Technical Project:

Windows Corporate Infrastructure

Summary

This project documents the implementation and operation of a minimal corporate Windows environment based on Active Directory, deployed under the *lab.unai* domain. The approach is practical and operational: it details what was done, why it was done, and how it was validated, reproducing real sysadmin workflows typical of enterprise environments.

The lab consists of a Domain Controller (DC1) and a Windows client (HOST1), integrating core services expected in a Windows domain: AD DS, DNS, DHCP, Group Policy, and File Services. The goal is not to cover every possible scenario, but to correctly implement the essential pillars required in small-to-medium corporate environments, providing clear evidence of functionality, coherent technical decisions, and solid validation criteria.

The documentation prioritizes clarity, traceability, and reproducibility, showing not only the final configuration but also validation steps from the client and the resolution of common issues. The result is a project aligned with real operational practice, reflecting workflows expected from system, platform, or advanced support roles.

1. Technical Objectives and Scope

1.1 General Objective

Build and operate a Windows environment based on Active Directory that enables controlled reproduction of core system administration tasks within a corporate domain.
The environment must allow:

- Identity management through users, groups, and Organizational Units (OUs)
- Centralized configuration and restrictions through Group Policy
- Access control to shared resources using NTFS permissions and security groups
- Client-side validation of connectivity, name resolution, and policy application
- Resolution of basic issues using standard operating system tools

The approach is practical and operational, aligned with real sysadmin workflows, avoiding artificial or purely demonstrative configurations.

1.2 Specific Objectives (executed blocks)

Block 1 – Active Directory Administration

- Design and creation of the Organizational Unit structure:
    - 00-Admins
    - 10-Users
    - 20-Computers
    - 30-Groups
    - 40-Servers
    - 90-Disabled
- Creation and management of domain users
- Creation of security groups and membership assignments
- Application of least privilege through group-based permissions
- Moving users between OUs and managing account states (enabled / disabled)

Block 2 – Group Policy Management

- Creation and linking of GPOs to specific OUs
- Configuration of functional policies (user restrictions, passwords, USB)
- Password policy applied in the Default Domain Policy and validated from the client
- Verification of GPO application via *gpupdate* and *gpresult*
- Network drive mapping using Group Policy Preferences (Drive Maps) scoped by group
- Intentional GPO troubleshooting (incorrect OU, security filtering)

Block 3 – File Services & Permissions

- Creation of the shared resource *FIN* on DC1
- Configuration of share and NTFS permissions
- Exclusive access control via groups:
    - GRP-Share-ReadOnly
    - GRP-Share-ReadWrite
- Practical validation of access, writing, and denial using different users
- Use of **Effective Access** analysis when required

Block 4 – Client Management & Troubleshooting

- Resolution of client issues related to DNS, networking, and policies
- Use of diagnostic tools:
    - *ipconfig /all*
    - *nslookup*
    - *gpresult*
- Validation of correct final state after applying fixes

Block 5 – Operational Scenarios

- Simulation of user onboarding, offboarding, and role changes
- Controlled removal of access through groups and account disabling
- Use of the *90-Disabled* OU for offboarding management
- Validation of real impact on access to resources after each operation

1.3 Project Scope

Included

- Active Directory Domain Services in a single domain
- Internal DNS integrated with AD
- DHCP for dynamic address assignment
- Group Policy and Group Policy Preferences
- SMB File Services with NTFS permissions controlled by groups
- Client-side validation and basic troubleshooting

Excluded

- Hybrid environments (Azure / Entra ID / Intune)
- High availability, multiple Domain Controllers, or advanced role segmentation

Design Criteria

- Minimal, clear, and reproducible topology
- Technically justified decisions aligned with real environments
- Documentation focused on operation rather than artificial volume or complexity
- Consistent naming and structure across the environment:
    - Servers: *DC1, HOST1*
    - Groups: *GRP-**
    - OUs: numbered and ordered

2. Environment Design and Architecture

2.1 General Environment Structure

The lab was designed with a minimal yet fully operational topology, sufficient to reproduce real Windows administration workflows without introducing unnecessary complexity or artificial scenarios.
The goal was not to simulate a large-scale infrastructure, but to correctly understand and operate the essential components of a corporate domain and their interactions.

Main components

DC1

- Operating System: Windows Server Standard (Desktop Experience)
- Installed roles:
    - Active Directory Domain Services (AD DS)
    - DNS Server
    - DHCP Server
    - File Services

Function:

- Central authentication point for the domain
- Group Policy application
- Internal name resolution
- Access control to shared resources

HOST1

- Operating System: Windows 10 Enterprise
- Joined to the domain: lab.unai

Function:

- Operational validation machine

- Domain user login
- GPO application and verification
- Access to shared resources

The design criterion was to centralize services on a single Domain Controller, prioritizing operational clarity, traceability, and ease of troubleshooting.
Scenarios such as multiple DCs or high availability are intentionally out of scope for this project.

2.2 Lab Topology

The lab topology is logical, simple, and fully controlled, based on an internal isolated network managed by the hypervisor.

Topology characteristics

- Private NAT network managed by VMware Workstation (VMnet8)
- Common IP segment for all lab machines
- Direct communication DC1 ↔ HOST1
- Domain operation independent of external connectivity

Key component relationships

- HOST1 uses DC1 exclusively as its DNS server
- Authentication, name resolution, and policy application rely on the Domain Controller
- All access to shared resources is handled through DC1

This design enables:

- Rapid isolation of issues
- Clear identification of DNS, GPO, or permission problems
- Reduced variables during troubleshooting

The topology is meant to make causes and effects visible, not to hide them behind layers of complexity.

2.3 Network and Connectivity

The network configuration follows a fundamental principle in Windows/Active Directory environments:
the domain should rely exclusively on its own DNS.

Applied configuration

Virtual network

- Type: NAT (VMnet8 – VMware Workstation)
- Gateway: 192.168.119.2
- Segment: 192.168.119.0/24

DC1

- IP address: 192.168.119.50/24 (static)
- Primary DNS: 192.168.119.50 (self)
- Gateway: 192.168.119.2
- DNS forwarders configured:
    - 8.8.8.8
    - 1.1.1.1

HOST1

- IP address: assigned via DHCP
- Received IP: 192.168.119.147
- DNS received via DHCP: 192.168.119.50 (DC1)
- Gateway: 192.168.119.2

Validations performed

- Full verification using ipconfig /all
- Correct resolution of dc1.lab.unai from the client

- Successful domain user authentication
- Correct application of Group Policies

Key design decision
The client does not use external DNS servers.
Any deviation from this model leads to:

- Authentication failures
- GPOs not applying
- Inconsistent service resolution within the domain

2.4 Environment Resources

Resource assignment was kept aligned with real lab usage, avoiding both under-allocation and artificial over-provisioning.

Physical host

- CPU: Intel Core i7-12700KF
    - 12 cores / 20 threads
    - 3.6 GHz base / up to 5.0 GHz turbo
- RAM: 16 GB DDR4

Storage

- Drive C: NVMe SSD 232 GB (host operating system)
- Drive D: HDD 3.64 TB (main storage for VMs and backups)
- Drive E: SATA SSD 931 GB (additional capacity)

Connectivity

- NAT network (VMnet8) managed by VMware Workstation

DC1 (Domain Controller)

- CPU: 4 vCPU
- RAM: 4 GB
- Disk: 60 GB
- Network: NAT (VMnet8)

Sufficient resources to run AD DS, DNS, DHCP, and File Services reliably in a lab environment.

HOST1 (Client)

- CPU: 2 vCPU
- RAM: 4 GB
- Disk: 40 GB
- Network: NAT (VMnet8)

Minimum resources required for:

- User logon
- Policy application
- Access to shared resources

Maximum performance was not the goal.
The priority was stability, predictability, and functional clarity.

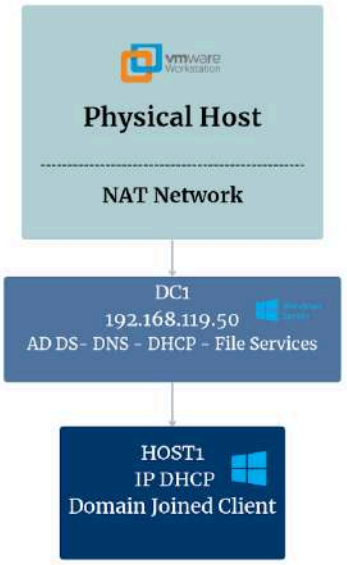
2.5 Environment Diagram

The environment is represented through a simple logical diagram consistent with the project's scope:

- A single Domain Controller (DC1) with centralized services
- One domain client (HOST1)
- A shared private network (NAT)

- Full dependency on DC1 for authentication, DNS, and policy application

This diagram accurately reflects the real laboratory and provides the foundation for the execution blocks described in the following sections.



3. Requirements and Required Resources

3.1 Hardware Requirements

The lab was deployed on a single physical host, sufficient to run a Domain Controller and a Windows client simultaneously without functional degradation or noticeable bottlenecks.

Host requirements

- CPU with virtualization enabled (Intel VT-x)
- Enough RAM to run:
    - 1 Windows Server VM
    - 1 Windows Client VM
- Available storage for:
    - ISO images
    - Virtual disks
    - Occasional snapshots

No advanced configurations were applied (NUMA, CPU pinning, per-VM dedicated disks), as they did not provide additional value for the scope of this project.

3.2 Software Requirements

The entire environment was built using standard software and native tools, avoiding unnecessary external dependencies.

Software used in the lab

- Hypervisor
    - VMware Workstation (local test environment)
    - Virtual network configured as NAT or Host-Only
- Server operating system
    - Windows Server
    - Roles installed during execution:

        - Active Directory Domain Services (AD DS)
        - DNS Server
        - DHCP Server
        - File Services
- Client operating system
    - Windows (client edition)
    - Joined to the lab.unai domain
- Administrative tools
    - Active Directory Users and Computers (ADUC)
    - Group Policy Management
    - Server Manager
    - Event Viewer
    - CMD Console and PowerShell

No third-party tools were installed. All work was carried out using native Windows ecosystem tools, replicating standard administration workflows in corporate environments.

3.3 Operational Dependencies and Considerations

Throughout the project, several critical dependencies were identified that directly affected the correct functioning of the domain.

DNS

- The client must use the Domain Controller exclusively as its DNS server
- Any deviation (external DNS, mixed configuration, or incorrect settings) causes:
    - Login failures
    - GPOs not applying
    - Issues accessing shared resources

Order of configuration

- Correct deployment sequence:
    - Network configuration and static IP
    - Active Directory Domain Services
    - DNS
    - DHCP
    - Client domain join

Breaking this sequence introduces issues that are difficult to isolate and diagnose later.

Time synchronization

- The Domain Controller acts as the time reference for the domain
- Time drift may lead to:
    - Kerberos authentication errors
    - Inconsistent client behavior

Cached credentials

- Changes in group memberships:
    - Do not apply until logoff/logon
    - Directly affect permission and access tests

This behavior was considered during validations.

Snapshots

- Controlled and punctual use, only before structural changes
- Rollbacks were not overused to avoid masking real errors

Relevant technical decision
The priority was to diagnose and correct issues instead of reverting snapshots, reinforcing an operational and realistic approach aligned with system administration in production environments.

4. Step-by-Step Environment Deployment

4.1 Virtualization Environment Preparation

4.1.1 Hypervisor and Networking

The laboratory was deployed on a local virtualization environment using a simple and controlled topology.

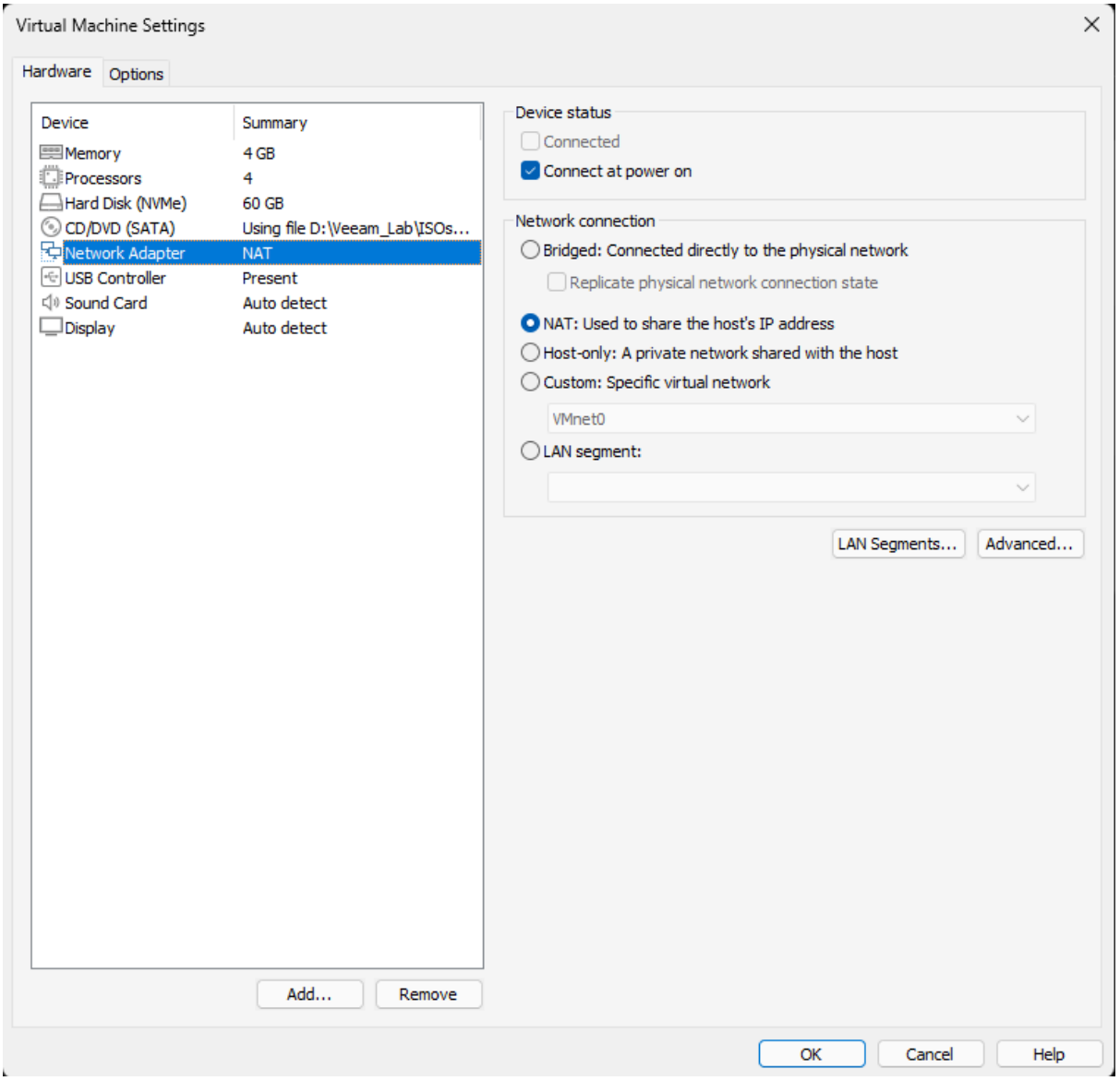
Base configuration:

- Hypervisor: VMware Workstation
- Network type: shared internal network (NAT / VMnet)
- Common IP segment for all machines in the lab

Applied criteria:

- All VMs share the same broadcast domain (L2)
- No additional routing or unnecessary segmentation introduced
- Simplicity improves troubleshooting of DNS, AD, and GPO

Figure 4.1 – VM network configuration for the server (adapter set to internal/NAT mode)



4.2 Creation of the Domain Controller Virtual Machine

4.2.1 VM Configuration

Configuration applied:

- Name: DC1
- Operating system: Windows Server Standard (Desktop Experience)

Assigned resources:

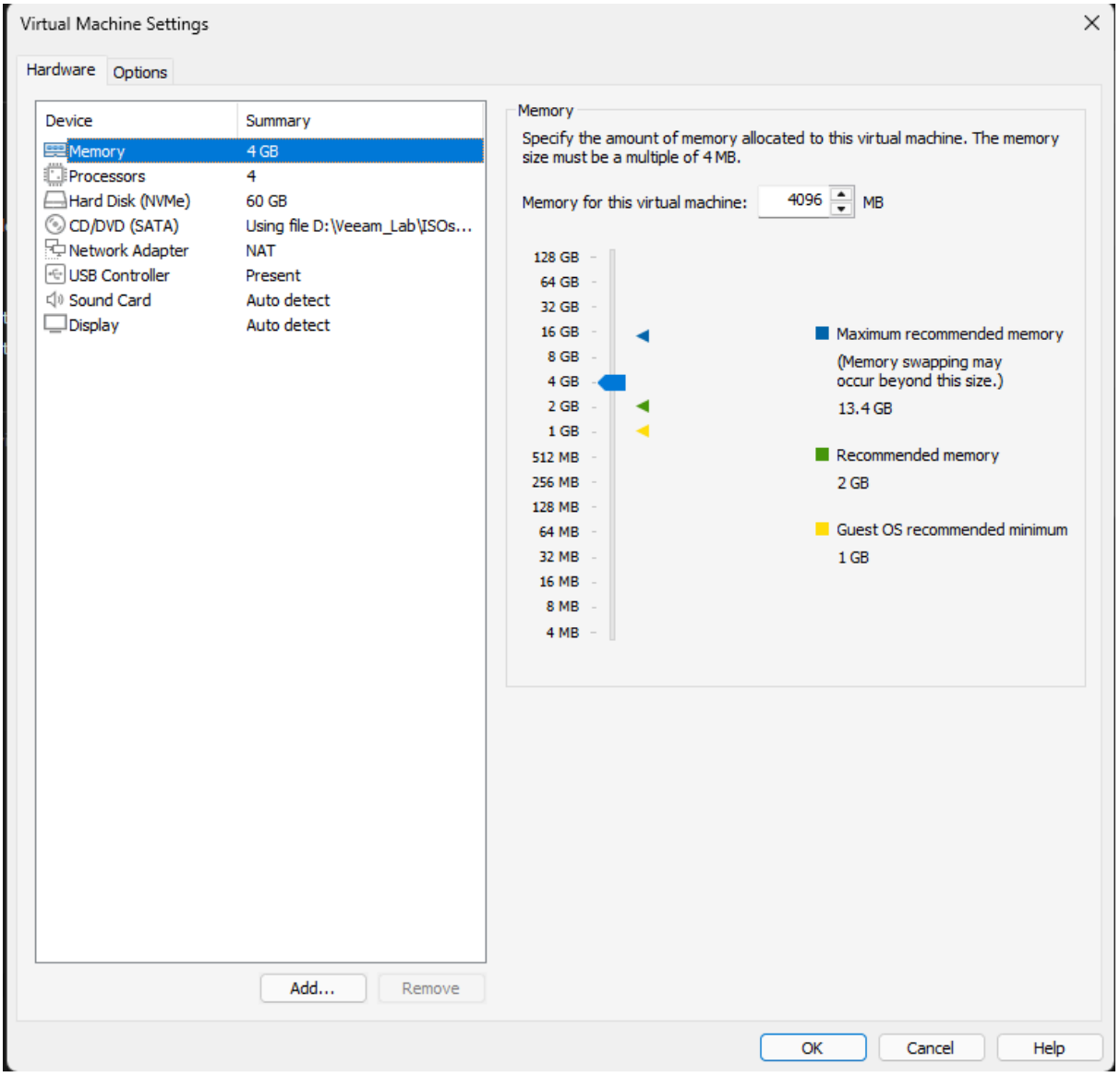
- CPU: 2 vCPU

- RAM: 4–8 GB
- Disk: 60 GB
- Network: 1 NIC

Technical decision:

- Desktop Experience was selected to simplify graphical administration and align with common setups in junior/intermediate roles.

Figure 4.2 – Domain Controller VM hardware configuration (CPU, RAM, disk, network)

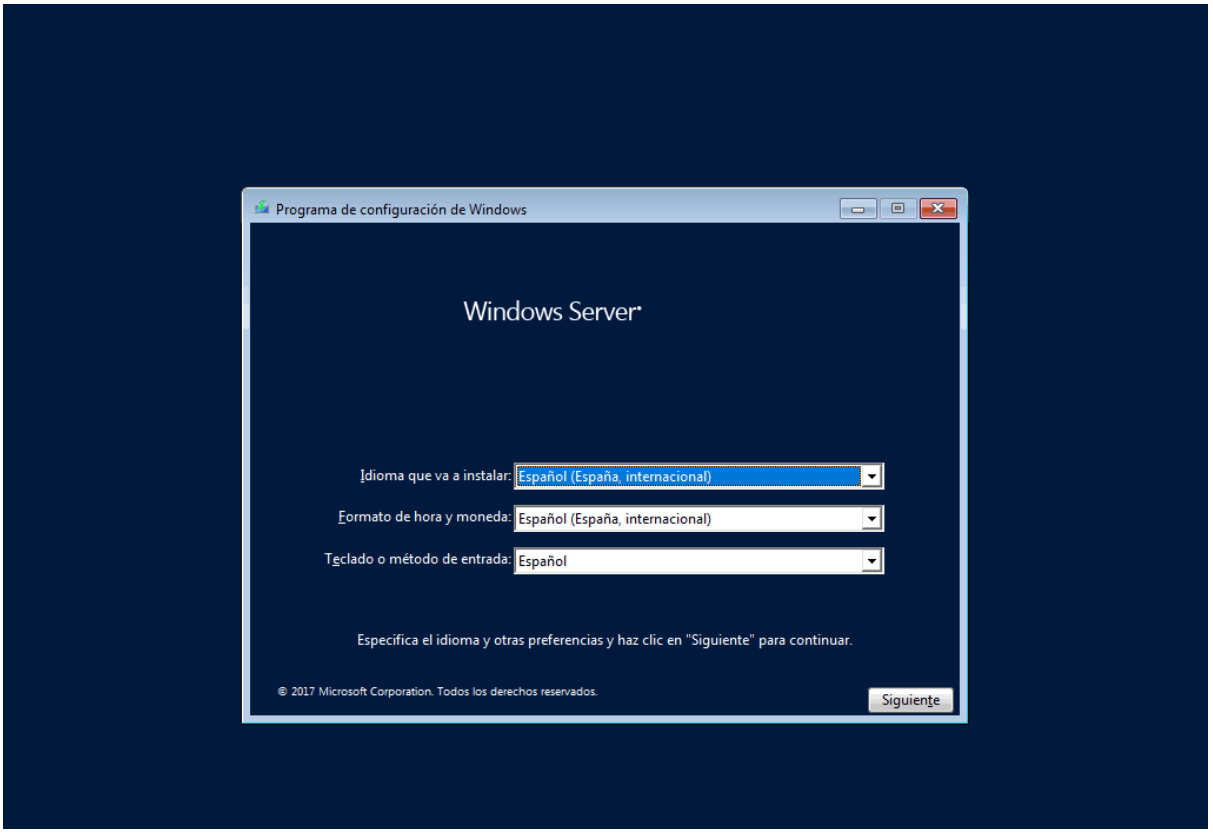


4.3 Initial Installation of Windows Server

4.3.1 Installation Process

- Clean installation from ISO
- Selected edition: Windows Server Standard (Desktop Experience)
- Initial account configured: Administrator
- No roles installed during this phase

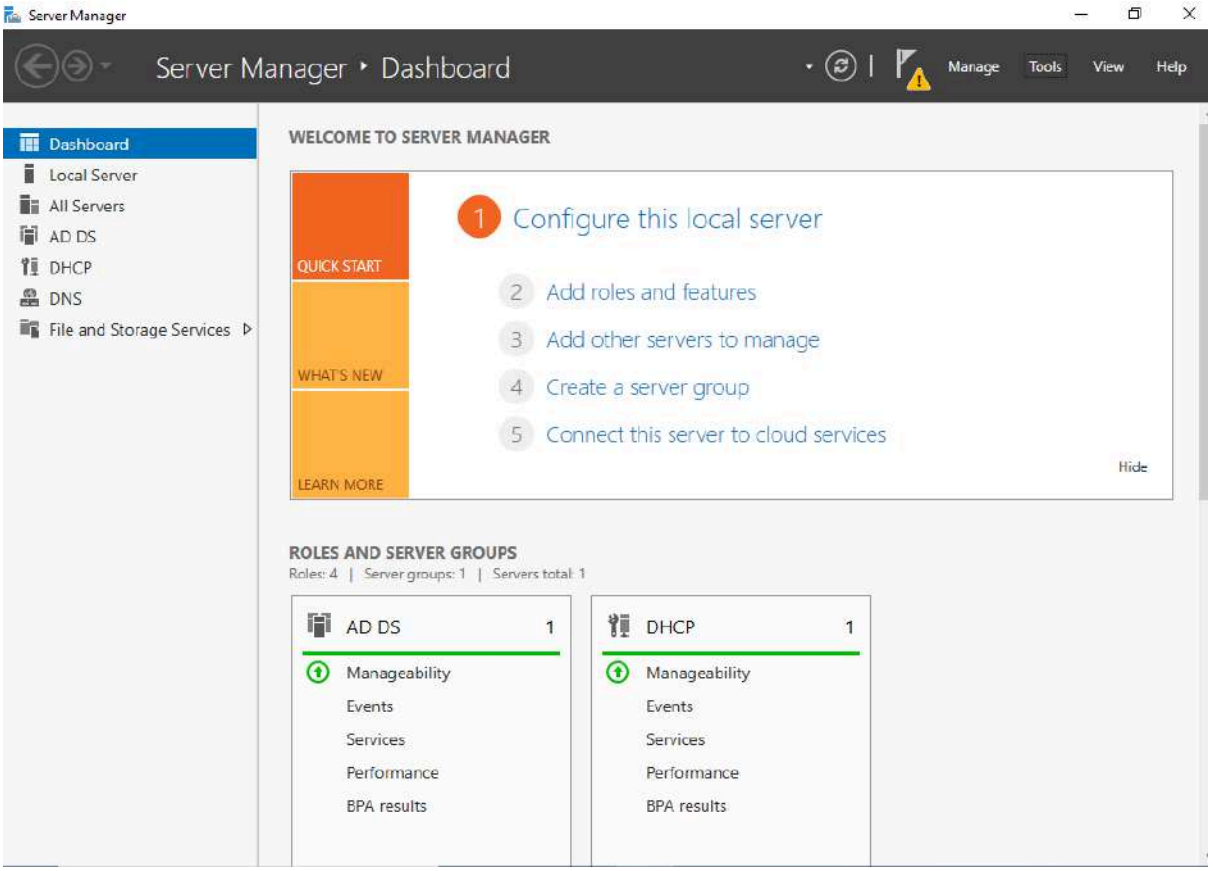
Figure 4.3 – Initial Windows Server installation completed



4.3.2 First Boot and Verification

- System booted successfully
- Server Manager showed no warnings
- Operating system stable and ready for configuration

Figure 4.4 – Initial desktop after first Windows Server logon



4.4 Server Network Configuration

4.4.1 Initial State

- Network interface configured via DHCP
- IP correctly assigned by the hypervisor's virtual network

4.4.2 Static IP Configuration

Configuration applied:

- Static IP within the lab range
- /24 subnet mask
- Gateway set according to virtual network
- DNS pointed to the server itself

Key technical decision:

- A Domain Controller must resolve its own name.
  Pointing to external DNS causes failures in AD, GPO, and authentication.

Figure 4.5 – NIC properties showing applied static IP configuration

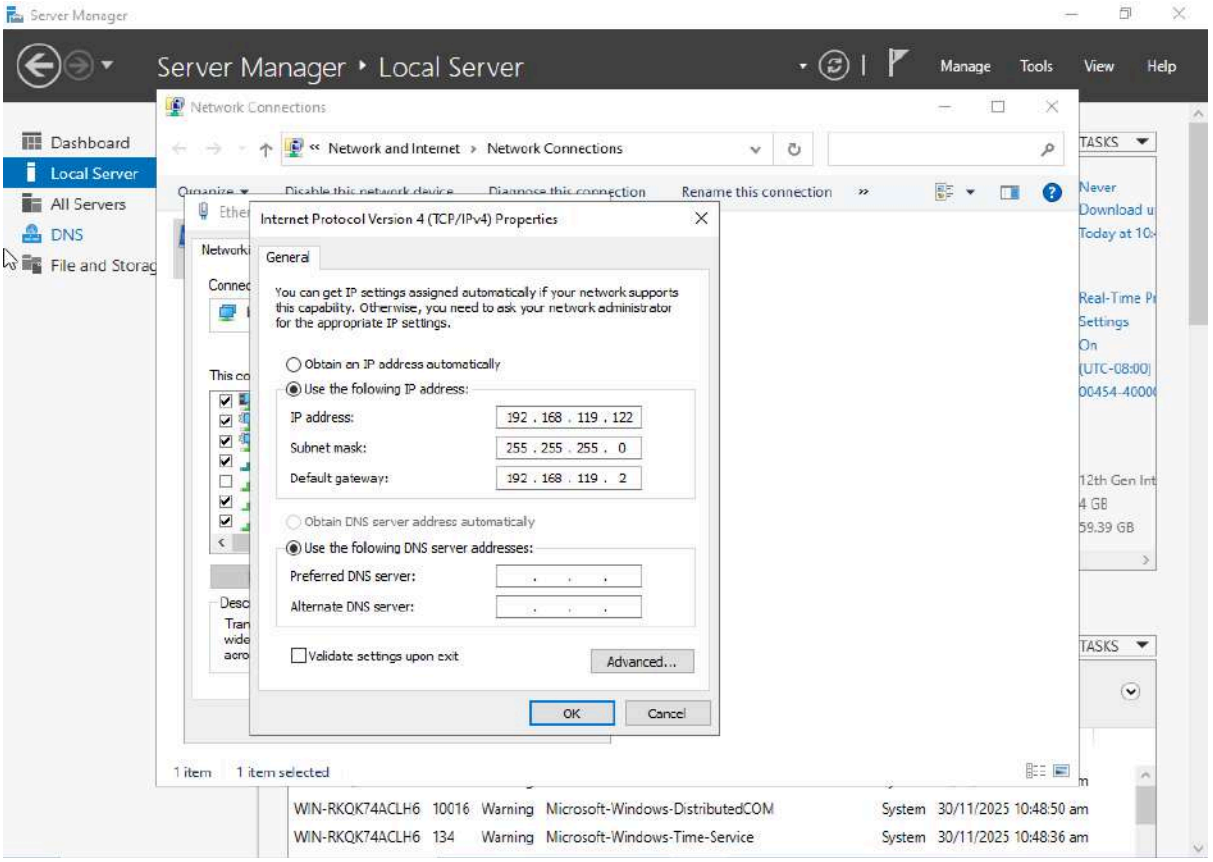
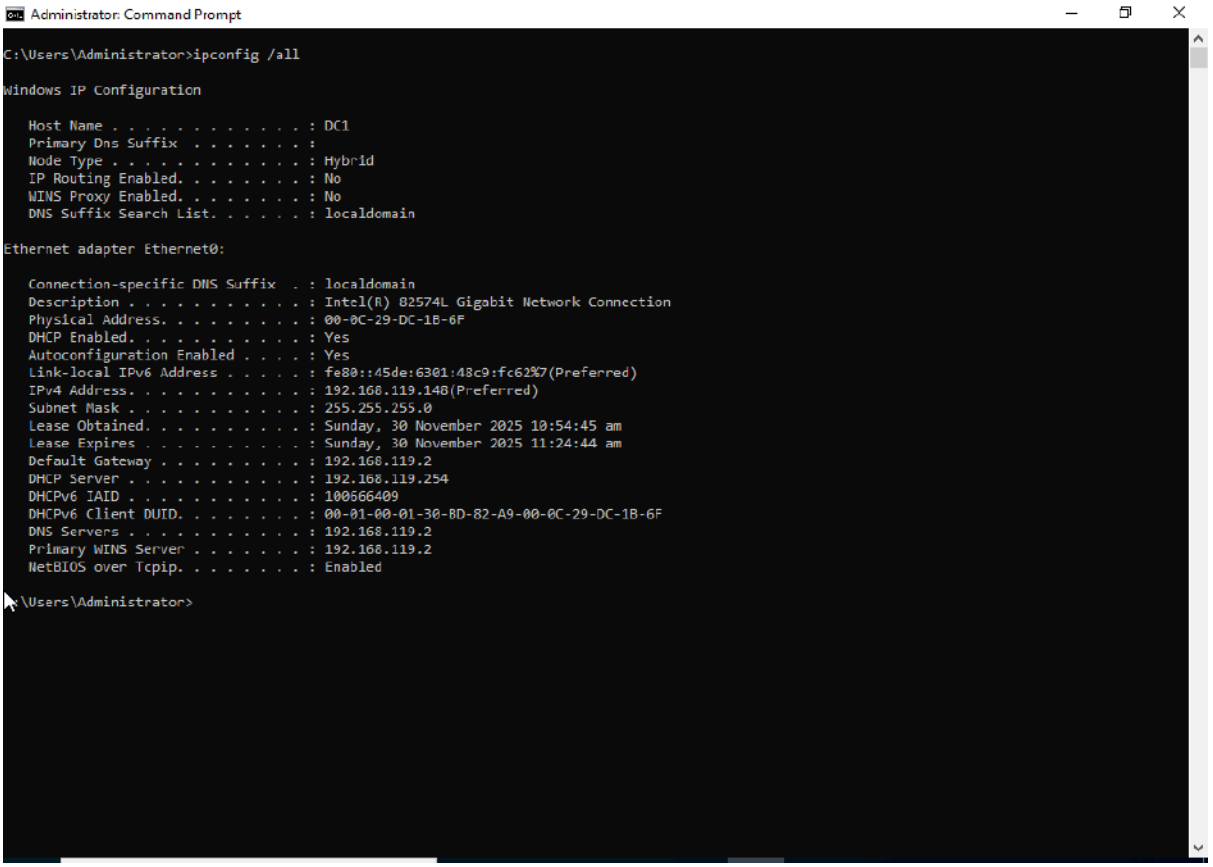


Figure 4.6 – `ipconfig /all` confirming static IP and internal DNS resolution



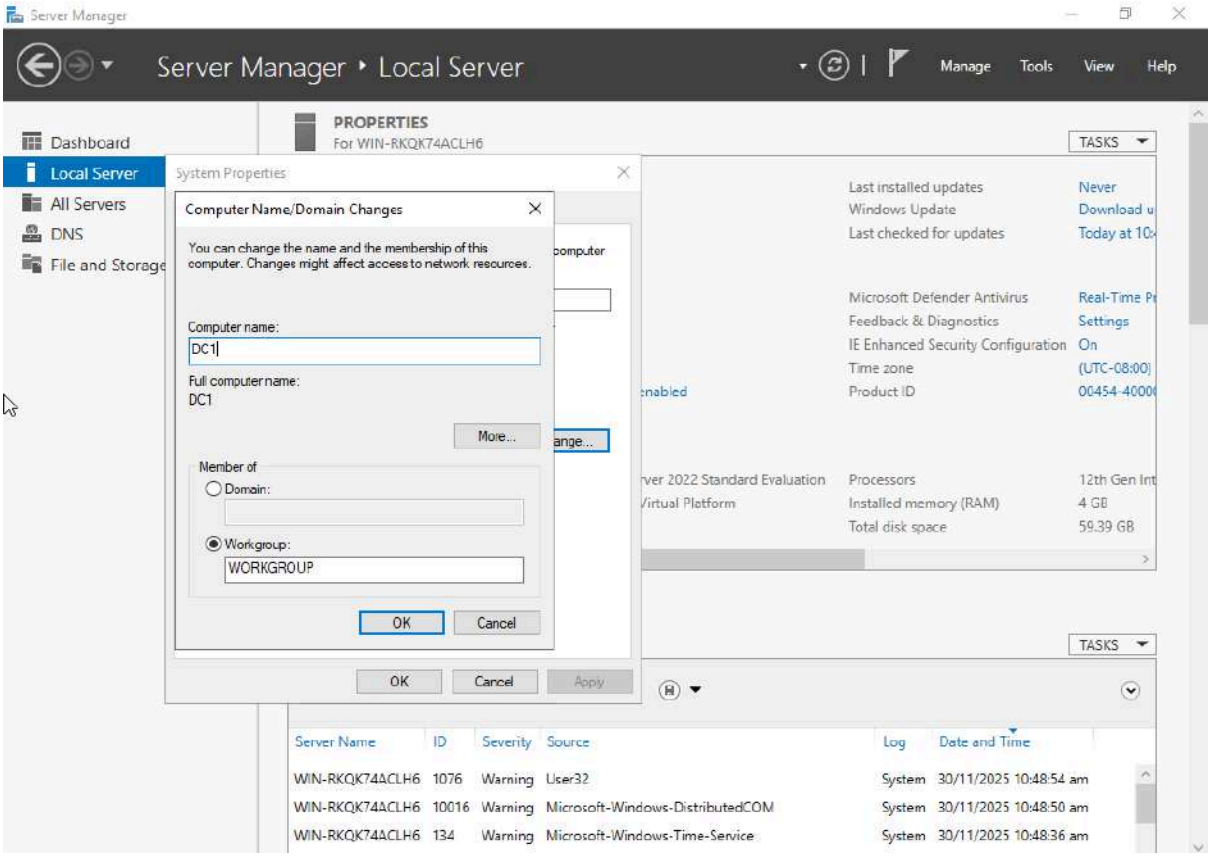
4.5 Server Renaming

4.5.1 Name Change

- Generic default name replaced with DC1

Applied path:
Server Manager → Local Server → Computer Name → Change

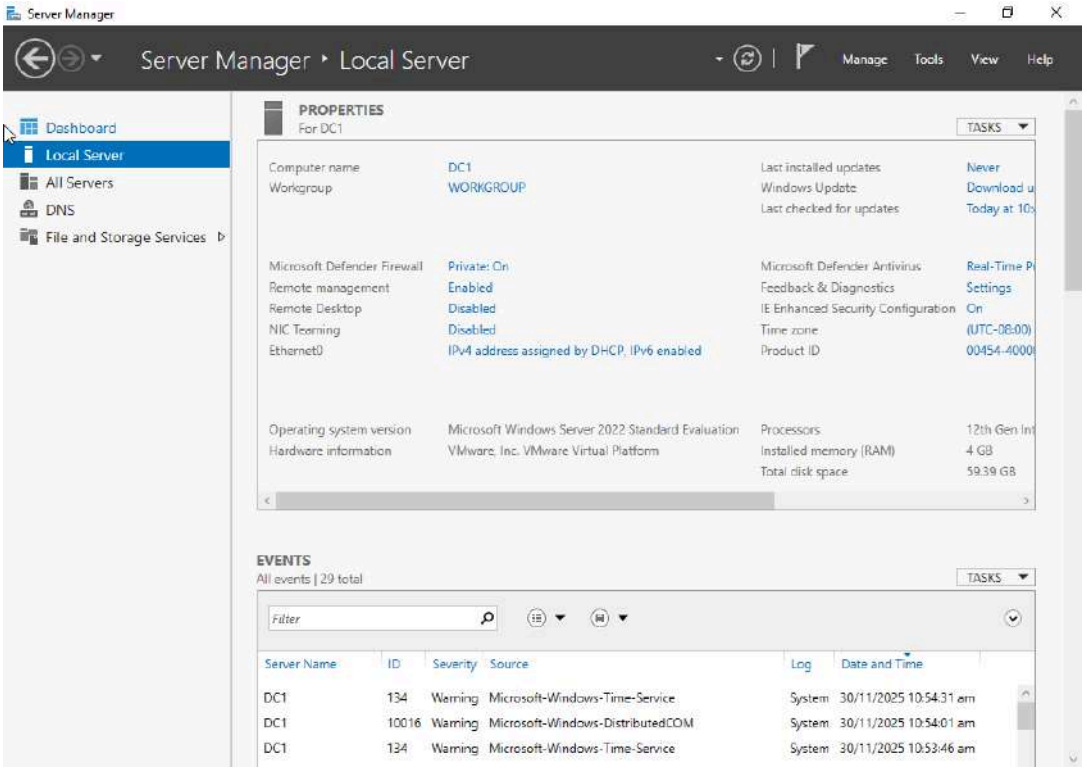
Figure 4.7 – System properties showing assigned hostname: DC1



4.5.2 Restart and Validation

- Restart completed successfully
- System starts with the new hostname

Figure 4.8 – Server Manager after reboot showing hostname DC1

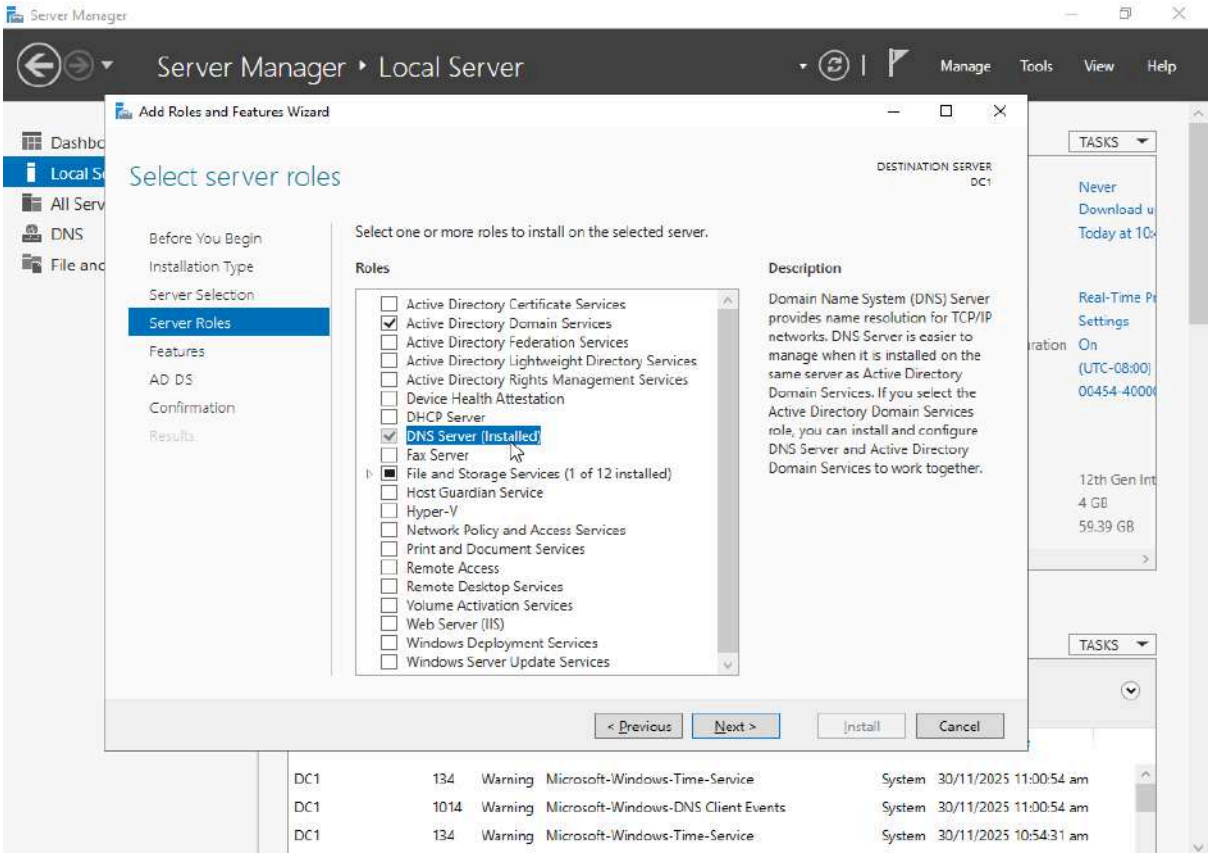


4.6 Installation of Active Directory Domain Services Role

4.6.1 Role Installation

- Installed role: Active Directory Domain Services
- Dependencies accepted (including DNS)

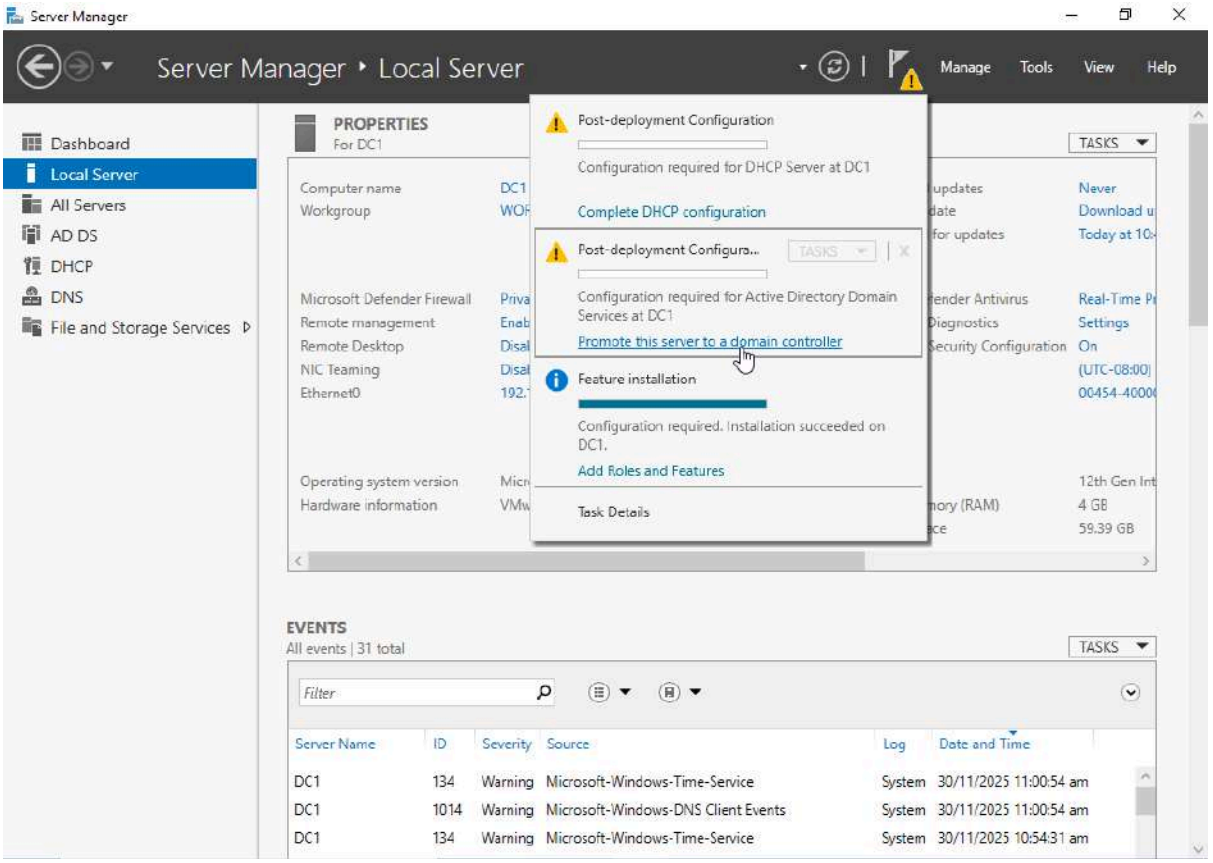
Figure 4.9 – Roles wizard showing AD DS selected for installation



4.6.2 Role Installed

- AD DS successfully installed
- Option to promote the server to Domain Controller now available

Figure 4.10 – Server Manager notification: “Promote this server to a domain controller”



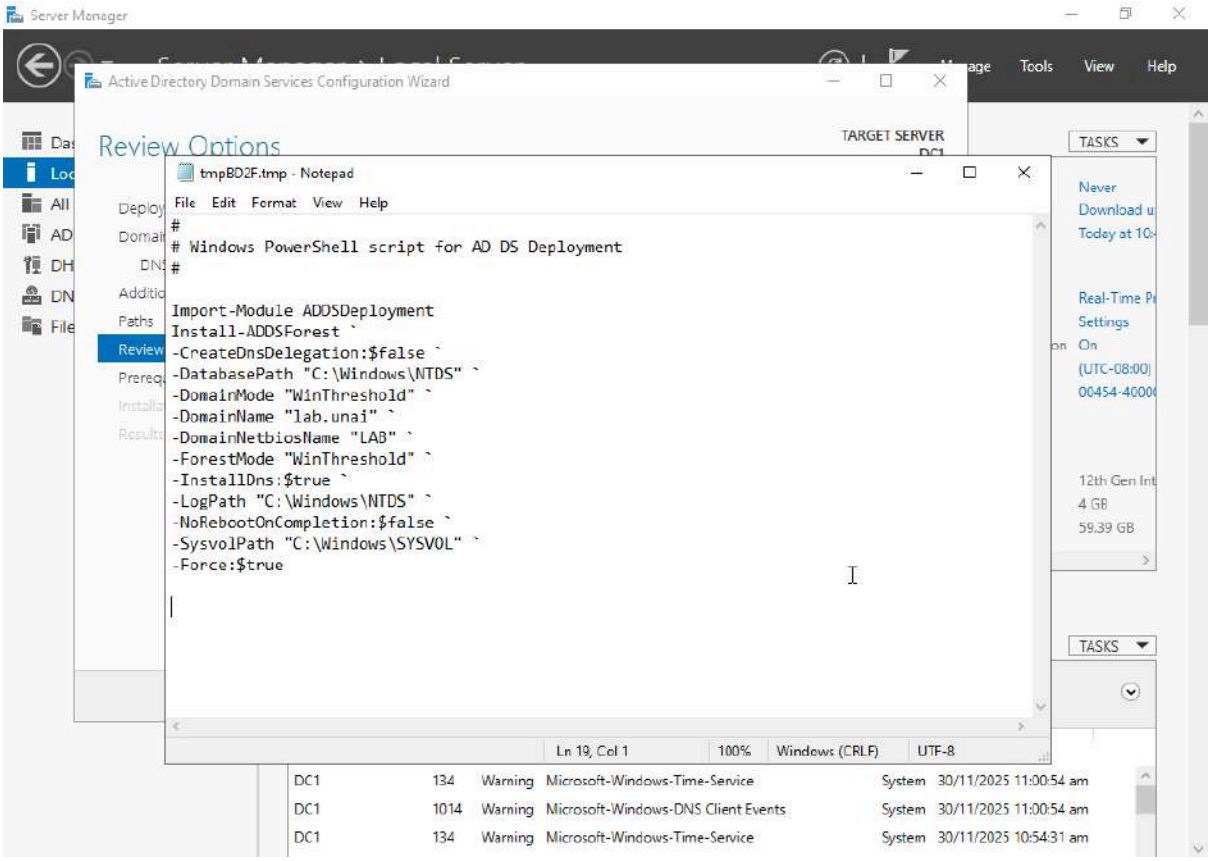
4.7 Promotion to Domain Controller

4.7.1 Domain Configuration

Defined parameters:

- New forest
- Internal domain: lab.unai
- DNS Server and Global Catalog enabled

Figure 4.11 – Promotion wizard showing domain configuration for lab.unai



4.7.2 Promotion Process

During promotion:

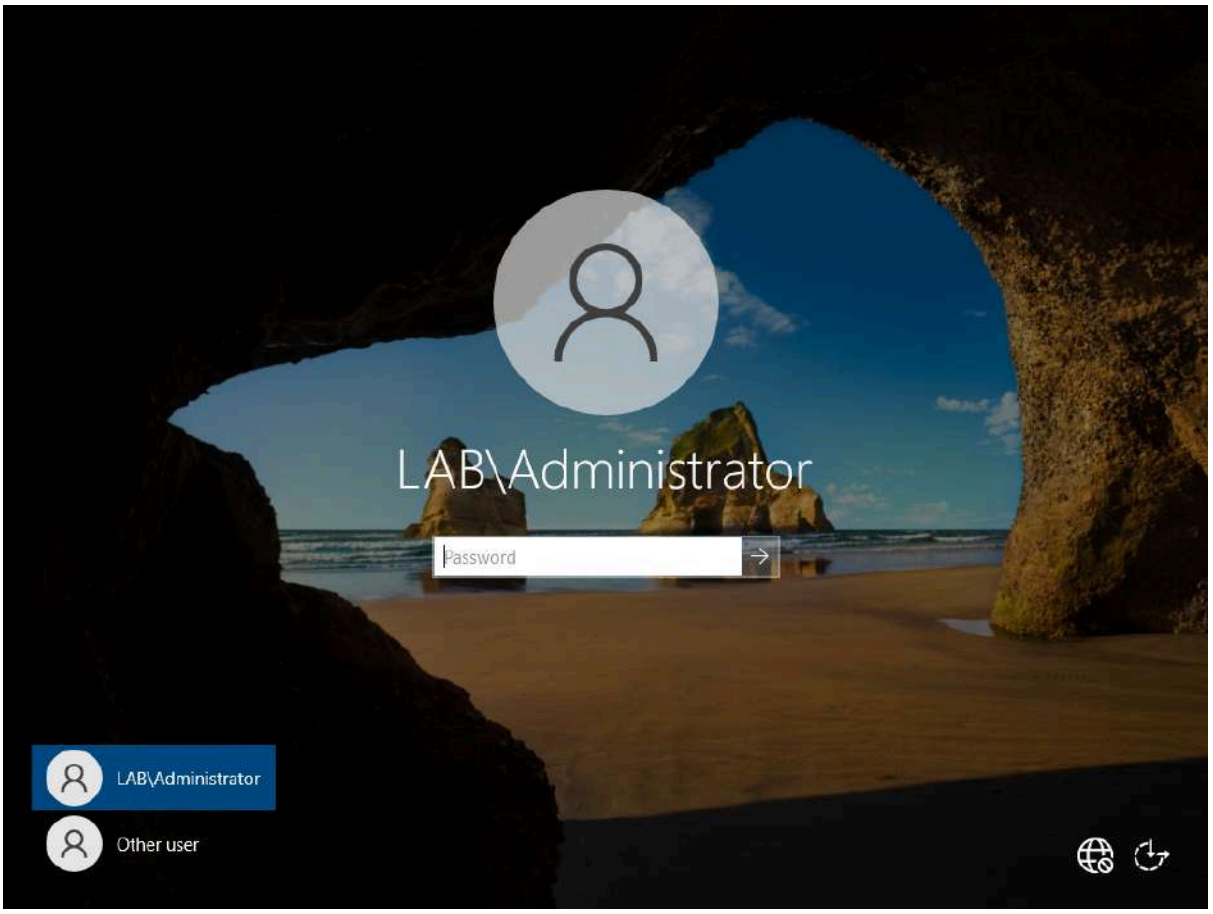
- Internal DNS created
- SRV records and zones generated
- SYSVOL and NTDS initialized
- Automatic system reboot executed

4.8 First Boot as Domain Controller

4.8.1 Sign-in

- Sign-in performed as **LAB\Administrator**

Figure 4.12 – Login screen showing LAB domain available



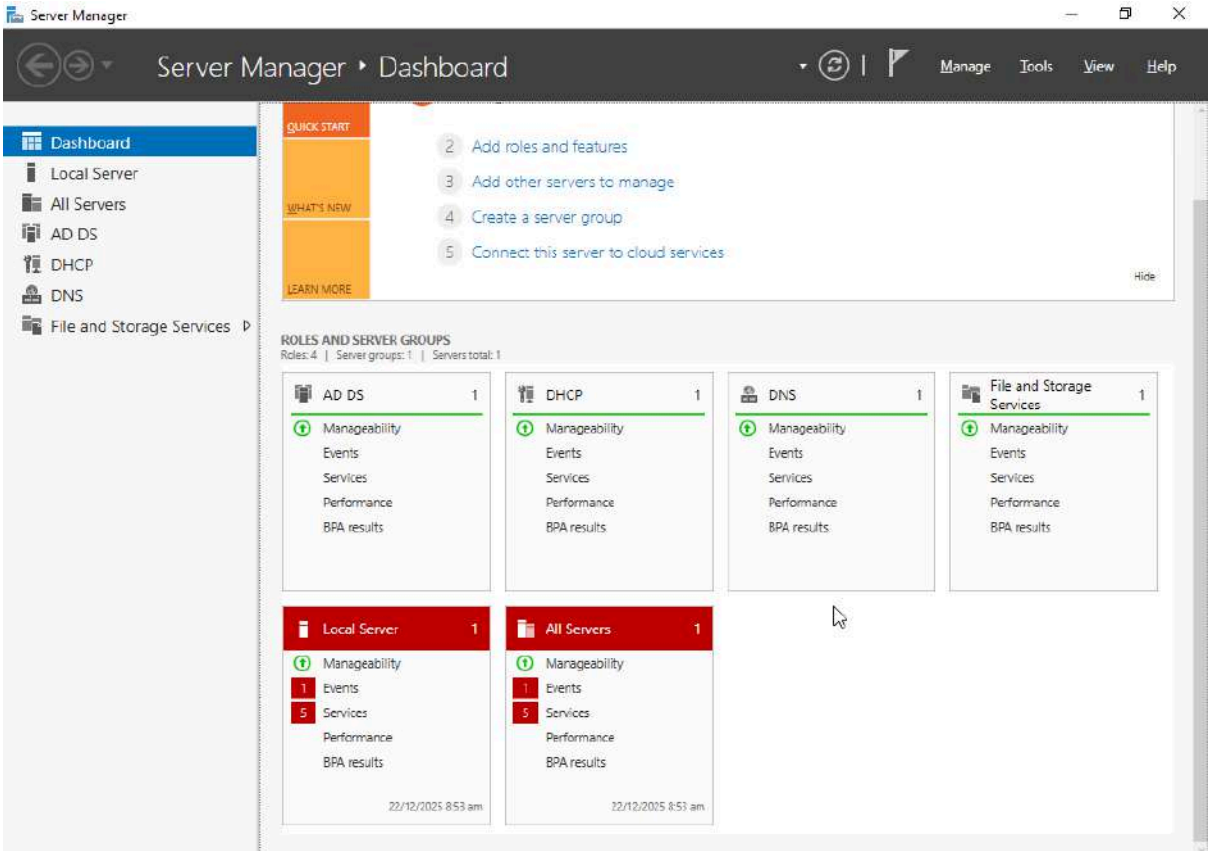
4.8.2 Verification of critical services

Services verified:

- Active Directory Domain Services
- DNS Server
- Netlogon
- Kerberos Key Distribution Center

Status: **Running**

Figure 4.13 – Server Manager confirming critical services in Running state

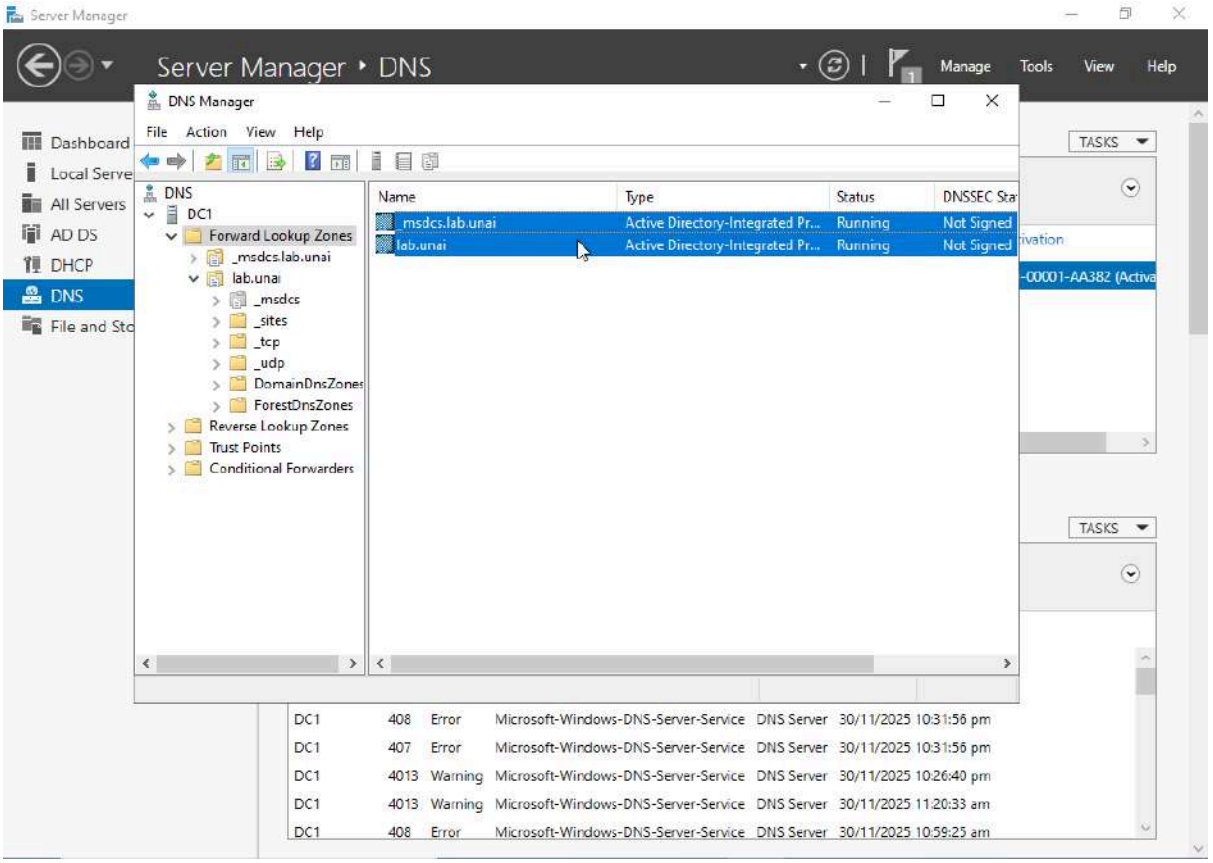


4.9 Verification of Internal DNS

4.9.1 Zone verification

- Forward lookup zone for the domain present
- `_msdcs` zone automatically created
- SRV records and DC A record correct

Figure 4.14 – DNS Manager showing forward zones and automatically created _msdcs



4.10 DNS Forwarders Configuration

4.10.1 Applied configuration

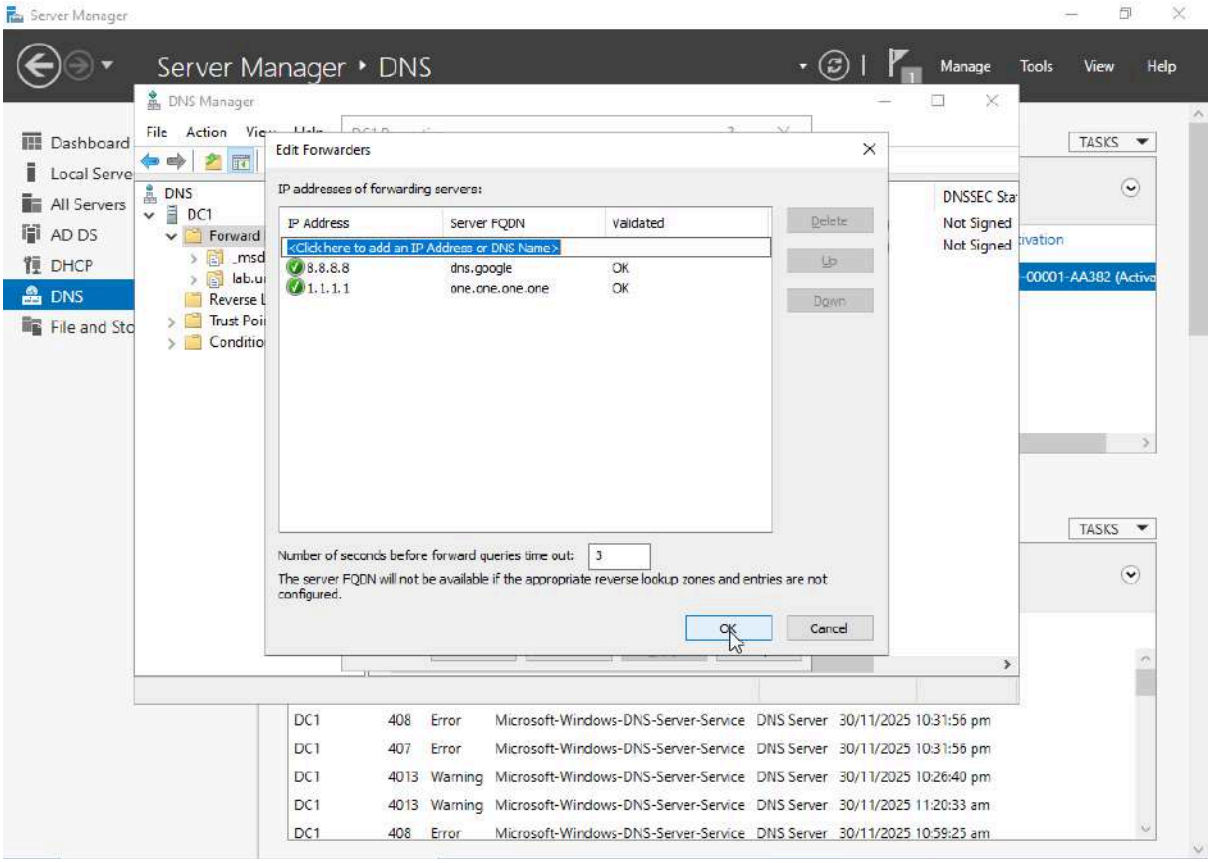
Forwarders configured:

- 8.8.8.8
- 1.1.1.1

Applied criteria:

- Used exclusively for external name resolution
- Do not affect internal AD functionality

Figure 4.15 – DNS properties showing configured forwarders (8.8.8.8 / 1.1.1.1)



4.11 DHCP Service Installation and Configuration

4.11.1 DHCP Server role installation

Actions performed:
The DHCP Server role was installed on DC1 using Server Manager.

Path:

- Server Manager → Add Roles and Features

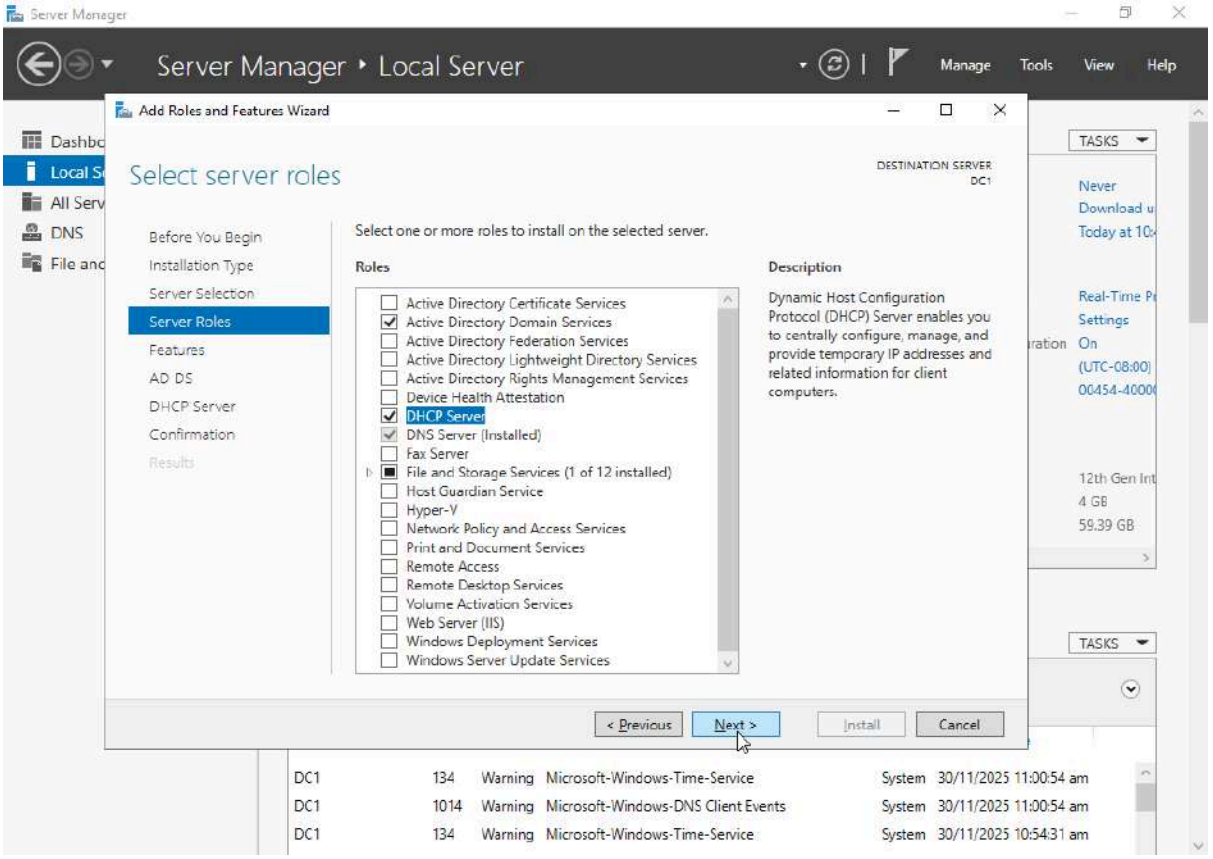
Applied configuration:

- Role-based installation
- Local server: DC1
- Selected role: DHCP Server
- Dependencies accepted

Result:

- Installation completed successfully

Figure 4.16 – Roles wizard showing DHCP Server selected



4.11.2 DHCP Server authorization in Active Directory

Actions performed:

- Post-install configuration wizard executed
- DHCP Server authorized in Active Directory using **LAB\Administrator** credentials

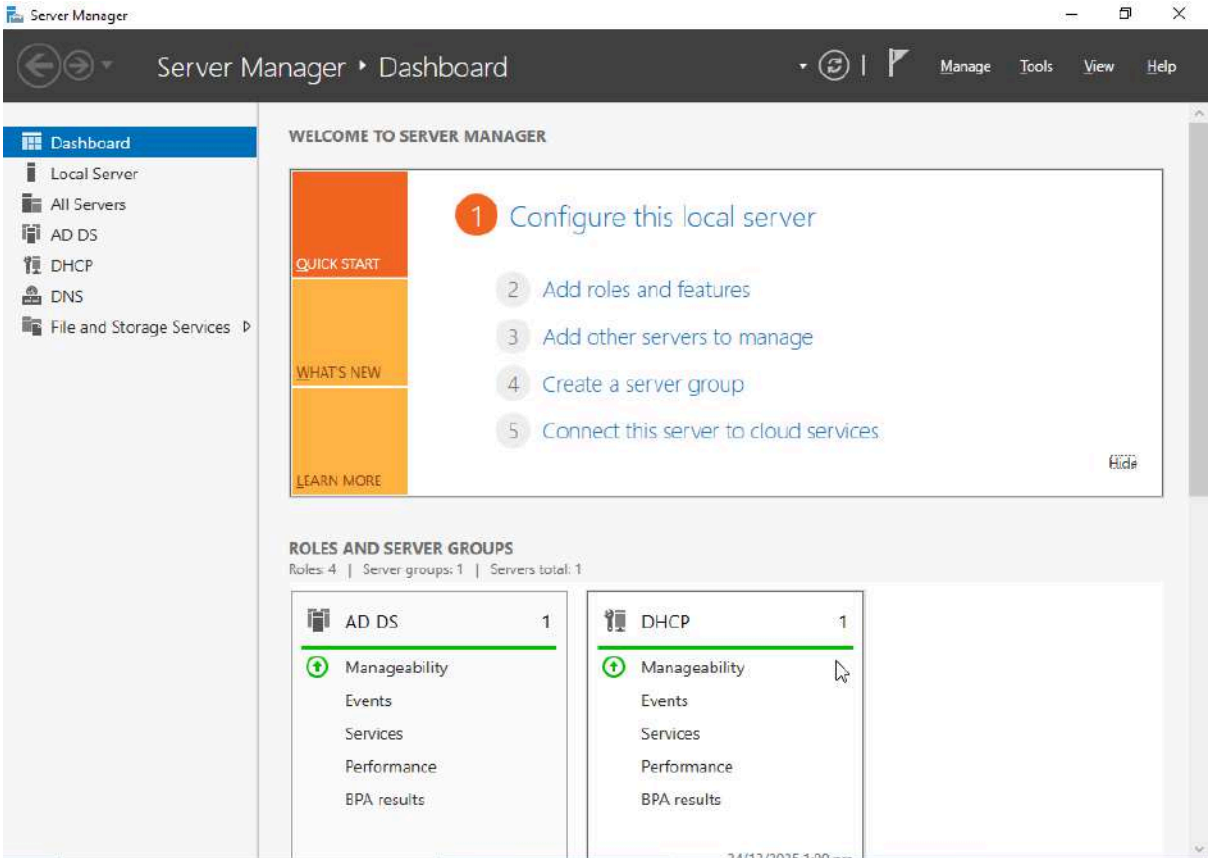
Result:

- DHCP server successfully authorized
- No warnings in Server Manager

Technical decision:

- In Active Directory environments, a DHCP server must be authorized to assign valid IP addresses. Without authorization, the service is not operational.

Figure 4.17 – Server Manager showing DHCP authorized in the domain



4.11.3 IPv4 scope creation

Actions performed:

- New IPv4 scope created via DHCP Manager

Path:

- Server Manager → Tools → DHCP → IPv4 → New Scope

Applied configuration:

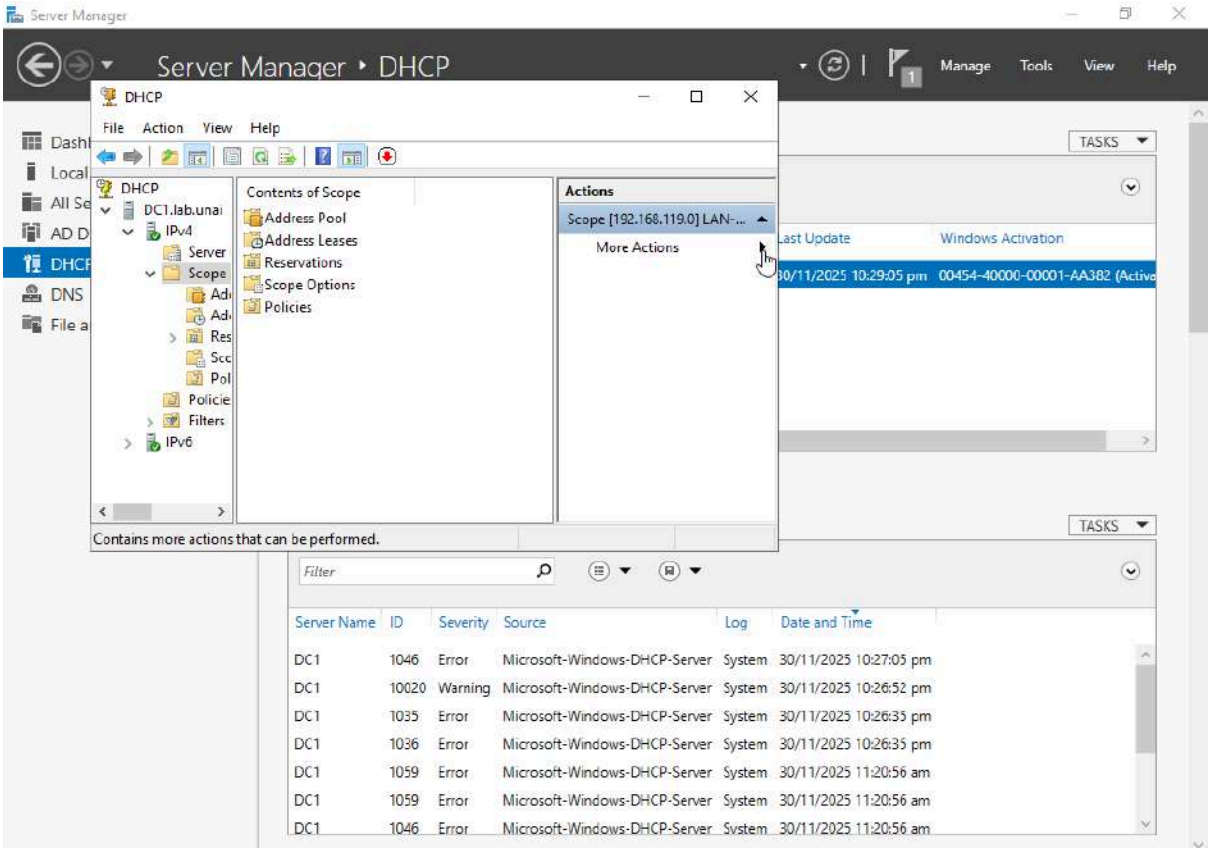
- Scope name: **LAN.192.168.119.x**
- Address range:

    - Start: **192.168.119.60**
    - End: **192.168.119.230**
- Subnet mask: **/24**
- Lease duration: **8 days (default)**
- Exclusions: none

Applied criteria:

- The range leaves room for static addresses (DC, gateway, additional VMs) without conflict with dynamic assignments.

Figure 4.18 – IPv4 scope created and visible in DHCP Manager



4.11.4 Scope options configuration

Scope options configured during scope creation:

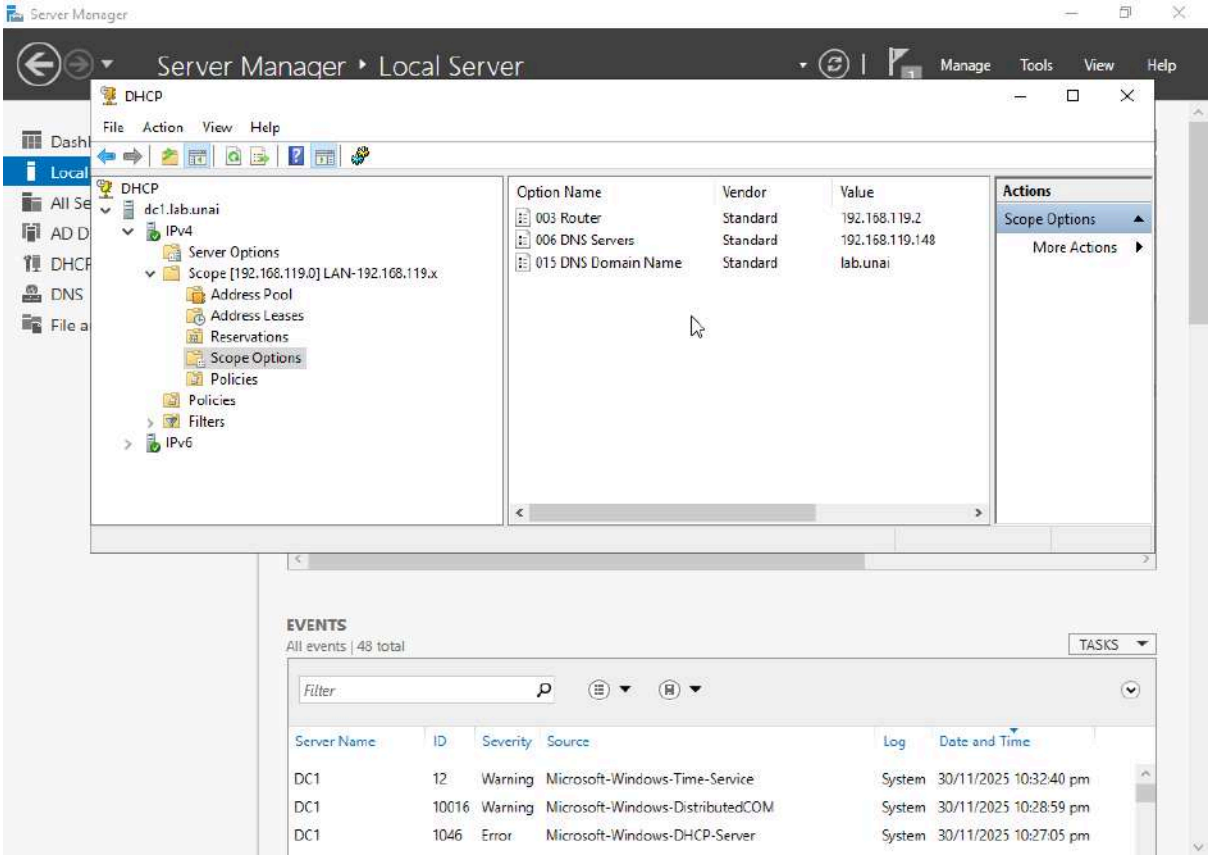
- **003 Router (Default Gateway):** IP of virtual network gateway

- **006 DNS Servers:** IP of Domain Controller (DC1)
- **015 DNS Domain Name:** lab.unai

Key technical decision:

- The client must use only the Domain Controller as DNS.
  Configuring external DNS in the scope breaks internal resolution and affects authentication, GPOs, and domain services.

Figure 4.19 – Configured scope options: gateway, DNS, and lab.unai domain



4.11.5 DHCP service activation and validation

Service state:

- Scope successfully activated
- DHCP service in **Running** state
- Authorized server visible in DHCP console

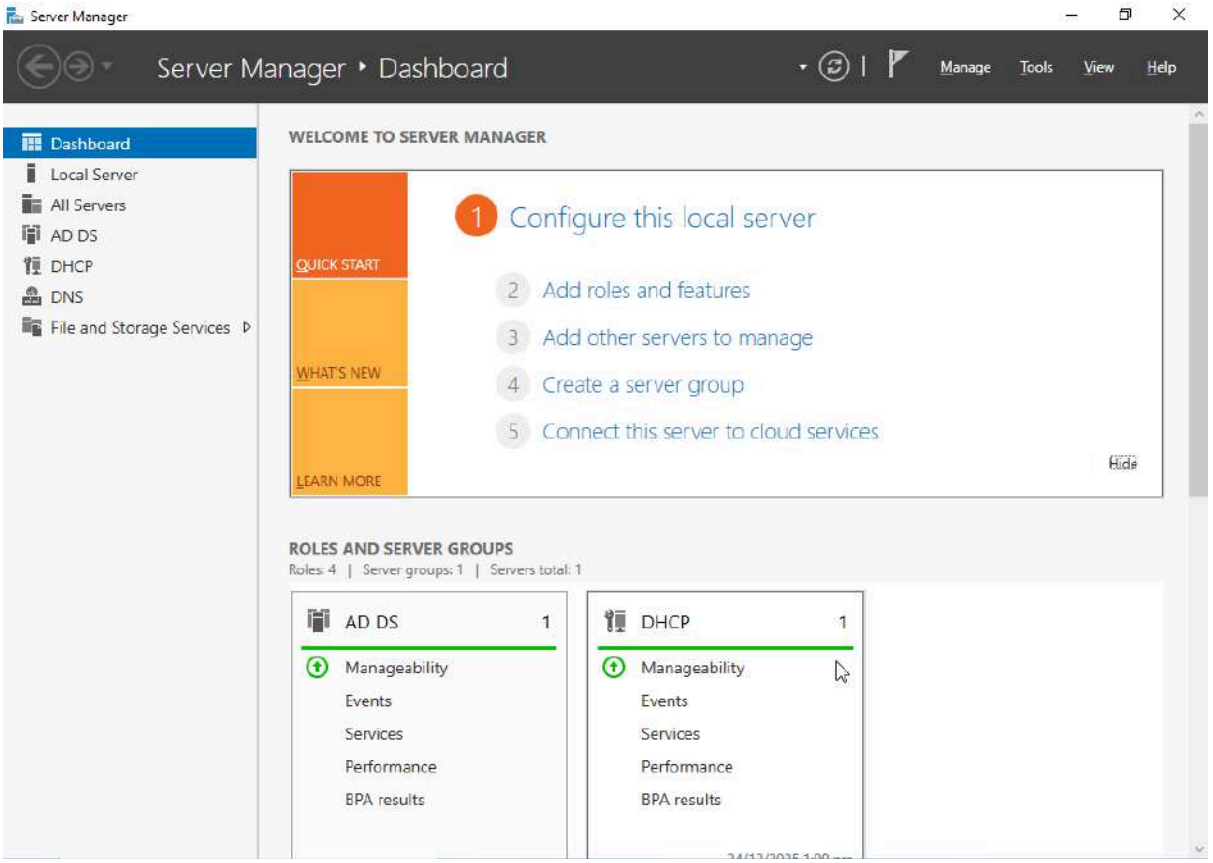
Validations performed:

- Checked in **services.msc** confirming service execution
- Scope visually confirmed as enabled in DHCP Manager

Note:

- No active clients yet, therefore the lease list is empty at this stage.

Figure 4.20 – DHCP service running and scope active without errors



4.12 Client Virtual Machine Creation

4.12.1 Operating system decision

Windows 10 Enterprise selected as domain client.

Applied criteria:

- Realistic corporate scenario
- Full domain-join support

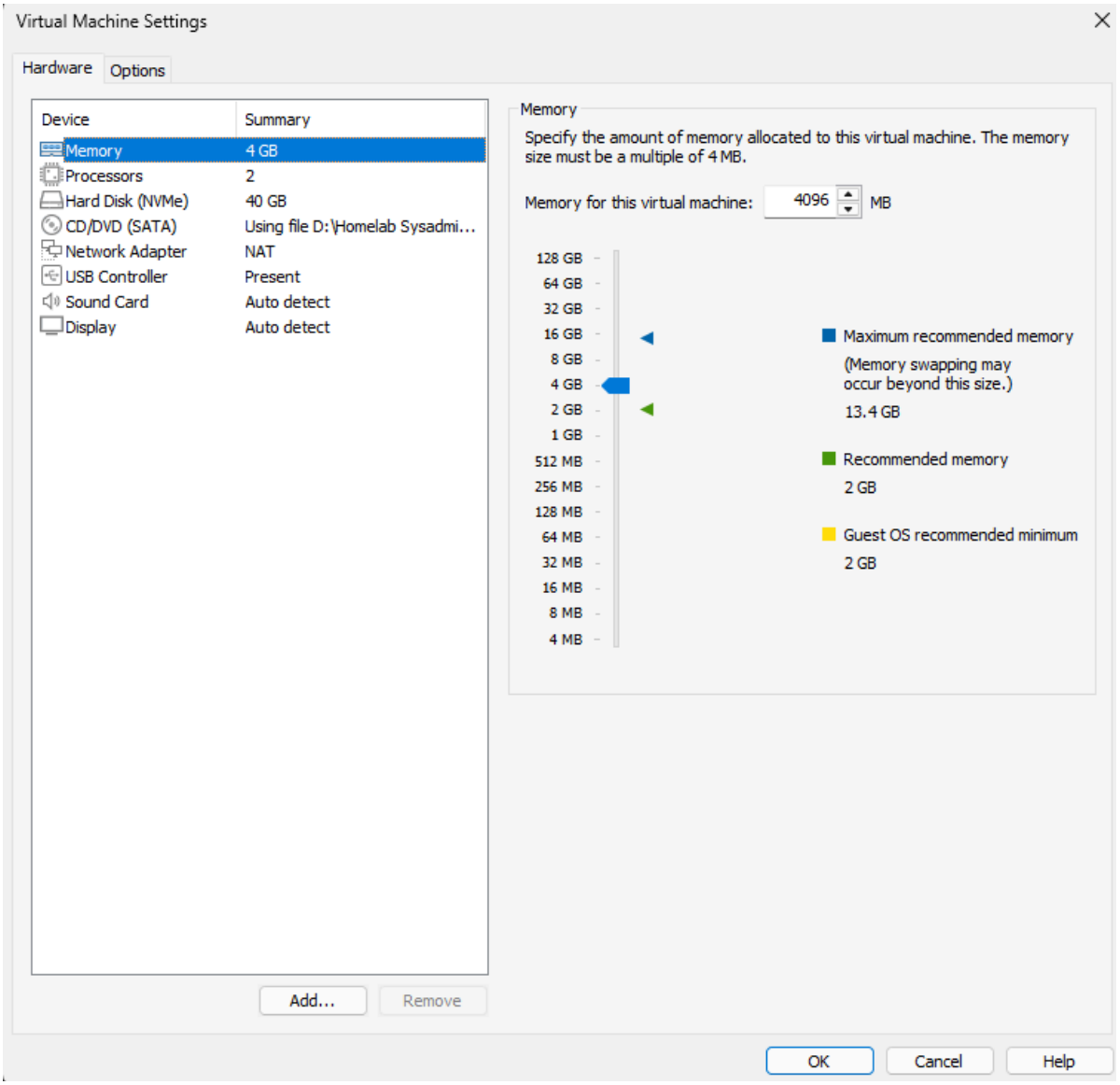
- Aligned with common technical validation workflows

4.12.2 VM configuration

Configuration applied:

- Name: **HOST1**
- Resources:
    - 2 vCPU
    - 4 GB RAM
    - 40–60 GB disk
- Network: same internal/NAT network as DC1

Figure 4.21 – Client VM hardware configuration

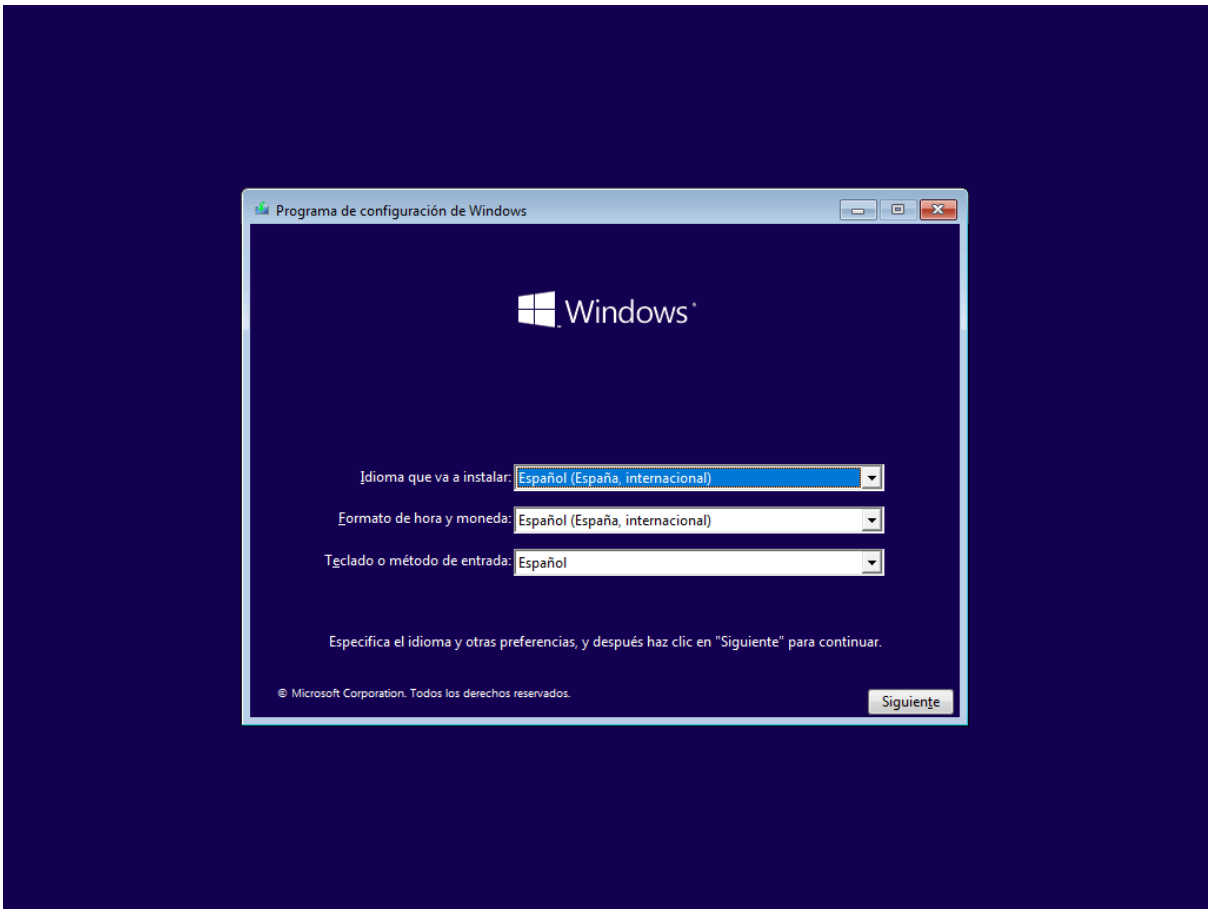


4.13 Client Operating System Installation

4.13.1 Initial installation

- Clean installation from ISO
- Edition: Windows 10 Enterprise
- Temporary local account created
- No license activation (lab environment)

Figure 4.22 – Initial client desktop after installation completed



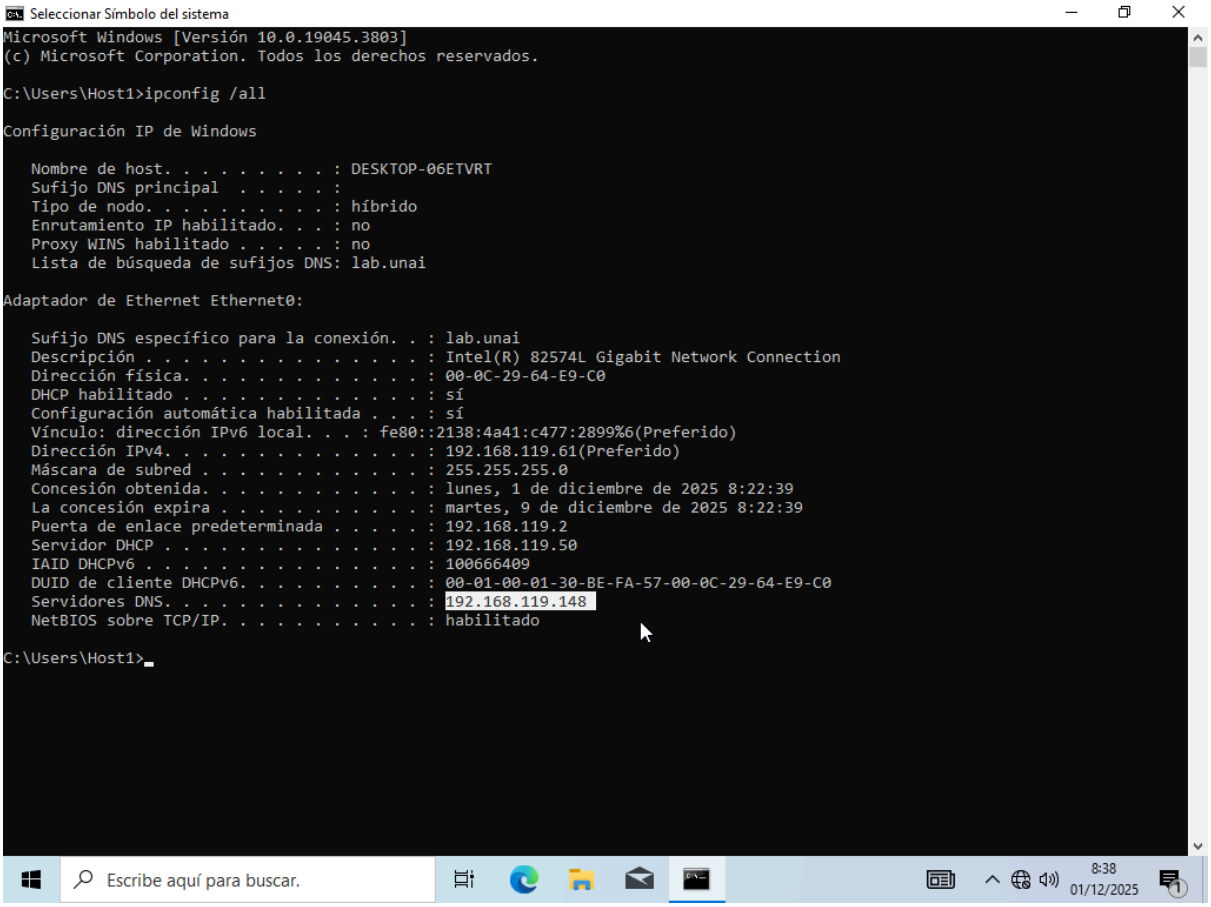
4.14 Network Verification on Client (pre-domain join)

4.14.1 DHCP validation

Validations performed:

- IP within DHCP scope range
- Correct gateway
- DHCP server: DC1
- DNS automatically assigned: DC1

Figure 4.23 – Full `ipconfig /all` output from HOST1

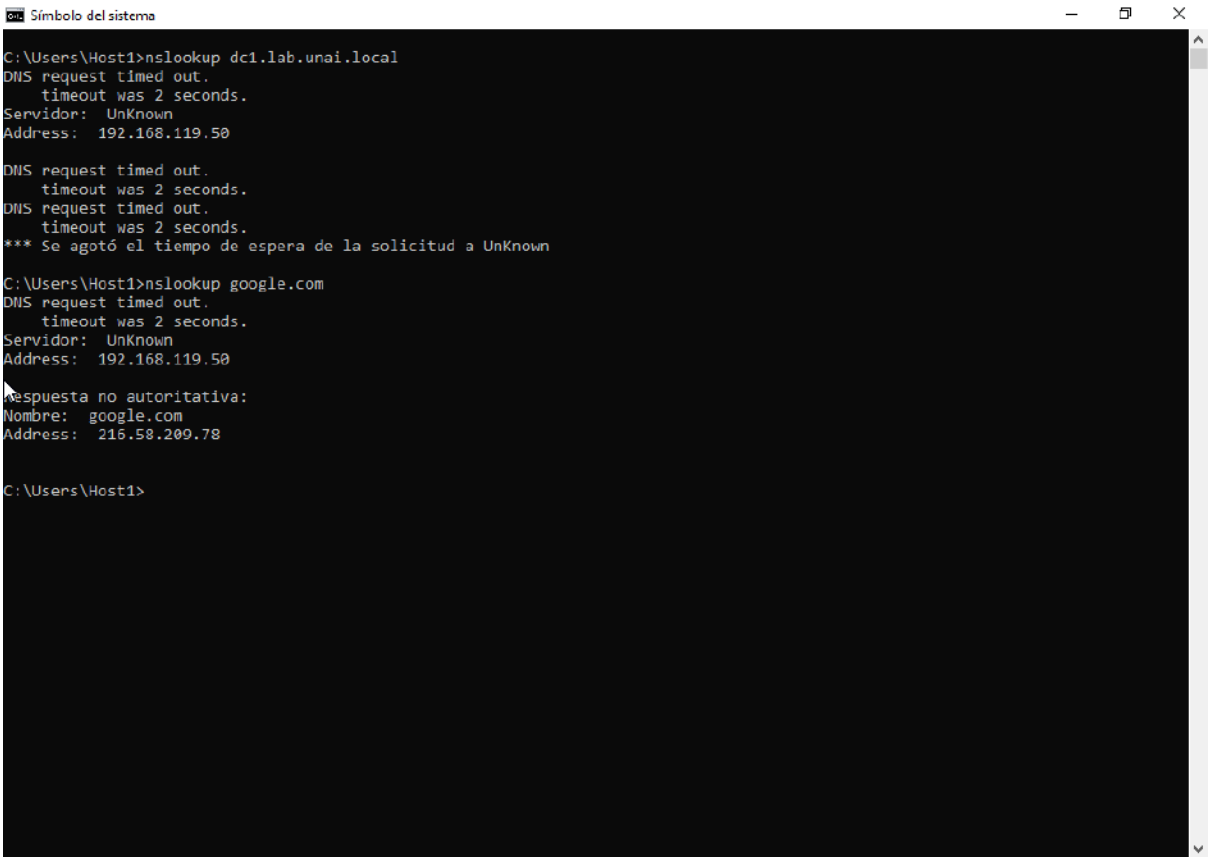


4.14.2 DNS validation

Validations performed:

- Correct resolution of **DC1.lab.unai**
- Connectivity with DC confirmed
- Internal DNS functioning correctly

Figure 4.24 – Ping and nslookup resolving the Domain Controller



4.15 Domain Join of the Client

4.15.1 Initial incident detection

Detected issue:

- Domain join option unavailable

Cause:

- Incorrect Windows edition (Home/Basic)

Decision applied:

- Use Windows 10 Enterprise

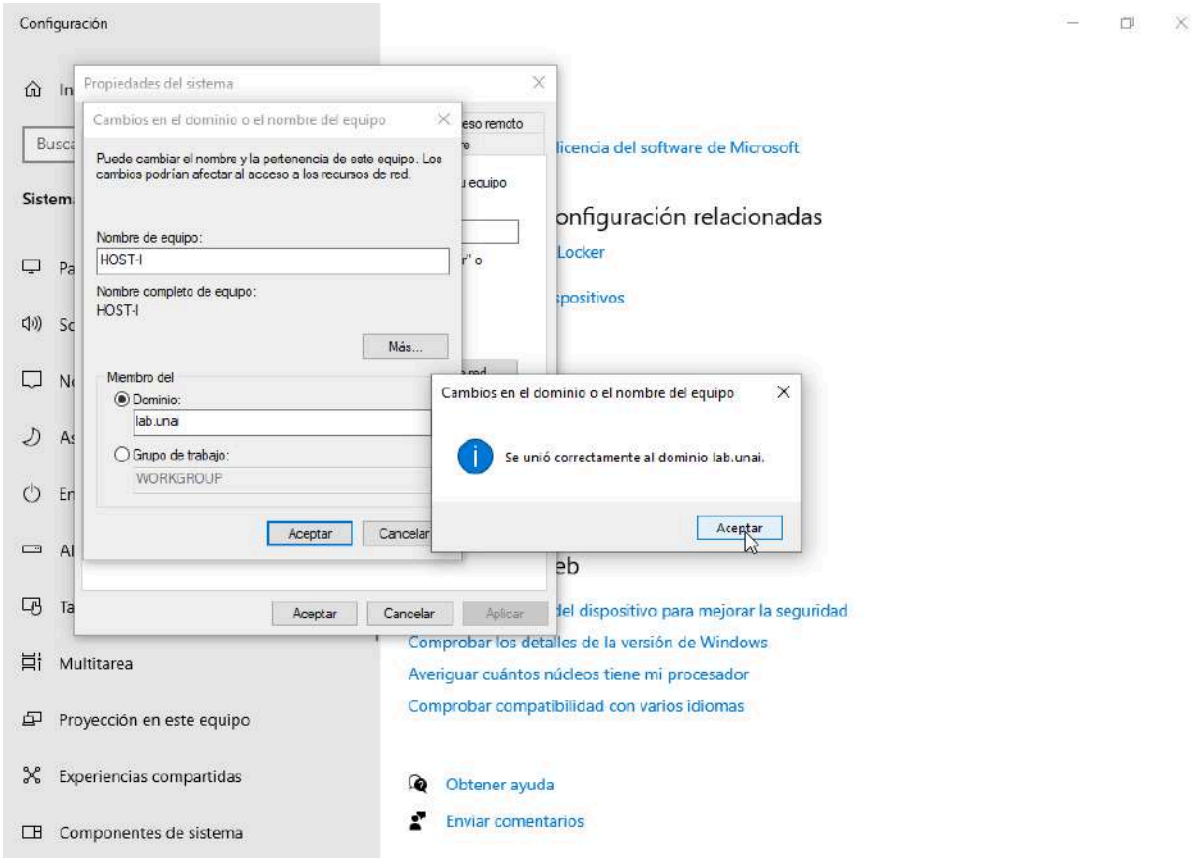
This is documented as validation of technical requirements, not as an infrastructure error.

4.15.2 Successful domain join

Process applied:

- Domain: **lab.unai**
- Credentials: **LAB\Administrator**
- Mandatory reboot after the join

Figure 4.25 – Domain join dialog showing lab.unai

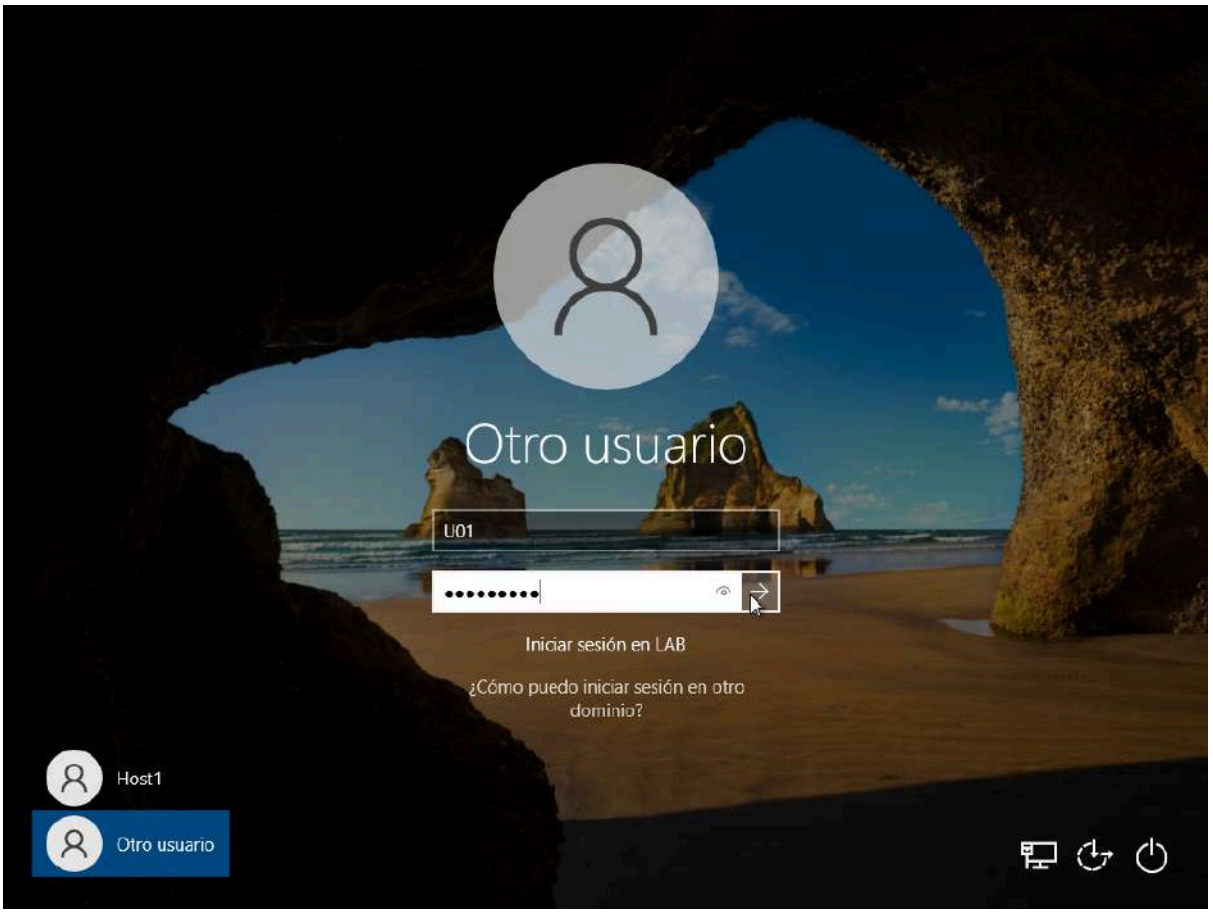


4.16 First Domain Login

4.16.1 Domain login

- Login performed using a domain account
- User profile created locally on the client

Figure 4.26 – Login screen showing “Other user” and domain available



4.16.2 Post-join validations

Validations performed:

- User authenticated against the domain
- DNS continues pointing to DC
- Internal and external resolution functional

Figure 4.27 – `whoami` confirming domain user

```
C:\Users\U01>whoami
lab\u01
```

Figure 4.28 – `ipconfig /all` with correct DNS

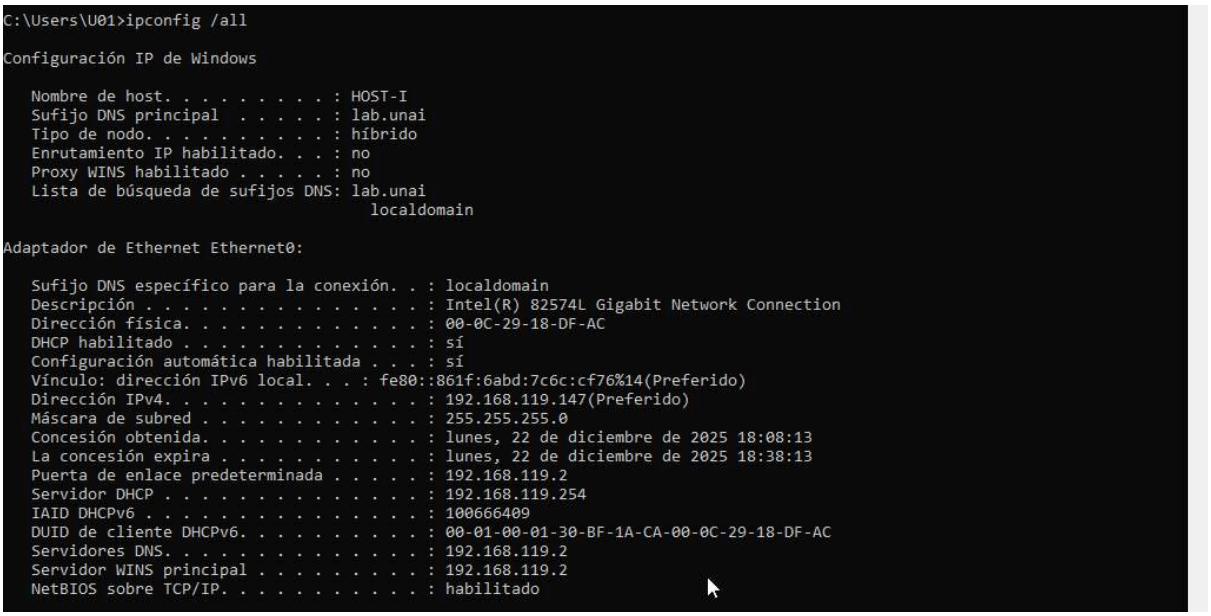


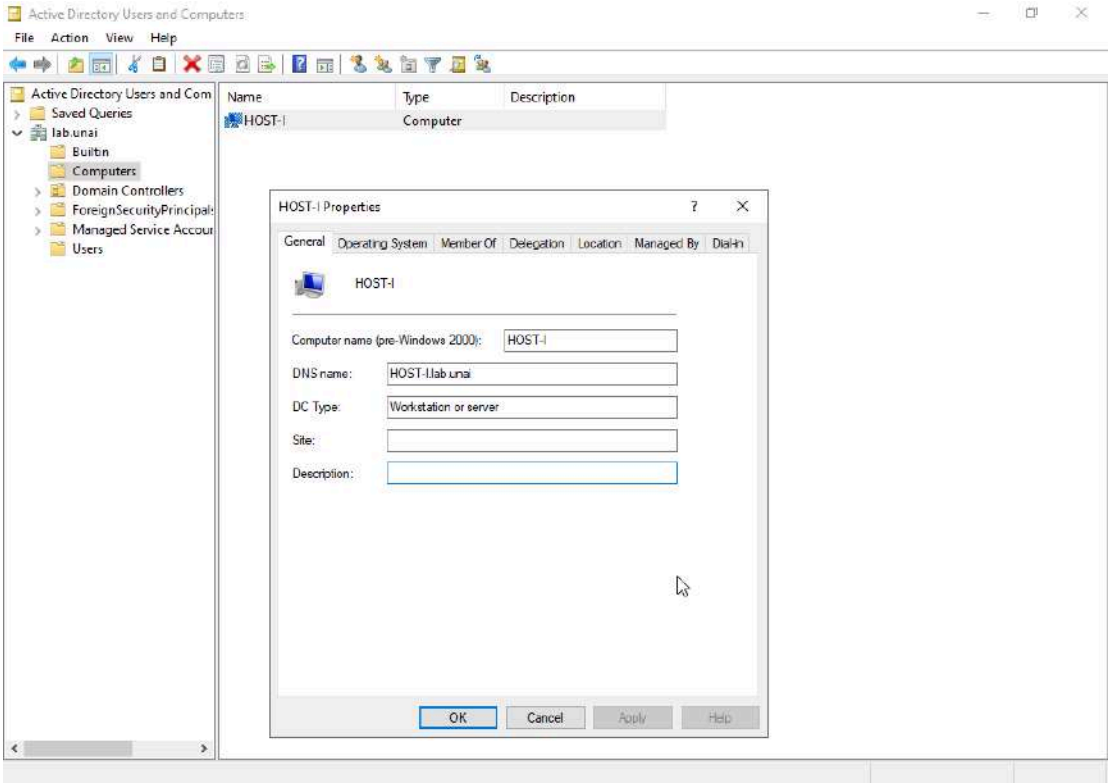
Figure 4.29 – `nslookup` resolving the Domain Controller

4.17 Final Verifications from the Domain Controller

4.17.1 Active Directory

- HOST1 appears in the **Computers** container
- Object is functional and manageable

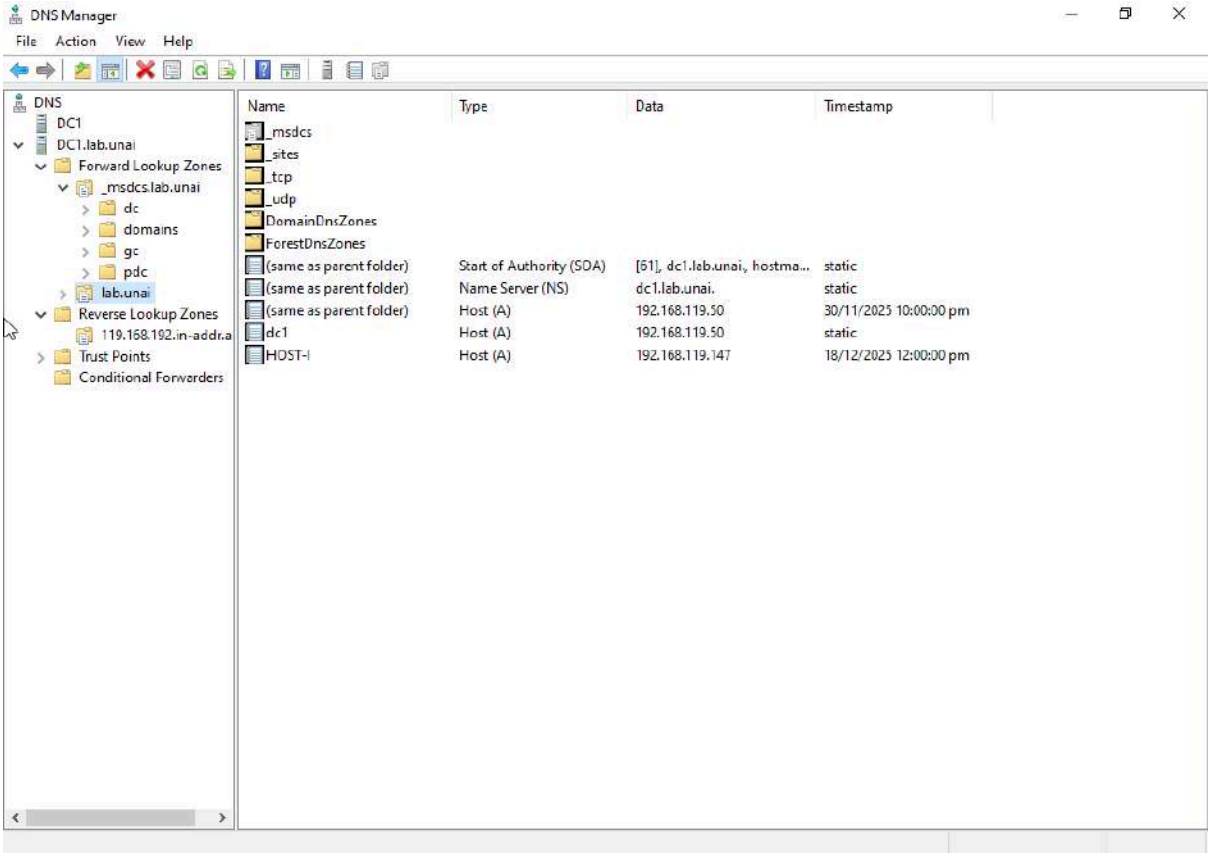
Figure 4.30 – ADUC showing HOST1 joined to the domain



4.17.2 DNS

- Client A record automatically created
- Forward resolution functional

Figure 4.31 – DNS Manager showing client A record



4.18 Final Environment State After Deployment

At the end of the deployment:

- Domain Controller fully operational
- Active Directory functional
- Internal DNS validated
- DHCP assigning correctly
- Client joined and authenticating
- Kerberos functioning

The environment is now ready for the operational execution blocks.

5. Operational Execution Blocks

5.1 Block 1 – Active Directory Administration

This block focuses on the logical organization of the domain, establishing a clear and maintainable structure of Organizational Units, users, computers, and groups, following real-world administration criteria used in corporate Windows environments.

5.1.1 Block objective

Define and validate a baseline Active Directory structure that allows:

- Proper organization of users, computers, and groups
- Easy application of Group Policies later on
- Guaranteed scalability and maintainability of the domain
- Clear separation of administrative roles and objects

5.1.2 Creation of the Organizational Unit (OU) structure

Actions performed

The following OU structure was created under the **lab.unai** domain:

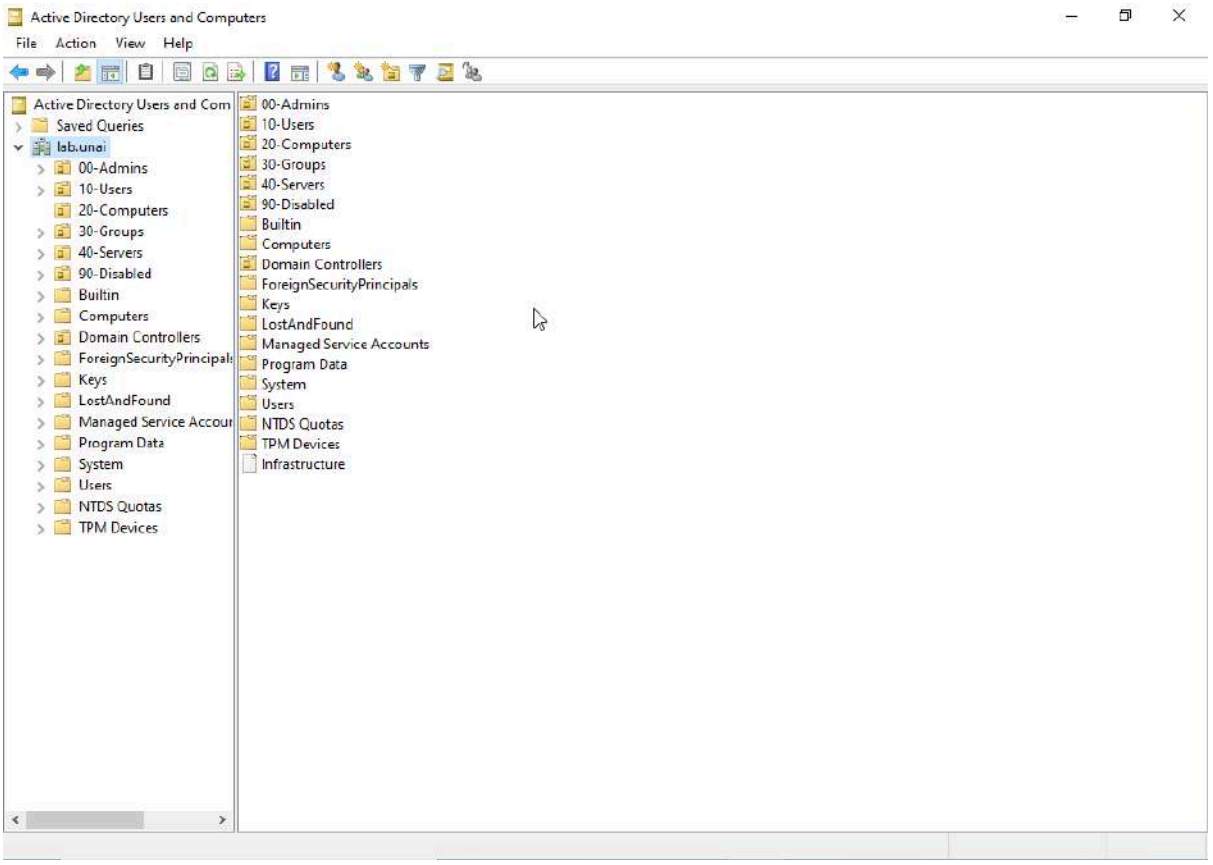
- 00-Admins
- 10-Users
- 20-Computers
- 30-Groups
- 40-Servers
- 90-Disabled

Criteria applied

- Numeric prefixes to enforce logical ordering
- Functional separation between identities, computers, and groups
- Dedicated OU for leavers (**90-Disabled**) with an operational focus

Evidence

Figure 5.1.1 – Active Directory Users and Computers view showing the full OU structure under lab.unai.



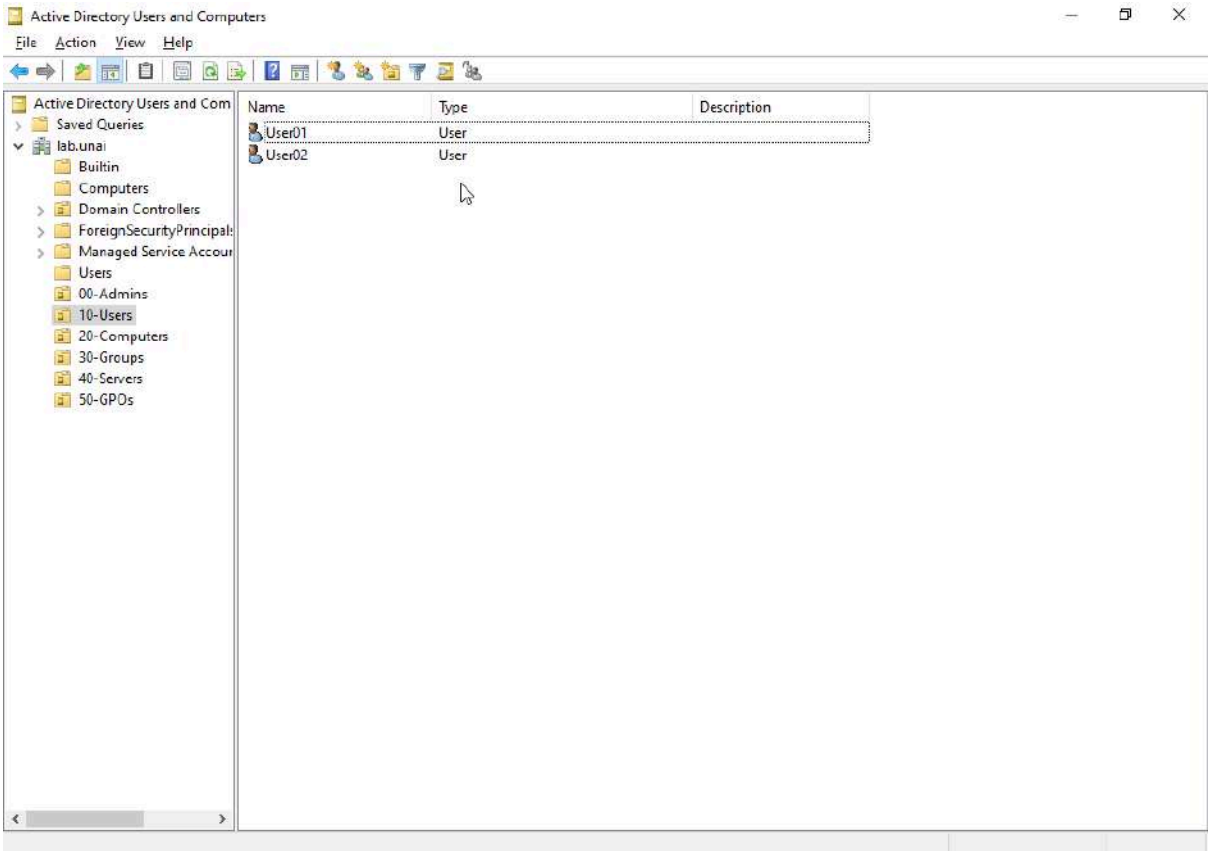
5.1.3 Creation and management of domain users

Actions performed

- Creation of domain user accounts
- Initial placement in the **10-Users** OU
- Verification of enabled status and basic attributes

Evidence

Figure 5.1.2 – ADUC showing the created users inside the 10-Users OU.



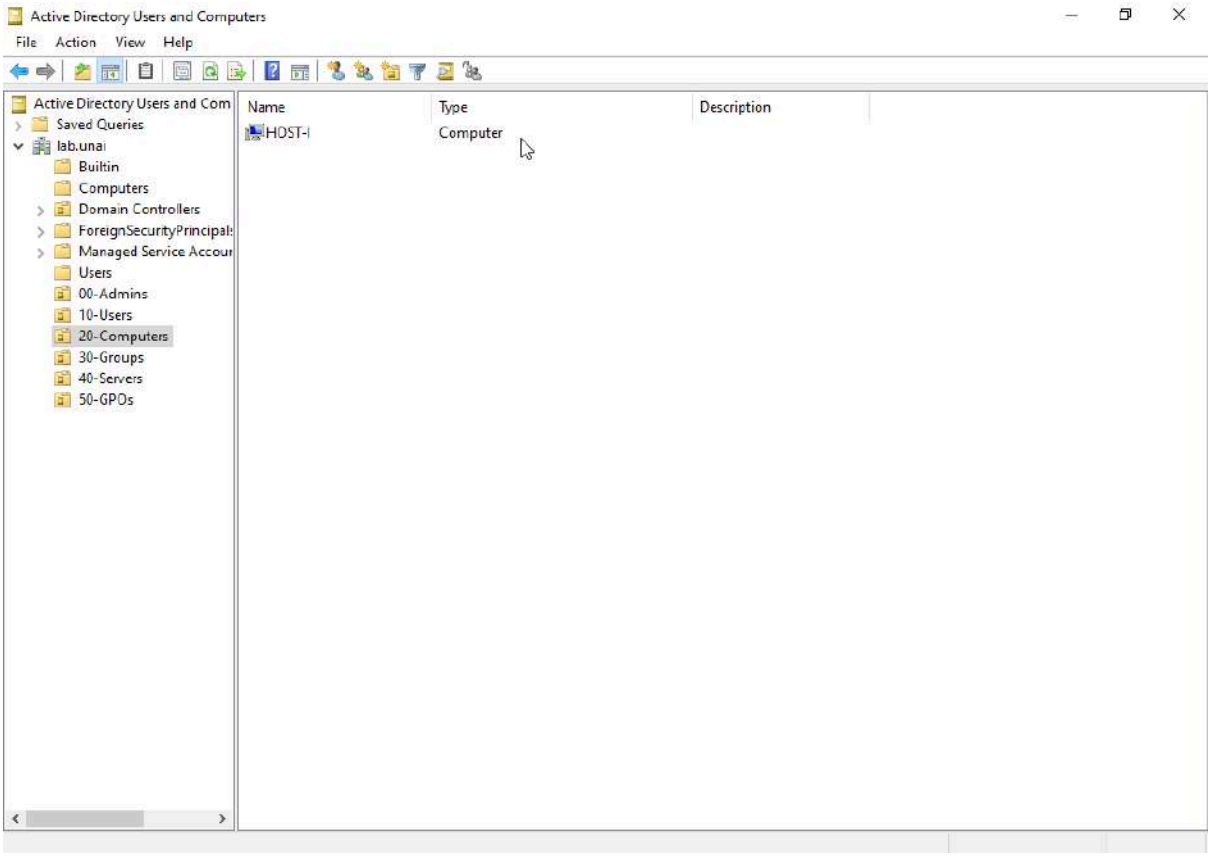
5.1.4 Computer organization in Active Directory

Actions performed

- Verification that the **HOST1** object was created automatically after joining the domain
- Movement of the computer from the default **Computers** container to the **20-Computers** OU

Evidence

Figure 5.1.3 – ADUC showing HOST1 located in the 20-Computers OU.



5.1.5 Creation of security groups

Actions performed

The following security groups were created in the **30-Groups** OU:

- **grp-share-ro**
    - No members
- **grp-share-rw**
    - No members
- **grp-office**
    - No members
- **grp-it-admins**

    - No members

- **grp-finances**
    - No members

Observations

- Creating groups with no initial members is intentional.
- These groups will be used in later blocks for:
    - NTFS permissions
    - Access control to shared resources
    - Group-based GPO targeting

Evidence

Figure 5.1.4 – ADUC showing grp-share-ro and grp-share-rw created under 30-Groups.

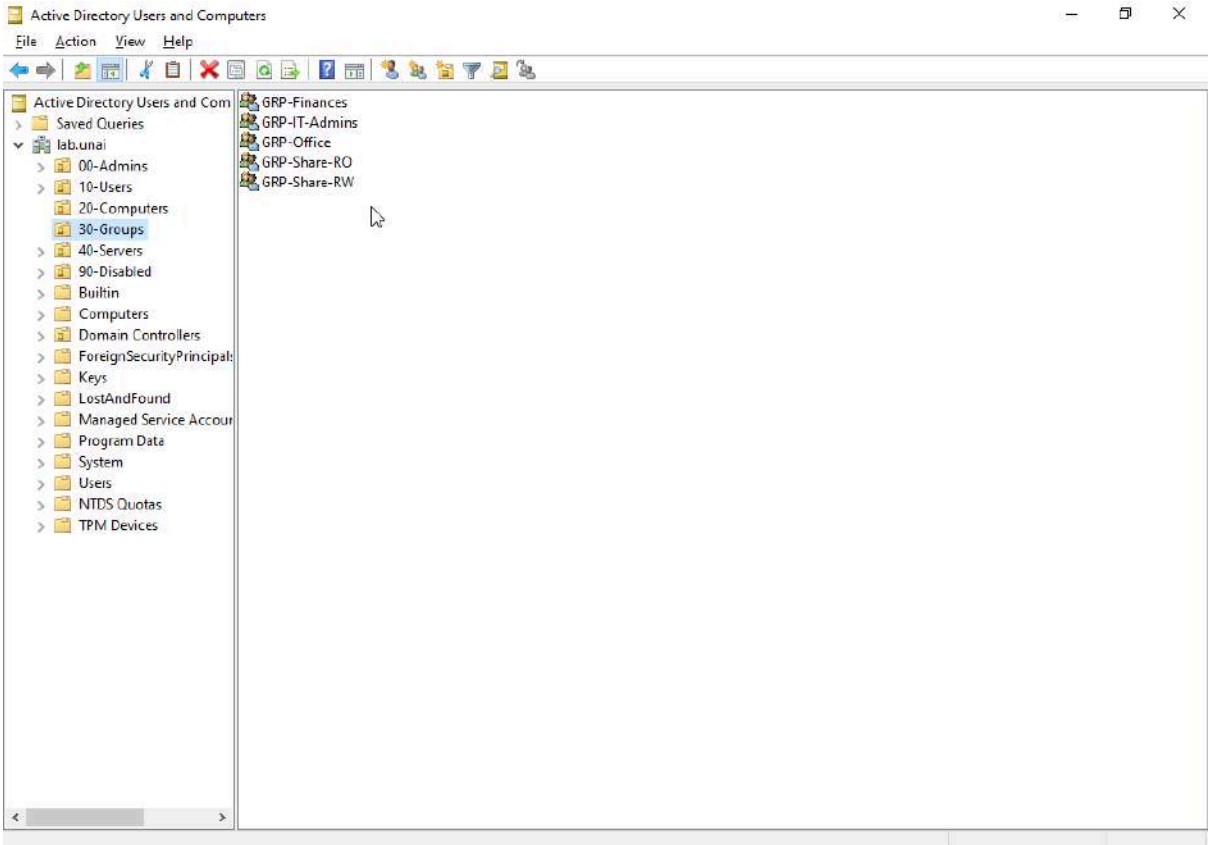
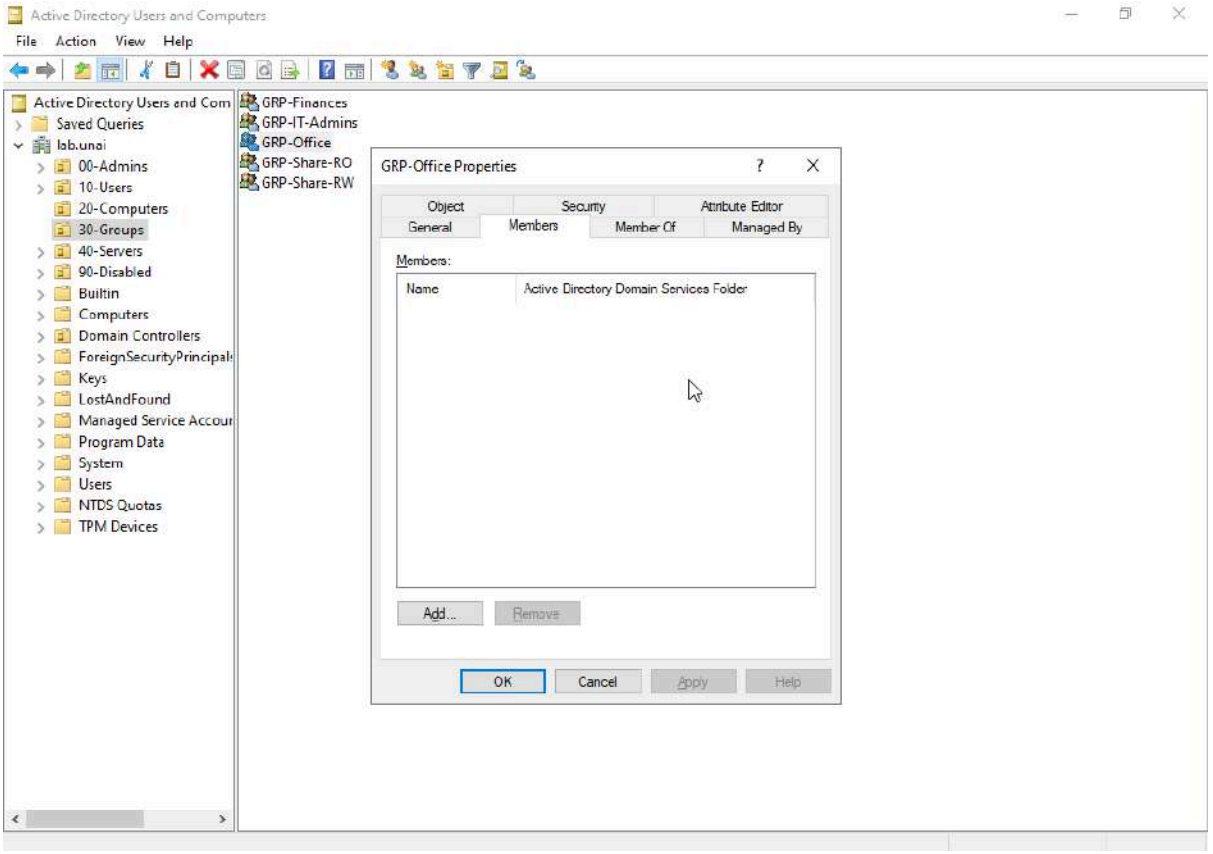


Figure 5.1.5 – Group properties showing membership configuration (empty).



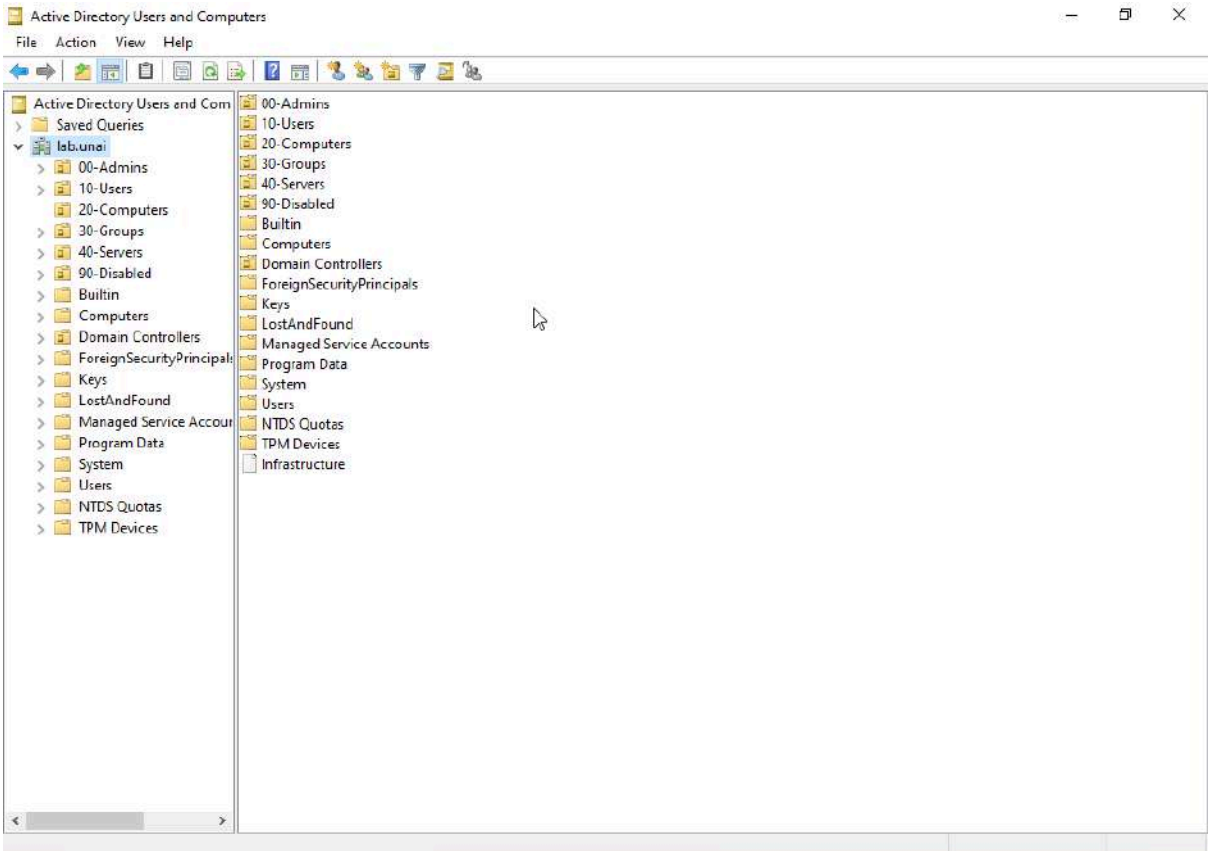
5.1.6 Validations performed

Using **Active Directory Users and Computers**, the following were verified:

- OU structure coherent and complete
- Users placed in the correct OU
- Computer **HOST1** present and manageable
- Groups visible and correctly named
- Overall domain consistency

Evidence

Figure 5.1.6 – General ADUC view confirming the final domain structure.



5.1.7 Block status

- The logical Active Directory structure is fully defined.
- Users and computers are correctly organized.
- Security groups are prepared for operational use.

The domain is now ready for:

- Group Policy application
- NTFS permission assignments
- More advanced administrative scenarios

5.2 Block 2 – Group Policy Management (GPO)

5.2.1 Block objective

- Apply user and computer policies using GPOs
- Verify their correct application from the client
- Clearly differentiate between user and computer policies
- Diagnose realistic scenarios of GPOs applied, not applied, or partially applied

5.2.2 User GPO – Block Control Panel

5.2.2.1 Configuration performed

- GPO name: **GPO-Block-ControlPanel**
- Type: **User Configuration**

Configuration path:

- User Configuration
  → Administrative Templates
  → Control Panel
  → **Prohibit access to Control Panel and PC settings = Enabled**

The GPO is linked to the **10-Users** OU.

Technical decision

- Common restriction in corporate environments
- Simple and easy to validate in practice

5.2.2.2 Validation and evidence

From the client:

- `gpupdate /force`
- Log off and log on again with a domain user
- Attempt to open Control Panel

- Verification with `gpresult /r`

Result

- Control Panel access correctly blocked
- The GPO appears as **Applied** in `gpresult`

Evidence

Figure 5.2.1 – `gpresult /r` output showing GPO-Block-ControlPanel.

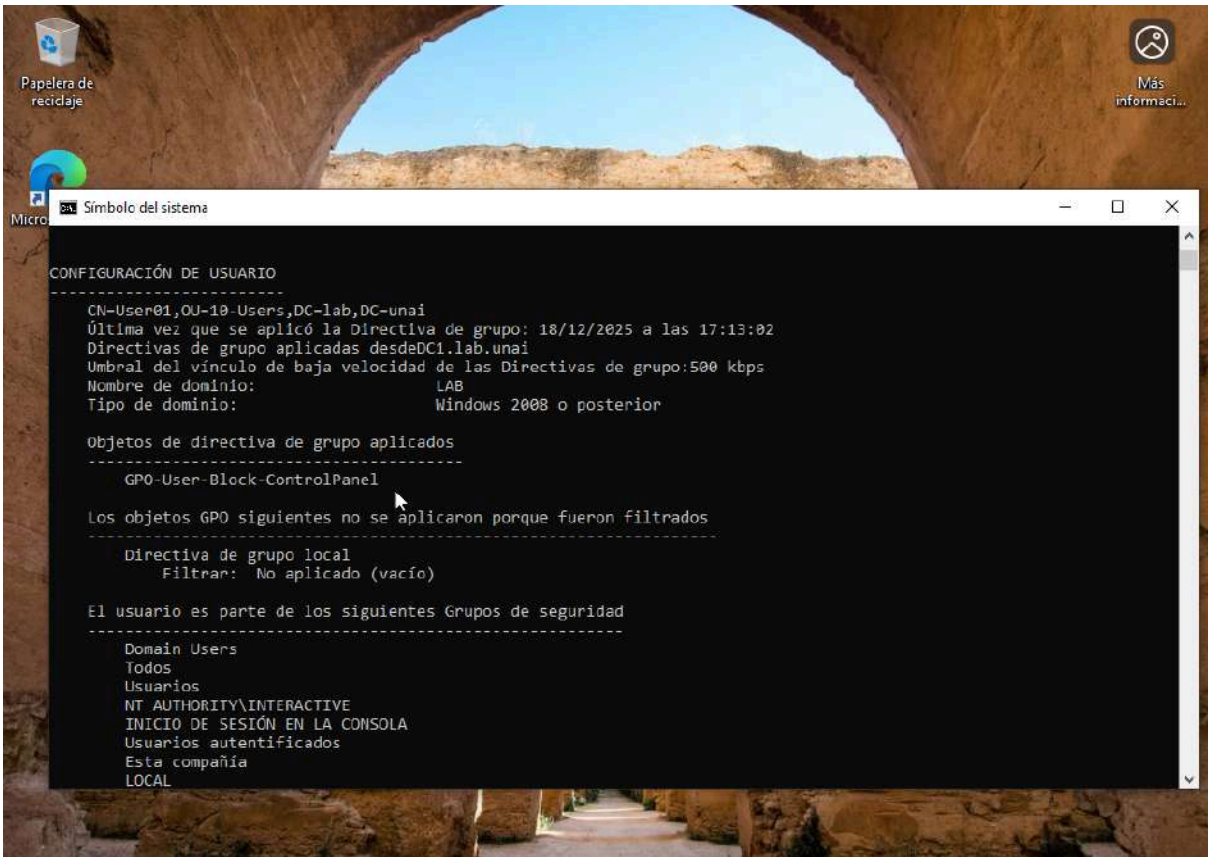
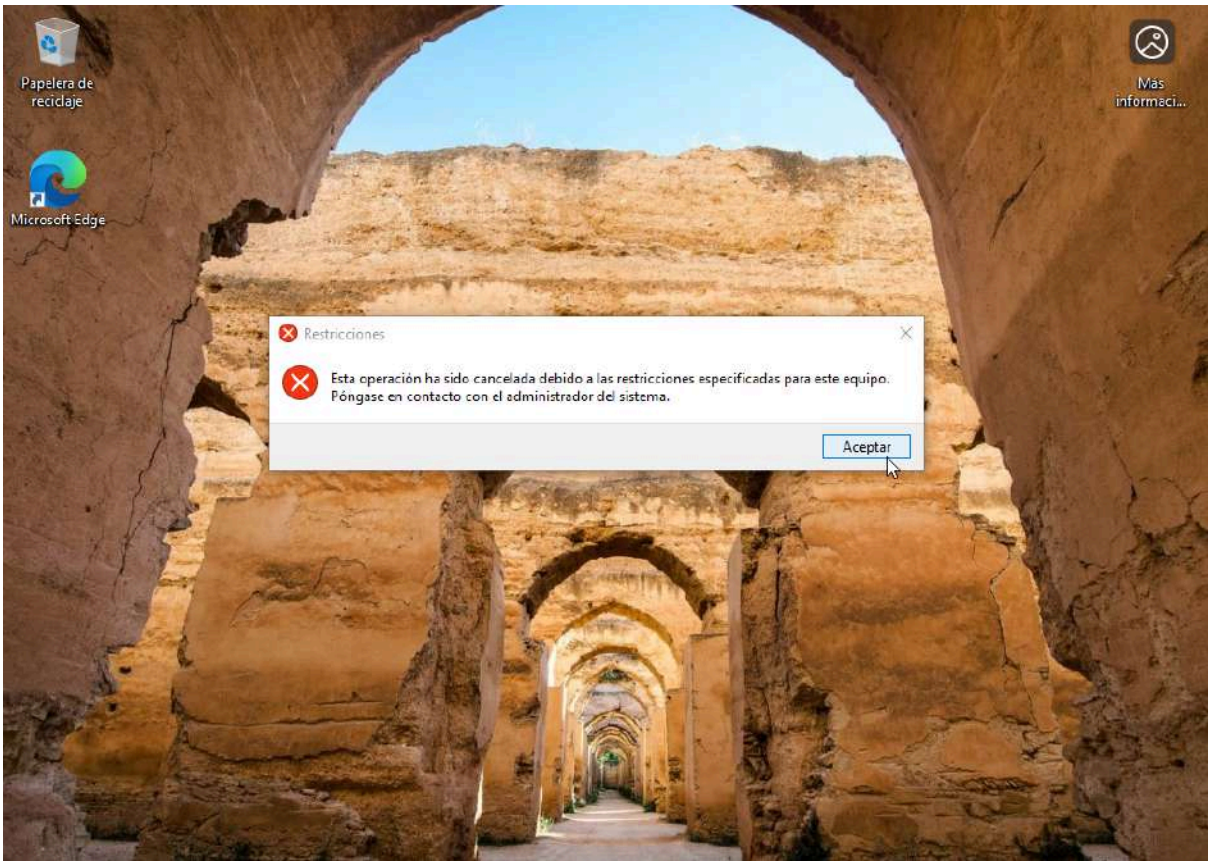


Figure 5.2.2 – Restriction message when trying to open Control Panel.



5.2.3 User GPO – Disable Command Prompt (CMD)

5.2.3.1 Configuration performed

- GPO name: **GPO-Disable-CMD**
- Type: **User Configuration**

Configuration path:

- User Configuration
  → Administrative Templates
  → System
  → **Prevent access to the command prompt = Enabled**
  → **Disable the command prompt script processing = Yes**

The GPO is linked to the **10-Users** OU.

Technical decision

- Common restriction in controlled environments
- Allows quick validation of user-scoped GPOs

5.2.3.2 Validation and evidence

From the client:

- `gpupdate /force`
- Log off and log back in
- Attempt to run `cmd.exe`
- Verification with `gpresult /r`

Result

- Command Prompt is correctly blocked
- GPO shows as applied in `gpresult`

Evidence

Figure 5.2.3 – `gpupdate /force` updating policies.

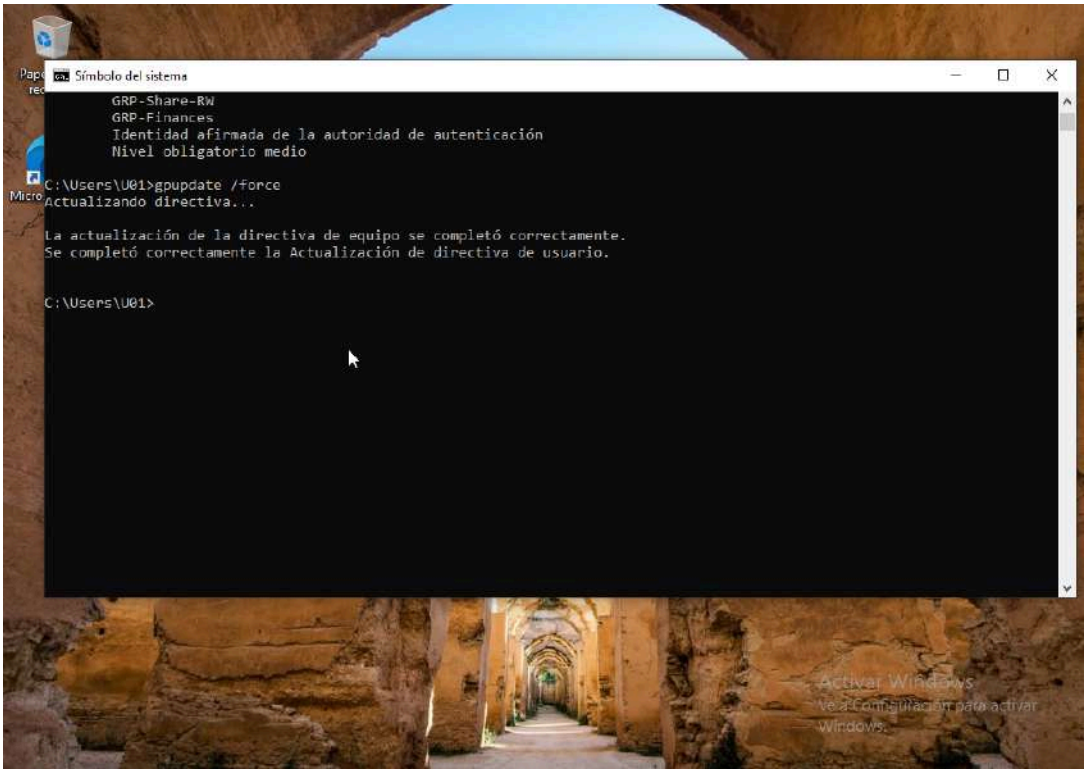
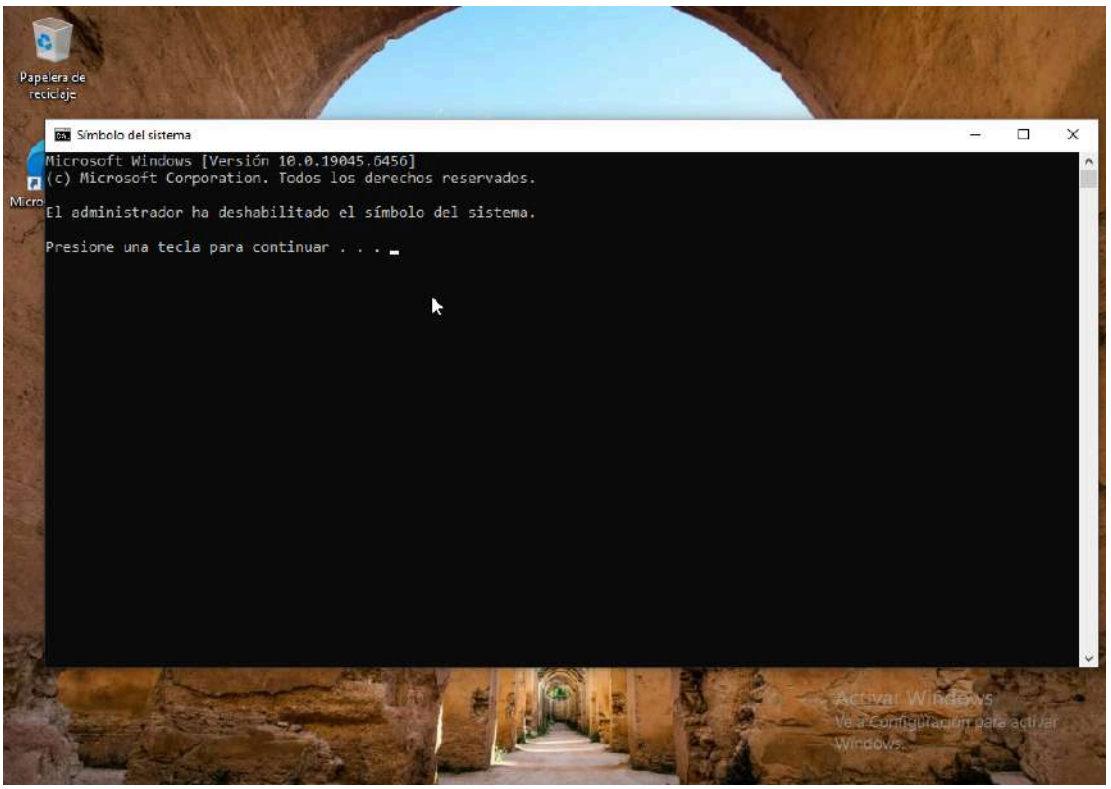


Figure 5.2.4 – Block message when launching CMD.



5.2.4 Computer GPO – Block USB devices

5.2.4.1 Configuration performed

- GPO name: **GPO-Block-USB**
- Type: **Computer Configuration**

Configuration path:

- Computer Configuration
  → Administrative Templates
  → System
  → Removable Storage Access
  → **All Removable Storage classes: Deny all access = Enabled**

The GPO is linked to the **20-Computers** OU.

Operational observation

- Initially, the policy was searched under user configuration.
- It was corrected after identifying it as a computer-scoped policy.

5.2.4.2 Validation and evidence

From the client:

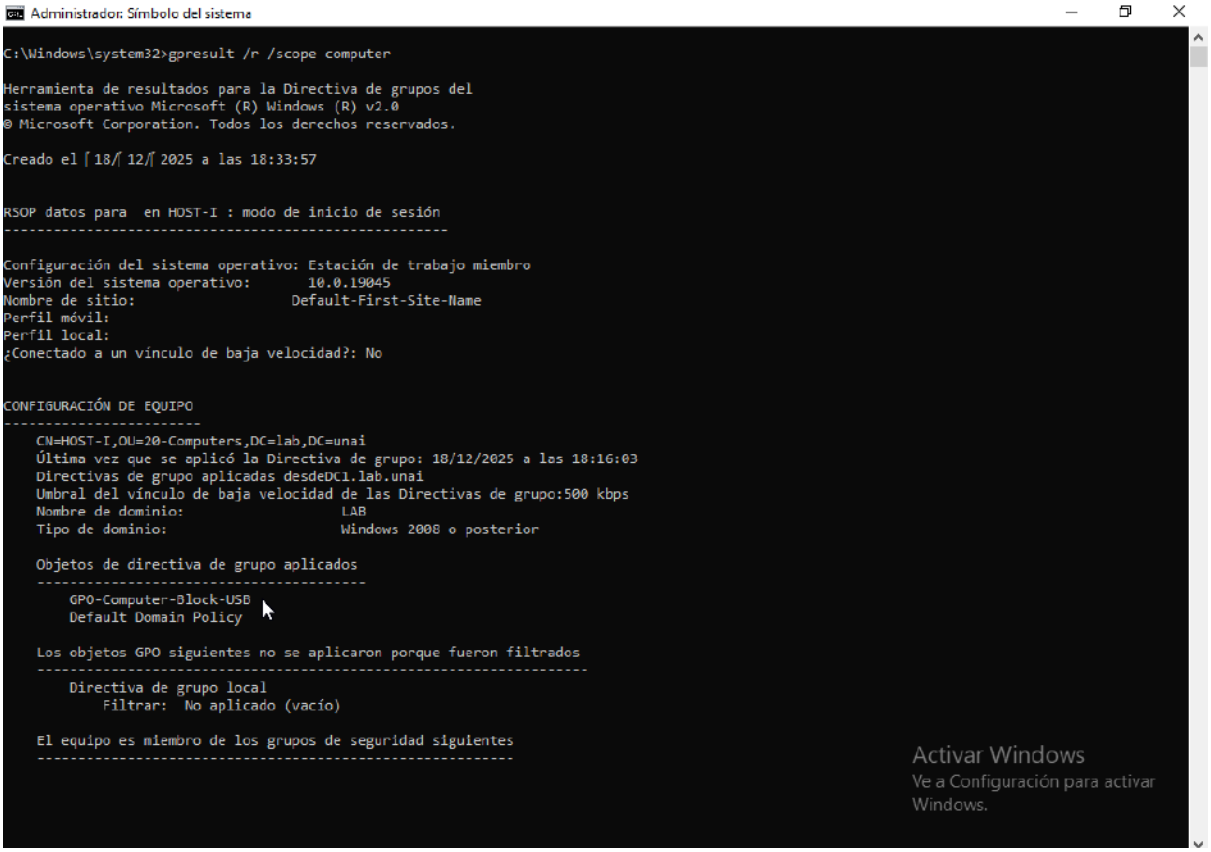
- `gpupdate /force`
- System reboot
- Verification with `gpresult /r /scope computer`

Result

- The GPO appears applied at computer level
- Policy is effective after reboot

Evidence

Figure 5.2.5 – `gpresult /r` showing GPO-Block-USB under Computer Configuration.



5.2.5 User GPO – Corporate wallpaper

5.2.5.1 Configuration performed

- GPO name: **GPO-Wallpaper**
- Type: **User Configuration**

Configuration path:

- User Configuration
  → Administrative Templates
  → Desktop
  → Desktop Wallpaper

Applied configuration:

- UNC path accessible from the client

- Tests performed with PNG and JPG images
- GPO linked to **10-Users** OU

5.2.5.2 Observed result and validation

From the client:

- `gpupdate /force`
- Logoff and reboots
- Logon with a domain user
- Verification with `gpresult /r`

Observed result

- The desktop background changes from the original one
- A solid black background is displayed
- The GPO appears as **Applied**

Technical conclusion

- The GPO itself is applied correctly
- The issue is visual/rendering-related
- It is not caused by DNS, permissions, link, or scope problems

Evidence

Figure 5.2.6 – `gpresult /r` showing GPO-Wallpaper.

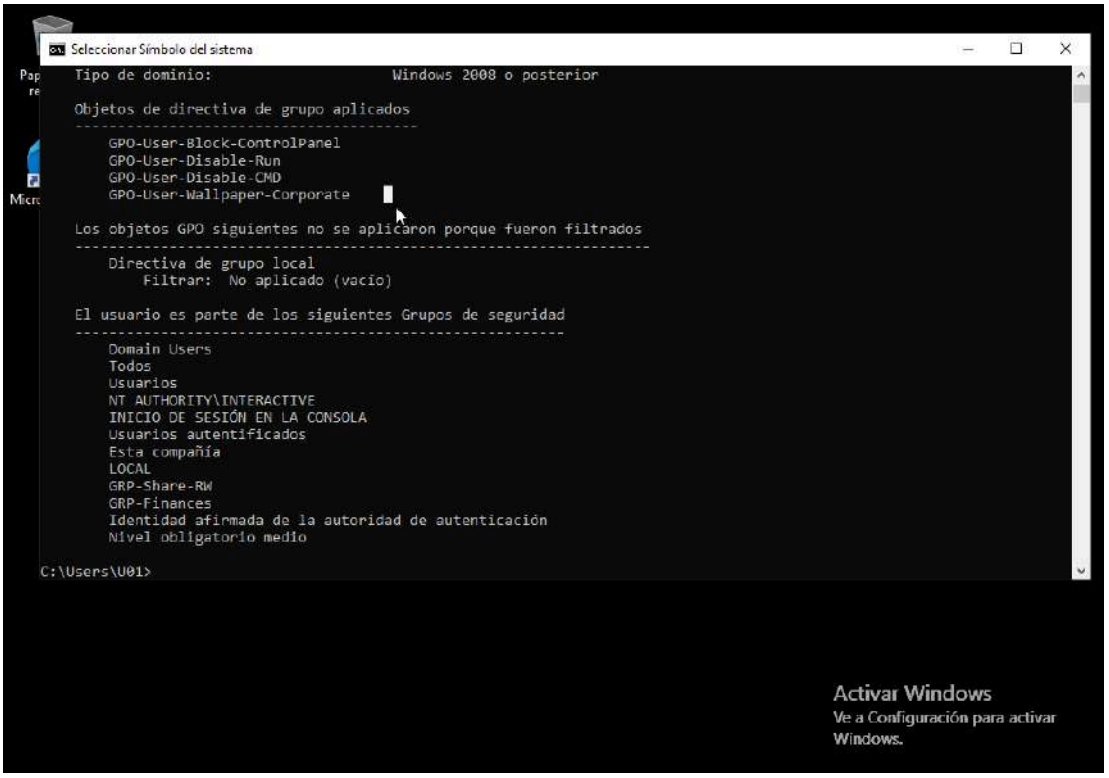
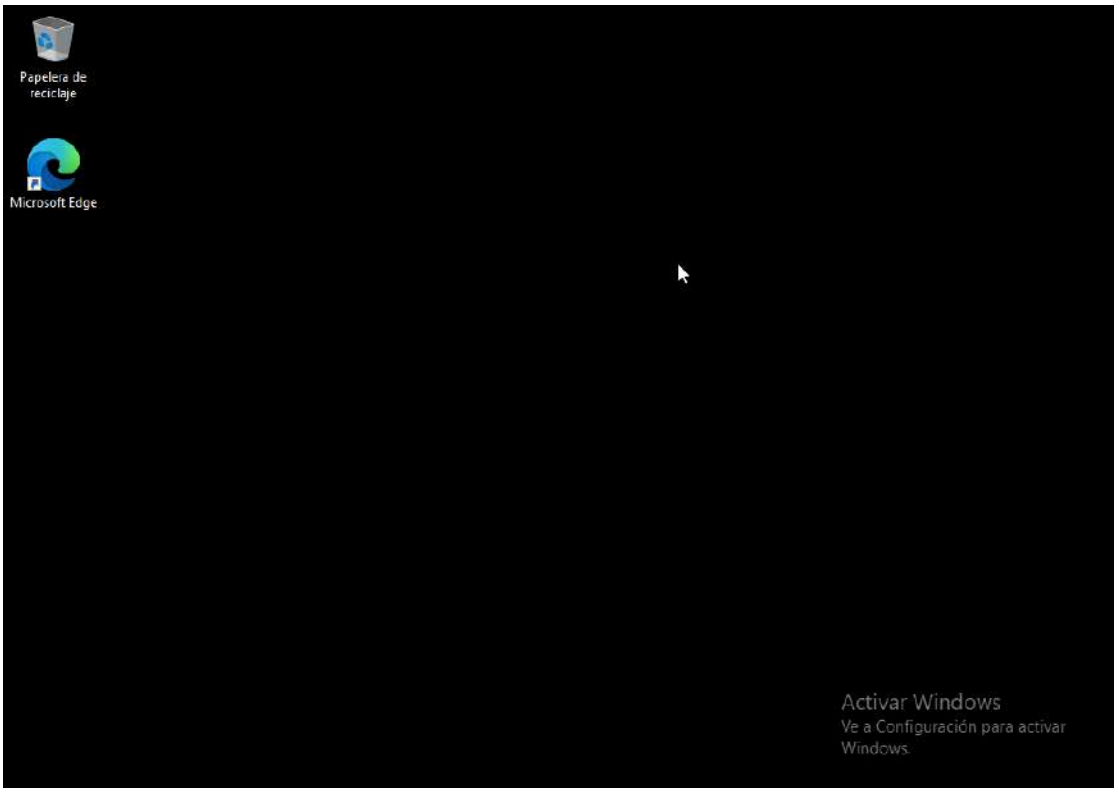


Figure 5.2.7 – Black background applied on the client.



5.2.6 Password policy – Default Domain Policy

5.2.6.1 Configuration performed

Applied through Default Domain Policy:

- Computer Configuration
  → Windows Settings
  → Security Settings
  → Account Policies
  → Password Policy

Configured values:

- Minimum password length: 8
- Password must meet complexity requirements: Enabled

5.2.6.2 Real validation

From the client:

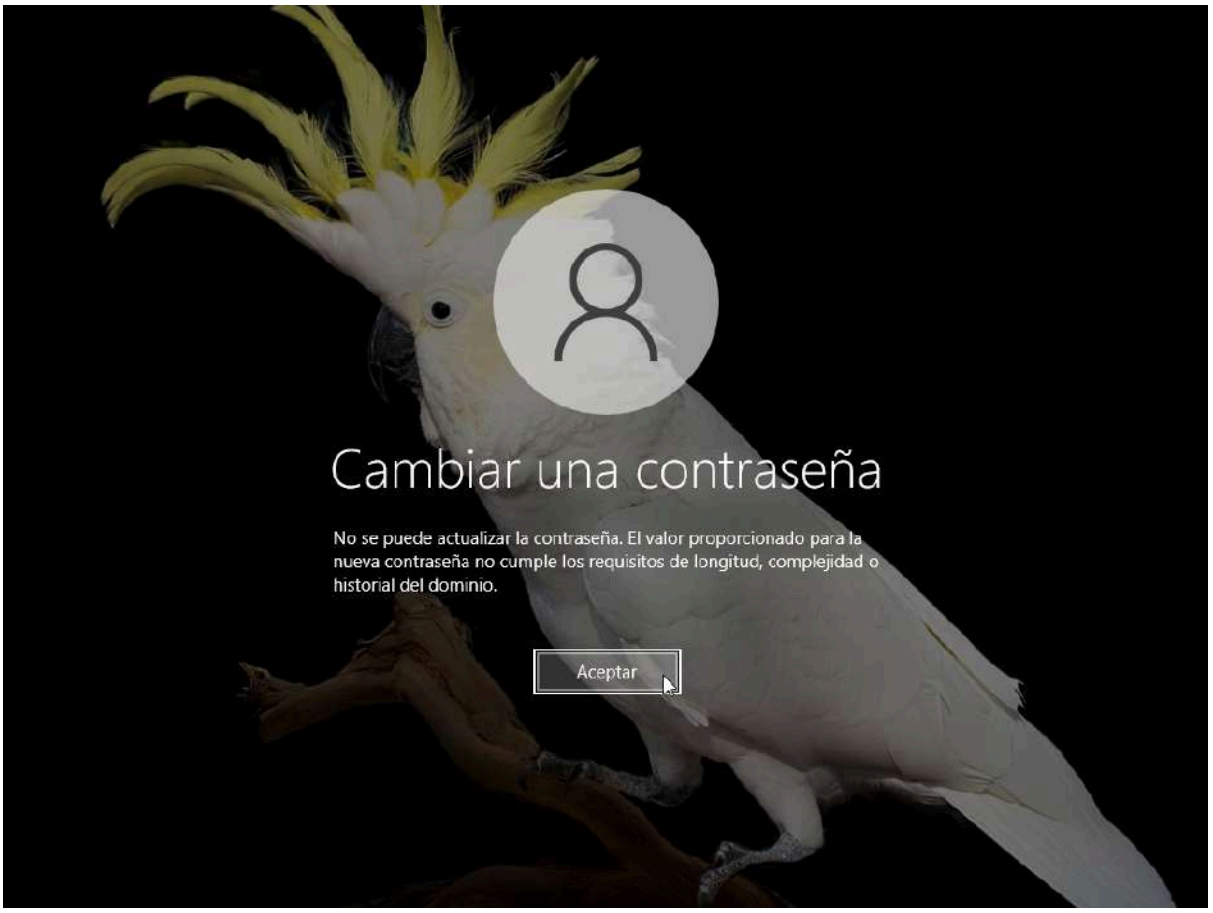
- `gpupdate /force`
- Attempt to change password using fewer than 8 characters

Result

- Password change rejected
- Error message indicating non-compliance with policy

Evidence

Figure 5.2.8 – Error message when attempting to set an invalid password.



5.2.7 GPO – Network drive mapping by group

5.2.7.1 Configuration performed

- GPO name: **GPO-Map-NetworkDrive-FIN**
- Type: **User Configuration → Preferences**

Configuration:

- Location: `\\DC1\FIN`
- Drive Letter: **F:**
- Label: **FIN**
- Reconnect: **Enabled**

- Group targeting: **GRP-Finances**

5.2.7.2 Validation

User member of the group:

- GPO applied
- Drive **F:** visible

User not in the group:

- GPO not applied
- Drive not mapped

Evidence

Figure 5.2.9 – Policy configuration in the GPO editor.

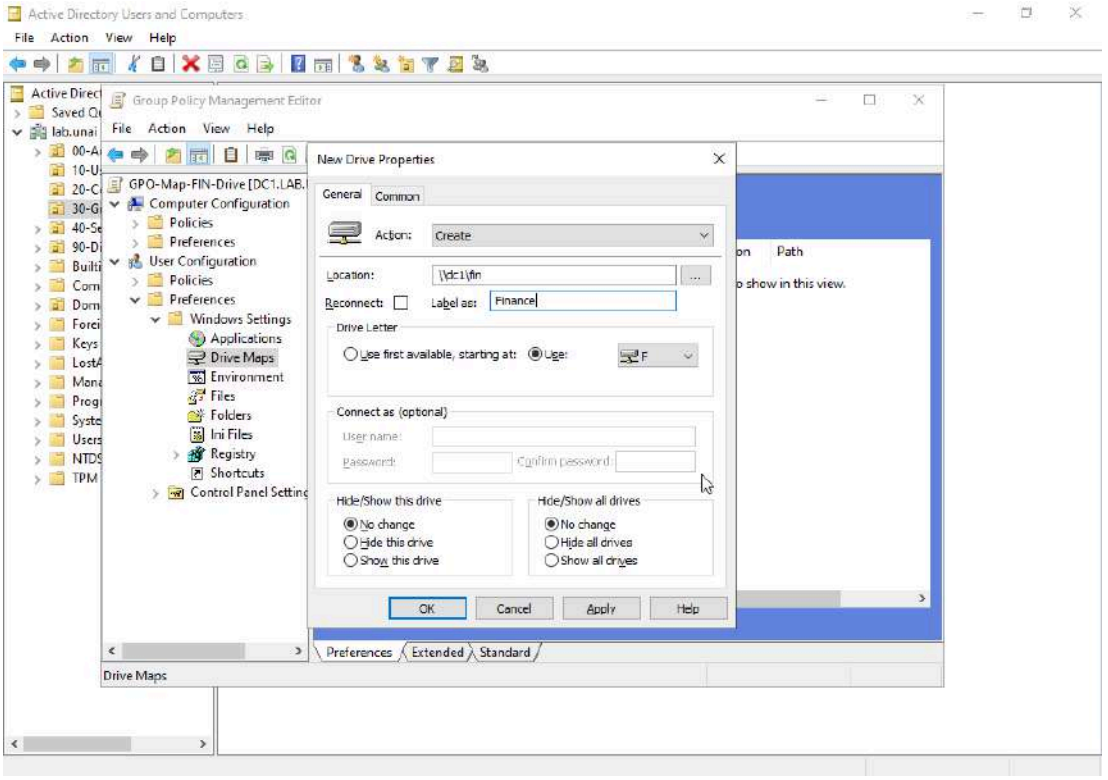


Figure 5.2.10 – GPO Targeting Editor pointing to the Finance group.

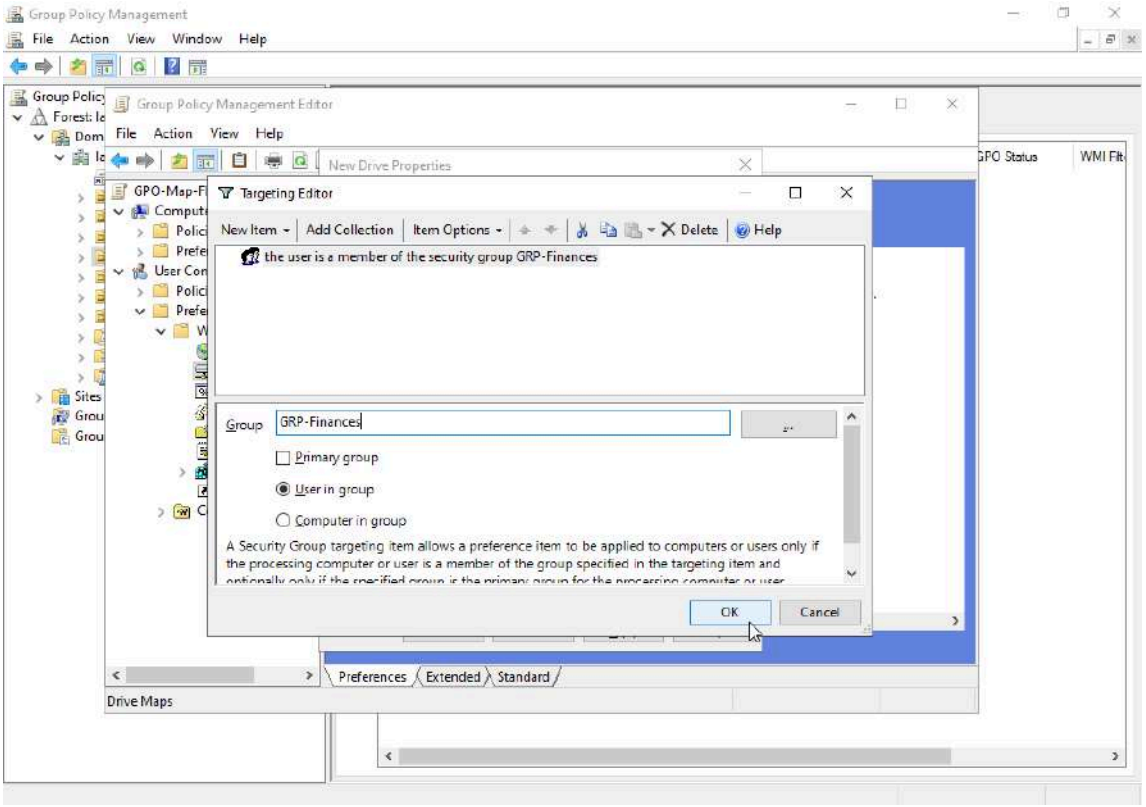


Figure 5.2.11 – F: drive mapped after GPO application for an authorized user.

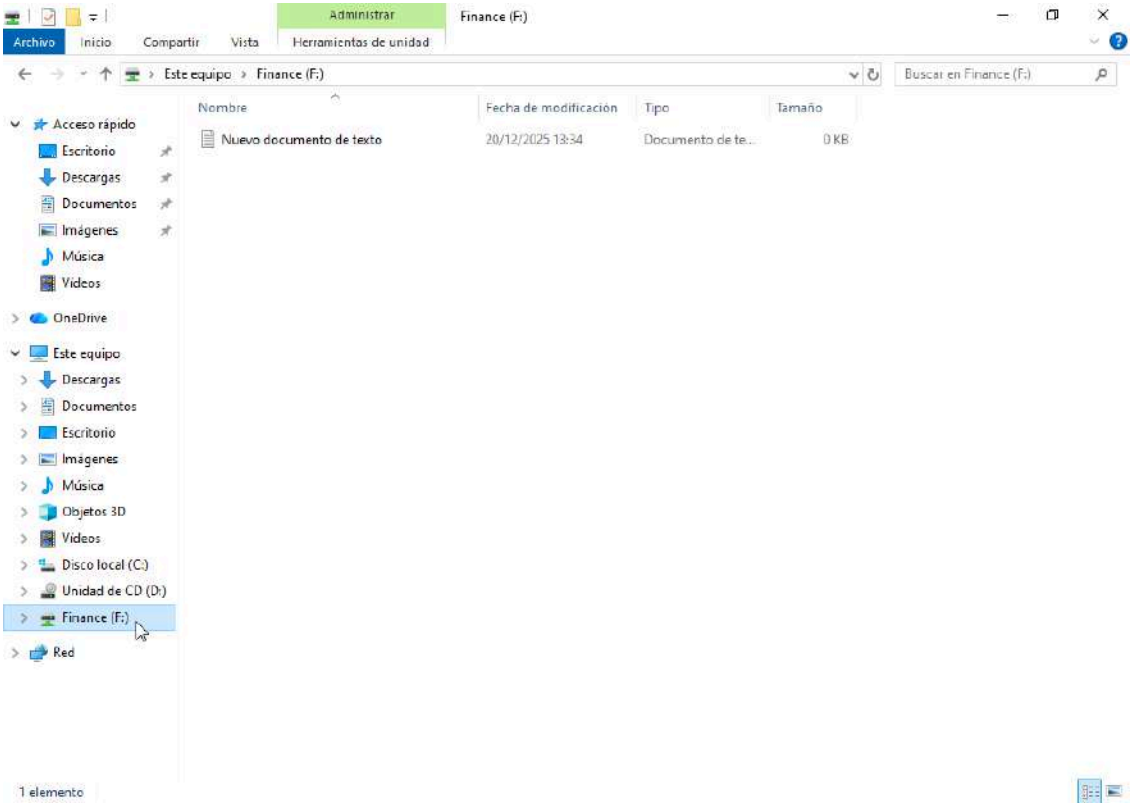
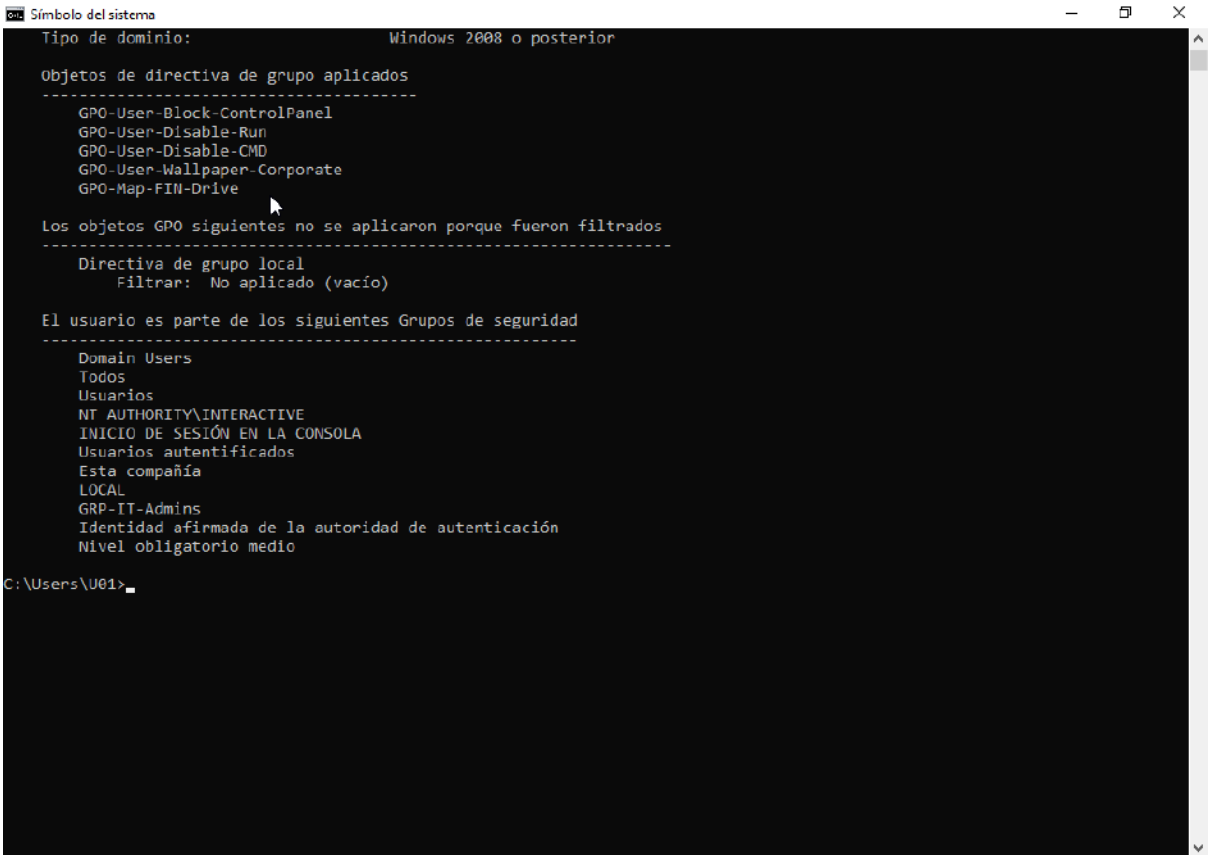


Figure 5.2.12 – `gpresult /r` showing the GPO applied for User01.



5.2.8 Intentional GPO troubleshooting (Security Filtering)

5.2.8.1 Scenario created

- User1 removed from **GRP-Finances**
- User remains in the correct OU
- `gpupdate /force` executed

5.2.8.2 Diagnosis and resolution

- GPO correctly created and linked
- Group filtering prevents application
- User added back into the group
- New logon and validation

Result

- Network drive successfully remapped
- GPO applied after fixing group membership

Evidence

Figure 5.2.13 – `gpresult /r` showing GPO not applied.

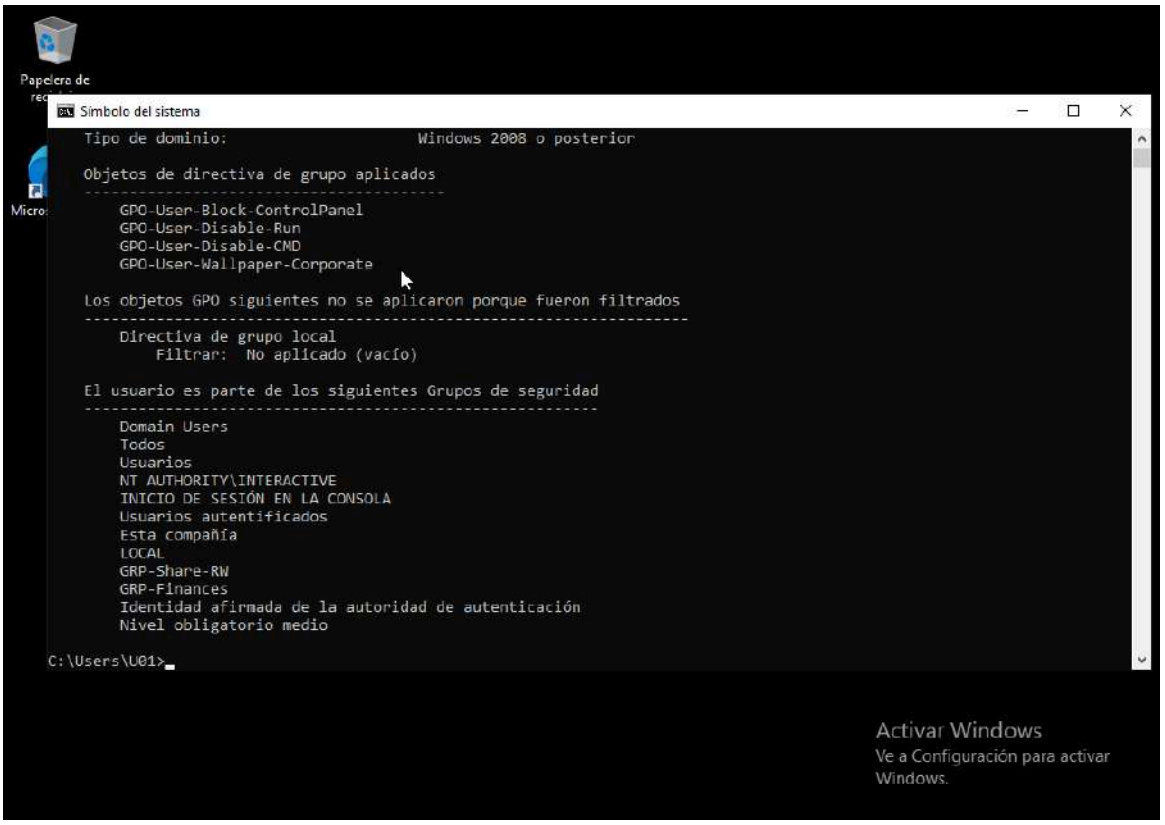
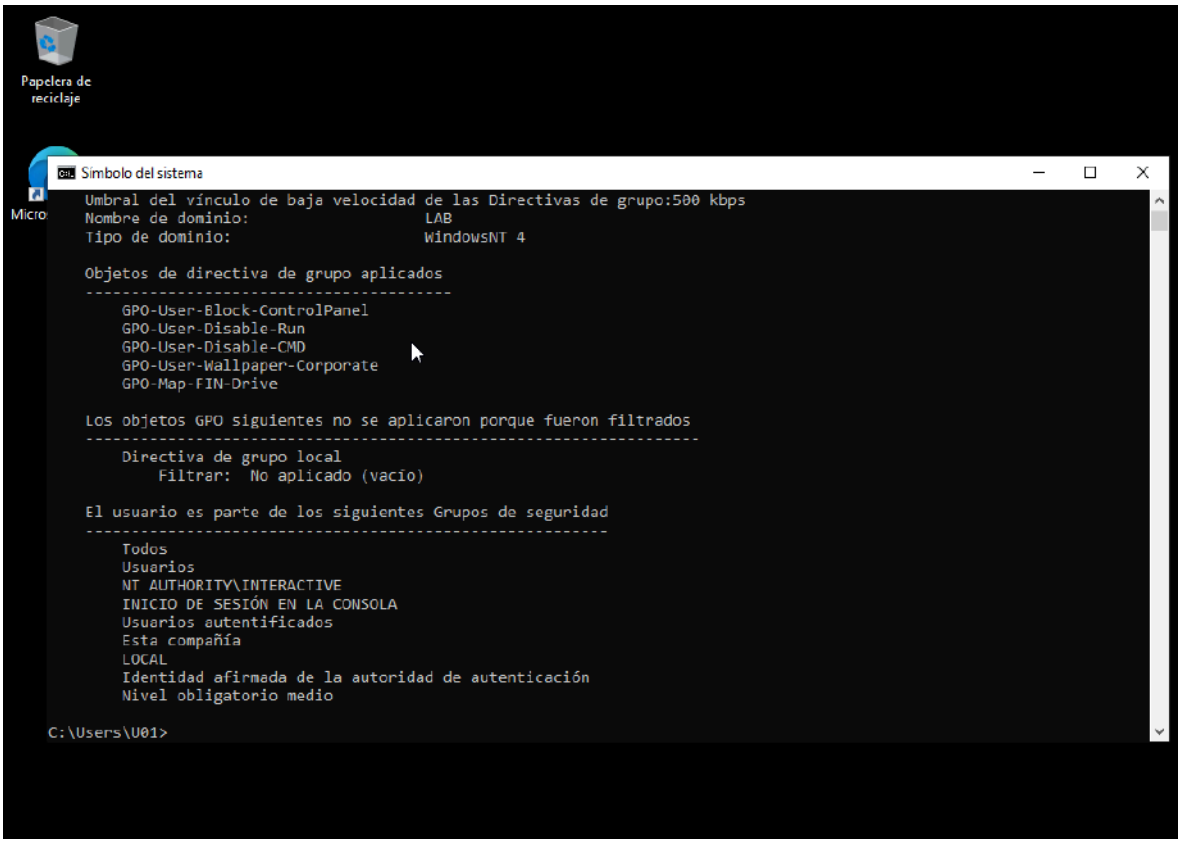


Figure 5.2.14 – GPO applied after correcting group membership.



5.2.9 Block status

- User and computer GPOs correctly applied
- Systematic validation using `gpupdate` and `gpresult`
- Imperfect/edge cases properly documented
- Troubleshooting based on method, scope, and evidence

5.3 Block 3 – File Services & Permissions

5.3.1 Block objective

- Implement a functional SMB shared resource
- Apply access control through security groups
- Correctly differentiate between Share and NTFS permissions
- Validate positive and negative access from a domain client

- Enforce the principle of least privilege

5.3.2 Design and technical decisions

5.3.2.1 Decision taken

- The **DC1** server also acts as File Server.
- This is acceptable in a lab environment to demonstrate skills.
- In production, the role would typically be separated, but that adds no extra value for this scenario.

5.3.2.2 Criteria applied

- Access management exclusively through groups
- Clear separation between:
    - Share permissions
    - NTFS permissions
- Strict application of the principle of least privilege

5.3.3 Folder structure creation

5.3.3.1 Action performed

On **DC1**, the folder was created:

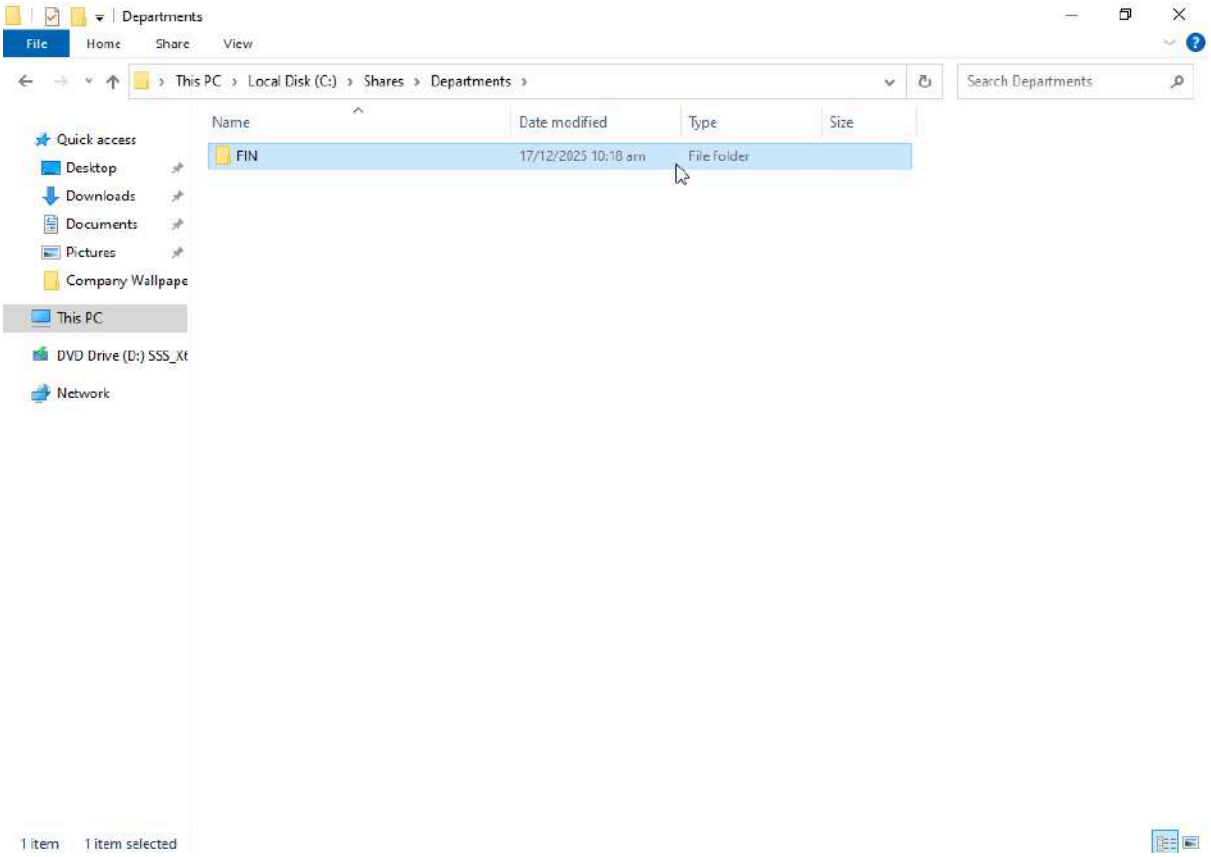
- `C:\Shares\Departments\FIN\`

5.3.3.2 Technical rationale

- Simple, controlled folder
- No complex pre-existing inheritance
- Allows defining permissions from scratch without system interference

Evidence

Figure 5.3.1 – `C:\FIN` folder created on the server file system.



5.3.4 Shared resource configuration (Share Permissions)

5.3.4.1 Folder share configuration

Path:

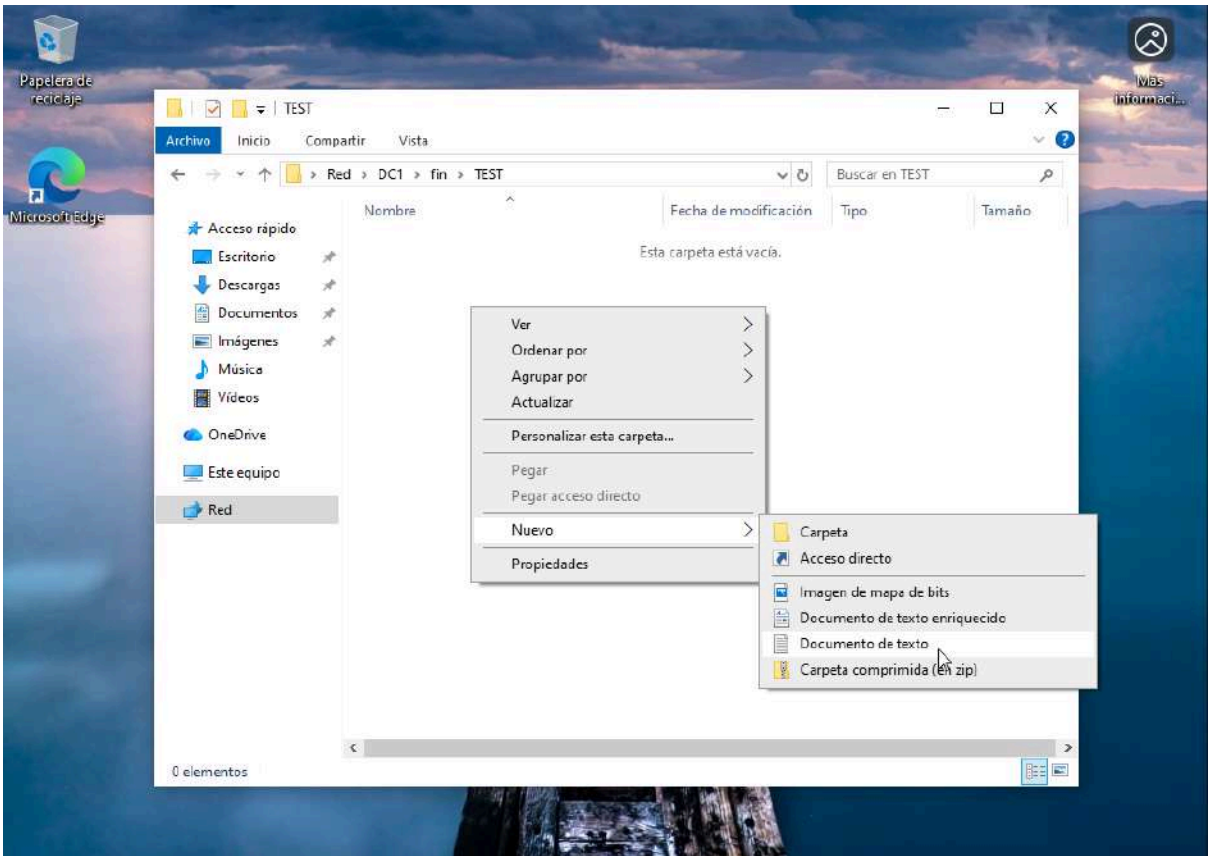
- `C:\FIN` → Properties → Sharing → Advanced Sharing

Applied configuration:

- **Share this folder:** enabled
- **Share name:** FIN

Evidence

Figure 5.3.2 – FIN share visible from the client via UNC path.



5.3.4.2 Share permissions (network level)

Configuration in **Advanced Sharing → Permissions**:

Removed:

- **Everyone**

Added:

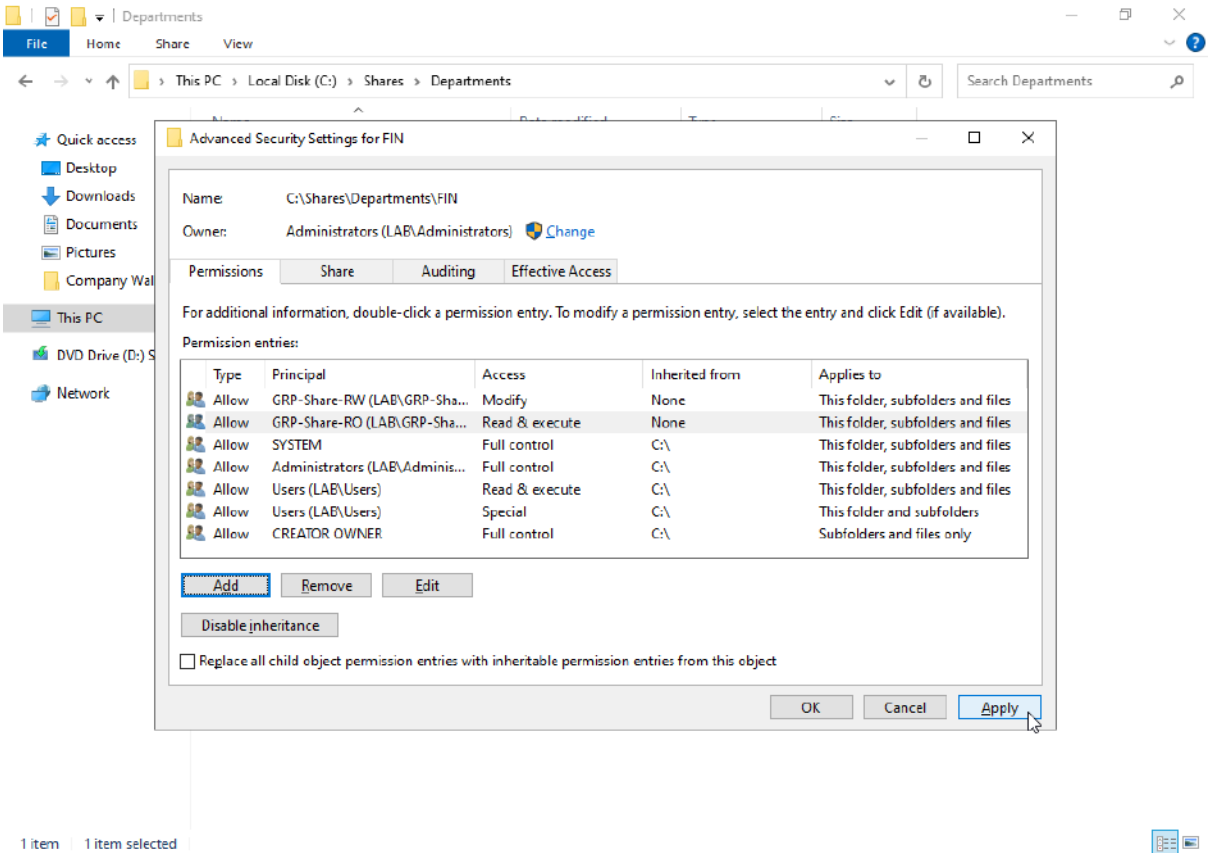
- **GRP-Share-RW → Full Control**
- **GRP-Share-RO → Read and execute**

Principle applied

- Share permissions relatively open
- Fine-grained control delegated to NTFS

Evidence

Figure 5.3.3 – Share permissions list showing only the defined groups.



5.3.5 NTFS permission configuration (disk level)

5.3.5.1 Inheritance management

Path:

- `C:\FIN` → Properties → Security → Advanced

Actions:

- Disable inheritance
- Convert inherited permissions into explicit entries

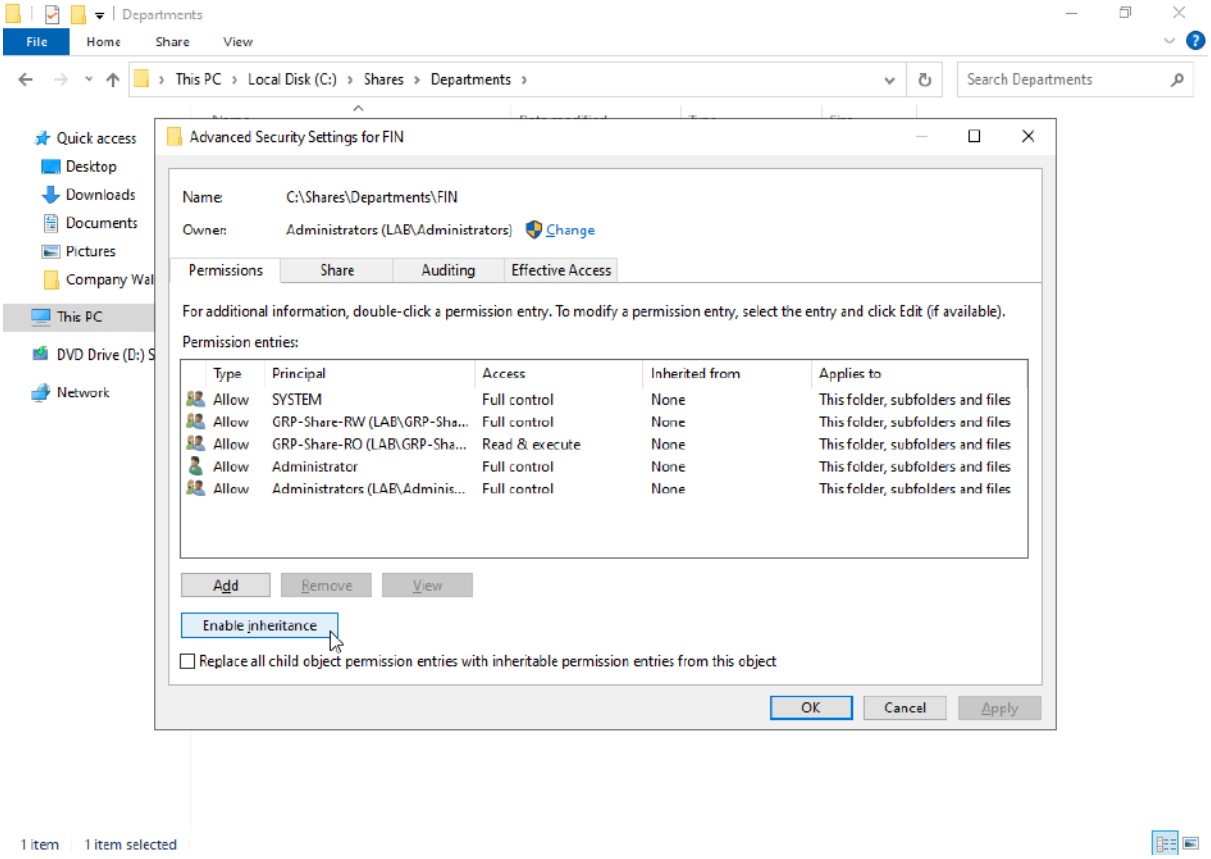
Technical reason

- Avoid uncontrolled implicit permissions

- Guarantee full traceability of access

Evidence

Figure 5.3.4 – NTFS inheritance disabled on the folder.



5.3.5.2 Final NTFS permissions

Explicitly defined permissions:

- **Administrators → Full Control**
- **SYSTEM → Full Control**
- **GRP-Share-RW → Modify**
- **GRP-Share-RO → Read & Execute**

There are no:

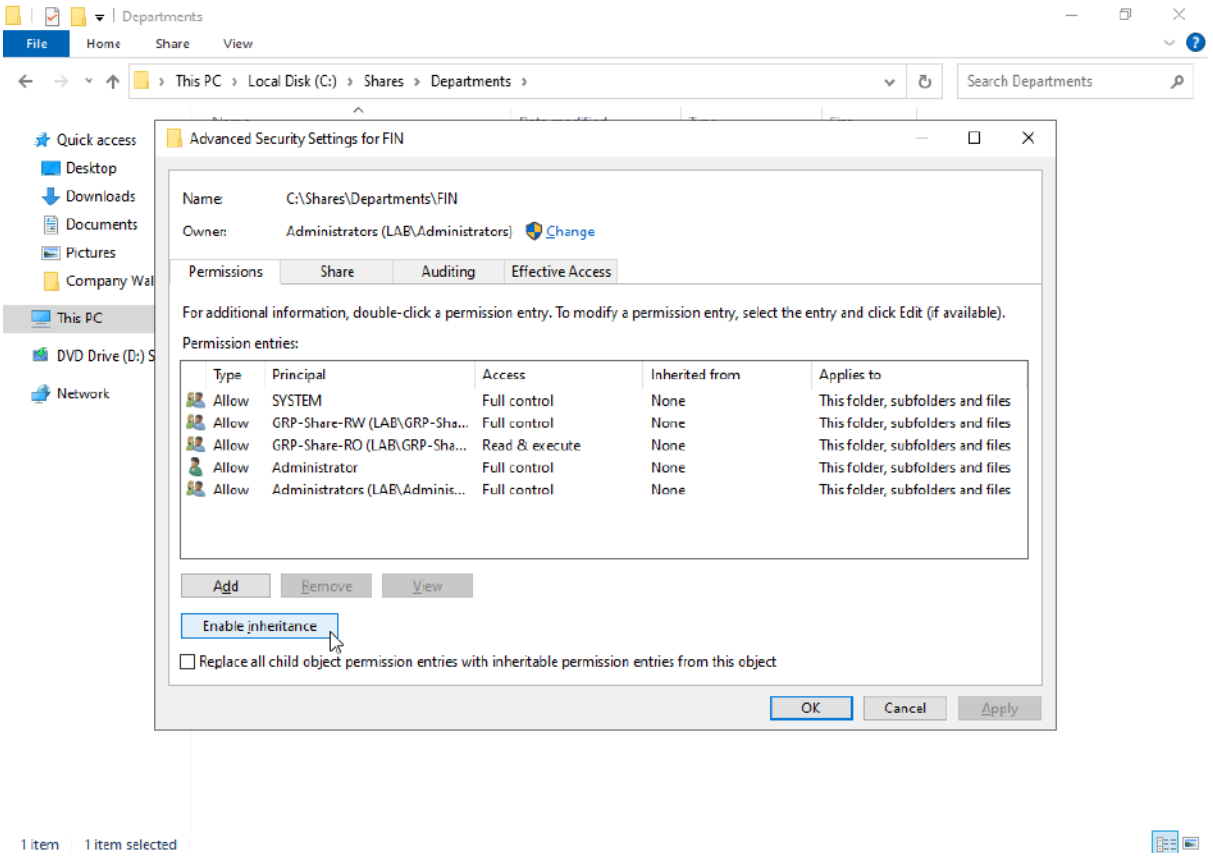
- Direct permissions assigned to users
- Active inherited permissions

Technical result

- Full access control through groups
- Strict enforcement of least privilege

Evidence

Figure 5.3.5 – Final NTFS permission list.



5.3.6 Groups and users involved

5.3.6.1 Groups used

Location: **30-Groups**

- **GRP-Share-RW**
- **GRP-Share-RO**

5.3.7 Tests from the domain client

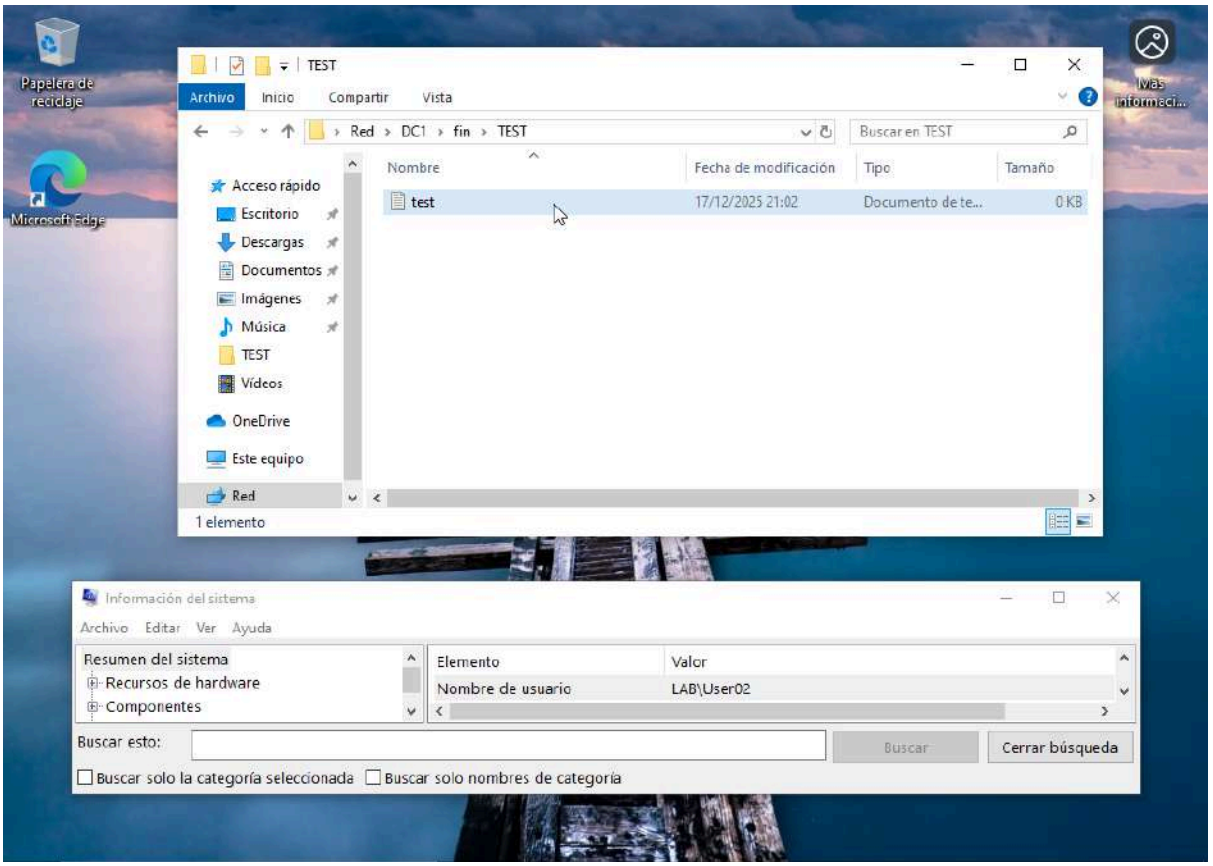
5.3.7.1 Access to the shared resource

Access methods:

- `\\DC1\FIN`
- File Explorer → Network → DC1 → FIN

Evidence

Figure 5.3.6 – Share accessible from the client.



5.3.7.2 User with Read & Write permissions

User:

- **User01**
- Member of **GRP-Share-RW**

Validations:

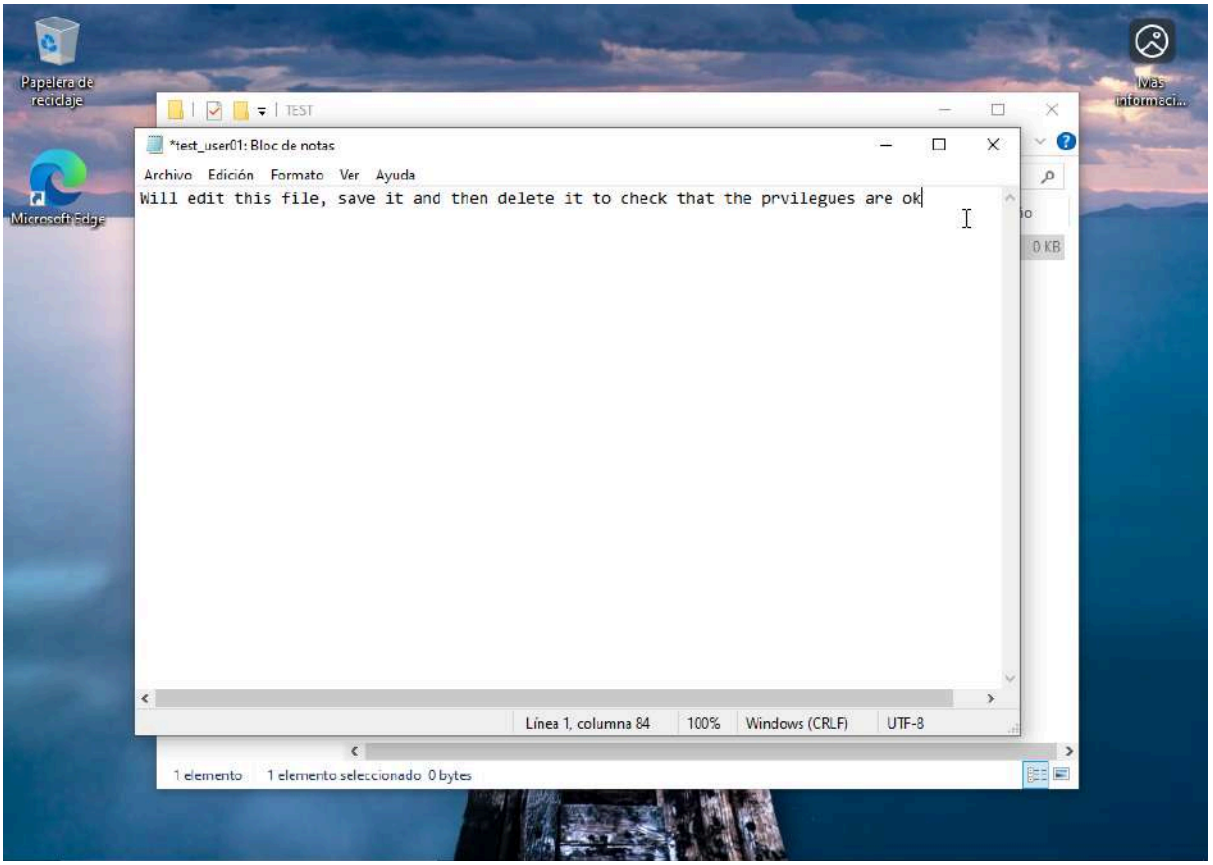
- Access allowed
- Creation, modification, and deletion of files

Result

- Correct Read/Write behavior

Evidence

Figure 5.3.7 – Write operations performed successfully.



5.3.7.3 User with Read Only permissions

User:

- **User02**
- Member of **GRP-Share-RO**

Validations:

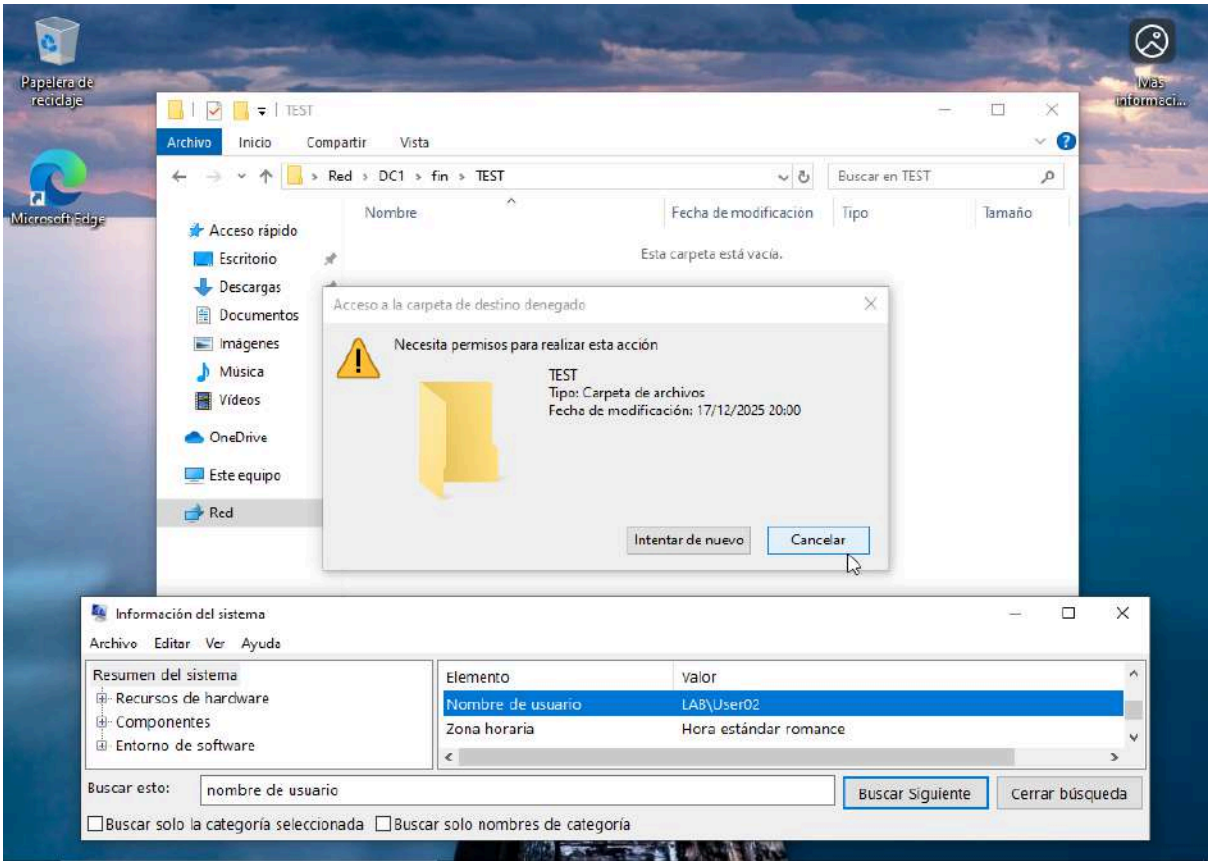
- Access allowed
- Write and modification denied

Result

- Restriction applied correctly

Evidence

Figure 5.3.8 – Access denied message when attempting to modify files.



5.3.7.4 Negative test – user without permissions

Action:

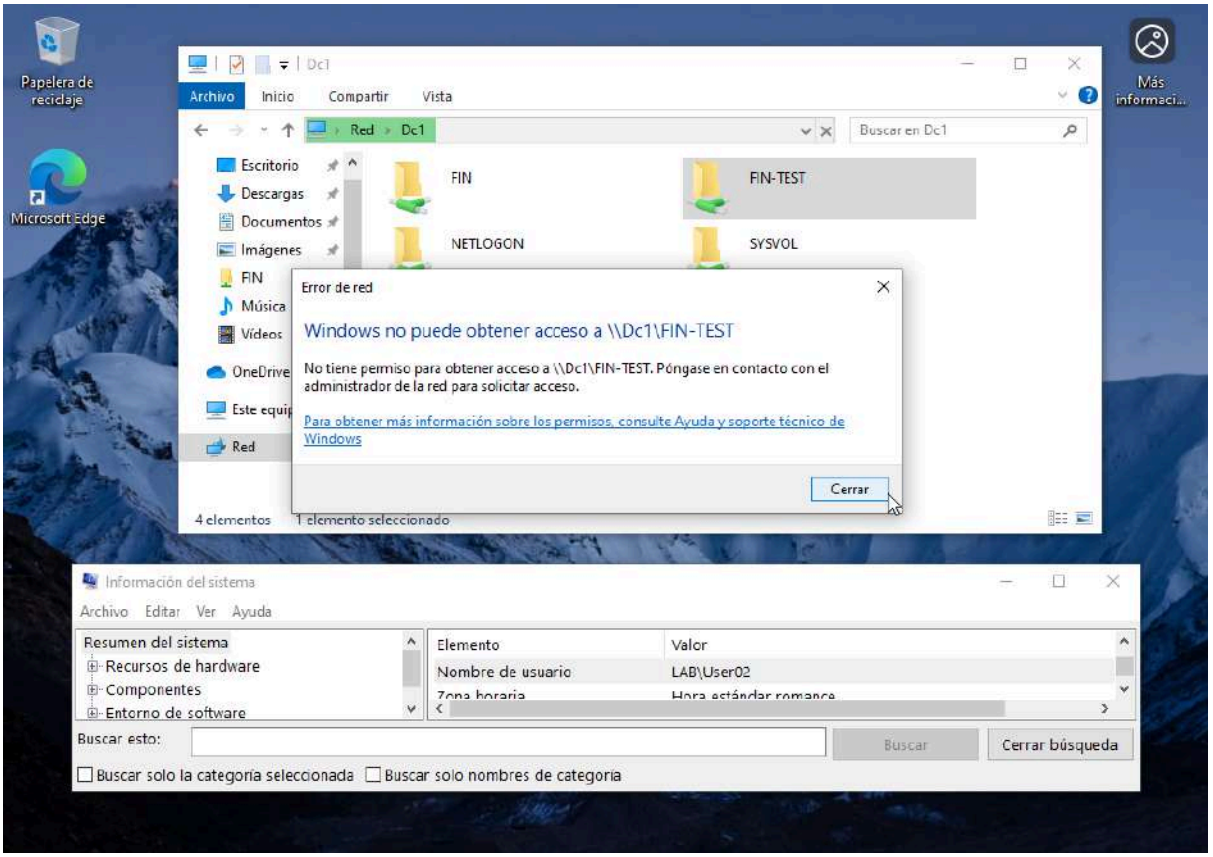
- Remove **User02** from both groups
- Log off and log back in to refresh the security token

Result

- Full access denied to the share
- No residual access

Evidence

Figure 5.3.9 – Access denied when trying to open `\\DC1\FIN`.



5.3.8 Tools used

- File Explorer (client)
- Active Directory Users and Computers
- NTFS Security properties
- Logoff / logon to refresh tokens

5.3.9 Technical observations

- Share and NTFS permissions are always evaluated together
- The most restrictive permission becomes effective
- Group-based management:
    - Reduces errors
    - Simplifies changes
    - Scales better
- Membership changes require a token refresh (logoff/logon)
- Access to **SYSVOL** and **NETLOGON** is expected and does not imply access to business data

5.4 Block 4 – Client Management & Troubleshooting

5.4.1 Block objective

- Reproduce realistic user, computer, and network incidents in a Windows domain.
- Apply methodical diagnosis: identify symptom, isolate cause, and validate the fix.
- Use only standard support tools (client + DC).
- Reinforce the operational differentiation between:
    - Account issue vs domain/computer issue
    - User Configuration vs Computer Configuration in GPO
    - IP vs DNS vs Gateway in connectivity

5.4.2 Incident 1 – User cannot log on

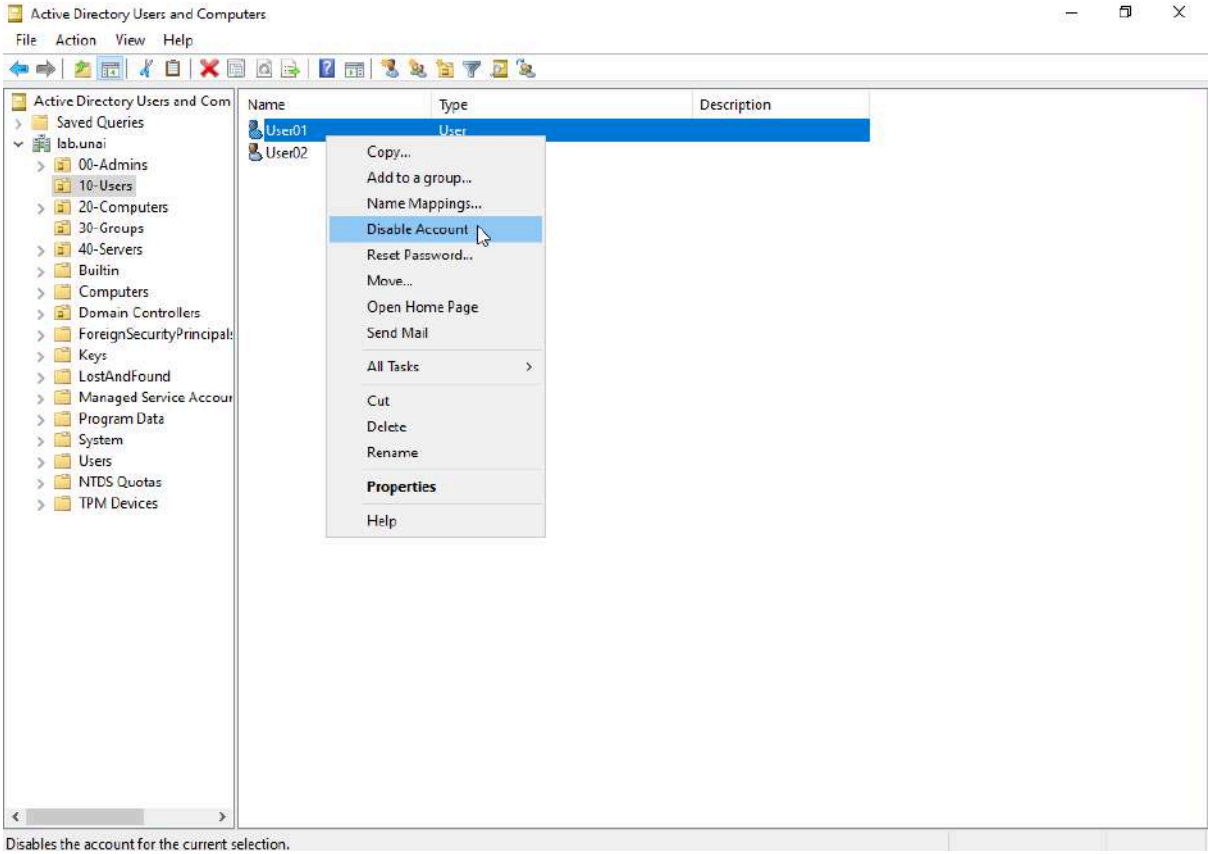
5.4.2.1 Induced incident

Action performed (DC1, ADUC):

- The **user01** account is manually disabled.

Evidence:

Figure 5.4.1 – User01 being disabled in ADUC.



5.4.2.2 Observed symptom

Behaviour (HOST1):

- When attempting to log on with **user01**, the system returns an authentication error.
- Access to the desktop is not granted.

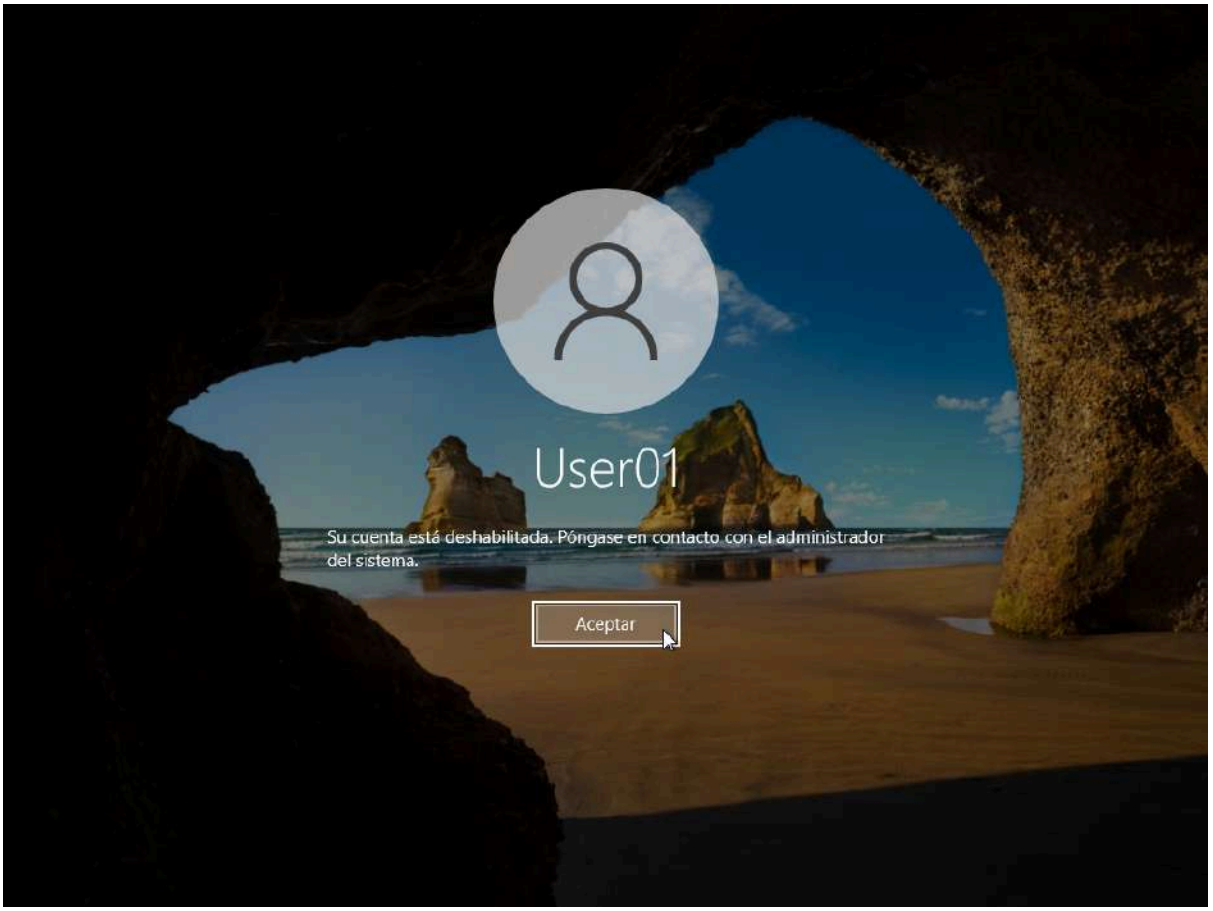
Technical interpretation:

- The domain is responding.
- The failure lies in the account, not in:
    - Network
    - Computer
    - DNS

- Domain

Evidence:

Figure 5.4.2 – Logon error message for user01.



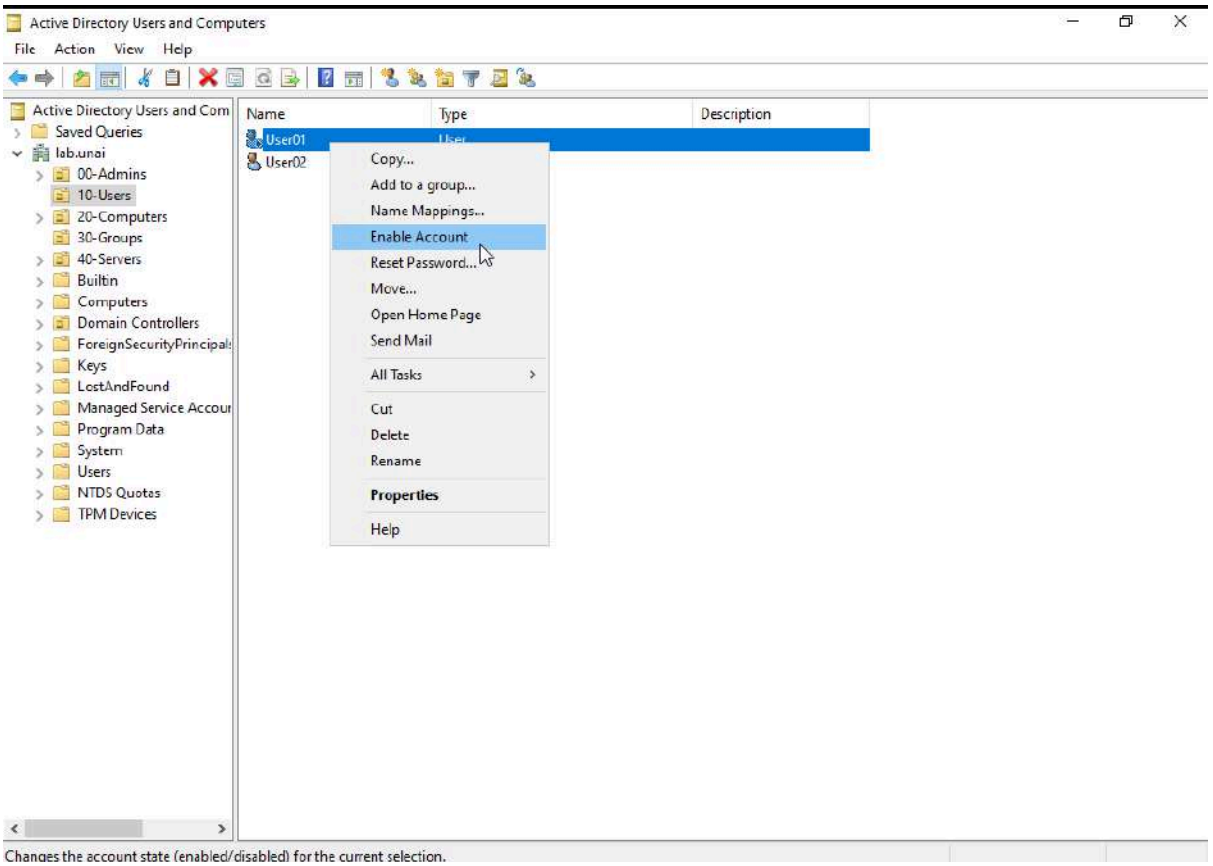
5.4.2.3 Resolution applied

Action performed (DC1, ADUC):

- The **user01** account is re-enabled.

Evidence:

Figure 5.4.3 – user01 account enabled again in ADUC.



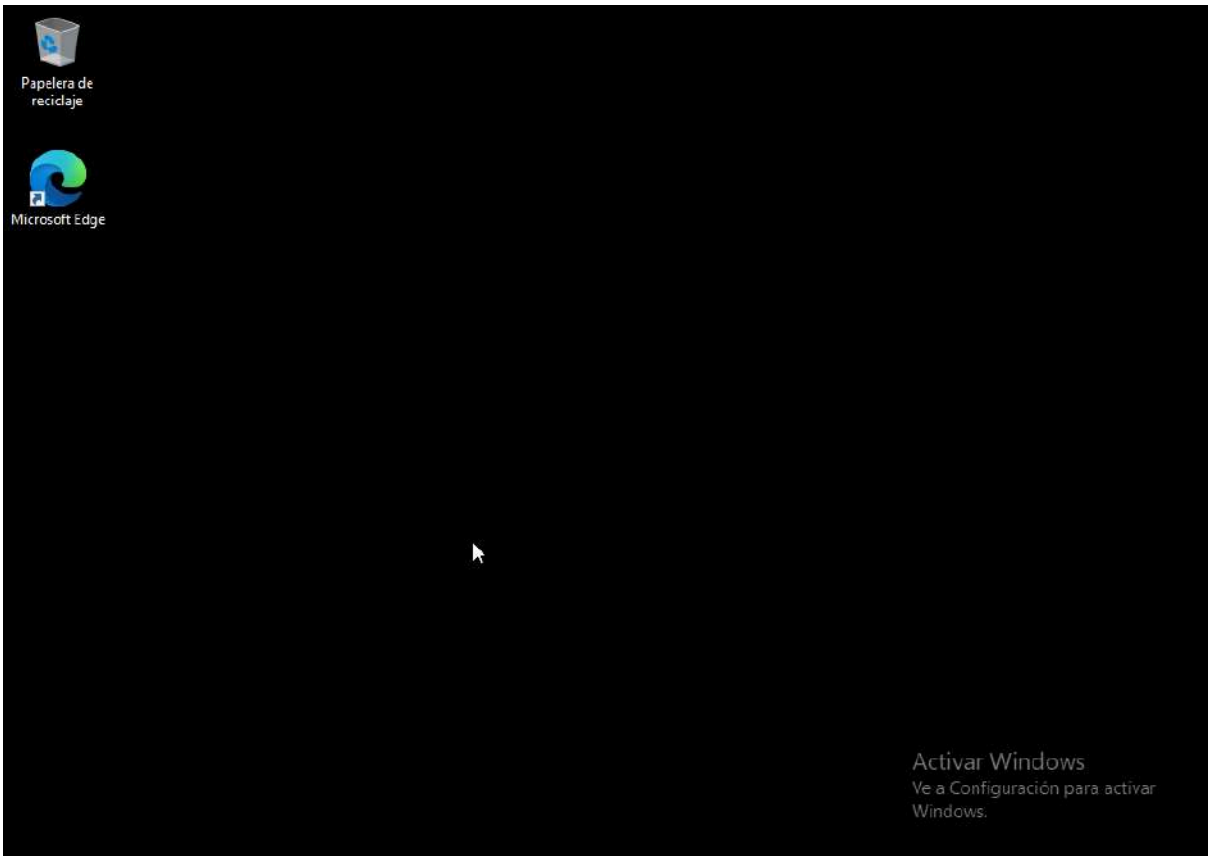
5.4.2.4 Validation

Result (HOST1):

- Successful logon with **user01**.
- Profile loads normally.

Evidence:

Figure 5.4.4 – Desktop loaded after logging in with user01.



5.4.2.5 Operational learning

- Distinguish an account-level failure from a domain/computer failure.
- A domain can be healthy even if a user cannot authenticate.

5.4.3 Incident 2 – Computer joined to the domain but GPO not applied

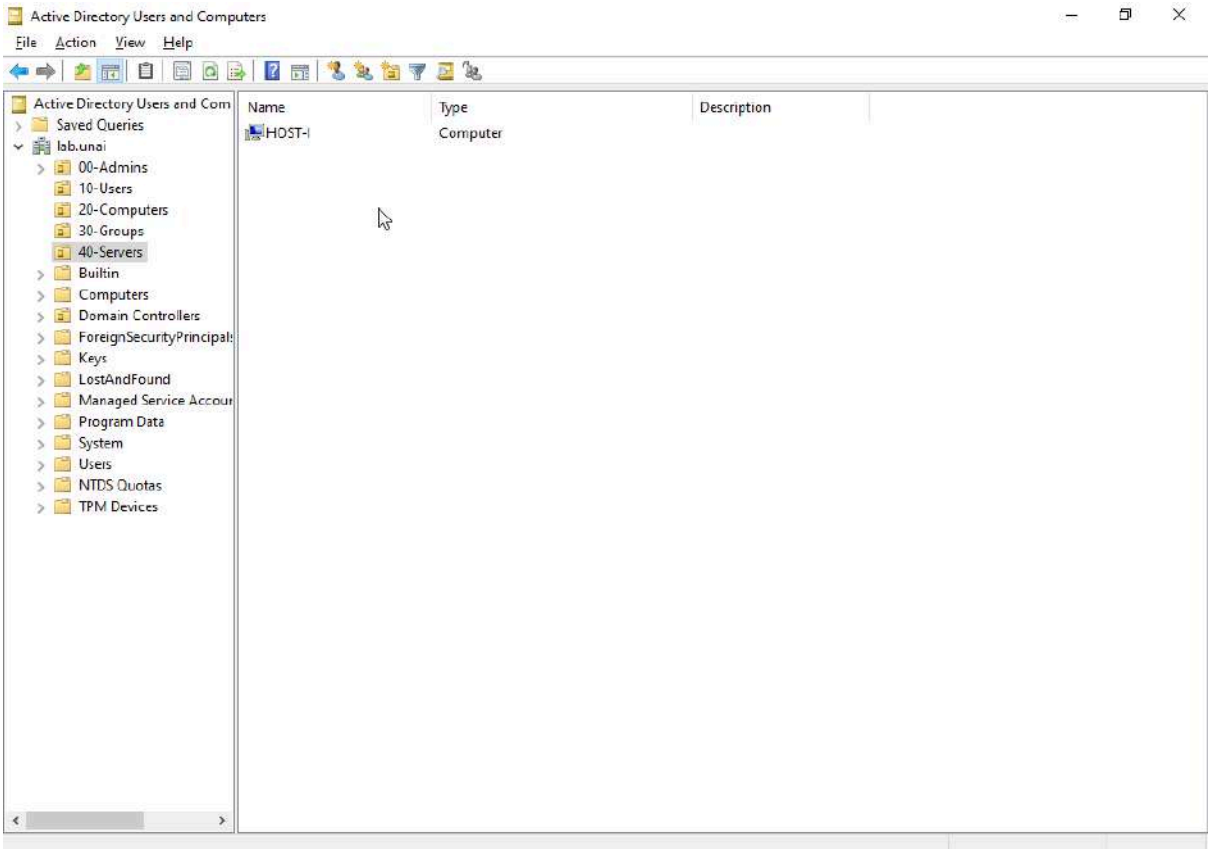
5.4.3.1 Induced incident

Action performed (DC1, ADUC):

- The client computer is moved out of the **20-Computers** OU, where the USB-blocking GPO is linked.

Evidence:

Figure 5.4.5 – HOST1 moved out of the 20-Computers OU.



5.4.3.2 Observed symptom

Check from the client (HOST1):

- `gpupdate /force` is run.
- `gpresult /r /scope computer` is run.

Result:

- The USB-blocking GPO does not appear as applied.
- User GPOs continue to work.

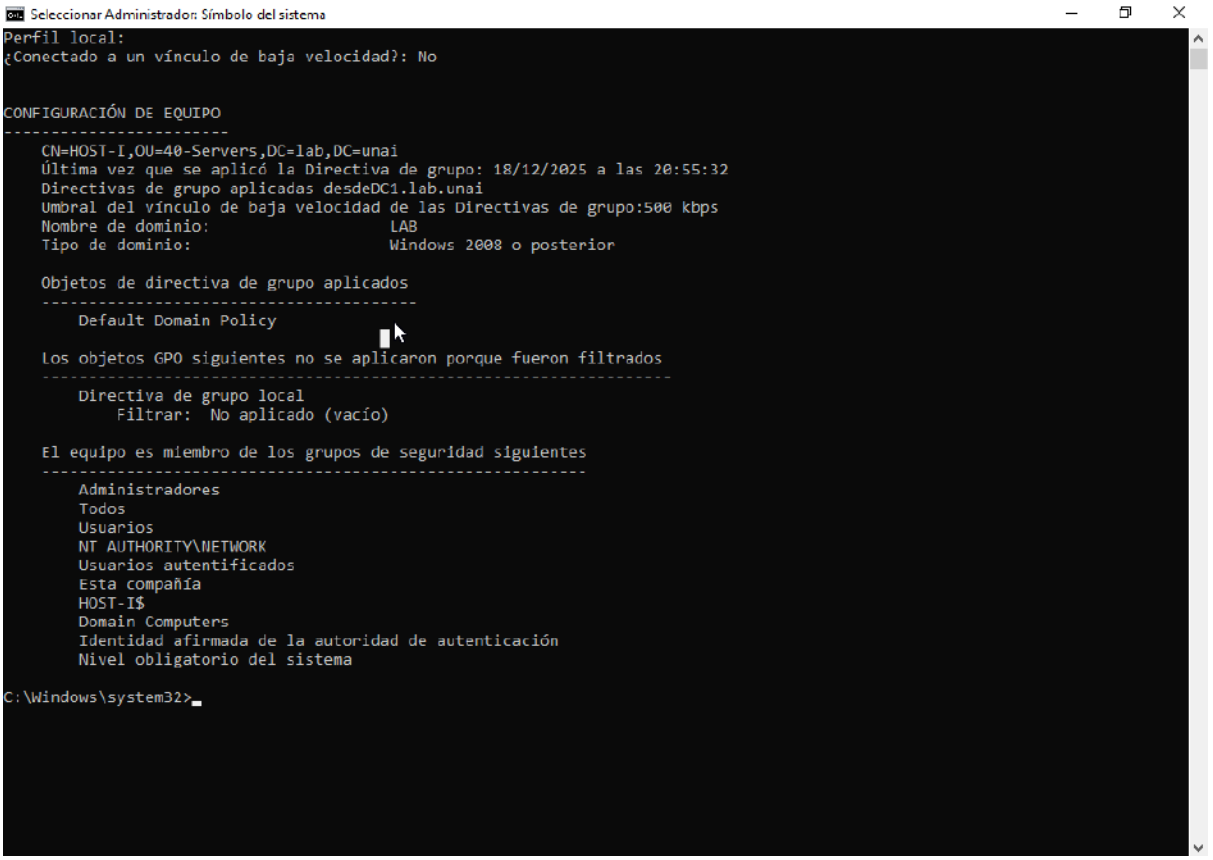
Key technical observation:

- The USB GPO is **Computer Configuration**.

- It must be validated using the computer scope.

Evidence:

Figure 5.4.6 – `gpresult /r /scope computer` without the USB GPO listed.



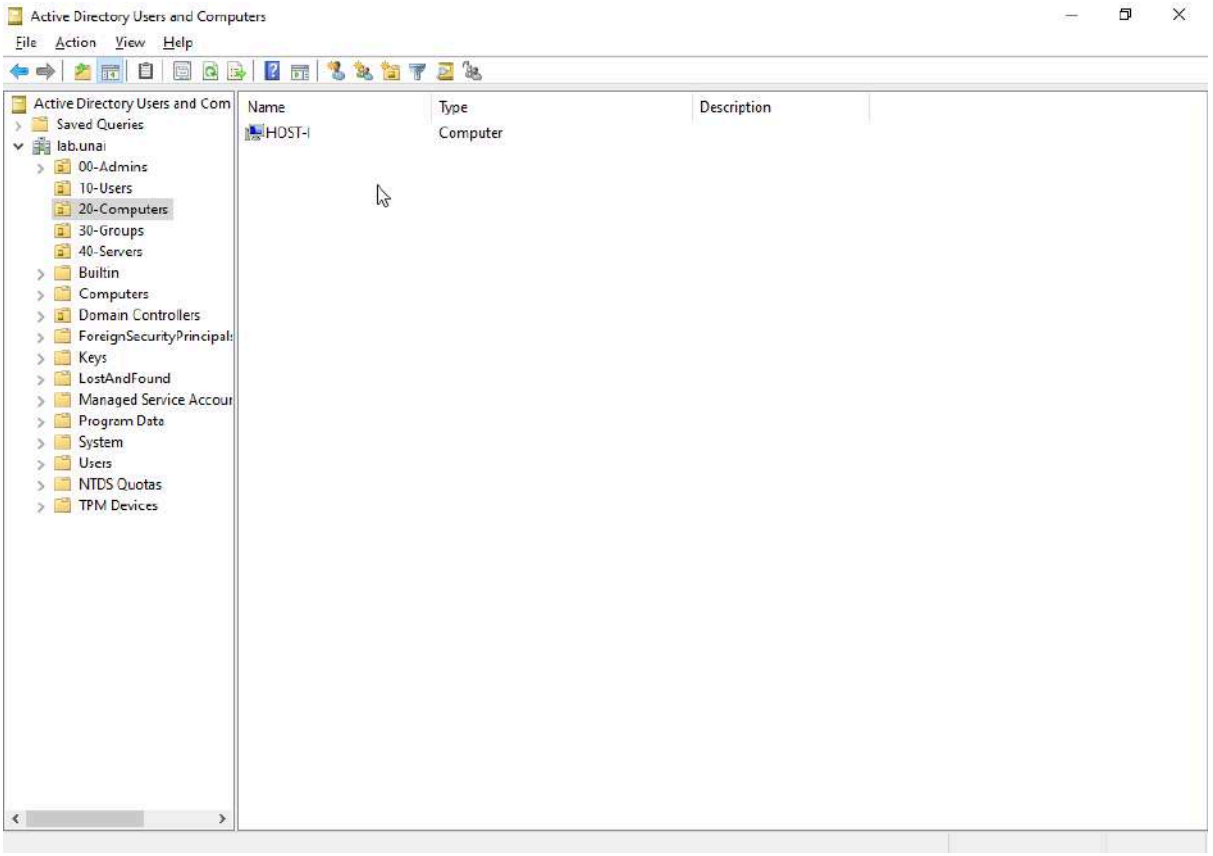
5.4.3.3 Resolution applied

Action performed (DC1, ADUC):

- The computer is moved back into the correct OU (**20-Computers**).

Evidence:

Figure 5.4.7 – HOST1 relocated into the 20-Computers OU.



5.4.3.4 Validation

Check from the client (HOST1):

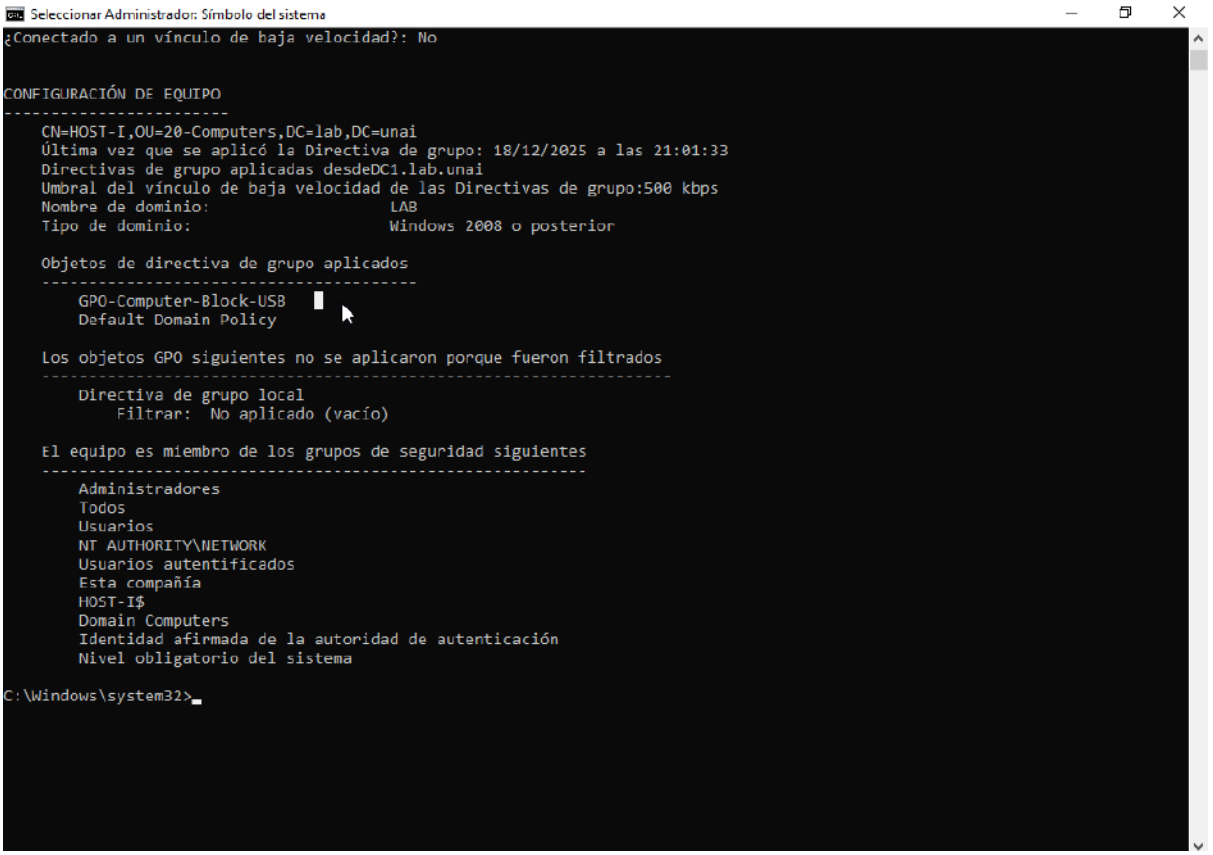
- `gpupdate /force` is run.
- `gpresult /r /scope computer` is run again.

Result:

- The USB-blocking GPO appears again as applied.

Evidence:

Figure 5.4.8 – GPO correctly listed under Computer Configuration.



5.4.3.5 Operational learning

- Clearly distinguish **User Configuration** vs **Computer Configuration**.
- Using `gpresult` with the correct scope prevents wrong diagnoses.
- A GPO can “disappear” due to OU/scope changes without any actual domain failure.

5.4.4 Incident 3 – Internal DNS not resolving

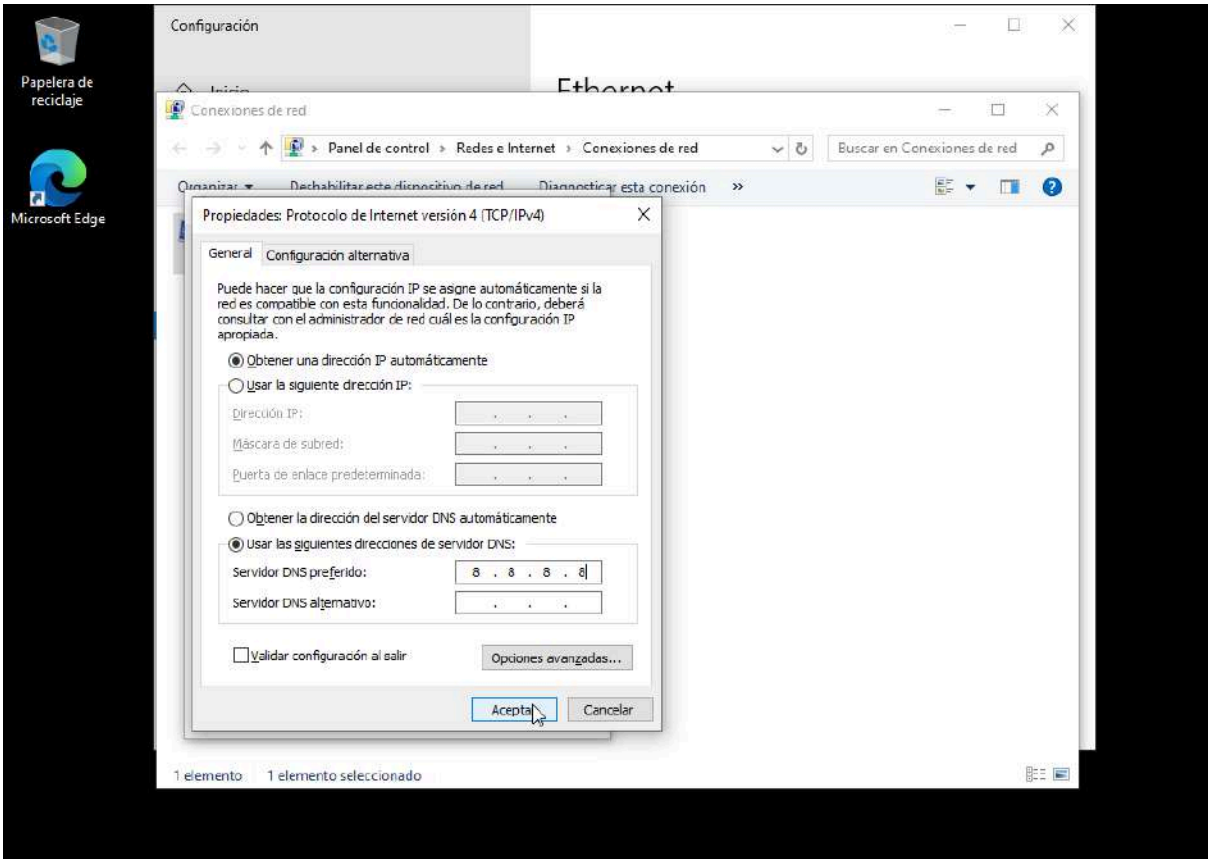
5.4.4.1 Induced incident

Action performed (HOST1):

- DNS is manually set to **8.8.8.8**.

Evidence:

Figure 5.4.9 – Adapter configuration with manual DNS 8.8.8.8.



5.4.4.2 Observed symptom

Check (HOST1):

- `nslookup DC1.lab.unai` is run.

Result:

- The DC cannot be resolved.

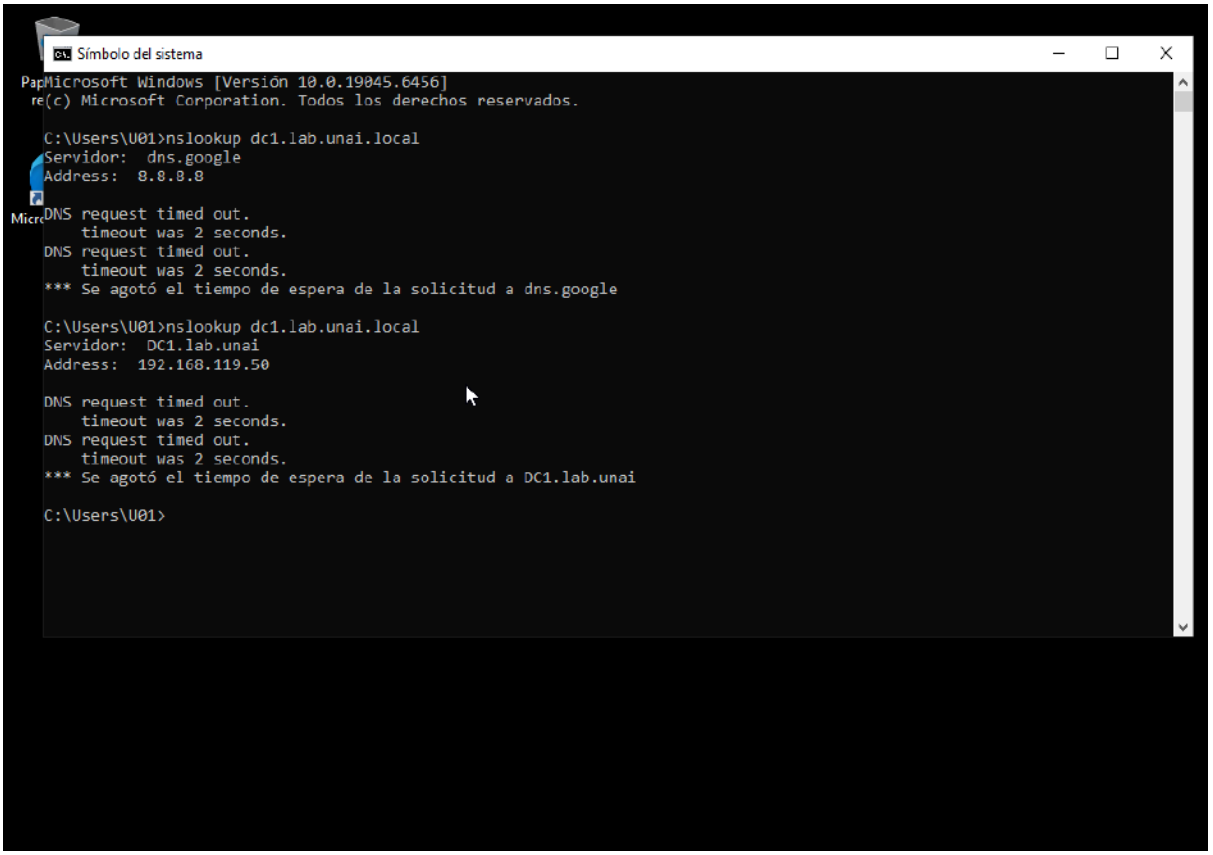
- The client cannot locate domain services.

Interpretation:

- The domain becomes unreachable even if:
    - There is a valid IP
    - Basic connectivity still exists

Evidence:

Figure 5.4.10 – Resolution error in `nslookup` for DC1.lab.unai and google.



5.4.4.3 Resolution applied

Action performed (HOST1):

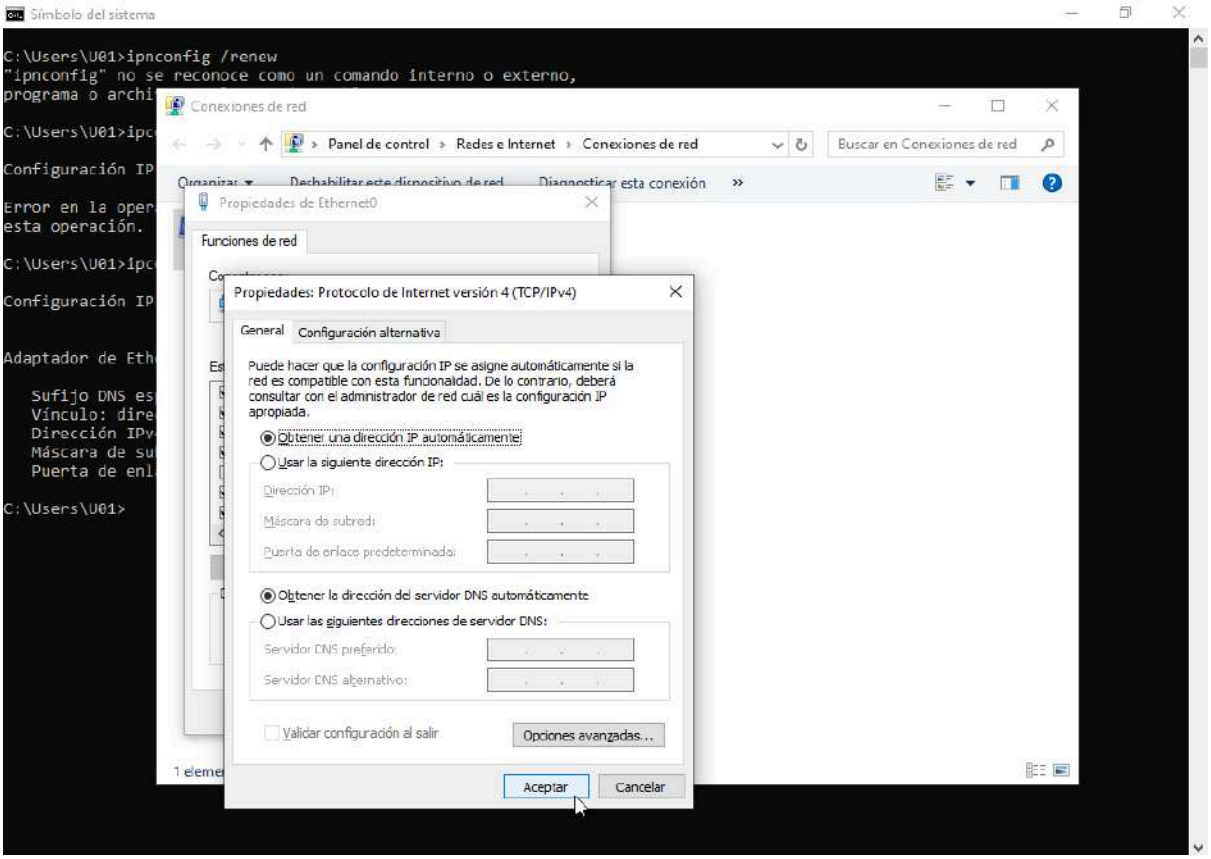
- Network configuration is restored to automatic (DHCP).

Real note from the lab:

- `ipconfig /renew` did not work correctly.
- Resolution was restored anyway after switching back to automatic.

Evidence:

Figure 5.4.11 – NIC set to automatic (DHCP) with DNS restored to the DC.



5.4.4.4 Validation

Checks (HOST1):

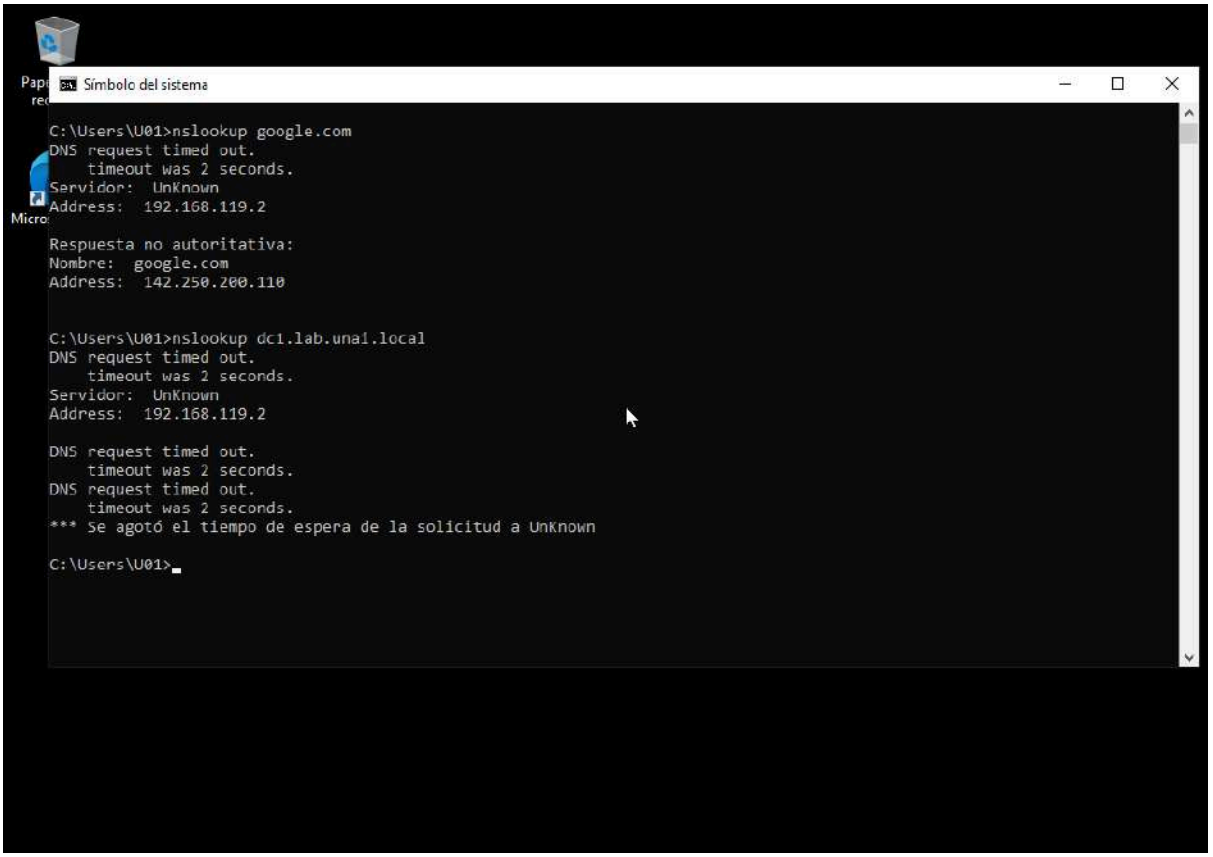
- `nslookup DC1.lab.unai`
- `nslookup google.com`

Result:

- Internal resolution working.
- External resolution also working.

Evidence:

Figure 5.4.12 – Valid response from both `nslookup` commands.



5.4.4.5 Operational learning

- Active Directory depends entirely on internal DNS.
- External DNS configured on the client breaks the domain even if “the network seems fine”.

5.4.5 Incident 4 – Computer has IP but no connectivity

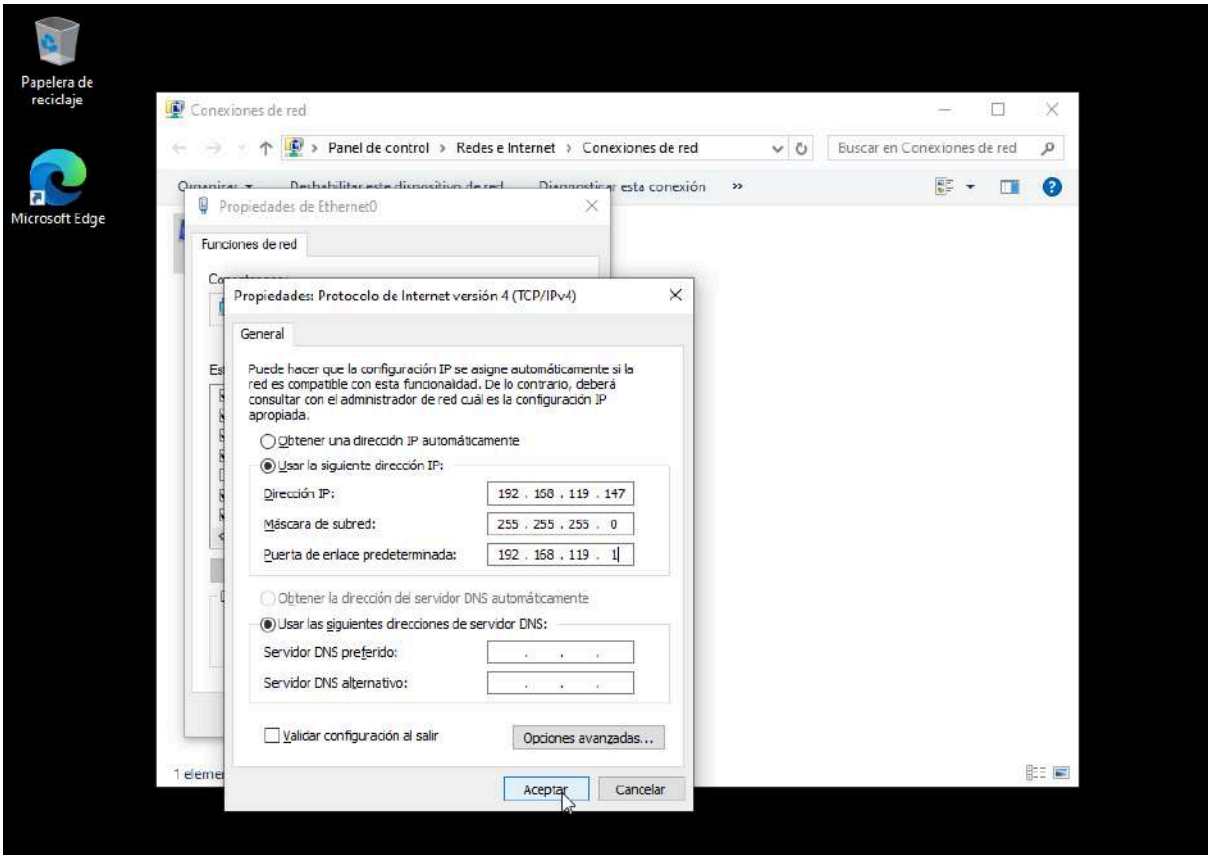
5.4.5.1 Induced incident

Action performed (HOST1):

- An incorrect gateway is manually configured while keeping IP and DNS correct.

Evidence:

Figure 5.4.13 – Wrong gateway manually configured.



5.4.5.2 Performed diagnostics

Commands used (HOST1):

- `ipconfig /all`
- `ping DC1`
- `ping 8.8.8.8`

- `nslookup google.com`

Typical result:

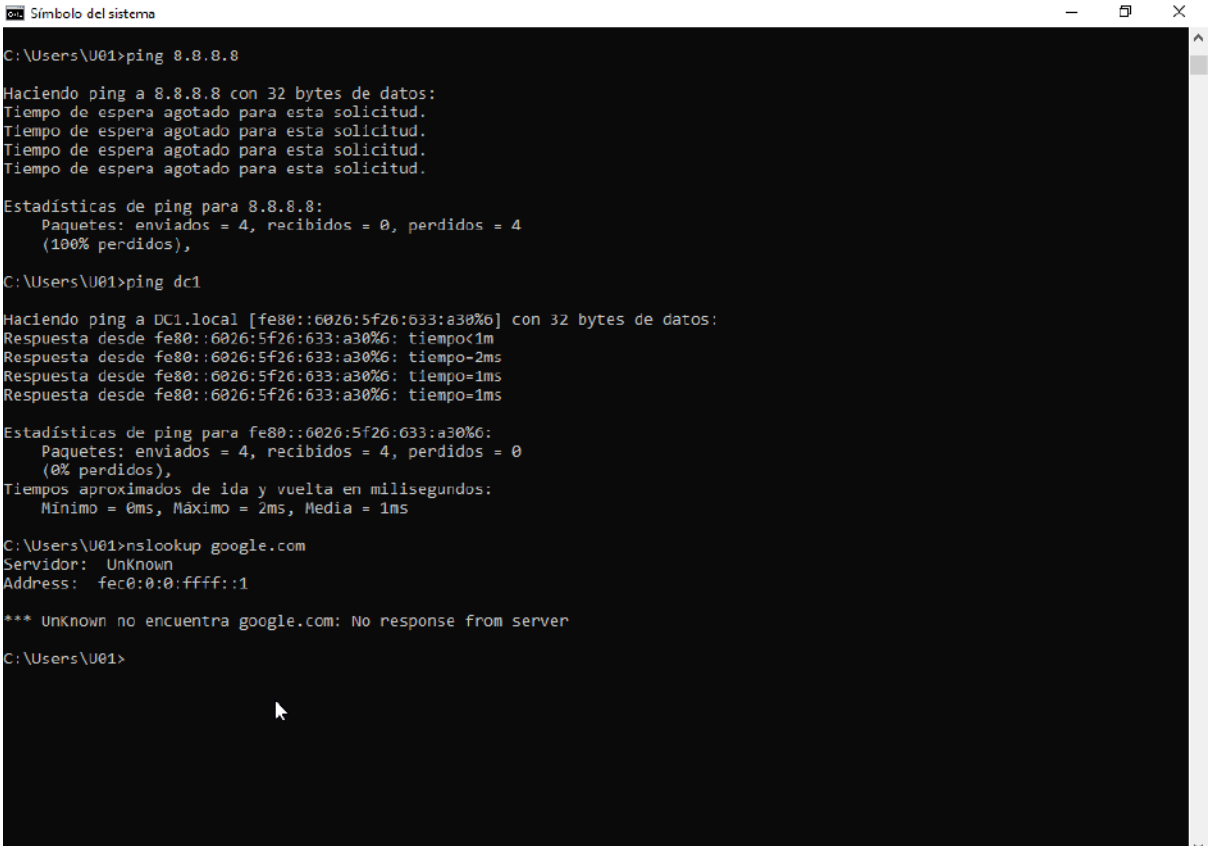
- IP is correct
- DNS works
- No outbound connectivity to external networks

Interpretation:

- Failure isolated to the gateway configuration.

Evidence:

Figure 5.4.14 – Internal ping successful and external ping failing.



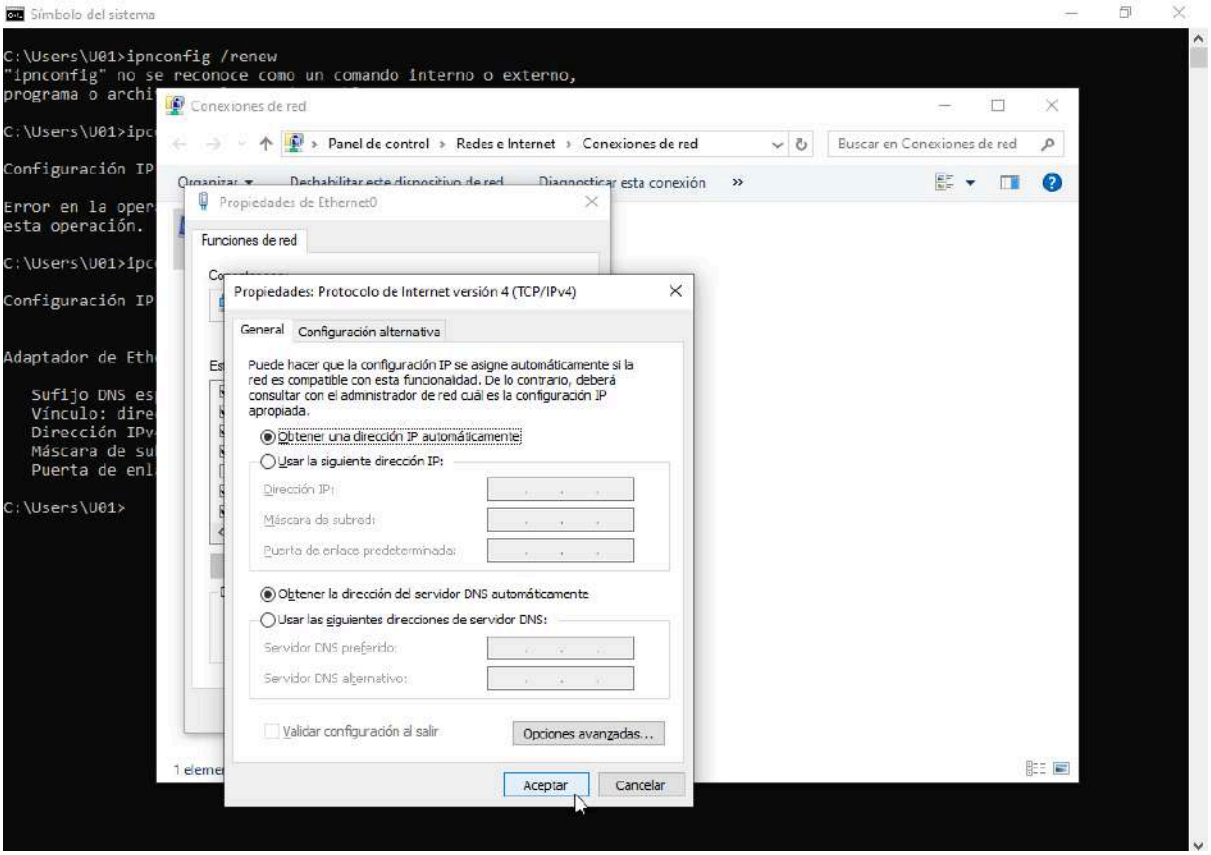
5.4.5.3 Resolution applied

Action performed (HOST1):

- Network configuration is restored to automatic (DHCP).

Evidence:

Figure 5.4.15 – Network restored to DHCP.



5.4.5.4 Validation

Checks (HOST1):

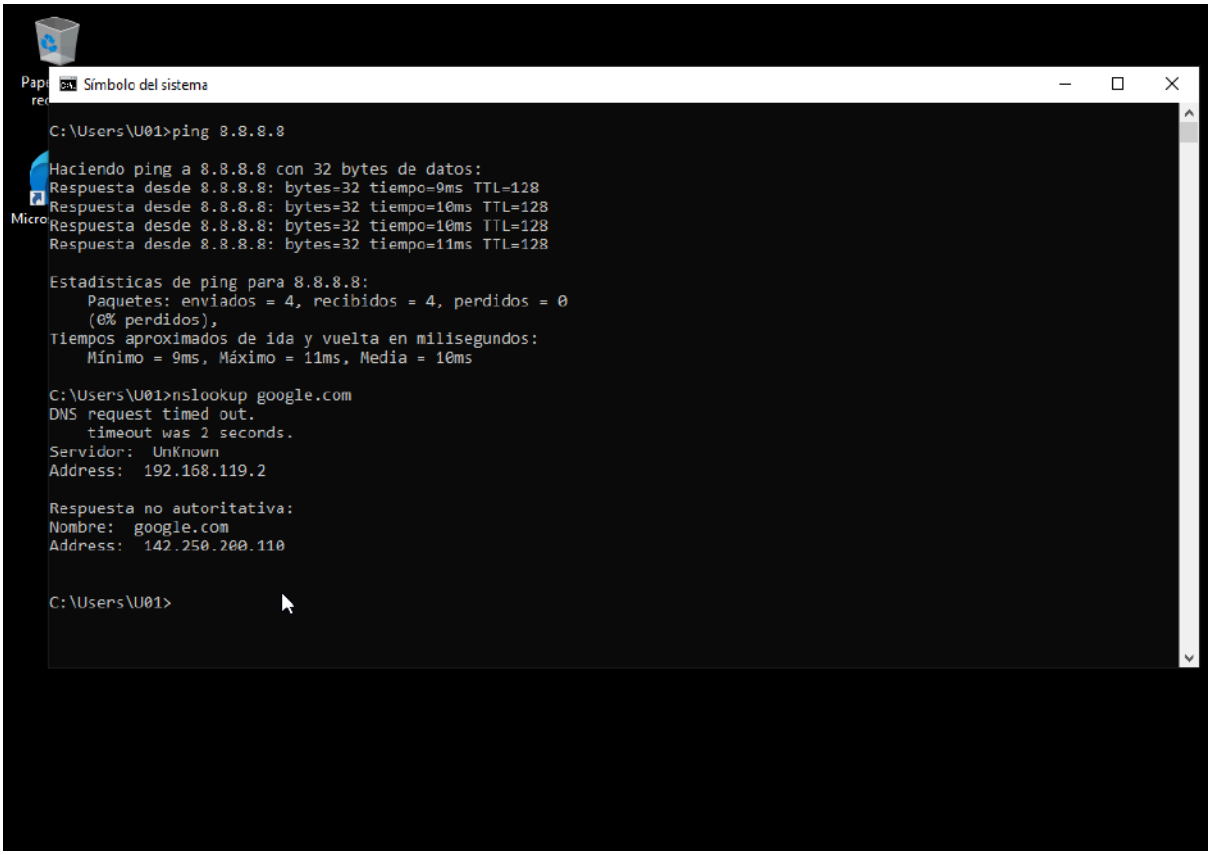
- `ping 8.8.8.8`
- `nslookup google.com`

Result:

- Connectivity restored.

Evidence:

Figure 5.4.16 – Successful ping and `nslookup` responses.



5.4.5.5 Operational learning

- Clearly separate:
    - IP
    - DNS
    - Gateway
- Having an IP does not guarantee that the system is actually functional.

5.4.6 Tools used

- `ipconfig /all`
- `ping`

- `nslookup`
- `gpupdate /force`
- `gpresult /r` (with the correct scope)
- ADUC for corrective actions
- Logon/logoff to refresh tokens

5.5 Block 5 – Operational Scenarios

5.5.1 Objective

- Execute real day-to-day administration scenarios on an already operational Active Directory domain.
- Manage user onboarding, offboarding, and role changes without modifying infrastructure.
- Apply all changes strictly through security groups and OUs.
- Always validate from the client the real impact of each operation.

5.5.2 Scenario 1 – User onboarding validation (end-to-end)

User used: **User02**

5.5.2.1 Actions performed

In Active Directory Users and Computers (DC1):

- Verified that **User02**:
    - Is enabled
    - Is not locked out
    - Resides in the **10-Users** OU
- Reviewed previously assigned group memberships

On the client computer (HOST1):

- Logon with domain credentials
- Access to the shared resource:
    - `\\DC1\FIN`
- Validation of effective permissions based on group membership
- Execution of:
    - `gpresult /r`

5.5.2.2 Validation

- Successful logon
- Resource access aligned with group membership
- Domain policies correctly received

Evidence:

Figure 5.5.1 – Desktop loaded with a domain session.

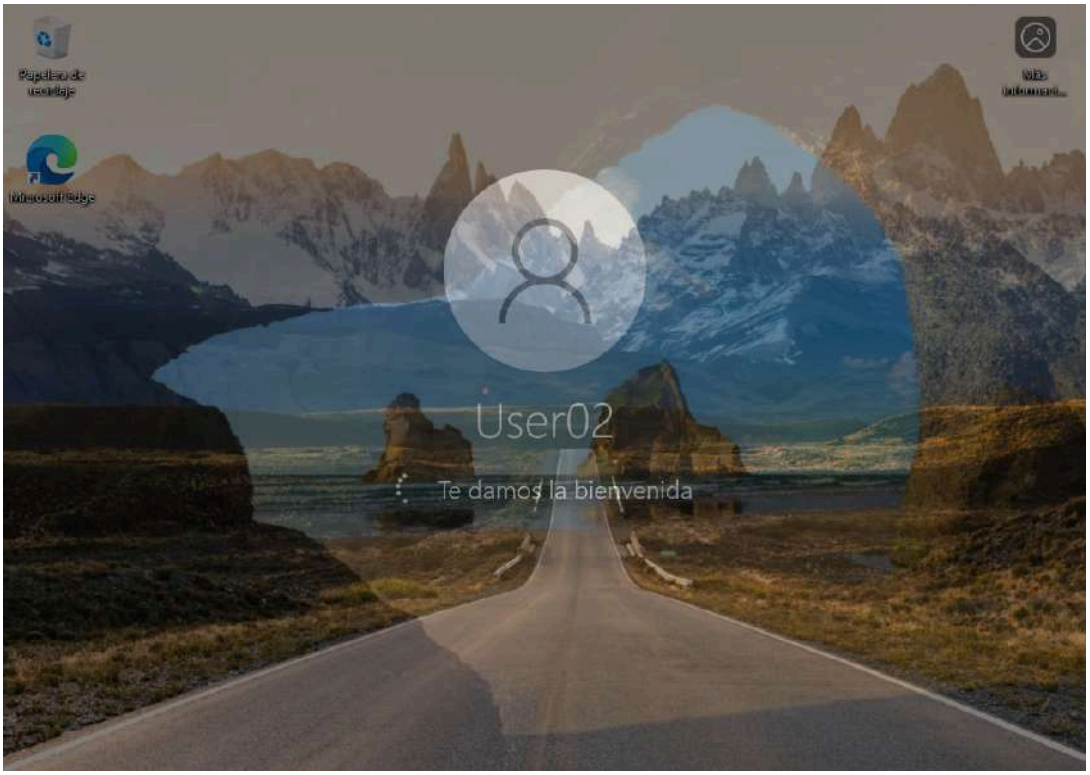


Figure 5.5.2 – Correct access to the FIN share.

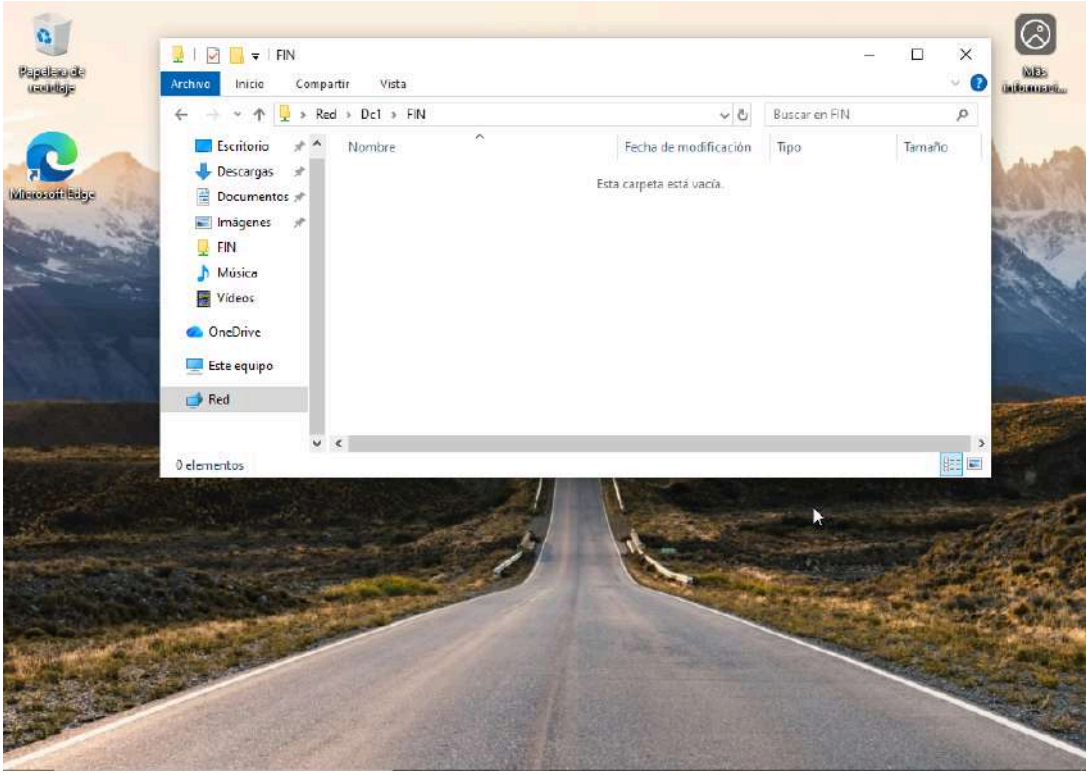
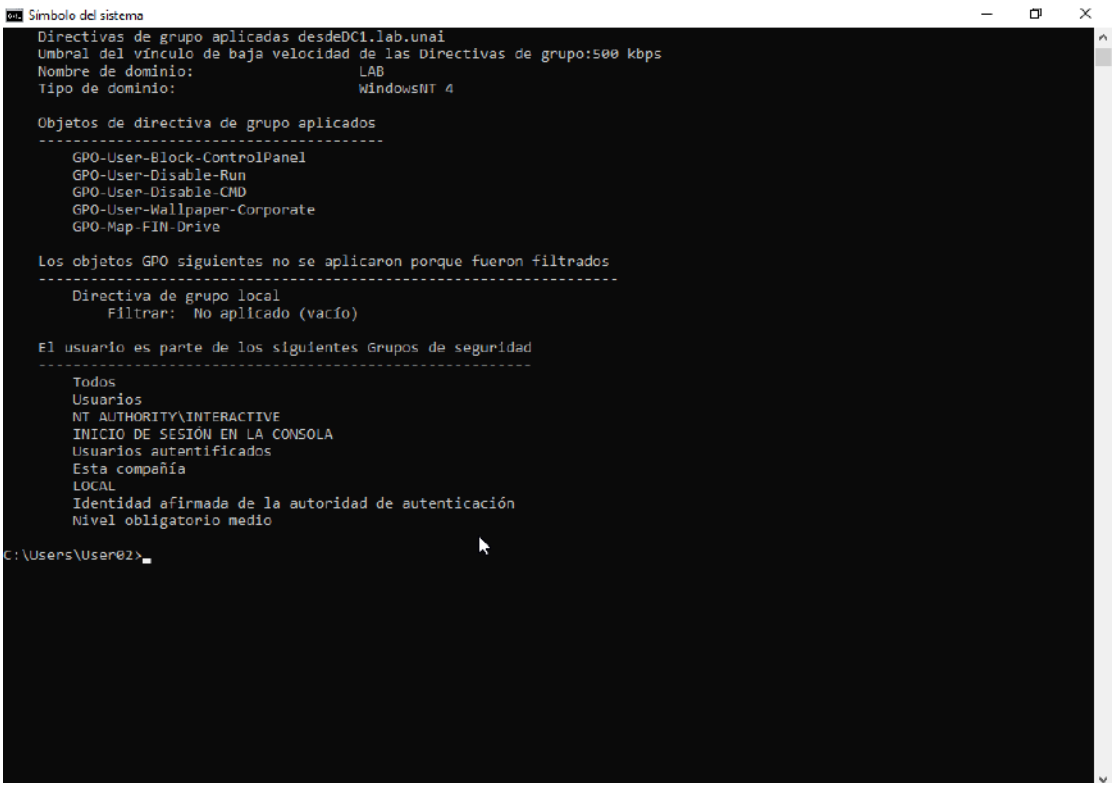


Figure 5.5.3 – GPOs applied according to `gpresult /r`.



5.5.2.3 Result

- Fully operational user end-to-end.
- Identity, permissions, and policies functioning in an integrated way.
- Onboarding validated without requiring further adjustments.

5.5.3 Scenario 2 – User offboarding (safe and orderly)

User used: **User02**

5.5.3.1 Access removal (groups)

In ADUC:

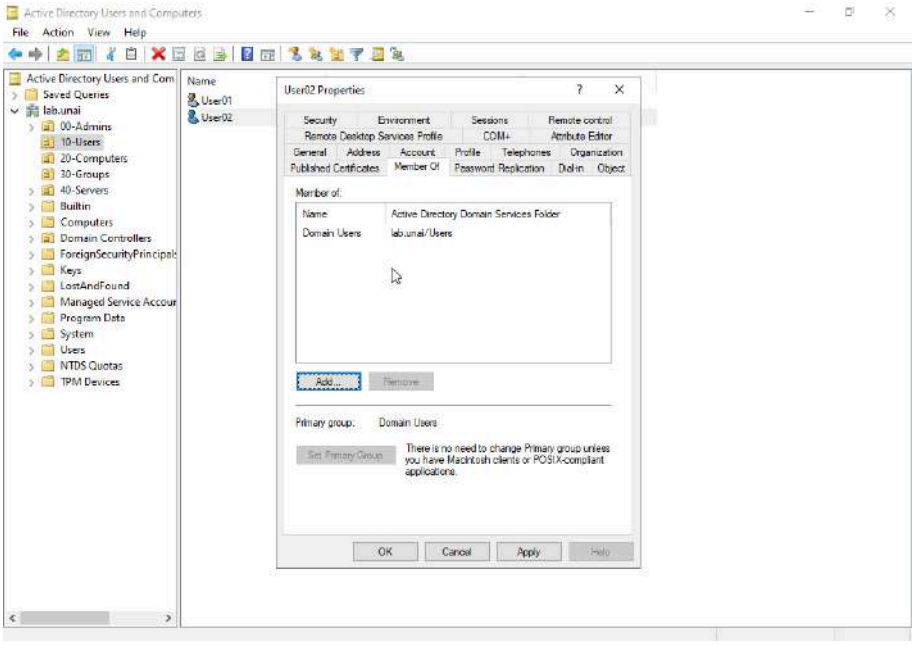
- **User02 → Properties → Member Of**
- All access-granting groups removed:
  - **GRP-Finances**
  - **GRP-Share-RO**
  - **GRP-Share-RW**
- Only default groups remain (Domain Users).

Validation:

- The user logically loses access to resources before disabling the account.

Evidence:

Figure 5.5.4 – Group memberships without access groups.



5.5.3.2 Move to inactive accounts OU

In ADUC:

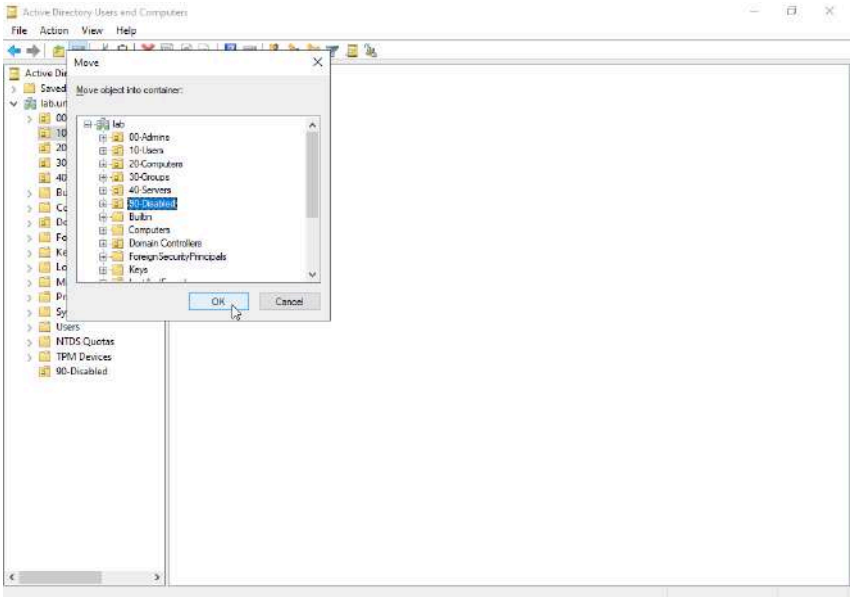
- Creation of the **90-Disabled** OU
- Move **User02** from **10-Users** to **90-Disabled**

Validation:

- Logical and visual separation of inactive accounts.

Evidence:

Figure 5.5.5 – User being placed in the 90-Disabled OU.



5.5.3.3 Account disabling

In ADUC:

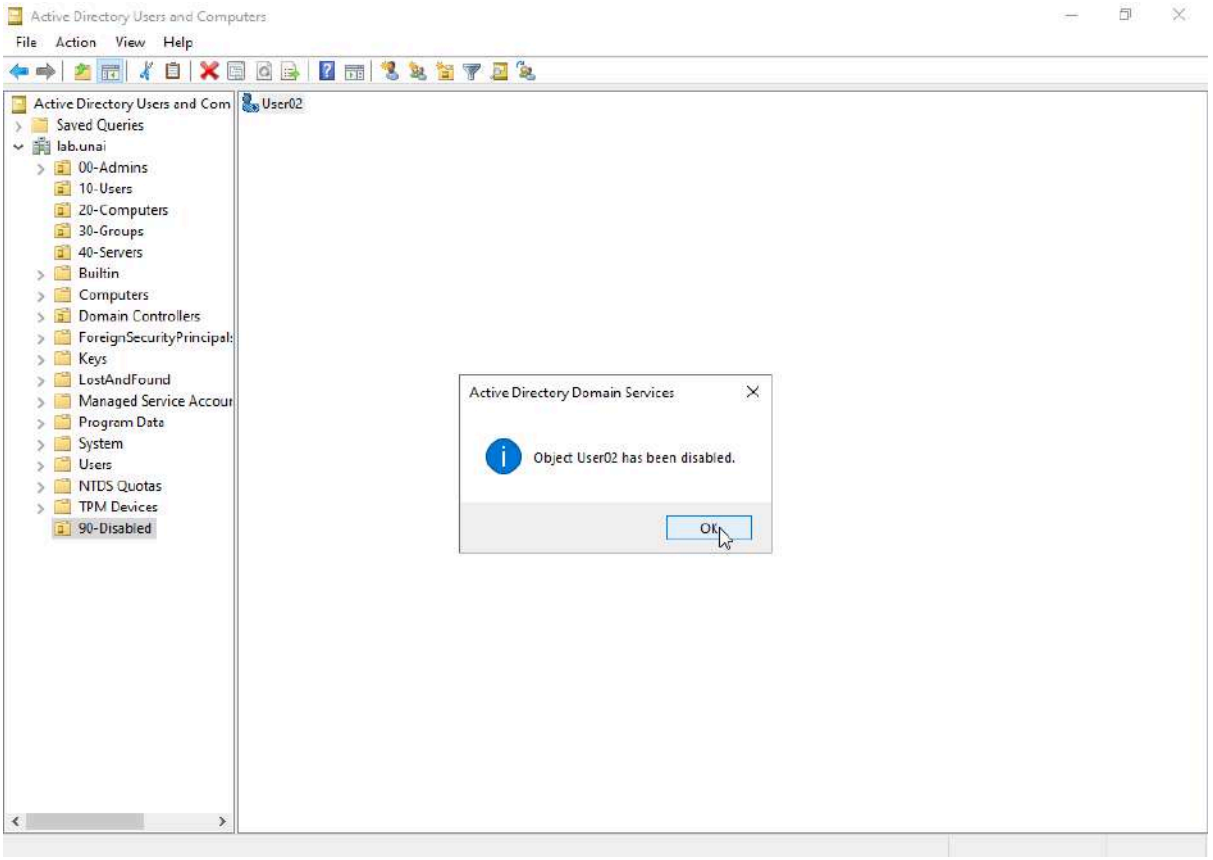
- Right-click on **User02** → **Disable Account**

Validation:

- Account marked as disabled.

Evidence:

Figure 5.5.6 – Disabled account visible in ADUC.



5.5.3.4 Validation from the client

On HOST1:

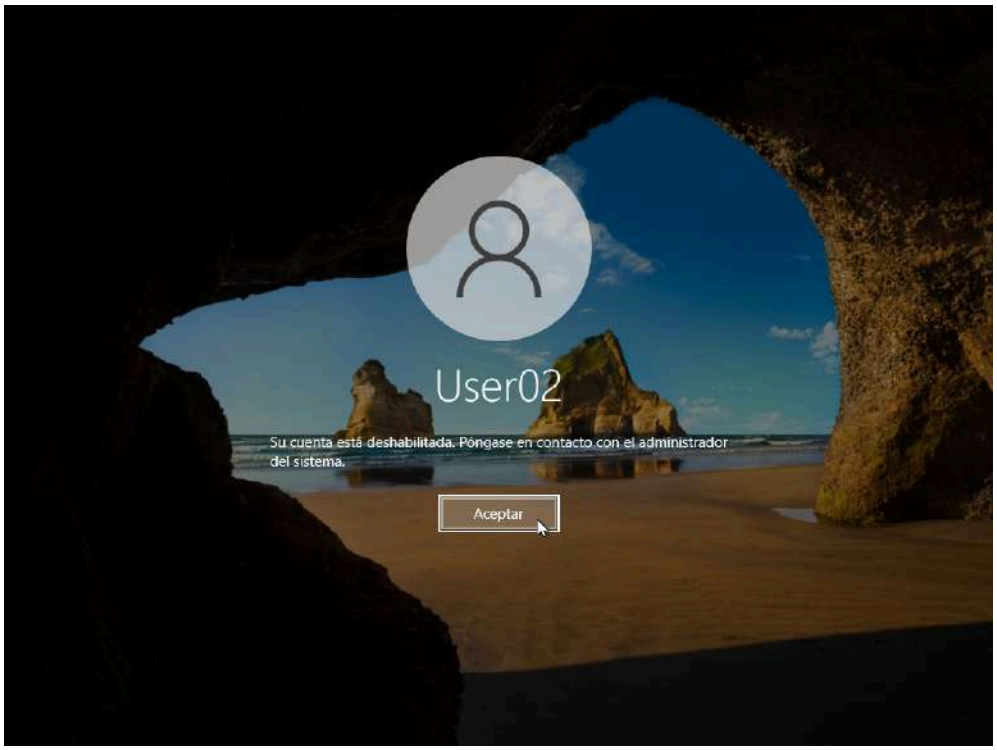
- Logon attempt with **User02**

Expected result:

- Authentication error due to disabled account.

Evidence:

Figure 5.5.7 – Logon error message.



5.5.3.5 Result

- Effective and verifiable offboarding.
- No residual access.
- Process is reproducible and aligned with best practices.

5.5.4 Scenario 3 – Department change (active user)

User used: **User01**

5.5.4.1 Initial state – Finance department

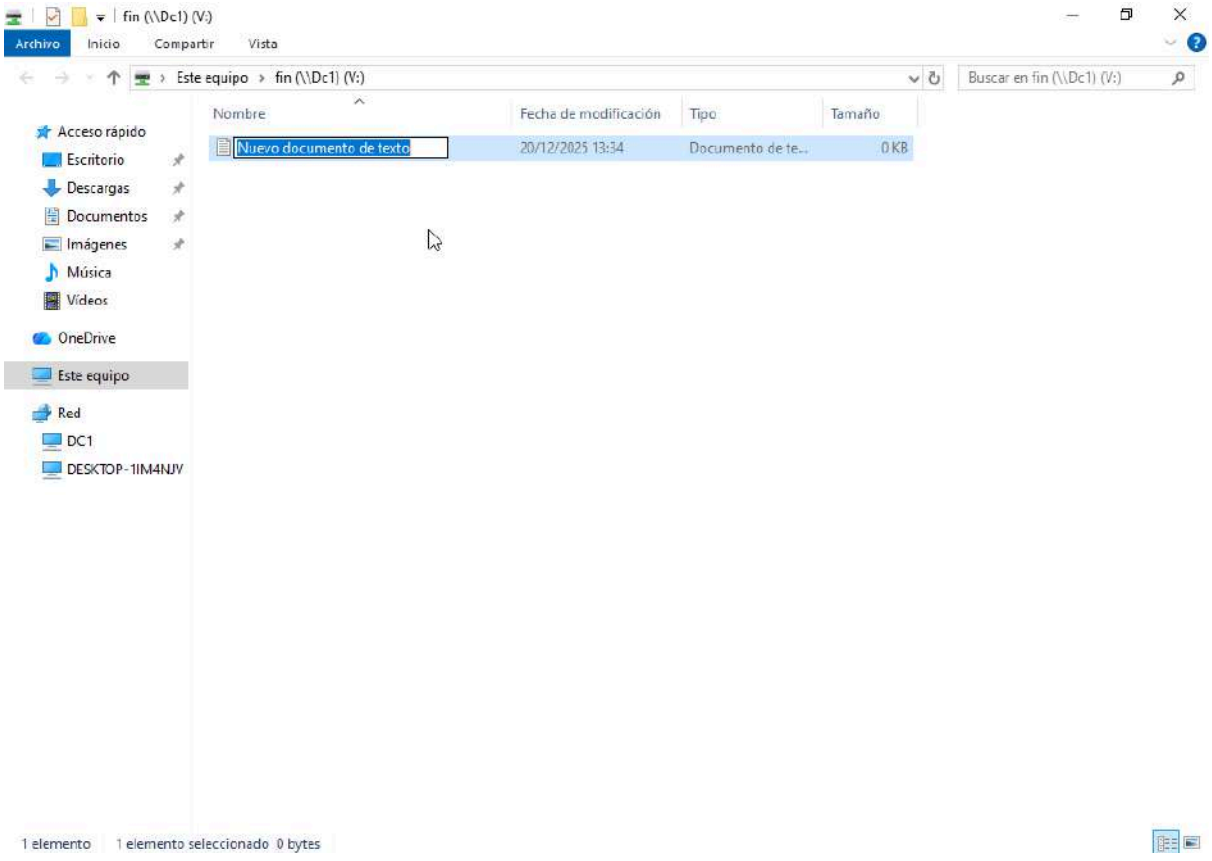
- OU: **10-Users**
- Groups:
    - **GRP-Finances**
    - **GRP-Share-RW**

Validation from the client:

- Correct access to `\\DC1\FIN`.
- Permissions aligned with the Finance role.

Evidence:

Figure 5.5.8 – Functional access to the shared resource.



5.5.4.2 Department change → IT

In ADUC:

- Remove Finance-related groups:
  - **GRP-Finances**
  - **GRP-Share-RW**
- Add the group:
  - **GRP-IT-Admins**

The following are not modified:

- NTFS permissions
- Share permissions
- Resource configuration

5.5.4.3 Post-change validation

On HOST1 (logon as User01):

- Attempt to access `\\DC1\FIN`

Result:

- Access denied, consistent with the principle of least privilege.

Evidence:

Figure 5.5.9 – Resource access error.

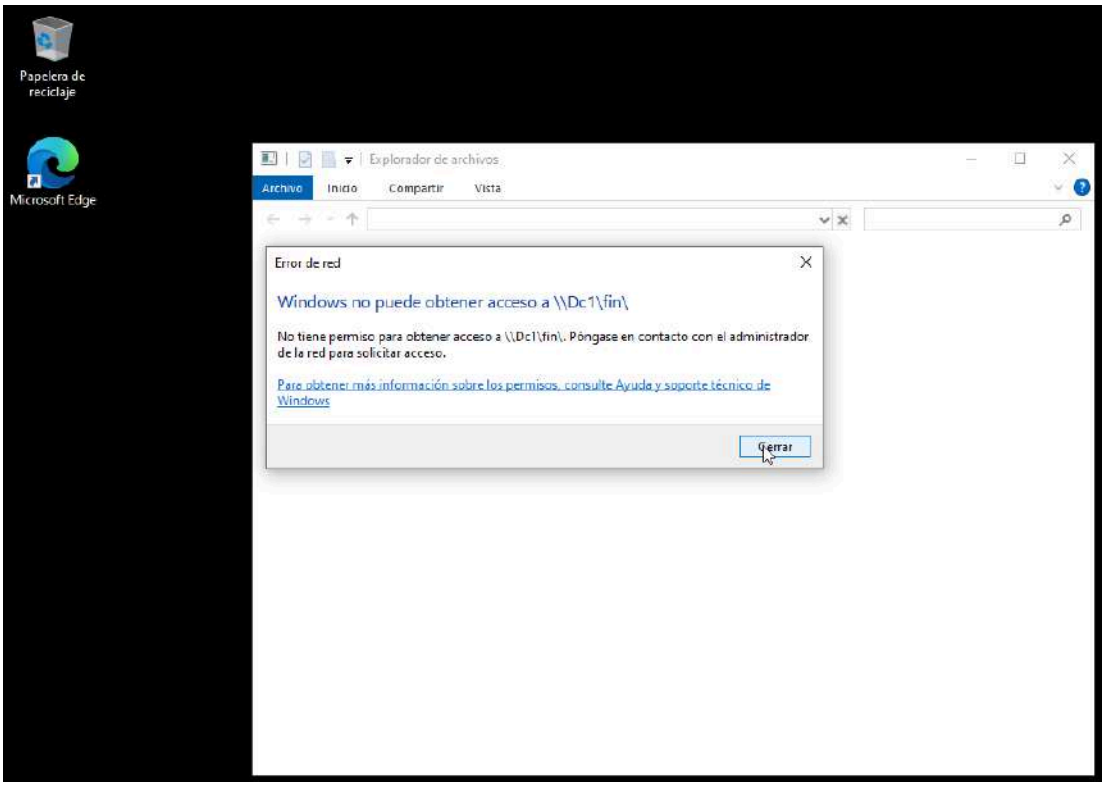
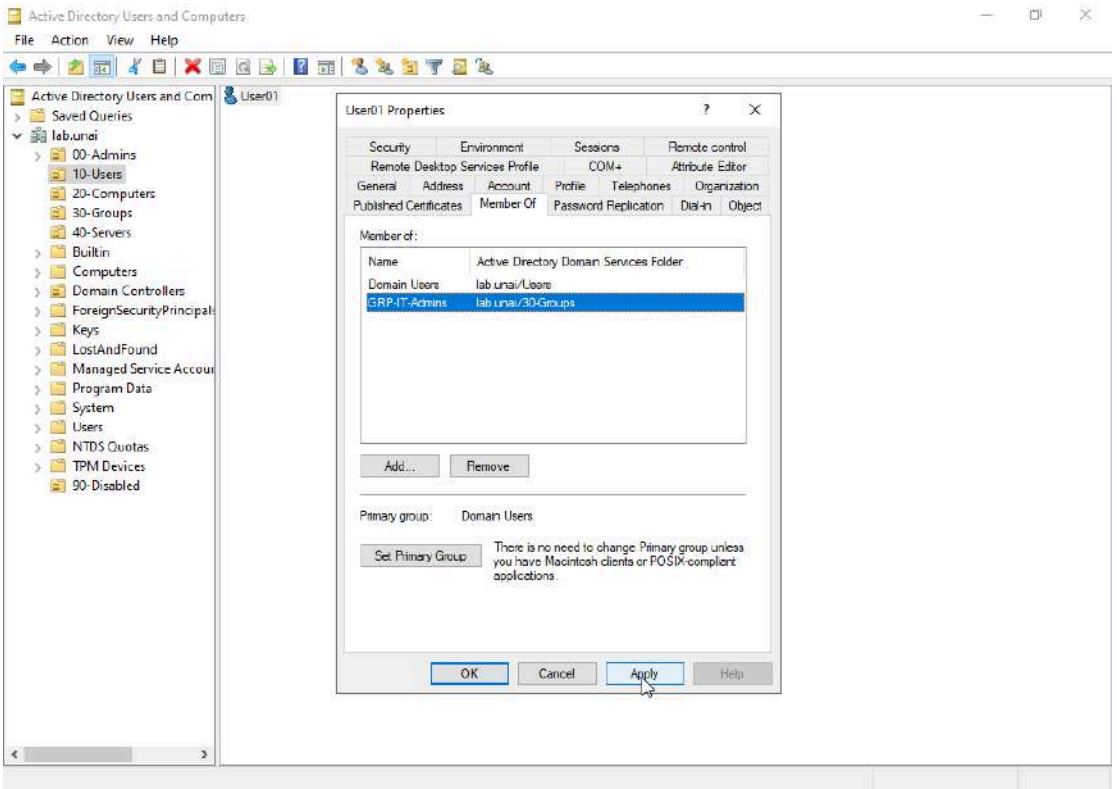


Figure 5.5.10 – Updated group memberships for the user in ADUC.



5.5.4.4 Result

- Role change fully effective without touching infrastructure.
- Access controlled exclusively through groups.
- Clean, scalable, and maintainable model.

5.5.5 Operational observations

- Access to resources depends on the session token, not on immediate AD changes.
- Group changes require logoff/logon.
- The issues observed were not:
    - NTFS errors
    - GPO failures
    - Share configuration problems

Technical value:

- Reinforces the real Windows security model.
- Avoids unnecessary troubleshooting on the infrastructure layer.
- Documents reasoning as well as execution.

5.5.6 Final status of the sub-block

User02

- No access groups.
- Moved to **90-Disabled**.
- Account disabled.

User01

- Active user.

- Group membership aligned with current role.
- Access validated from the client.

Operations performed

- No direct permissions assigned to users.
- No manual changes on resources.
- No adjustments outside Active Directory.

6. Design decisions and conclusions

6.1 Design decisions and scope

Throughout the project, deliberate decisions were made to avoid artificial complexity and to maintain the focus on real operational competencies aligned with what is expected in a small-to-medium corporate environment.

The following components were not implemented:

- Second Domain Controller
- DFS (Distributed File System)
- Complex Active Directory delegations
- Overly granular permissions or direct user-based ACLs

The technical justification is straightforward: the objective of the project is to demonstrate correct administration, realistic troubleshooting, and coherent use of best practices. Adding more components would not have delivered proportional value within the defined scope and would have shifted the effort away from real operational work toward unnecessary complexity.

The result is a coherent and well-scoped lab that can be confidently defended in an interview, with a clear focus on Active Directory, Group Policy, group-controlled permissions, and real troubleshooting. The design aligns with the typical responsibilities of a junior–mid systems administrator profile, prioritising sound judgement and method over purely technological breadth.

6.2 Real-world issues addressed

During the execution of the lab, typical scenarios found in Windows environments with Active Directory were reproduced and resolved without resorting to artificial configurations. Examples include:

- Critical dependencies between Active Directory and DNS, on both the Domain Controller and the client
- Logon failures caused by disabled accounts or active policies
- Group Policy behaviours related to:
    - Incorrect OU linkage
    - Differentiation between User Configuration and Computer Configuration

    - Group filtering (Security Filtering / targeting)

- Access issues to shared resources resulting from:
    - Incorrect group memberships
    - User tokens not being refreshed
- Network failures that appear ambiguous (“there is an IP, but nothing works”), properly isolating DNS, gateway, and the true scope of the issue

All scenarios were diagnosed using method and technical reasoning, rather than trial-and-error.

6.3 Consolidated technical learnings

Several key principles of system administration were reinforced through the project:

- Active Directory is a matter of **design**, not just object creation
- DNS is the **foundation of the domain**: if DNS fails, everything fails
- GPOs must be understood through **scope**, not intuition
- Permissions should always be managed through **groups**, not directly assigned to users
- The user logon token explains many access issues that are not infrastructure failures
- `gpresult` is sufficient for effective troubleshooting in junior–mid environments when used correctly
- Increasing complexity rarely fixes problems; understanding context does

These learnings were strengthened through real validations from the client side and direct observation of system behaviour.

6.4 Professional value of the project

This lab demonstrates the ability to build a functional Windows infrastructure from scratch, manage Active Directory with sound judgement, implement useful and verifiable GPOs, control permissions in a professional way, and diagnose real incidents methodically.

The project does not seek to be extensive or spectacular, but **correct**. It reflects a mindset consistent with production environments: justified decisions, clean execution, and clear,

defensible documentation. The result is a solid foundation on which more complex environments can be built without changing the mental framework or methodology applied.

6.5 Potential future extensions

Natural extensions of the environment have been identified, although they are not required for the current scope:

- Second Domain Controller
- Delegation of control by OU
- Fine-Grained Password Policies
- Separation of File Server and Domain Controller
- Advanced auditing

These extensions are considered evolutionary and optional, not essential to demonstrate the competencies covered in this project.