TEK-UP
Ecole Supérieure Privée
Technologie & Ingénierie

---

# Project Report

## Windows System Administration

Windows Server 2019


**Module:** Administration Système Windows

**Prepared by:** Mohamed Yacine Riabi
Abdallah Dridi

**Supervised by:** Oussama Riahi

---

Academic Year: 2025–2026

## Contents

# 1 Introduction

Active Directory is a core component of Windows-based enterprise infrastructures, providing centralized authentication, authorization, and resource management. Proper deployment and configuration of Active Directory services are essential to ensure system reliability, security, and administrative efficiency.

This project aims to explore the administration and security mechanisms of Windows Server 2019 through a hands-on approach. A complete Active Directory environment was deployed using virtualization, allowing the implementation of user and group management, Group Policy enforcement, network services, and security controls.

In addition to administrative tasks, the project also introduces a security perspective by examining common Active Directory attack techniques. This dual approach provides a comprehensive understanding of both system administration and cybersecurity principles in a controlled lab environment.

# 2 Exercise 1: Environment Preparation

This exercise aims to deploy a basic Active Directory infrastructure using VMware virtualization. The environment consists of two virtual machines: a Windows Server 2019 acting as the Domain Controller and a Windows 10 client workstation.

## 2.1 a) Windows Server 2019 Installation

A Windows Server 2019 virtual machine is installed and configured to act as the Primary Domain Controller (PDC) for the domain.

- Machine name: `PDC_MohamedYacineRiabi_AbdallahDridi`

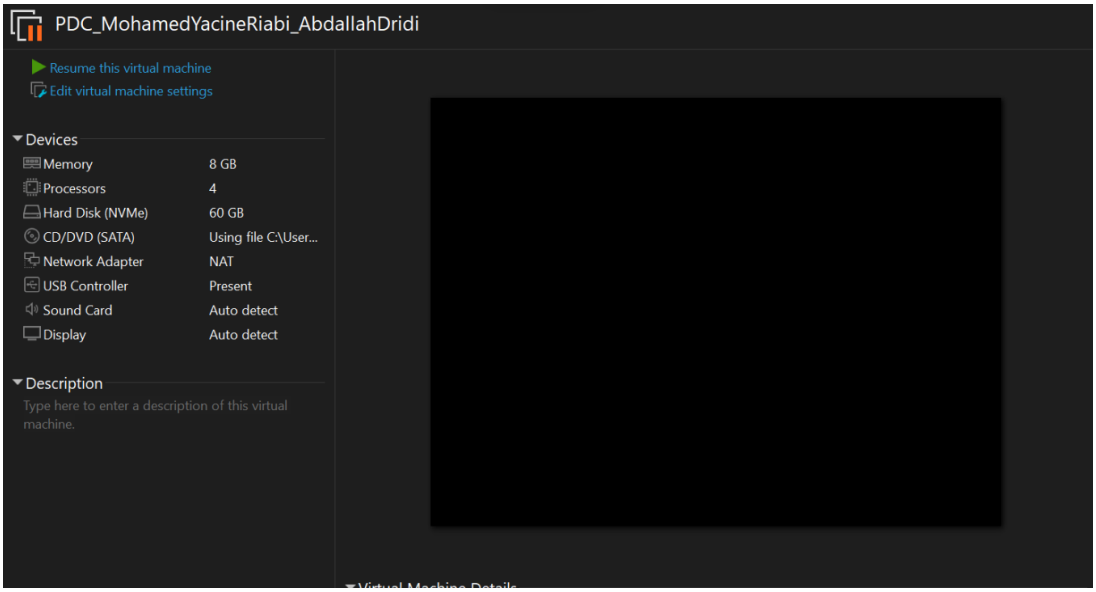


Figure 1: Windows Server 2019 virtual machine installation

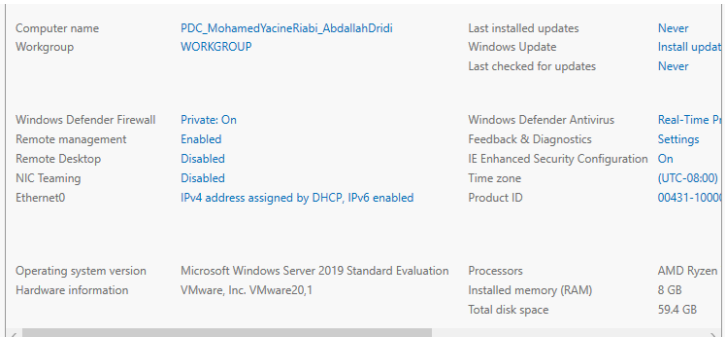


Figure 2: Server hostname configuration

## 2.2 b) Windows 10 Client Installation

A Windows 10 virtual machine is installed to serve as a client workstation. This machine will later be joined to the Active Directory domain for authentication and centralized management.

- Machine name: `PC1_MohamedYacineRiabi_AbdallahDridi`

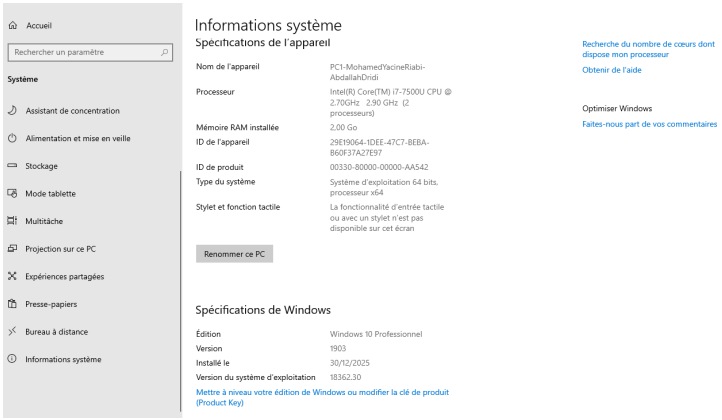


Figure 3: Windows 10 client prepared for domain integration

## 2.3 c) Active Directory Domain Creation

Active Directory Domain Services (AD DS) is installed on the Windows Server. A new domain named `test.local` is created, and the server is promoted to Domain Controller with DNS configured automatically.

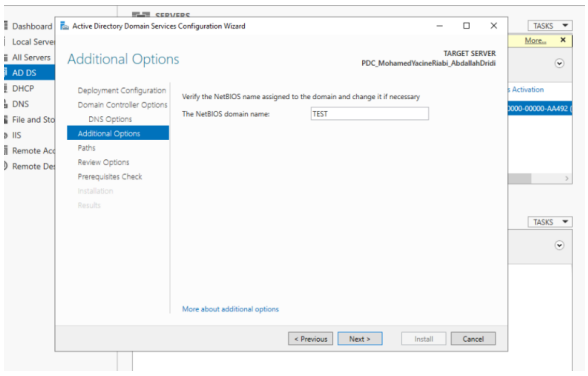


Figure 4: Creation of the `test.local` domain

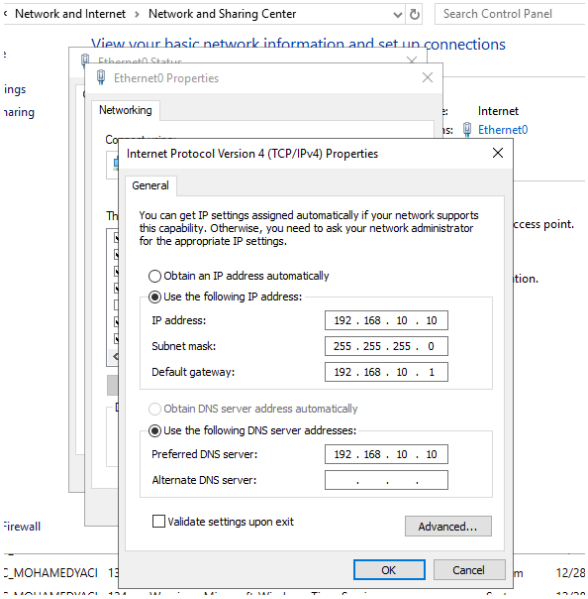


Figure 5: IPv4 network configuration on the server

```
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : PDC_MohamedYacineRiabi_AbdallahDridi
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-F9-35-78
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::78d4:7e8:cbe0:c7b6%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 83889193
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-30-E3-4A-63-00-0C-29-F9-35-78
   DNS Servers . . . . . . . . . . . : 192.168.10.10
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Figure 6: Verification of network configuration using `ipconfig`

## 3 Exercise 2: Active Directory Object Management

This exercise focuses on the management of Active Directory objects using the *Active Directory Users and Computers* console. Organizational Units (OUs), user accounts, and computer objects are created and verified within the `test.local` domain.

### 3.1 a) Creation of Organizational Units

The following Organizational Units (OUs) are created under the `test.local` domain in order to logically organize users and administrative resources.

- `services_informatiques_MohamedYacineRiabi_AbdallahDridi`
- `ressources_humaines_MohamedYacineRiabi_AbdallahDridi`
- `Administration_MohamedYacineRiabi_AbdallahDridi`
- `Classe_A_MohamedYacineRiabi_AbdallahDridi`

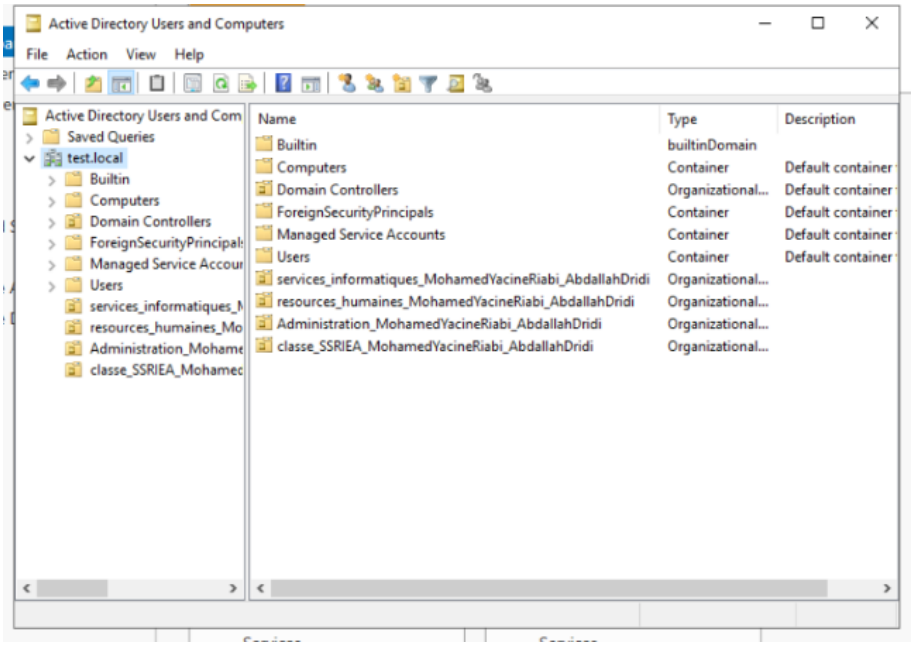


Figure 7: Organizational Units created in the `test.local` domain

## 3.2 b) User Creation in `services_informatiques`

A user account named `oussama riahi` is created in the `services_informatiques` OU. To enforce security best practices, the option *User must change password at next logon* is enabled.

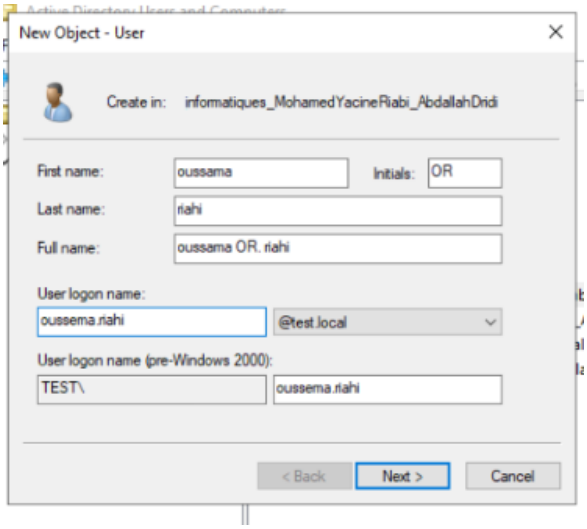


Figure 8: Creation of user `oussama riahi`

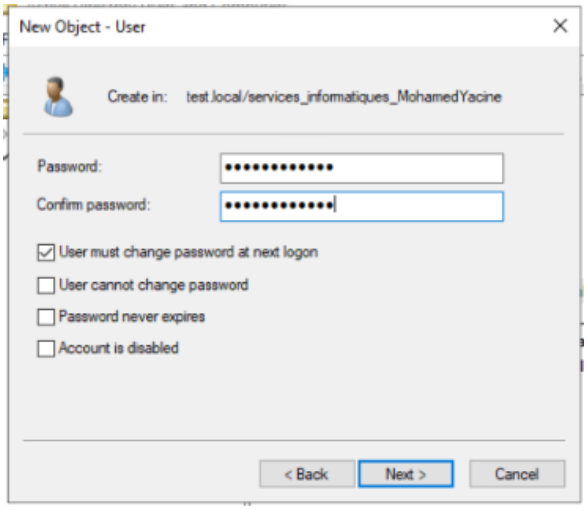


Figure 9: Password change required at first logon

## 3.3 c) User Creation in `Classe_A`

Student user accounts are created inside the `Classe_A` OU using their first and last names. Each account is configured to require a password change upon the first authentication.

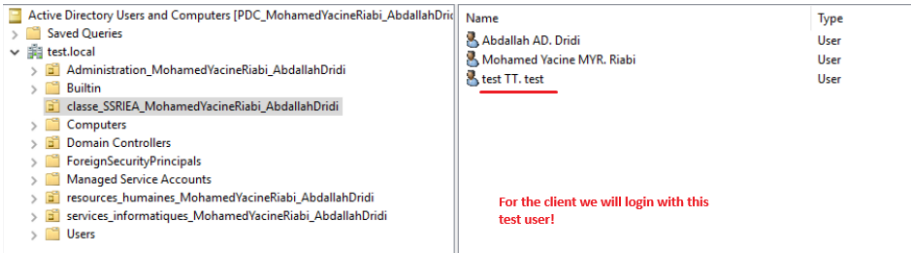


Figure 10: Student user accounts created in the `Classe_A` Organizational Unit

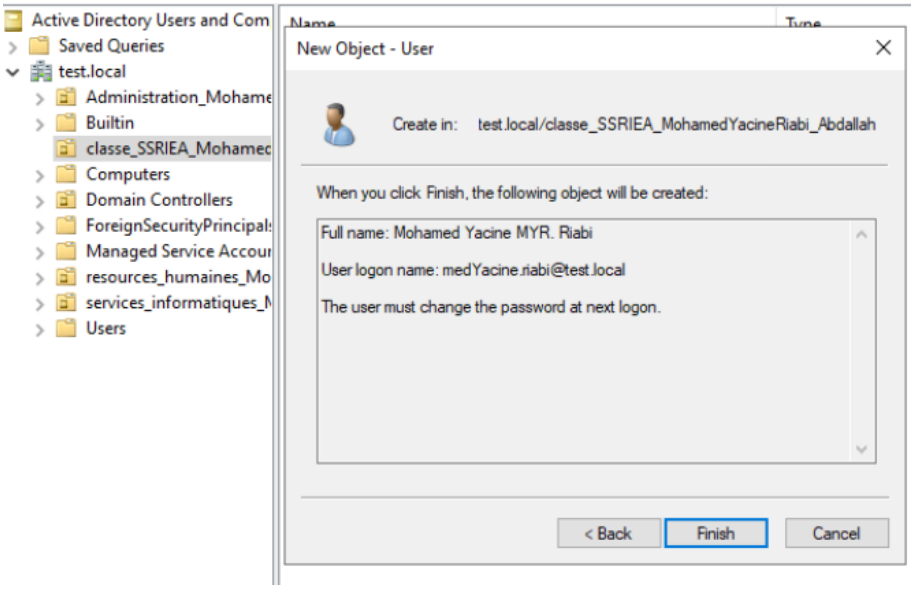


Figure 11: Student 1 creation

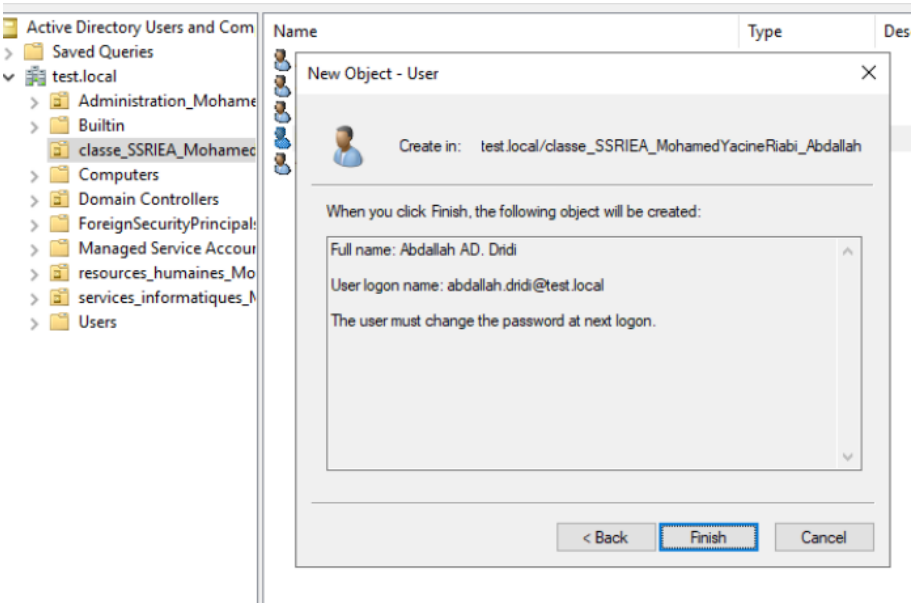


Figure 12: Student 2 creation

### 3.4 d) User Creation in `ressources_humaines`

A user account named **`aissa zeghabi`** is created in the **`ressources_humaines`** OU. The password policy is configured so that the password never expires.

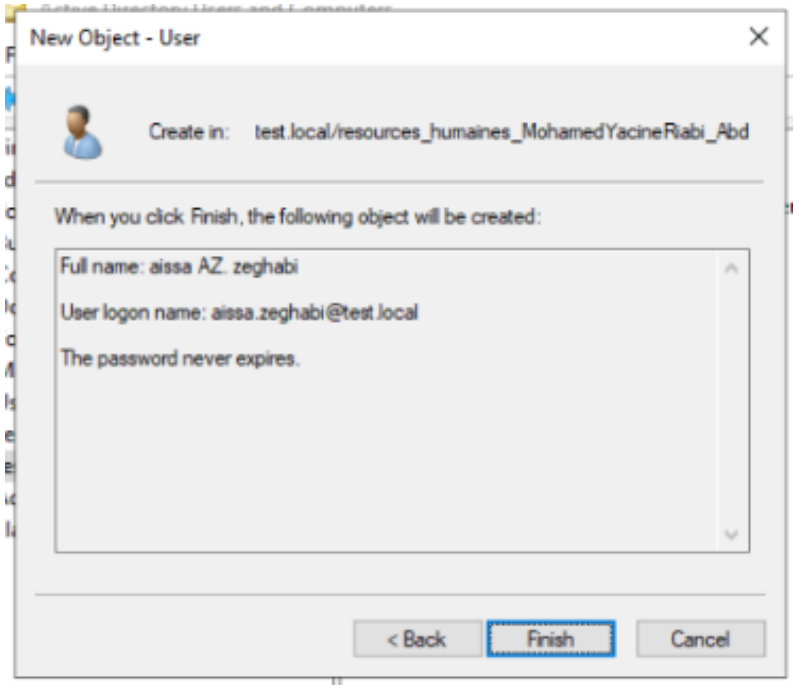


Figure 13: User **`aissa zeghabi`** configured with a non-expiring password

### 3.5 e) User Creation in `Administration`

Two administrative user accounts are created in the **`Administration`** OU.

- **`Amira Ghalmi`**
- **`Olfa Mabrouk`**

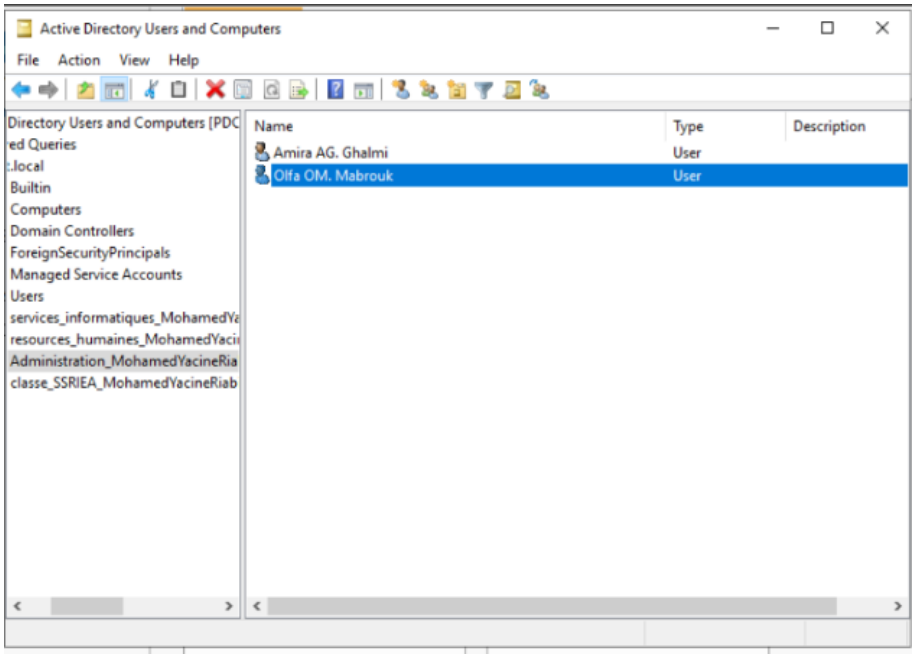


Figure 14: Administrative user accounts created in the `Administration` OU

### 3.6 f) Joining the Windows 10 Client to the Domain

The Windows 10 client machine `PC1_MohamedYacineRiabi_AbdallahDridi` is configured with appropriate IPv4 settings and joined to the `test.local` domain using domain administrator credentials.

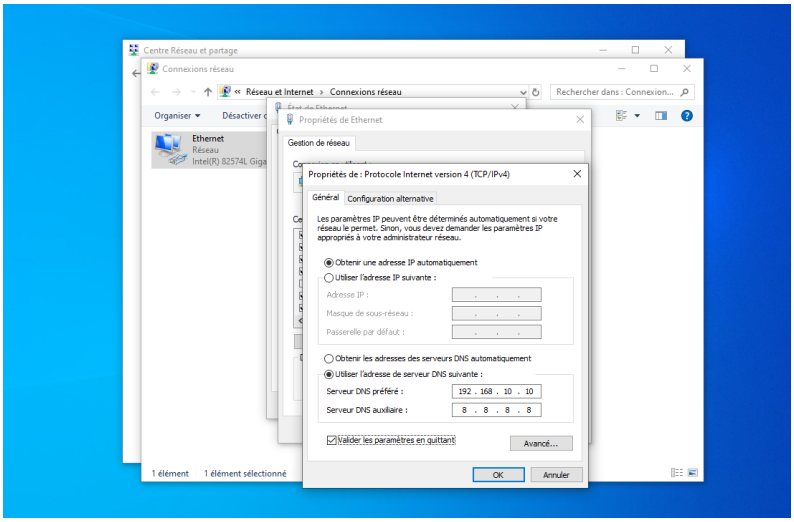


Figure 15: IPv4 network configuration of the Windows 10 client

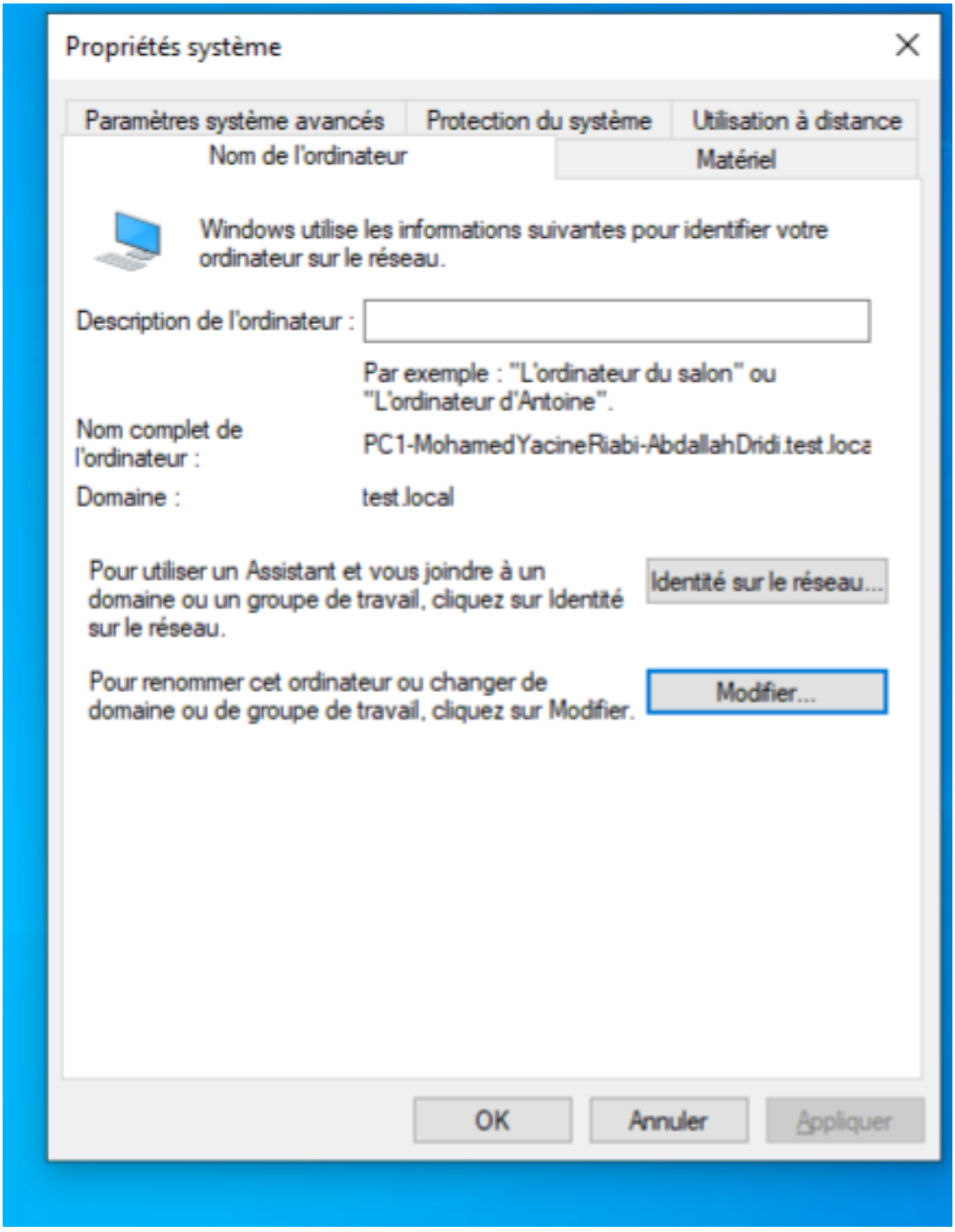


Figure 16: Windows 10 client successfully joined to the `test.local` domain

### 3.7 g) Verification of Client Computer Object

After joining the domain, the successful registration of the client machine is verified on the Windows Server using the *Active Directory Users and Computers* console. The computer account appears in the default `Computers` container.

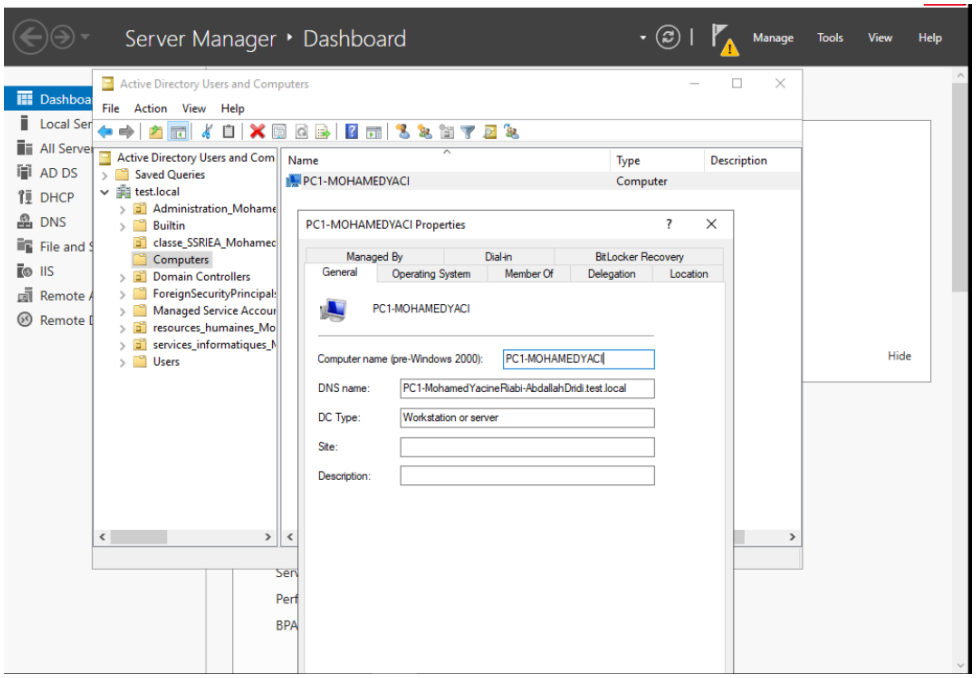


Figure 17: Client computer object visible in Active Directory

### 3.8 h) Authentication Test

A login attempt is performed on the Windows 10 client using the test account created in the `Classe_A` OU. The successful authentication confirms correct user configuration and full domain integration.

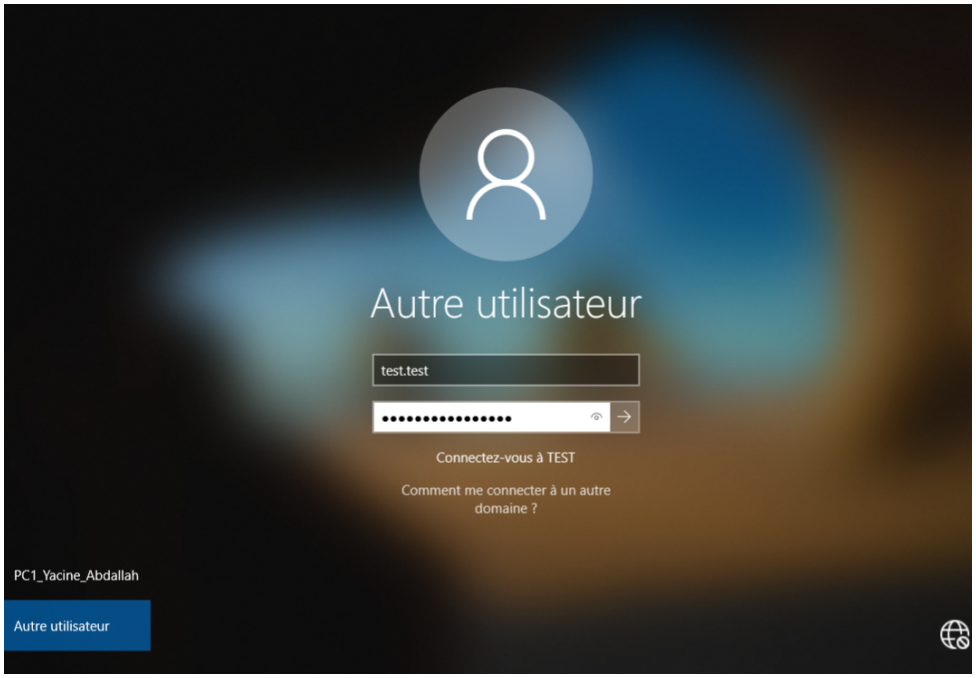


Figure 18: Successful authentication using a domain user account

# 4 Exercise 3: Group Policy Management

This exercise focuses on the implementation of Group Policy Objects (GPOs) to enforce security restrictions and administrative controls across different Organizational Units (OUs) within the `test.local` domain.

All GPOs follow the naming convention below:

`GPO_<POLICY_NAME>_MohamedYacineRiabi_AbdallahDridi`

## 4.1 a) GPOs Applied to `Classe_A`

The following GPOs are linked to the `Classe_A` Organizational Unit in order to restrict access to system-level tools for student users.

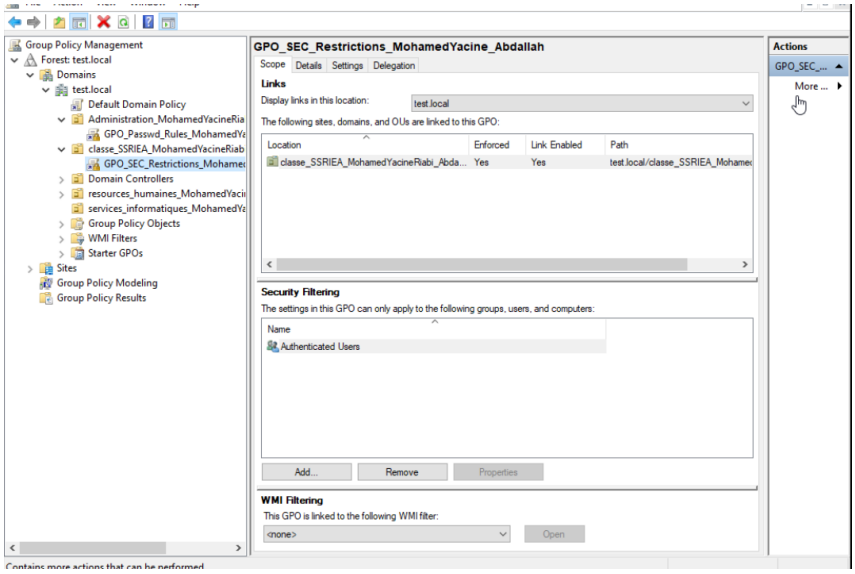


Figure 19: Group Policy Objects linked to the `Classe_A` Organizational Unit

### Disable Command Prompt

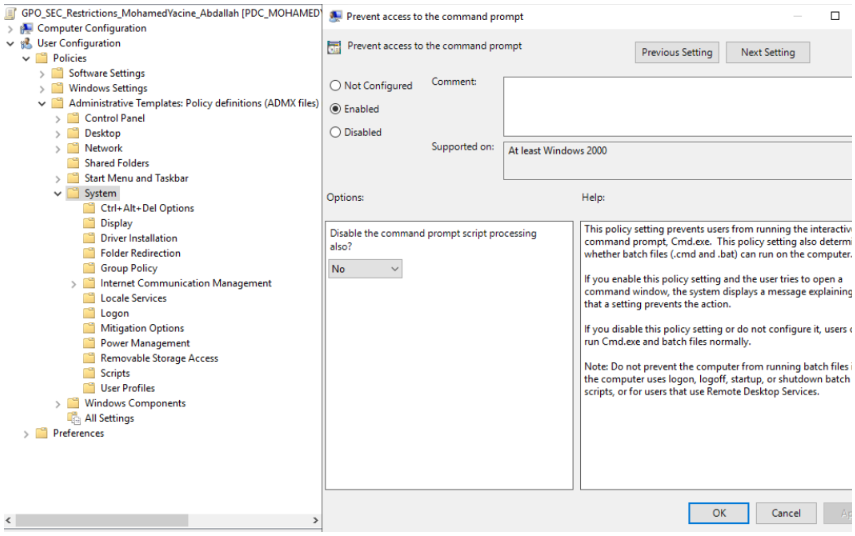


Figure 20: GPO configuration preventing access to the Command Prompt (cmd.exe)

### Disable Control Panel and Settings

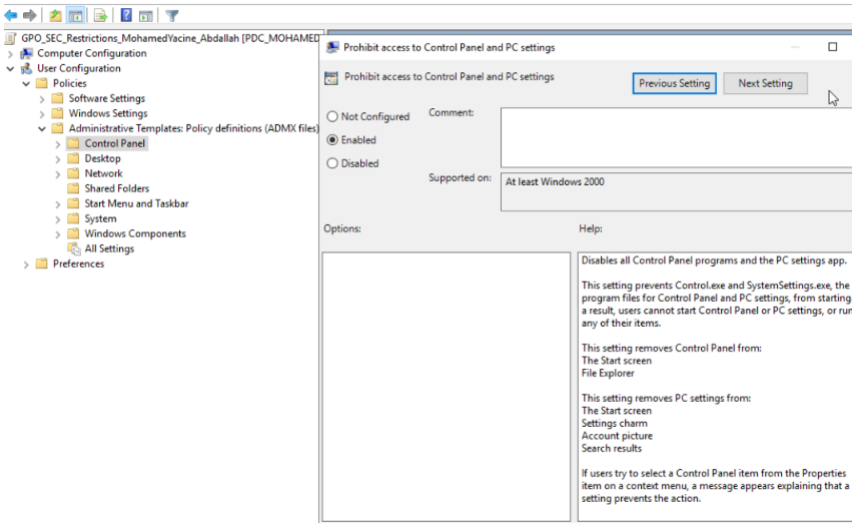


Figure 21: GPO disabling access to the Control Panel and PC Settings

### Disable Registry Editing Tools

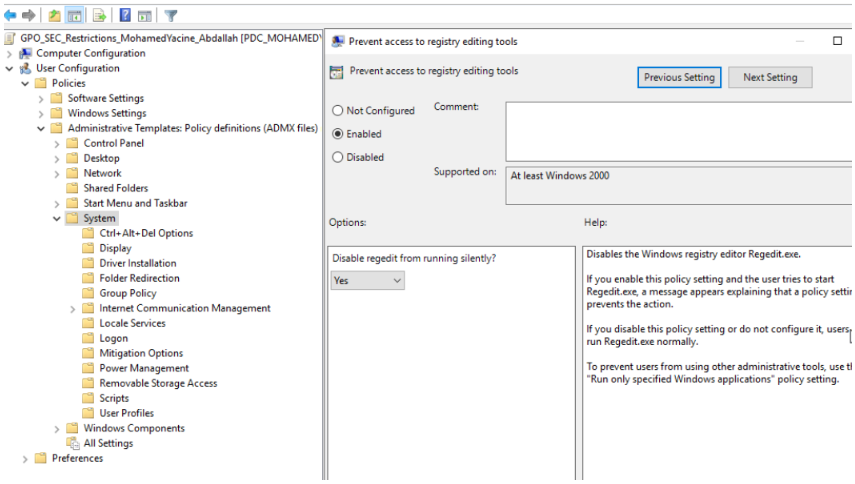


Figure 22: GPO preventing access to registry editing tools

### Disable PowerShell Execution

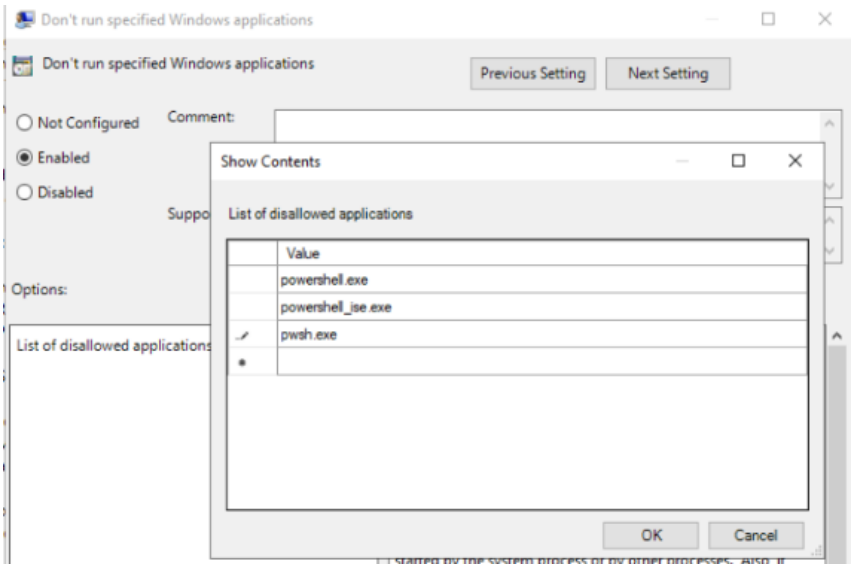


Figure 23: GPO blocking execution of PowerShell (powershell.exe)

## 4.2 b) GPOs Applied to `Administration`

Security hardening and auditing policies are applied to administrative users.

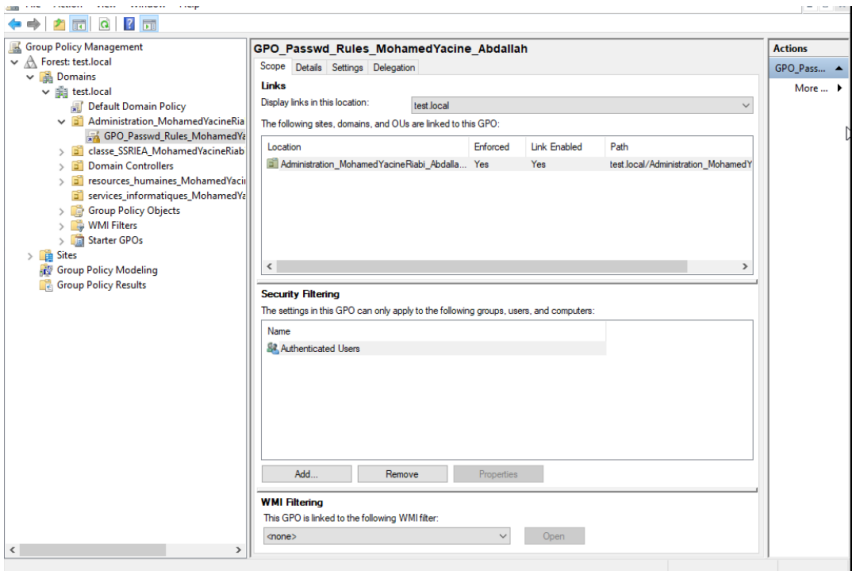


Figure 24: Group Policy Objects linked to the `Administration` Organizational Unit

### Password Policy Enforcement

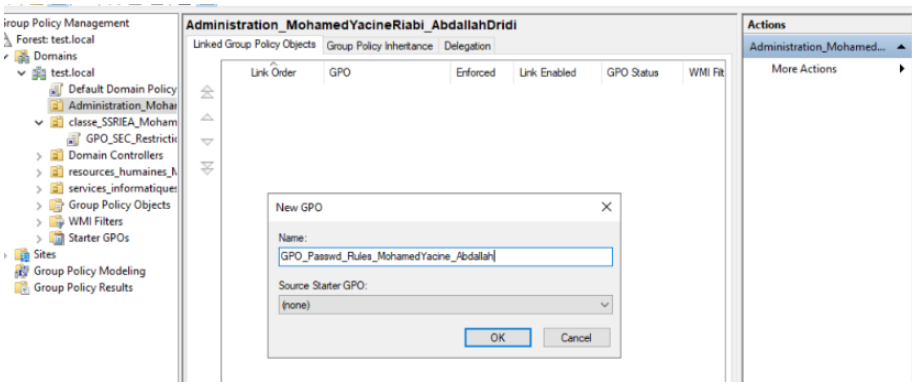


Figure 25: Creation of password policy GPO for administrative users

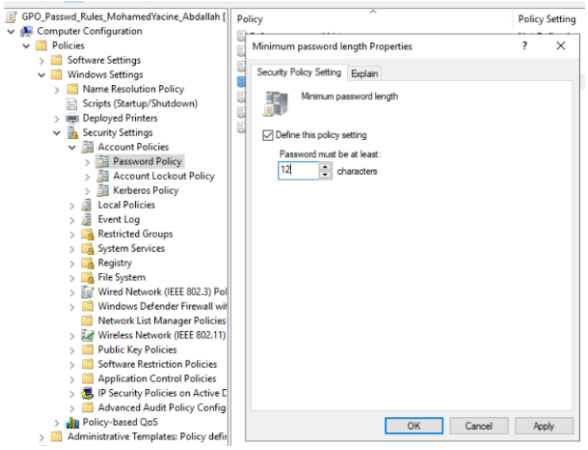


Figure 26: Minimum password length set to 12 characters

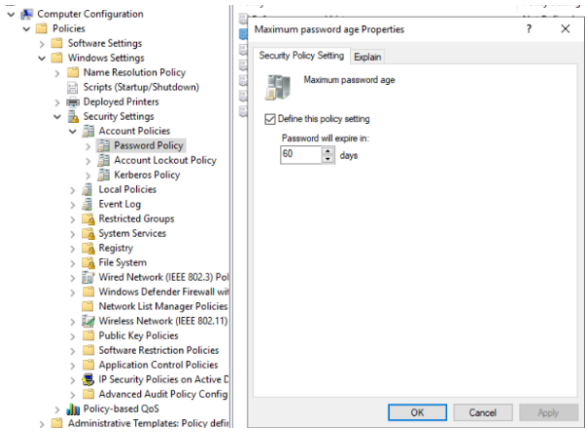


Figure 27: Maximum password age set to 60 days

### Screen Lock After Inactivity

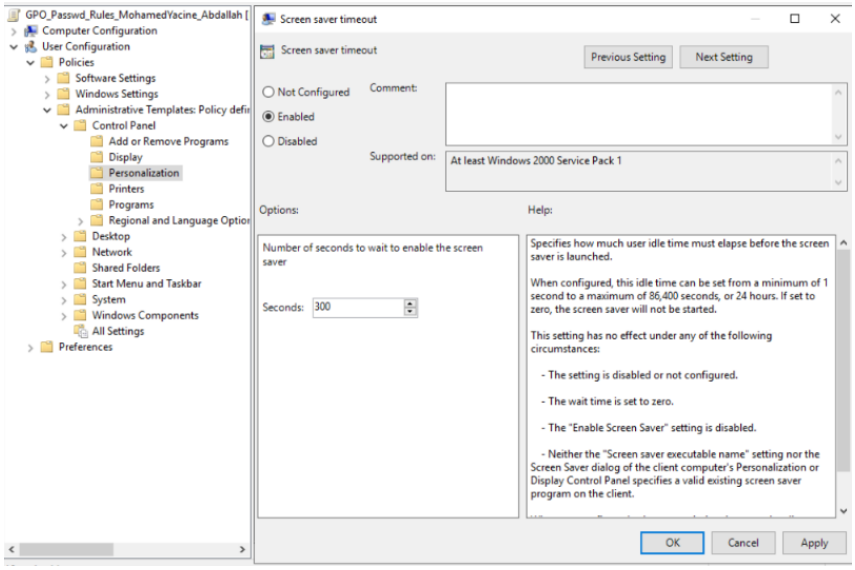


Figure 28: Screen saver enforced after 5 minutes of inactivity

### Disable Local Administrator Account

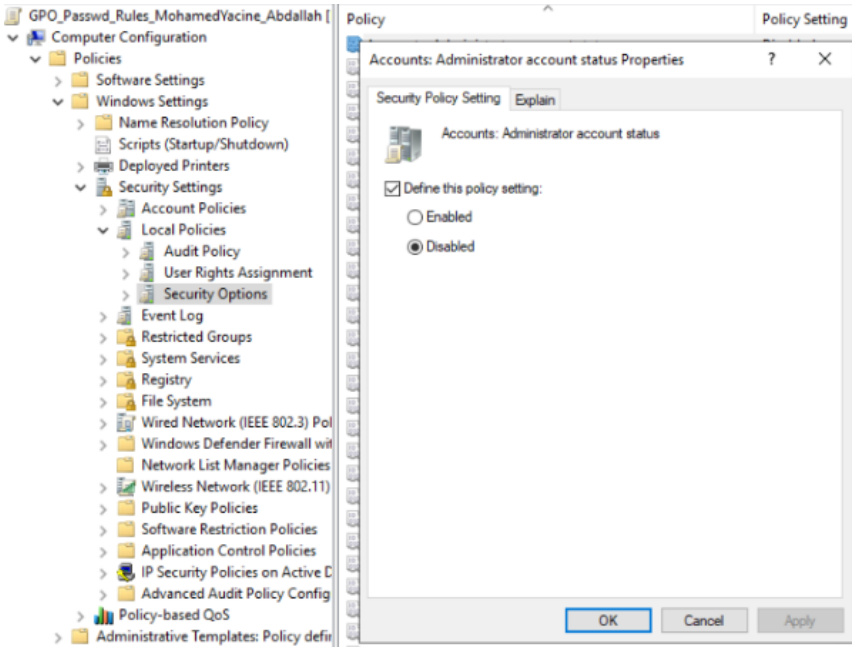


Figure 29: Local administrator account disabled via Group Policy

### Audit Policy Configuration

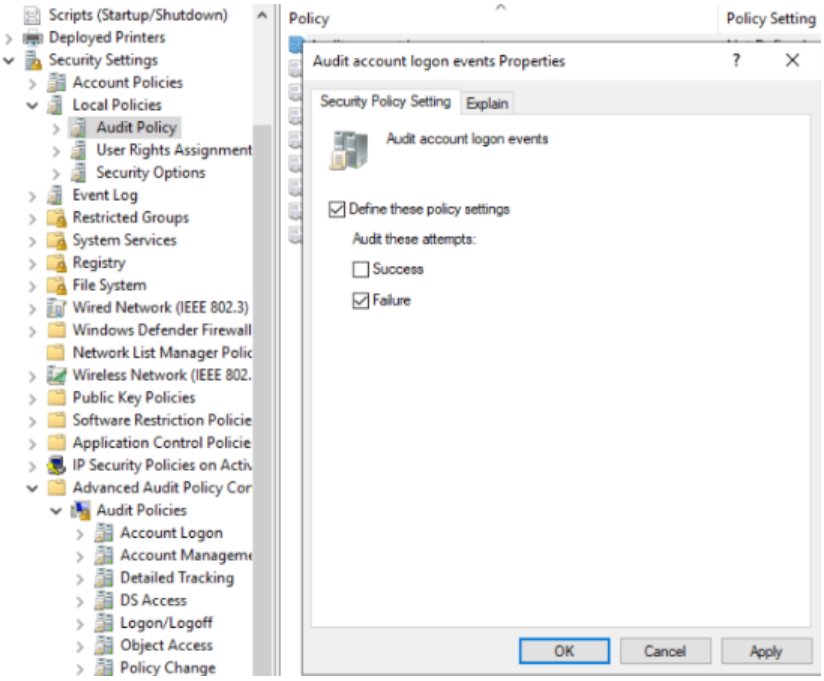


Figure 30: Audit policy enabled for account logon failures

| Policy | Policy Setting |
|---|---|
| Audit account logon events | Failure |
| Audit account management | Not Defined |
| Audit directory service access | Not Defined |
| Audit logon events | Success, Failure |
| Audit object access | Not Defined |
| Audit policy change | Success, Failure |
| Audit privilege use | Success, Failure |
| Audit process tracking | Not Defined |
| Audit system events | Success, Failure |

Figure 31: Configured audit policies for security monitoring

### 4.3 c) GPOs Applied to `ressources_humaines`

User interface and network configuration restrictions are applied to HR users.

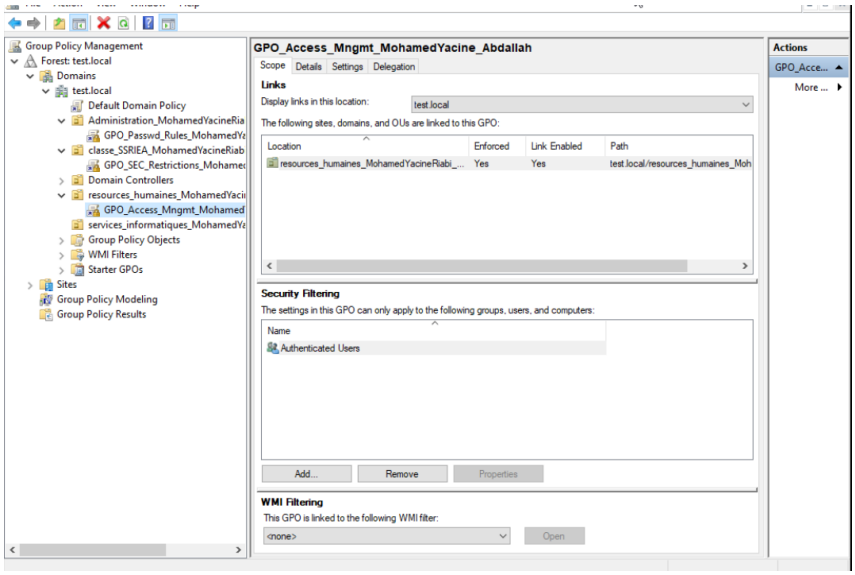


Figure 32: Group Policy Objects linked to the `ressources_humaines` Organizational Unit

### Restrict Network Connection Properties

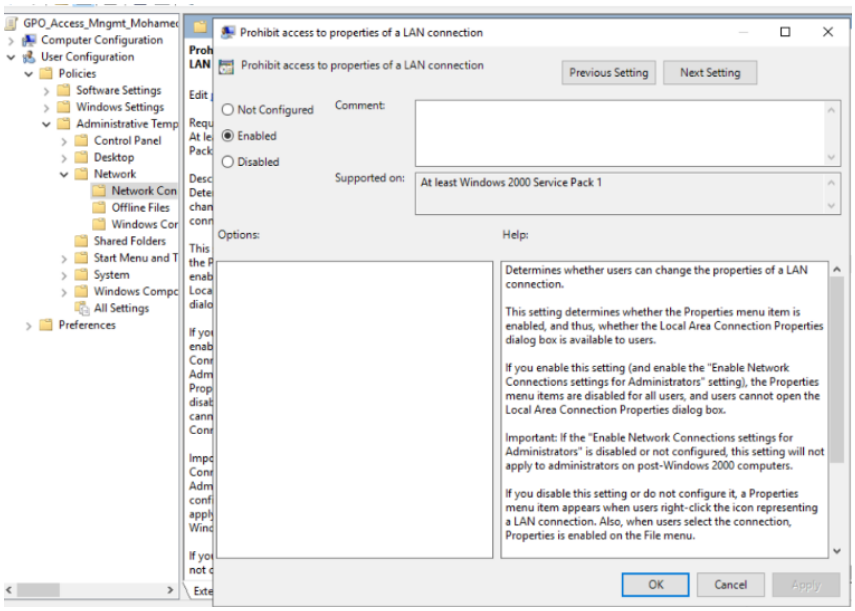


Figure 33: GPO preventing access to network connection properties

### Lock Taskbar

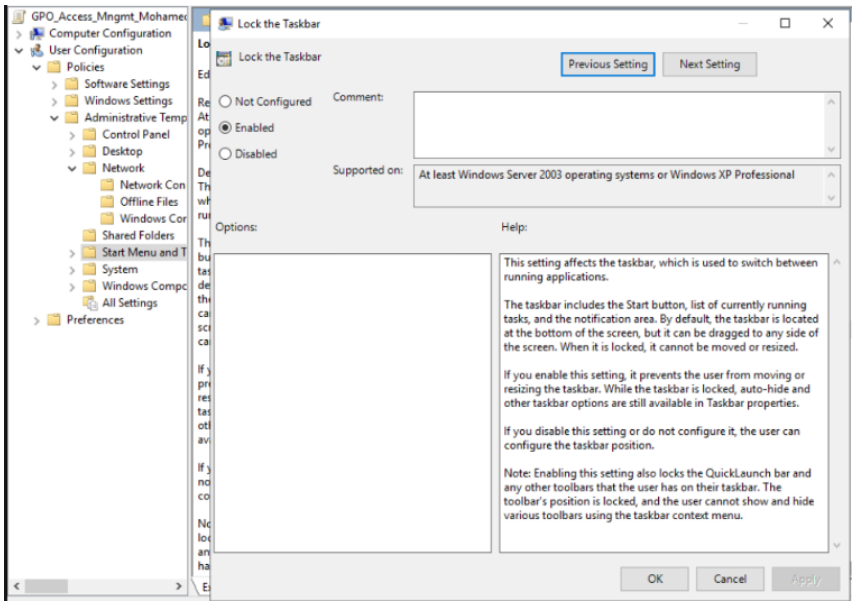


Figure 34: Taskbar locked using Group Policy

### Disable Power Options in Start Menu

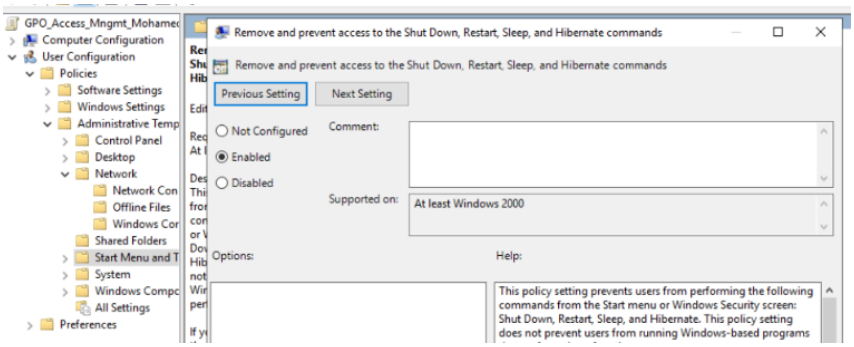


Figure 35: Shutdown, restart, and sleep options removed from Start menu

## 4.4 d) Group and Privilege Management in `services_informatiques`

Administrative privileges are centralized using a dedicated security group.

### Creation of IT Group

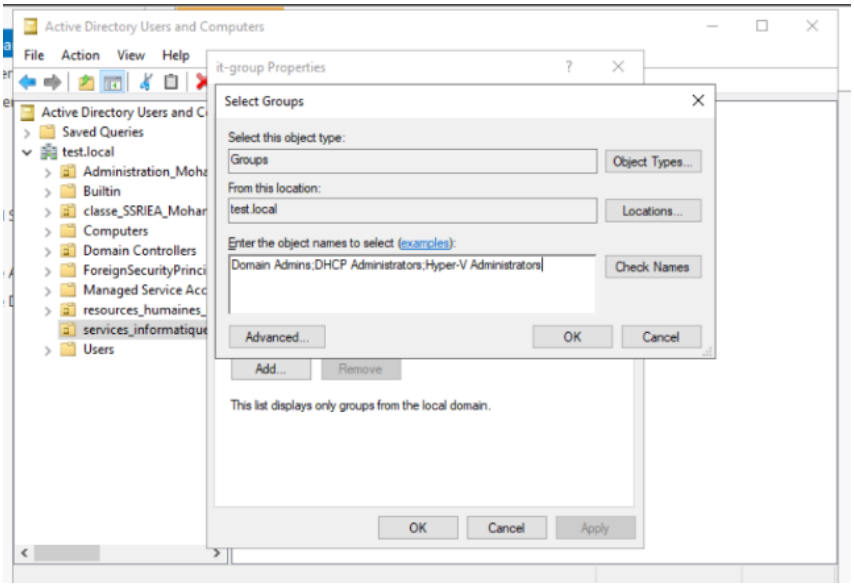


Figure 36: Creation of the `it-group` security group

**Assignment of Privileged Groups**

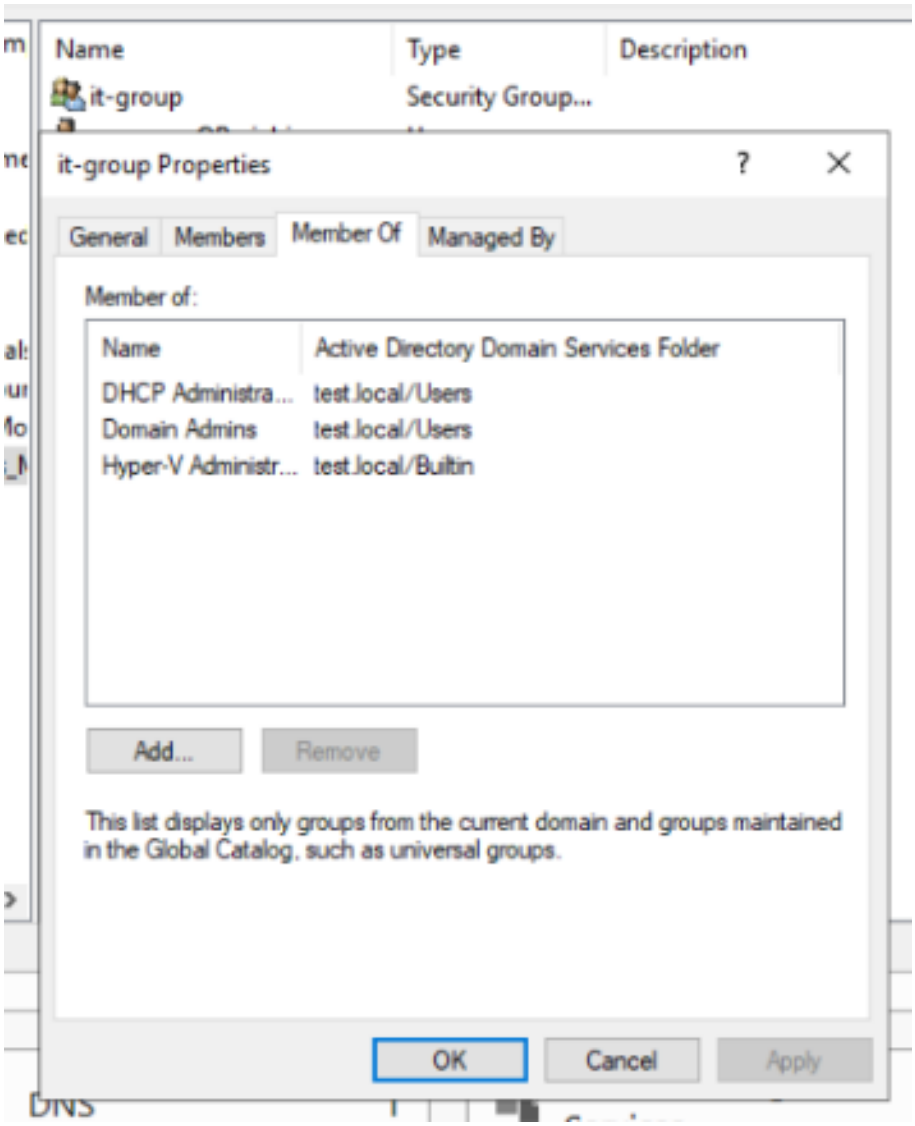


Figure 37: Privileged groups added as members of `it-group`

### User Membership Assignment

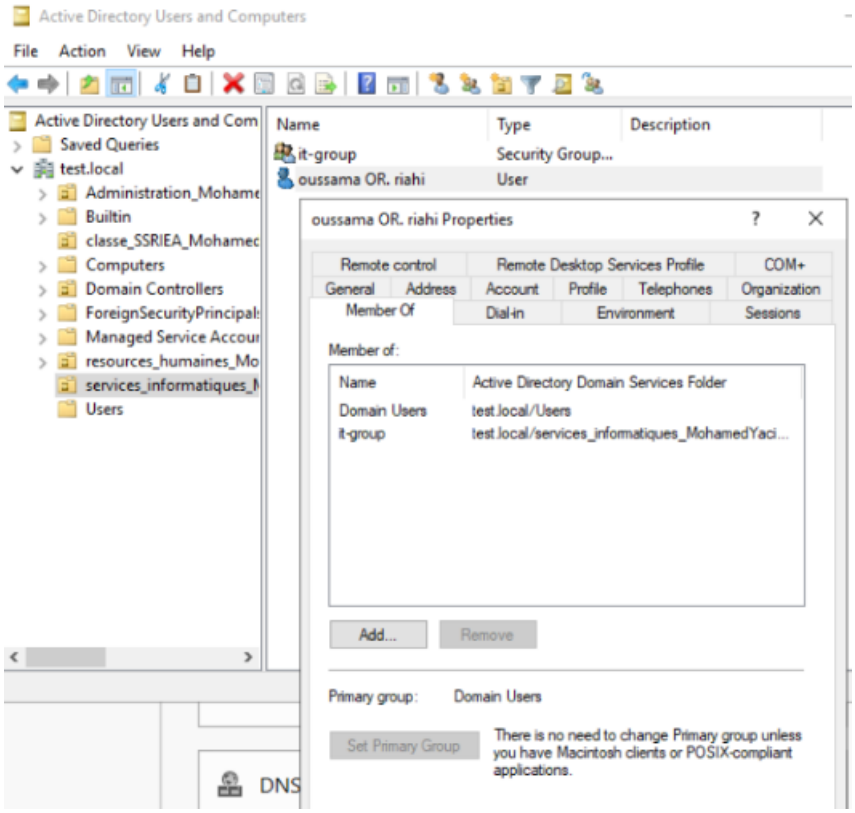


Figure 38: User `oussama riahi` added to the `it-group`

## 5 Exercise 4: DHCP Configuration

This exercise focuses on configuring the Dynamic Host Configuration Protocol (DHCP) service on Windows Server 2019 to automatically assign IPv4 network parameters to domain clients within the `test.local` infrastructure.

### 5.1 a) DHCP Role Installation and Scope Creation

The DHCP role is installed on the Windows Server. A new DHCP scope is created and named according to the required convention.

- Scope name: `dhcp_MohamedYacineRiabi_AbdallahDridi`

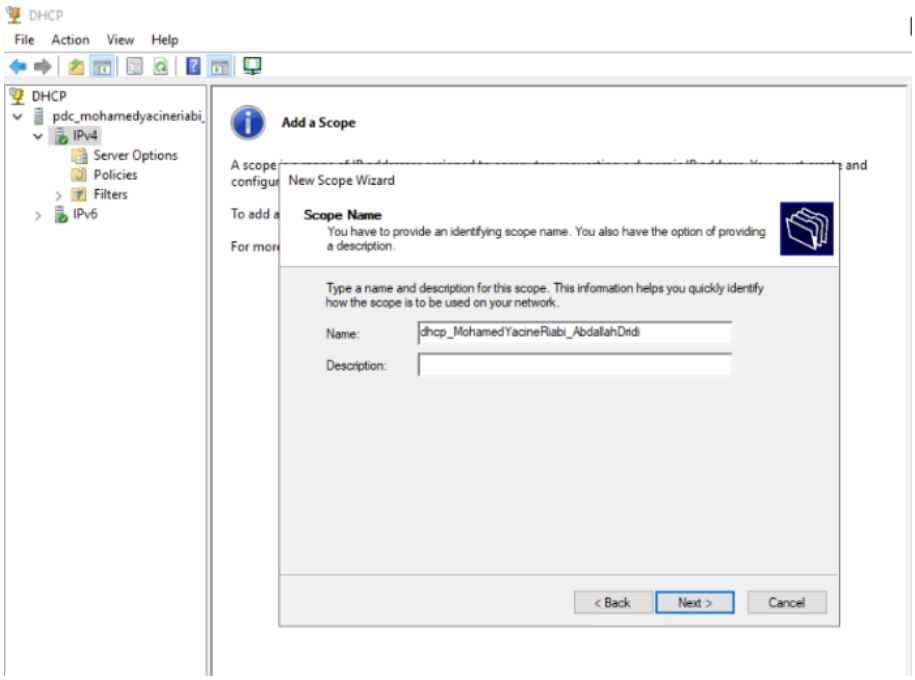


Figure 39: Creation of the DHCP scope on Windows Server

## 5.2 b) DHCP Management Console

The DHCP service is managed using the *DHCP Management Console*, accessible from the Server Manager tools.

## 5.3 c) IPv4 Address Range Definition

An IPv4 address range is defined to specify the pool of addresses that can be dynamically assigned to client machines.

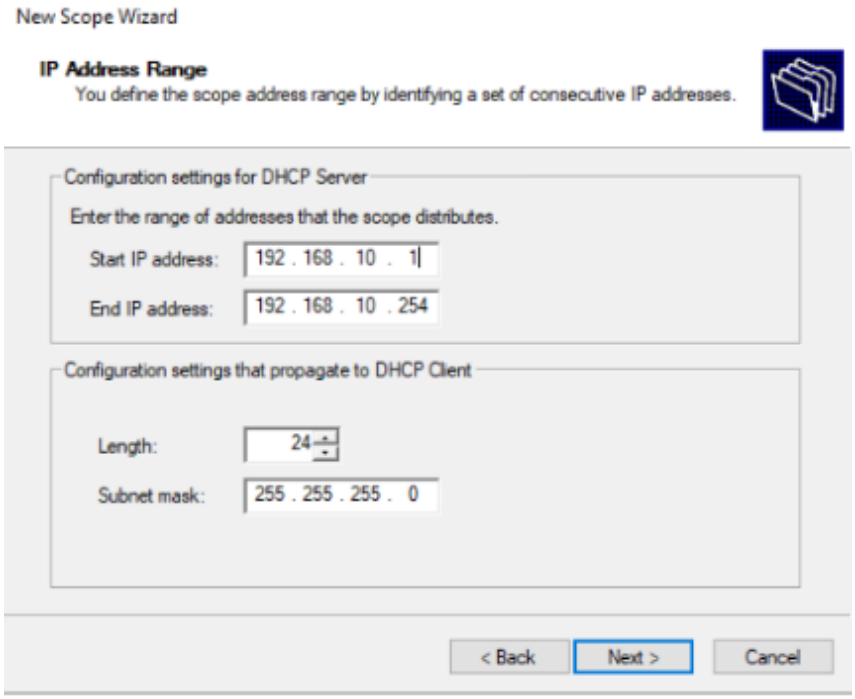


Figure 40: Definition of the IPv4 address range for the DHCP scope

## 5.4 d) Exclusion of IPv4 Addresses

Specific IPv4 addresses are excluded from the scope to prevent them from being assigned dynamically.

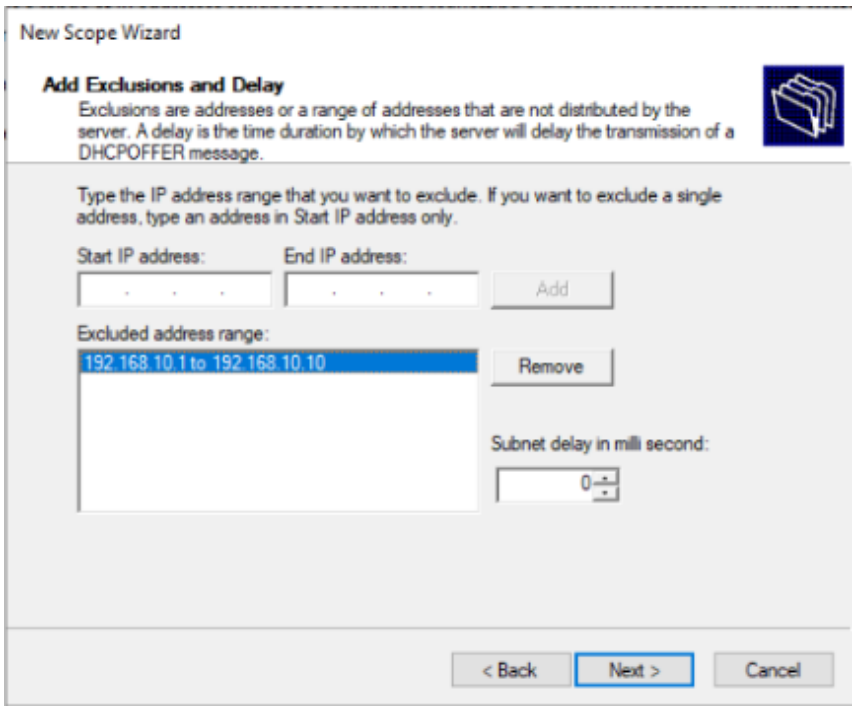


Figure 41: Excluded IPv4 address range within the DHCP scope

## 5.5 e) DHCP Lease Duration Configuration

The DHCP lease duration is configured to a fixed period of three (3) days.

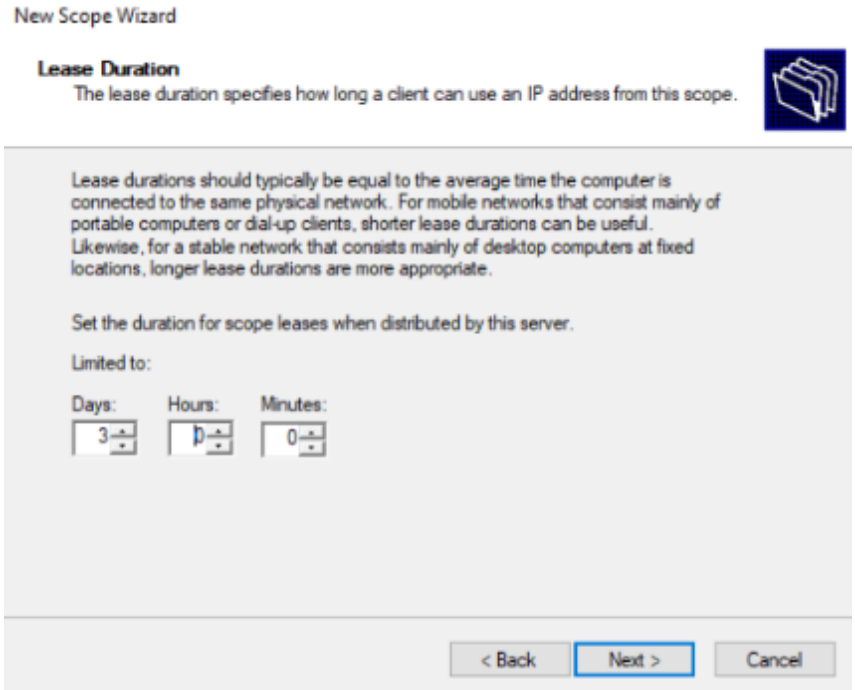


Figure 42: DHCP lease duration set to three days

### 5.6 f) Default Gateway Configuration

A default gateway (router) IPv4 address is defined and distributed automatically to DHCP clients.

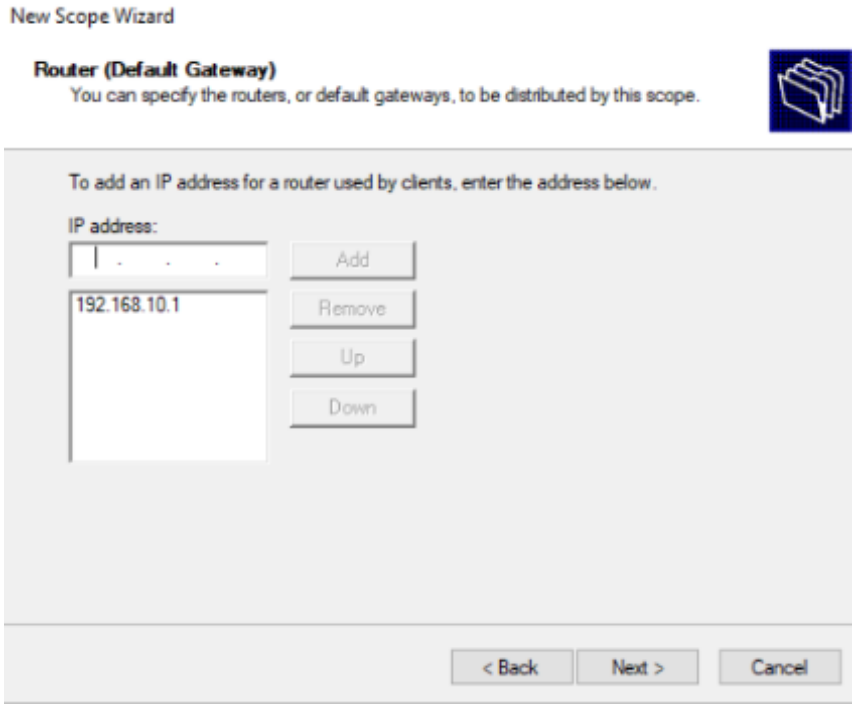


Figure 43: Default gateway configured for DHCP clients

### 5.7 g) Domain Name Distribution

The domain name `test.local` is configured as the default DNS domain distributed to DHCP clients.

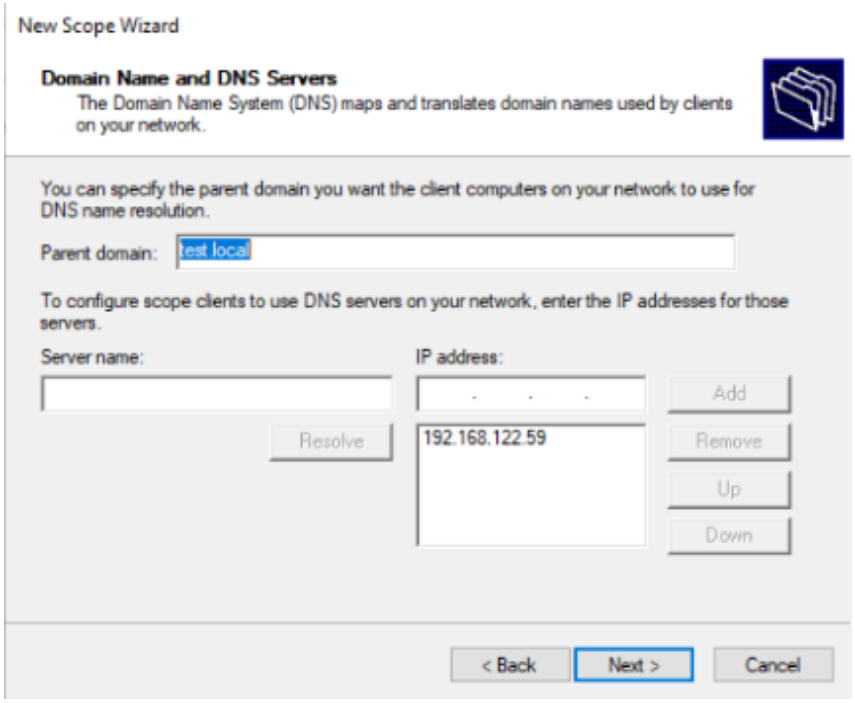


Figure 44: Distribution of the `test.local` domain name via DHCP

## 5.8 h) Client IPv4 Configuration Verification

On the Windows 10 client machine, network parameters are obtained automatically via DHCP. The assigned IPv4 configuration is verified using the `ipconfig /all` command.

```
C:\Users\PC1_Yacine_Abdallah>ipconfig /all

Configuration IP de Windows

   Nom de l'hôte . . . . . : PC1-MohamedYacineRiabi-AbdallahDridi
   Suffixe DNS principal . . . . . : test.local
   Type de noeud. . . . . : Hybride
   Routage IP activé . . . . . : Non
   Proxy WINS activé . . . . . : Non
   Liste de recherche du suffixe DNS.: test.local

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : test.local
   Description. . . . . : Intel(R) 82574L Gigabit Network Connection
   Adresse physique . . . . . : 52-54-00-3B-D0-E1
   DHCP activé. . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . .: fe80::b96c:38a6:3627:24e4%4(préféré)
   Adresse IPv4. . . . . .: 192.168.10.11(préféré)
   Masque de sous-réseau. . . . . : 255.255.255.0
   Bail obtenu. . . . . : mardi 30 décembre 2025 22:33:50
   Bail expirant. . . . . : vendredi 2 janvier 2026 22:33:50
   Passerelle par défaut. . . . . : 192.168.10.1
   Serveur DHCP . . . . . : 192.168.10.10
   IAID DHCPv6 . . . . . : 106058752
   DUID de client DHCPv6. . . . . : 00-01-00-01-30-E5-6A-CE-52-54-00-3B-D0-E1
   Serveurs DNS. . . . . : 192.168.122.59
   NetBIOS sur Tcpip. . . . . : Activé

C:\Users\PC1_Yacine_Abdallah>_
```

Figure 45: IPv4 configuration successfully assigned to the Windows 10 client

### 5.9 i) Verification of DHCP Client Leases

On the DHCP server, connected client machines are verified through the active lease list.

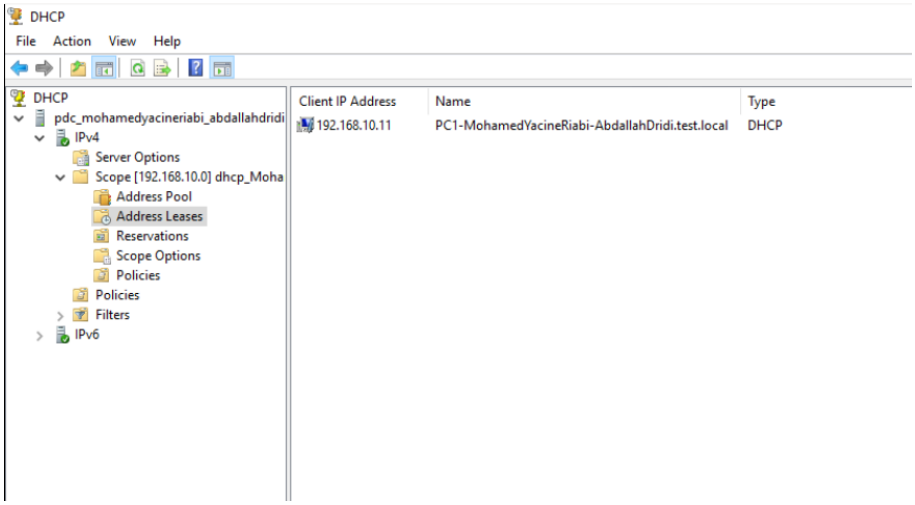


Figure 46: Active DHCP leases displayed on the server

### 5.10 j) DHCP Reservation Configuration

A DHCP reservation is created to assign a fixed IPv4 address to the Windows 10 client based on its MAC address.

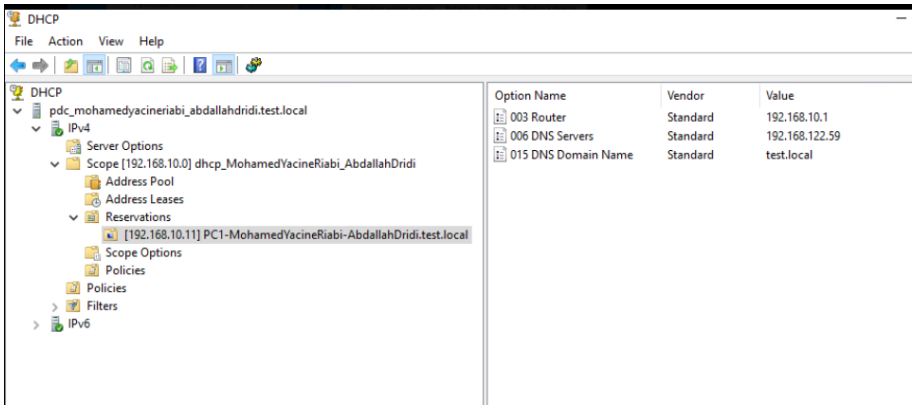


Figure 47: DHCP reservation created for the Windows 10 client

## 6 Exercise 5: Windows Server Security Mechanisms

### 6.1 5.1 Backup Configuration and Recovery

This part focuses on implementing backup and recovery mechanisms using the Windows Server Backup feature in order to ensure data availability and resilience.

### a) Installation of Windows Server Backup Feature

The *Windows Server Backup* feature is installed on the server to enable backup and recovery operations.

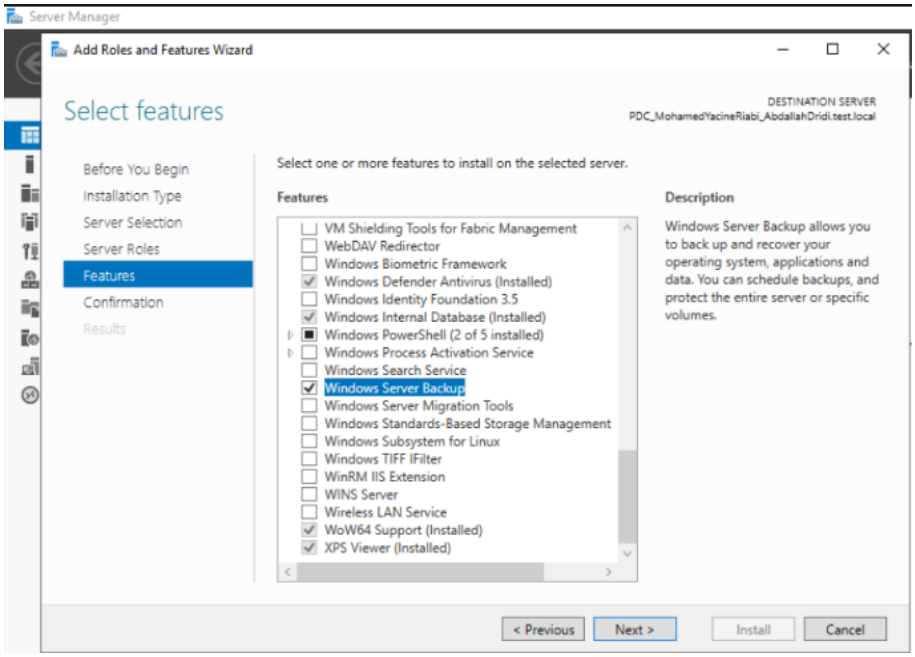


Figure 48: Installation of the Windows Server Backup feature

### b) Backup Options Overview

The Windows Server Backup tool provides several backup options, including full server backup, custom backup, and file or folder-level backup. For this exercise, a custom backup is selected.

### c) Creation of Data Directory

A directory named `data_MohamedYacineRiabi_AbdallahDridi` is created to store data that will be protected by the backup mechanism.

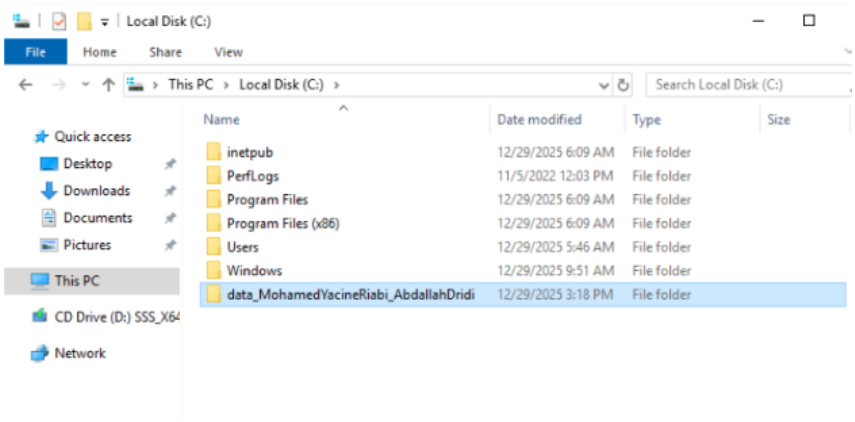


Figure 49: Creation of the data directory to be backed up

### d) File Creation Inside Data Directory

A text file is created inside the data directory to simulate user data.

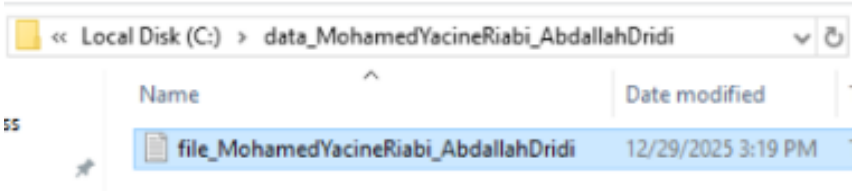


Figure 50: Text file created inside the data directory

### e) Backup Configuration

The backup is configured to include the `data` directory using the Windows Server Backup tool.

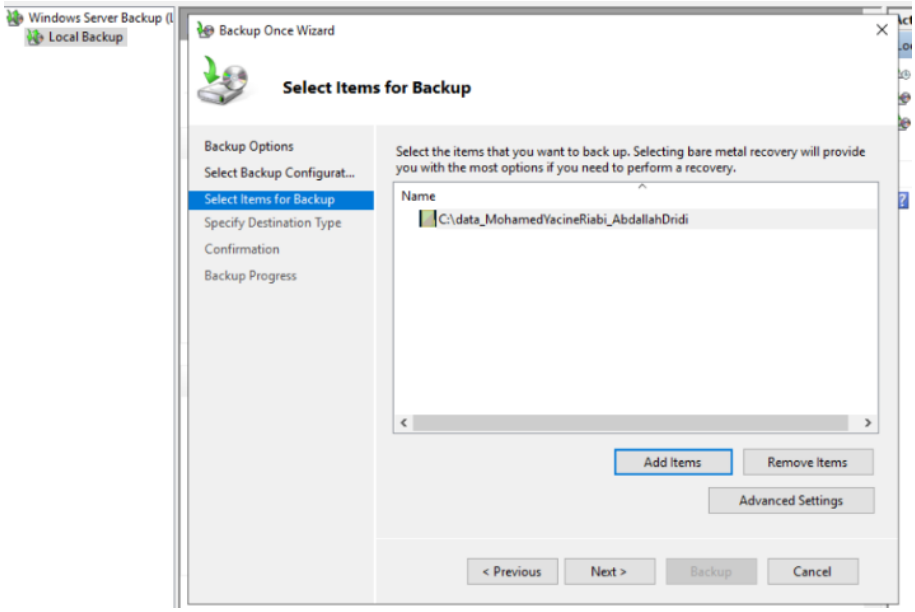


Figure 51: Configuration of the backup job including the data directory

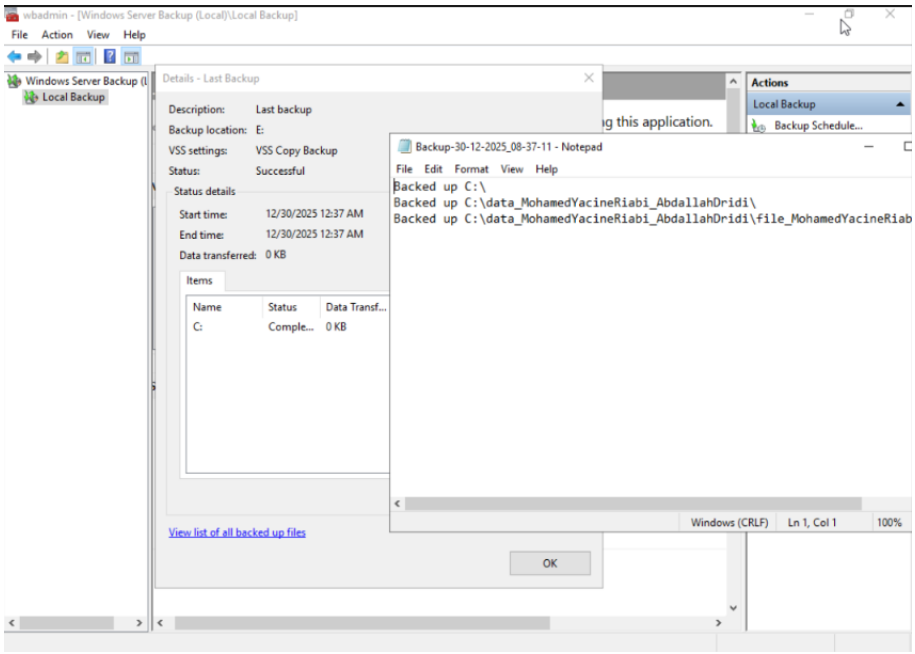


Figure 52: Backup job details and confirmation

### f) Deletion of the Data File

The previously created text file is deleted from the `data` directory to simulate data loss.

### g) Data Recovery Using Backup

The deleted file is restored using the Windows Server Backup recovery feature.

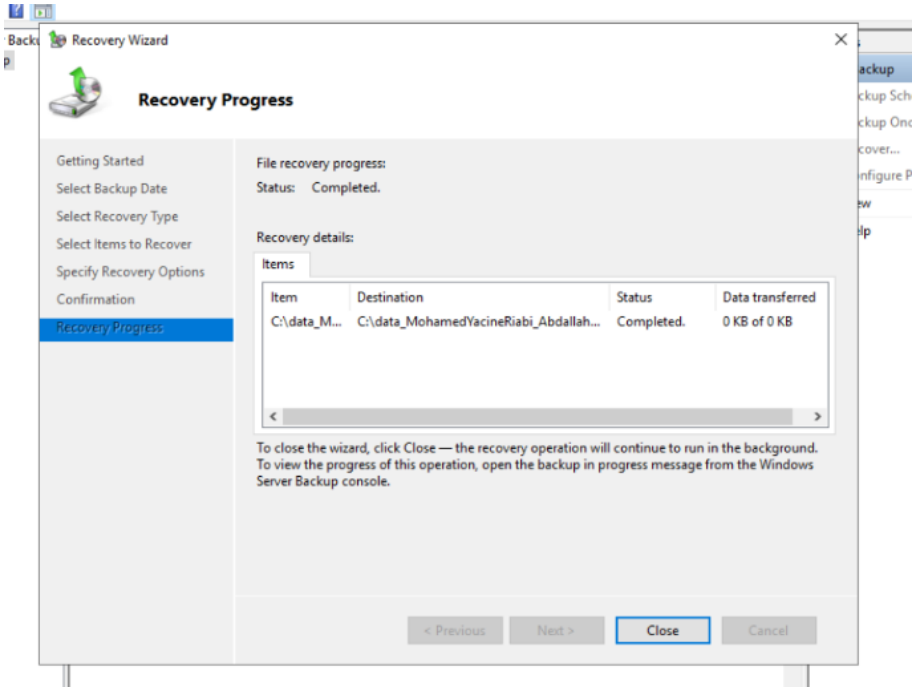


Figure 53: Progress of the data recovery process

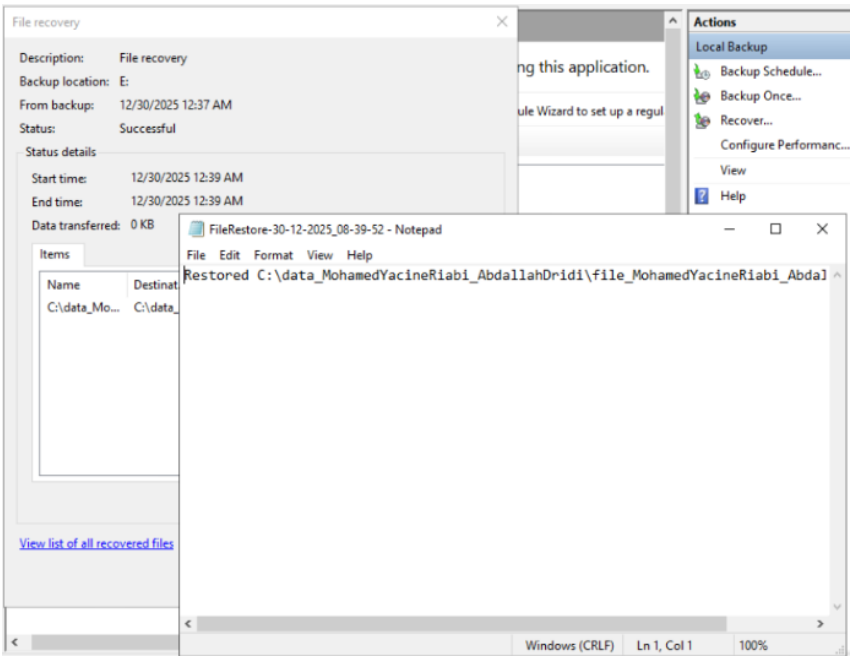


Figure 54: Successful recovery of the deleted file

## 6.2 5.2 Firewall Configuration

This subsection focuses on configuring and managing Windows Defender Firewall rules to control network traffic and enforce security policies. All firewall rules are named according to the following convention:

`<RULE_NAME>_MohamedYacineRiabi_AbdallahDridi`

### a) Firewall Status Verification

The status of Windows Defender Firewall is verified to ensure that the firewall is enabled and actively protecting the system.

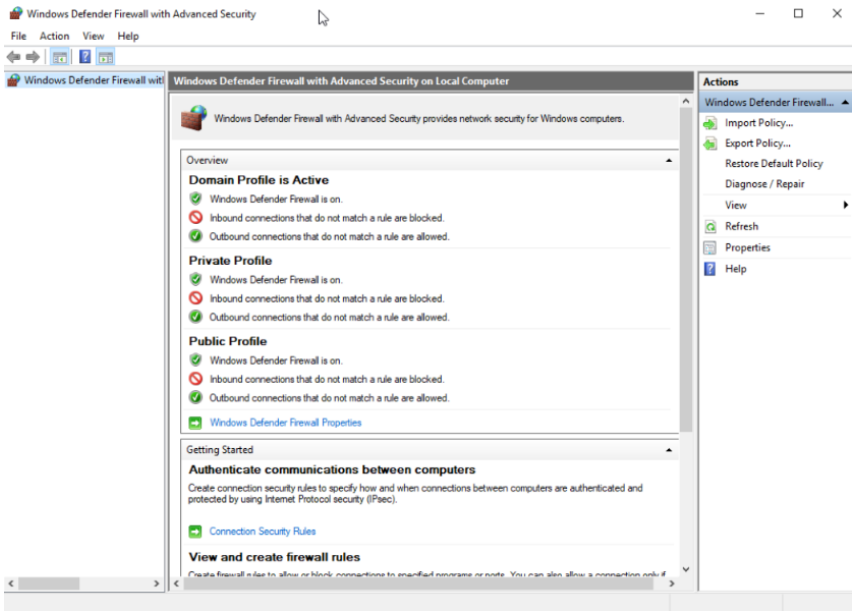


Figure 55: Verification of Windows Defender Firewall status

### b) ICMP Traffic Blocking

An inbound firewall rule is created to block ICMP traffic (ping requests), preventing network reachability checks.

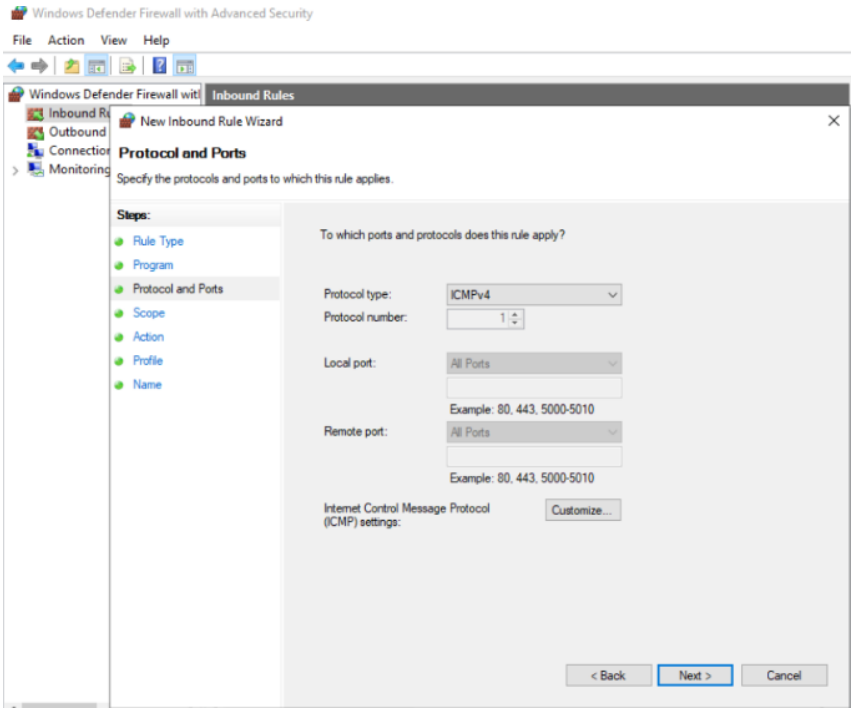


Figure 56: Creation of a new inbound firewall rule for ICMP traffic

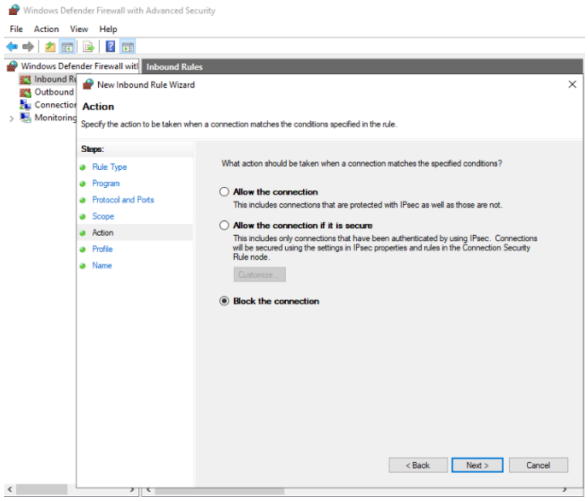


Figure 57: ICMP rule action set to block

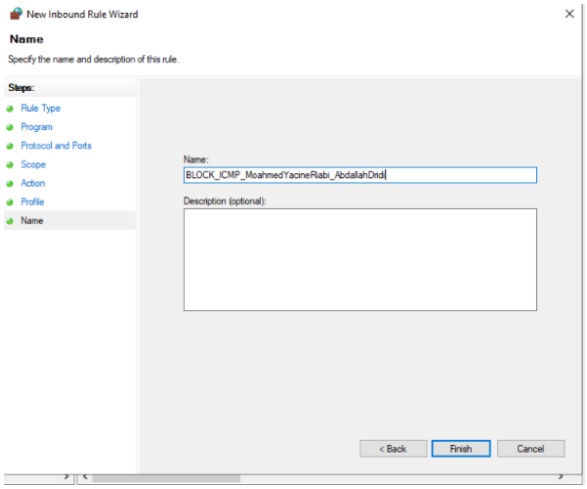


Figure 58: Naming of the ICMP blocking rule

### c) Blocking Web Browser Internet Access

An outbound firewall rule is created to block internet access for a web browser (Google Chrome / Internet Explorer).

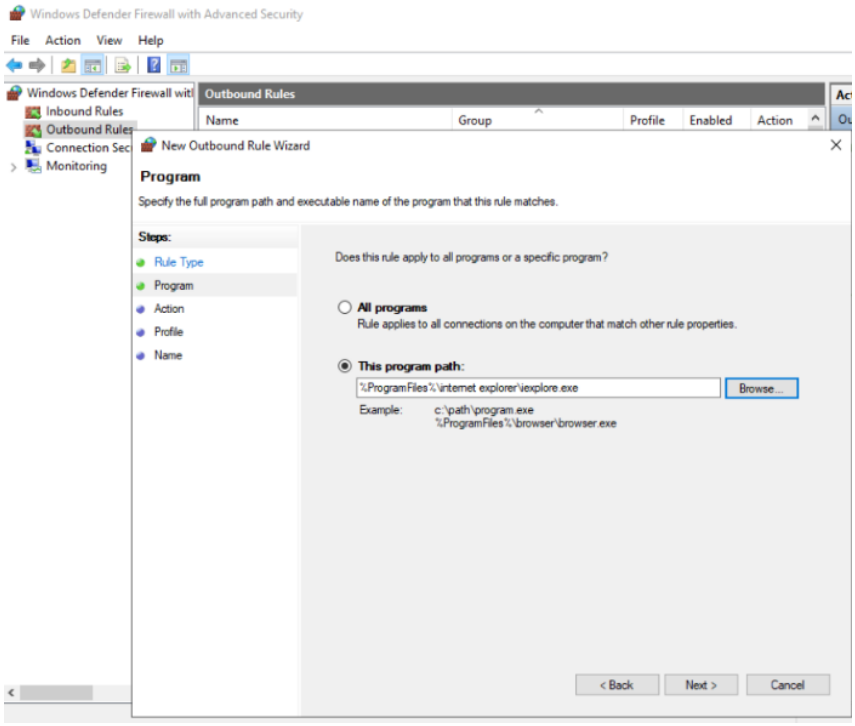


Figure 59: Creation of outbound firewall rule for browser traffic

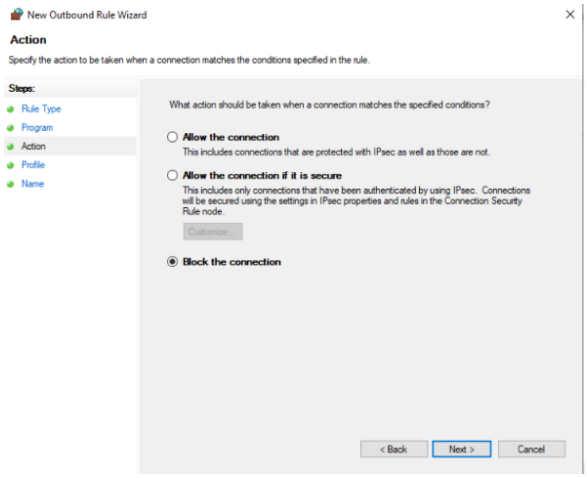


Figure 60: Outbound browser traffic blocked

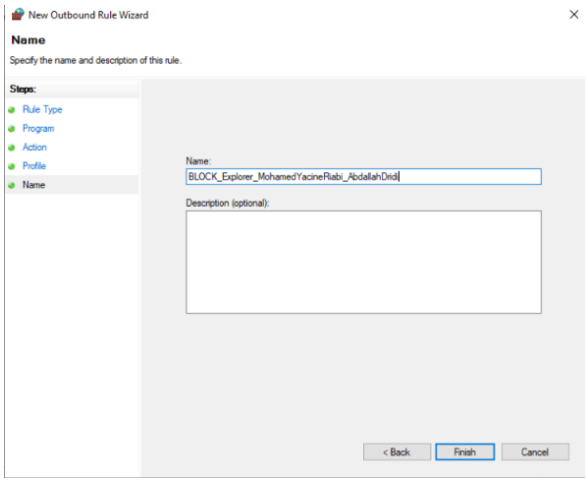


Figure 61: Naming of the browser blocking rule

### d) Blocking TELNET Traffic

An inbound firewall rule is created to block TELNET traffic on port 23.

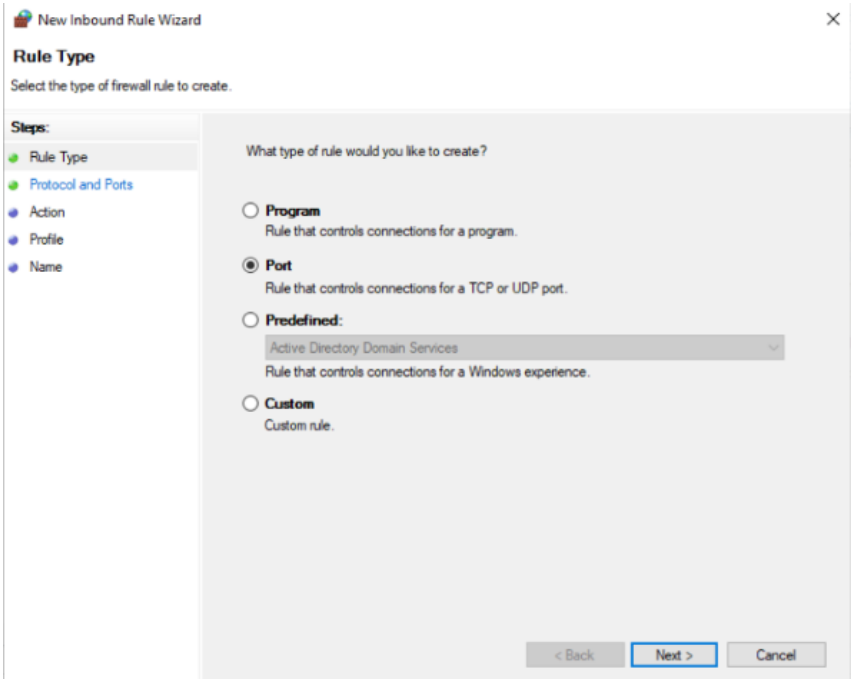


Figure 62: Creation of a new inbound firewall rule

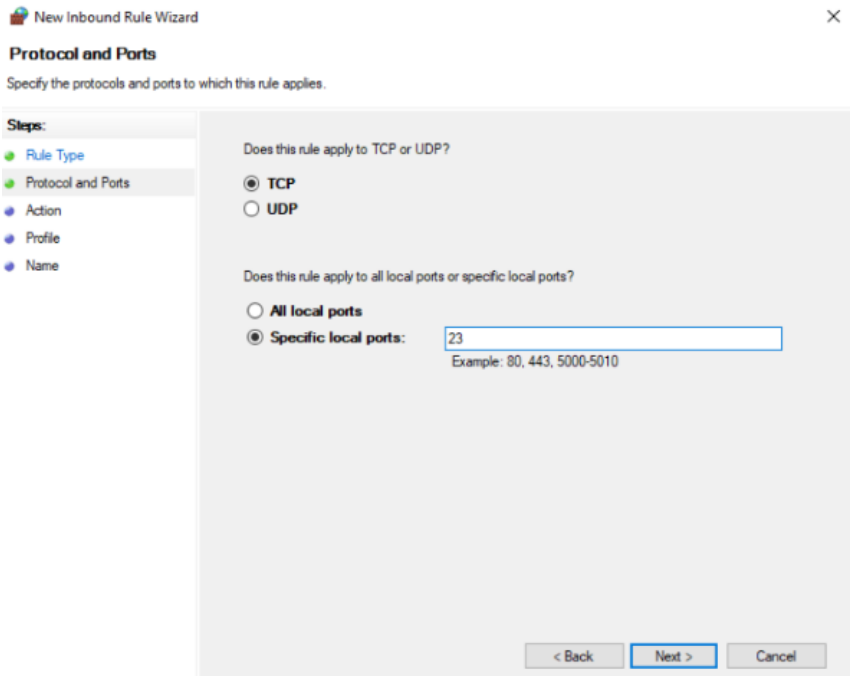


Figure 63: TELNET port (23) selected for blocking

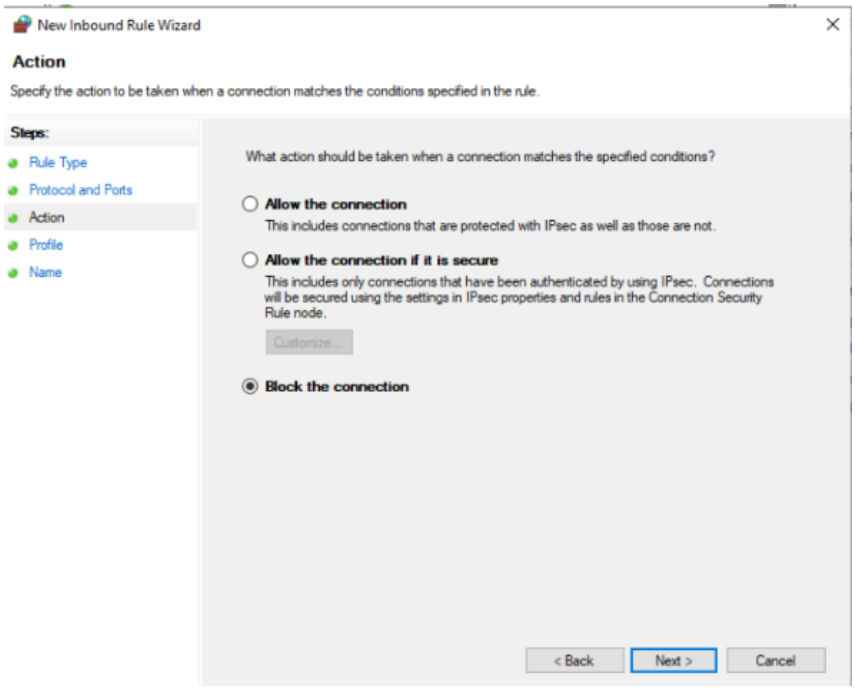


Figure 64: Inbound TELNET traffic blocked

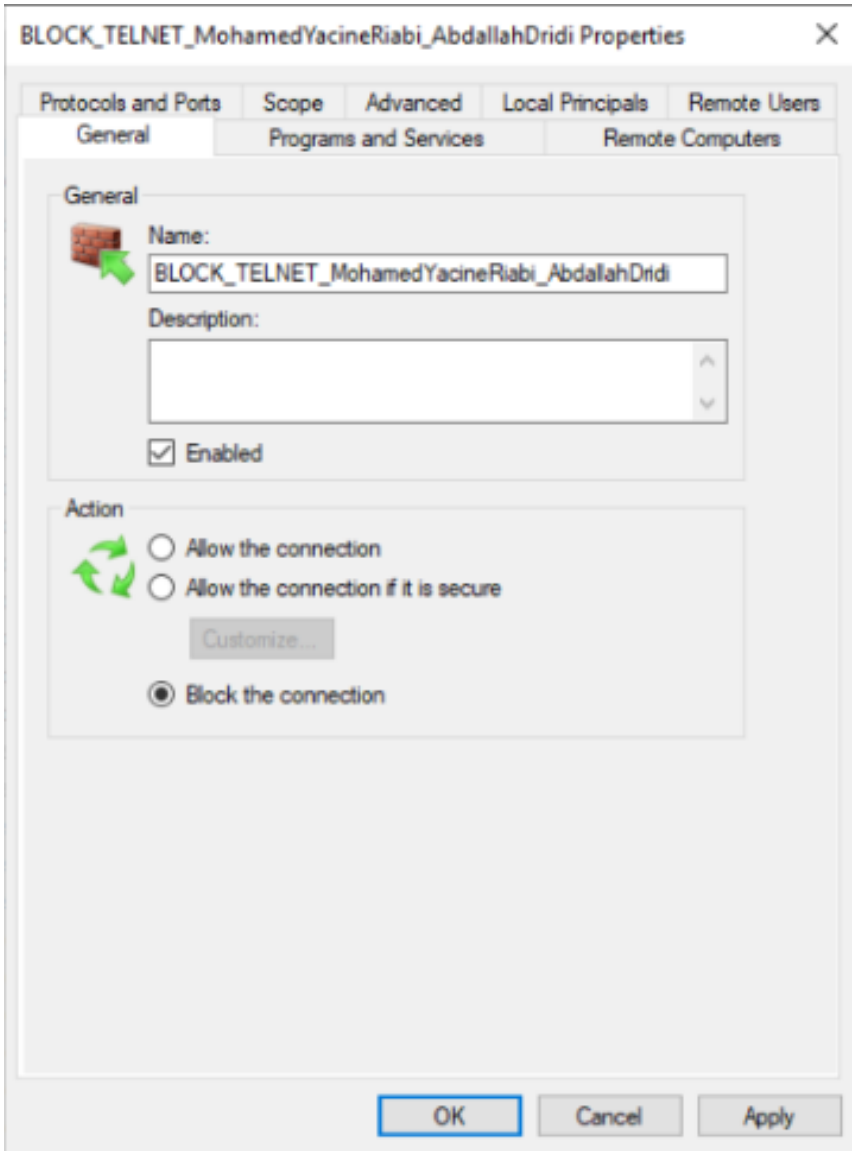


Figure 65: Firewall rule successfully blocking TELNET traffic

**e) Blocking FTP Traffic**

An inbound firewall rule is created to block FTP traffic on ports 20 and 21.

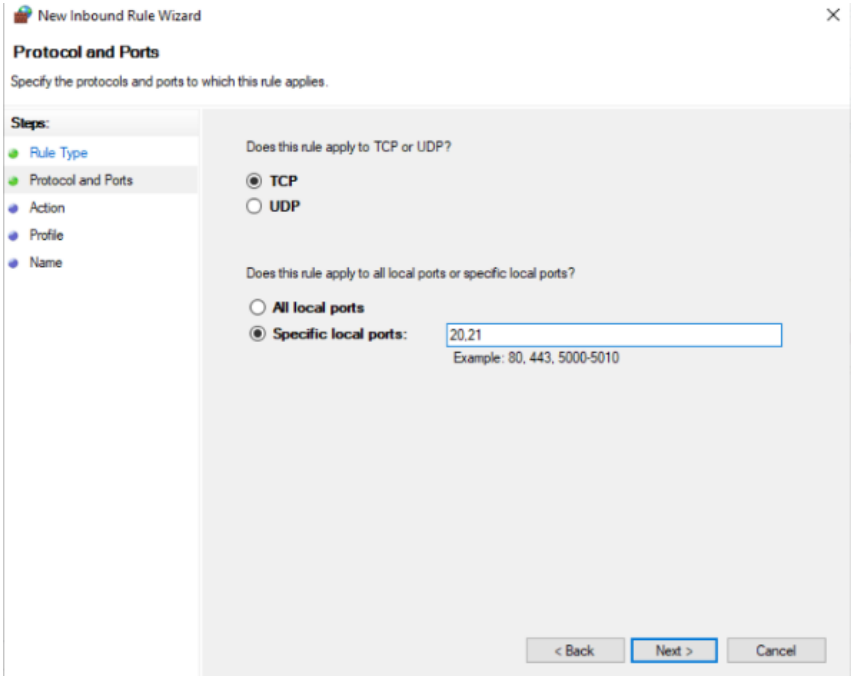


Figure 66: FTP ports (20 and 21) selected for blocking

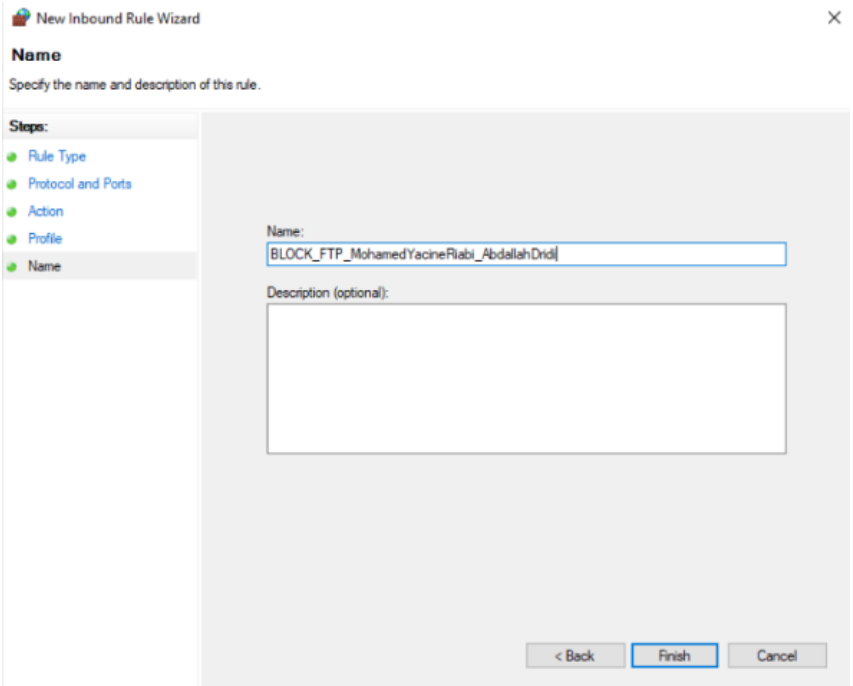


Figure 67: Firewall rule blocking FTP traffic

### f) Exporting Firewall Rules

The configured firewall rules are exported to a file to allow backup or transfer to another machine.

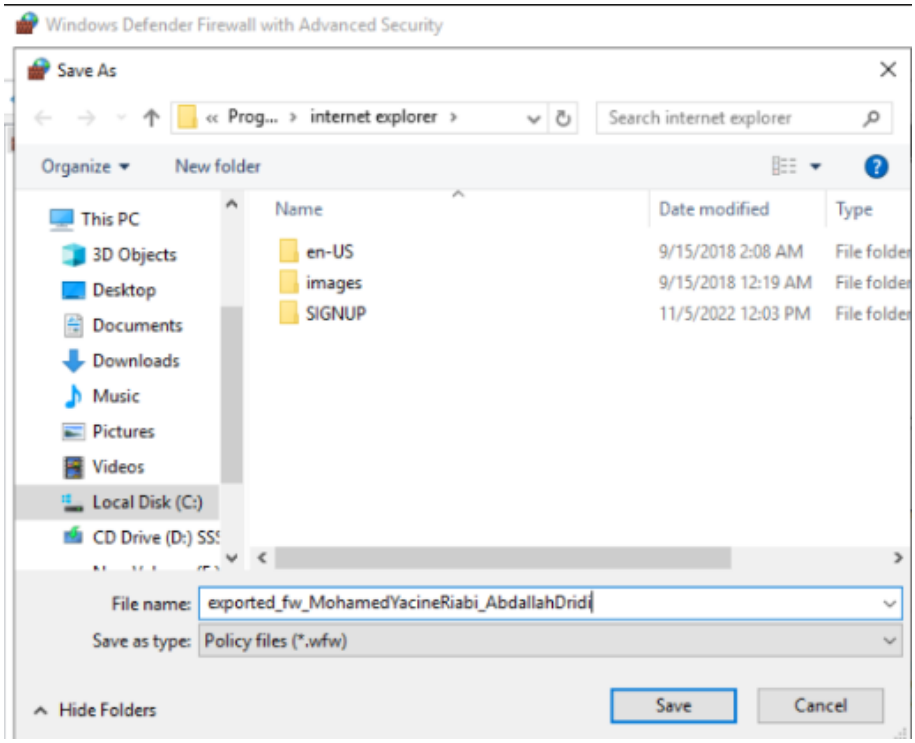


Figure 68: Export of Windows Defender Firewall rules

### g) Importing Firewall Rules

The exported firewall rules are imported into another machine, ensuring consistent security policy enforcement across systems.

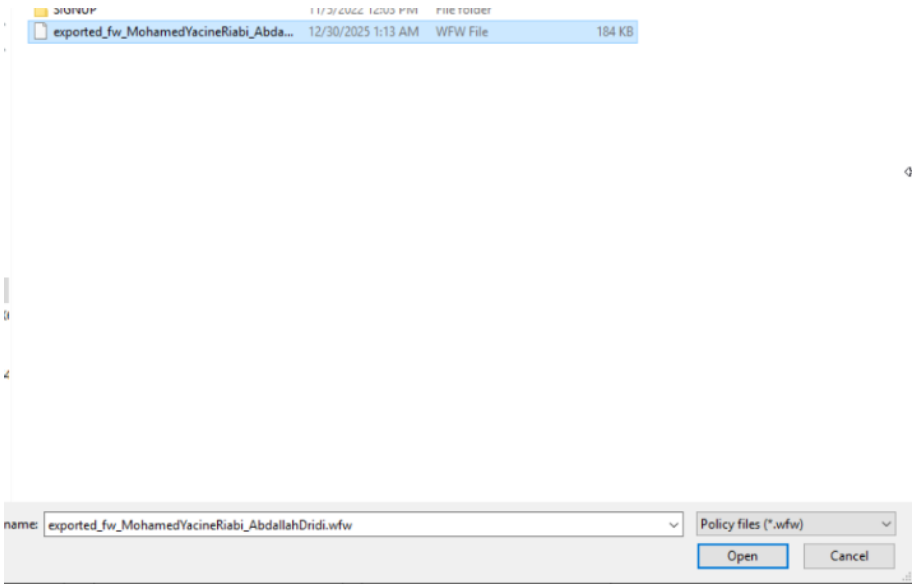


Figure 69: Importing Firewall Rules

## 7 Exercise 6: Active Directory Penetration Testing

This exercise presents a theoretical security assessment of the Active Directory environment through the study of two common and realistic attack techniques: **Kerberoasting** and **Password Spraying**. These attacks were selected because they target different but complementary aspects of Active Directory security. Kerberoasting focuses on weaknesses in service account credential management within the Kerberos authentication protocol, while password spraying exploits weak password hygiene and insufficient authentication monitoring across domain user accounts.

- Kerberoasting and Password Spraying presentation

Both attack techniques are covered within the same presentation and were submitted via email as part of the project deliverables.

## 8 Conclusion

Through this project, we implemented and secured a complete Windows Server 2019 infrastructure based on Active Directory. The environment covered core administration tasks including domain deployment, user and group management, Group Policy enforcement, DHCP configuration, backup and recovery mechanisms, and firewall hardening.

In addition, a controlled penetration testing exercise was conducted to demonstrate real-world Active Directory attack scenarios and highlight common misconfigurations. This allowed us to better understand both the offensive and defensive aspects of Windows Server security.

Overall, this project strengthened our practical skills in system administration and cybersecurity, while emphasizing the importance of proper configuration, monitoring, and hardening of enterprise Windows environments.