An-Najah National University

Faculty of Engineering and Information Technology

Network Administration Lab Report

Automation Merged

EXP#8

Dr. Bakr Abd Al-Haq

Team Members: Ali Khuffash, Wajd Abd Al-Hadee

Table of Contents

1. Abstract

This report documents the setup and configuration of a Windows Server 2022-based Active Directory Domain Services (AD DS) and a File Server within a virtualized network environment. The tasks include domain controller deployment, client joining to the domain, user and computer object creation, and NTFS permissions implementation. The goal is to simulate a real enterprise environment for managing centralized authentication and resource sharing across multiple virtual machines (VMs).

2. Introduction

In enterprise networks, centralized management of users, devices, and data access is essential for efficiency and security. This project introduces students to Active Directory Domain Services and File Server setup using Windows Server 2022 within a virtual lab environment. The lab enhances understanding of domain management, role assignment, user permission controls, and secure file sharing using NTFS permissions. The implementation closely mimics real-world enterprise IT environments and builds foundational system administration skills.

3. Objectives

- To install and configure Active Directory Domain Services on Windows Server 2022.
- To create and manage user and computer accounts in Active Directory.
- To join client machines to the domain.
- To set up a dedicated File Server using Windows Server 2022.
- To manage NTFS permissions for secure file sharing.
- To simulate real-life scenarios involving user access and permission limitations.

4. Pre-requisites & Resources

- Hardware and Software:

VirtualBox or any virtualization platform.

- ISO files:

  Windows Server 2022

  Windows 10

- Virtual Machines:

  Four virtual machines configured as follows:

PC	VM	OS	Hostname	RAM	CPU cores	Hard Disk
PC1	GRPxDC (Domain Controller)	Windows Server 2022 (Desktop)	GRPxDC	4 GB	2	200 GB HDD
	GRPxFS (File Server)	Windows Server 2022 (Desktop)	GRPxFS	4 GB	2	200 GB HDD
PC2	GRPxClient1 (Client Machine)	Windows 10	GRPxClient1	4 GB	2	200 GB HDD
	GRPxClient2 (Second Client Machine)	Windows 10	GRPxClient2	4 GB	2	200 GB HDD

All VMs use the Bridged Network Adapter with Static IP addressing.
x means the number the team takes.

5. Methodology

5.1 Creating Virtual Machines

Four VMs were created with the appropriate names and configurations. The domain controller (GRP7DC) was installed with Windows Server 2022, while the clients and file server were installed with Windows 10 and Windows Server 2022 respectively.

5.2 Active Directory Domain Services Setup

Static IP configured on GRP7DC. See figure 5.2.1

Figure 5.2.1 Clicking on IPv4 address from the server manager to Configure Static IP.

Configuring and Setting Static IP on GRP7DC. See figure 5.2.2 and figure 5.2.3

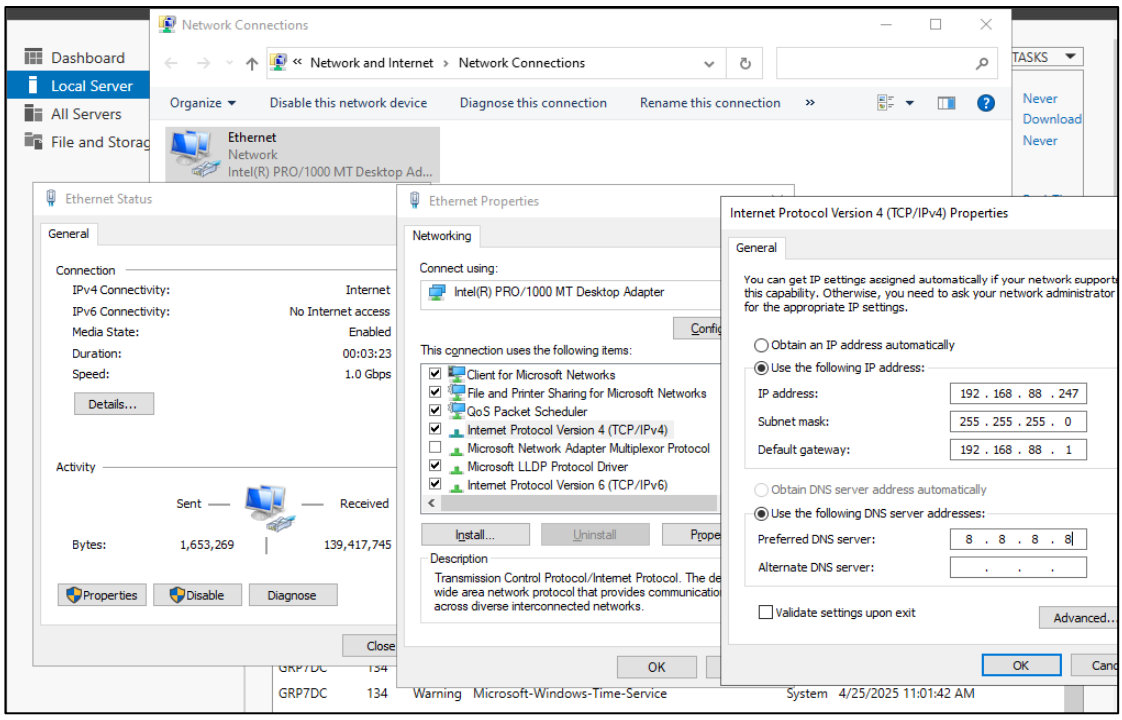

Figure 5.2.2 Changing Network Settings to Apply Static IP on GRP7DC

Figure 5.2.3 The IP of GRP7DC is enabled successfully.

The Active Directory Domain Services (AD DS) role is essential for setting up a domain controller, which will manage and authenticate all the network's user accounts and resources. By installing this role on the GRP7DC server, you're enabling it to handle the domain management tasks, such as creating, managing, and authenticating users and computers within the domain.

Once the AD DS role is installed, the server can be promoted to a domain controller. This allows GRP7DC to store the directory database, manage security policies, and authenticate users, making it a central piece of your network infrastructure.

See Figure 5.2.4, figure 5.2.5 and figure 5.2.6 to learn how to prepare your device a DC.

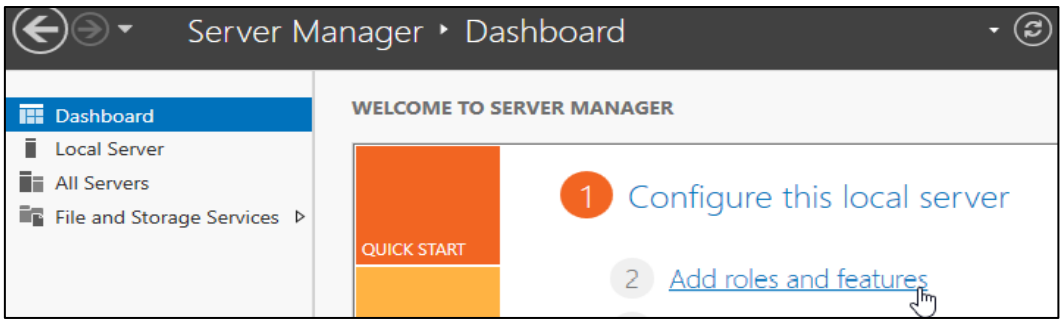

Figure 5.2.4 Open the Add Roles and Features wizard.

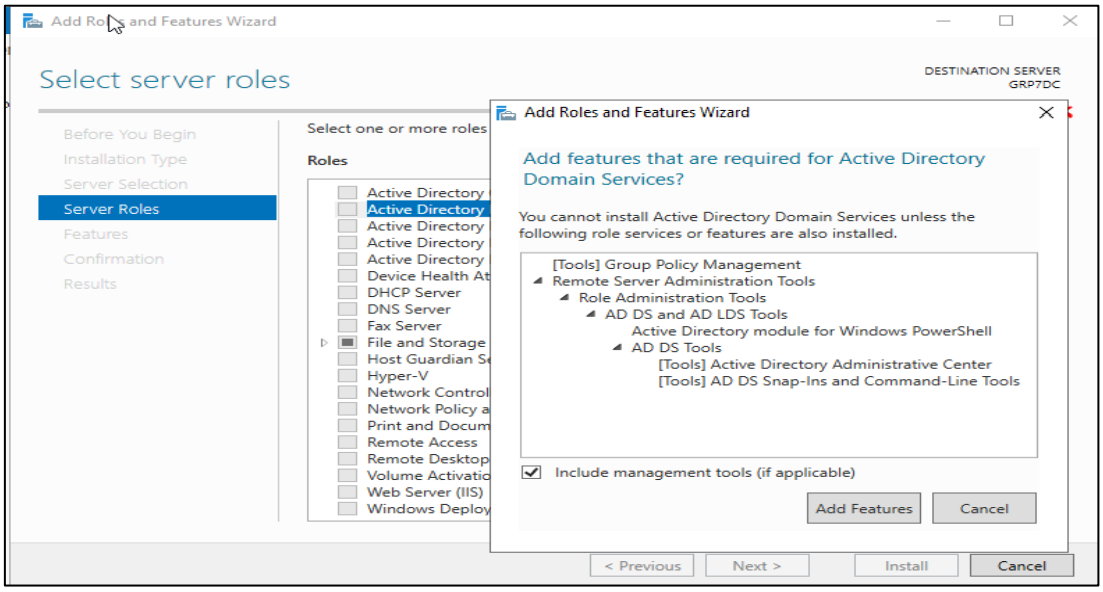

Figure 5.2.5 Select Server Roles screen Roles tick "Active Directory Domain Services.

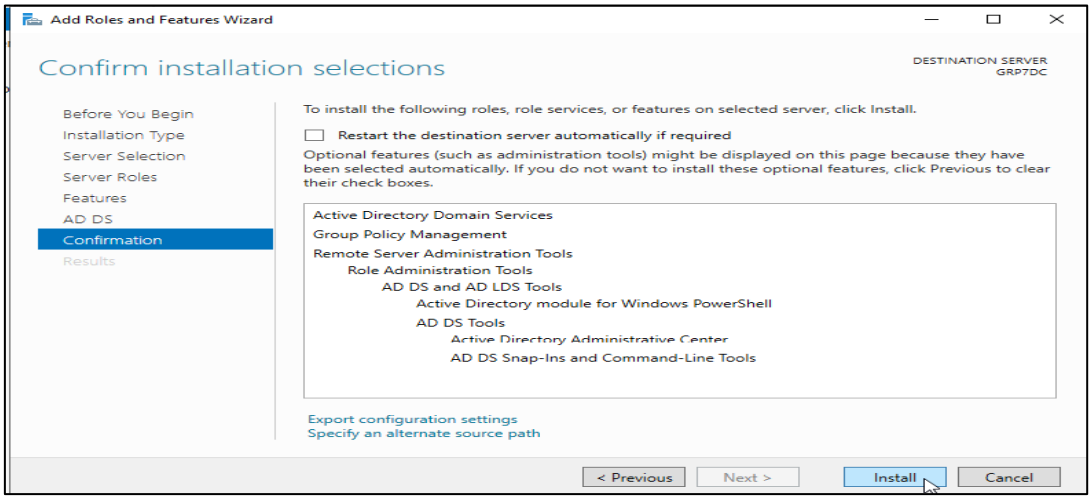

Figure 5.2.6 Clicking Install to Begin Active Directory Domain Services Installation.

The domain controller promotion process begins by selecting the option "Promote this server to a domain controller" in the Server Manager, initiating the setup for domain services. See figure 5.2.7

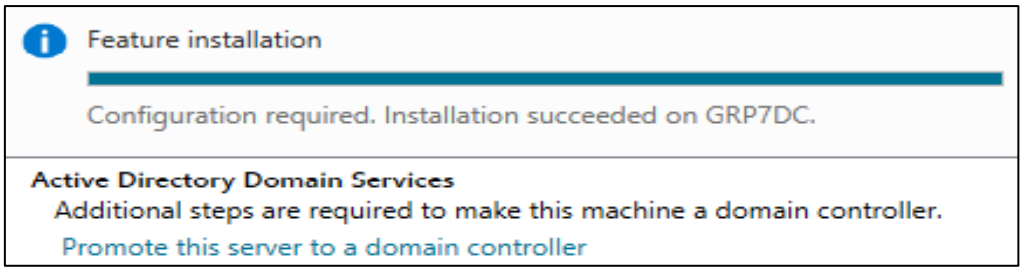

Figure 5.2.7 Initiating Domain Controller Promotion by Clicking "Promote this server.

The Active Directory Configuration Wizard is launched to guide the setup process for promoting the server to a domain controller. See figure 5.2.8

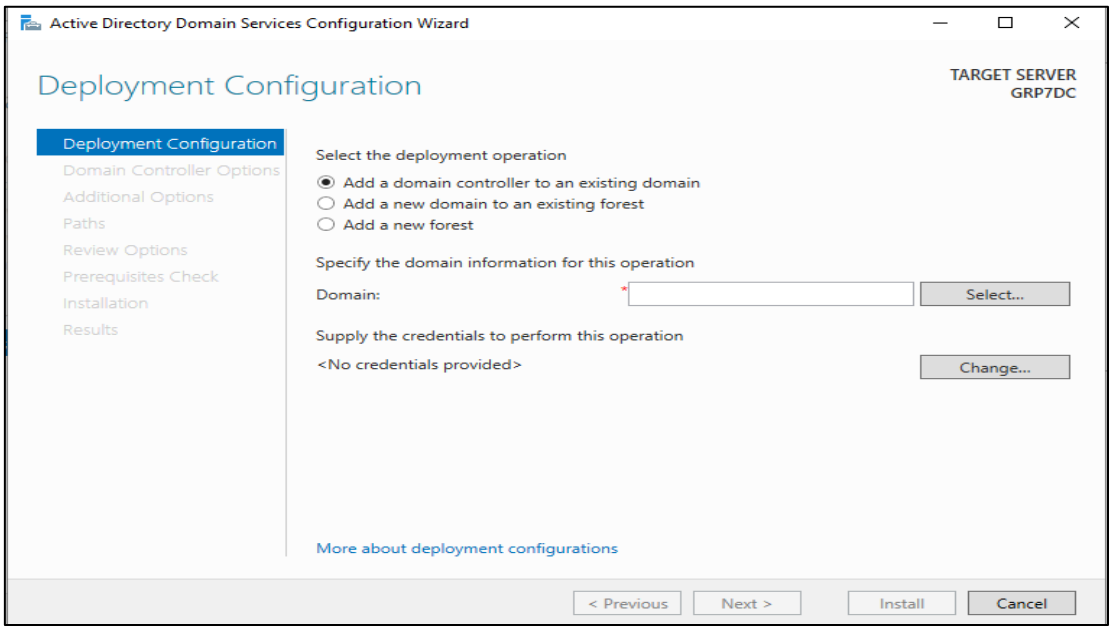

Figure 5.2.8 Launching Active Directory Configuration Wizard.

A new forest is created by defining the root domain as AdminGRP7.Lab, establishing the primary domain structure for the network. See figure 5.2.9

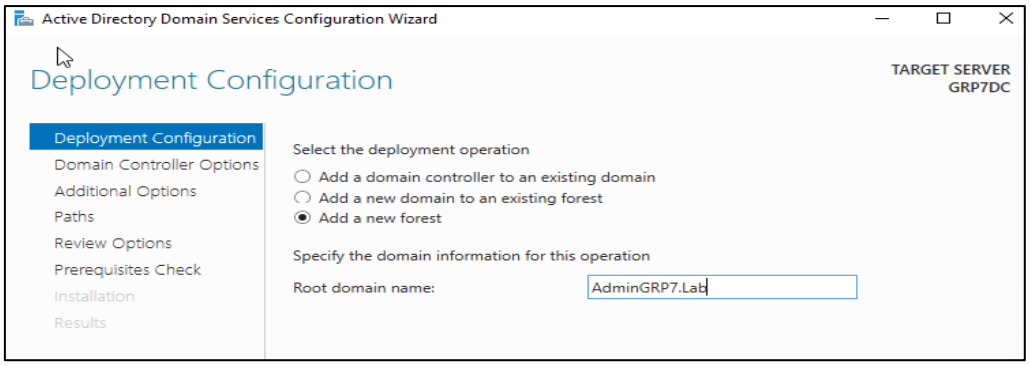

Figure 5.2.9 Adding a New Forest and Defining Root Domain as AdminGRP7.Lab.

The domain and forest functional levels are configured, and the Directory Services Restore Mode (DSRM) password is set, ensuring proper access and security protocols. See figure 5.2.10

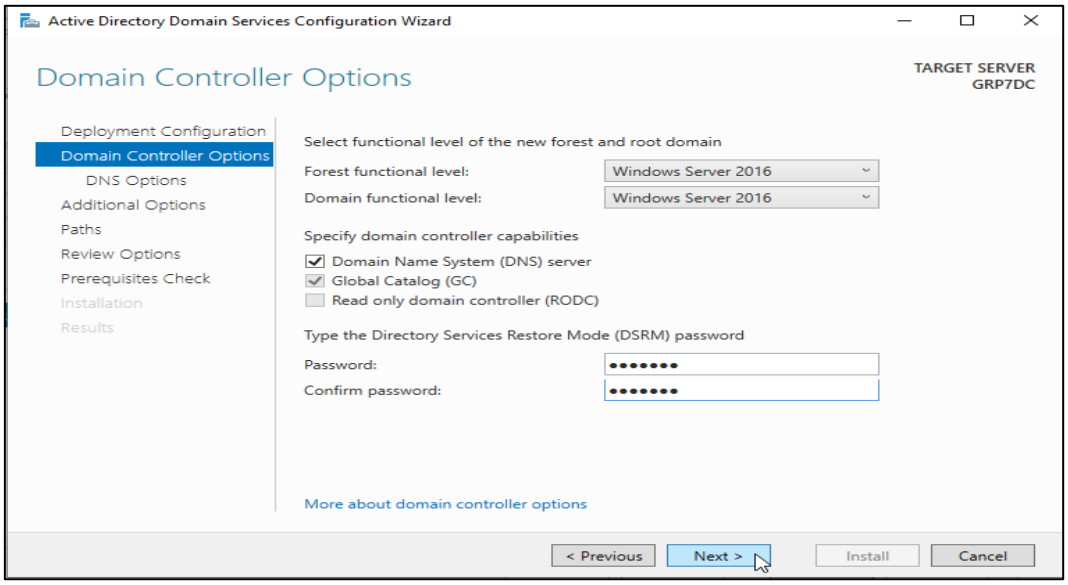

Figure 5.2.10 Configuring Domain and Forest Levels, Setting DSRM Password.

A final review of the configuration settings after leave the next settings as default is prerequisite check is performed to verify the system's readiness for installation, and the install button is enabled once all conditions are met. And the installation process is initiated by clicking the Install button, beginning the domain controller setup procedure The system automatically restarts after the installation completes, applying the necessary changes to the server configuration.

See figure 5.2.11, figure 5.2.12 and figure 5.2.13

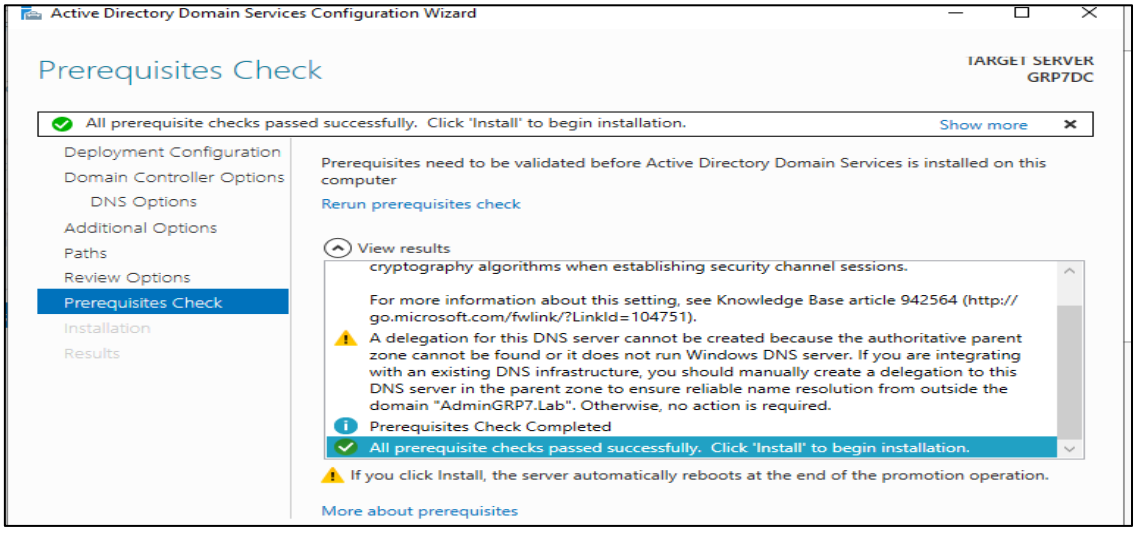

Figure 5.2.11 Running Prerequisite Check and Enabling Install Button.

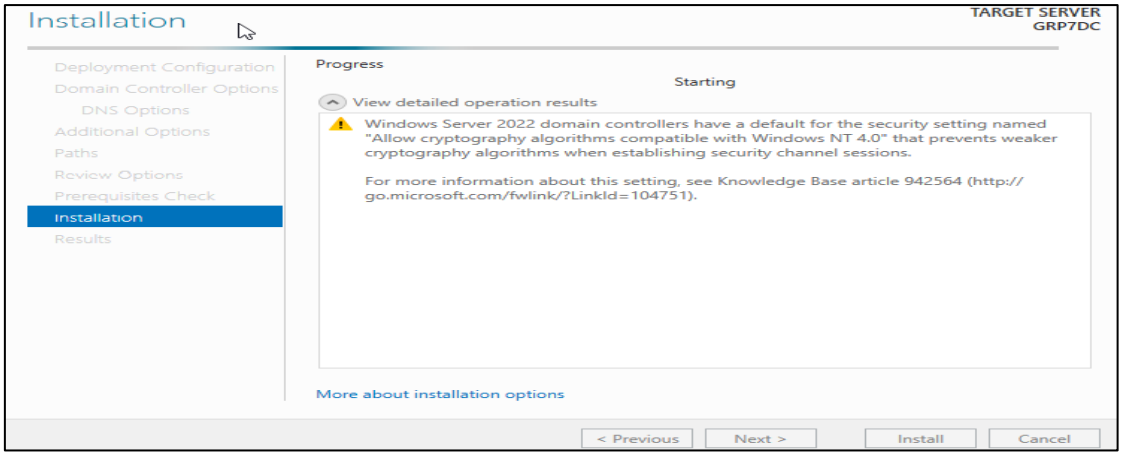

Figure 5.2.12 Starting Installation Process by Clicking Install.

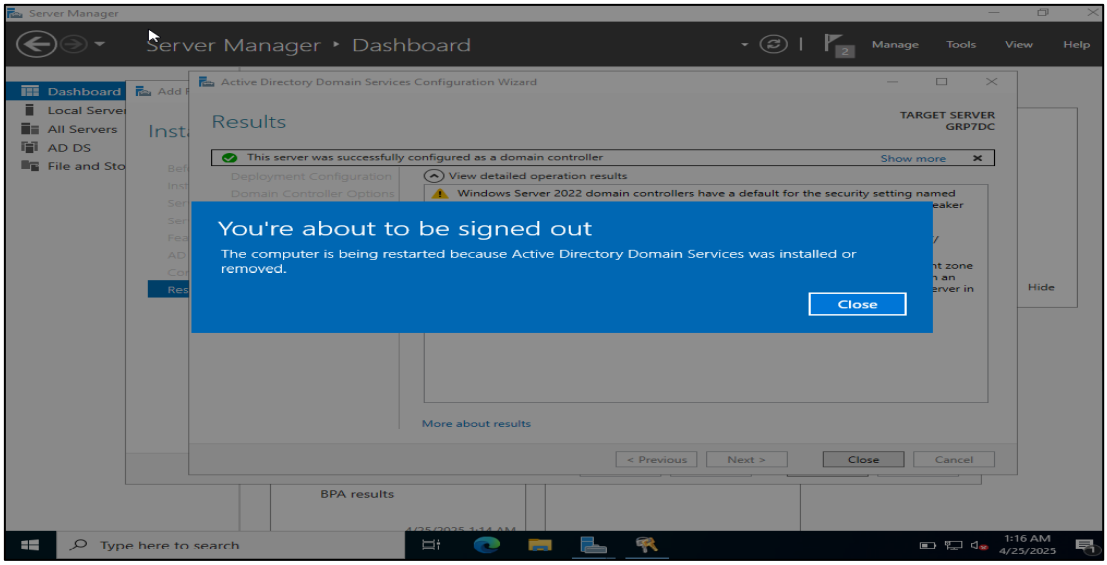

Figure 5.2.13 Automatic Restart After Installation Completes.

After the reboot, the domain controller is logged into using the domain administrator account, confirming the successful promotion and setup of the server. See figure 5.2.14

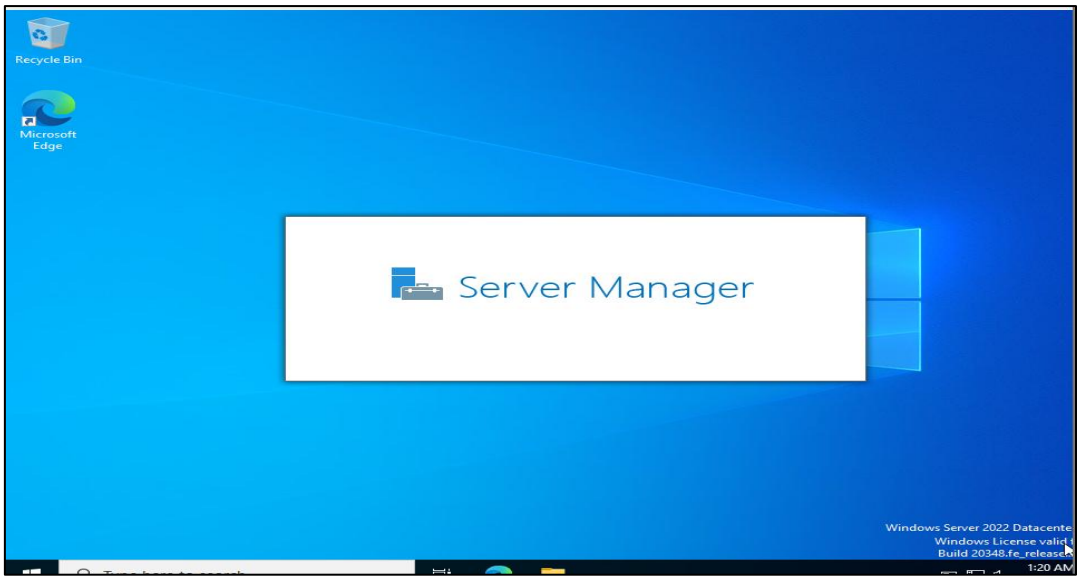

Figure 5.2.14 Logging into Domain Controller as Domain Admin After Reboot.

The process of accessing the Active Directory Administrative Center begins by opening Server Manager, selecting Active Directory Domain Services (AD DS), and then right-clicking on the server to choose the Active Directory Administrative Center. This tool is used for managing Active Directory objects. See figure 5.2.15

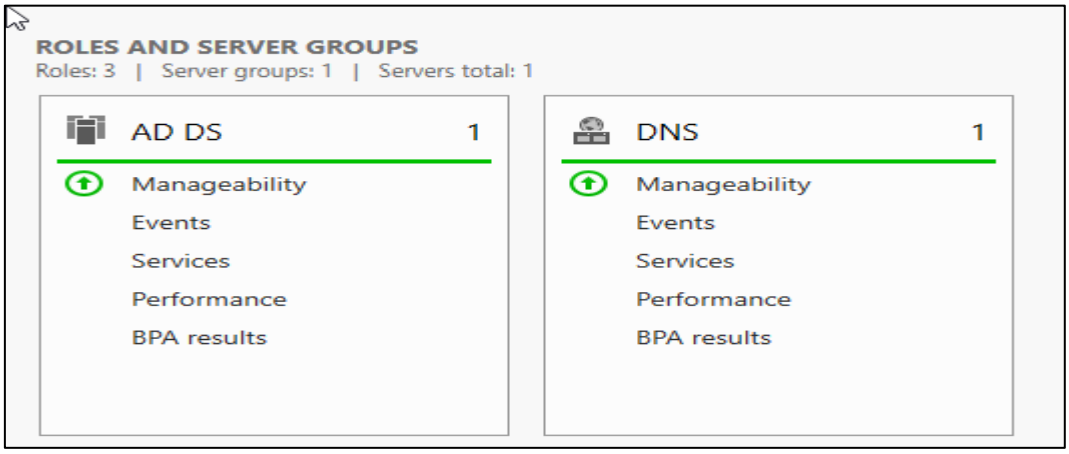

Figure 5.2.15 Clicking the AD DC.

The Active Directory Administrative Center is selected from the available options in the AD DS menu. This center provides a graphical interface for managing Active Directory objects, such as users and computers. See figure 5.2.16

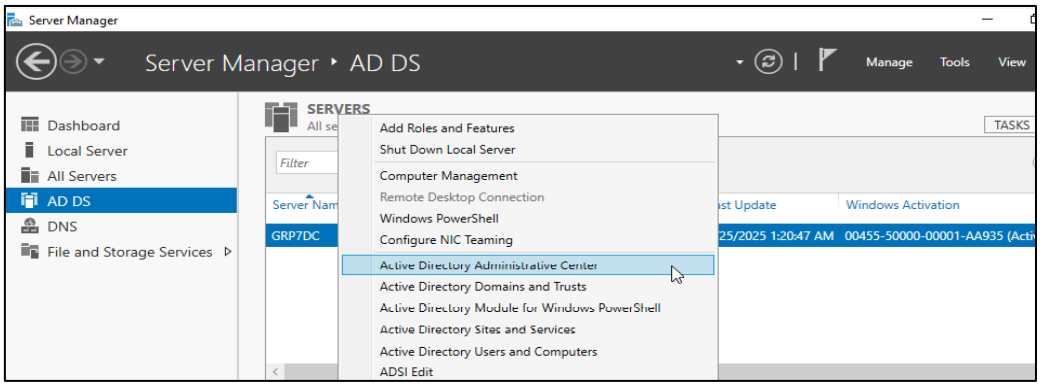

Figure 5.2.16 Selecting Active Directory Administrative Center.

In the Active Directory Administrative Center, navigation is performed to the Users functional group, where user accounts are managed and configured within the domain. See figure 5.2.17

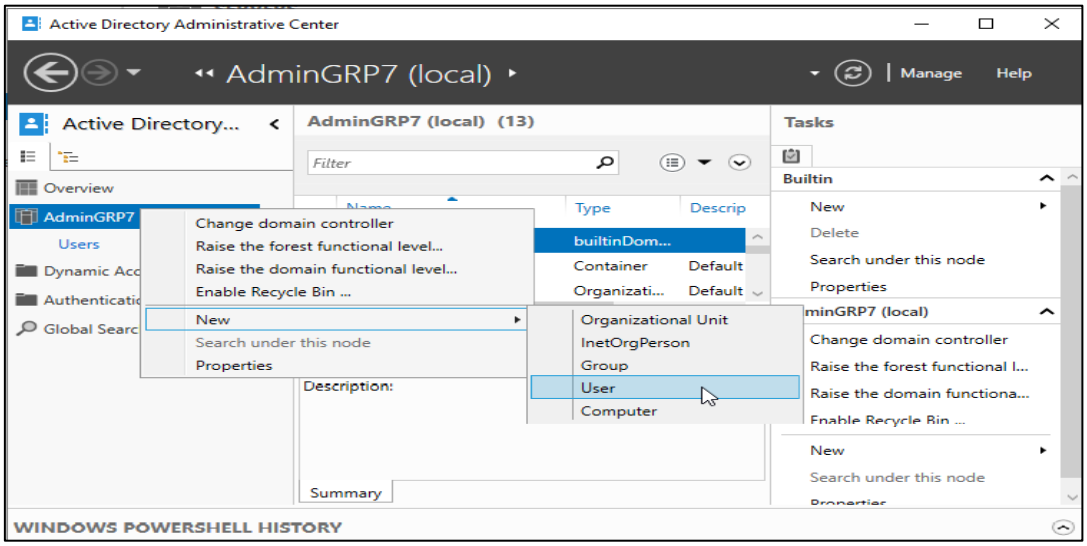

Figure 5.2.17 Creating a New User with Specified Details in Active Directory.

A new user is created in Active Directory with specified details, such as the User Principal Name (UPN), account name, and other relevant settings like the password, enabling proper user management within the domain. See figure 5.2.18

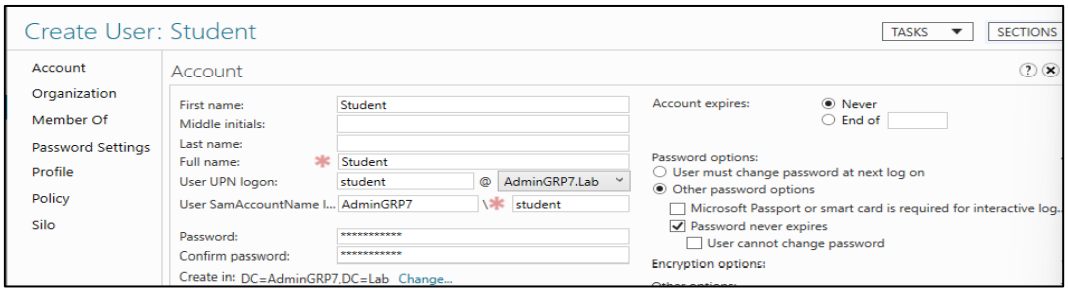

Figure 5.2.18 Finalizing User Creation and Confirming Settings.

A new computer object, GRP7Client1, is created in Active Directory, allowing the machine to be registered and managed as part of the domain, ensuring that it can authenticate and communicate with other network resources. See figure 5.2.19 and figure 5.2.20

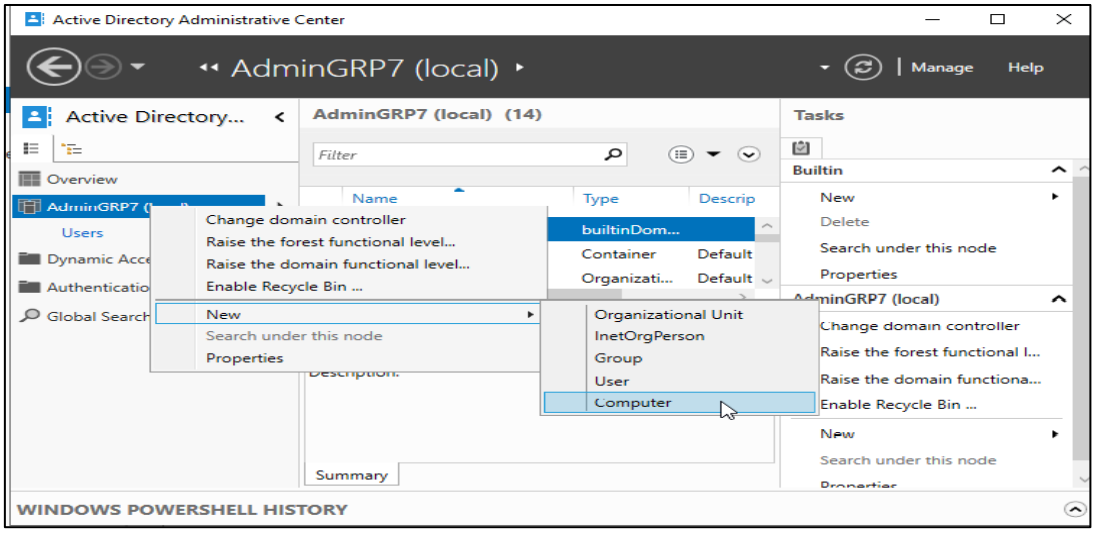

Figure 5.2.19 Creating a New Computer Object (GRP7Client1) in Active Directory.

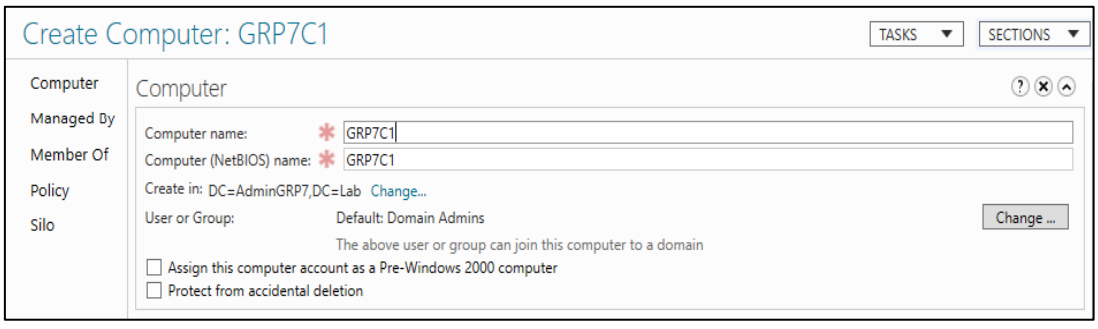

Figure 5.2.20 Finalizing Computer Creation and Confirming Settings.

5.3 Domain Joining

The IP address and DNS server on GRP7Client1 are configured to ensure the client can properly communicate with the domain controller and join the domain. This setup is essential for domain authentication and name resolution. The following commands are used on both workstations to install Git. See figure 5.3.1

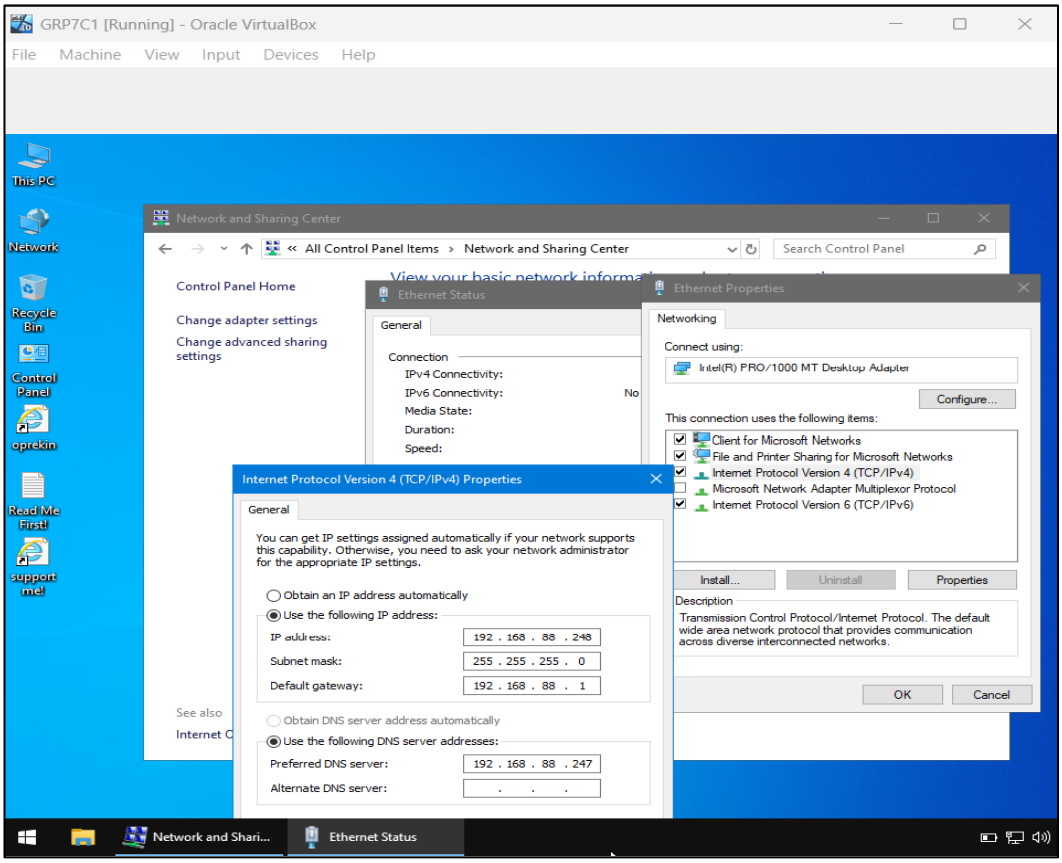

Figure 5.3.1 Configuring IP Address and DNS Server on GRP7Client1 for Domain Joining.

The System Settings are accessed from the Control Panel to make necessary adjustments, including changing the computer's name and domain membership. See figure 5.3.2

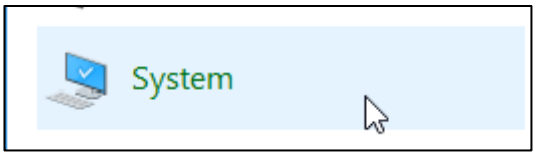

Figure 5.3.2 Accessing System Settings from Control Panel.

The "Change Settings" option under Computer Name, Domain, and Workgroup Settings is selected to begin the process of modifying

the computer's domain configuration and name settings.
See figure 5.3.3

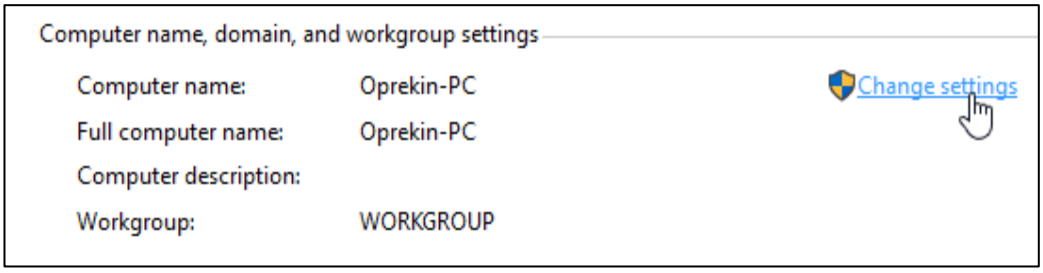

Figure 5.3.3 Clicking "Change Settings" Under Computer Name, Domain.

The computer name is changed, and AdminGRP7.Lab is entered as the domain name to join GRP7Client1 to the existing domain, allowing it to be managed as part of the domain infrastructure. See figure 5.3.4

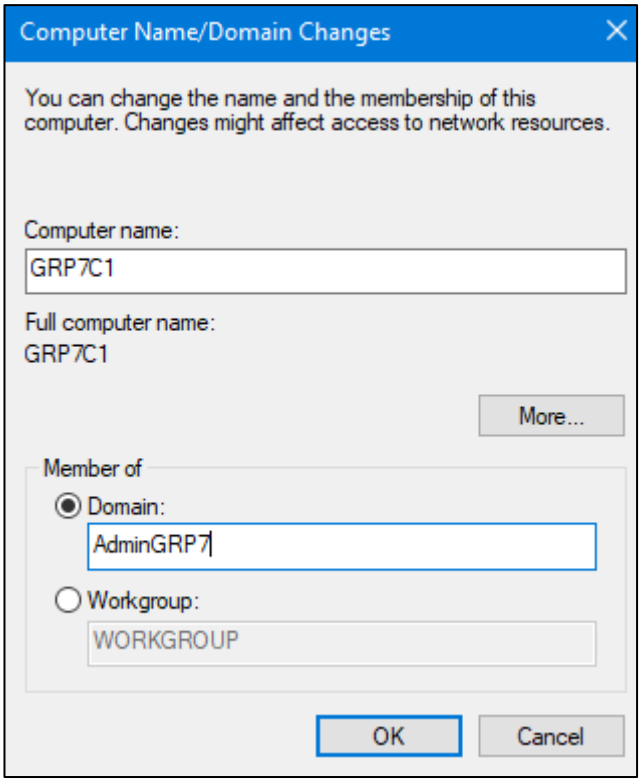

Figure 5.3.4 Changing Computer Name and Joining Domain AdminGRP7.Lab.

Administrator credentials are entered to authorize the computer's joining to the domain, ensuring the process is executed with the necessary administrative privileges.

See figure 5.3.5 and figure 5.3.6

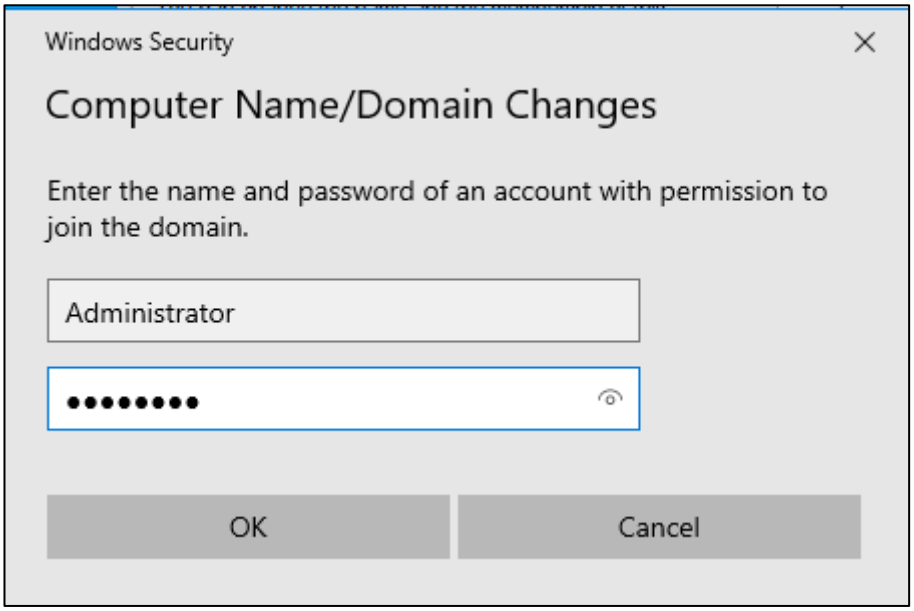

Figure 5.3.5 Entering Administrator Credentials to Join Domain.

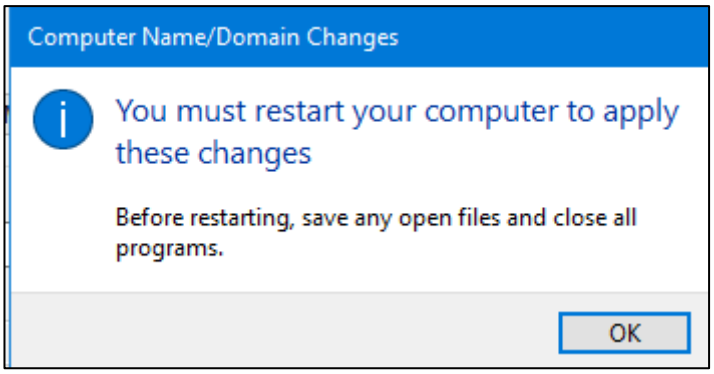

Figure 5.3.6 The process is done successfully.

Following the on-screen instructions, the computer is restarted to complete the process of joining the domain, allowing it to establish a connection with domain services. See figure 5.3.7

Figure 5.3.7 Following On-Screen Instructions to Restart PC.

After the restart, the user logs into the domain using the Student account, confirming that the computer is now successfully joined to the domain and accessible with the domain credentials. See figure 5.3.8, figure 5.3.9 and figure 5.3.10

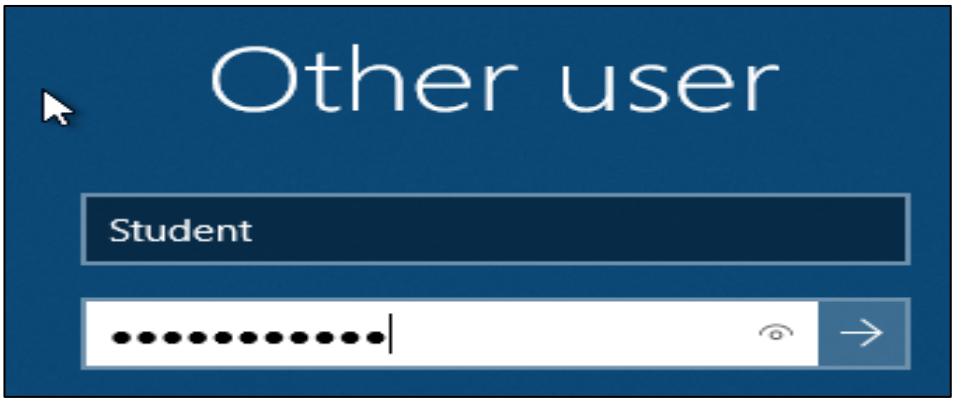

Figure 5.3.8 Logging by the username and the password.

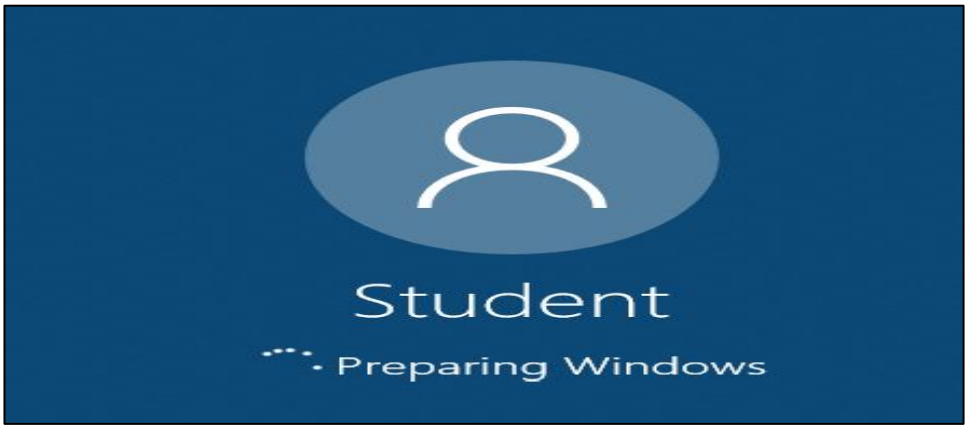

Figure 5.3.9 Preparing Windows.

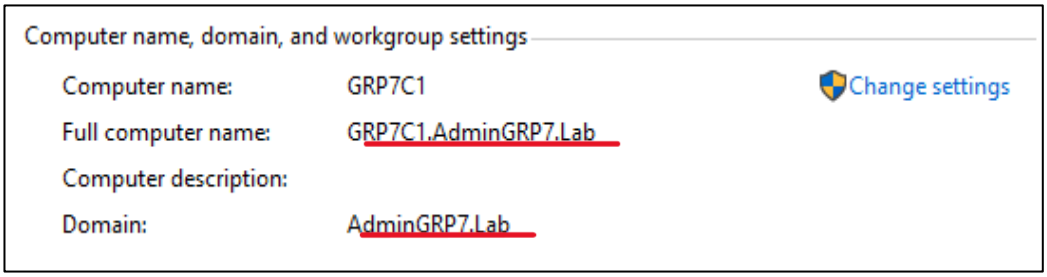

Figure 5.3.10 Logging into Domain with Student Account After Restart.

5.4 File Server Setup

Windows 10 VM and Windows Server 2022 VM are created to set up the necessary virtual machines for client and file server roles,

ensuring the environment is ready for domain integration and resource sharing.

see figure 5.4.1

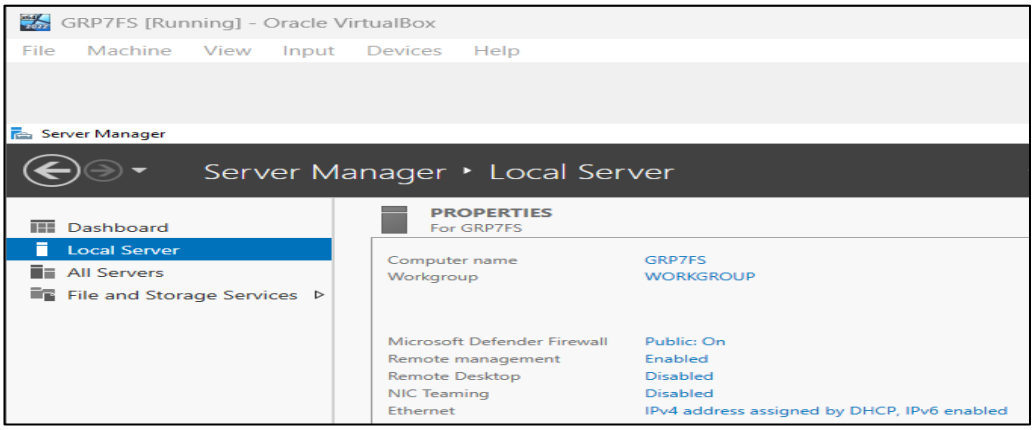

Figure 5.4.1 Creating Windows 10 VM and Windows Server 2022 VM for File Server.

A static IP address is assigned to the File Server (GRP7FS), ensuring the server maintains a consistent and unchanging network address. This setup is crucial for stable access to shared resources on the server by domain-joined clients. See figure 5.4.2 and figure 5.4.3

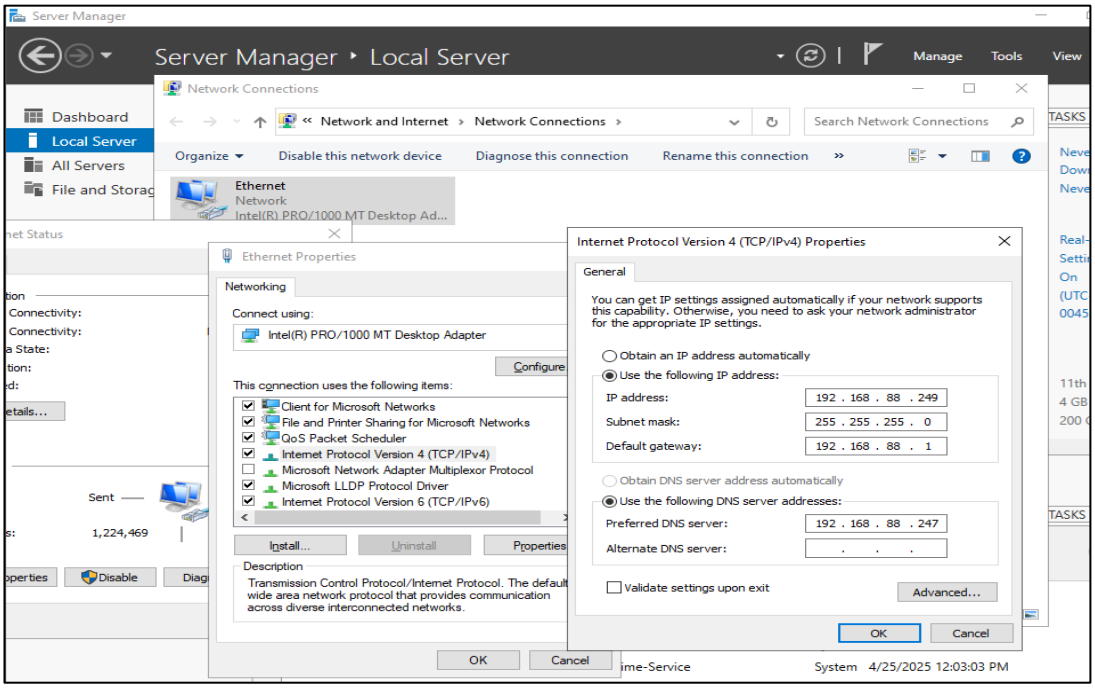

Figure 5.4.2 Assigning Static IP Address to File Server (GRP7FS).

Figure 5.4.3 Modifying IP Configuration on File Server (GRP7FS).

The File Server (GRP7FS) and a new client are added to the domain through the Domain Controller. This process allows the new devices to be managed within the domain, enabling access to shared resources and centralized authentication services. See figure 5.4.4 and figure 5.4.5

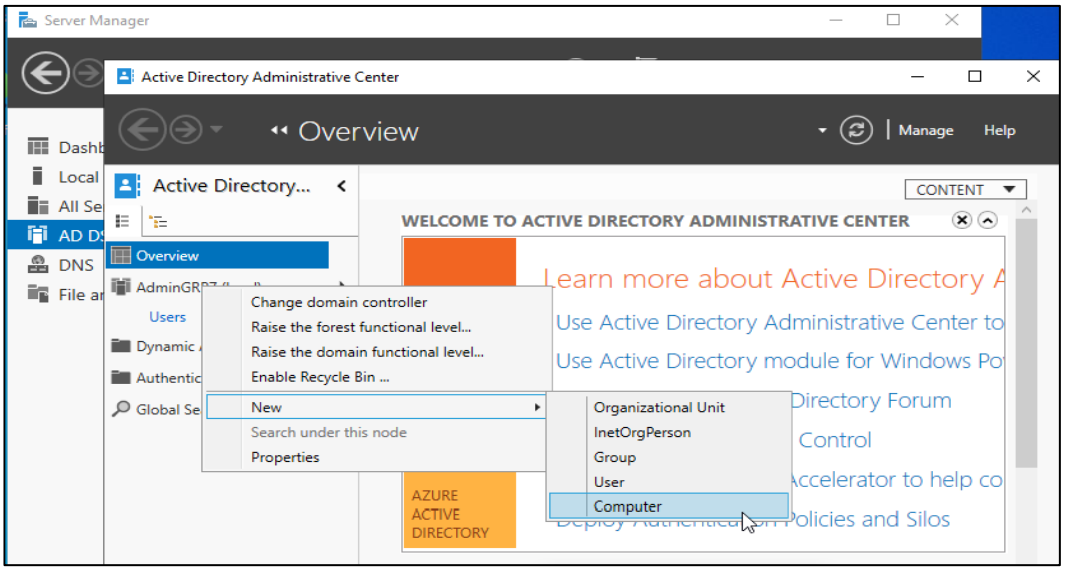

Figure 5.4.4 Creating a New Computer Object (GRP7Client1) in Active Directory.

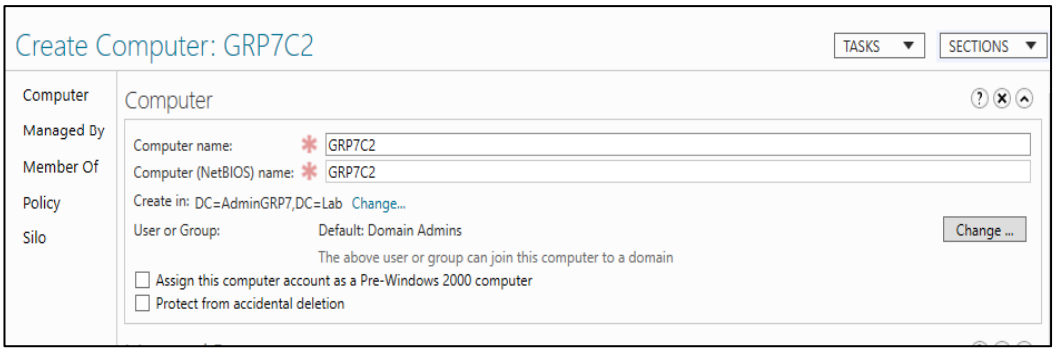

Figure 5.4.5 Adding File Server and New Client to Domain via Domain Controller.

It is confirmed that all virtual machines (VMs) have unique MAC and IP addresses while being part of the same domain, ensuring no conflicts and proper network operations within the domain environment.

See figure 5.4.6 and figure 5.4.7

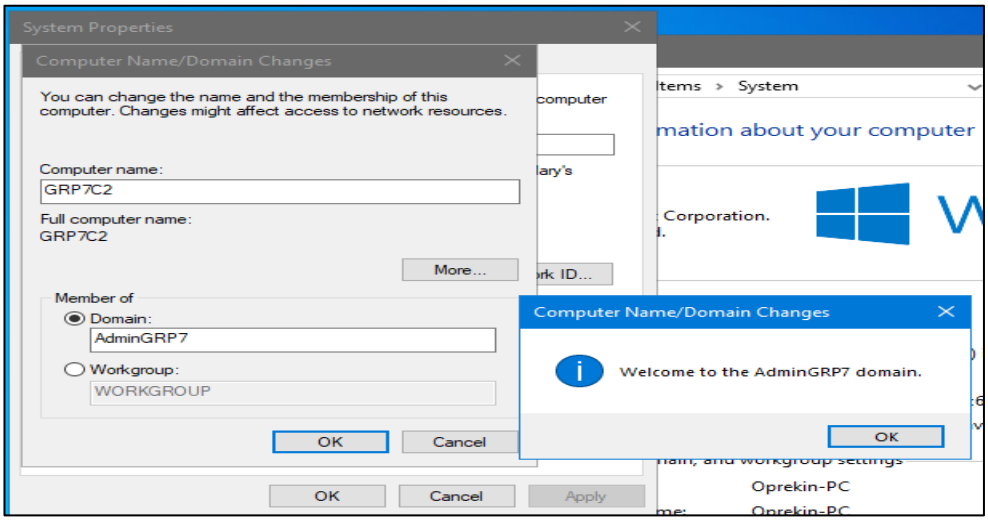

Figure 5.4.6 The new client was added to the domain.

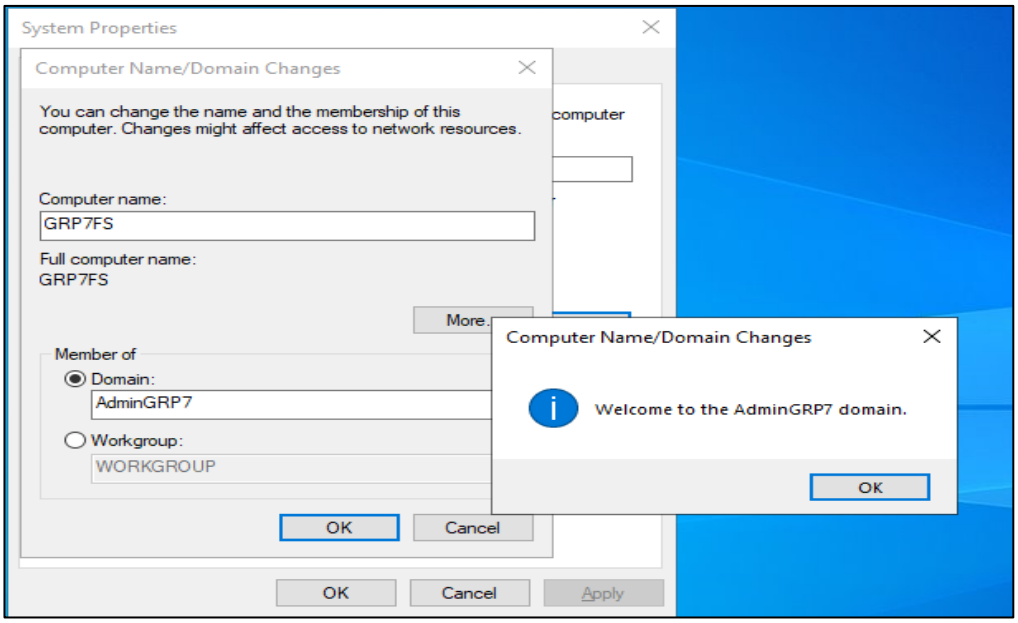

Figure 5.4.7 The file server was added to the domain.

Organizational Units (OUs) named Nablus and Servers are created in Active Directory to organize and manage resources effectively within the domain. These OUs will help in grouping related objects, such as the File Server and other server resources.

See figure 5.4.8 and figure 5.4.9

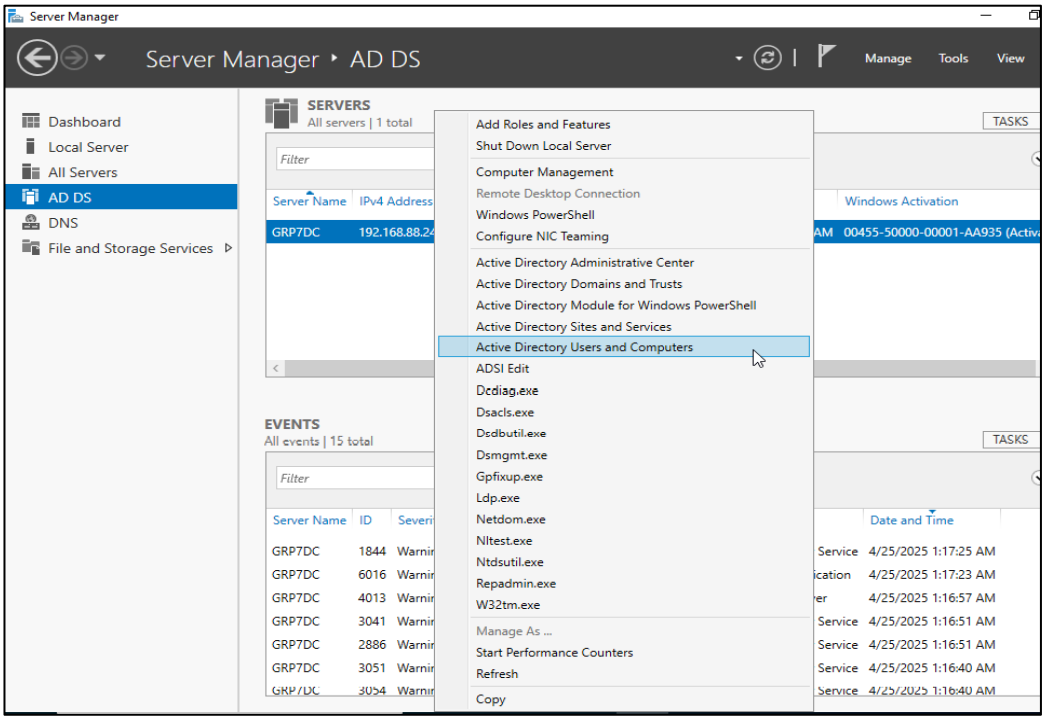

Figure 5.4.8 Go to the Active Directory Users and Computers.

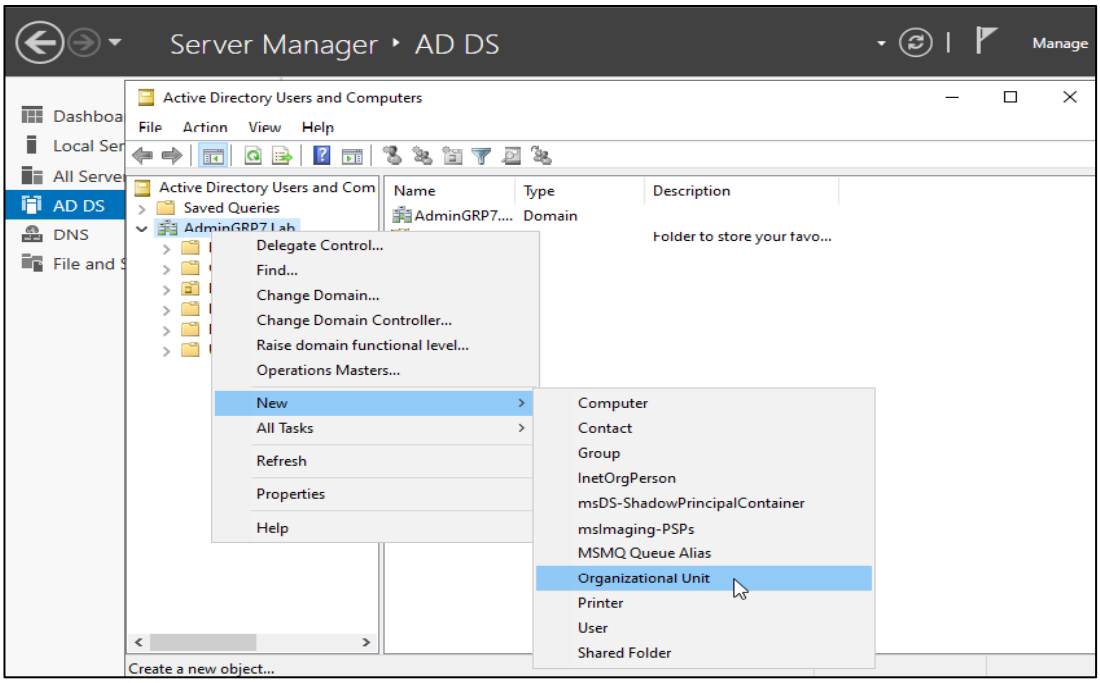

Figure 5.4.8 Creating Organizational Units (OU) Nablus and Servers in Active Directory.

Give the OU Names. See figure 5.4.9, figure 5.4.10 and figure 5.4.11

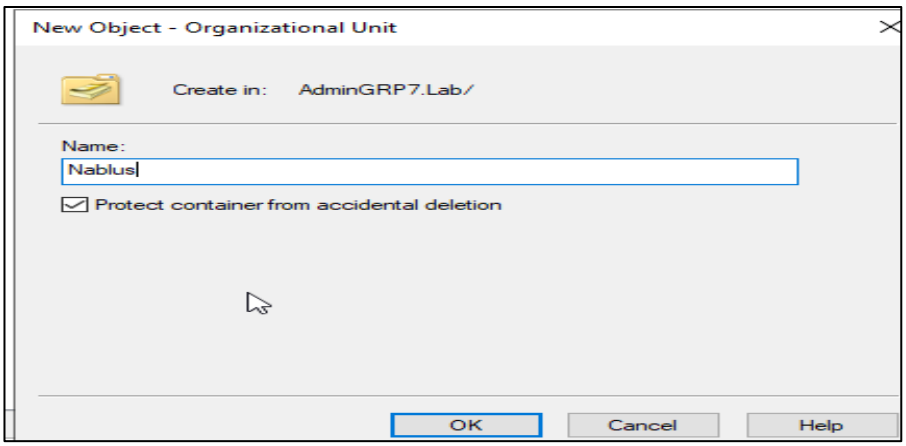

Figure 5.4.9 Nablus OU.

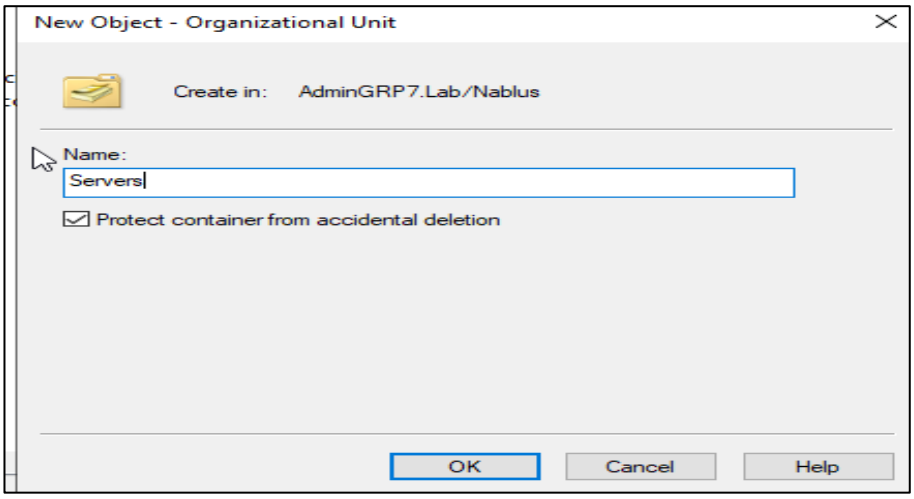

Figure 5.4.10 Servers OU.

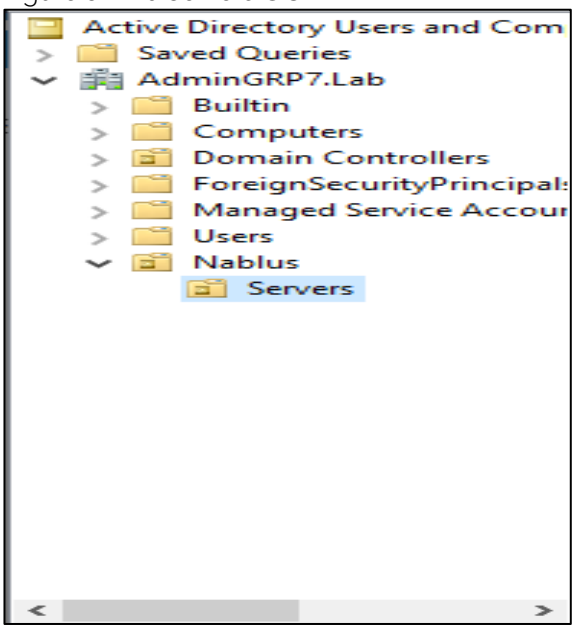

Figure 5.4.11 The final Result of Creating OU's

The File Server object is moved to the Nablus\Servers Organizational Unit (OU) in Active Directory, ensuring that the File Server is properly classified and managed within the network's organizational structure. See figure 5.4.12

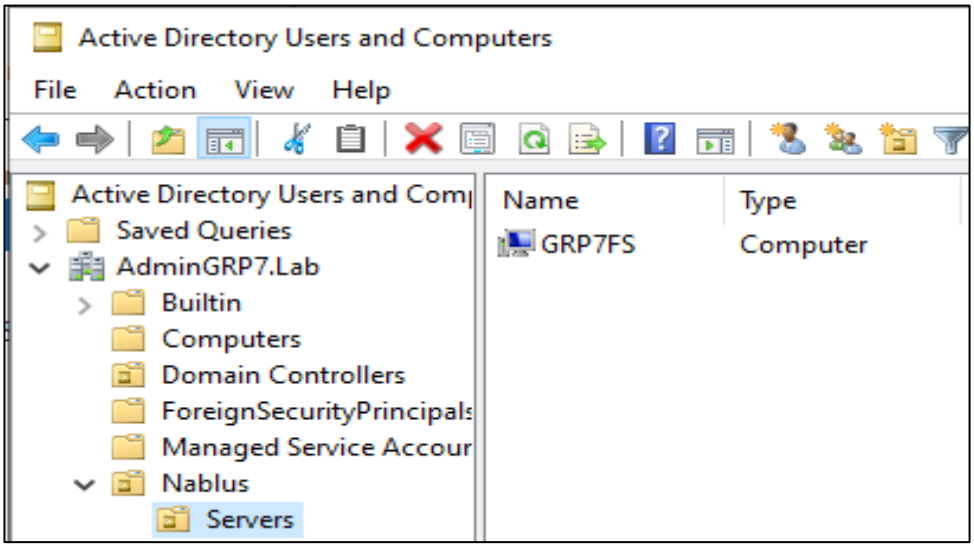

Figure 5.4.12 Moving File Server Object to Nablus\Servers Organizational Unit.

New user accounts, including FSAdmin, User1, and User2, are created in the Nablus\Users Organizational Unit (OU), allowing proper management of domain users and their associated permissions. See figure 5.4.13, figure 5.4.14, figure 5.4.15, figure 5.4.16 and figure 5.4.17

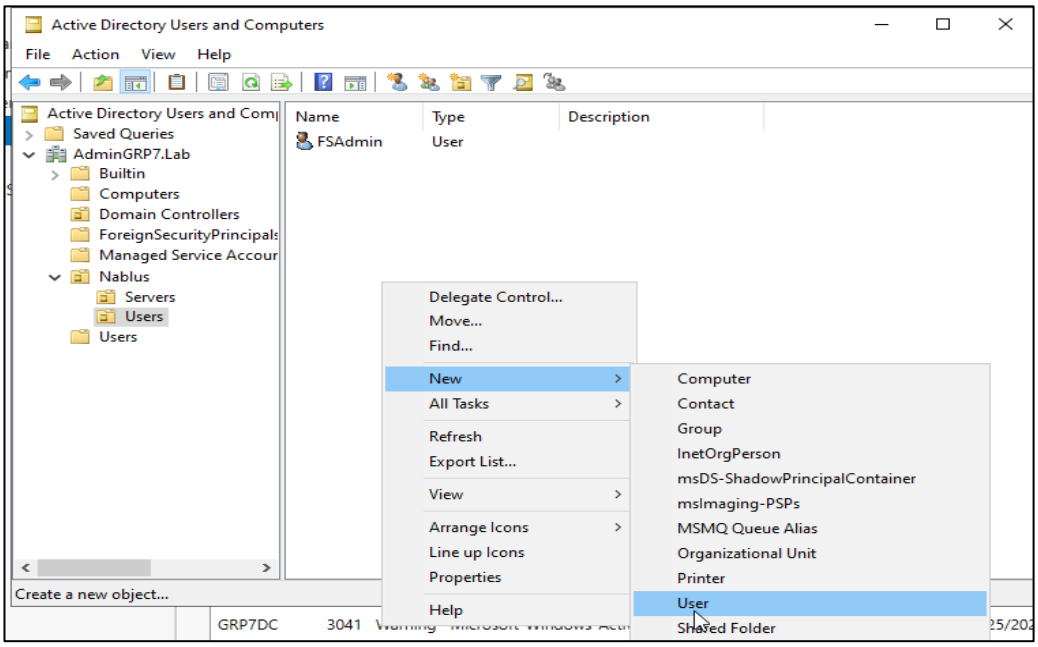

Figure 5.4.13 Creating Users inside the Users OU.

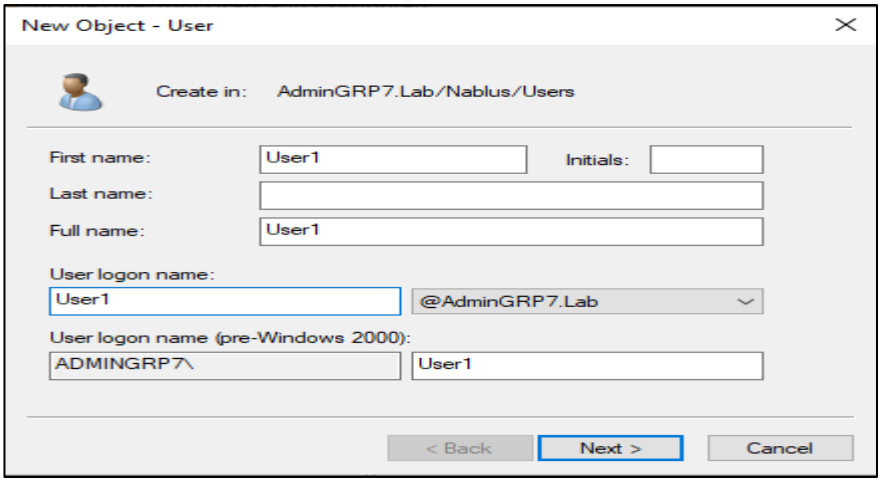

Figure 5.4.14 Naming the user then click Next.

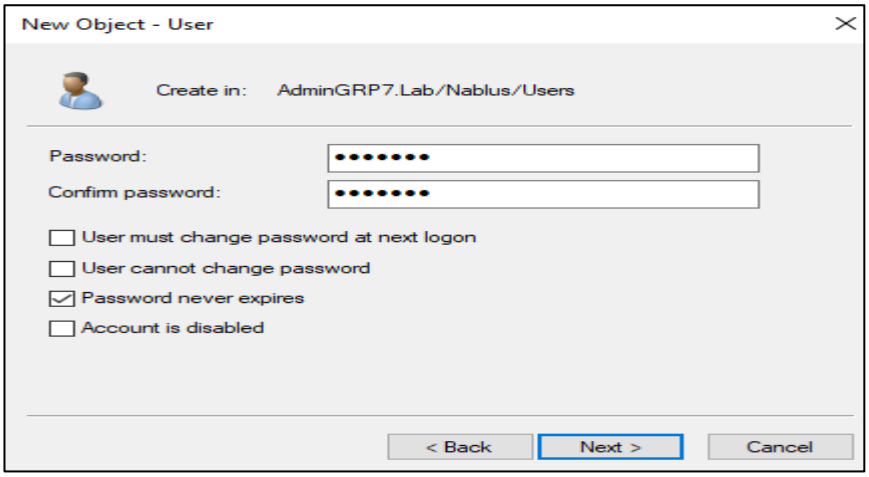

Figure 5.4.15 Type the password for the new user.

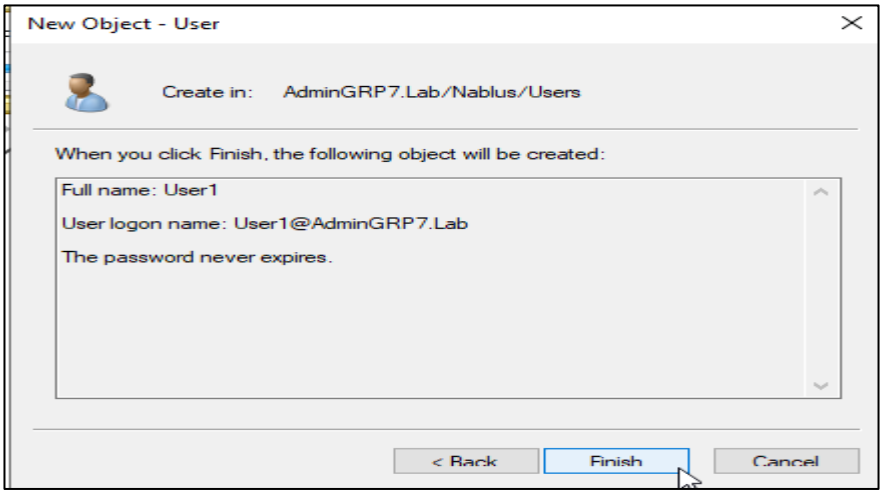

Figure 5.4.16 Finish the process of creating the user.

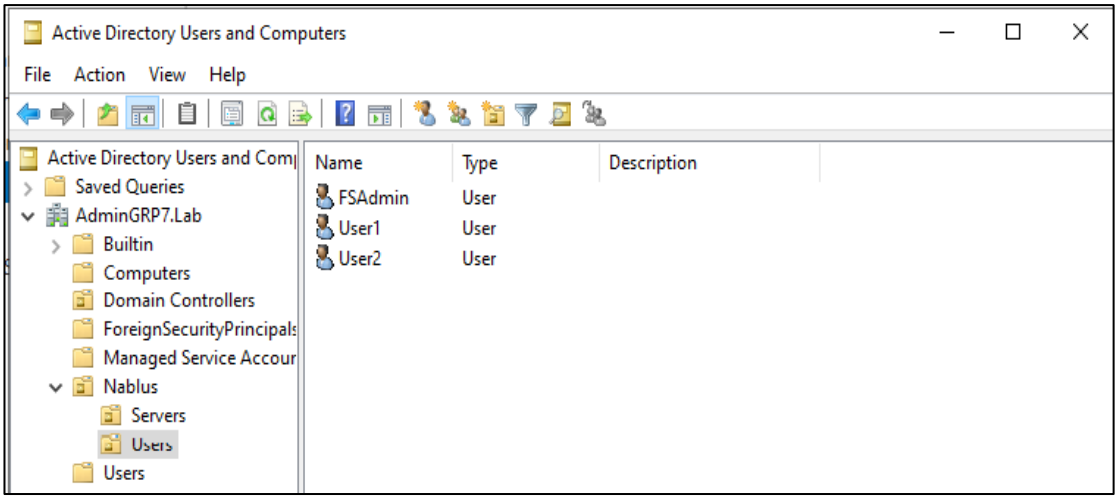

Figure 5.4.17 Creating Users FSAdmin, User1, and User2 in Nablus\Users OU.

The Domain Administrator account is used to log into the File Server, ensuring that the administrator has full access and control over the server for configuration and management tasks. See figure 5.4.18, figure 5.4.19, figure 5.4.20, figure 5.4.21 and figure 5.4.22

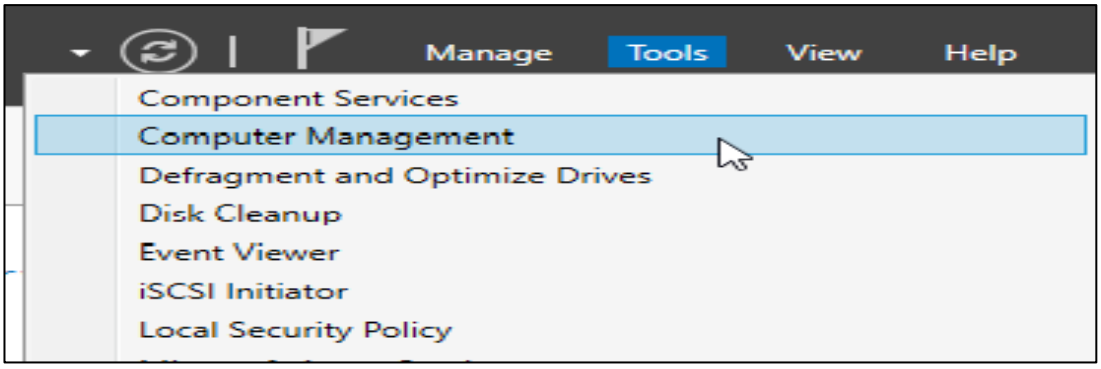

Figure 5.4.18 Selecting Computer Management from the Tools Menu in Server Manager.

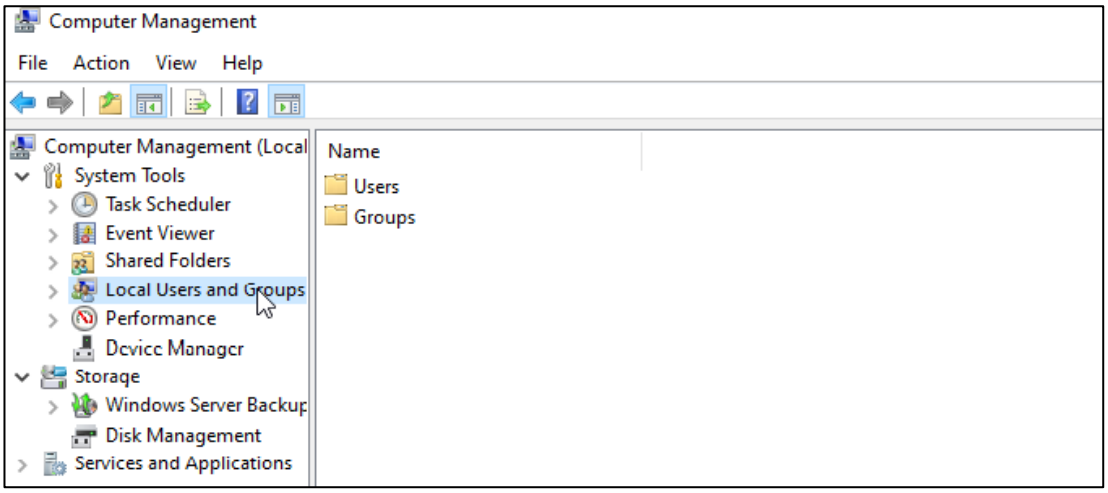

Figure 5.4.19 Navigating to Local Users and Groups in Computer Management.

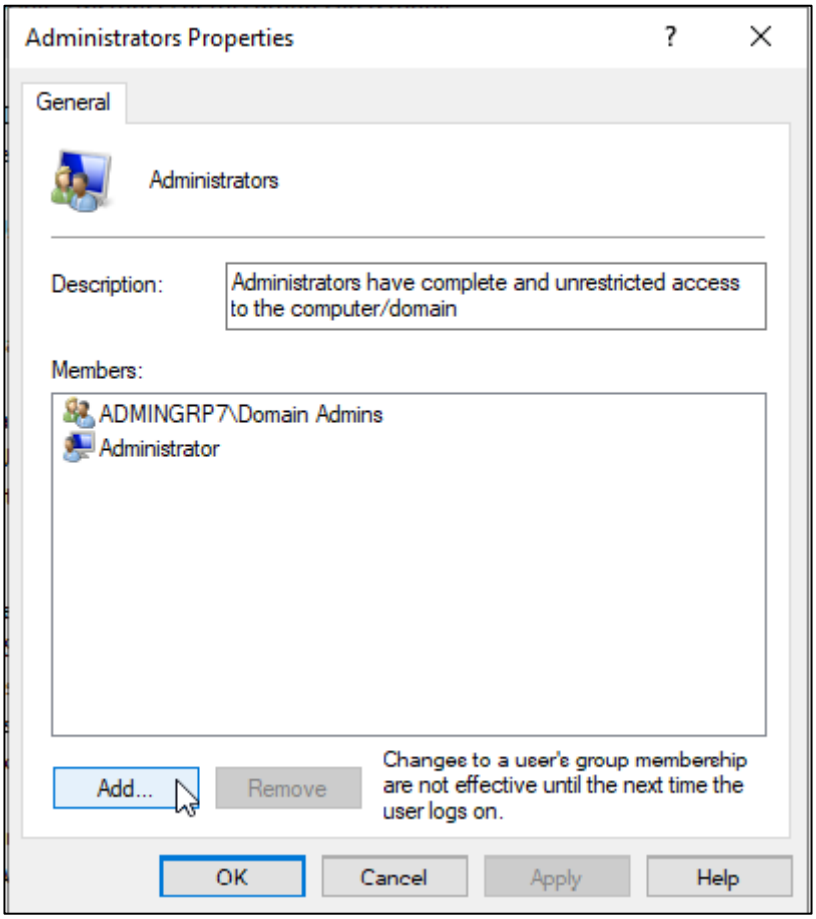

Figure 5.4.20 Adding FSAdmin to Administrators Group in Local Users and Groups.

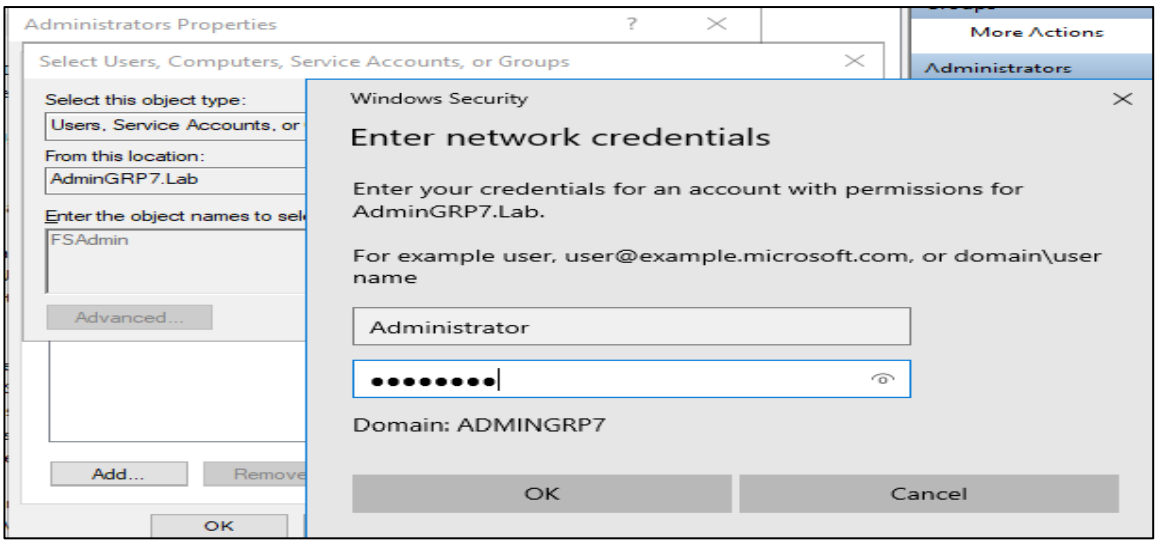

Figure 5.4.21 Entering Administrator Password to Confirm Adding FSAdmin to Administrators Group.

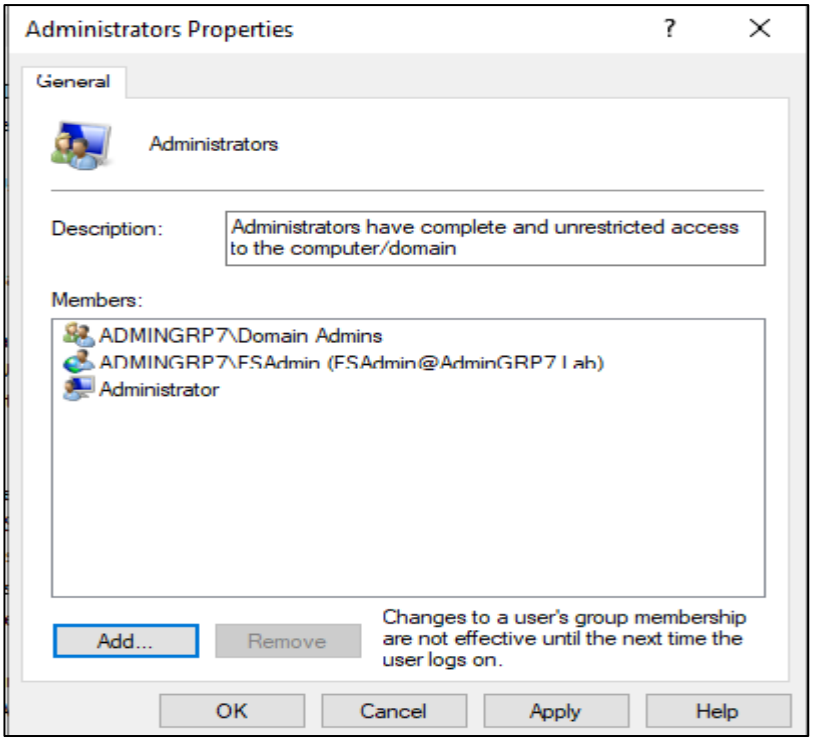

Figure 5.4.22 FSAdmin Gained Administrative Access After Being Added to Administrators Group.

FSAdmin is granted administrative rights on the File Server through Computer Management, allowing the user to perform administrative tasks on the server, such as managing shares and file permissions. After logging off from the administrator account, FSAdmin logs back in to the File Server to verify that the newly assigned administrative rights are active and functional. See figure 5.4.23

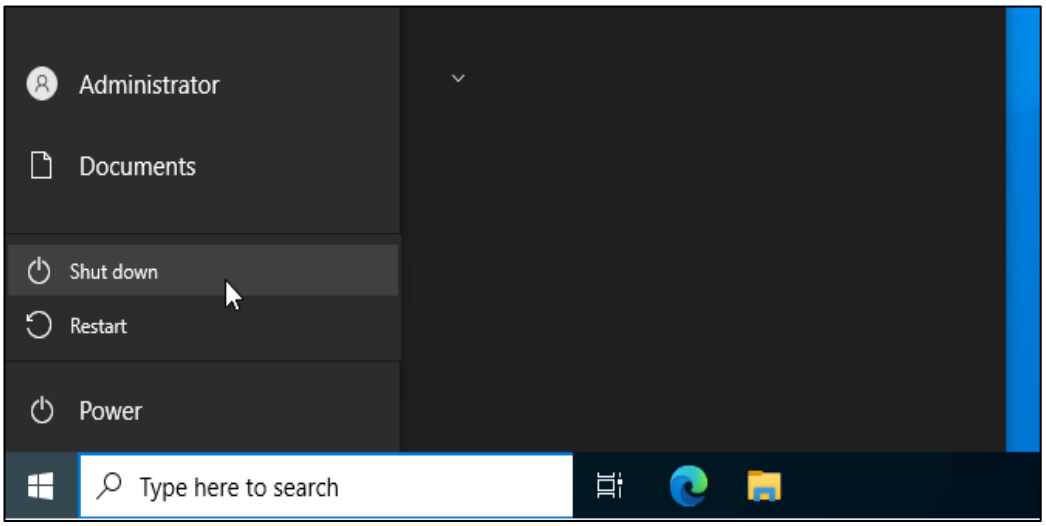

Figure 5.4.23 Logging Off and Re-Logging in as FSAdmin.

The Add Roles and Features option in Server Manager is accessed to begin the process of adding server roles and features to

the File Server for further configuration and service deployment. See figure 5.4.24

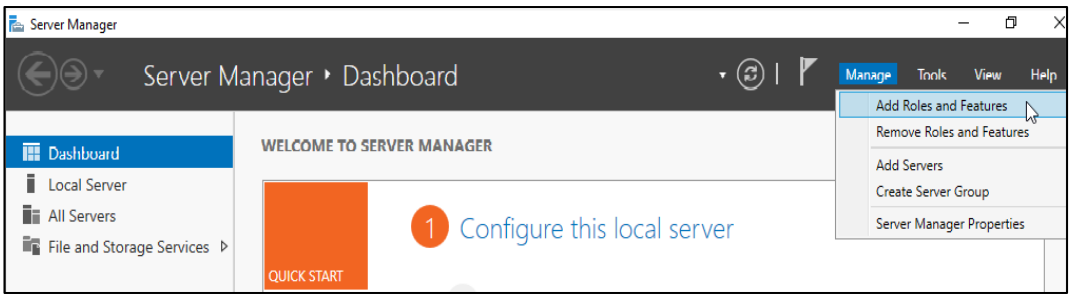

Figure 5.4.23 Navigating to Add Roles and Features in Server Manager.

The File Server role is installed under File and Storage Services in Server Manager, enabling the server to handle file storage, sharing, and related services necessary for the network. See figure 5.4.24 and figure 5.4.25

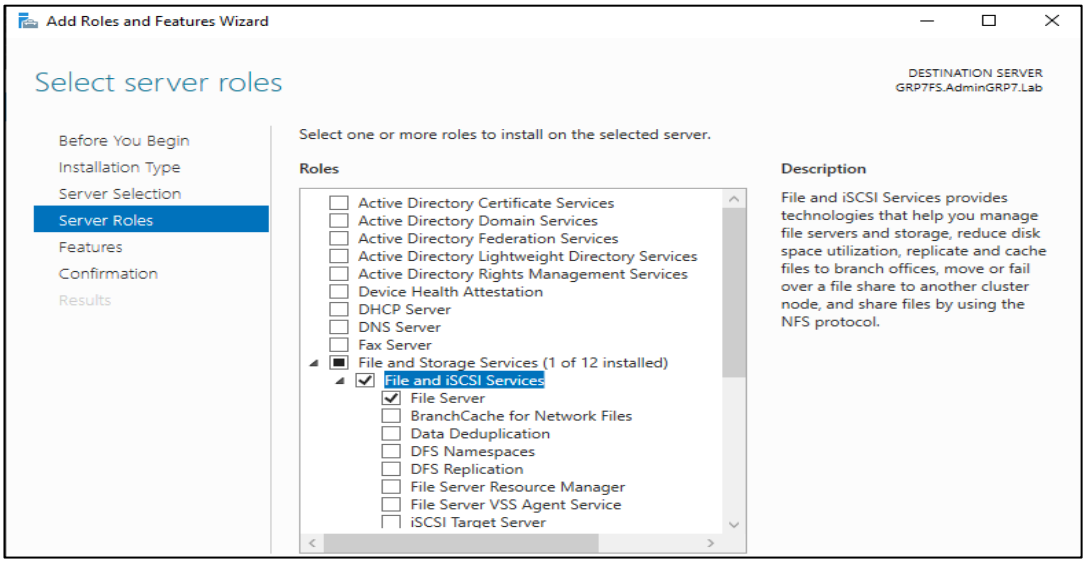

Figure 5.4.24 File and Storage Services > File and iSCSI Services >File Server.

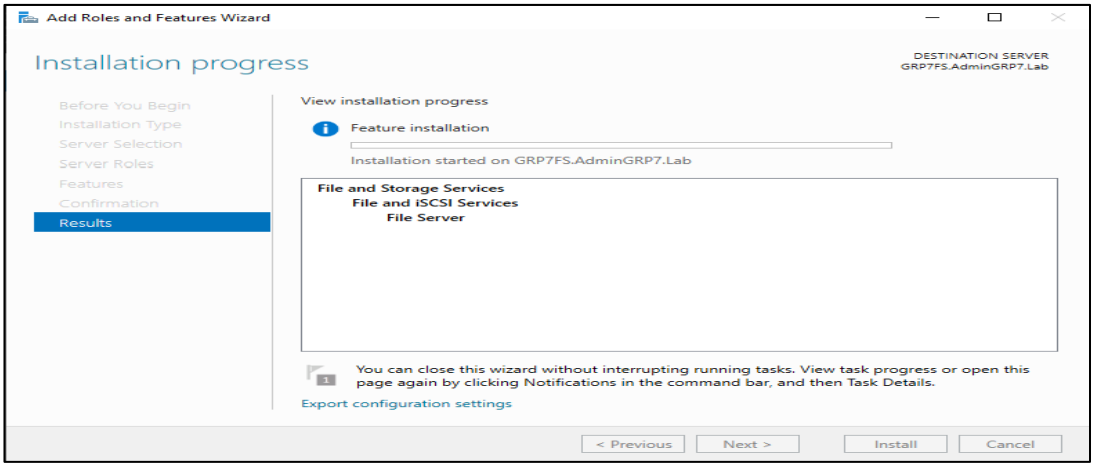

Figure 5.4.25 Installing File Server Role in File and Storage Services.

5.5 User Management and NTFS Permissions

NTFS Permissions

To manage file servers and share data between users, it is essential to understand NTFS file permissions. NTFS (New Technology File System) is the file system that Microsoft uses in its operating systems. NTFS supports assigning file and folder permissions to authenticated users and groups. These permissions are as follows:

1. Full Control: Allows users to read, write, change, and delete files and folders. In addition, users can change permissions settings for all files and subfolders.
2. Modify: Allows users to read and write files and subfolders, and also allows the deletion of folders.
3. Read & Execute: Allows users to view and run executable files, including scripts.
4. List Folder Contents: Permits viewing and listing files and subfolders, as well as executing files. This permission is inherited by folders only.
5. Read: Allows users to view the folder and subfolder contents.
6. Write: Allows users to add files and subfolders, and allows writing to a file.

In Server Manager, the File and Storage Services option is selected from the left-hand side menu to access the file sharing configuration and management tools. See figure 5.5.1

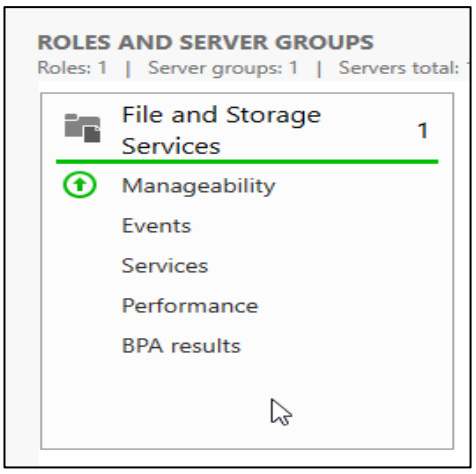

Figure 5.5.1 Selecting File and Storage Services in Server Manager.

The New Share Wizard is started to initiate the process of creating a new file share on the server, enabling users to access shared resources. See figure 5.5.2

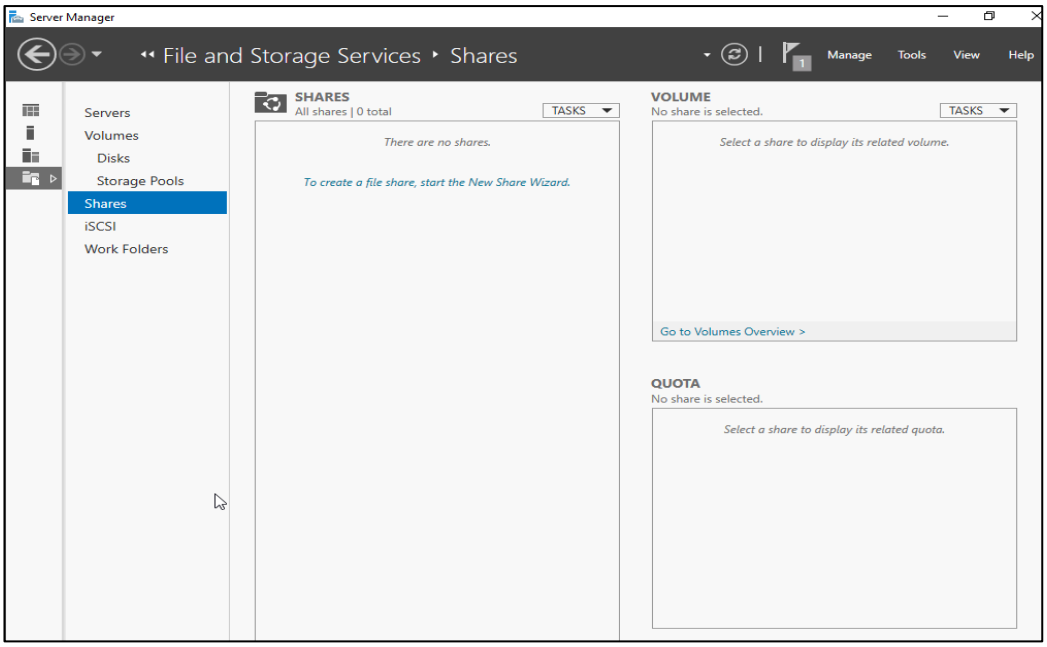

Figure 5.5.2 Starting the New Share Wizard to Create a File Share.

The SMB Share - Quick option is selected for file sharing, which provides a simple and efficient way to share files over the network using the SMB protocol. See figure 5.5.3

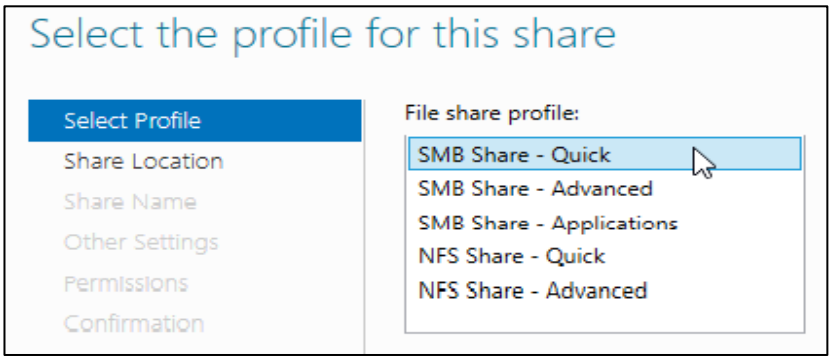

Figure 5.5.3 Selecting SMB Share - Quick Option for File Sharing.

The default share location is accepted in the wizard, allowing the file share to be created without specifying a custom location, streamlining the setup process. The share is named UsersData, and the setup process is completed by finishing the New Share Wizard, making the share available for users. See figure 5.5.4

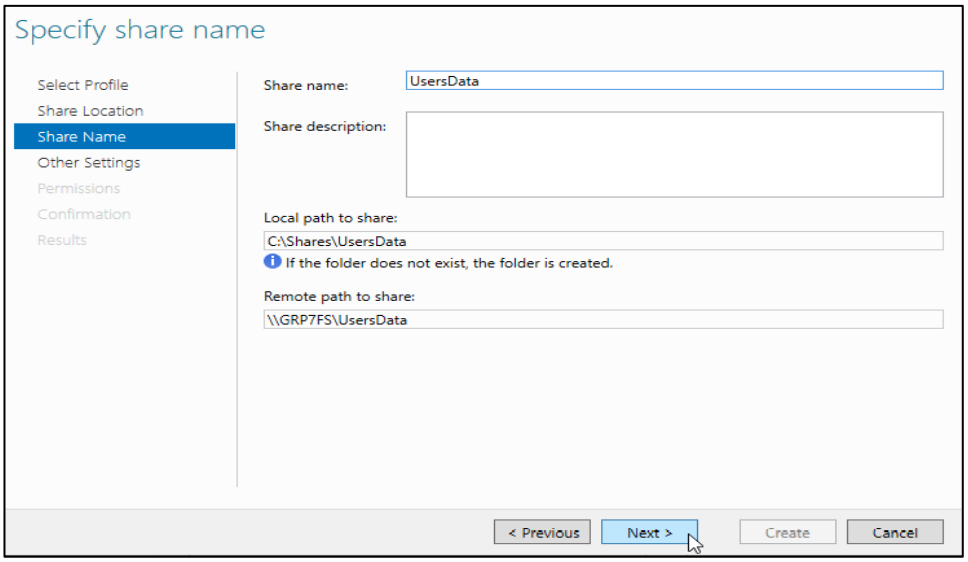

Figure 5.5.4 Proceeding with Default Share Location in New Share Wizard.

Access-Based Enumeration (ABE) is enabled for the share, ensuring that users only see the files and folders they have permission to access, and the file share setup is completed. See figure 5.5.5 and figure 5.5.6

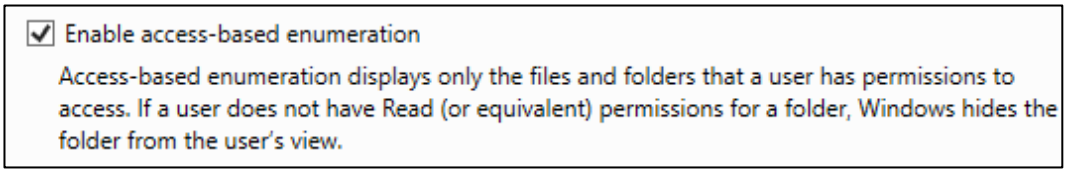

Figure 5.5.5 Enabling Access-Based Enumeration and Completing the File Share Setup.

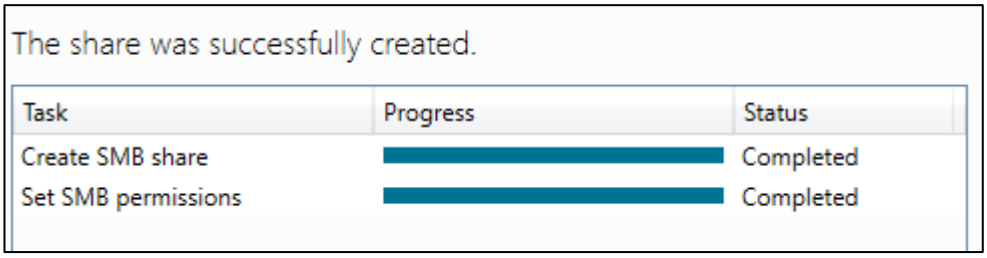

Figure 5.5.6 The share was successfully created.

The security settings for the UsersData share are modified by adding appropriate permissions for users, ensuring that only authorized users can access or modify the files. See figure 5.5.7 and figure 5.5.8

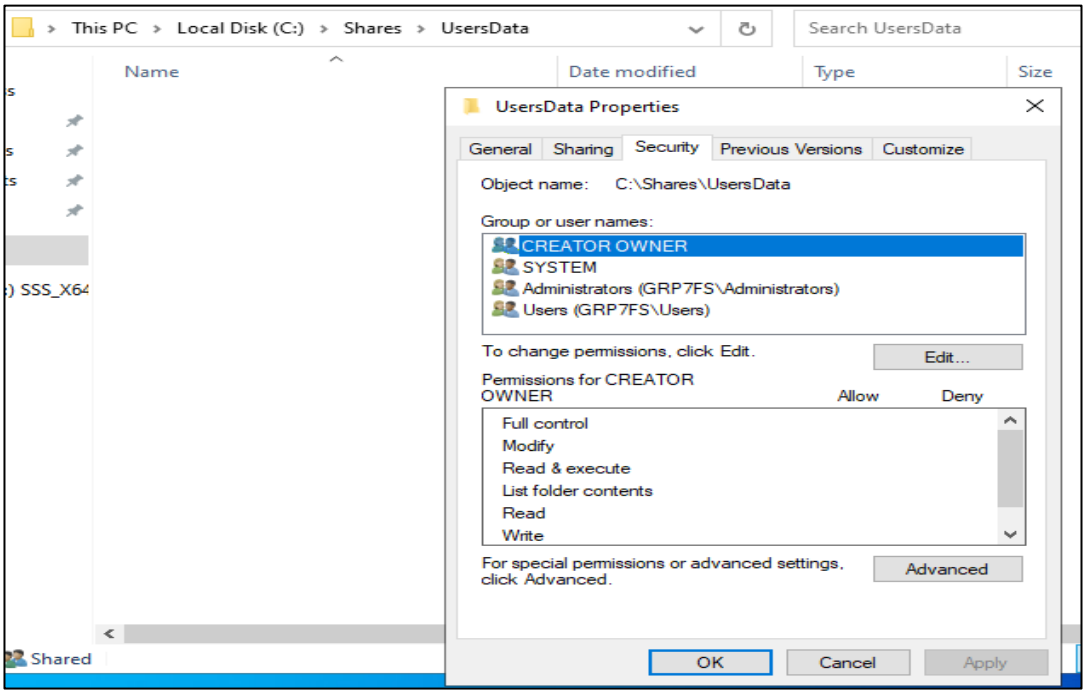

Figure 5.5.7 Modifying Security Settings for UsersData Share and Adding Permissions.

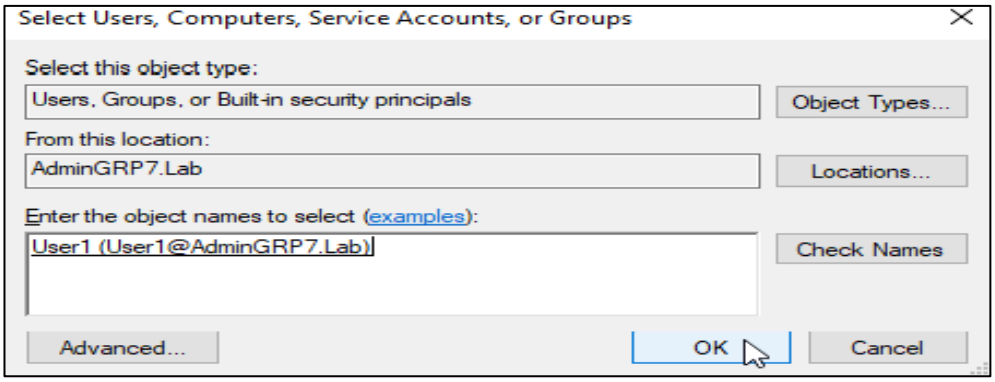

Figure 5.5.8 Adding the users on the group of users.

User1 is granted Read, Write, and Execute permissions, while User2 is assigned Modify permissions on the UsersData share, allowing them to access and edit specific files. See figure 5.5.9 and figure 5.5.10

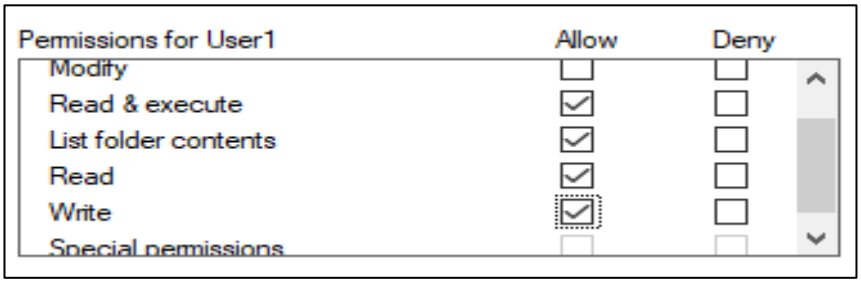

Figure 5.5.9 Assigning Read, Write, and Execute Permissions to User1

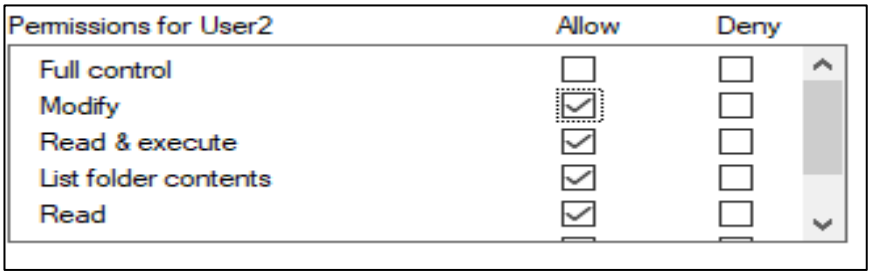

Figure 5.5.10 Assigning Modify Permission to User2

The Advanced permissions for the UsersData folder are reviewed, providing detailed control over who can access the files and the level of permissions assigned. See figure 5.5.11

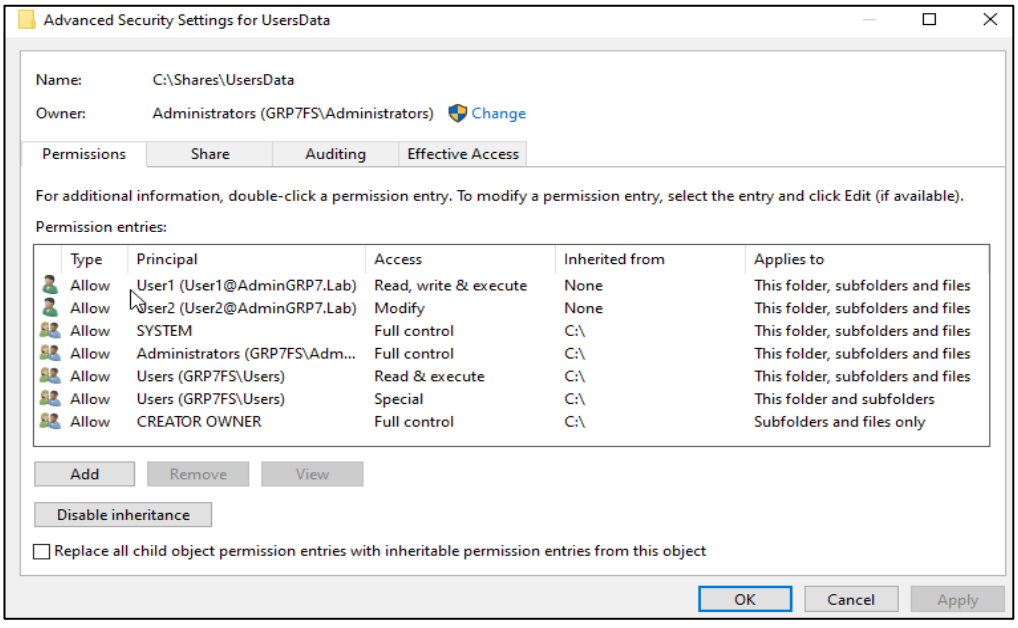

Figure 5.5.11 Viewing Advanced Permissions for UsersData Folder

Two new folders, User1 and User2, are created inside the UsersData share to organize and separate the data for each user. See figure 5.5.12

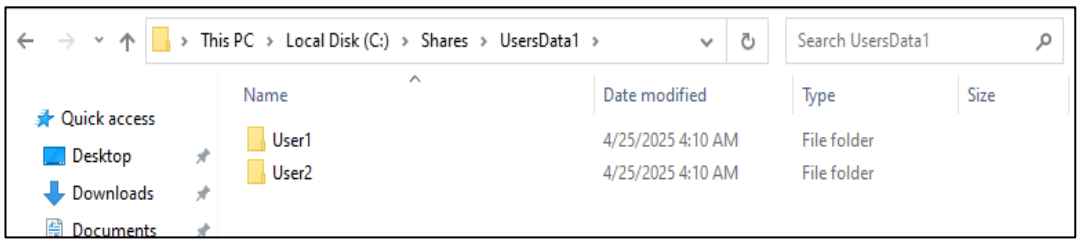

Figure 5.5.12 Creating User1 and User2 Folders Inside UsersData.

User1 File.txt and User2 File.txt are created using Notepad, each containing the respective user's name, and saved in the corresponding user's folder inside UsersData. See figure 5.5.13 and figure 5.5.14

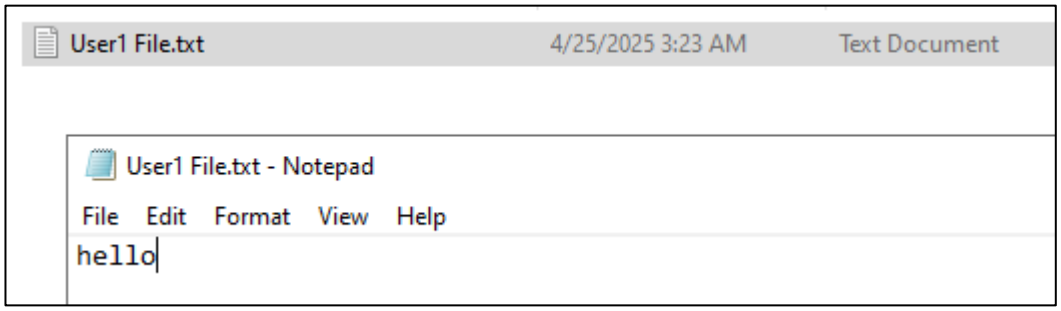

Figure 5.5.13 Creating and Saving User1 File.txt and User2 File.txt in Their Respective Folders.

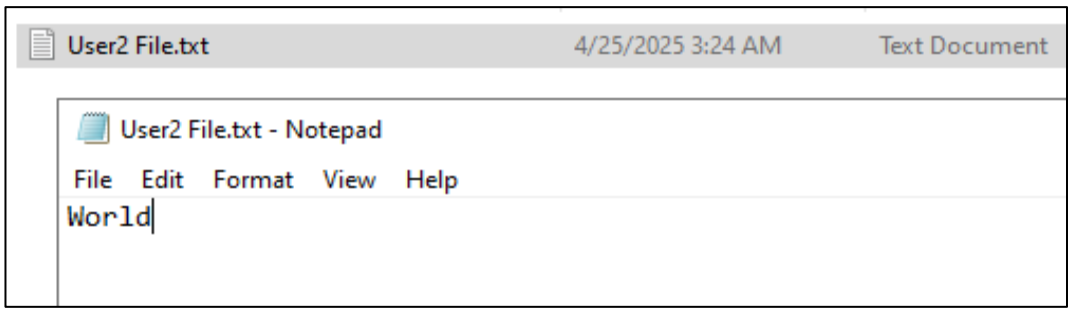

Figure 5.5.14 Creating and Saving User1 File.txt and User2 File.txt in Their Respective Folders(2).

5.6 Accessing the Shares

The File Share \\GRP7FS is accessed from Client1 with User1 logged in. This allows the user to interact with files in the shared folder according to their permissions. See figure 5.6.1, figure 5.6.2 and figure 5.6.3

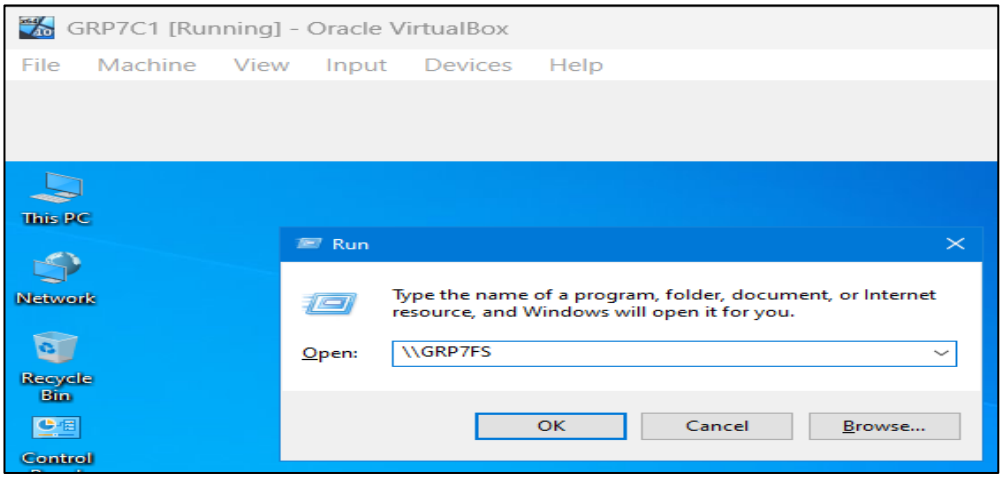

Figure 5.6.1 Accessing File Share \\GRP7FS from Client1 with User1 Logged In.

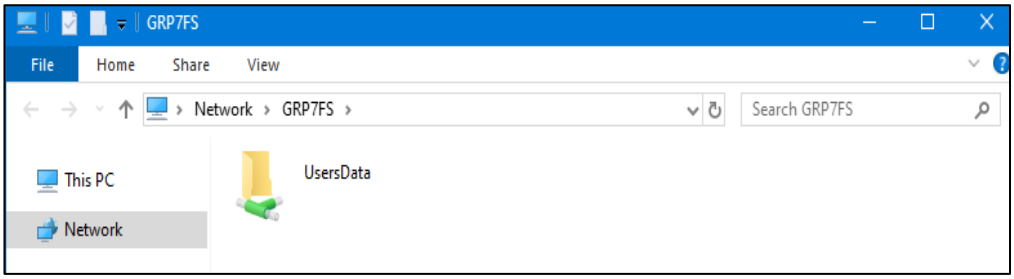

Figure 5.6.2 UsersData file on the Clinet1.

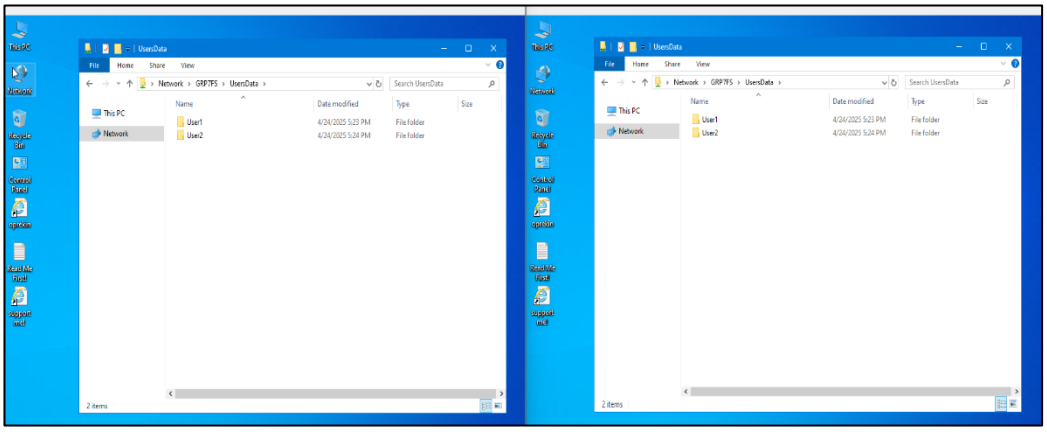

Figure 5.6.3 UsersData content file on both Clinets.

An attempt is made to delete the User1 File.txt, but permission is denied, as User1 does not have the required permissions to delete files owned by others in the shared folder. See figure 5.6.4

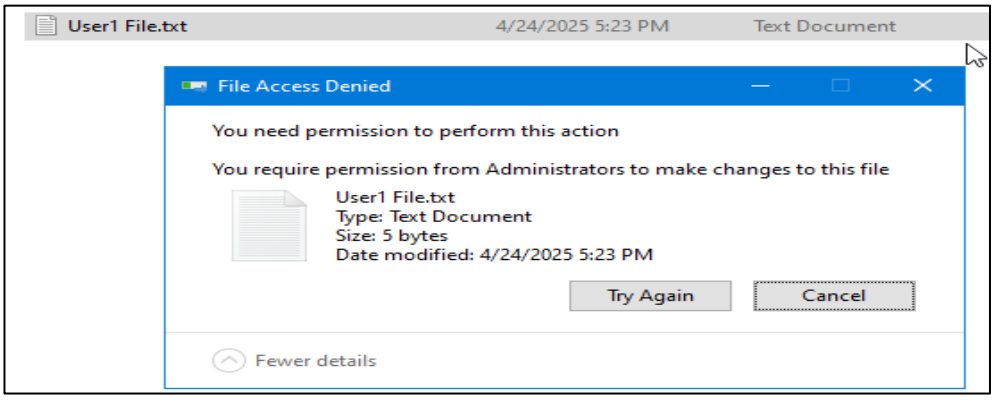

Figure 5.6.4 Attempting to Delete User1 File.txt – Permission Denied.

As the File Owner, User1 successfully creates and deletes a file in their folder, demonstrating that the owner has full control over their own files. See figure 5.6.5 and figure 5.6.6

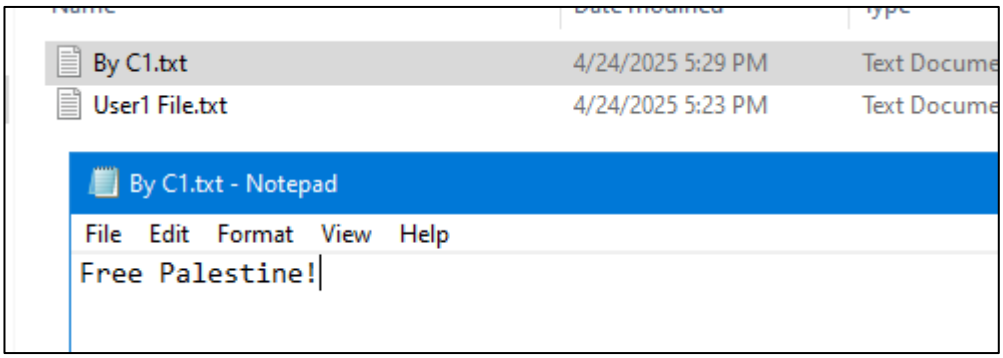

Figure 5.6.5 Create a new Notepad by User1 inside User1 folder.

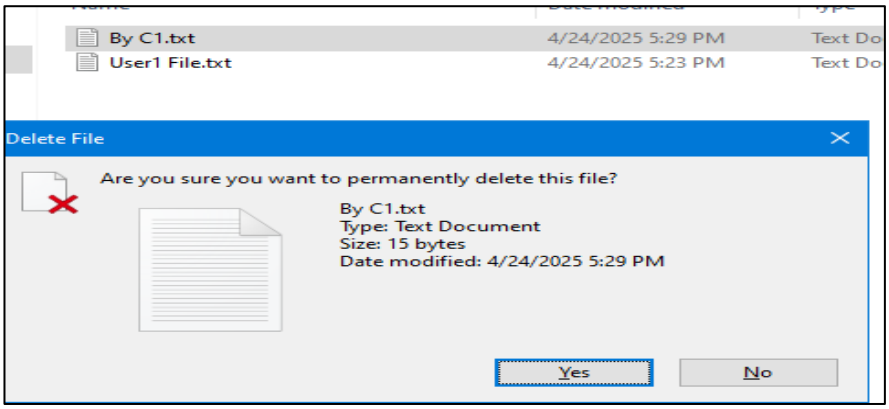

Figure 5.6.6 Creating and Deleting a File in User1 Folder as File Owner.

User1 successfully modifies User1 File.txt and saves the changes, confirming that User1 has read, write, and execute permissions for their own files. See figure 5.6.7 and figure 5.6.8

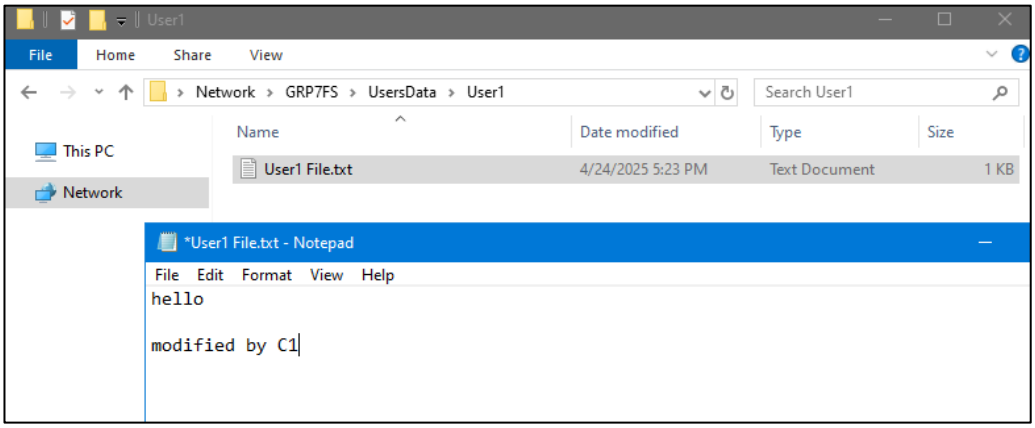

Figure 5.6.7 Modifying User1 File.txt and Saving Changes.

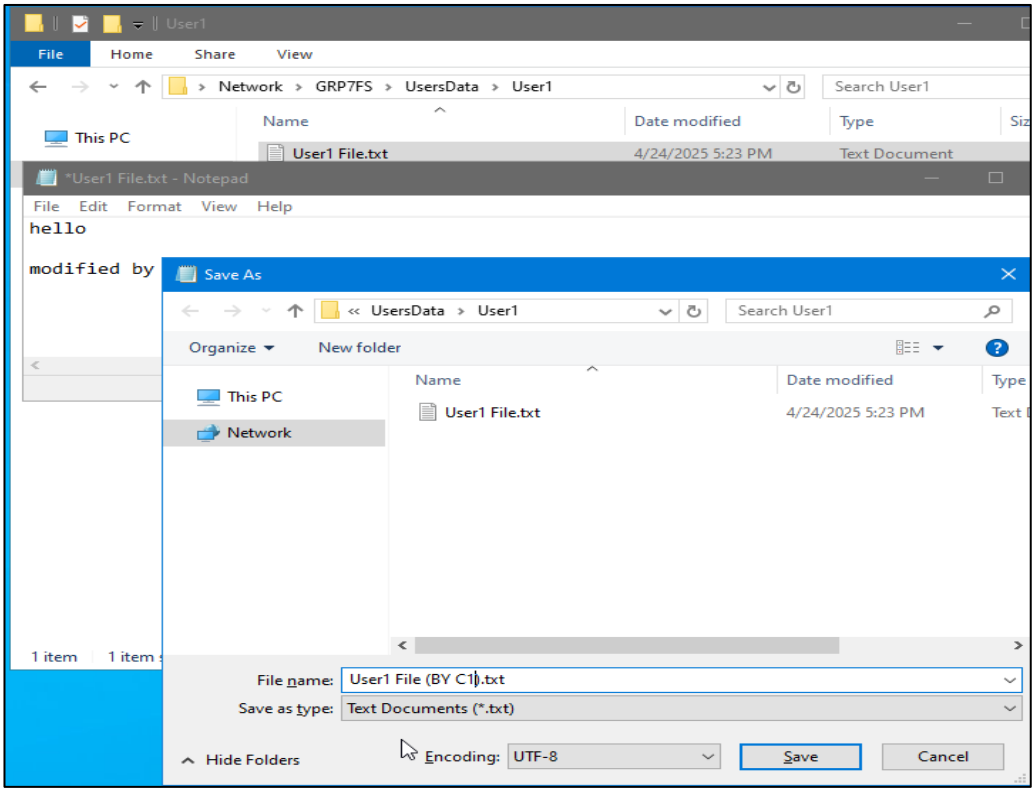

Figure 5.6.8 It will make a copy of the original file with new changes.

User2 is able to delete User2 File.txt due to having Modify permissions for their folder, allowing them to manage files within their own directory. See figure 5.6.9

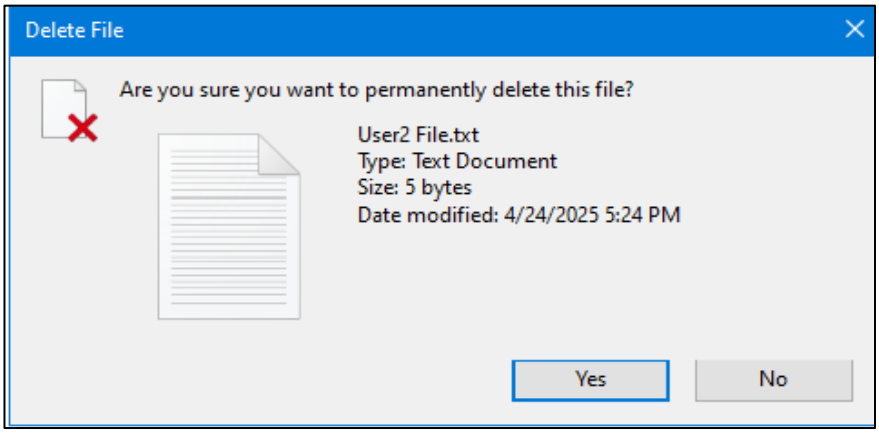

Figure 5.6.9 Deleting User2 File.txt with Modify Permissions.

An attempt is made to modify User2 permissions, but the action is denied, as User2 does not have sufficient administrative privileges to change permissions on their files. See figure 5.6.10

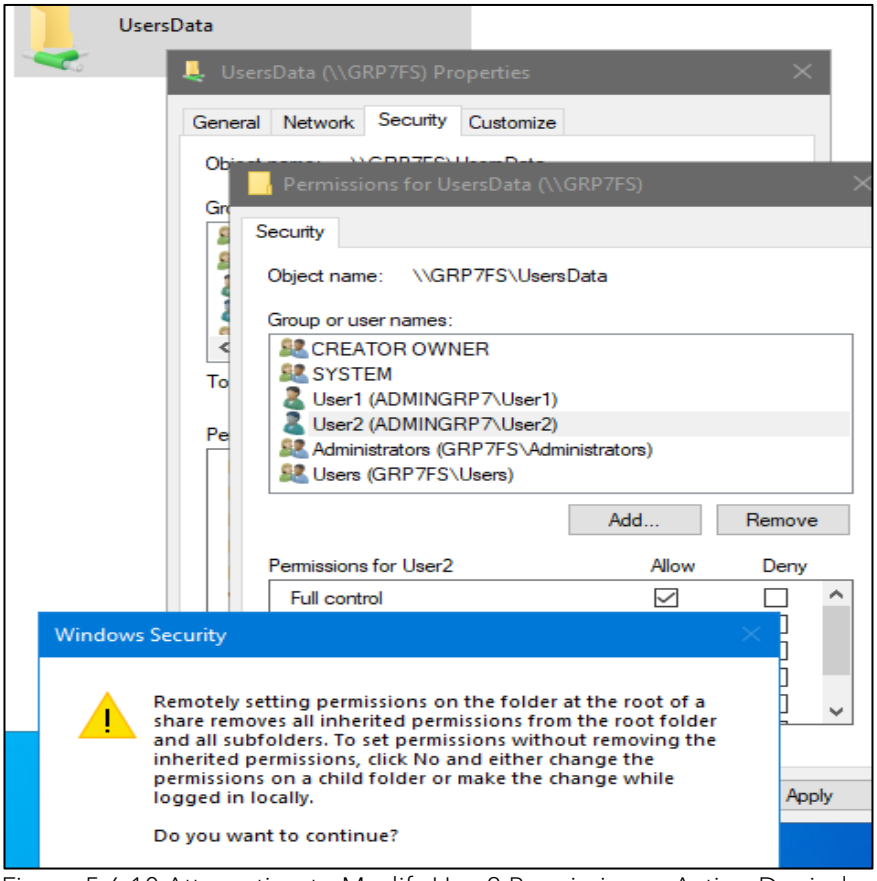

Figure 5.6.10 Attempting to Modify User2 Permissions – Action Denied.

The permissions on the UserData folder on GRP7FS are modified, and User1 is granted Full Control. This change allows User1 to have full administrative rights over their files and folders within the shared directory. See figure 5.6.11

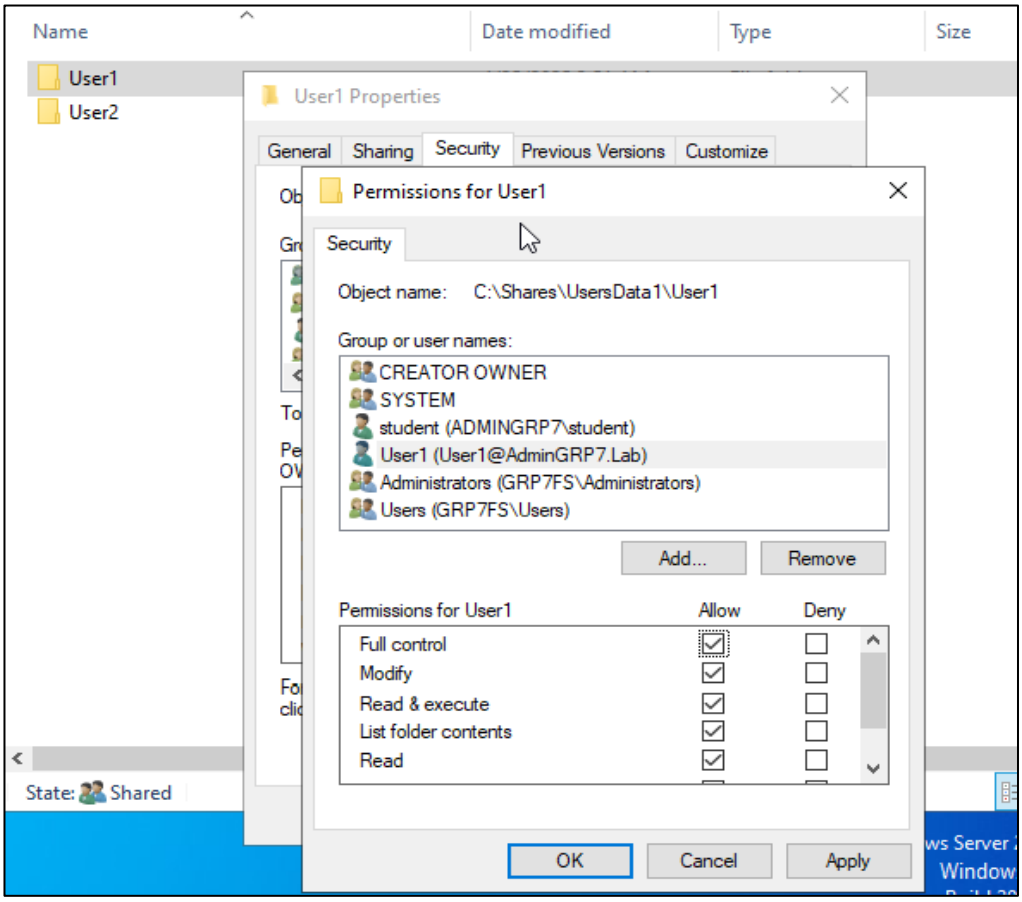

Figure 5.6.11 Modifying Permissions on UserData Folder on GRP7FS and Granting User1 Full Control.

User1 accesses \\GRP7FS\UserData from Client1 after being granted Full Control. User1 now has the necessary permissions to modify folder settings and file permissions. User1 successfully deletes User1 File.txt after the permissions update, confirming that the new full control privileges allow full file management capabilities.See figure 5.6.12 and figure 5.6.13

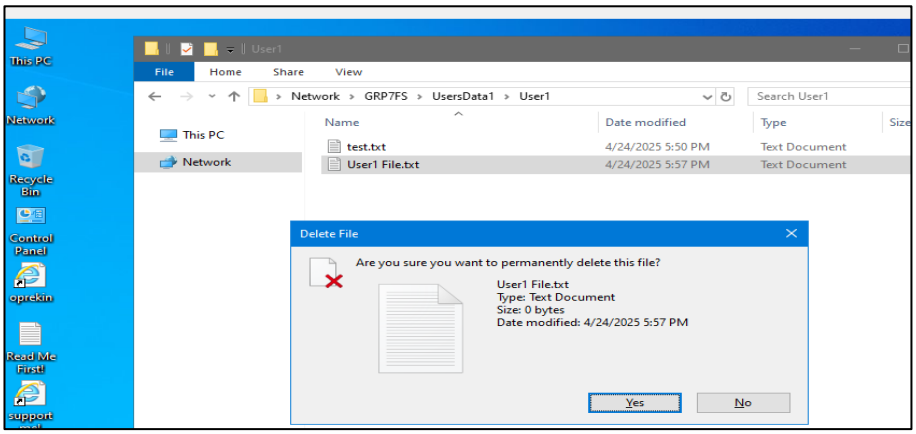

Figure 5.6.12 Trying to Delete User1 File.txt After Permissions Update.

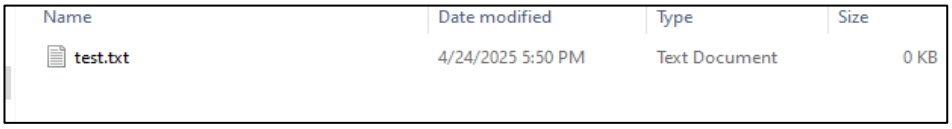

Figure 5.6.13 Successfully Deleting User1 File.txt After Permissions Update.

User1 modifies User2's permissions by removing Modify access from User2, restricting their ability to modify files in the shared folder. See figure 5.6.14

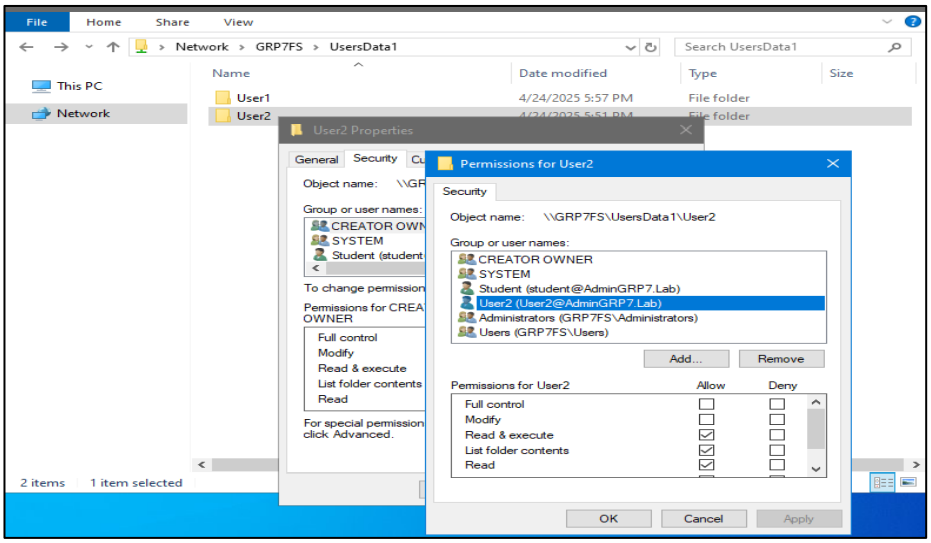

Figure 5.6.14 Modifying User2 Permissions by Removing Modify Access.

6. Results and Observations

- Domain setup and client joining were successful with domain credentials used for login.
- FSAdmin was granted admin privileges and could manage the file server independently.
- NTFS permissions were applied successfully:
    - User1 could not delete existing files but could create and delete their own files.
    - User2 could delete existing files but couldn't alter other users' permissions.
    - Upon granting Full Control to User1, all permission-related limitations were lifted.
- Access behavior accurately reflected permission settings as expected

7. Conclusion

This lab project provided hands-on experience in setting up and managing a Windows-based enterprise network using Active Directory and File Server services. It highlighted the importance of centralized management, domain control, and permission enforcement in organizational IT environments. By simulating real-world scenarios, students gained practical skills essential for future roles in network administration and cybersecurity.

8. References

- Microsoft Docs – Active Directory Domain Services Overview
- Microsoft Docs – NTFS Permissions
- Lab Guidelines from Dr. Ahmed Awwad & Eng. Ibrahim Amreya

9. Appendices

Appendix A:

VM Naming Scheme

- GRP7DC – Domain Controller
- GRP7Client1 – Client Machine 1

- GRP7Client2 – Client Machine 2
- GRP7FS – File Server

Appendix B:

IP Configuration

- GRP7DC: (IP = 192.168.88.247), (DNS = 8.8.8.8)
- GRP7Client1: (IP = 192.168.88.248), (DNS = 192.168.88.247)
- GRP7Client2: (IP = 192.168.88.250), (DNS = 192.168.88.247)
- GRP7FS: (IP = 192.168.88.249), (DNS = 192.168.88.247)