Installing and Hardening Active Directory (AD)

Active Directory Simulation

This project demonstrates the deployment, configuration, and basic hardening of a Windows Server Active Directory, Domain Services (AD, DS) environment for a simulated organization named CyberTech Solutions. The goal is to showcase core Windows Server administration, identity and access management (IAM), and Group Policy implementation in an enterprise style setup.

Project Overview

CyberTech Solutions is a small IT services firm with the following structure:

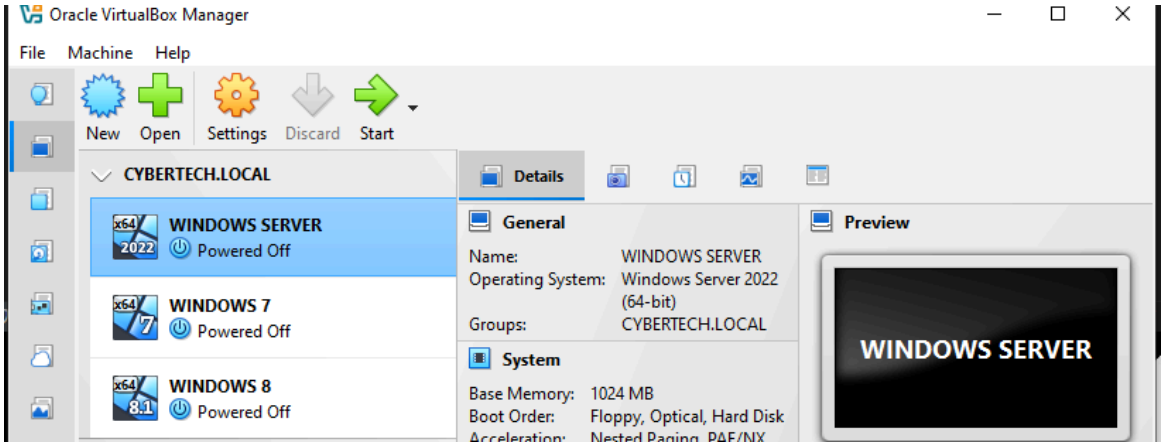
- 1 Windows Server (AD Domain Controller)
- 1 windows 8 Clients PC (HR)
- 1 Windows 7 Clients PC (IT)

The project covers:

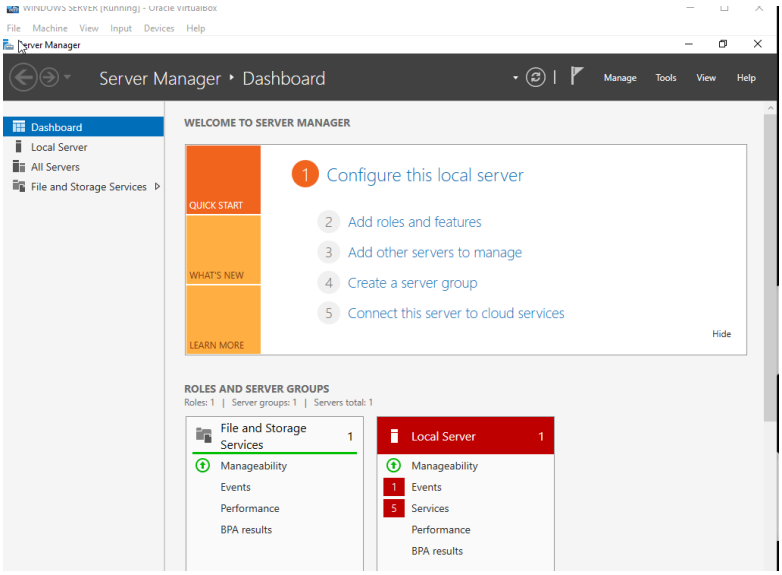
- Active Directory Domain controller installation and configuration.
- Client machines joined to the domain.
- Organizational Unit (OU) design.
- Group Policy Object (GPO) configuration.
- Basic Active Directory hardening practices.

- **Active Directory Domain Controller Installation and Configuration.**

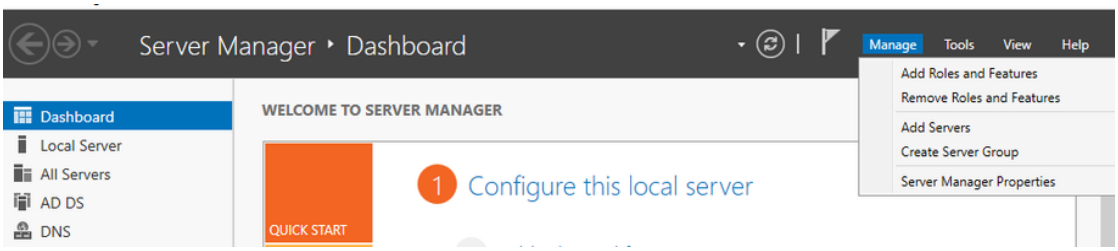
I started by creating 3 VMs (Windows server, windows 7 and windows 8), where window server will server as the company windows server which will be used to control other windows or users. The two other VMs (Windows 7 & 8) will be the user. All 3 VMs are put under the same subnet and same group.



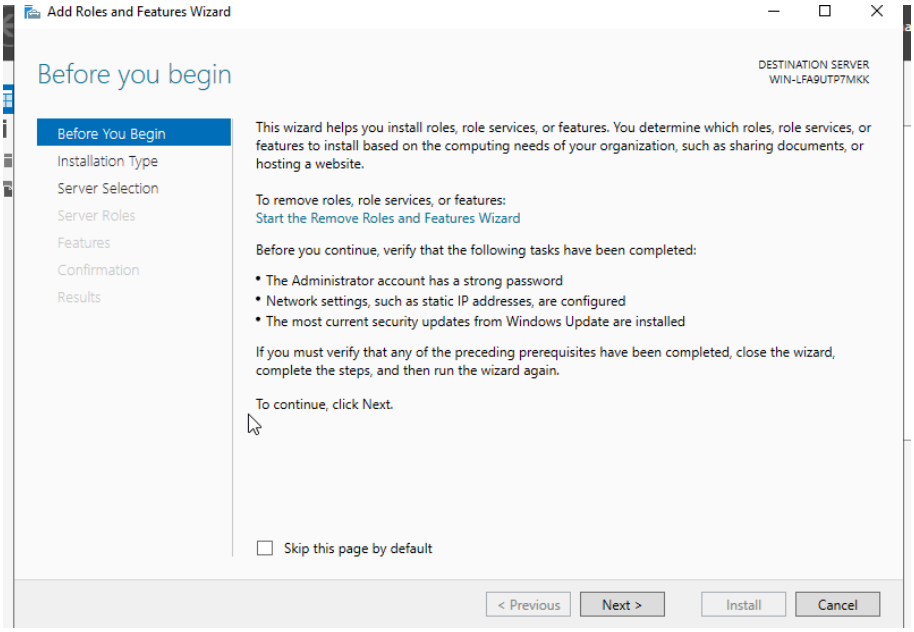
The window server was lunched and I installed an Active Directory on the server.



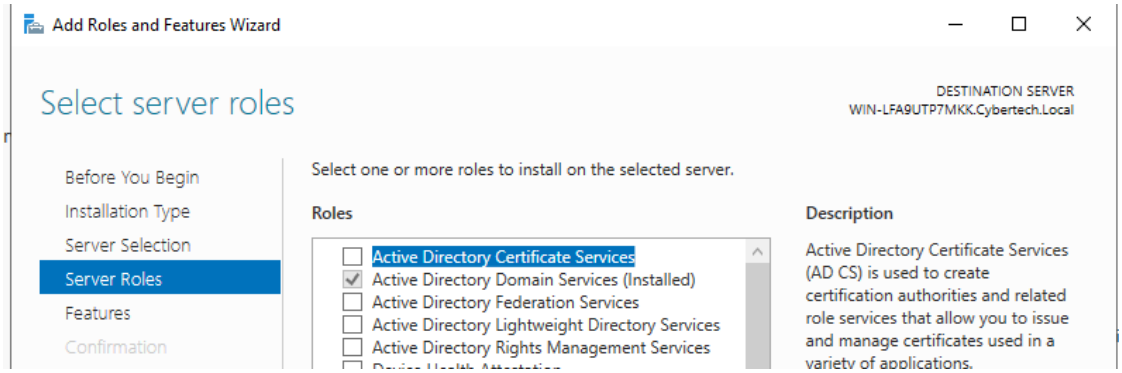
I clicked on “manage”



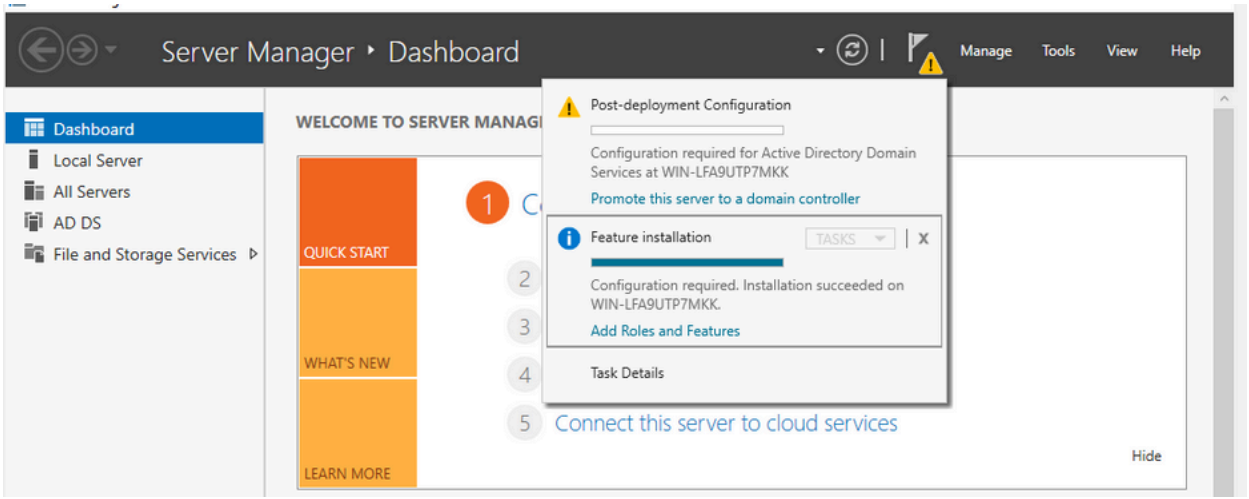
Then I clicked on “add roles and features”



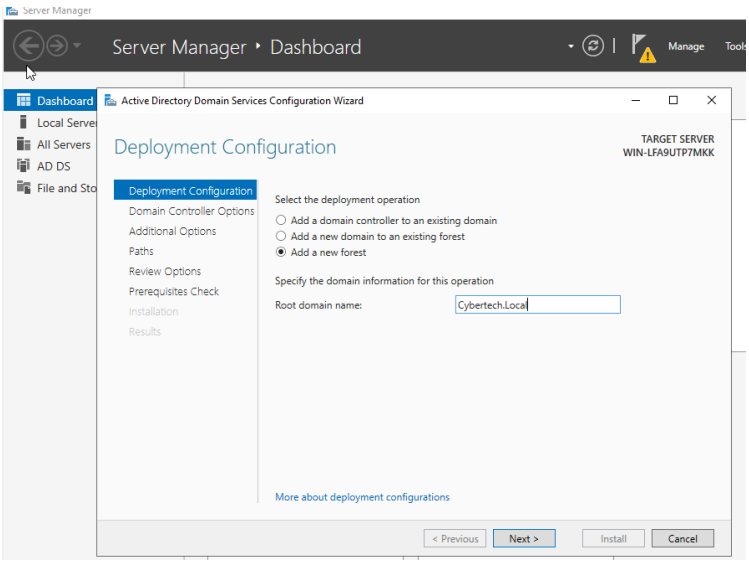
I selected “Active Directory Domain Service” and installed it



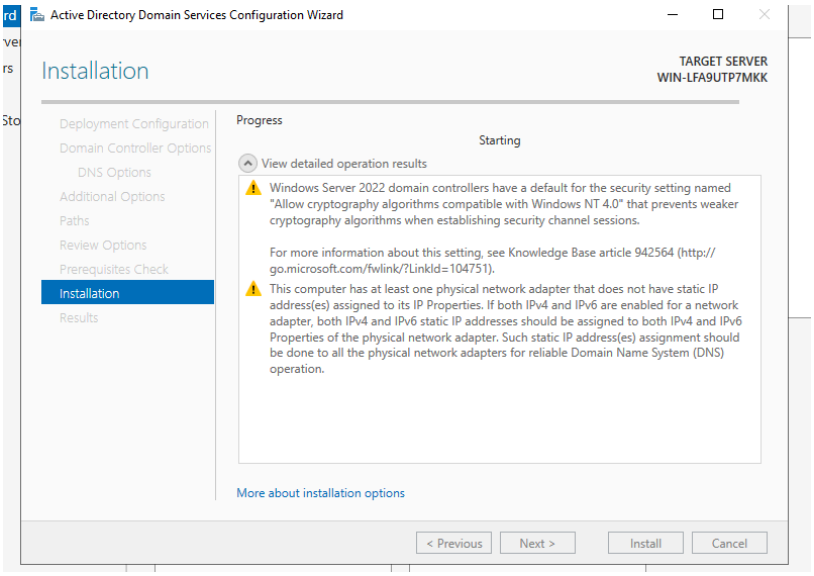
After the installation of the Active Directory Domain Server, I promoted the server to a domain controller.



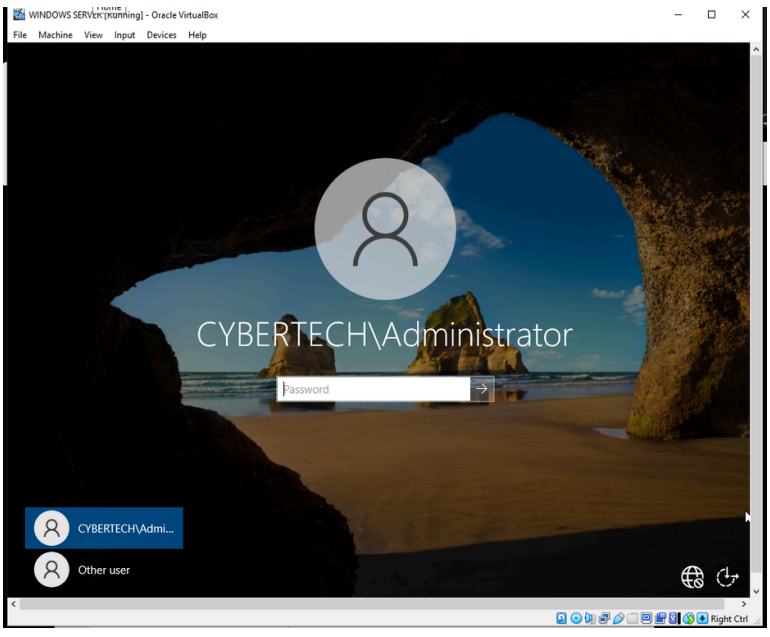
I select “add a new forest” and gave it a domain name (Cybertech.Local) which is the name of the organization.



After Installation was done, the system restart automatically and we were able to sign on as an administrator with the password I had configured the domain controller with.

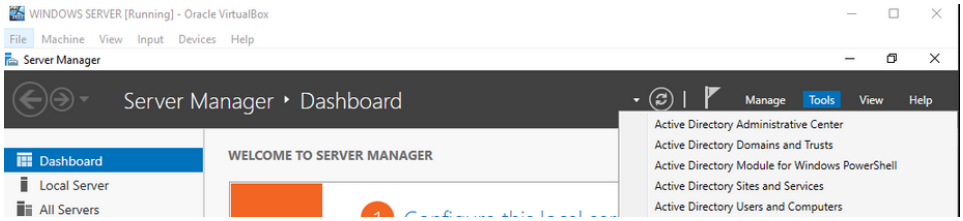


Logging in as an administrator.

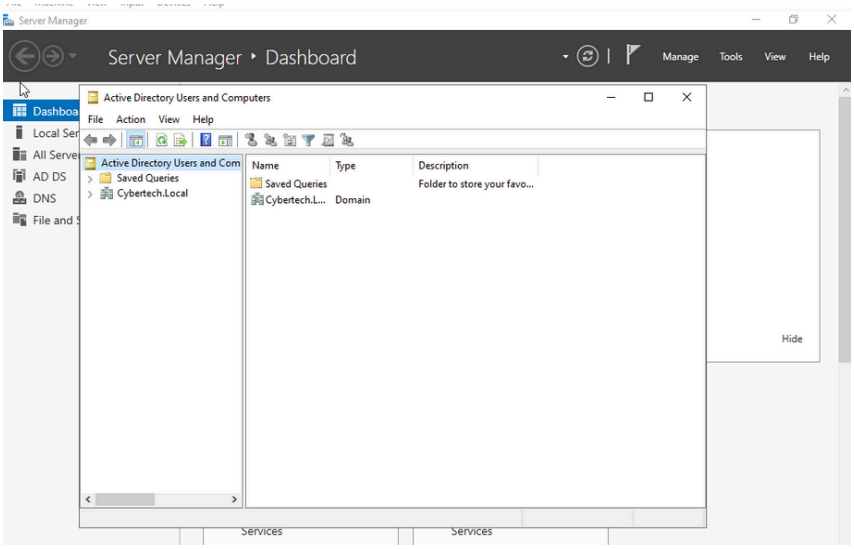


- **Organizational Units (OU) Creation and assigning user to VMs**

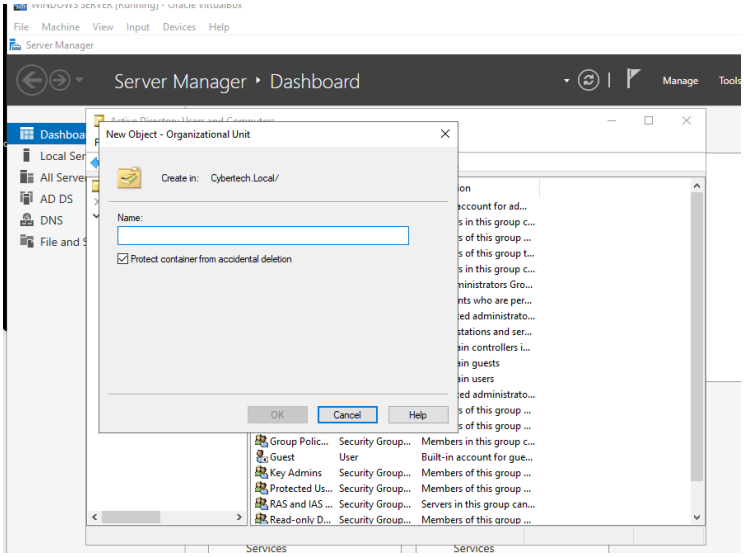
In the server manager, I clicked on the tools bar and clicked on Active Directory and computers



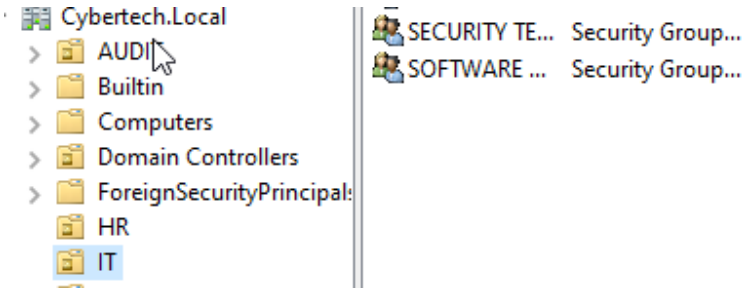
Once it appeared, I can see the Cybertech.Local server.



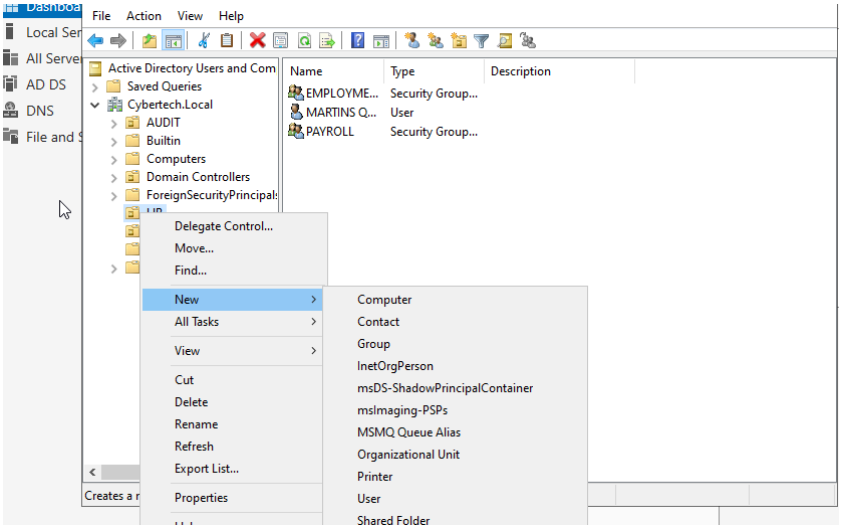
I right clicked on the Cybertech. Local server, and clicked on new and select the Organizational Unit option



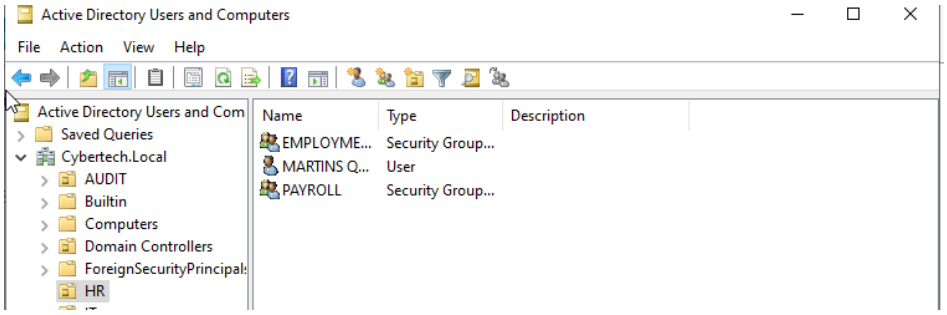
I created two organizational unit named HR & IT



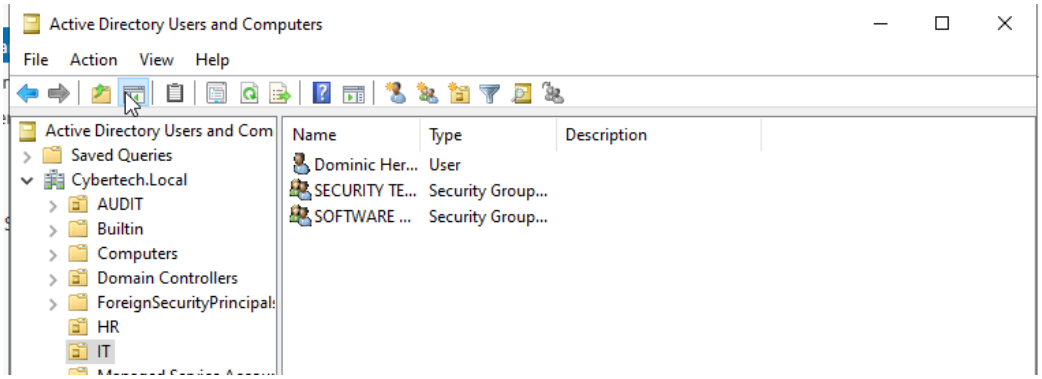
Under each Organization Unit, I created a group and also a user. I right clicked on the HR OU I created and selected new and chose group.



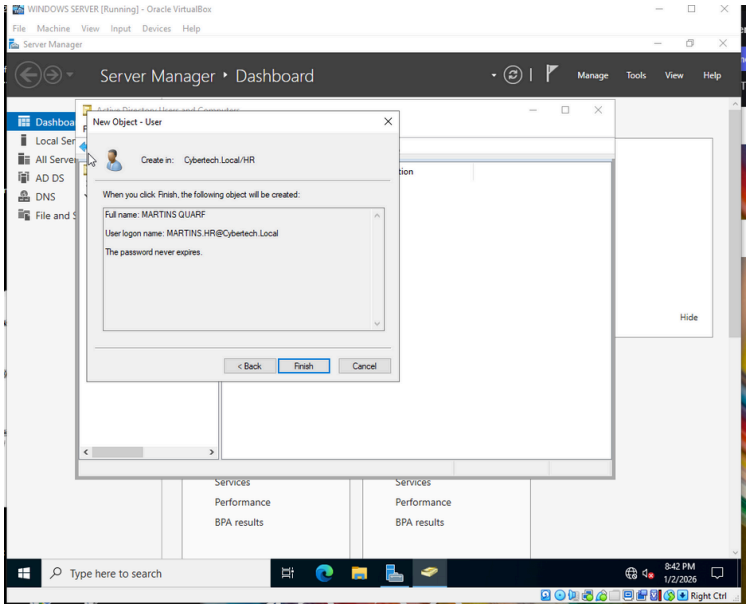
I created “Employment Documents” and “ Payroll” group under the HR OU,

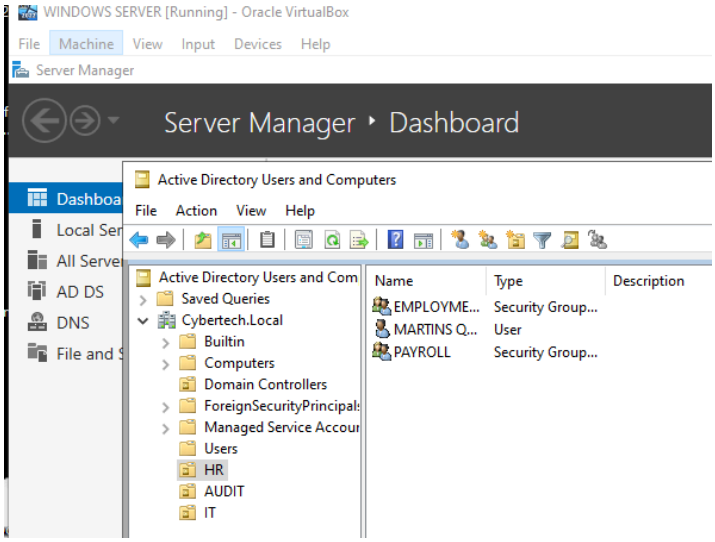


I created “Security Team” and “Software Team” groups.

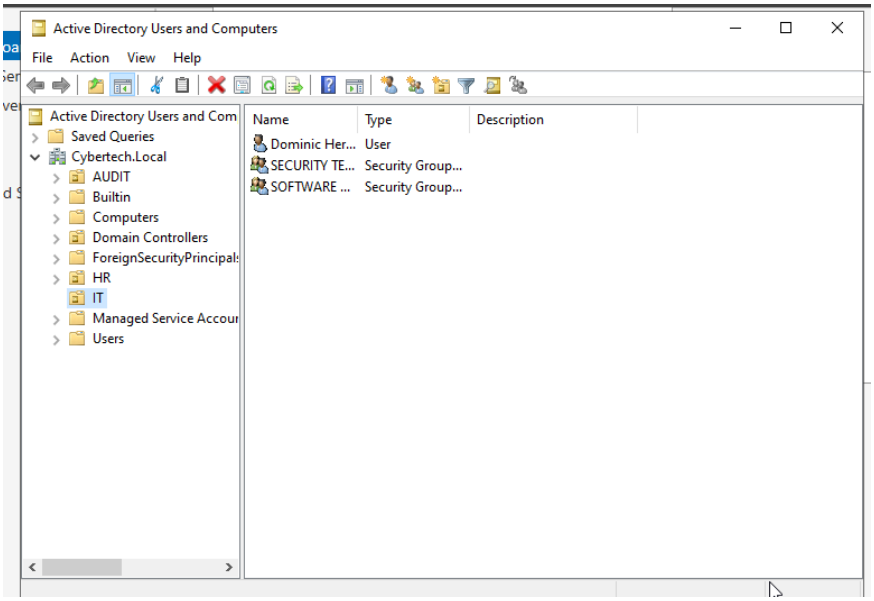


After creating groups, I created user for each group. For the HR, I created Martins Quarf and under the IT, I created Dominc Herdenson. I right clicked on the HR and clicked on new and select “user”





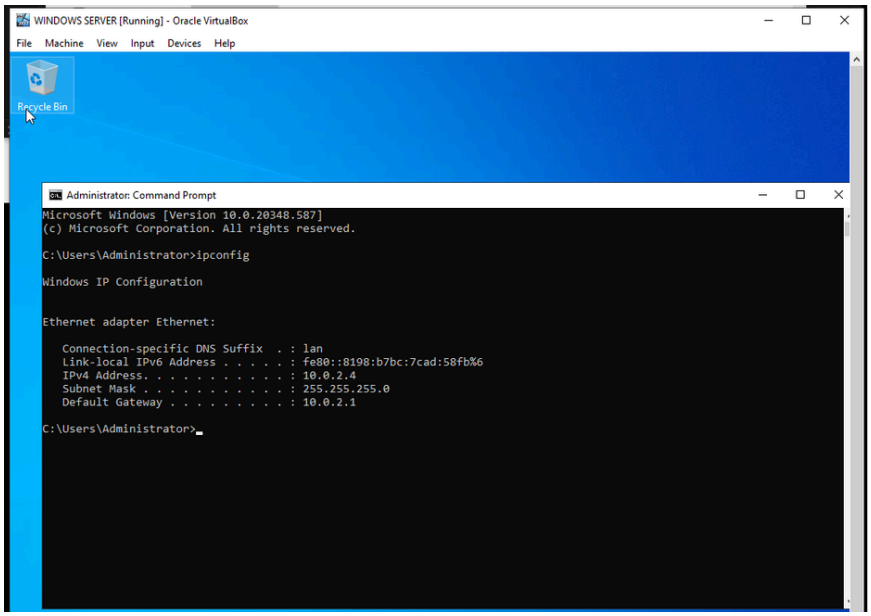
I repeated the same steps for IT and both users can be seen.



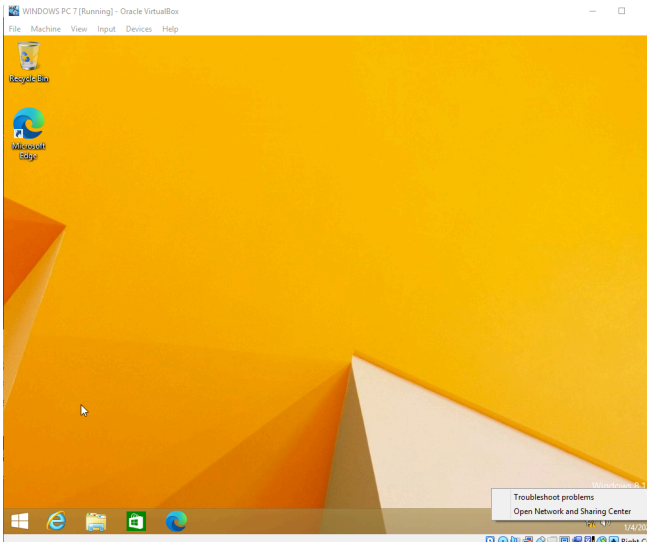
- **Client Machines joined to the main domain server.**

Next thing I want to do is configure the user and link them together on the other two VMs (windows 7 &8) I created.

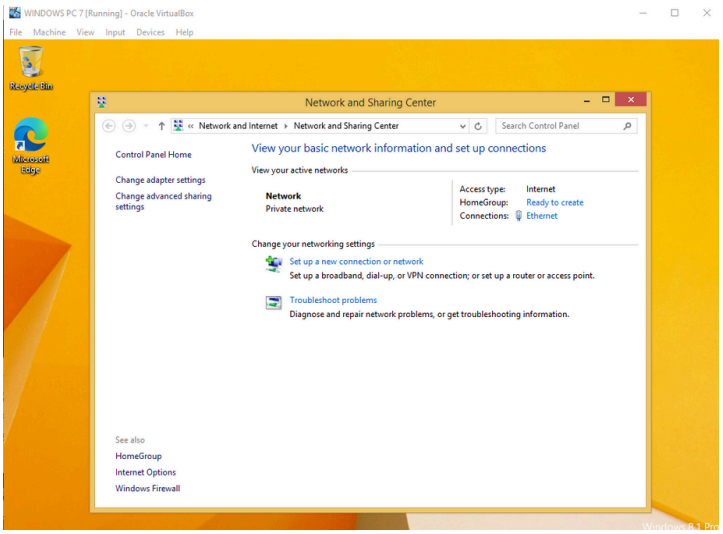
The first thing I did was to generate the IP address of the main server. Using the CMD Prompt, I typed “IPCONFIG” to get the IP address of the main server.

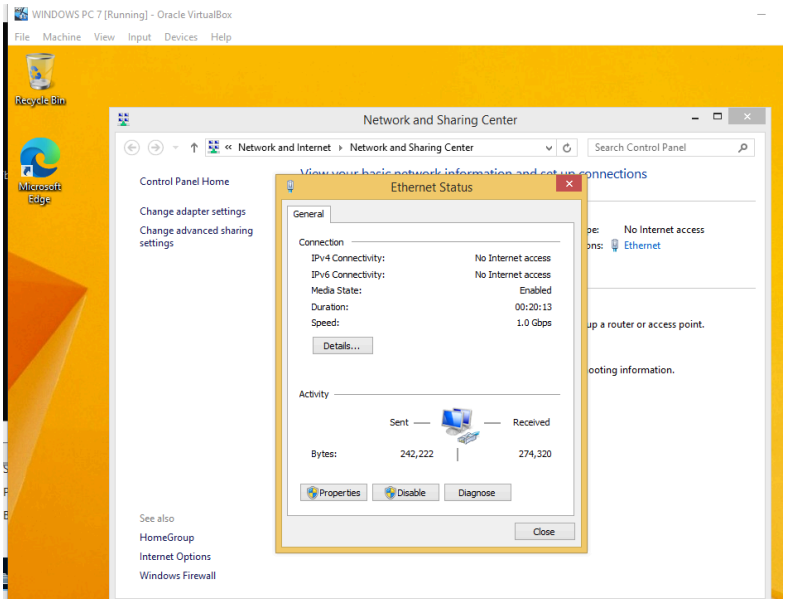


After that, I lunched my Windows 7, and I firstly configure the network settings by right clicking on internet access at the right bottom

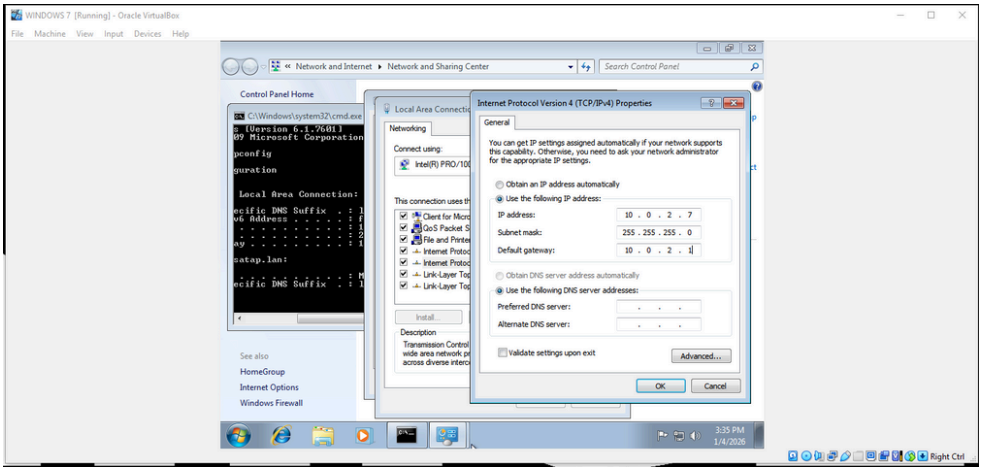


I clicked on “Open Network and sharing center” and I clicked on “Ethernet” then I clicked on “properties”



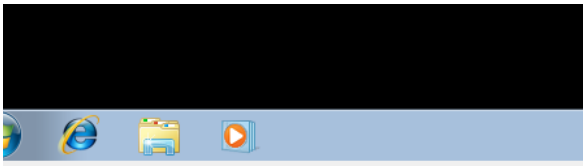


I selected the “internet protocol version 4 (TCP/IPV4) and I click on “properties” and I selected “use the following “IP address”. I got the IP address of the windows 7 itself and input it in the tabs. And I also input the IP address of the main server I already have in the “preferred DNS Server” tab and click ok.

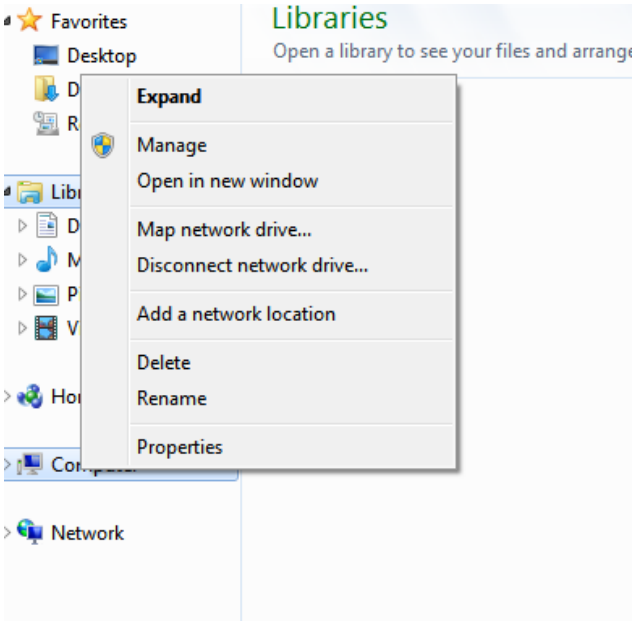


The next step is to assign user to the VM.

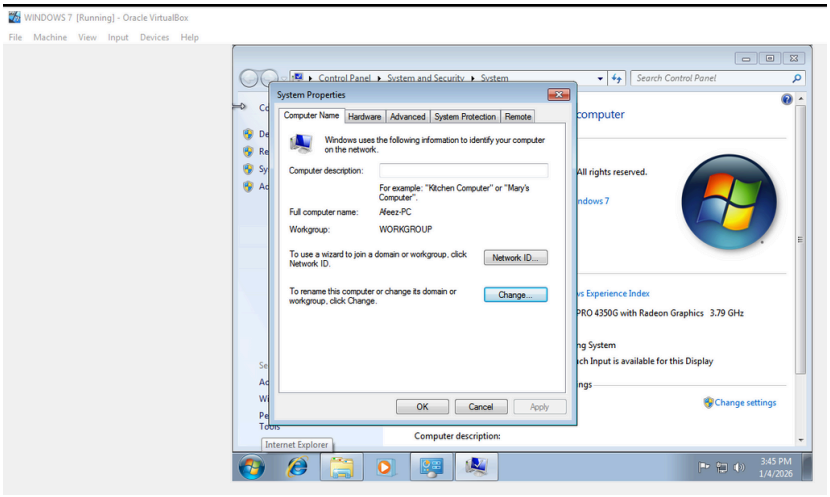
I clicked on the file explorer,

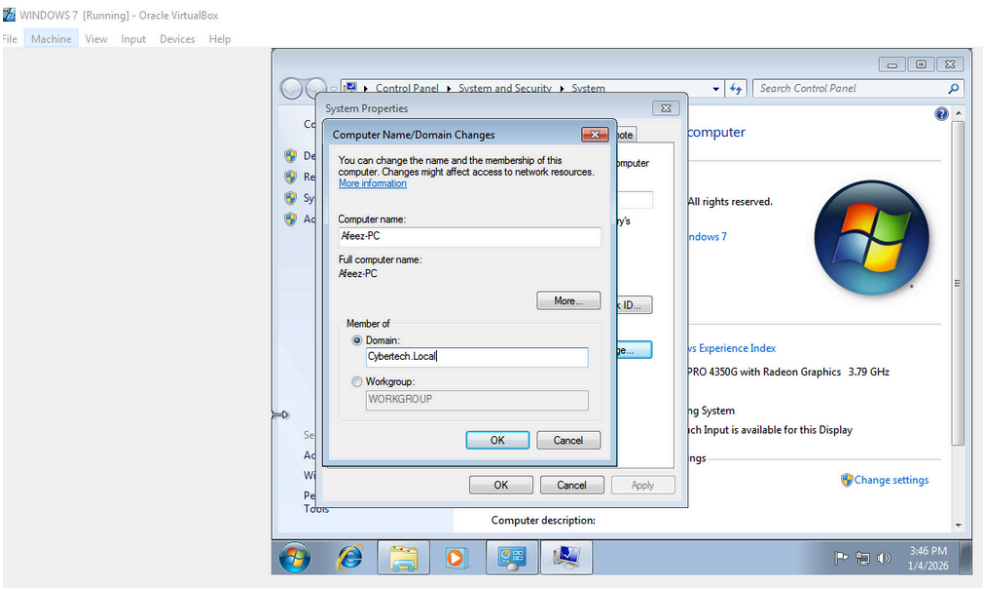


I right clicked on the “computer” and clicked on properties

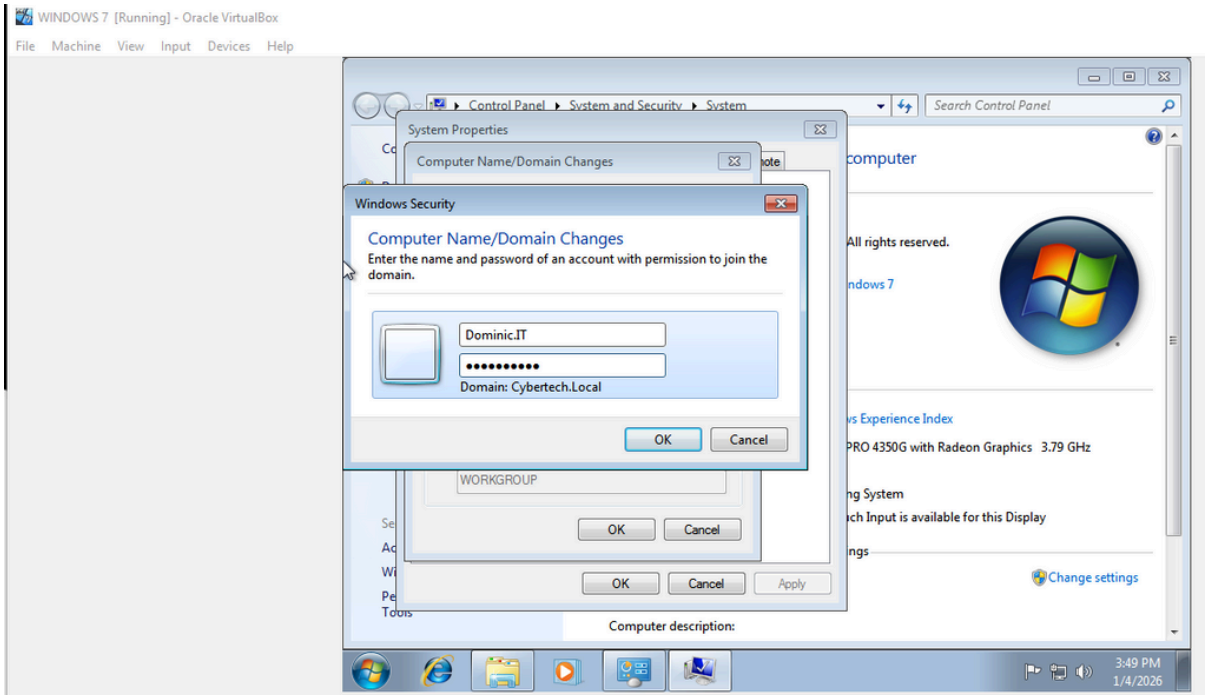


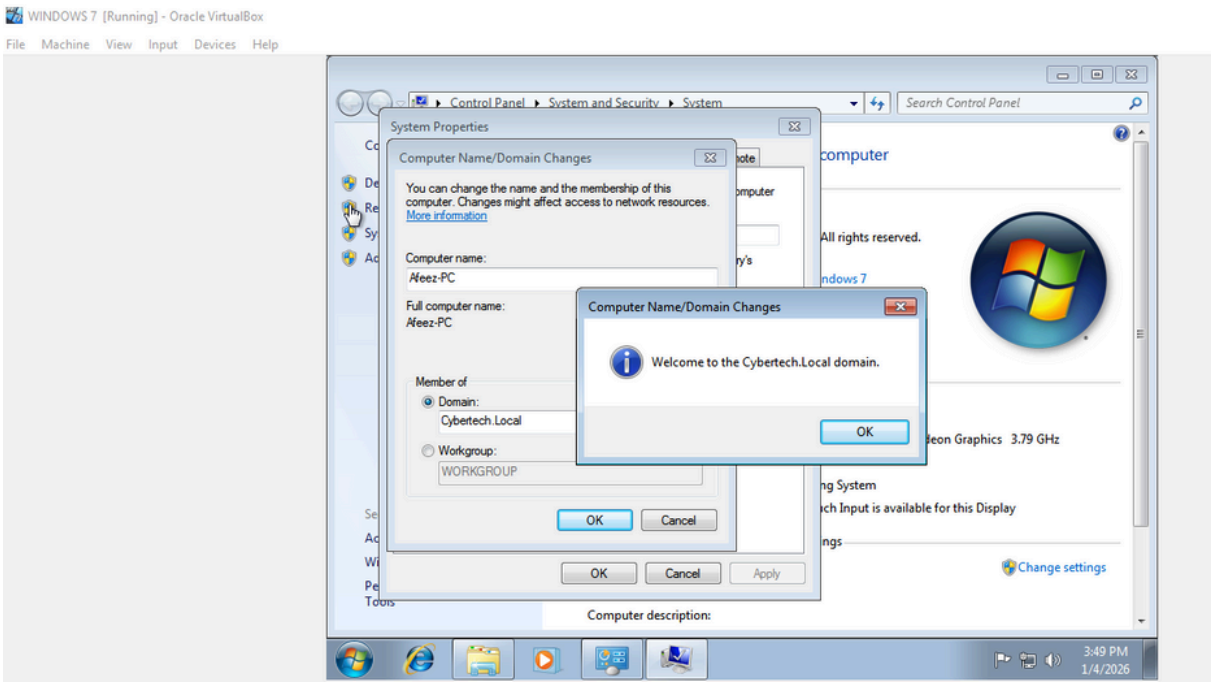
After, I clicked on system properties and I change the domain name to “Cybertech.Local”.



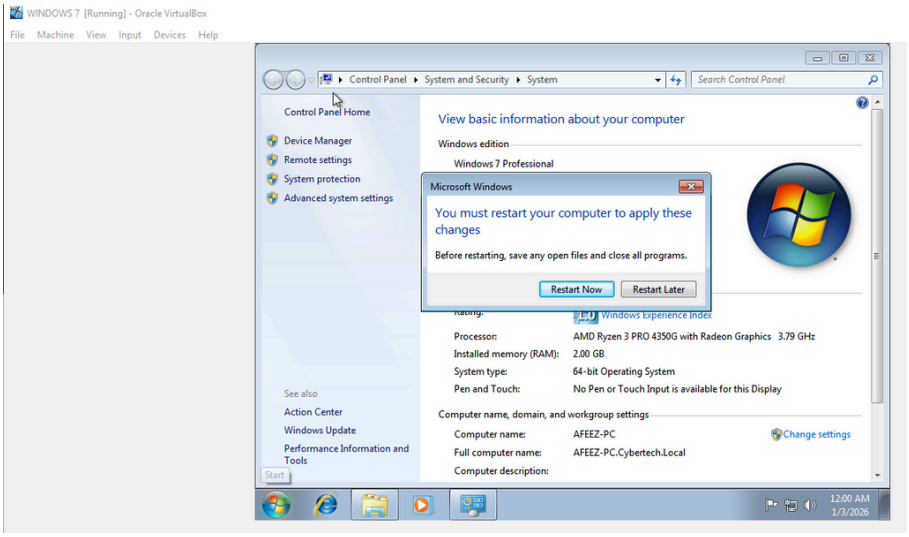


I input the username and password I created for the user under the IT Organizational Unit. I clicked OK and it display a successful connect to the domain.

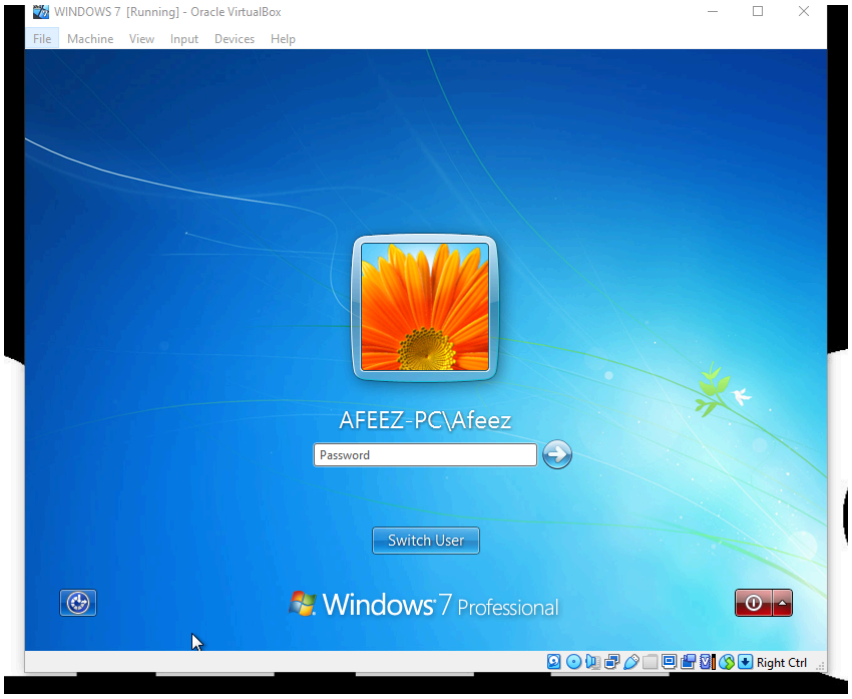


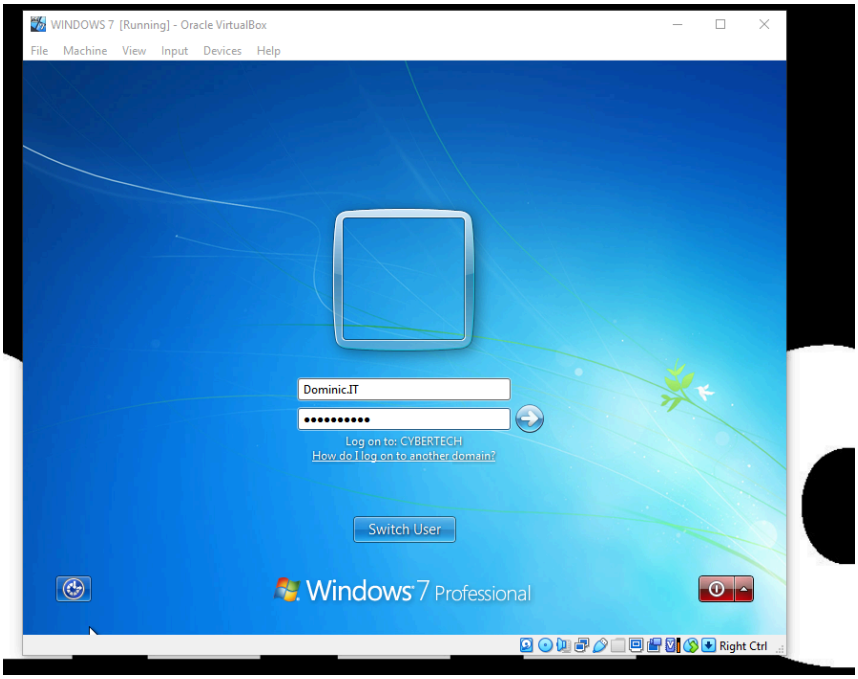


the system prompted for a restart and I clicked restart now.

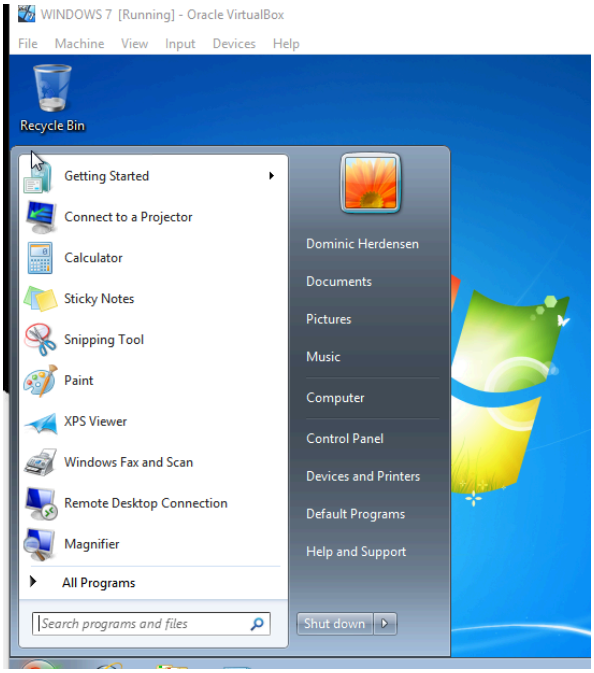


The VM restarted and it gave the option to switch user and I logged in the details of the user I assigned to the VM.





I logged in and the user I assigned to the VM was successfully logged on.



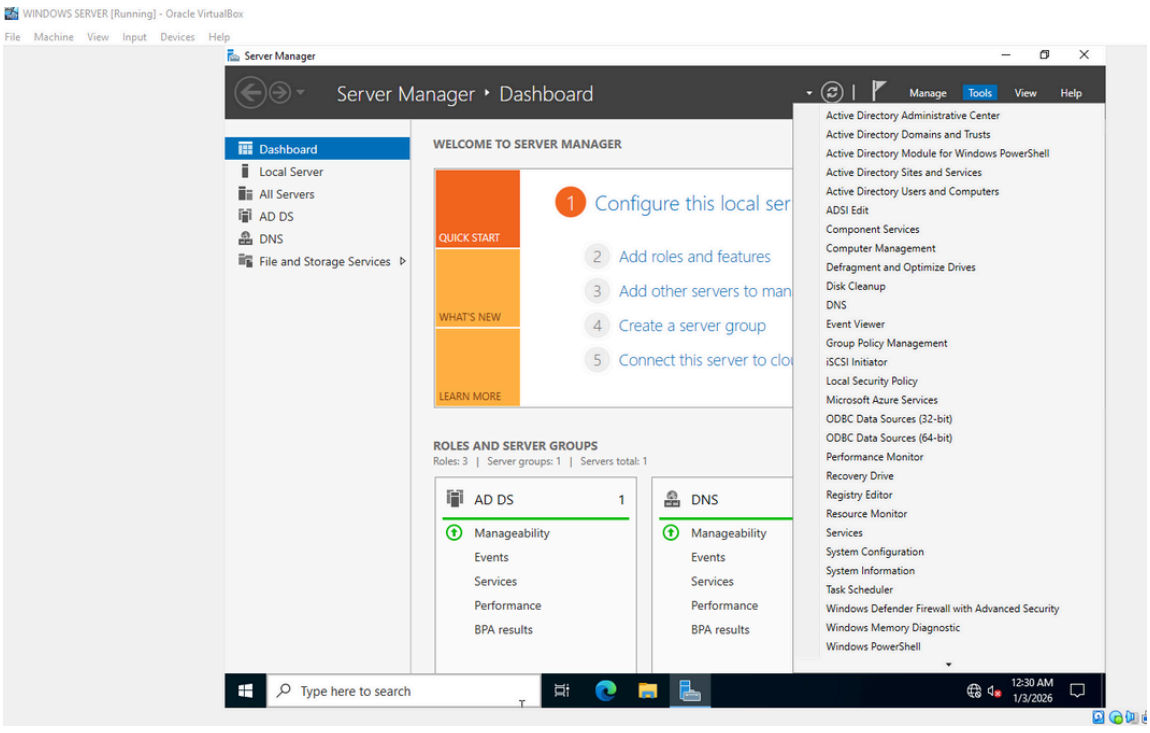
I did the same steps for windows 8 and assigned the other user on it as well.

- **Group Policy Object (GPO) configuration.**

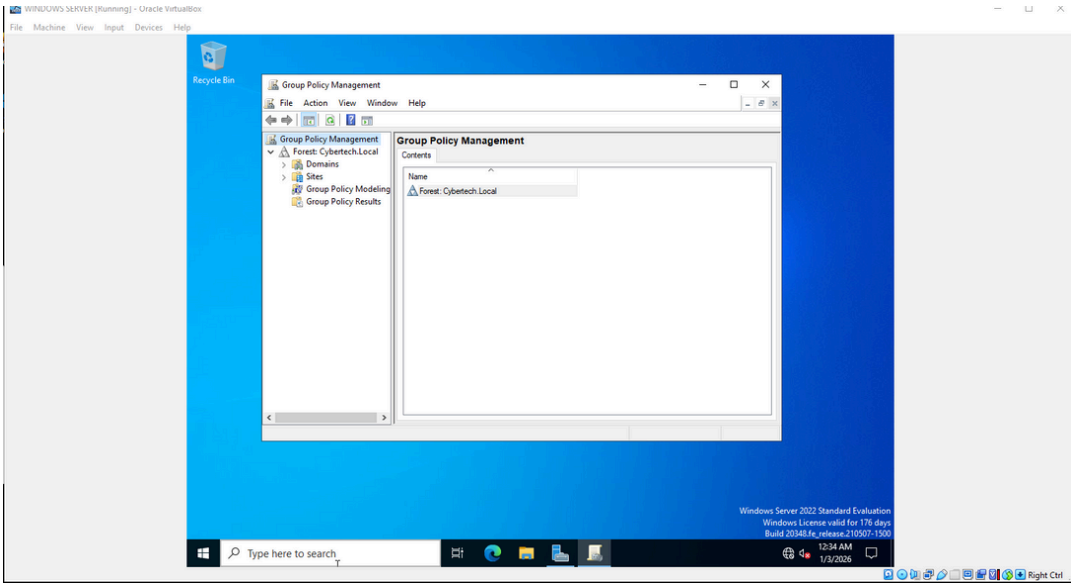
The next step I want to is to add a group policy. The policy will be to;

- [ ] Disable access to shut down
- [ ] Disable the restart access
- [ ] Disable all removeable storage device

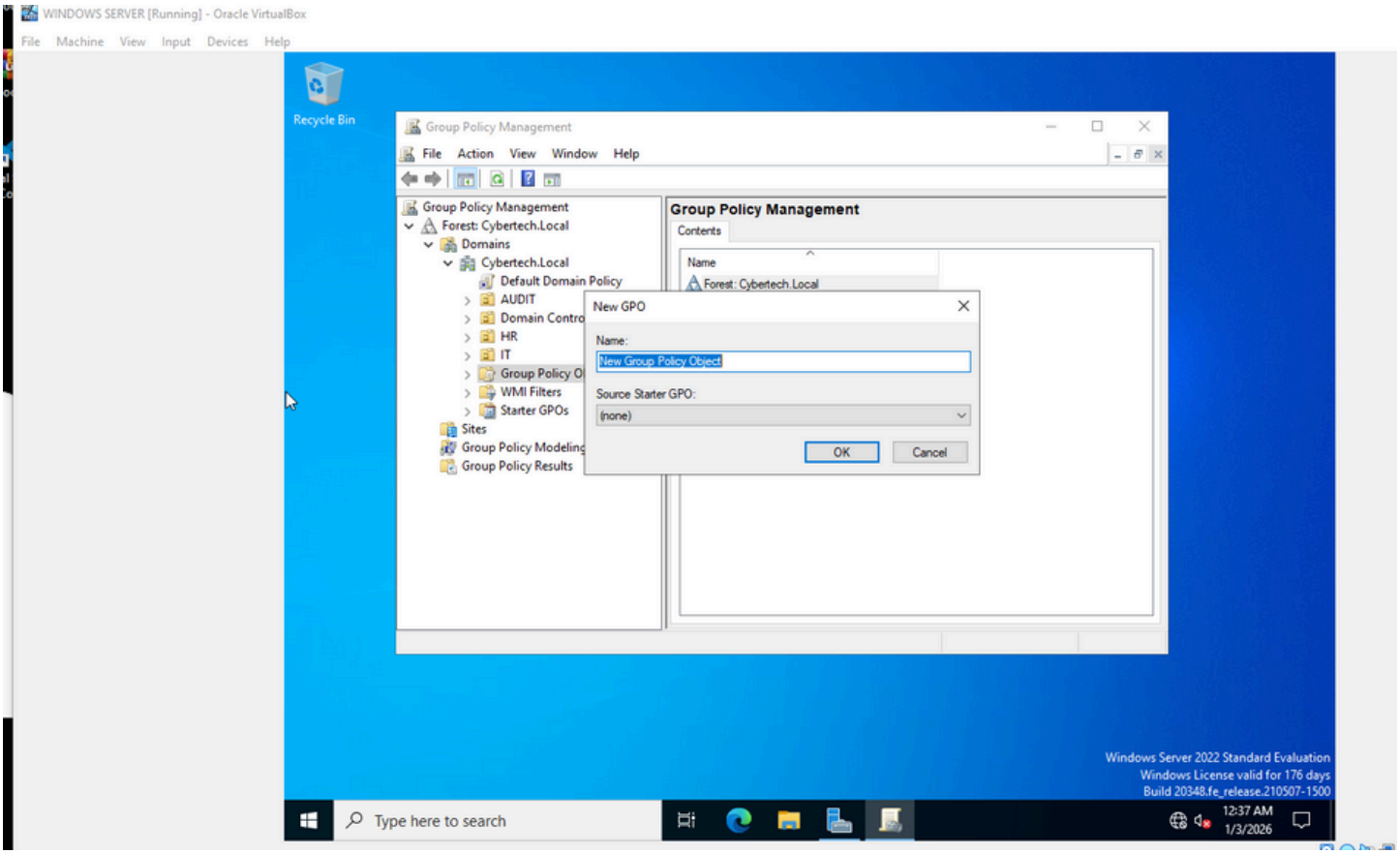
I will go on my main server under the server manager, I clicked on the “tools” tab and clicked on “Group Policy Management”.



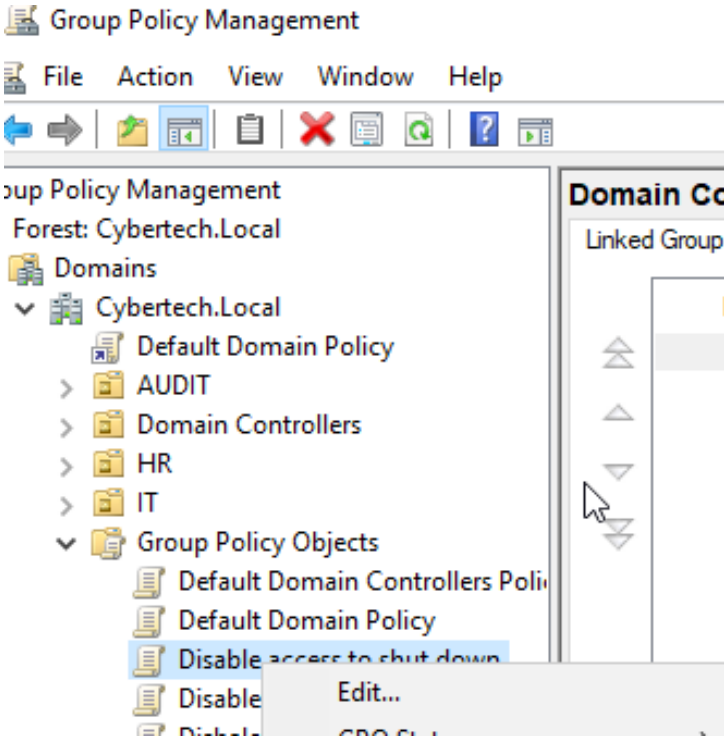
I clicked on the cyber tech forest and I expand it

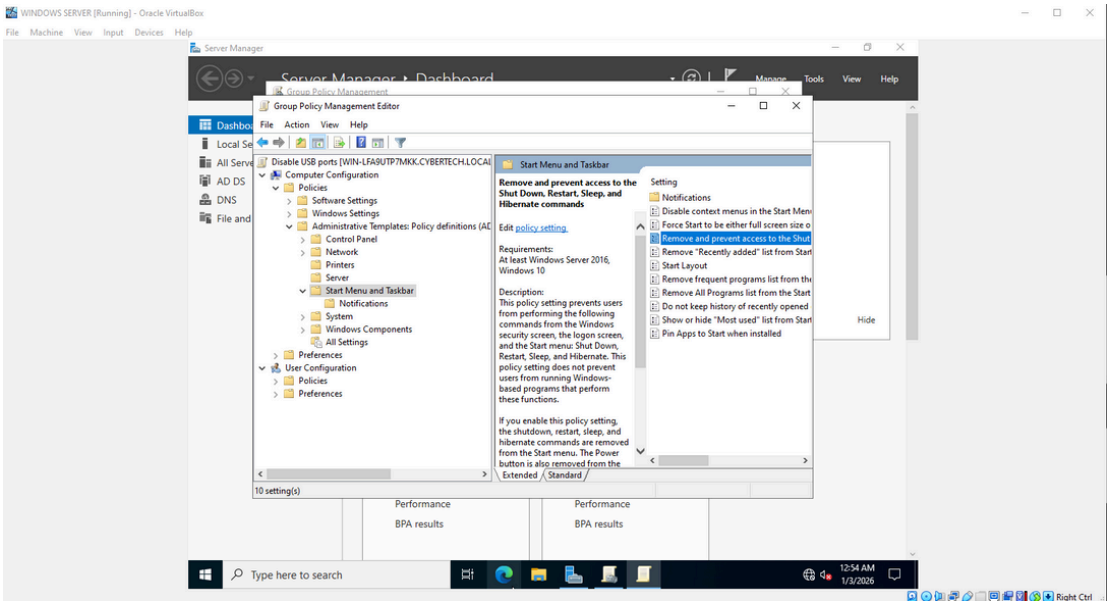


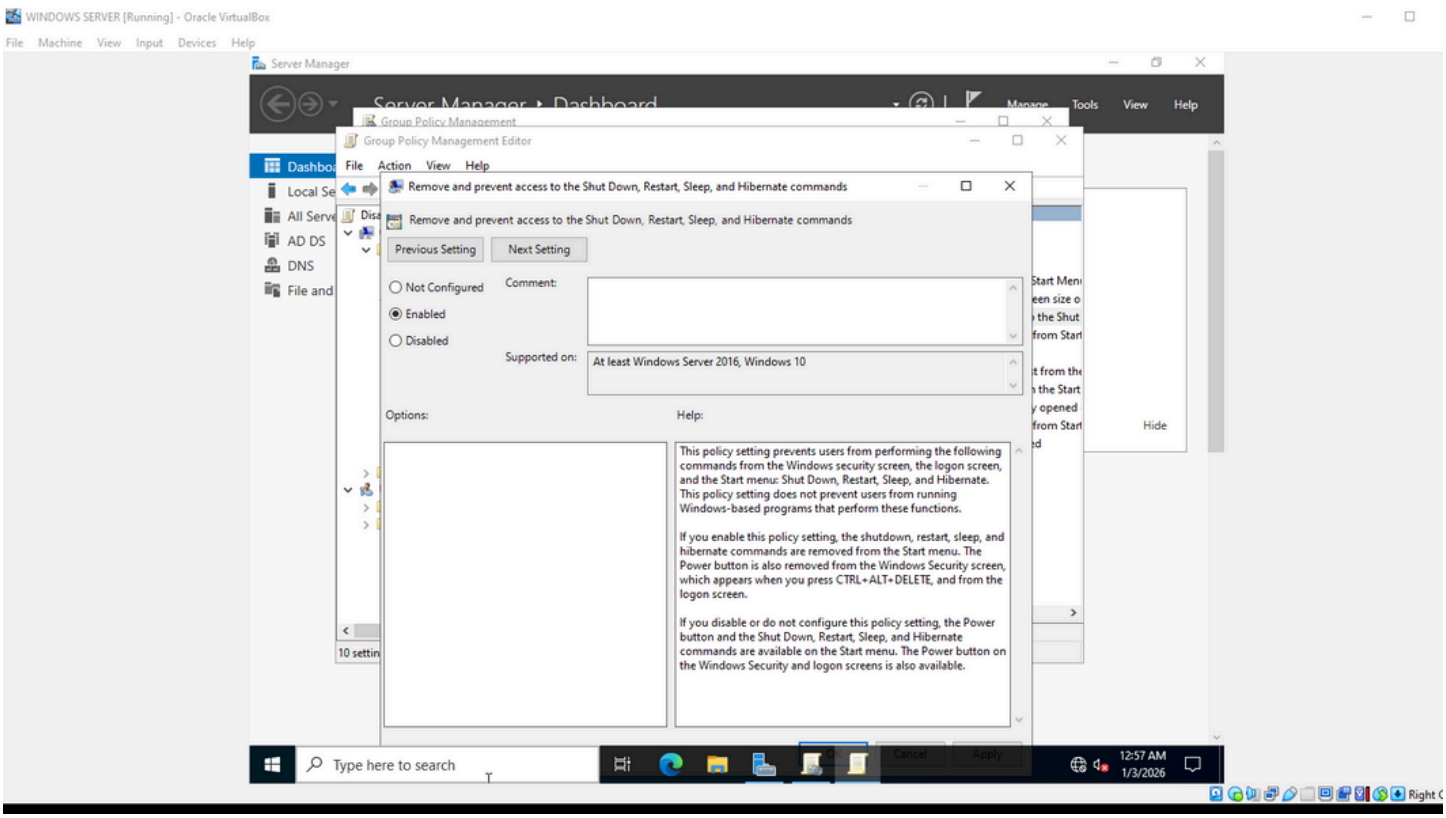
I right clicked on “Group Policy Object” and I created a new policy.



After creating the policy, I click on edit, and I will searched the policy and locate it under “Start Menu and Taskbar”. I found the policy and I enabled it. I clicked apply and ok.


Group Policy Management
File Action View Window Help
Forest: Cybertech.Local
Domains
Cybertech.Local
Default Domain Policy
AUDIT
Domain Controllers
HR
IT
Group Policy Objects
Default Domain Controllers Poli
Default Domain Policy
Edit...

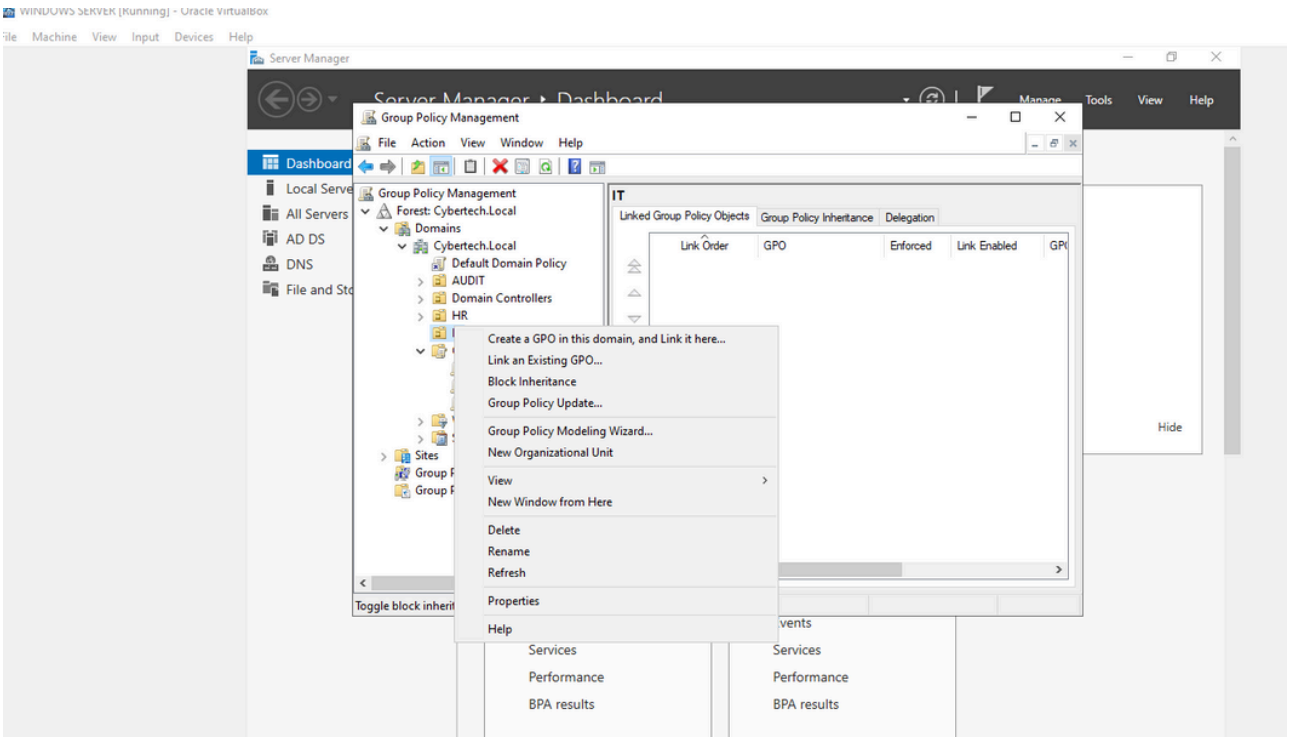

WINDOWS SERVER [Running] - Oracle VirtualBox
Server Manager
Group Policy Management Editor
Disable USB ports [WIN-LFA9UTP7MKK.CYBERTECH.LOCAL
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy definitions (AD
Control Panel
Network
Printers
Server
Start Menu and Taskbar
Notifications
System
Windows Components
All Settings
Preferences
User Configuration
Policies
Preferences
Start Menu and Taskbar
Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands
Edit policy setting
Requirements:
At least Windows Server 2016, Windows 10
Description:
This policy setting prevents users from performing the following commands from the Windows security screen, the logon screen, and the Start menu: Shut Down, Restart, Sleep, and Hibernate. This policy setting does not prevent users from running Windows-based programs that perform these functions.
If you enable this policy setting, the shutdown, restart, sleep, and hibernate commands are removed from the Start menu. The Power button is also removed from the
Setting
Notifications
Disable context menus in the Start Menu
Force Start to be either full screen size o
Remove and prevent access to the Shut
Remove "Recently added" list from Start
Start Layout
Remove frequent programs list from the
Remove All Programs list from the Start
Do not keep history of recently opened
Show or hide "Most used" list from Start
Pin Apps to Start when installed
Extended Standard
10 setting(s)
Performance
BPA results
Performance
BPA results
Type here to search
12:54 AM
1/3/2026
Right Ctrl



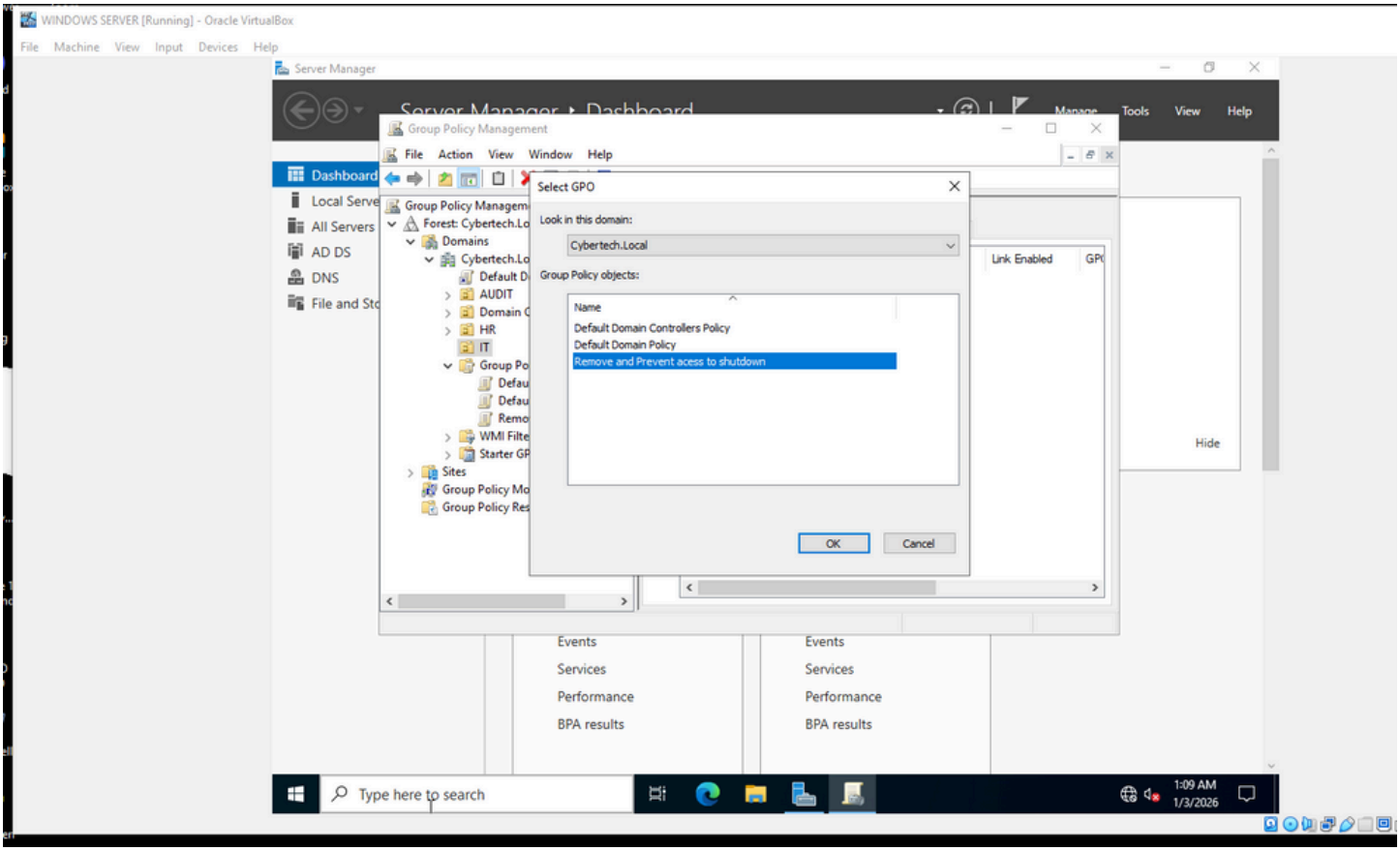
After the policy has been enabled and applied, I linked it to an organizational unit.

I went to the group policy management and I right clicked on the Organization Unit i want the policy to apply to.

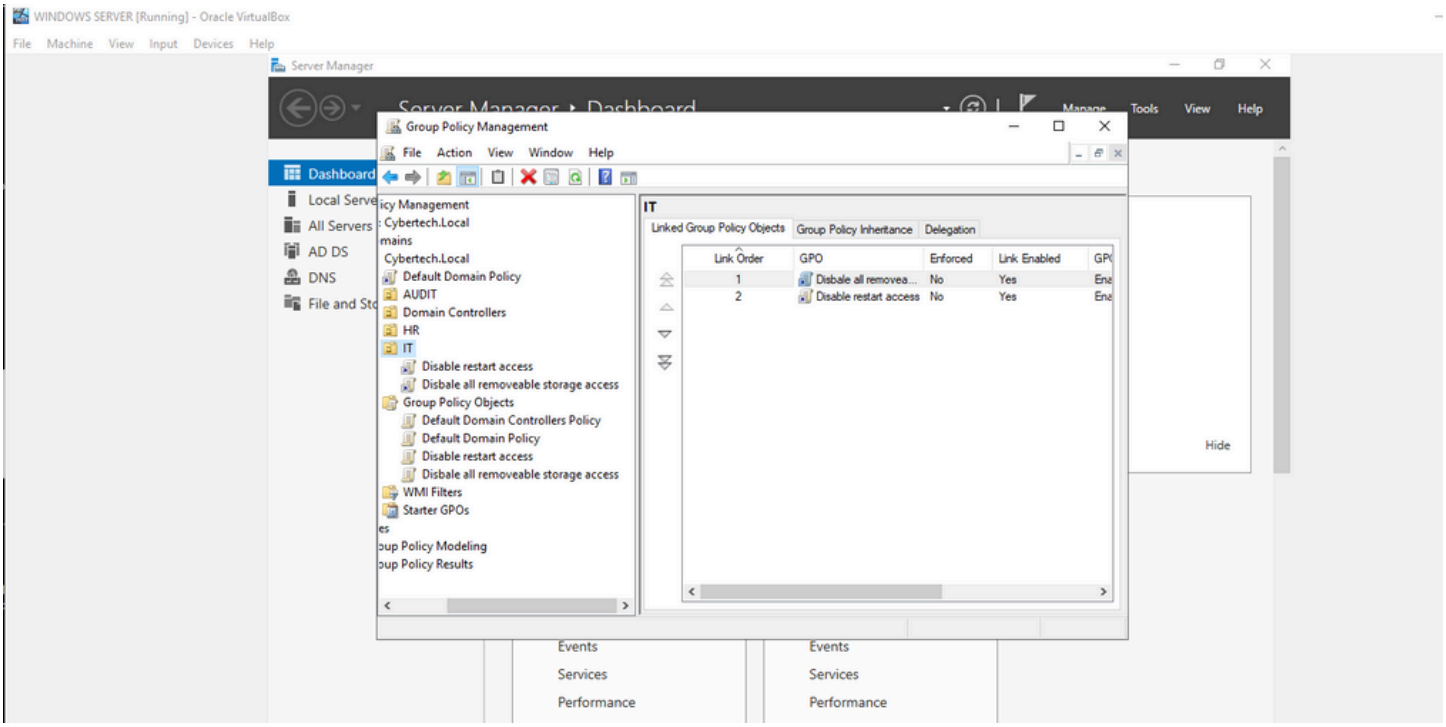
I selected the IT organization unit and i right clicked on it. After, I clicked on “Link an Existing GPO”



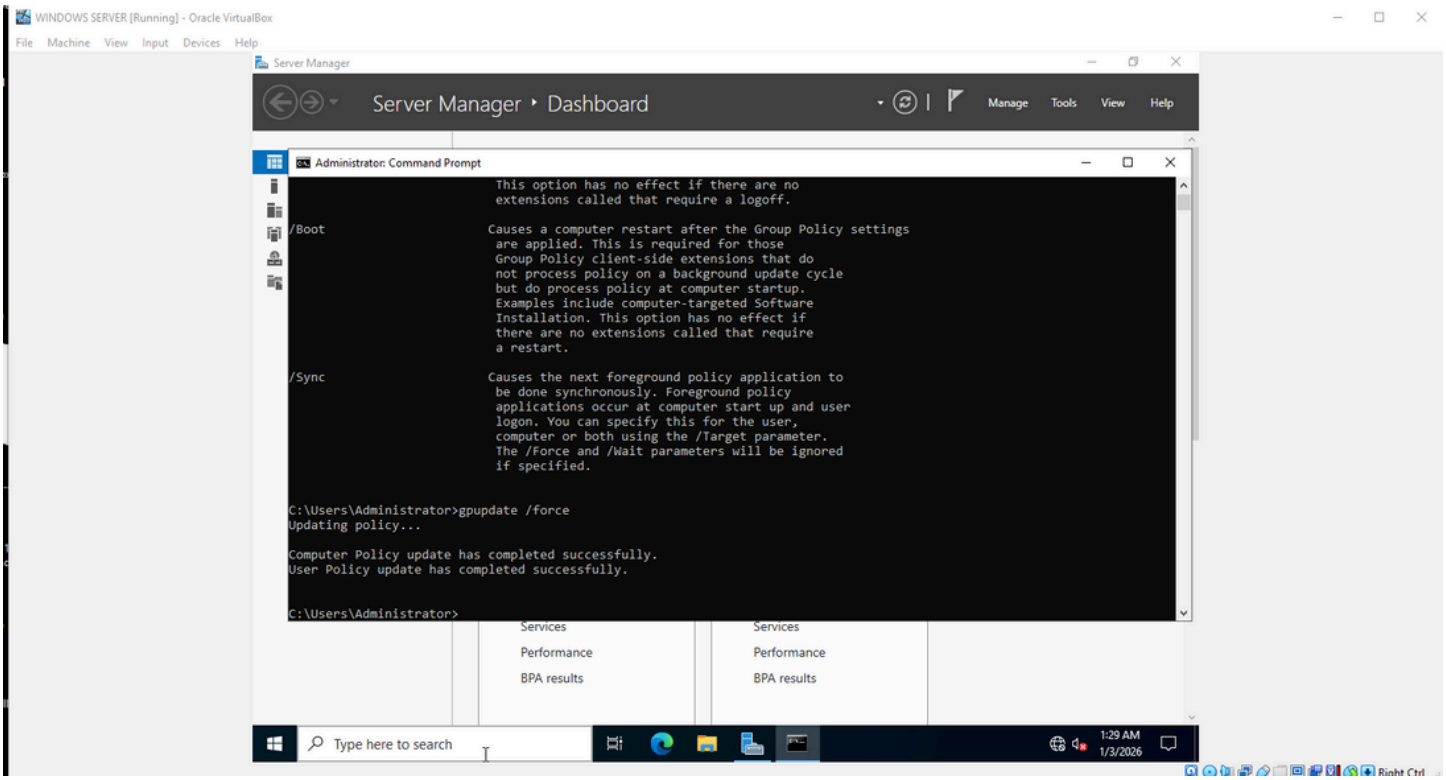
I selected the policy I created which is “Remove and Prevent access to shutdown”

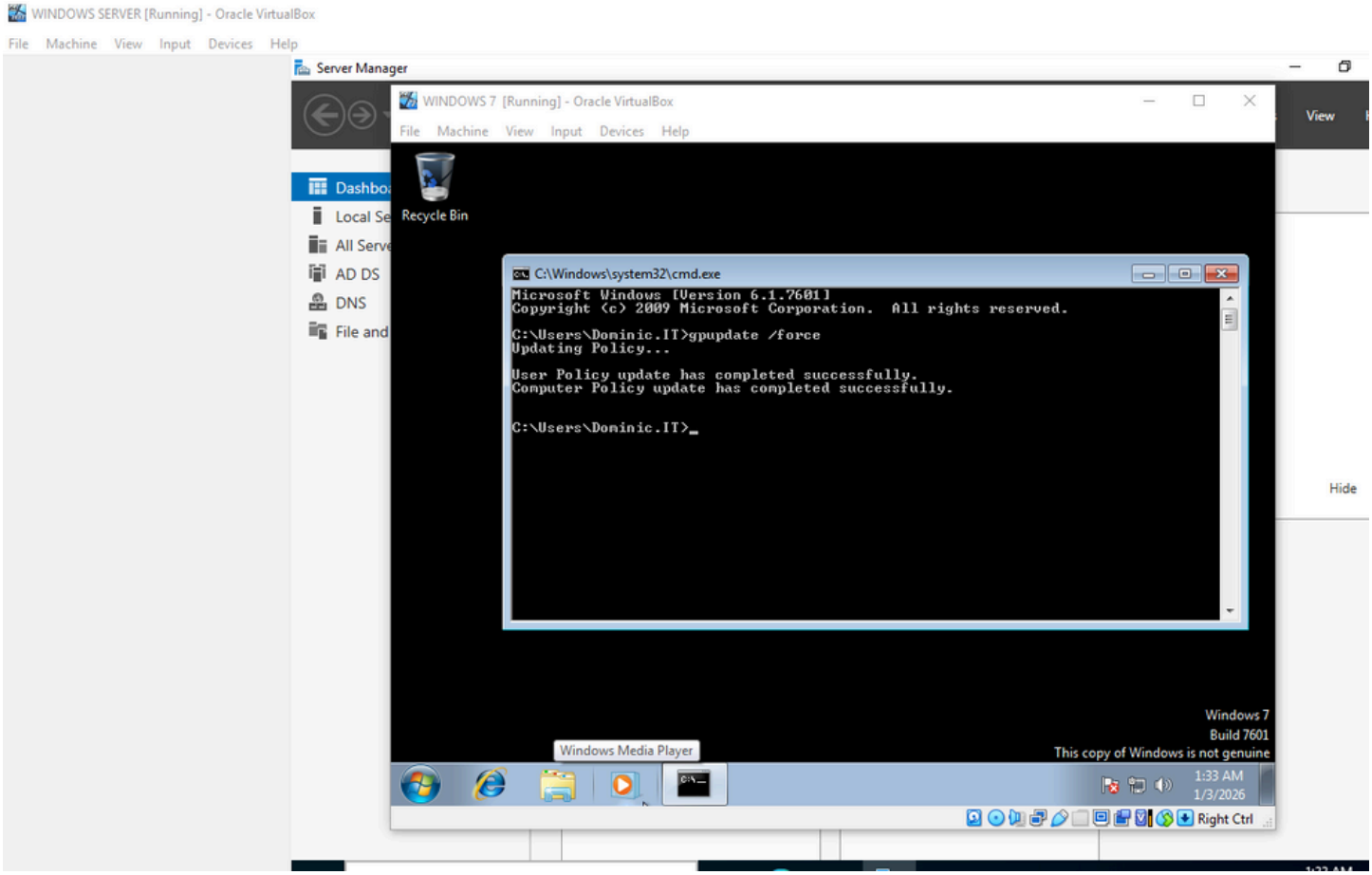


I added other policies and I confirmed if the policy are linked to the organization unit.



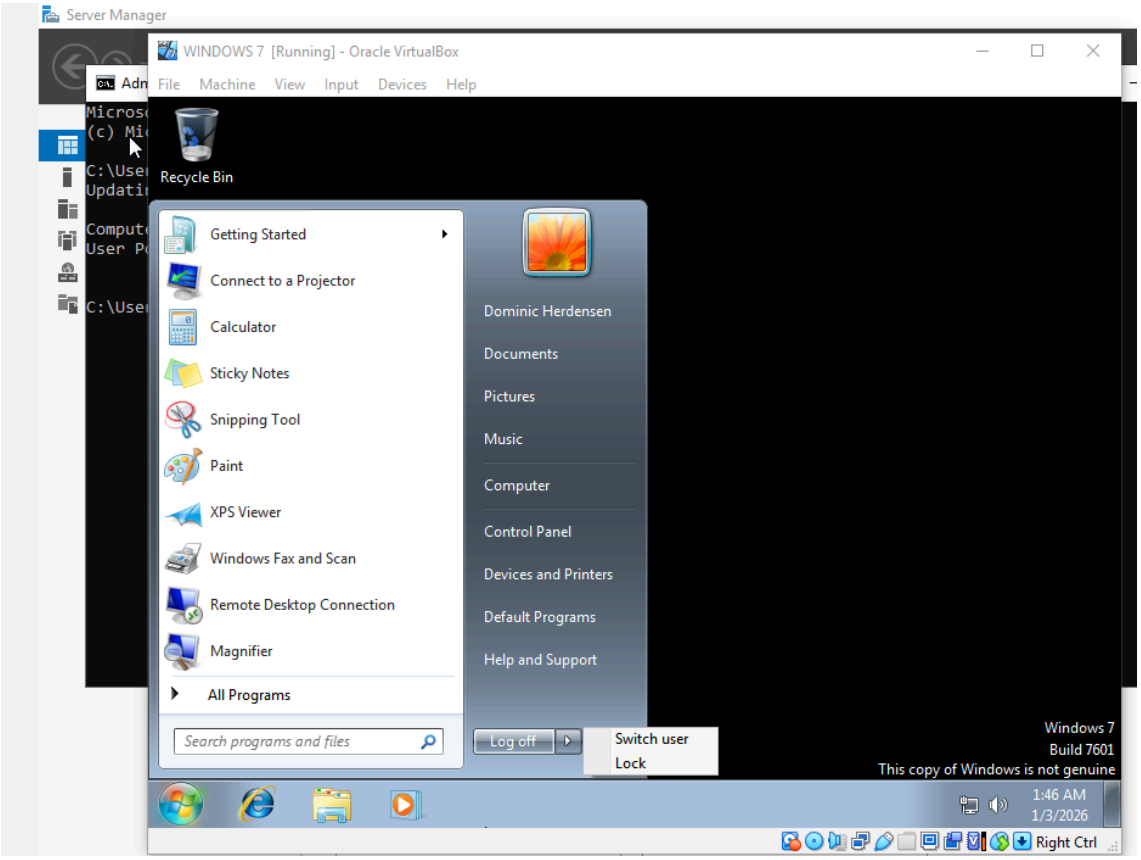
After that, I update the policy in the main server and also on the other VM (windows 7) by using the CMD prompt and typing the “gpupdate /force”

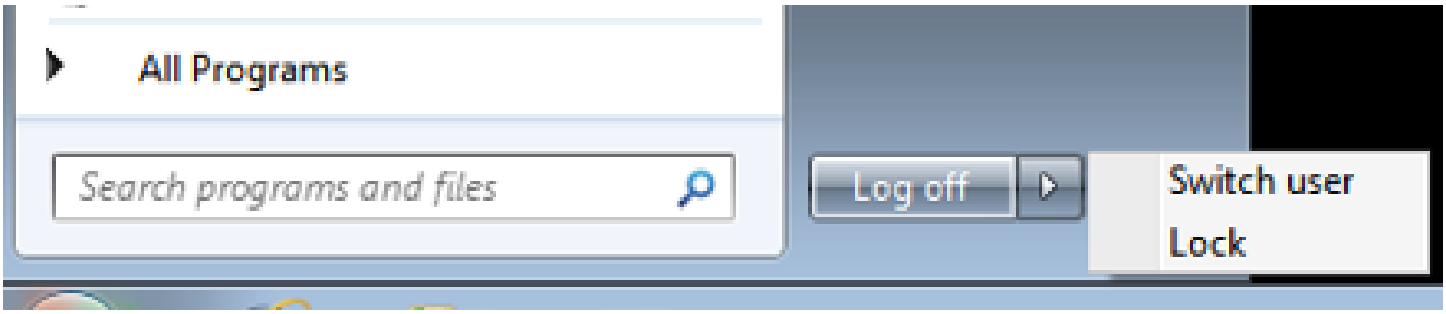




After it has been updated, I confirmed if the policy was enforced properly.

I confirmed by going on the user logged in and confirmed that the shut down option was not there.





key Takeaways.

- Gained practical experience with windows server roles and domain setup.
- Implemented centralized access control using group policy.
- Learned how to structure users and department with OUs.
- Applied IAM concepts in a real world stimulated environment.