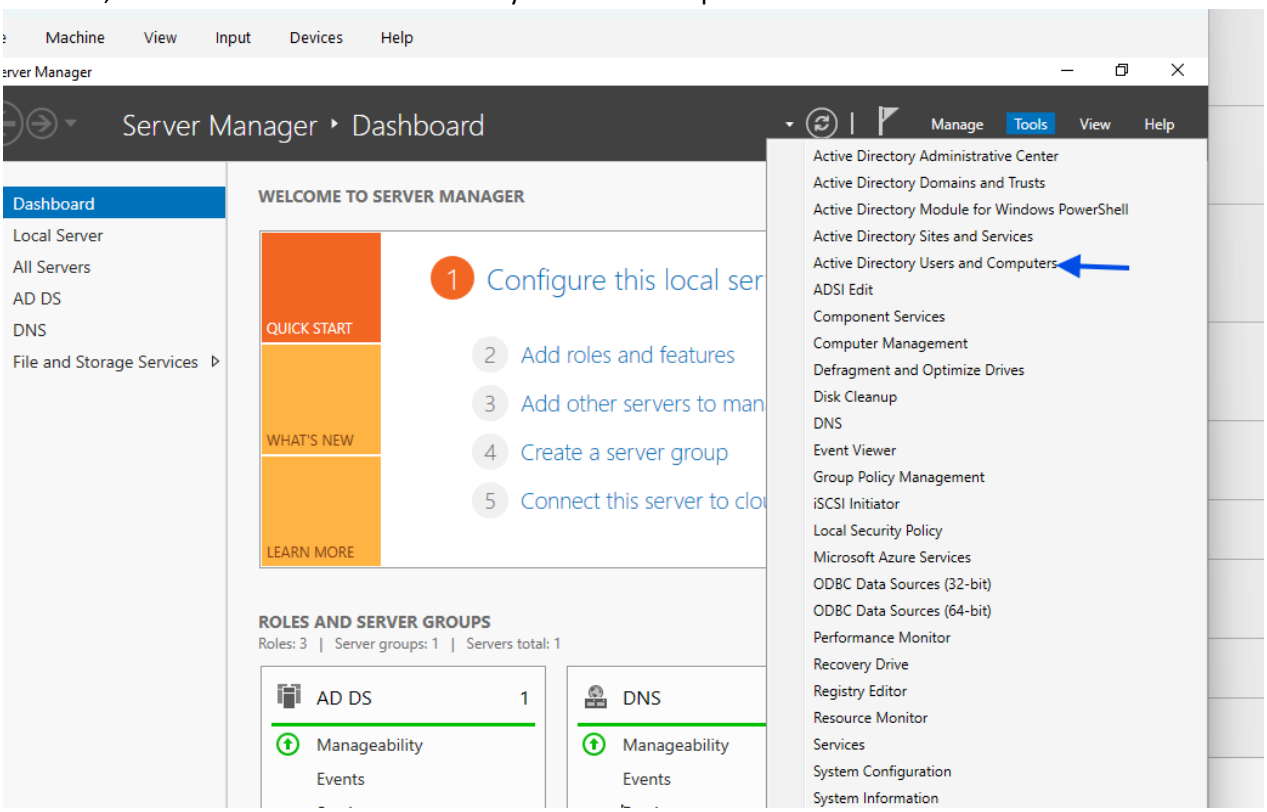
Upon completion of installation, server will restart

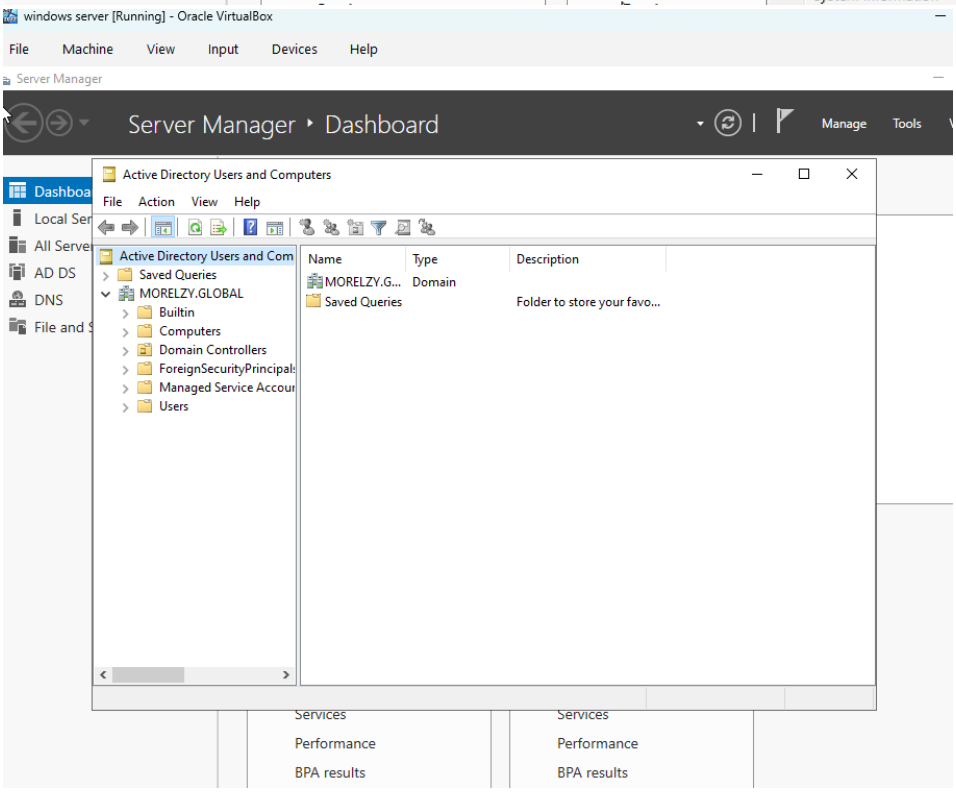


CREATING ORGANISATIONAL UNITS

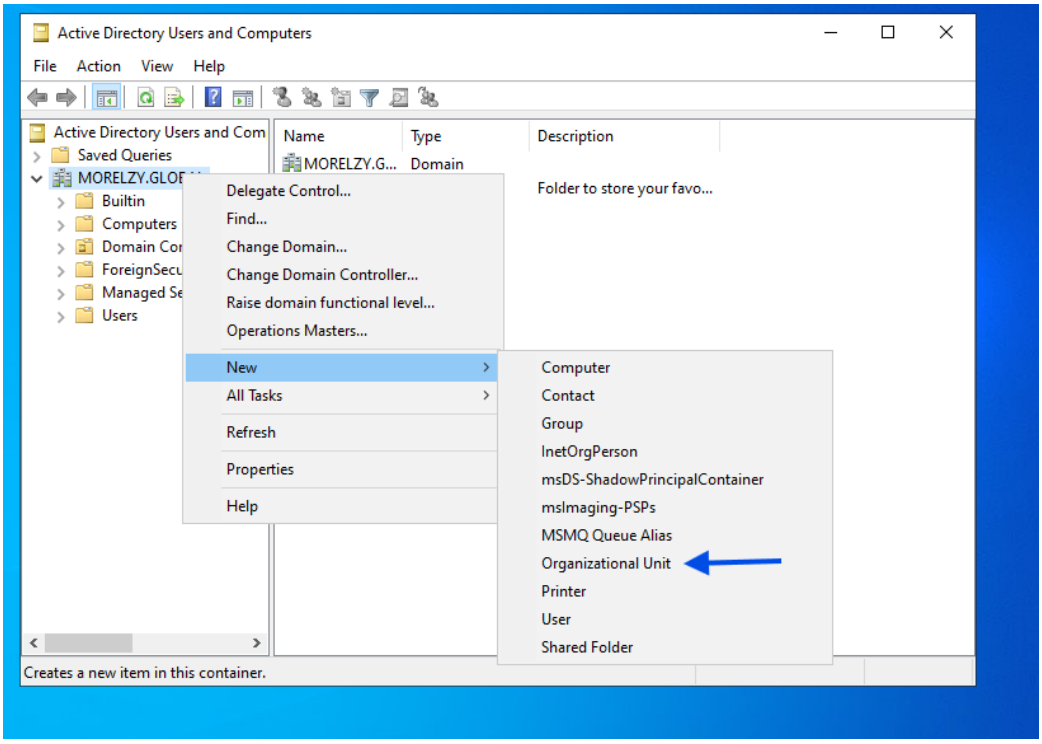
After servers has restarted, next step is to create organisational units

To do so, we select Tools>> active directory users and computers

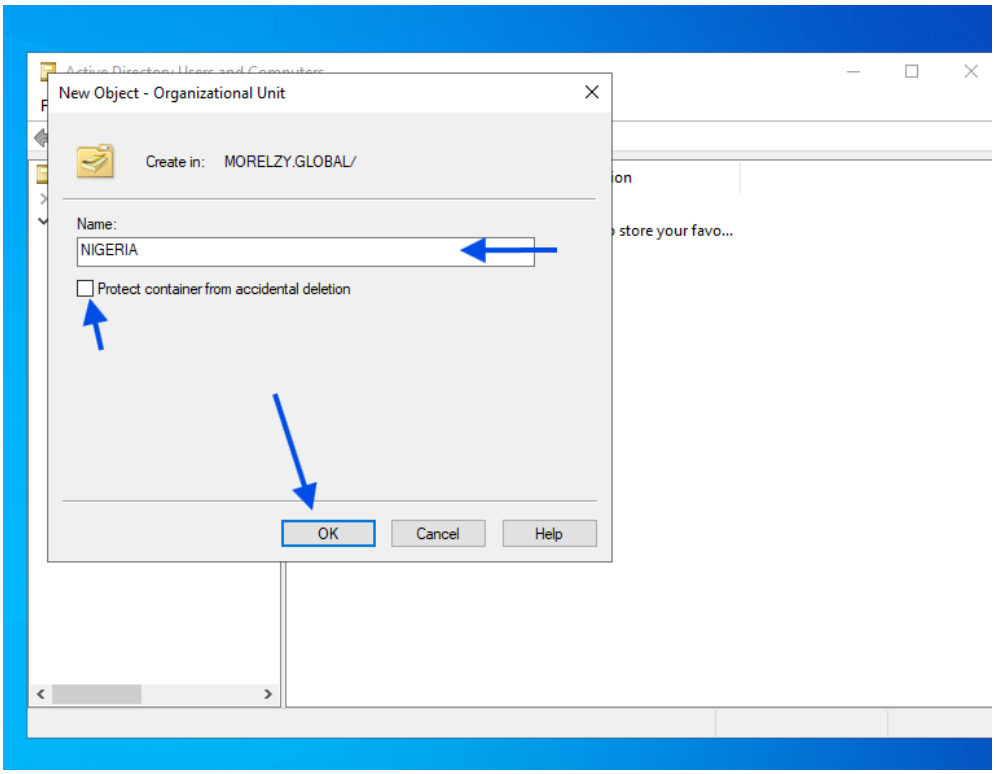




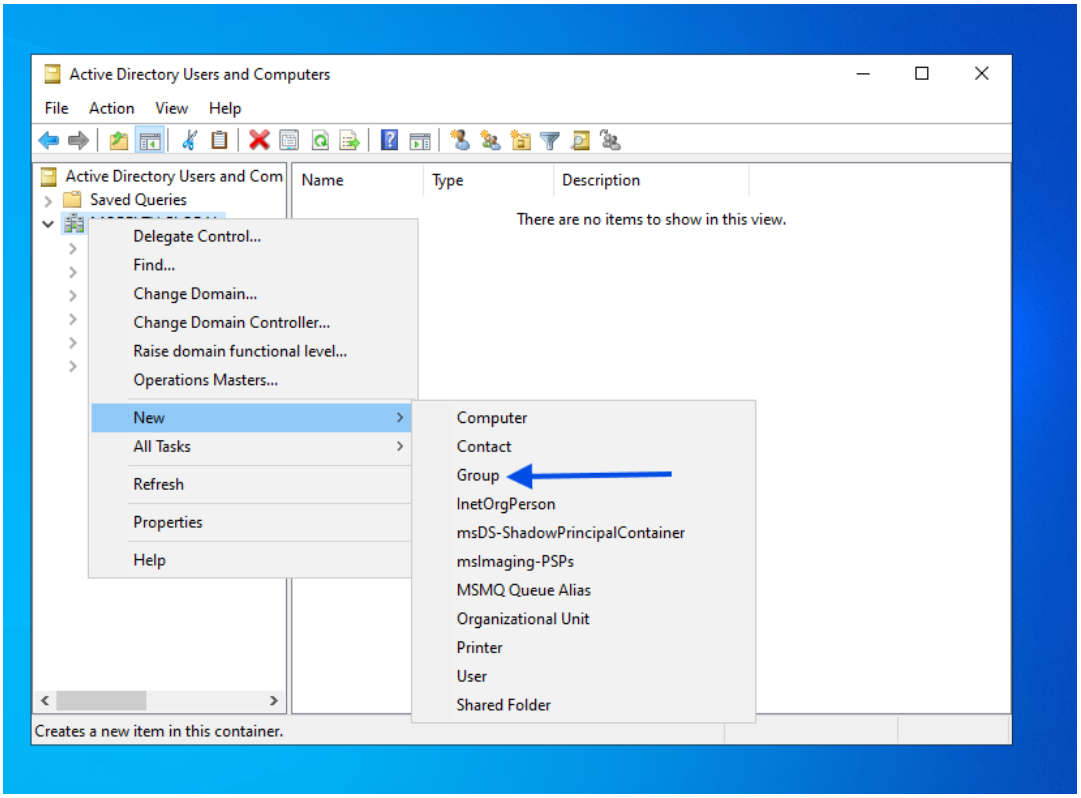
Next, right click on root domain name, select new and click on organisational unit



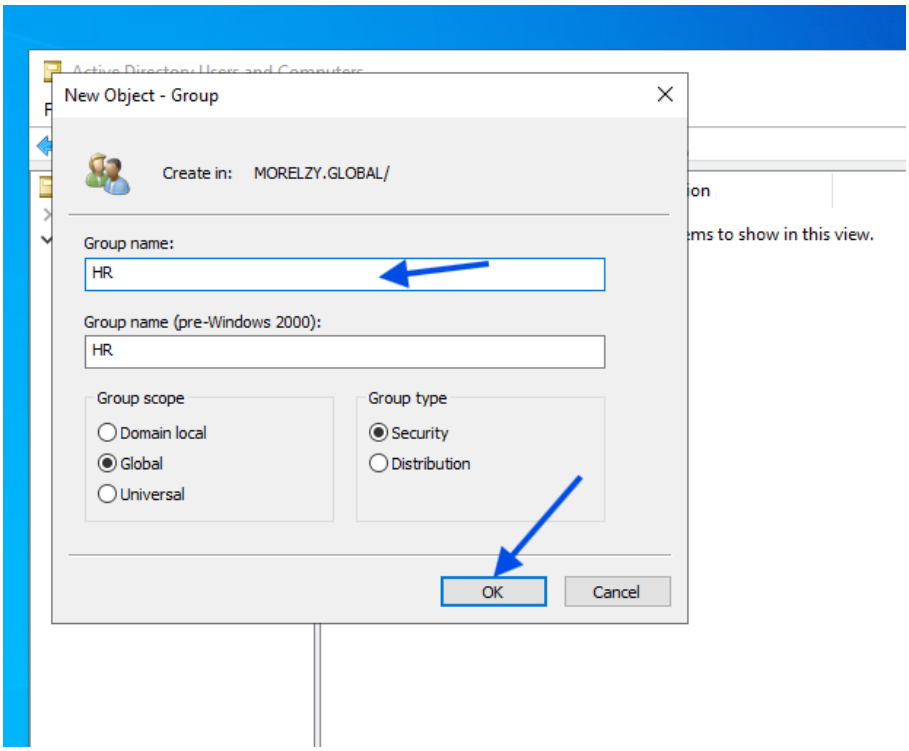
Name your organisational unit and click ok. Replicate for as many organisational units as required



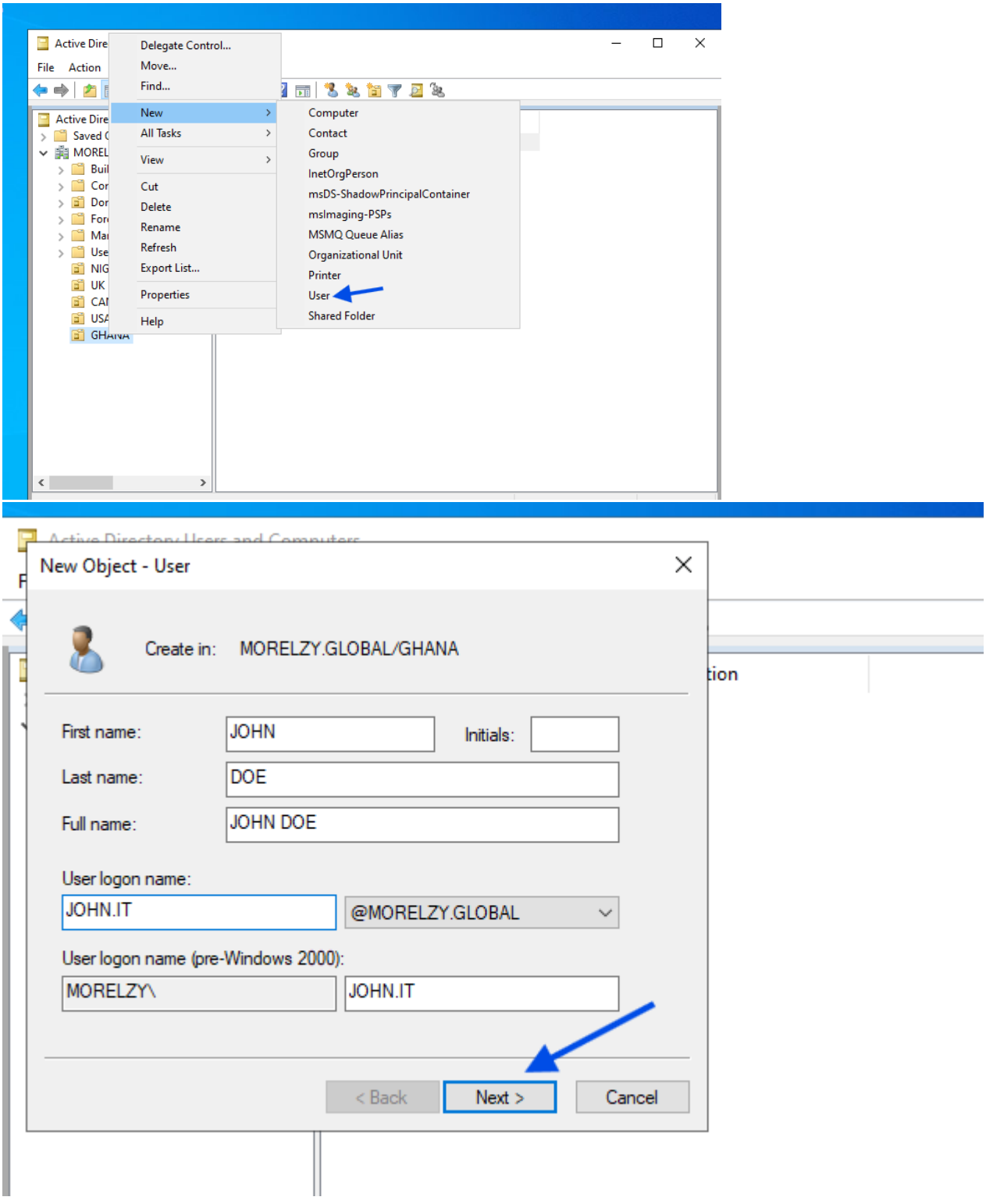
To create Groups, right click on Root domain>> new>> groups



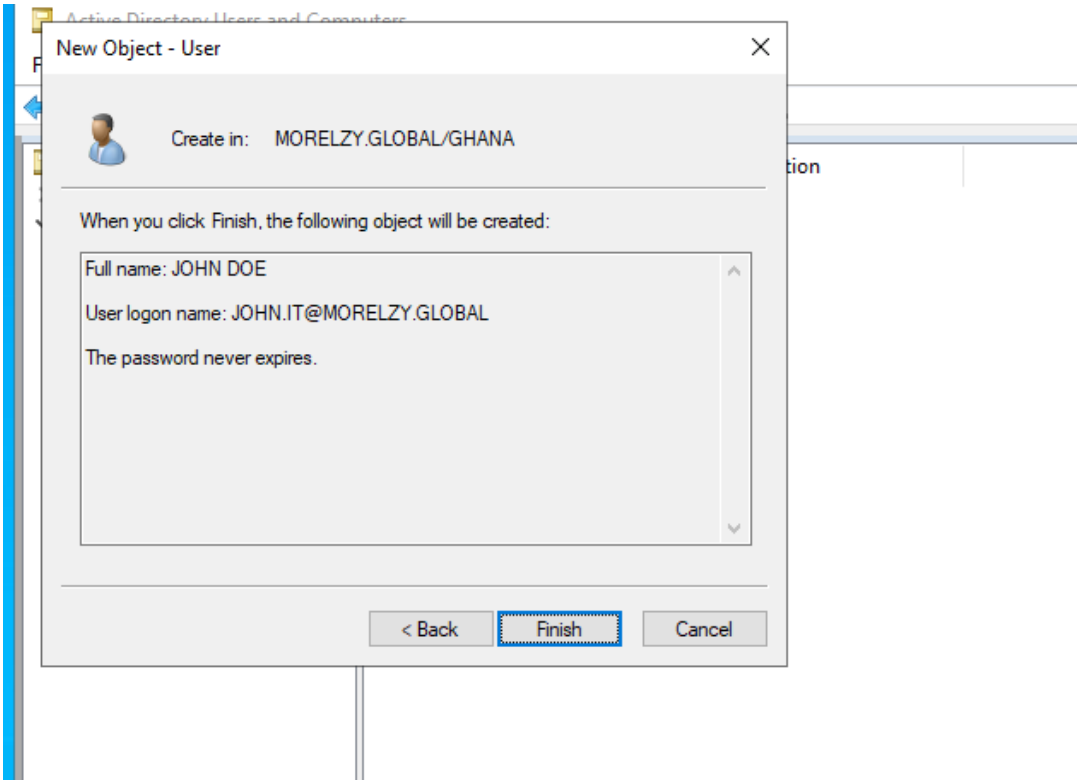
Provide group name and click ok, create as many groups as required

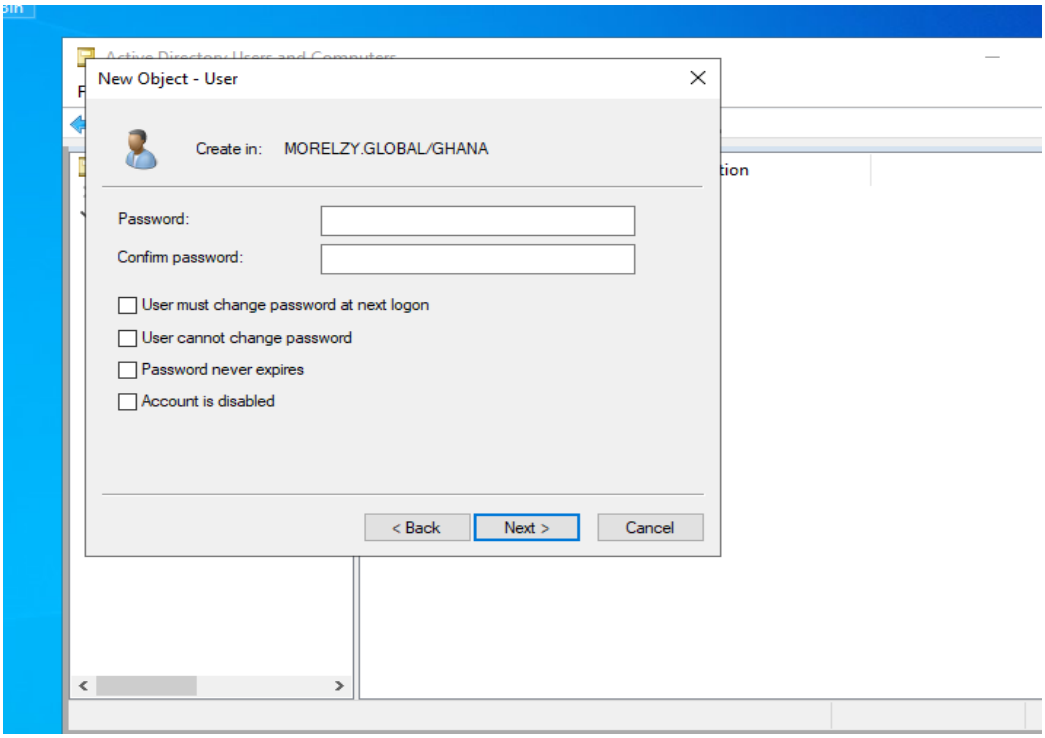


In the same manner, we will also create users



Select password setting you require, for the purpose of this labs we will select passwords never expire (this is not best practice)



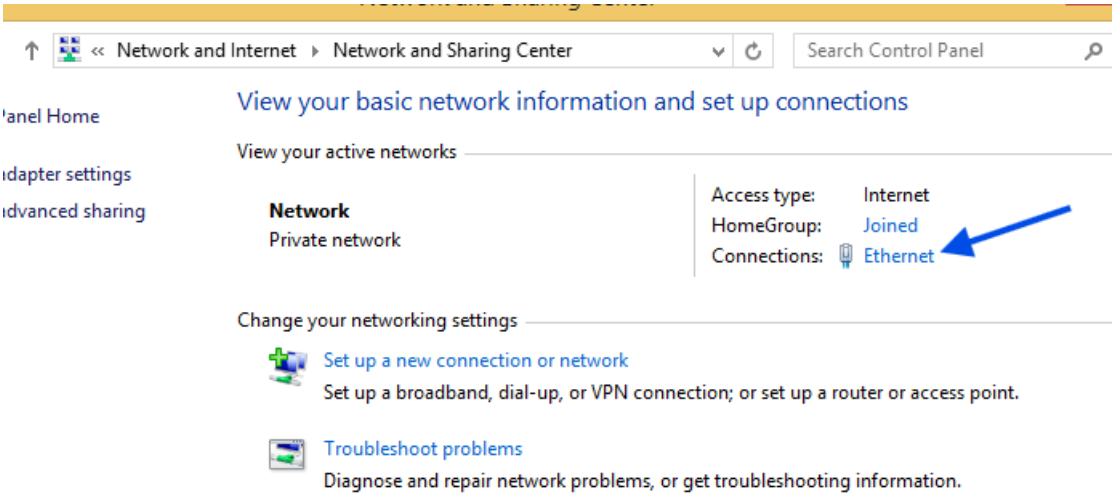


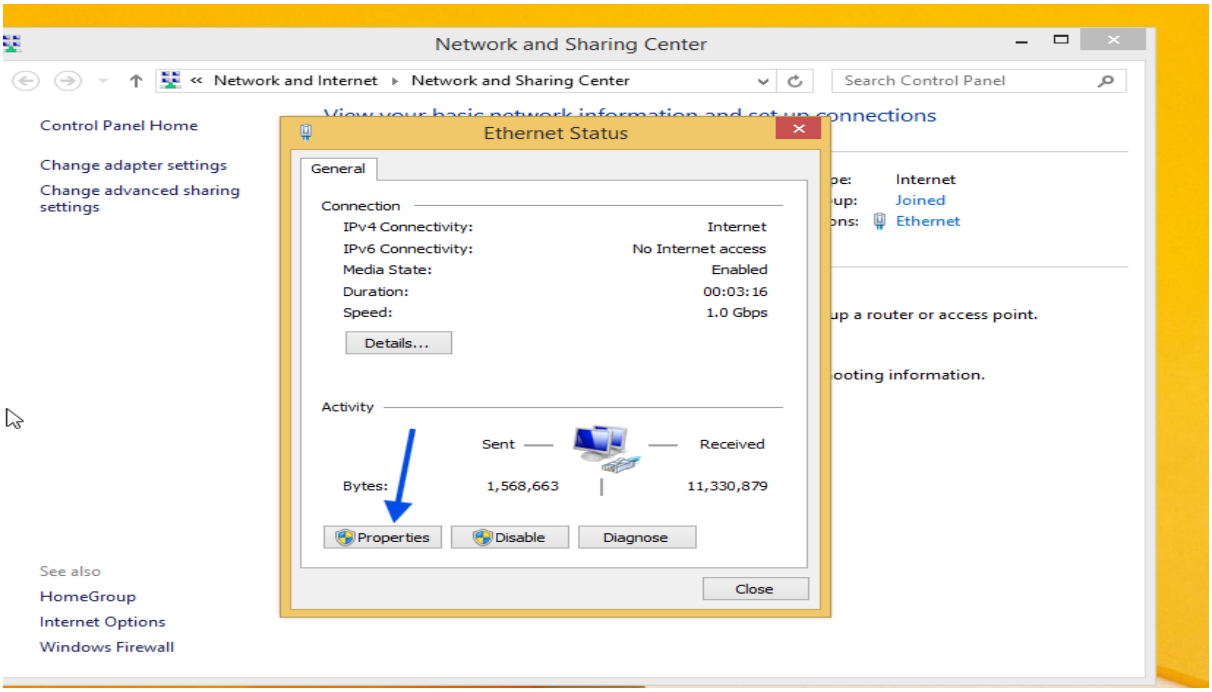
NETWORK CONFIGURATION

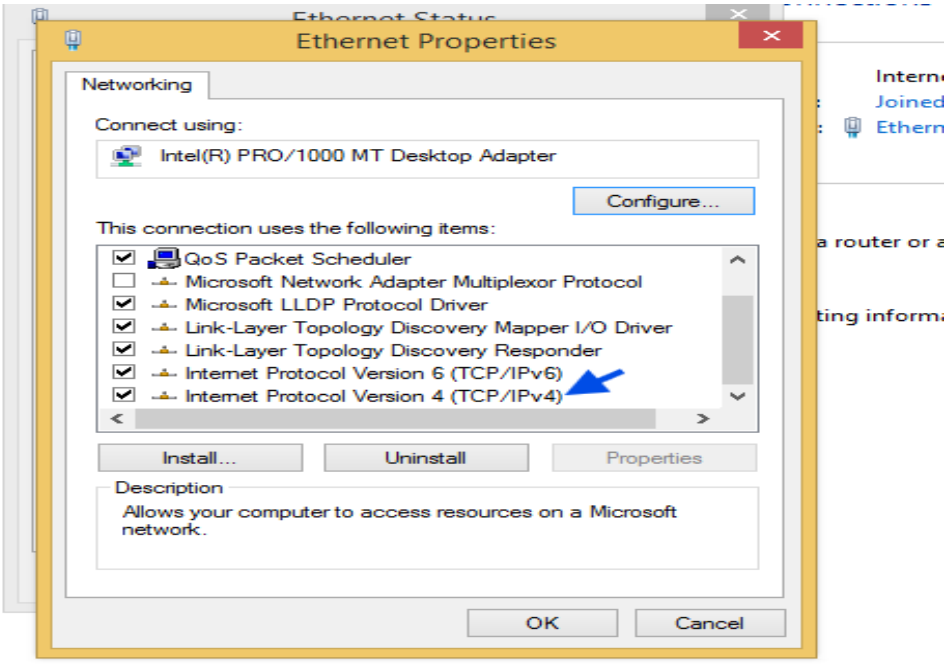
In this section we will be configuring the network.

From control panel>> Network and internet >> network and sharing center

Follow the steps in the image below

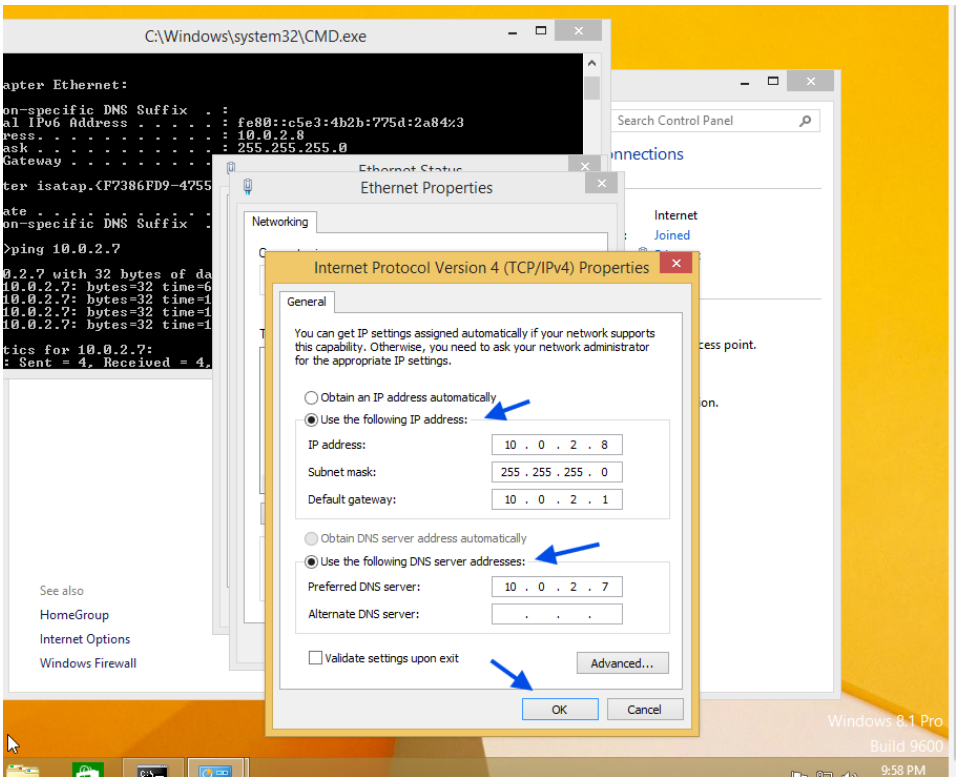






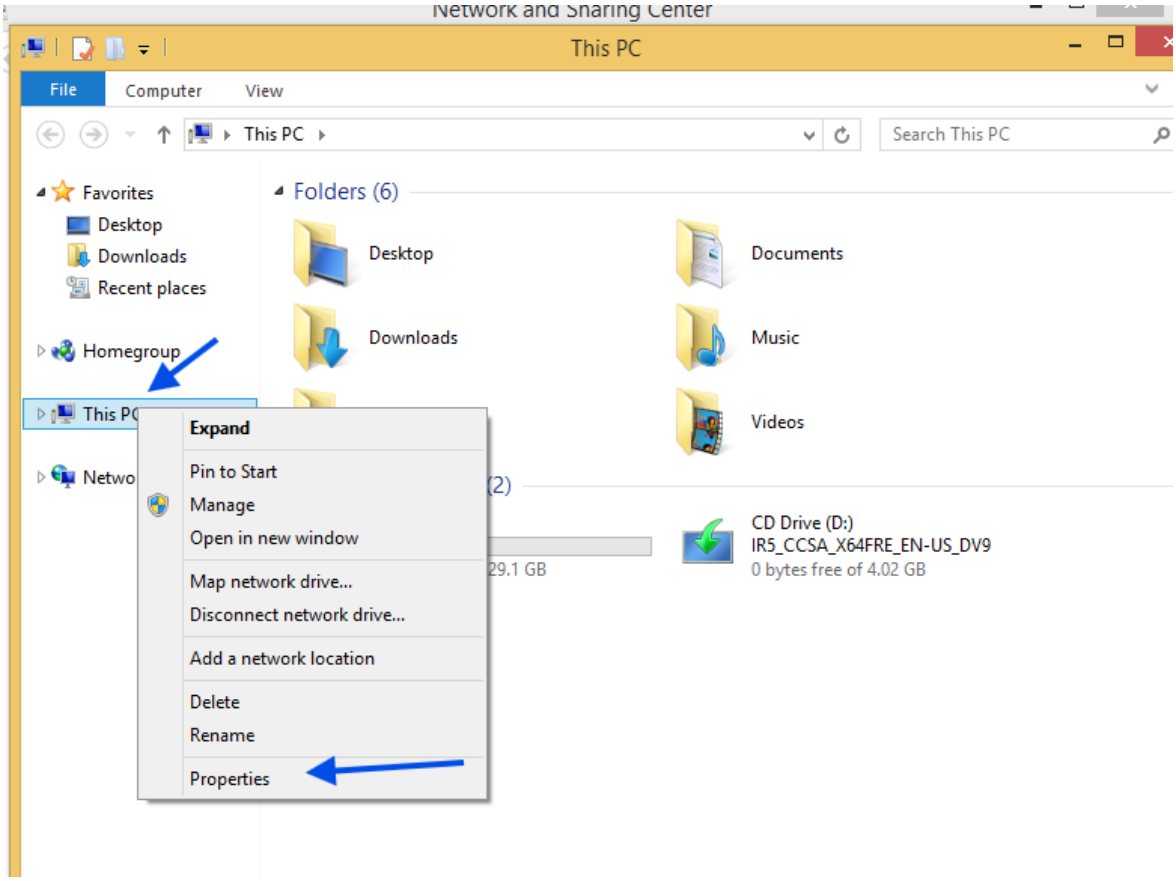
Select Static IP and provide the IP address of the PC (you can get the ip address by typing “ipconfig’ in CMD)

preferred DNS server is the IP of the windows server, click OK

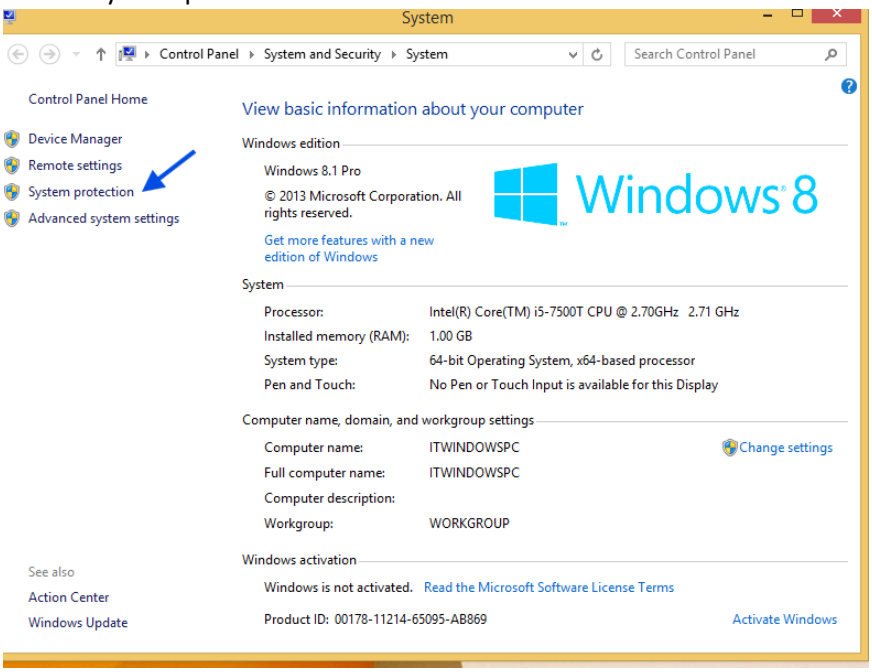


Next we add the system to the domain and sign in with the user account created

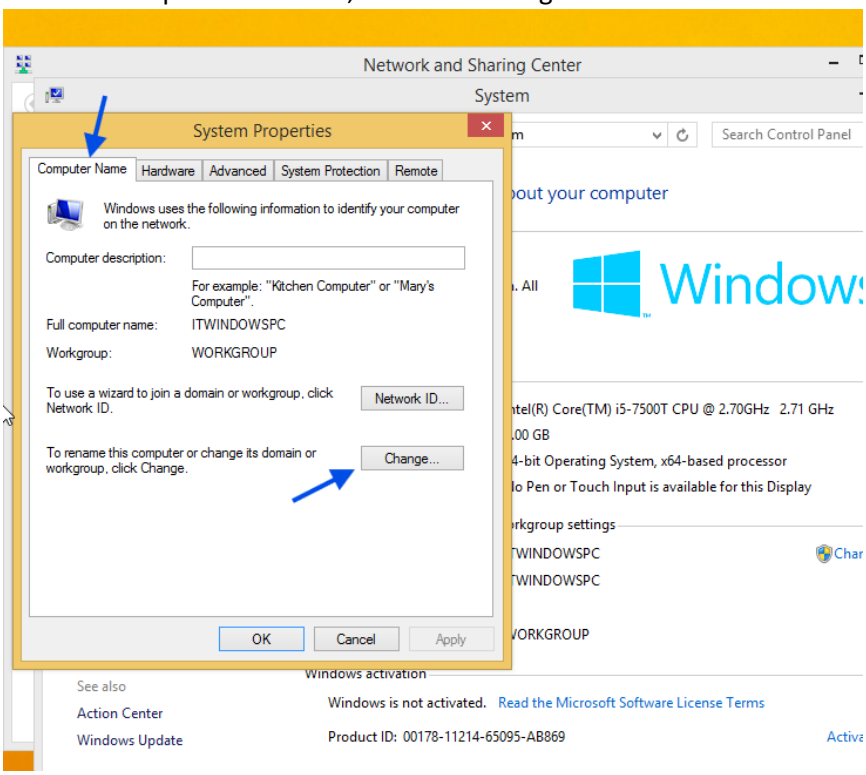
Right click on “MY PC” and click on properties



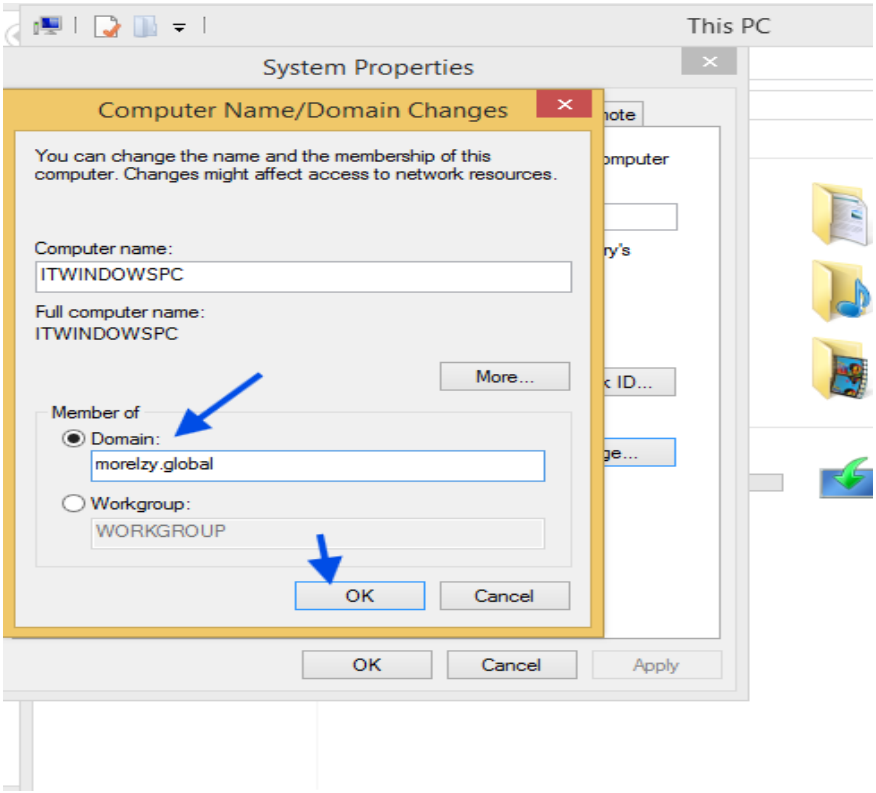
Select “system protection” on the left



Clock on computer name tab, then click change

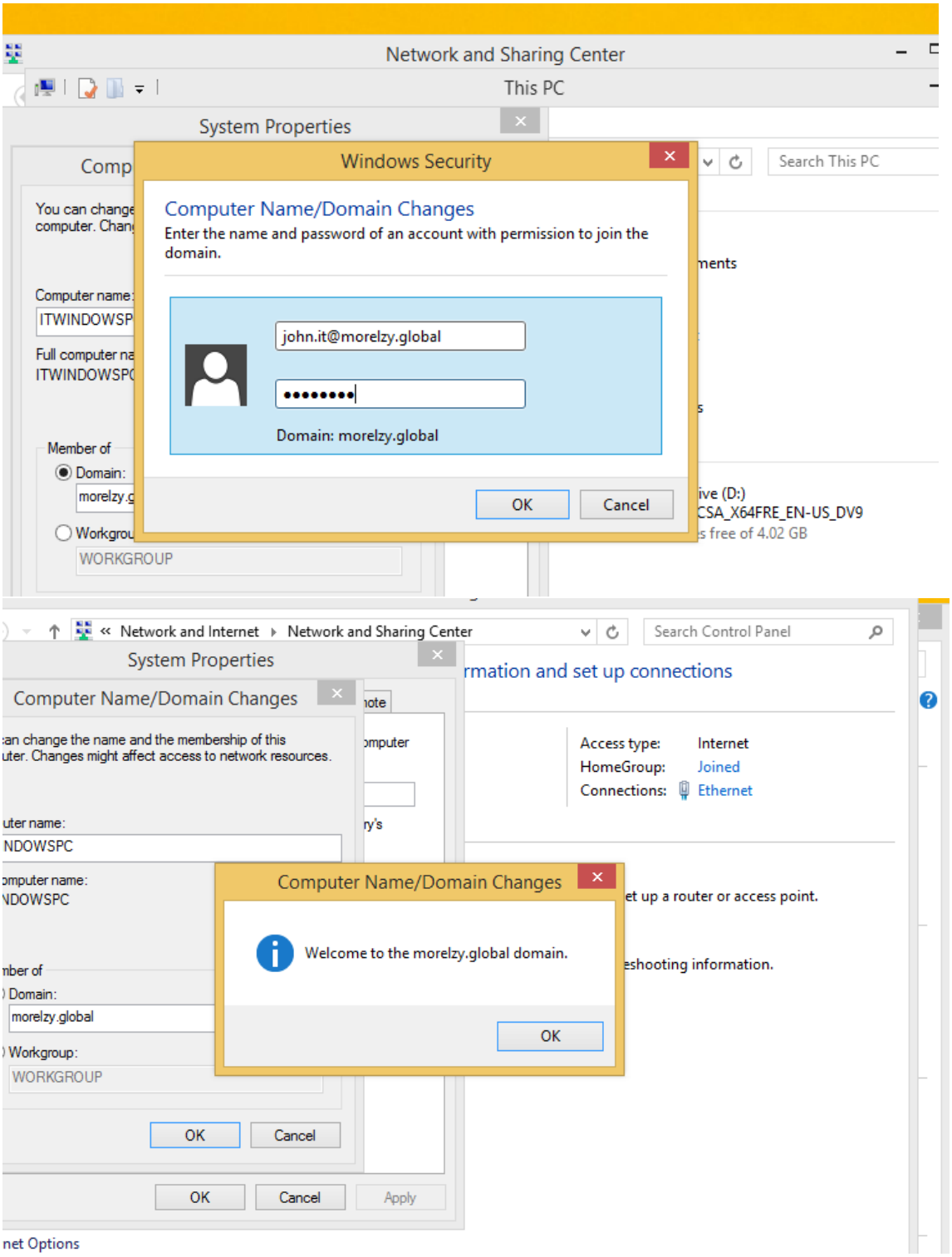


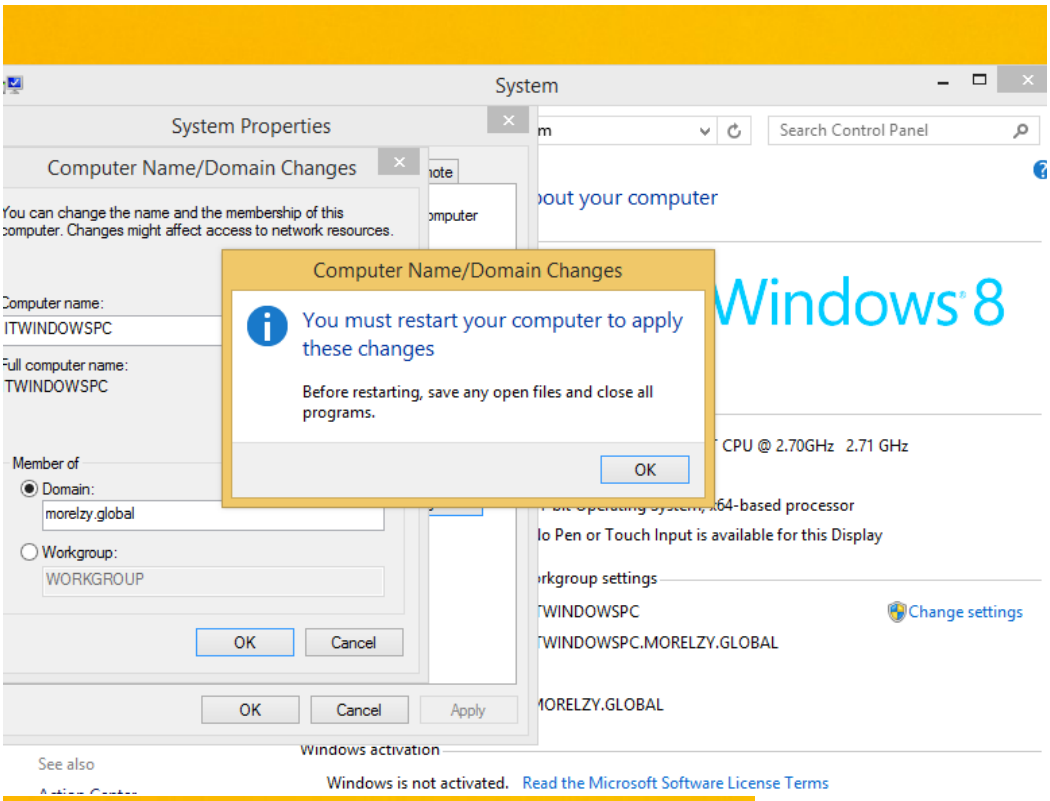
Provide domain name and click OK

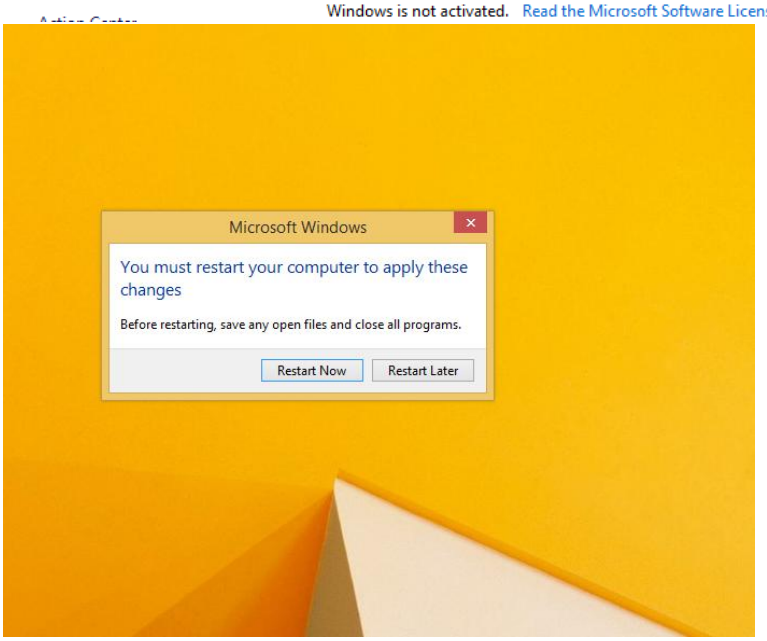


There will be a sign in pop up, sign in with name and password of user created

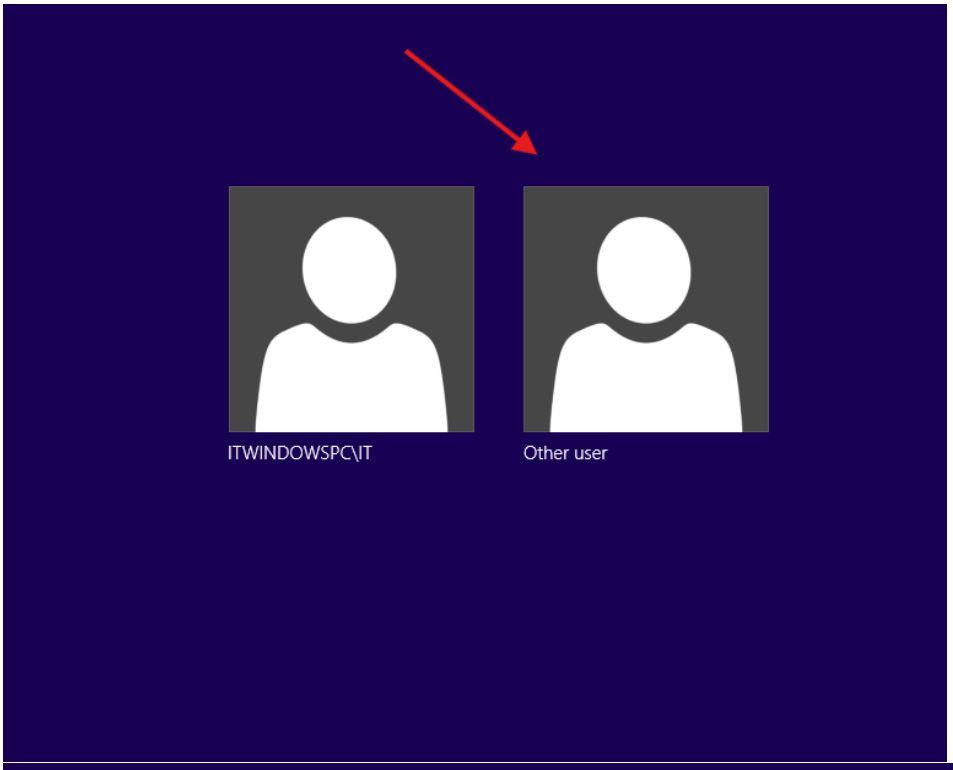
Click okay and the system will restart

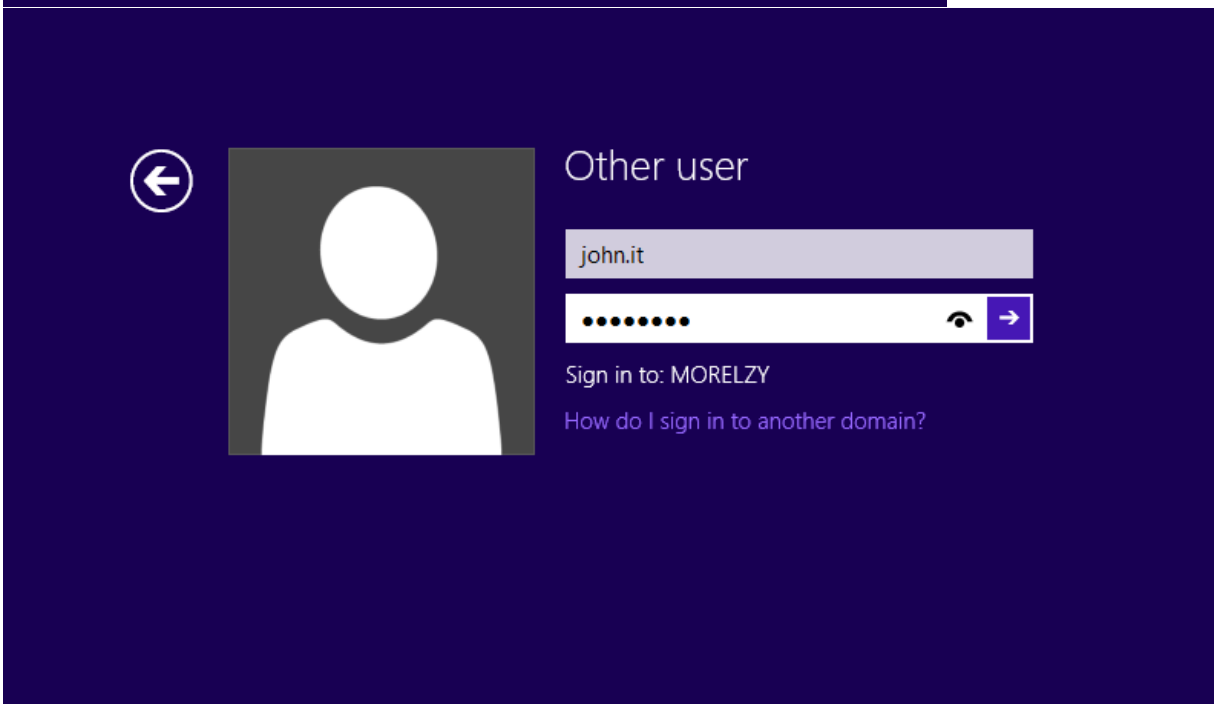




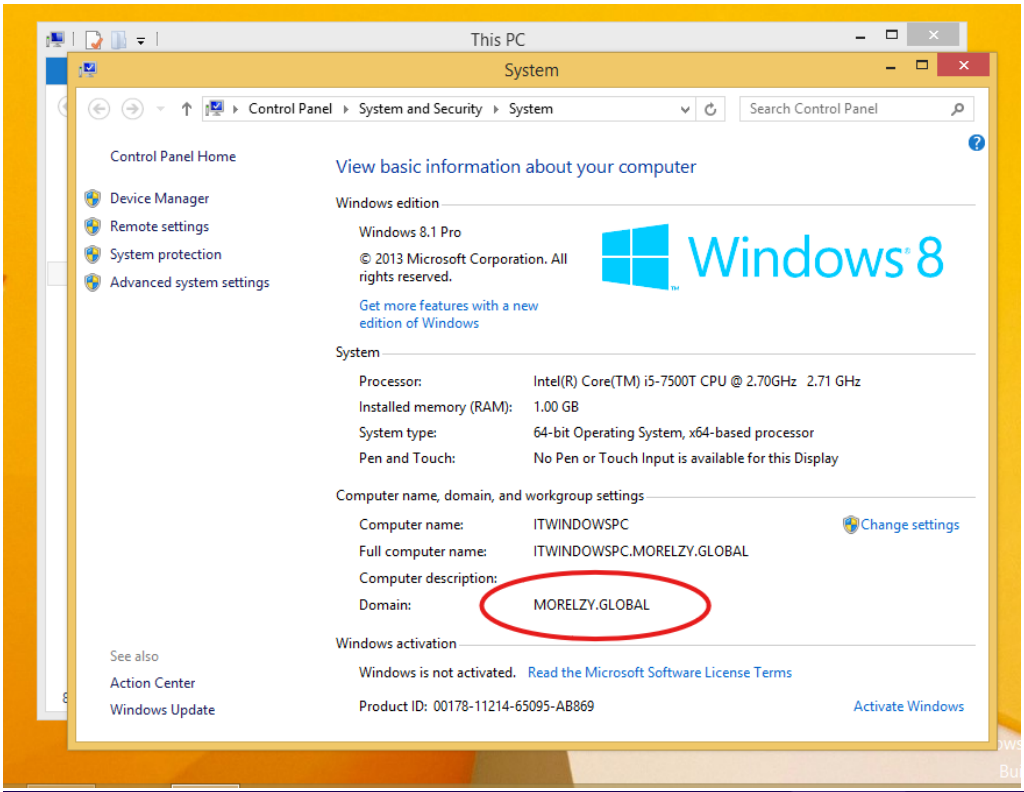


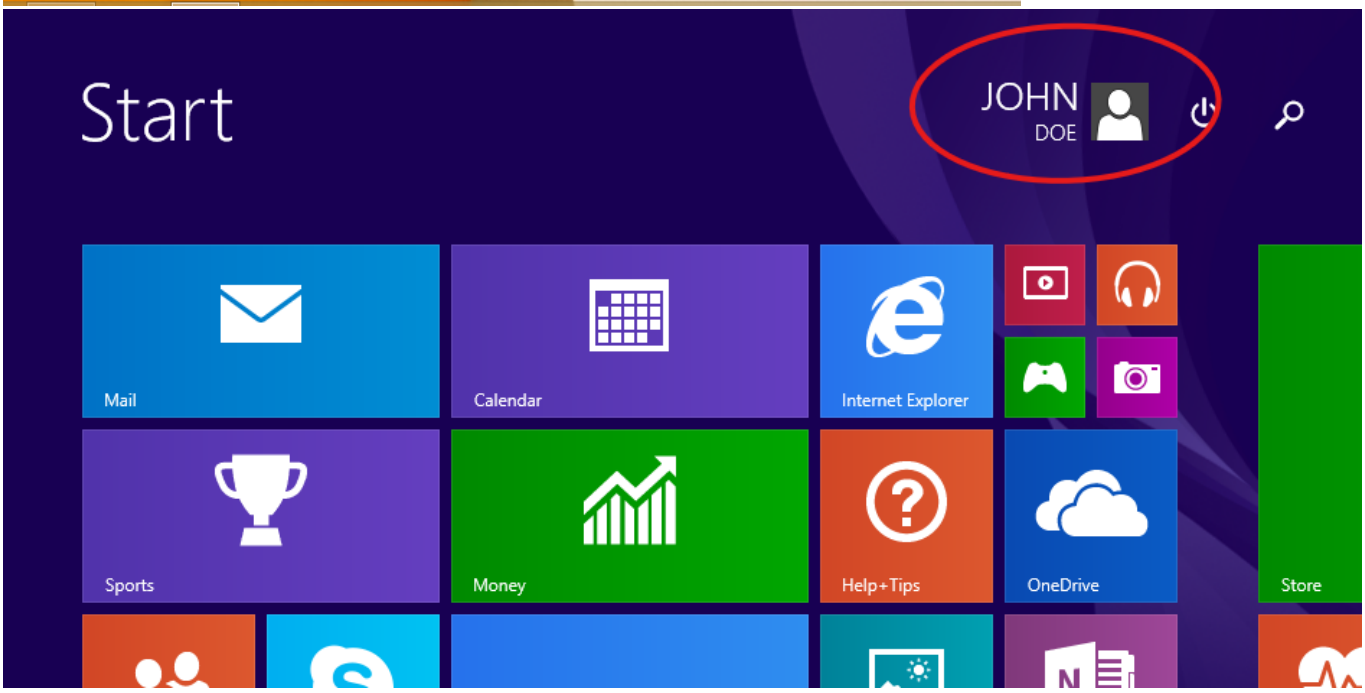
Once restarted, sign in as another user with the credentials of the user we created (Not the Local Admin account)





Confirm that PC domain name has changed and that you are logged in as the user created and not the local Admin of the PC

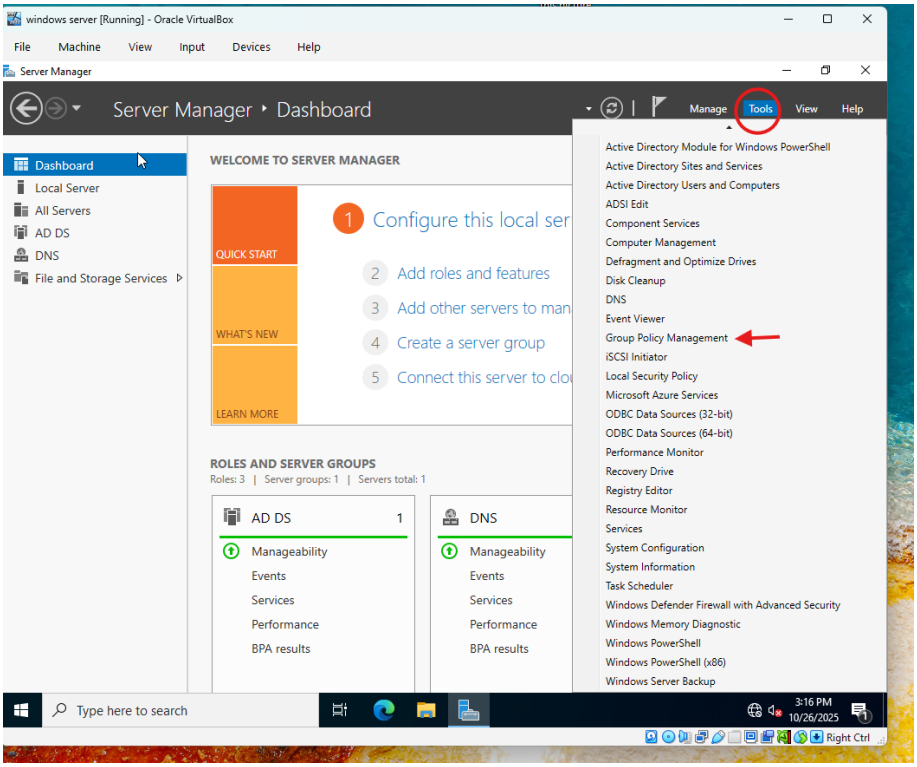

This PC
System
Control Panel ▸ System and Security ▸ System
Search Control Panel
Control Panel Home
Device Manager
Remote settings
System protection
Advanced system settings
View basic information about your computer
Windows edition
Windows 8.1 Pro
© 2013 Microsoft Corporation. All rights reserved.
Get more features with a new edition of Windows
Windows 8
System
Processor: Intel(R) Core(TM) i5-7500T CPU @ 2.70GHz 2.71 GHz
Installed memory (RAM): 1.00 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display
Computer name, domain, and workgroup settings
Computer name: ITWINDOWSPC
Change settings
Full computer name: ITWINDOWSPC.MORELZY.GLOBAL
Computer description:
Domain: MORELZY.GLOBAL
Windows activation
Windows is not activated. Read the Microsoft Software License Terms
Product ID: 00178-11214-65095-AB869
Activate Windows
See also
Action Center
Windows Update


Start
JOHN
DOE
Mail
Calendar
Internet Explorer
Sports
Money
Help+Tips
OneDrive
Store

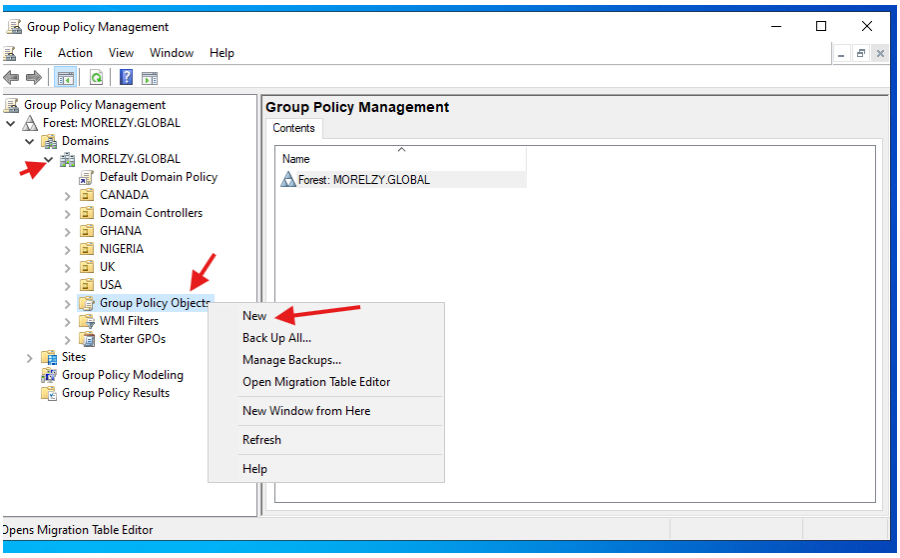
CREATING AND IMPLEMENTING A GROUP POLICY

We will be adding policies and linking them to groups and users.

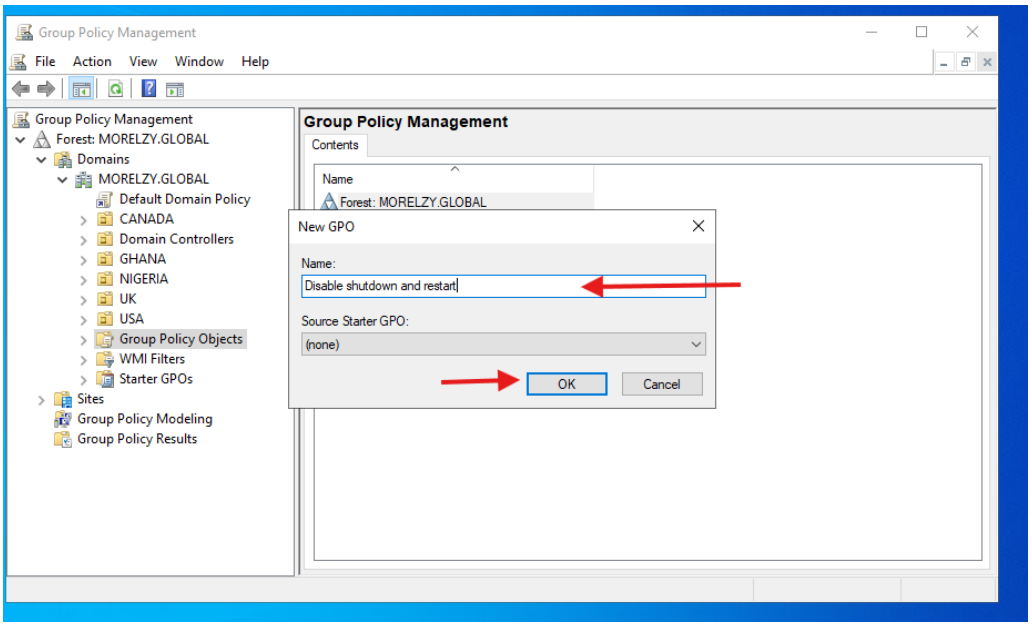
On the windows sever manager dashboard, select tools and click Group policy management



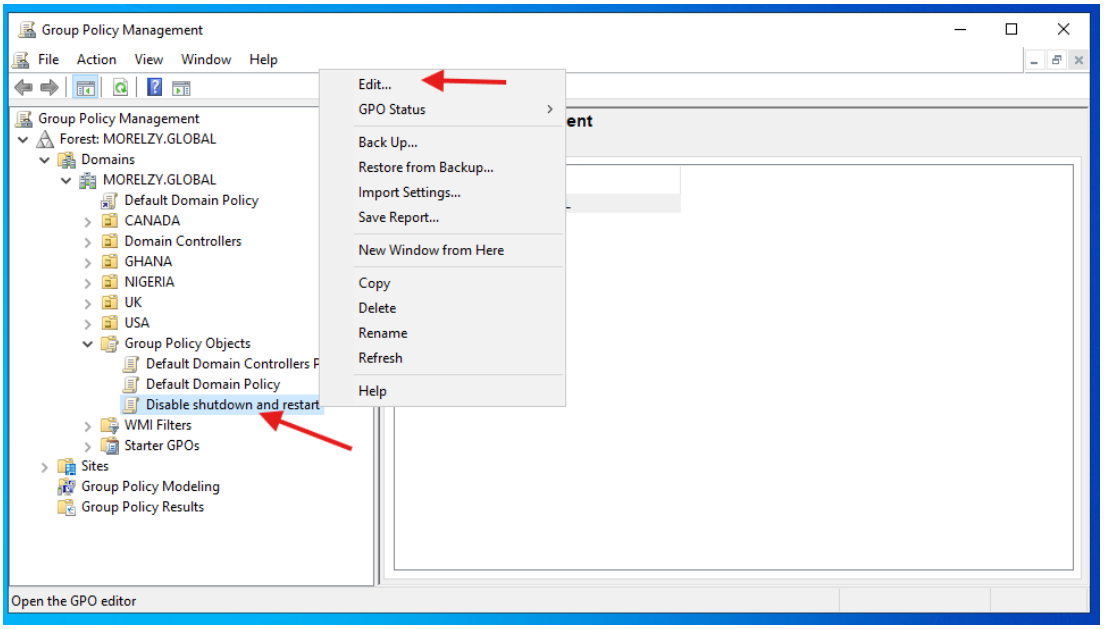
Select company domain>> right click group policy object>> select new



Create a name for the GPO and click ok



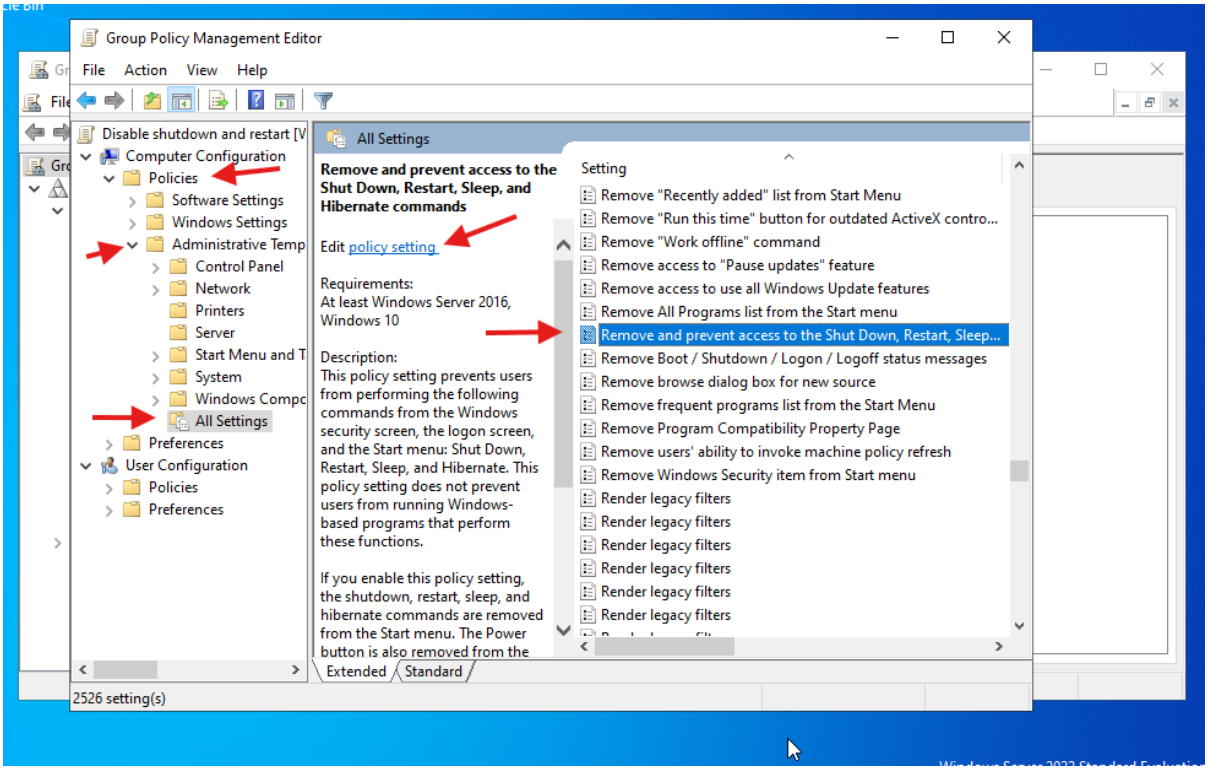
Now, we right cick on the GPO we created and click on edit to add the policy



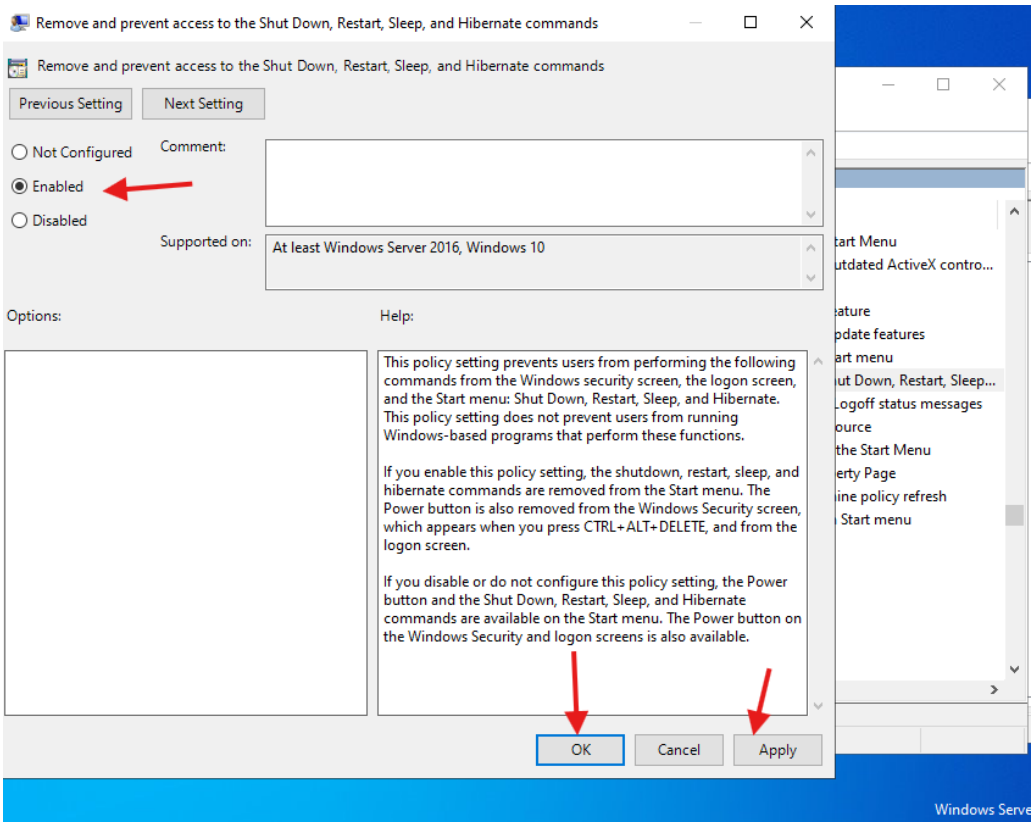
Depending on what we are trying to achieve, we can create the policy on either COMPUTER CONFIGURATION or USER CONFIGURATION, it can also be done on both.

Under Computer config, expand Policies, expand Adminstrative templates, select all settings.

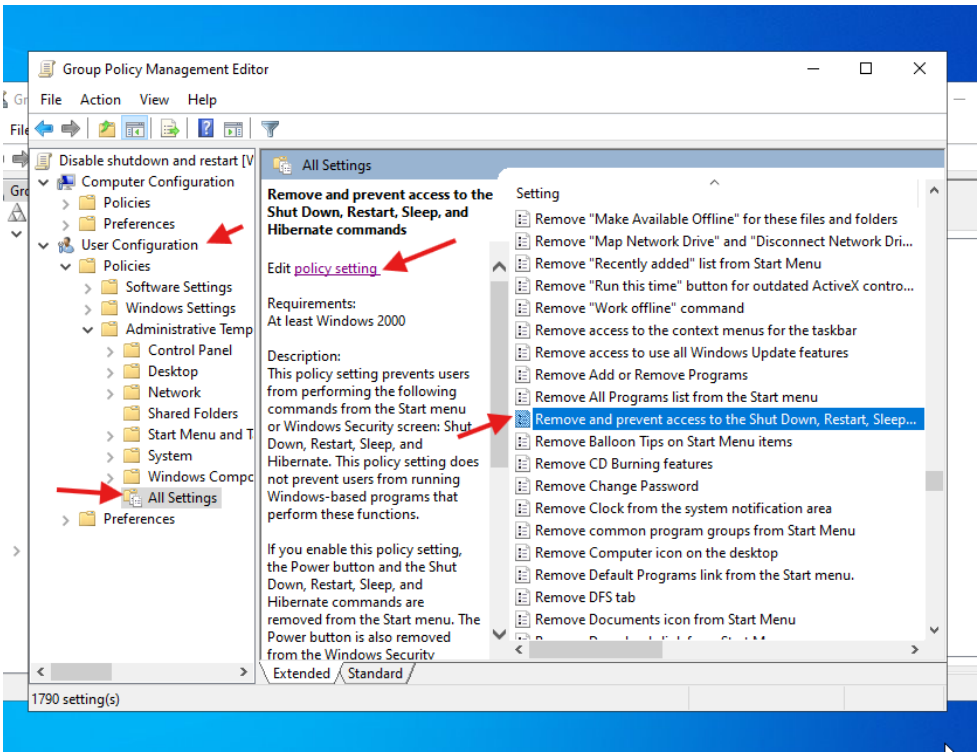
Locate the setting requires(in this example, we will go with removing access to shutdown, restart, sleep and hibernate) the click on edit policy setting



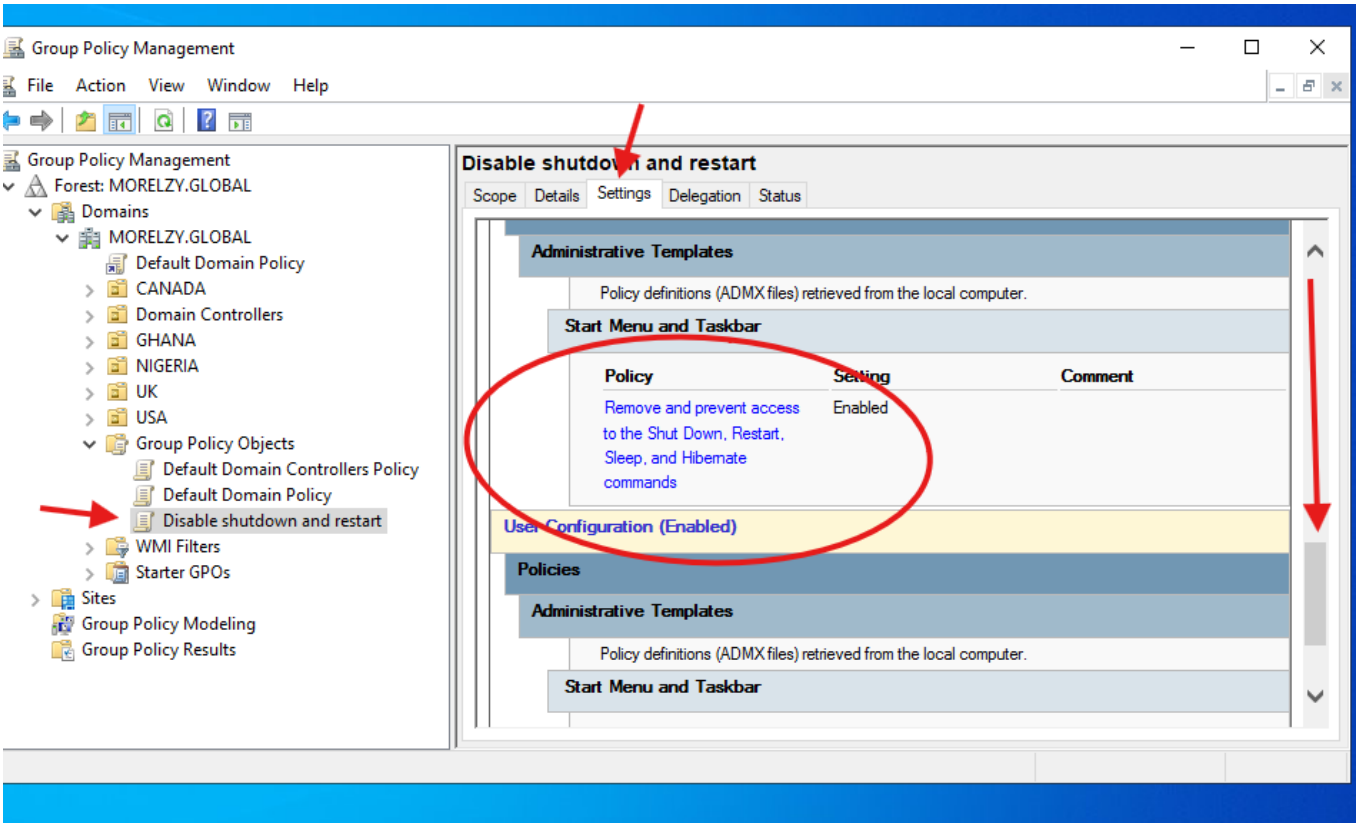
Check Enable, click on apply and click OK



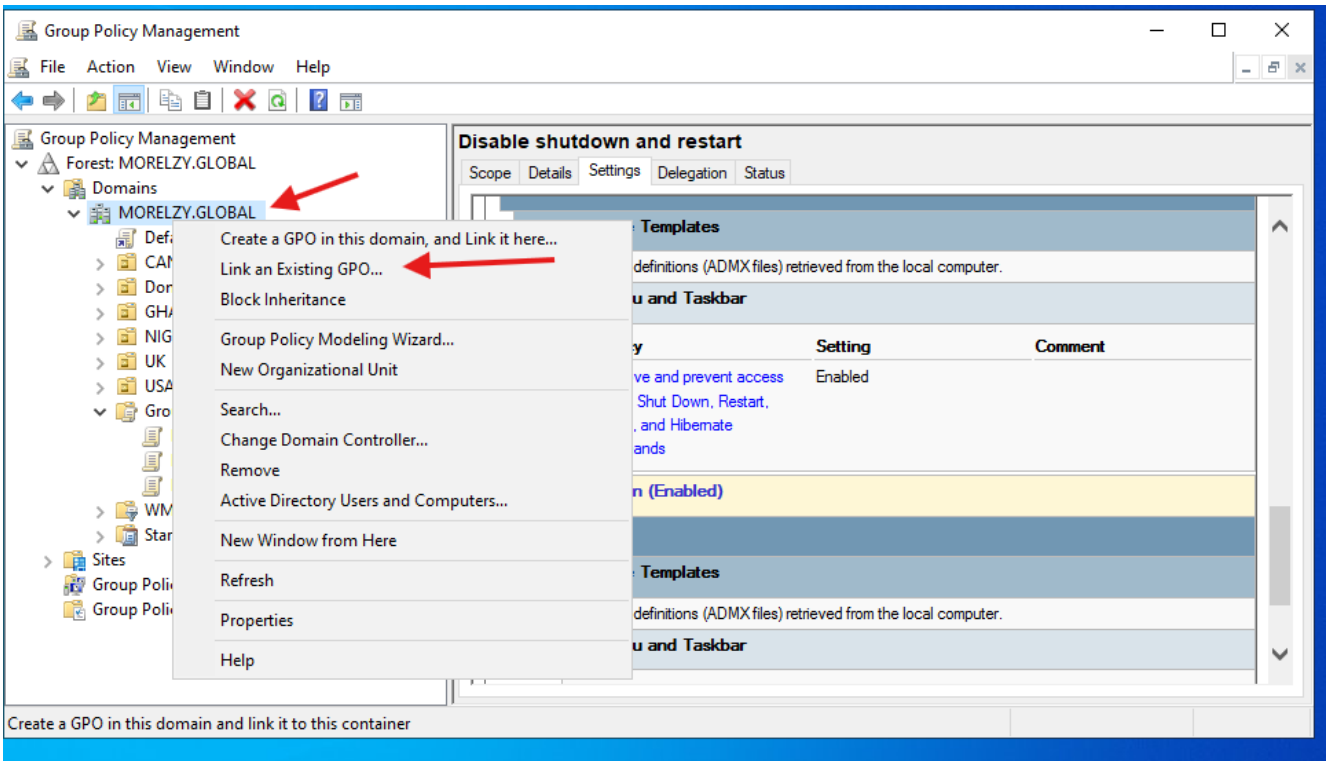
Repeat same steps for USER CONFIG

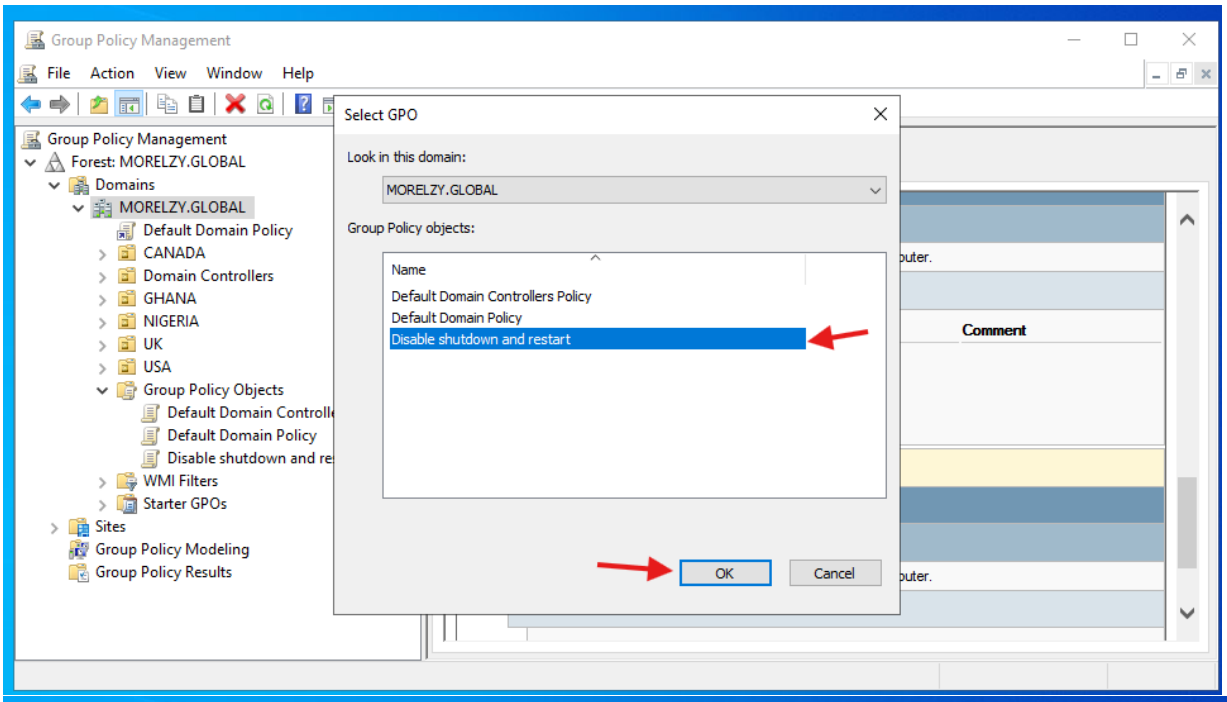


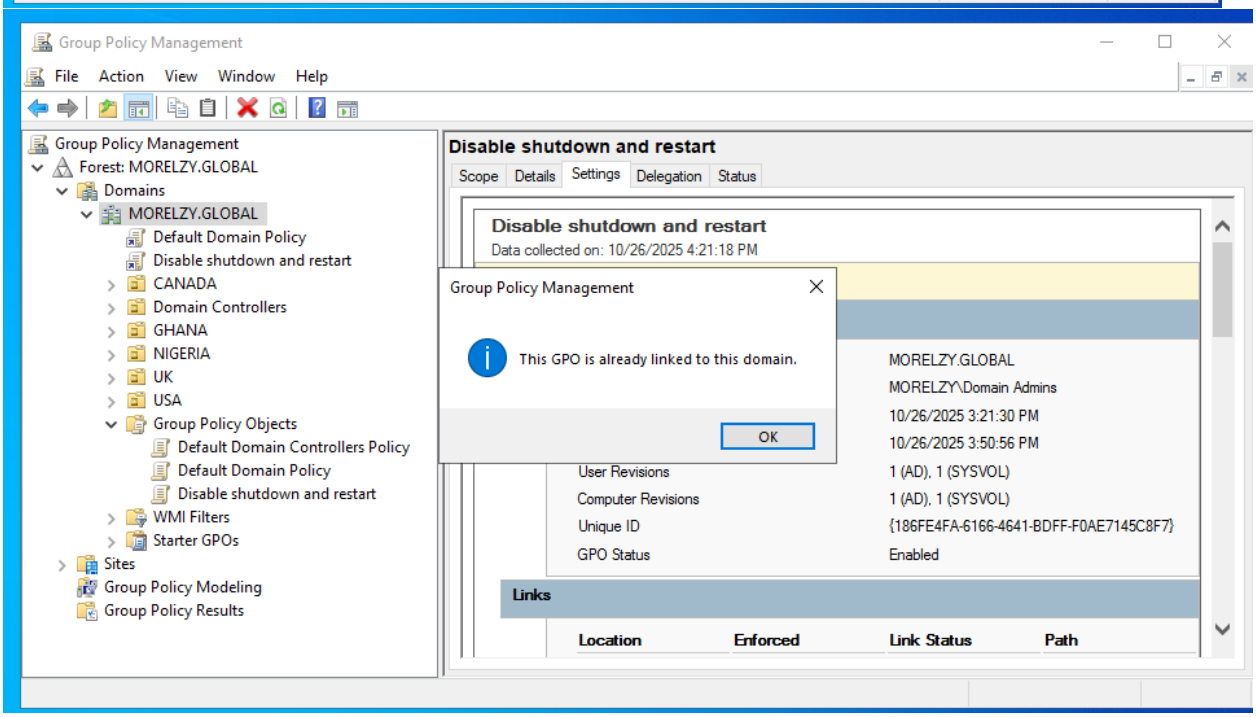
Confirm on GPO to see if policy was added



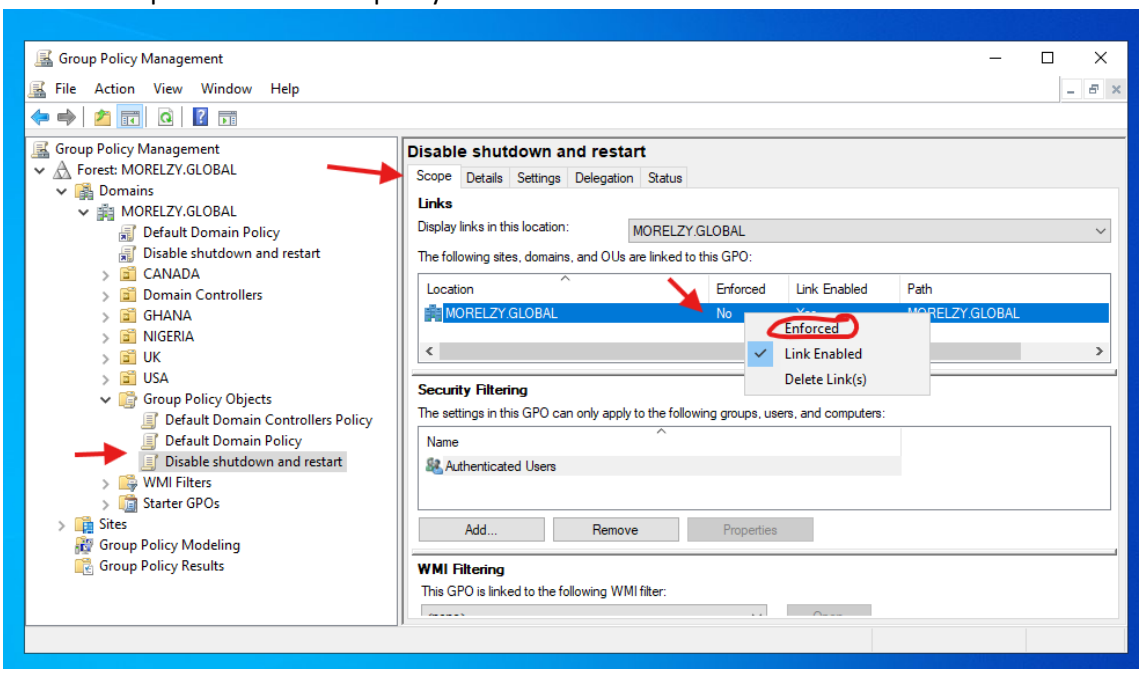
Next we link the GPO to our domain



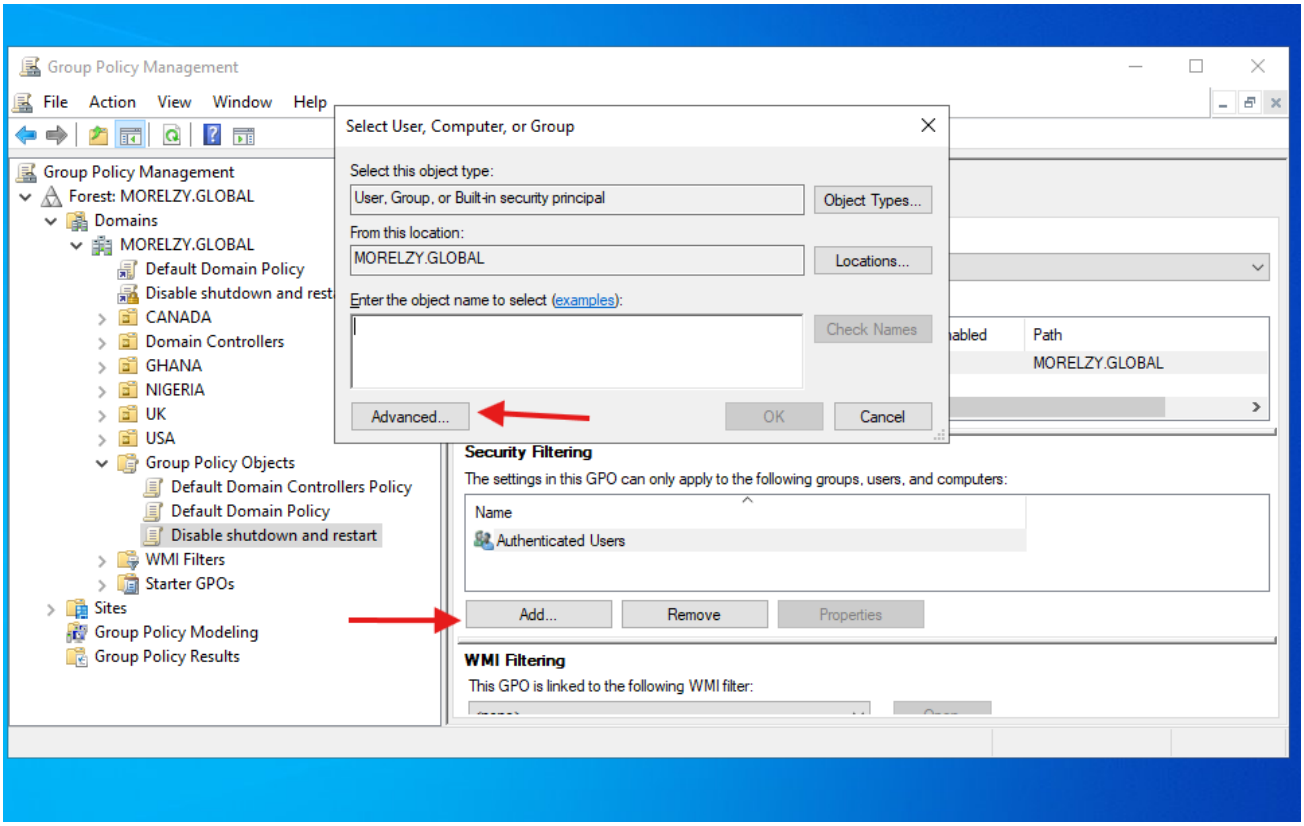

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: MORELZY.GLOBAL
Domains
MORELZY.GLOBAL
Default Domain Policy
CANADA
Domain Controllers
GHANA
NIGERIA
UK
USA
Group Policy Objects
Default Domain Policy
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Select GPO
Look in this domain:
MORELZY.GLOBAL
Group Policy objects:
Name
Default Domain Controllers Policy
Default Domain Policy
Disable shutdown and restart
OK
Cancel
Comment

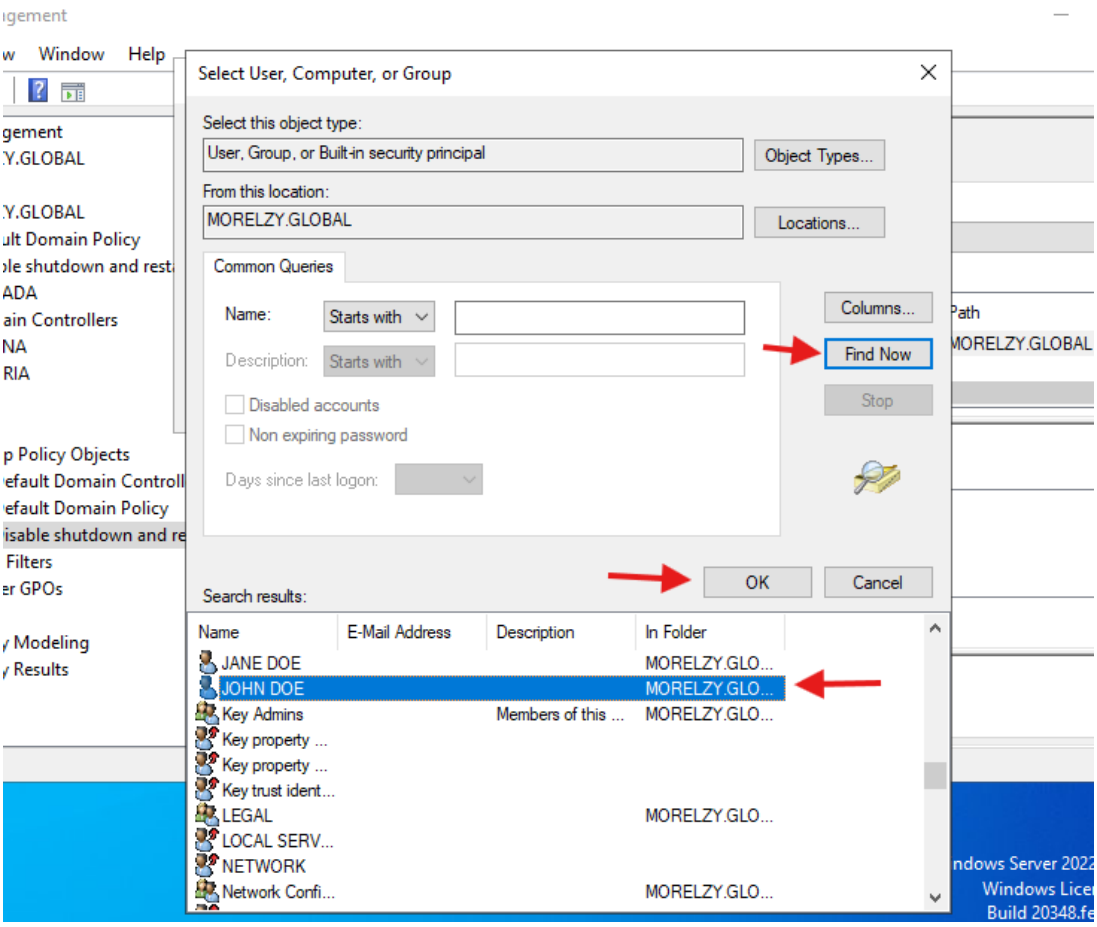

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: MORELZY.GLOBAL
Domains
MORELZY.GLOBAL
Default Domain Policy
Disable shutdown and restart
CANADA
Domain Controllers
GHANA
NIGERIA
UK
USA
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
Disable shutdown and restart
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Disable shutdown and restart
Scope Details Settings Delegation Status
Disable shutdown and restart
Data collected on: 10/26/2025 4:21:18 PM
Group Policy Management
This GPO is already linked to this domain.
OK
MORELZY.GLOBAL
MORELZY\Domain Admins
10/26/2025 3:21:30 PM
10/26/2025 3:50:56 PM
User Revisions
1 (AD), 1 (SYSVOL)
Computer Revisions
1 (AD), 1 (SYSVOL)
Unique ID
{186FE4FA-6166-4641-BDFF-F0AE7145C8F7}
GPO Status
Enabled
Links
Location
Enforced
Link Status
Path

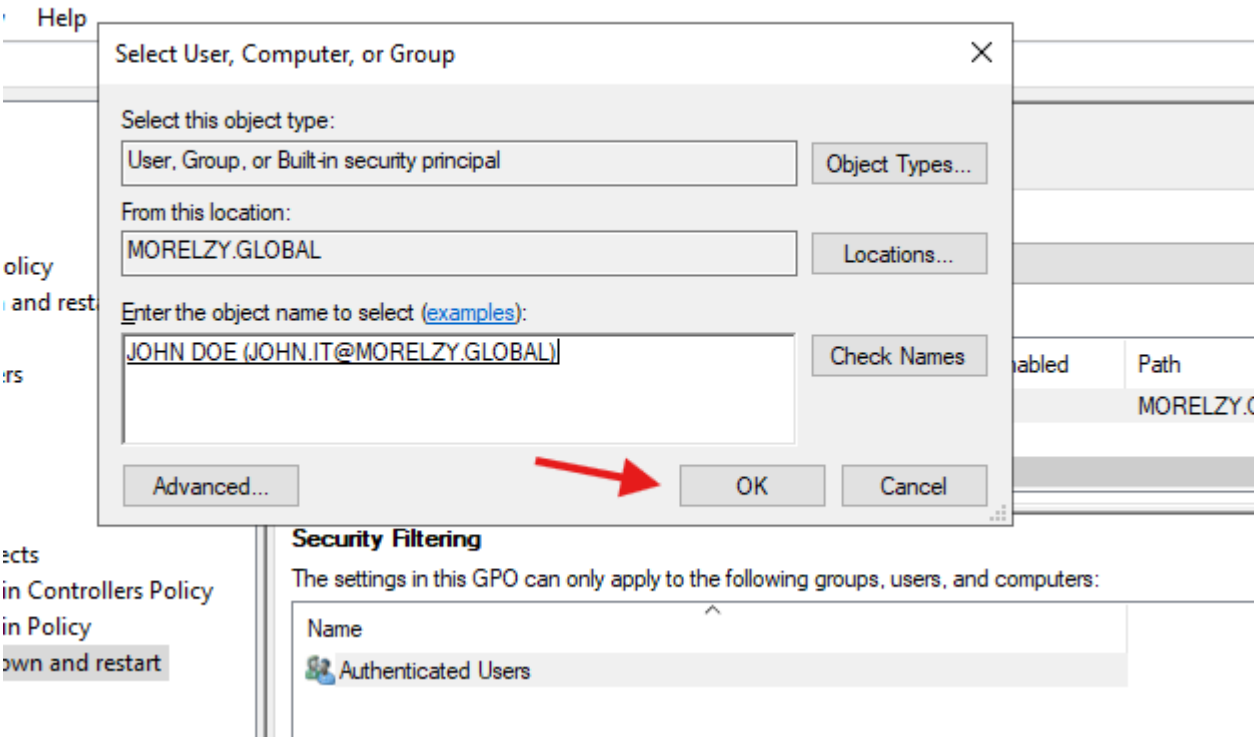
Our next step is to enforce the policy

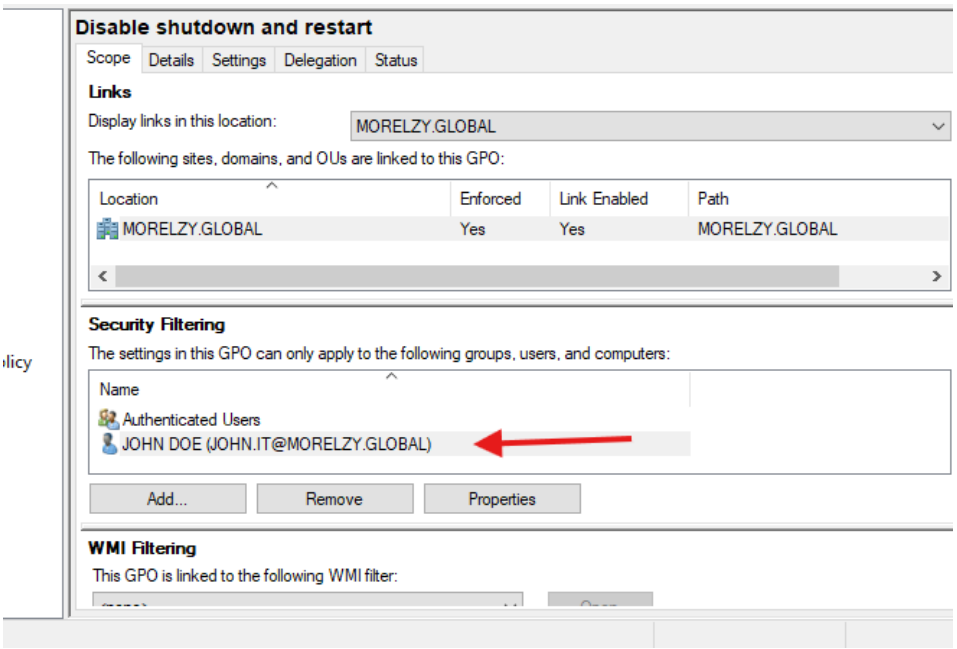


Then we add user to the policy




Window
Help
Select User, Computer, or Group
Select this object type:
User, Group, or Built-in security principal
Object Types...
From this location:
MORELZY.GLOBAL
Locations...
Common Queries
Name:
Starts with
Description:
Starts with
Disabled accounts
Non expiring password
Days since last logon:
Columns...
Find Now
Stop
OK
Cancel
Search results:
Name
E-Mail Address
Description
In Folder
JANE DOE
MORELZY.GLO...
JOHN DOE
MORELZY.GLO...
Key Admins
Members of this ...
MORELZY.GLO...
Key property ...
Key property ...
Key trust ident...
LEGAL
MORELZY.GLO...
LOCAL SERV...
NETWORK
Network Confi...
MORELZY.GLO...
Path
MORELZY.GLOBAL


Help
Select User, Computer, or Group
Select this object type:
User, Group, or Built-in security principal
Object Types...
From this location:
MORELZY.GLOBAL
Locations...
Enter the object name to select (examples):
JOHN DOE (JOHN.IT@MORELZY.GLOBAL)
Check Names
Advanced...
OK
Cancel
Path
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users



With that done, the policy is now active.

We can force the update manually on the users PC by running CMD “gpupdate /force” or simply boot the PC for it to take effect.

We can log in to confirm user has no access to shutdown or restart.