WINDOWS SERVER DOMAIN SETUP WITH GPOS AND DRIVE MAPPING

Active Directory, GPO Management, and Drive Mapping Automation

Summary

This project set up a Windows Server domain with OUs, Security Groups, and users for different departments. I used PowerShell to automate repetitive tasks like creating users and mapping drives, while Group Policy Objects (GPOs) were applied to enforce both domain-wide security and department-specific settings.

Tebogo Matseding

tmatseding@outlook.com

Table of Contents

Ensure GPOs are updated

Verify GPO mapping was created

Installing DHCP server

Set scope

Install print server

Configure printers and deploy them on GPOs

Point PC1 DNS to DC

Rename PC1 and join to domain

Signing in with domain users

Map the disk

Verify the disk was added

Verify that it denies those without authorization

Adding Printers

Verify Printer rules are applied

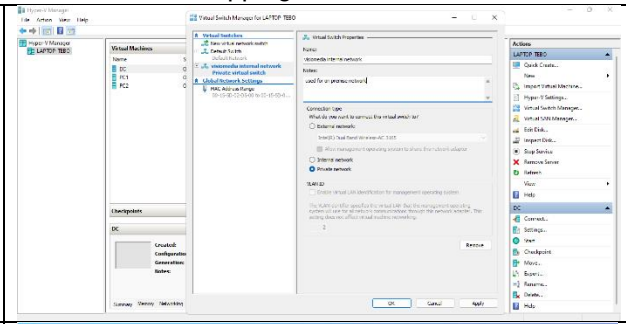
Verify Printer allows access to those who are authorized

Introduction

This project is mainly focused on Group Policy Objects (GPOs) and drive mapping. While ADDS, DHCP, and other roles were installed, the emphasis is on enforcing domain-wide security and department policies. Scripts for users, OUs, SGs, and drive mappings are included as references.

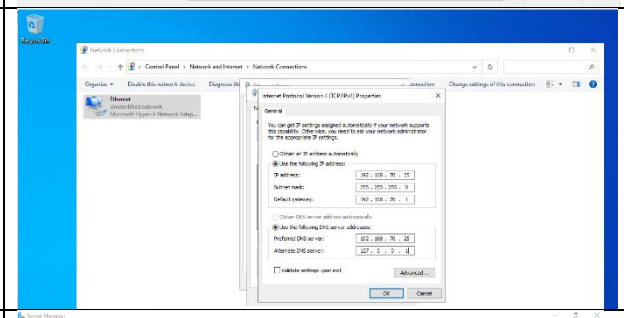
Create a Private Network

Created a private network to isolate the environment for domain testing.



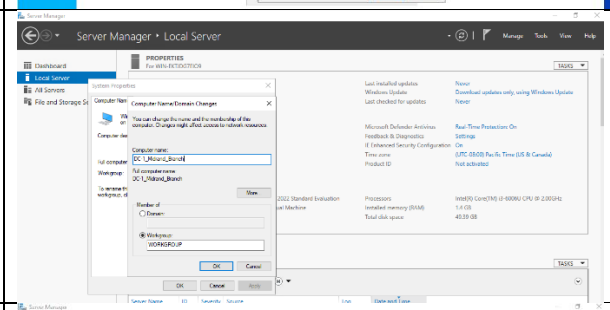
Assigning the server, a static address

Assigned the domain controller a static IP to ensure stability for DNS, DHCP, and domain authentication.



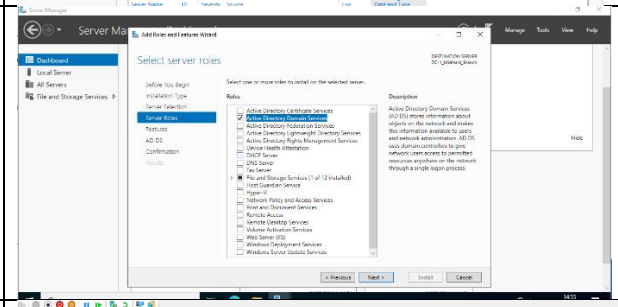
Assigning the server, a new name

Renamed the server to a clear naming convention for easy identification across the domain.



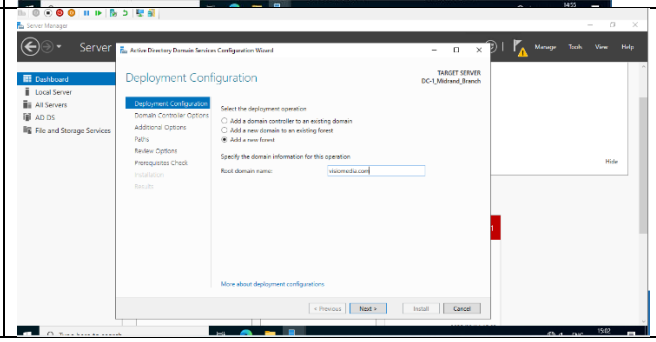
Adding ADDS Feature

Installed the Active Directory Domain Services role to manage users and resources.



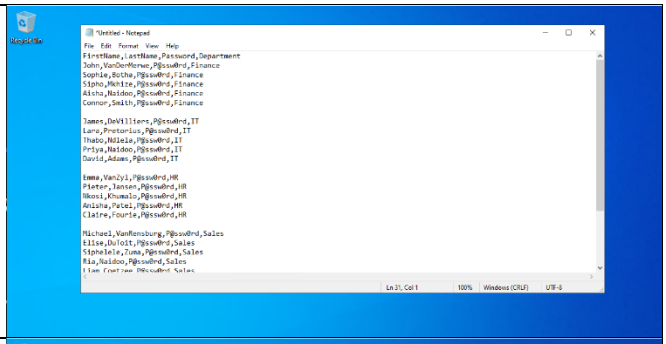
Promoting the server to a domain controller

Configured the server as the primary domain controller for the environment. This enabled centralized management of authentication and policies.



CSV File

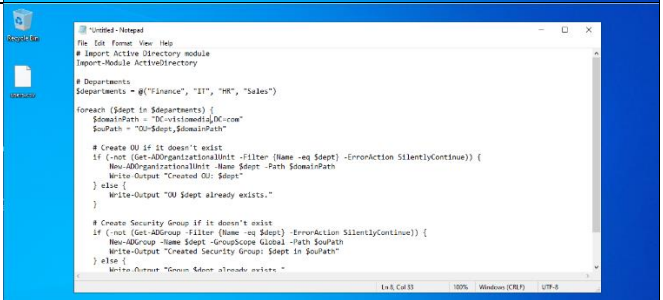
CSV file prepared with user details. I created this file in another project and if you are interested in using it here is the link:



OU and SG script

Created a PowerShell script to automatically build Organizational Units and Security Groups for IT, Sales, Finance, Marketing, and HR.

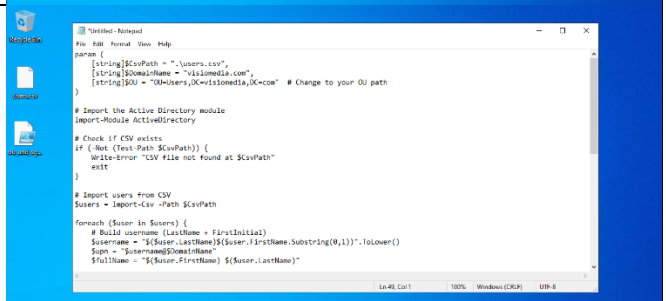
Link to script:



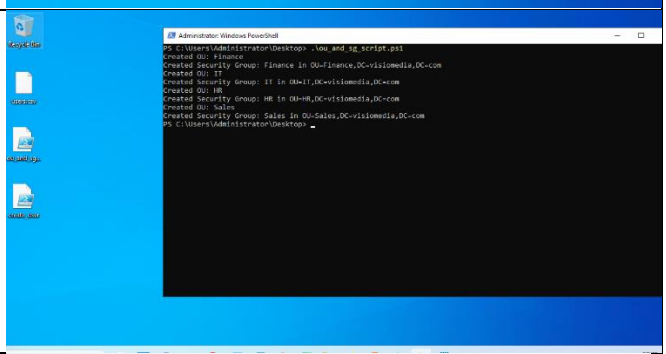
User creation script

Used a PowerShell script to bulk-create domain users with a naming format of **<LastName><FirstInitial>@domain.com** Each user was added to their department's Security Group.

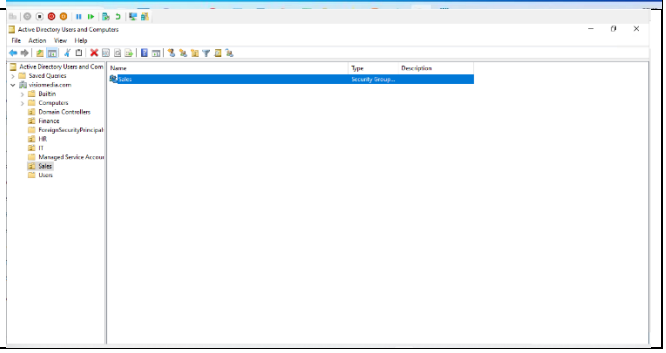
Link to script:

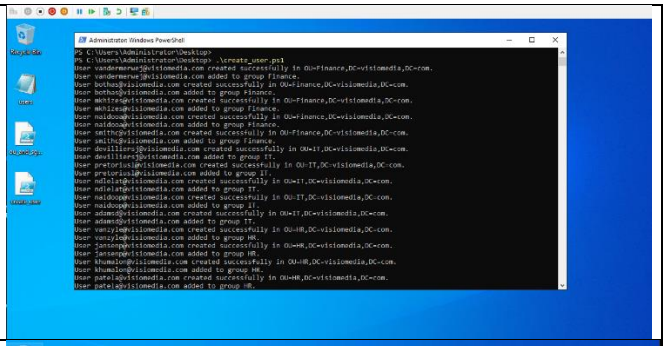
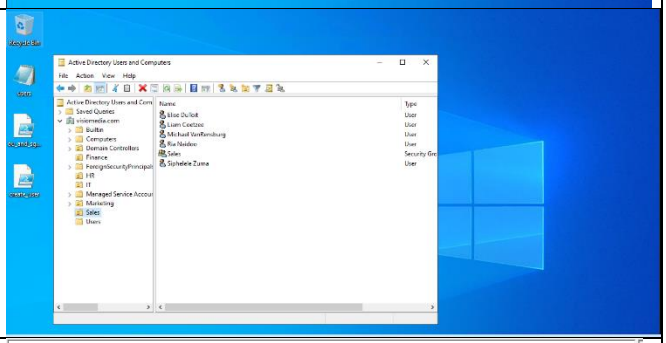
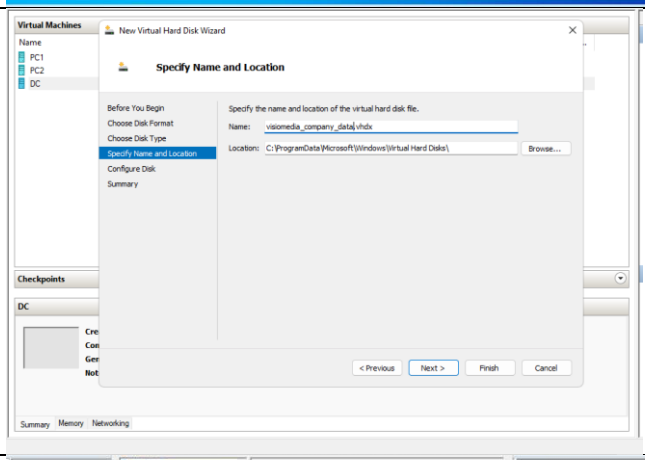
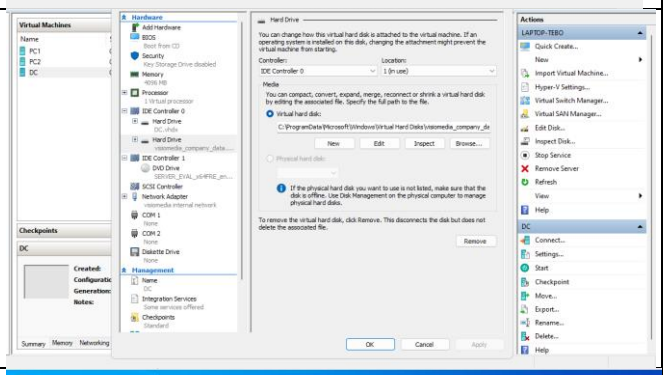
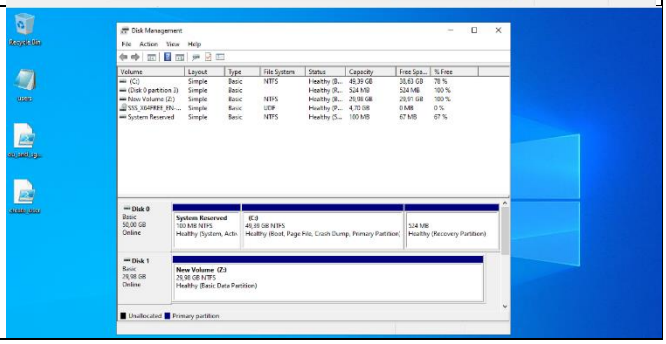


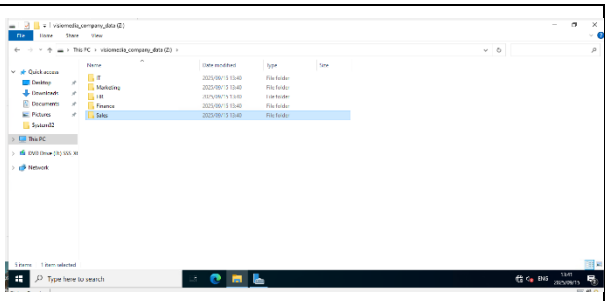
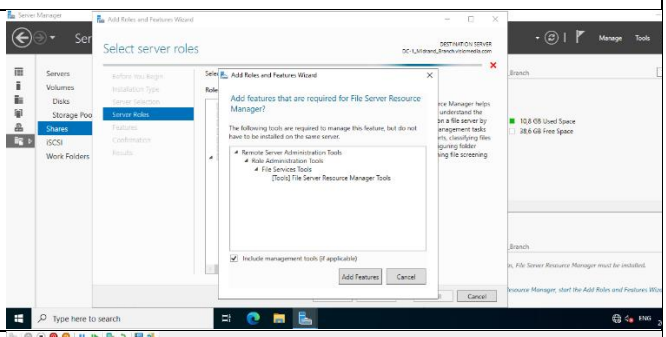
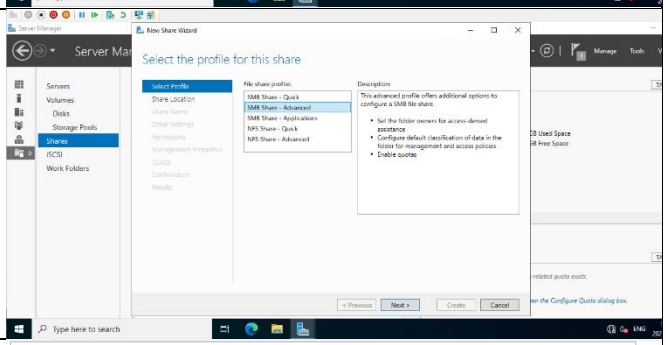
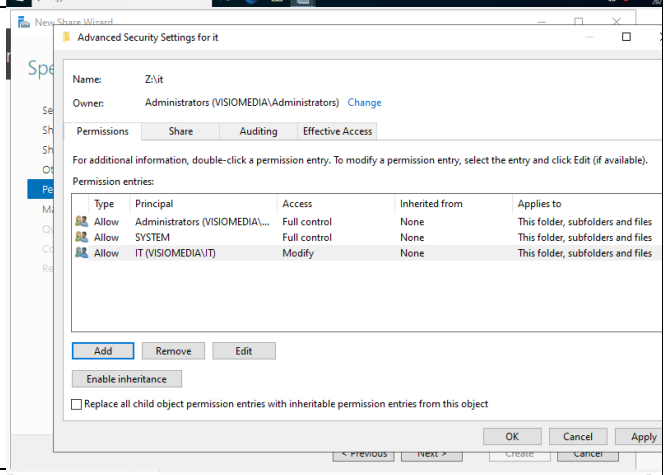
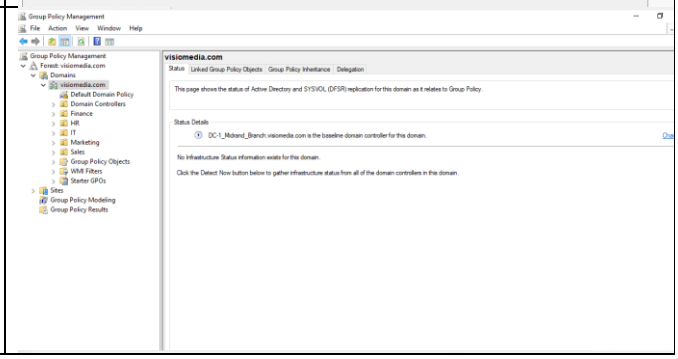
OU and SG script worked



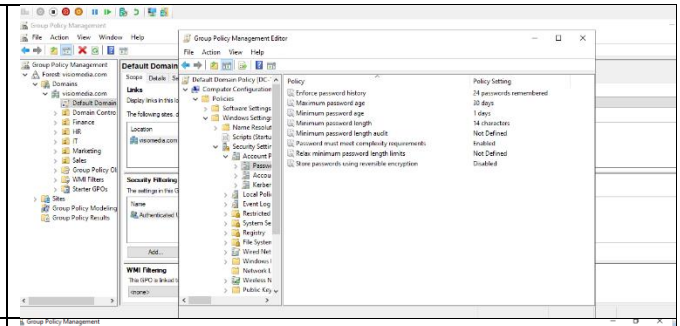
Verify OUs and SGs were created



User creation script worked	
Verify creation of users	
Create storage disk	
Adding hard disk to my DC	
Initialize the disk	

Creating folders Created folders for IT, Sales, Finance, Marketing, and HR to store departmental files.	
Install file server Enabled the File Server role to support SMB shares.	
Configure shares Each folder was shared over SMB and assigned NTFS permissions so only the respective department and administrators could access it.	
Allow certain access to authorized users	
Group Policy Management	

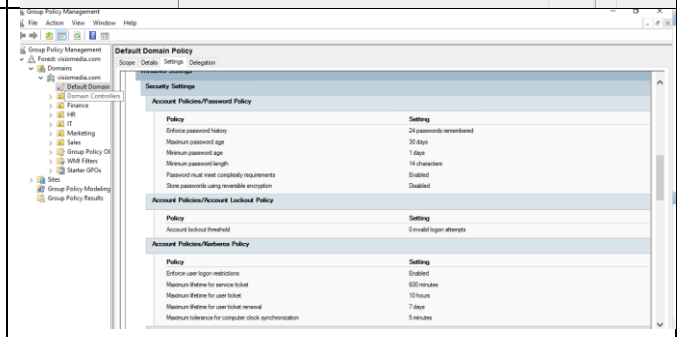
Set default policies



Default Polices overview

Enforced baseline organization-wide rules:

- Minimum 12-character password
- Complexity required
- Password expiry every 90 days
- Account lockout after 5 failed attempts (15 min)
- Guest account disabled
- Enable auditing for logon/logoff and changes
- Windows Updates forced automatically



GPOs for the rest of my department

Finance GPO
Deny execute access to removable disks
Deny read access to removable disks
Deny write access to removable disks
Drive mapping applied

HR GPO
Sleep timeout (on battery)
Unattended sleep timeout (on battery)
Attended sleep timeout (plugged in)
Drive mapping applied

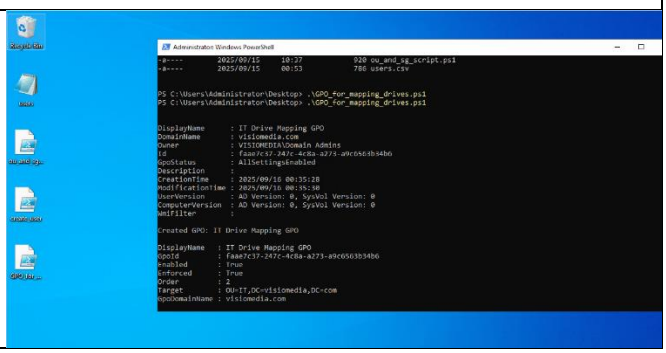
IT GPO
Added administrators to roaming profiles
Drive mapping applied

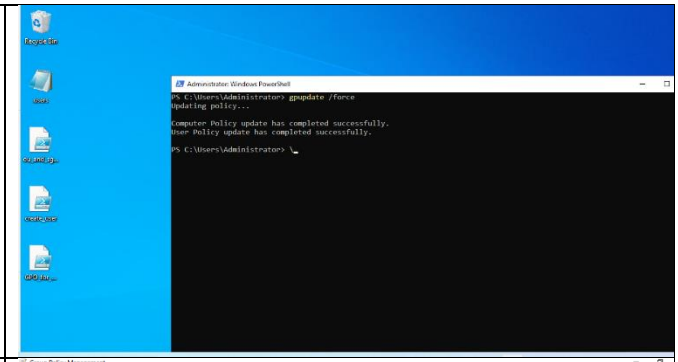
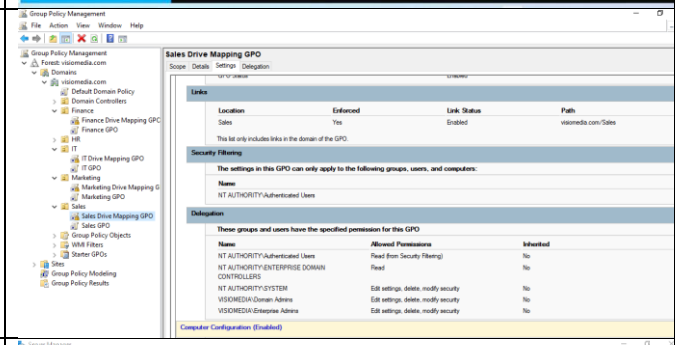
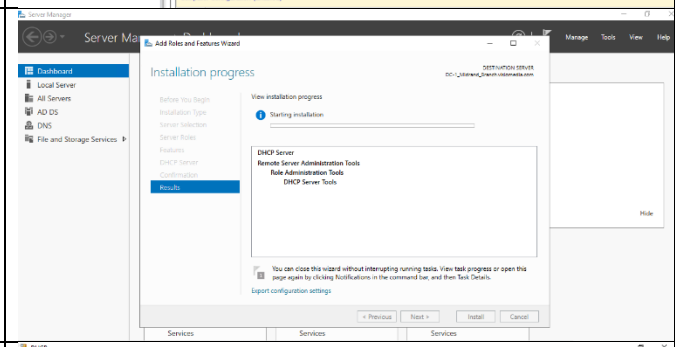
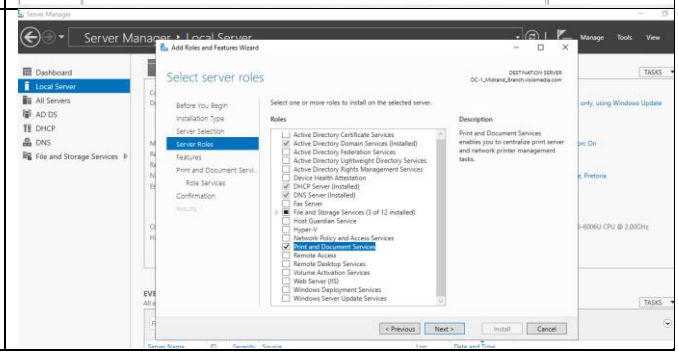
Sales GPO
Prevent deleting browsing history
Disable InPrivate browsing
Drive mapping applied

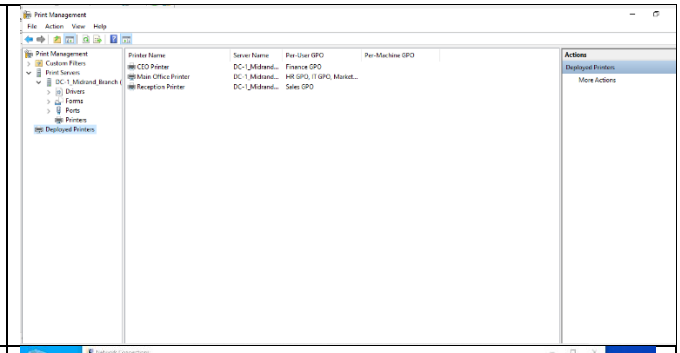
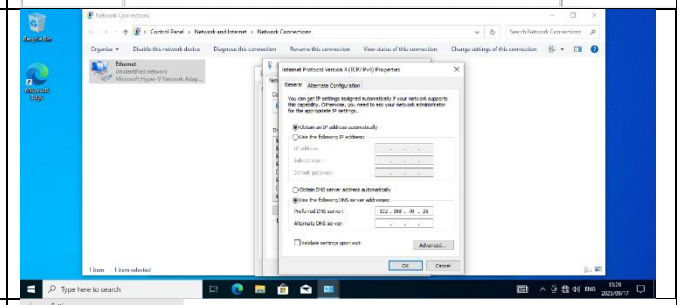
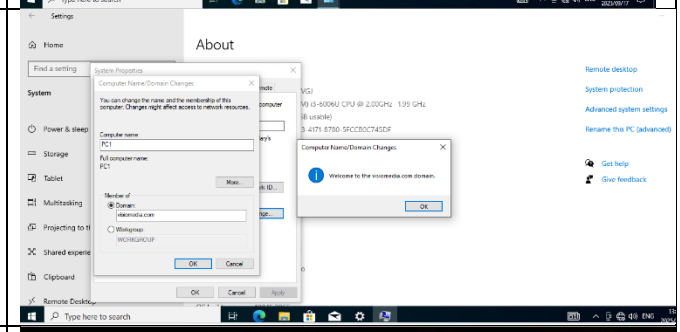
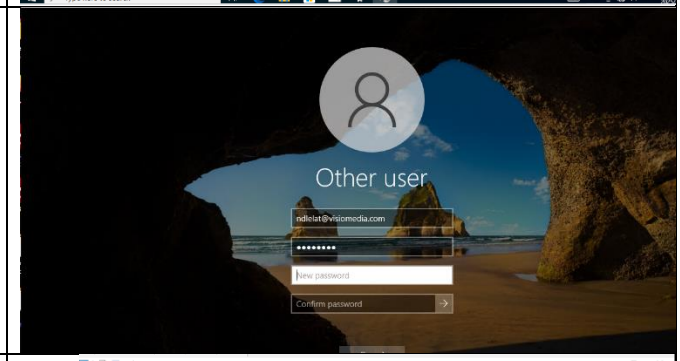
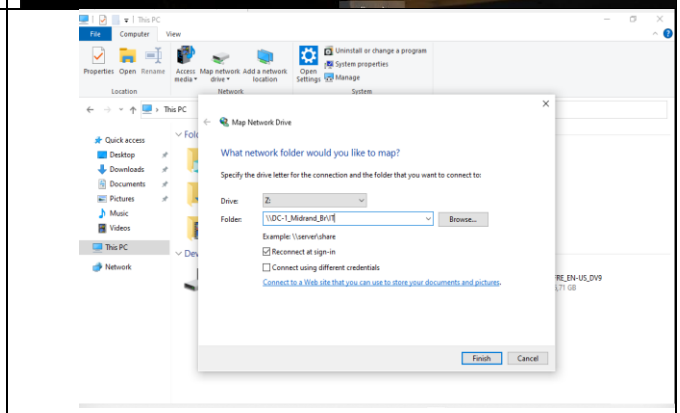
Marketing GPO
Block access to Microsoft Store
Disable OneDrive for storage
Drive mapping applied

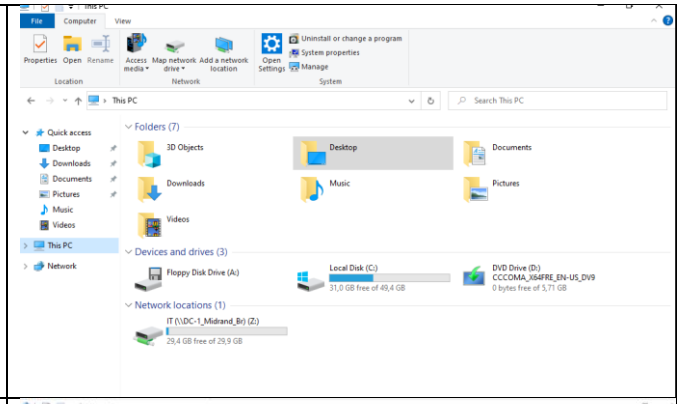
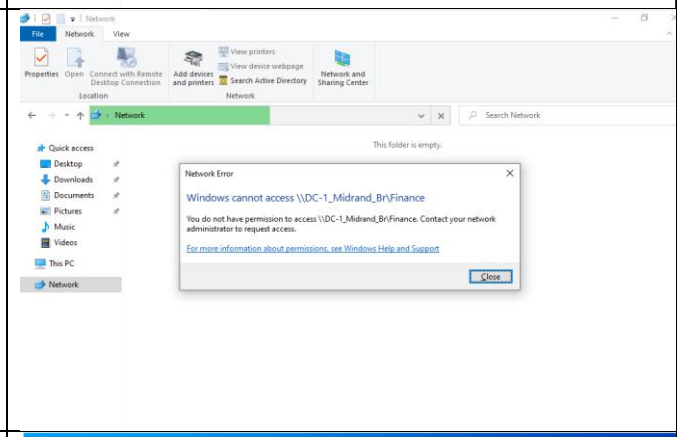
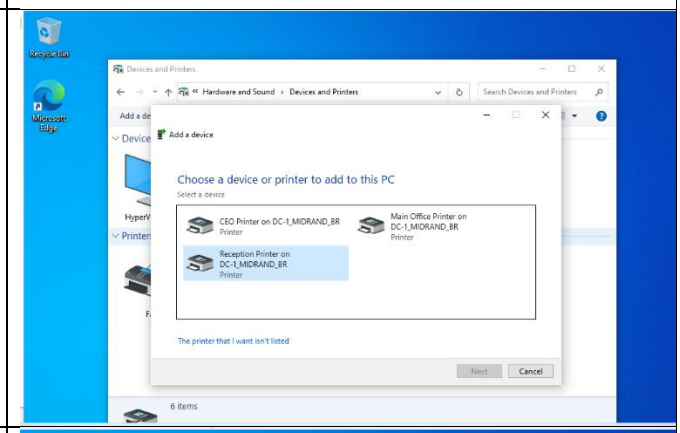
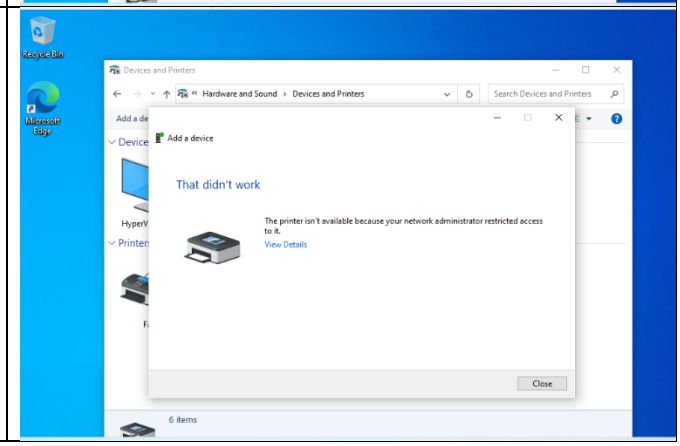
Creating Maps for Disks

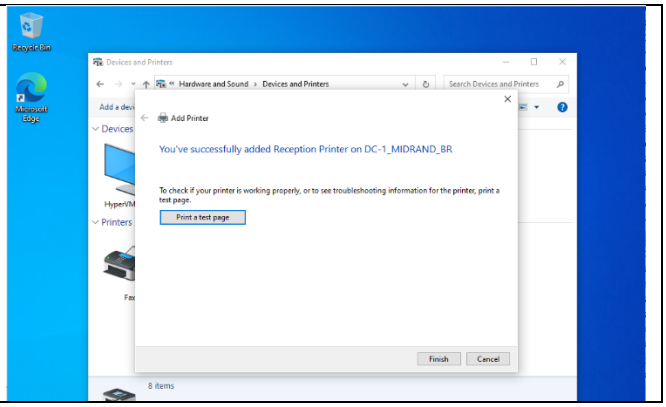
Created a script that built GPOs for each department to map their SMB shares to dedicated drive letters



Ensure GPOs are updated Ran gpupdate /force on clients and confirmed that mapped drives appeared automatically for users in the correct OU.	
Verify GPO mapping was created	
Installing DHCP server Added the DHCP role to the DC.	
Set scope Defined a scope for client IP addresses. Reserved addresses were set aside for the DC and network printers to prevent conflicts.	
Install print server	

Configure printers and deploy them on GPOs Printers were deployed through GPOs so users in specific OUs had access automatically.	
Point PC1 DNS to DC	
Rename PC1 and join to domain	
Signing in with domain users	
Map the disk	

Verify the disk was added	
Verify that it denies those without authorization	
Adding Printers	
Verify Printer rules are applied	

Verify Printer allows access to those who are authorized	

Project Summary

This project successfully built a Windows Server domain environment with a focus on Active Directory structure, GPO enforcement, and resource management. The domain controller was set up with OUs and Security Groups for multiple departments, and PowerShell was used to automate repetitive tasks such as creating users and drive mappings. File shares and printers were configured with appropriate access restrictions, and DHCP was deployed to provide consistent IP addressing with reservations for critical devices.

Group Policy Objects (GPOs) formed the core of the project — enforcing both organization-wide security baselines (password policies, auditing, Windows Updates) and department-specific rules tailored to IT, Finance, HR, Marketing, and Sales. Testing from a domain-joined client confirmed that users received mapped drives, printers, and policy restrictions automatically, while unauthorized access was blocked.

Overall, the project demonstrated how automation and GPOs can simplify management while maintaining a secure and organized Windows Server environment.

Improvements & Next Steps

There are several areas where this project could be improved or expanded:

Add Redundancy

- Deploy a second Domain Controller for fault tolerance.
- Configure DHCP failover for high availability.

Advanced GPOs

- Add software deployment via GPO (example: install apps automatically for departments).
- Apply stricter firewall and security baselines using Microsoft Security Baseline templates.

Monitoring & Auditing

- Enable centralized event log forwarding.
- Configure audit policies to monitor file access and administrative changes more closely.

Backup & Recovery

- Automate system state backups for Active Directory.
- Test restore scenarios to ensure recovery in case of corruption.

User Experience Enhancements

- Add folder redirection or roaming profiles to centralize user data.
- Configure logon/logoff scripts for additional automation.

Migration Practice (Future Goal)

- Simulate migrating ADDS roles to another DC.
- Test FSMO role transfers and AD restores.